EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Program on Technology Innovation: Early Integration of Safety Assessment into Advanced Reactor Design

Preliminary Body of Knowledge and Methodology

2018 TECHNICAL REPORT

Program on Technology Innovation: Early Integration of Safety Assessment into Advanced Reactor Design

Preliminary Body of Knowledge and Methodology

3002011801

Final Report, September 2018

EPRI Project Manager
A. Sowder

All or a portion of the requirements of the EPRI Nuclear Quality Assurance Program apply to this product.

YES (NO)

ELECTRIC POWER RESEARCH INSTITUTE
3420 Hillview Avenue, Palo Alto, California 94304-1338 ▪ PO Box 10412, Palo Alto, California 94303-0813 ▪ USA
800.313.3774 ▪ 650.855.2121 ▪ askepri@epri.com ▪ www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATION(S) BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCUMENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

REFERENCE HEREIN TO ANY SPECIFIC COMMERCIAL PRODUCT, PROCESS, OR SERVICE BY ITS TRADE NAME, TRADEMARK, MANUFACTURER, OR OTHERWISE, DOES NOT NECESSARILY CONSTITUTE OR IMPLY ITS ENDORSEMENT, RECOMMENDATION, OR FAVORING BY EPRI.

THE FOLLOWING ORGANIZATIONS, UNDER CONTRACT TO EPRI, PREPARED THIS REPORT:

Vanderbilt University

University of California at Los Angeles (UCLA)

THE TECHNICAL CONTENTS OF THIS PRODUCT WERE **NOT** PREPARED IN ACCORDANCE WITH THE EPRI QUALITY PROGRAM MANUAL THAT FULFILLS THE REQUIREMENTS OF 10 CFR 50, APPENDIX B. THIS PRODUCT IS **NOT** SUBJECT TO THE REQUIREMENTS OF 10 CFR PART 21.

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

Electric Power Research Institute, EPRI, and TOGETHER…SHAPING THE FUTURE OF ELECTRICITY are registered service marks of the Electric Power Research Institute, Inc.

Copyright © 2018 Electric Power Research Institute, Inc. All rights reserved.

ACKNOWLEDGMENTS

The following organizations, under contract to the Electric Power Research Institute (EPRI), prepared this report:

Vanderbilt University
Department of Civil and Environmental Engineering
2301 Vanderbilt Place
Nashville, TN 37235

Principal Investigators
S. Krahn (project lead)
C. Leach
B. Chisholm
A. Croff
P. Marotta

University of California at Los Angeles (UCLA)
B. John Garrick Institute for the Risk Sciences
School of Engineering
404 Westwood Plaza
Los Angeles, CA 90095

Principal Investigators
K. Fleming
D. Johnson

This report benefitted from an independent technical review by Richard Wachowiak, Principal Technical Leader in EPRI's Risk and Safety Management Program, and from comments from Joe Donahue, Vice President of Nuclear Energy for Duke Energy.

This report describes research sponsored by EPRI.

This publication is a corporate document that should be cited in the literature in the following manner:

Program on Technology Innovation: Early Integration of Safety Assessment into Advanced Reactor Design—Preliminary Body of Knowledge and Methodology. EPRI, Palo Alto, CA: 2018. 3002011801.

ABSTRACT

Many advanced reactor concepts employ combinations of coolants, fuels, materials, and power conversion technologies that, if commercialized, could offer new options and substantial improvements in terms of safety, economics, performance, and long-term energy security. However, many technology developers—especially those new to nuclear—face substantial challenges in building a safety case in a balanced, incremental manner for technologies that have limited or no licensing and operational track records, incorporate novel design elements, and may include unique radiological and non-radiological source terms. Concurrently, most tools and methods available to evaluate the safety of nuclear technology slated for commercialization have been developed and applied in a back-fit fashion and are largely based on experience from light water reactor (LWR) technology development, licensing, and operations. Any embedded technology and regulatory mindset may limit flexible and efficient application to novel design concepts and new operational paradigms.

Early integration of safety assessment into the design process via the application of fit-for-purpose tools and methods should support efficient design iteration and improvement as well as productive engagement with regulatory authorities. In addition, advanced nuclear technology development would benefit from a technology-neutral approach that utilizes hazards identification, risk characterization, and design integration techniques in a coordinated and efficient process—from conceptual design through start of operations.

In light of challenges and concerns identified via engagement with advanced reactor developers and other stakeholders, EPRI seeks to define an approach and assemble best practices based on established process hazard analysis (PHA) methods to initiate and facilitate the design-to-license process. Established qualitative and semi-quantitative PHA methods offer a practical means to begin the development of the building blocks needed to support more quantitative design evaluations, including probabilistic risk assessment (PRA). The intent is to benefit from risk-based insights early in the design process and to incrementally develop and quantify the safety design basis as the reactor design matures.

This report assembles best practices for and defines a structured incremental, iterative, and balanced approach to safety assessment of advanced reactor designs. The approach emphasizes the application of established, internationally recognized tools—including PHA and PRA methods—and complements ongoing efforts to integrate risk-informed, performance-based approaches into advanced reactor design and licensing.

Keywords

Advanced nuclear reactors
Advanced nuclear technology
Advanced reactor design
Probabilistic risk assessment (PRA)
Process hazard analysis (PHA)
Safety assessment methods

Deliverable Number: 3002011801

Product Type: Technical Report

Product Title: Program on Innovation Technology: Early Integration of Safety Assessment into Advanced Reactor Design—Preliminary Body of Knowledge and Methodology

PRIMARY AUDIENCE: Advanced reactor developers and vendors

SECONDARY AUDIENCE: Regulatory authorities, potential owner-operators, and other stakeholders with an interest in the evaluation of advanced reactor technologies

KEY RESEARCH QUESTION

Reactor developers seeking advanced reactor design certification and/or licensing face challenges in developing a safety case because many designs come with limited to no commercial operating experience, incorporate novel design elements, and may include unique radioactive material inventories as well as other non-traditional hazards. Established qualitative and semi-quantitative process hazard analysis (PHA) methods provide a bridge to more quantitative analysis, including probabilistic risk assessment (PRA). These methods are ideal as they are amenable to numerous iterations, are adaptable to any design maturity and level of detail, and can be used to generate event trees and fault trees.

RESEARCH OVERVIEW

Advanced nuclear technology development would benefit from a technology-neutral approach that utilizes hazards identification, risk characterization, and design integration techniques in a coordinated and efficient process—from conceptual design through start of operations. This report describes the development and application of hazard analysis methods for evaluation of early-stage advanced reactor designs and is organized around three main elements: a preliminary body of knowledge, a proposed methodology, and treatment of the interface with quantitative risk assessment methods.

- A concise body of knowledge summarizes best practices for and experience with the application of PHA and PRA methods to advanced reactor designs and is organized around seven key topics:
  - Systems Engineering
  - Early Stage Safety Analysis and PHA
  - PRA Model Development
  - Standards for Achieving PRA Technical Adequacy
  - Previous Advanced Reactor PRAs
  - Data Collection and Analysis and Treatment of Uncertainties
  - General and Miscellaneous
- A consolidated methodology is proposed for progressively incorporating established safety assessment tools and methods throughout all advanced reactor design stages to support an optimized design-license-build-operate life cycle.
- A general description is provided of the relationship and interface between qualitative and semi-quantitative hazard analysis tools and more quantitative risk assessment exercises. For simplicity and clarity, the approach and overall project are collectively referred to as “PHA-to-PRA” herein.

KEY FINDINGS

- Sufficient experience exists for conducting analyses early and throughout the design of advanced reactors using tools and methods that are not limited by their legacy of application to specific technologies and regulatory mindsets.
- The PHA-to-PRA process is likely to begin by focusing on subsets of systems (or subsystems) that have been selected on the bases of available information and anticipated relative importance to safety risk, performance risk, cost and schedule to develop, and cost to change.
- Experience to date with the development of a structured approach to the application of standard hazard assessment methods suggests substantial benefit and value are realized through the following:
  - Comprehensive identification of physical and chemical phenomena important to safety
  - Early and iterative utilization of PHA and quantitative consequence analysis
  - Incremental development of PRA building blocks
  - Identification of technology-relevant risk metrics
  - Early institution of systems engineering in order to perform industry-standard PHA studies of systems, subsystems, and their interfaces
  - Early establishment of a working interface between safety and engineering technologists
- Support for development and implementation of risk-informed, performance-based design and licensing practices

WHY THIS MATTERS

Early application of safety assessment tools and methods during reactor system design can provide real value and facilitate advancement by identifying important knowledge and design performance gaps when changes can be incorporated with the least impact to cost, schedule, and licensing. Insights regarding relative likelihood and severity of event sequences can then be used to adjust design priorities or to consider design alternatives. The PHA-to-PRA process is suited for examination of relevant information developed throughout the design process as it becomes available. The use of other appropriate safety analysis tools should also be considered and may be necessary at times. This work proposes a structured approach and summarizes best practices and experience to assemble existing and proven tools for hazard identification and safety basis development. The goal is to maximize the effectiveness of tools and efficiency of their application by the advanced reactor developer community.

HOW TO APPLY RESULTS

This report provides advanced reactor developers/vendors and other stakeholders with a general overview of the best practices for and experience with PHA and PRA methods as well as a generalized methodology for their application to advanced reactor designs. This work is intended to complement and support existing and new standards and regulatory approaches associated with design, licensing, and operation of advanced reactor technologies. The user may benefit from case studies illustrating application of the methodology to non-LWR technologies that have been documented in conference proceedings and in upcoming EPRI technical publications.

LEARNING AND ENGAGEMENT OPPORTUNITIES

- EPRI has established an Advanced Reactor Technical Advisory Group (TAG) under the Advanced Nuclear Technology Program to provide a forum for exchanging information and obtaining input on the direction and nature of EPRI's strategic focus on advanced reactor technology.
- EPRI continues to seek and welcome collaborative opportunities for the development and application of tools and methods that support commercialization of advanced nuclear technology, including piloting of safety assessment methods on specific advanced reactor designs, systems, and subsystems. Confidence in and maturity of the PHA-to-PRA methodology can be further expanded through continued application and demonstration.

EPRI CONTACTS: Andrew Sowder, Technical Executive, asowder@epri.com

PROGRAM: Advanced Nuclear Technology, 41.08.01, 2018

IMPLEMENTATION CATEGORY: Strategic Long-Term

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com

© 2017 Electric Power Research Institute (EPRI), Inc. All rights reserved. Electric Power Research Institute, EPRI, and TOGETHER...SHAPING THE FUTURE OF ELECTRICITY are registered service marks of the Electric Power Research Institute, Inc.

DEFINITIONS

The following terms, acronyms, and initialisms appearing in figures and text are defined as follows:

AECL – Atomic Energy of Canada Limited

AIChE – American Institute of Chemical Engineers

ANS – American Nuclear Society

ASME – American Society of Mechanical Engineers

BoK – Body of Knowledge

CCPS – Center for Chemical Process Safety

CCS – Component Cooling System

CDF – Core Damage Frequency

CFSRS – Core Fuel Salt Release System

COR – Code of Record

CPI – Chemical Process Inventory

CPQRA – Chemical Process Quantitative Risk Analysis

CSDR – Conceptual Design Safety Report

DBA – Design Basis Accident

DOE – Department of Energy

EPRI – Electric Power Research Institute

ESD – Event Sequence Diagram

ETA – Event Tree Analysis

FHR – Fluoride-Salt-Cooled, High-Temperature Reactor

FMEA – Failure Modes and Effects Analysis

FOM – Figure of Merit

FTA – Fault Tree Analysis

GFR – Gas-Cooled Fast Reactor

HAZOP – Hazards and Operability

HEP – Human Error Probability

HTGR – High Temperature Gas-Cooled Reactor

IAEA – International Atomic Energy Agency

IE – Initiating Event

HTGR – High Temperature Gas-cooled Reactor

INL – Idaho National Laboratory

ISA – Integrated Safety Analysis

ISAM – Integrated Safety Assessment Methodology

LBE – Licensing Basis Event

LERF – Large Early Release Frequency

LFR – Lead-Cooled Fast Reactor

LFTR – Liquid Fluoride Thorium Reactor

LMP – Licensing Modernization Project

LOOP – Loss of Offsite Power

LWR – Light Water Reactor

MHTGR – Modular High Temperature Gas-Cooled Reactor

MLD – Master Logic Diagram

MSFR – Molten Salt Fast Reactor

MSR – Molten Salt Reactor

MSRE – Molten Salt Reactor Experiment

NGNP – Next Generation Nuclear Plant

NPP – Nuclear Power Plan

NRC – Nuclear Regulatory Commission

OGS – Off-gas System

ORNL – Oak Ridge National Laboratory

PDBE – Preliminary Design Basis Event

PHA – Process Hazards Analysis

PIE – Postulated Initiating Event

PIRT – Phenomena Identification Ranking Table

PRA – Probabilistic Risk Assessment

PRC – Plant Response Category

PRISM – Power Reactor Inherently Safe Module

PSA – Probabilistic Safety Assessment

QHO – Quantitative Health Objective

RIE – Representative Initiating Event

RMP – Risk Management Plan

SAC – Specific Administrative Control

SCWR – Super Critical Water Reactor

SDS – Safety Design Strategy

SFR – Sodium-Cooled Fast Reactor

SMP – Safety Management Plan

SSC – Structures, Systems, and Components

TMSR-SF1 – Thorium Molten Salt Reactor, Solid Fuel #1

VHTR – Very High Temperature Reactor

CONTENTS

ABSTRACT ..... **V**

EXECUTIVE SUMMARY ..... **VII**

1 **INTRODUCTION** **1-1**

1.1 Context and Motivation 1-2

1.2 Objective and Scope 1-3

1.3 How to Use this Report 1-4

1.4 References 1-5

2 **OVERVIEW OF PROCESS HAZARD ANALYSIS METHODS** **2-1**

2.1 Selection and Application of PHA Methods 2-1

2.2 Focus on HAZOP Analysis 2-2

2.3 References 2-4

3 **BODY OF KNOWLEDGE** **3-1**

3.1 Systems Engineering 3-2

3.1.1 Background 3-2

3.1.2 Technical Discussion 3-3

3.1.2.1 DOE-STD-1189-2016, DOE Standard on Integration of Safety into the Design Process 3-3

3.1.2.2 ANS/ANSI-53.1-2011, American National Standard: Nuclear Safety Criteria and Safety Design Process for Modular Helium-Cooled Reactor Plants 3-5

3.1.2.3 NUREG/CR-6065, Systems Analysis of the CANDU 3 Reactor 3-5

3.1.2.4 ANS-30.1, Integrating Risk and Performance Objectives into New Reactor Nuclear Safety Designs 3-7

3.1.3 Summary Observations 3-8

3.1.4 References 3-8

3.2 Early Stage Safety Analysis and PHA 3-9

3.2.1 Background 3-9

3.2.2 Technical Discussion 3-10
3.2.2.1 Generation IV International Forum Integrated Safety Assessment Methodology (ISAM) 3-10
3.2.2.2 HAZOP: Guide to Best Practice 3-13
3.2.2.3 Bechtel River Protection Project Low-Activity Waste Plant Nuclear Safety Model 3-14
3.2.3 Summary Observations 3-15
3.2.4 References 3-16
3.3 PRA Model Development 3-17
3.3.1 Background 3-17
3.3.2 Technical Discussion 3-18
3.3.2.1 NUREG/CR-2300, PRA Procedures Guide 3-18
3.3.2.2 NUREG-0492, Fault Tree Handbook 3-19
3.3.3 Summary Observations 3-20
3.3.4 References 3-20
3.4 Standards for Achieving PRA Technical Adequacy 3-21
3.4.1 Background 3-21
3.4.2 Technical Discussion 3-21
3.4.2.1 ASME/ANS Probabilistic Risk Assessment Standard for Advanced Non-LWR Nuclear Power Plants 3-21
3.4.2.2 U.S. NRC Regulatory Guide 1.200, An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities 3-23
3.4.2.3 IAEA TECDOC-1804, Attributes of Full Scope Level 1 Probabilistic Safety Assessment (PSA) for Applications in Nuclear Power Plants 3-25
3.4.3 Summary Observations 3-26
3.4.4 References 3-27
3.5 Previous Advanced Reactor PRAs 3-27
3.5.1 Background 3-27
3.5.2 Technical Discussion 3-28
3.5.2.1 PRISM PRA 2017, Development of Advanced Non-LWR PRAs 3-28
3.5.2.2 Modernization of Technical Requirements for Licensing of Advanced Non-Light Water Reactors: Probabilistic Risk Assessment Approach 3-30
3.5.3 Summary Observations 3-33
3.5.4 References 3-33
3.6 Data Collection and Analysis and Treatment of Uncertainties 3-34
3.6.1 Background 3-34

3.6.2 Technical Discussion 3-35
3.6.2.1 Guidelines for Process Equipment Reliability Data (with Data Tables) 3-35
3.6.2.2 IAEA-TECDOC-478, Component Reliability Data for Use in Probabilistic Safety Assessment 3-36
3.6.2.3 'Expert Information' versus 'Expert Opinions'- Another Approach to the Problem of Eliciting/Combining/Using Expert Knowledge in PRA 3-38
3.6.2.4 NUREG-1855, Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decision-making 3-39
3.6.3 Summary Observations 3-40
3.6.4 References 3-40
3.7 General and Miscellaneous 3-41
3.7.1 Background 3-41
3.7.2 Technical Discussion 3-42
3.7.2.1 IAEA-TECDOC-CD-1749, Defense-in-Depth – Advances and Challenges for Nuclear Installation Safety 3-42
3.7.2.2 IAEA-TECDOC-626 Safety-Related Terms for Advanced Nuclear Plants…… 3-43
3.7.2.3 NUREG/CR-1278, Handbook of Human Reliability Analysis 3-44
3.7.3 Summary Observations 3-45
3.7.4 References 3-45

***4* PRELIMINARY PHA-TO-PRA METHODOLOGY 4-1**
4.1 Approach to Qualitatively Assess Hazards and Mitigating Features 4-1
4.2 Application of PHA Results to Meet PRA Input Needs 4-2
4.2.1 System Characterization 4-7
4.2.2 Considerations for Using PHA Results 4-8
4.2.3 Design Insights from PHA-to-PRA 4-10
4.3 Demonstrating the Methodology 4-10
4.3.1 Case Study on the MSRE 4-10
4.3.2 Pilot Application on an Advanced Reactor Design 4-11
4.4 Summary 4-11
4.5 References 4-12

***5* MOVING FROM EARLY SAFETY ANALYSIS TO PRA 5-1**
5.1 References 5-4

***A* RESUMES OF PROJECT TEAM MEMBERS A-1**

LIST OF FIGURES

Figure 4-1 Integration of safety-in-design: Sample iteration of PHA-to-PRA inputs.....4-3
Figure 5-1 Visualized scheme for progression from early safety analysis to PRA.....5-1

LIST OF TABLES

Table 3-1 Summary of selected advanced non-LWR PRAs 3-28
Table 4-1 Relationship of PHA outputs to PRA inputs 4-4

1
INTRODUCTION

Public and private sector interest in advanced nuclear reactor technologies is growing as planners, policy makers, and leaders in government and commercial sectors recognize the value of future technology options for scalable, dispatchable, concentrated, and low-emission energy generation. Many advanced reactor concepts employ a combination of new coolants, fuels, materials, and power conversion technologies that, if commercialized, could offer substantial improvements over current generation technology in terms of safety, economics, performance, and long-term energy security. However, advanced nuclear energy technologies will only be commercialized if they can be licensed by regulatory authorities in the country where they are to be deployed. In pursuing this goal, many technology developers – especially those new to nuclear – face substantial challenges building a safety case in a balanced, incremental manner for technologies that feature limited or no licensing and operational track record, novel design elements, and unique radiological and non-radiological source terms.

Early integration of safety assessment via the application of fit-for-purpose tools and methods can support a more efficient design process and support engagement with regulatory authorities for licensing. Based on challenges and concerns raised by developers and other stakeholders, EPRI seeks to define an approach and assemble best practices based on proven Process Hazard Analysis (PHA) methods to initiate and facilitate the design-to-license process. Established qualitative and semi-quantitative PHA methods offer a practical means to begin the development of the building blocks needed to support Probabilistic Risk Assessment (PRA)[1] of advanced reactor designs. The intent is to benefit from risk-based insights early in design and to incrementally develop and quantify the safety design basis as the reactor design matures. Accordingly, EPRI aims to develop an approach to address a number of identified gaps and needs, including the following.

- Most of the methods, standards, and tools available to evaluate and license the safety of commercial nuclear power facilities are based on the experience gained from light water reactor (LWR) technology development, licensing, and operations. The embedded LWR mindset may not be sufficiently flexible or technology-neutral to allow for efficient application to advanced reactor designs.
- The various tools and methods for hazard identification and safety basis development have not been coordinated into a streamlined process that maximizes their effectiveness and efficiency for application early in the design process.

[1] The term Probable Risk Assessment (PRA) is used throughout this report; however, the term Probabilistic Safety Assessment (PSA) is frequently used internationally. The two are considered to be interchangeable for the purposes of this work.

- Advanced nuclear power technology development can benefit from a technology-neutral approach to safety-in-design that utilizes hazards identification, risk characterization, and design integration techniques in a coordinated and efficient process from conceptual design through start of operations.

For simplicity and clarity, the term “PHA-to-PRA” is used to refer to proposed approach and overall project throughout this report.

1.1 Context and Motivation

The PHA-to-PRA methodology is proposed with the awareness of and intended alignment with existing and developing industry and regulatory activities related to advanced non-light water reactor (non-LWR) technology, as discussed further below. This work also builds on a first-of-a-kind hazard and technology readiness assessment of an early stage liquid-fuel molten salt reactor concept, Flibe Energy’s Liquid-Fluoride Thorium Reactor (LFTR), conducted in collaboration with Southern Company and described in EPRI report 3002005460 [1]. The LFTR assessment laid the foundation for the PHA-to-PRA methodology described in this report via three activities: (1) rendering of preliminary design information into a standardized systems design description format, (2) performance of a preliminary process hazards analysis, and (3) determination of technology readiness levels for key systems and components.

Integration of appropriate safety and risk assessment methods early into the design process for advanced nuclear reactors can provide valuable insights and feedback when changes are less costly. Qualitative and semi-quantitative PHA methods are considered to be well-suited for such applications and can be used to generate outputs that readily support the development of more quantitative models used to estimate risk. Also, use of PHA methods in this manner is consistent with approaches endorsed by the US Nuclear Regulatory Commission (NRC) [2] and the draft ASME/ANS *Standard for Probabilistic Risk Assessment for Advanced Non-LWR Nuclear Power Plan Applications* [3]. The approach is also consistent with international safety-in-design methods, such as the Generation IV International Forum’s Integrated Safety Assessment Methodology (ISAM) [4], and the safety assessment approach recommended by the International Atomic Energy Agency [5]. Developers can benefit from the early use of safety assessment in order to start building the safety case, needed for reactor design certification and licensing, as early as possible. Spreading investment in safety assessment appropriately over the full design development process can reduce technical, financial, and regulatory risks at later stages of reactor design [6].

Regulators can also benefit from the availability of structured safety assessment methods suitable for non-traditional advanced reactor designs. In the United States, the NRC has identified the need to develop the ability to review non-LWR technologies and to identify and resolve technology-inclusive policy issues that impact safety and regulatory reviews of non-LWR nuclear power plants [7]. Likewise, a number of U.S. industry-led groups and initiatives have been established to improve greater communication and coordination of activities among advanced reactor technology stakeholders and to seek improved approaches to licensing and engagement with the NRC [8].

A variety of advanced non-LWR technologies are being pursued globally that encompass a wide range of reactor fuels, coolants, moderators, and heat transfer systems. The Generation IV International Forum (GIF) formally recognizes six reactor systems under the Generation IV (GEN IV) designation: the gas-cooled fast reactor (GFR), lead-cooled fast reactor (LFR), molten salt reactor (MSR), sodium-cooled fast reactor (SFR), supercritical-water-cooled reactor (SCWR), and very-high temperature reactor (VHTR) [9]. Due to the variation among the design details and operating conditions in these reactor designs, the hazard profile associated with each technology can differ greatly. For example, there is significant variability among the fuel material, chemistry, neutron spectrum, and system geometry among specific MSR designs [10]. Each design decision can affect the frequency and consequences associated with a given event sequence, and can produce event sequences that are design specific.

The NRC has expressed the desire to adopt a standard, technology-inclusive approach for reviewing and licensing advanced reactors [11]. In order to allow for a common assessment approach to benefit multiple stakeholders, a flexible, technology-neutral approach to identify hazards and assess risk in the system is desirable. The EPRI PHA-to-PRA project therefore offers one approach to advanced reactor developers for design evaluation, incorporation of safety insights, and incremental construction of a safety case.

Many regulatory requirements are deterministic and/or prescriptive in nature and have origins dating back to the dawn of commercial nuclear power [12, 13]. As a result, the set of accident sequences considered most risk-significant are largely based on commercial reactor designs with extensive operating experience such as LWRs [13]. Because most advanced reactor designs can differ substantially from those comprising the global operating fleet, it is likely that many accident sequences do not apply, and conversely, many risk-significant event sequences for advanced reactors may not be covered by those considered for current commercial designs.

If the applicable hazards of an advanced reactor design can be identified and the risk significance assessed systematically early in the design process, the analysis can lead to design decisions that can help to efficiently mitigate the risk of the most risk-significant accident scenarios. A more comprehensive and risk-informed approach for investigating the risk-significant occurrences is needed to identify those event sequences that should be of greatest priority to the designers in order to assist in verifying that the reactor design will perform the anticipated mission and meet the public health risk safety goals.

1.2 Objective and Scope

In order to define objectives and scope for the PHA-to-PRA project, EPRI held a workshop at Vanderbilt University on July 17-18, 2017 [6]. The workshop included subject matter experts in reactor design, hazard analysis, PRA, risk-informed performance based licensing, and other affiliated domains.

The overall objective defined for the PHA-to-PRA project is to identify, coordinate, and deploy the best available and emerging industry practices in a technology-neutral manner in order to establish a method to integrate safety assessment into the design process for advanced reactors beginning at early stages of development. The intended benefits include:

- The availability of a technique that is not entrenched in LWR technology and, therefore, does not inappropriately de-emphasize or emphasize hazards and phenomena that may or may not apply to other technologies.
- The demonstration of a safety assessment approach that can be efficiently integrated with early stages of design and advance as designs evolve and mature.
- The demonstration of the importance of early integration of safety-in-design for new technologies for the purpose of identifying and prioritizing risk-significant design issues and technical uncertainty. This is intended to aid developers in identifying cost-effective and timely strategies for issue resolution and design maturation, *e.g.*, alternatives analysis, design modifications, earlier formulation of safety function design criteria, additional research, laboratory testing, and scale testing.
- The demonstration of a safety-in-design technique that could support a more risk-informed and performance-based licensing framework and could be used in an incremental step-wise approach to licensing (thereby reducing schedule and scope uncertainty).

A four-phase project emerged from the workshop. Phase 1 of the project is the development of a guide that (1) identifies and documents experience and best practices relevant to integrating safety in design for new nuclear power technology and (2) outlines a general approach for applying appropriate safety assessment tools and methods throughout the design process. **This report represents the deliverable from Phase 1 of the EPRI PHA-to-PRA project.**

Phase 2 of the project involves application of the methodology via one or more case studies for an existing reactor, system, or subsystem design. The lessons learned and methods developed from the case study will then be applied to Phase 3 of the project, a pilot study on a contemporary non-LWR advanced reactor design effort. The pilot study will focus on the interface between design and safety and the incorporation of safety assessment insights into early stages of design. Phases 2 and 3 will be coordinated with the development of ANS Standard 30.1, *Integrating Risk and Performance Objectives into New Reactor Nuclear Safety Design*. A proposed Phase 4 would focus on technology transfer via training on the methodology developed and demonstrated in Phases 1 – 3.

1.3 How to Use this Report

This report describes an overall approach for application of hazard analysis methods for evaluation of early-stage advanced reactor designs and is organized around three main elements: a preliminary “body of knowledge”, a proposed methodology, and treatment of the interface with quantitative risk assessment methods.

Section 2 of this report provides a concise overview of PHA methods and is provided for the reader who may desire an introduction to the subject or a re-introduction that includes recent developments.

Section 3 presents a preliminary Body of Knowledge (BoK) that captures experiences, lessons learned and best practices that reflect a range of nuclear and non-nuclear industries and applications deemed to be most relevant to the development and application of the proposed PHA-to-PRA methodology. Each BoK entry is categorized under one of seven topical areas and provides a summary of key references including noteworthy points about applications or limitations. The BoK also provides secondary references in each knowledge area for more in depth study based on reader interests and needs. Consequently, individual reference lists are provided for each topical area in Section 3 for closer proximity of citations to references.

Section 4 outlines the proposed methodology for application of standard industry hazard analysis methods in the advanced reactor design process. Section 5 describes the role of the PHA-to-PRA methodology in the context of building a balanced nuclear safety case to support and complement established safety assessment methods and design processes.

1.4 References

1. *Technology Assessment of a Molten Salt Reactor Design: The Liquid-Fluoride Thorium Reactor (LFTR)*. EPRI, Palo Alto, CA. October 2015. Report 3002005460.
2. U.S. Nuclear Regulatory Commission. "Policy Statement on the Regulation of Advanced Reactors." *Final Policy Statement*. 73 FR 60612. Washington, D.C., October 7, 2008.
3. *Probabilistic Risk Assessment Standard for Advanced Non-LWR Nuclear Power Plant Applications*. (Trial Use Draft Standard). ASME/ANS RA-S-1.4-2013. American Society of Mechanical Engineers/American Nuclear Society, December 2013.
4. Generation IV International Forum Risk and Safety Working Group. *An Integrated Safety Assessment Methodology (ISAM) for Generation IV Nuclear Systems. (Version 1.1)*. GEN IV International Forum, June 2011.
5. *Procedures for Conducting Probabilistic Safety Assessment for Non-Reactor Nuclear Facilities*. IAEA-TECDOC-1267. Vienna (Austria): International Atomic Energy Agency, 2002.
6. *EPRI Workshop on Process Hazard Analysis to Probabilistic Risk Assessment for Advanced Reactors Proceedings: Vanderbilt University, Nashville, TN, July 18-19, 2017*. EPRI, Palo Alto, CA. October 2017. Report 3002011917.
7. U.S. Nuclear Regulatory Commission. “Policy Issue: Advanced Reactor Program Status.” SECY-18-0011. Washington, D.C., 2018.
8. Cowan, Pamela B. “NEI Activities in Support of Advanced Non-Light Water Reactors.” Letter to the U.S. Nuclear Regulatory Commission. Nuclear Energy Institute, Washington, D.C., January 11, 2017.
9. Generation IV International Forum. *Technology Roadmap Update for Generation IV Nuclear Energy Systems*. Paris (France): OECD Nuclear Energy Agency for Generation IV International Forum, 2014.
10. Dolan, Thomas J., ed. *Molten Salt Reactors and Thorium Energy*. Woodhead Publishing, 2017.

11. U.S. Nuclear Regulatory Commission. “Achieving Modern Risk-Informed Regulation.” SECY-18-0060. Washington, D.C., May 23, 2018.

12. U.S. Nuclear Regulatory Commission. *WASH-1400. The Reactor Safety Study: The Introduction of Risk Assessment to the Regulation of Nuclear Reactors*. NUREG/KM-0010. Washington, DC: Office of Nuclear Reactor Regulation, 2016.

13. Keller, W. and M. Modarres. “A Historical Overview of Probabilistic Risk Assessment Development and Its Use in the Nuclear Power Industry: A Tribute to the Late Professor Norman Carl Rasmussen.” *Reliability Engineering and System Safety*, Vol. 89, No. 3, pp. 271-285 (2005).

2
OVERVIEW OF PROCESS HAZARD ANALYSIS METHODS

PHA techniques for safety analysis were developed within the chemical process industry in the late 1960s and 1970s in response to major industrial accidents. Following the 1984 toxic gas release from a pesticide plant in Bhopal, India, guidance on the use of these techniques was formalized in a technical guide prepared under the auspices of the Center for Chemical Process Safety (CCPS), an applied research group within the American Institute of Chemical Engineers (AIChE) [1]. This benchmark continues to be updated and used widely in industry. The CCPS describes six PHA methods that are considered suitable for assessment of hazardous processes and facilities in varying stages of design and operations. These methods are referenced by both NRC [2] and DOE [3] for hazard analysis of new and modified nuclear facilities and processes.

The six PHA methods explicitly recognized by the CCPS are listed below:

- Checklist Analysis
- What-If Analysis
- Checklist/What-If (Combined) Analysis
- Hazard and Operability (HAZOP) Analysis
- Failure Mode and Effects Analysis (FMEA)
- Fault Tree Analysis (FTA)

2.1 Selection and Application of PHA Methods

The collection of PHA techniques, described in detail in [1], provide a range of methods available to perform industry-standard hazard analyses that span a broad spectrum of applications with respect to design complexity and maturity. Choosing among these options to evaluate safety in a design is based on several factors, notably the design information available for the evaluation, as well as the intended use of the results. Therefore, hazard analysis is intended to be an iterative process; its value is maximized if it is allowed to evolve with the design using methods best suited to design maturity being analyzed. In step form, the PHA process can be characterized by as follows:

Phase I: Identification of Scenarios

a. List processes and systems

b. Perform a preliminary risk ranking of processes and systems

c. Select the appropriate PHA method for each process or system

d. Establish the PHA team by skill set, experience, and project function

e. Select a process or system to be analyzed.

Phase II: Conduct the PHA

a. Assemble the PHA team and train its members

b. Schedule the PHA

c. Conduct the PHA

Phase III: Document the PHA Results and Action Items

a. Report the analysis results and action items

b. Address and track action items to completion

Some PHA techniques are more suited to be performed on systems that are currently in early stages of design. For instance, the "What If" analysis method is well-suited in situations where design information is still quite limited. In the pre-conceptual phase of a design process, "What If" can be used to establish an early technical link between engineering and safety design and to provide initial qualitative insights regarding potential safety concerns as well as a rough relative ranking of those concerns, if desired. As design advances to the conceptual stage, sufficient information becomes available to support application of the HAZOP method. With further additional design detail, use of FMEA and FTA methods become feasible. The more design information that is available, the more detailed and impactful the PHA results become. But even at the conceptual design state, the HAZOP method is acknowledged to produce results that can directly support early PRA development efforts [4]. Because of its extensive application in the PHA-to-PRA methodology, this following discussion will focus on exclusively on the HAZOP method as a logical point of entry for more quantitative assessment.

2.2 Focus on HAZOP Analysis

A HAZOP analysis is a structured and systematic technique to identify potential hazards and operability problems in a facility that features hazardous materials or conditions. A guiding assumption of the HAZOP process is that safety-significant incidents are a result of deviations from normal operating conditions. The HAZOP process is ideally performed by a team of subject matter experts that spans a broad range of relevant technical expertise and includes safety and engineering experts with a thorough understanding of the process and facility design. For advanced nuclear power reactor design, this may include team members with knowledge and experience in nuclear engineering and physics, chemical process engineering, materials science, power plant maintenance and operations, mechanical engineering, electrical engineering, health physics, and toxicology, for instance. Technical depth and breadth, as well as the size of team are factors for optimal technical synergy. The expert team comprehensively and systematically analyzes the available design information to identify possible off-normal events of safety significance [1].

A HAZOP study is conducted using guide words to describe deviations from intended operation in order to facilitate brainstorming and identification of a broad range of potentially hazardous event sequences. The objective of the study is to populate a table in which each row corresponds to a specific operational deviation (or upset condition). A set of simple guide words (e.g., "no," "more/less," "before/after," and "faster/slower") are used to characterize the distinction between the deviated and the standard system conditions, with respect to a measured parameter of importance. Subsequent columns in the table include HAZOP team insights about the deviations such as possible cause(s), possible consequences, and associated relevant safety systems that are intended to prevent the deviation or mitigate the consequences. The HAZOP information is collected and documented in a structured process designed to elicit a comprehensive analysis of the design. Insights are captured in the documentation and assessed for their importance. Identified hazards can be ranked and prioritized to help inform the next iteration of the design process. Action items are assigned for follow-up work to advance the state of knowledge (e.g., specify areas for additional detailed analysis, testing or research) or to advance the design process (e.g., identify systems important to safety, recommend safety system setpoints, recommend defense-in-depth strategies, identify the need for design alternatives studies).

PHA methods such as HAZOP are recognized in the nuclear industry as useful tools to support PRA model development. One such use is the task of identifying design specific initiating events. One of the technical requirements in the ASME/ANS *Standard for Probabilistic Risk Assessment for Advanced Non-LWR Nuclear Power Plant Applications* [4] (derived from a similar requirement in the PRA standard for LWRs [5]) specifies that, for each potentially significant source of radioactive material, mechanisms by which this material could be mobilized to escape initial confinement must be identified. The standard explicitly recognizes that FMEA, HAZOP, or equivalent methods can be used for this purpose.

In this project, broader applications of PHA methods are being investigated to support the development of PRA models early in system design, especially for new reactor technologies and design variants, which do not have an established history or prior PRA development and application. Among the advanced non-LWR concepts currently in development, there is a history of PRA development for some designs, High Temperature Gas-Cooled Reactors (HTGRs) and Sodium Cooled Fast Reactors (SFRs), for example. However, even for HTGRs and SFRs, the technical information provided by a PHA had to be generated in some manner before PRA development. Meanwhile, there is little or no legacy PRA work to build on for the evaluation of Molten Salt Reactors (MSRs).

PHA techniques have supported the design of non-LWR designs. As noted above, PHA techniques like HAZOP studies have been recognized as useful tools for the systematic identification of initiating events for PRA. In addition, HAZOP techniques have been used to guide the development of control systems and control set point settings for the Pebble Bed Modular Reactor (PBMR) project in South Africa [6]. The Licensing Modernization Project (LMP) White Paper on PRA development, submitted to the NRC for review and comment, recommends introduction of the PRA development early in the design and before the completion of the conceptual design [7]. Further, as noted in the NRC's draft guidance document DG-1353 [8]:

> Prior to first introduction of the design-specific PRA, it is necessary to develop a technically sound understanding of the potential failure modes of the reactor concept, how the reactor plant would respond to such failure modes, and how protective strategies

> will be incorporated into formulating the safety design approach. The incorporation of safety analysis methods appropriate to early stages of design, such as FMEA and PHA, provide industry-standardized practices to ensure that such early stage evaluations are
>
> systematic, reproducible and as complete as the current stage of design permits. The subsequent use of the PRA to develop or confirm the events, safety functions, key SSCs, and adequacy of defense in depth provides a structured framework to risk-inform the application for the specific reactor design.

The purpose is to incorporate risk insights into the initial design rather than wait to back-fit them in a less cost effective manner after the reactor safety design approach has been formulated. Given that PHA has useful applications to support design development, it makes sense to consider the introduction of PHA early in the design to both support the design and to provide structure to the initial development of a PRA for all of the advanced non-LWR technologies and designs. It is important to note that the PHA is not performed in isolation from other design and safety analysis efforts, however. This subject is discussed further in Section 5 of this report, which illustrates how the PHA-to-PRA method is intended to be integrated with other established elements of safety analysis, such as Phenomena Identification and Ranking Table (PIRT) analysis and mechanistic calculation of accident phenomena and consequences.

2.3 References

1. American Institute of Chemical Engineers, Center for Chemical Processing Safety. *Guidelines for Hazard Evaluation Procedures, Third Edition.* Hoboken, NJ: John Wiley & Sons, 2008.
2. “Integrated Safety Analysis: Why It Is Appropriate for Fuel Cycle Facilities.” White Paper submitted to the U.S. Nuclear Regulatory Commission, Washington, D.C.: Nuclear Energy Institute. September 2010.
3. U.S. Department of Energy. *DOE Standard on Development of Probabilistic Risk Assessments for Nuclear Safety Applications*. DOE-STD-1628-2013, Washington, D.C., 2013.
4. *Probabilistic Risk Assessment Standard for Advanced Non-LWR Nuclear Power Plant Applications*. (Trial Use Draft Standard) RA-S-1.4-2013. American Society of Mechanical Engineers/American Nuclear Society. 2013.
5. *Addenda to ASME/ANS RA-S–2008 Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications.* ASME/ANS-Ra-SB-2013. American Society of Mechanical Engineers/American Nuclear Society. September 2013.
6. Joubert, J., N. Kohtz, and I. Coe. "South African Safety Assessment Framework for the Pebble Bed Modular Reactor." *Fourth International Topical Meeting on High Temperature Reactor Technology.* American Society of Mechanical Engineers, September 28–October 1, 2008, Washington, D.C.
7. Southern Company Services. *Modernization of Technical Requirements for Licensing of Advanced Non-Light Water Reactors: Risk-Informed Performance-Based Guidance for Non-Light Water Reactor Licensing Basis Development*. SC-29980-xx. (Working Draft Report, Revision N) 2018.

8. U.S Nuclear Regulatory Commission. *Guidance for a Technology-Inclusive, Risk-Informed, and Performance-Based Approach to Inform the Content of Applications for Licenses, Certifications, and Approvals for Non-Light Water Reactors. Draft*. DG-1353. Washington, D.C., August 2018.

3
BODY OF KNOWLEDGE

A "body of knowledge" (BoK) is a manageably-sized collection of specifically selected references that has been developed and employed by professional groups to promote education and common understanding of a particular subject area, practice, or discipline. For example, BoKs have been developed for systems engineering, software engineering, project management, and environmental engineering disciplines. The BoK generally takes the form of a curated collection of document citations accompanied by brief descriptions and relevant notes about the use of each document. A BoK is a guide to a library of documents, not the library itself, providing just enough information about each document to convey a sense of its content and purpose relative to the BoK domain.

The preliminary BoK presented in this section describes experiences and best practices relevant to the development and application of the PHA-to-PRA methodology for advanced (non-LWR) reactor design efforts. The BoK was developed following a formal process by an expert team comprising expertise and experience in safety analysis and design for nuclear, chemical process and high-hazard systems. Team member resumes are provided in Appendix A.

The BoK development process started with the team identifying an initial list of key references for an area of practice. These lists of references, along with short summaries of the major references, were compiled and circulated to the full team for comment and revision. Once the list of references was fairly stable, a preliminary outline of the knowledge areas (a term used in BoK development to denote a category of practical information) represented by the compiled reference list was developed. The references were then sorted into the most appropriate knowledge area. From this compilation and sorting effort an initial outline for the BoK was developed, circulated for comment, and further refined. After agreement was reached on the outline, writing assignments were established to draft the sections of the BoK based upon an abbreviated set of format and content expectations.

The reference summaries are categorized into seven knowledge areas or topics:

1. Systems Engineering
2. Early Stage Safety Analysis and PHA
3. PRA Model Development
4. Standards for Achieving PRA Technical Adequacy
5. Previous Advanced Reactor PRAs
6. Data Collection, Analysis, and Treatment of Uncertainties
7. General and Miscellaneous

The PHA-to-PRA BoK describes industry-standard tools and methods that have been developed and used in the chemical process, aerospace, and nuclear industries for early design stage safety analysis. These tools include PHA, along with tools for developing initial PRA models, such as event trees and fault trees.

For consistency, each BoK Knowledge Area entry in this section covers the following standard set of content and structure (where X = 1 to 7):

- 3.X Knowledge Area – one of seven topics
- 3.X.1 Background – general discussion on Knowledge Area
- 3.X.2 Technical Discussion – concise description of key references for knowledge area
- 3.X.3 Summary Observations – summary of Knowledge Area
- 3.X.4 References – reference information for primary references described in Technical Discussion and secondary references for each Knowledge Area

Within each Technical Discussion entry, an evaluation of the content of each reference is provided that includes "noteworthy content" that specifically relates to the application of the PHA-to-PRA methodology to advanced reactor design. The references for each knowledge area summarized in this BoK are listed at the end of each subsection for ready access to the reader. Secondary references are also provided in each reference list. The secondary references may either be cited explicitly in the BoK Technical Discussion or may be provided as additional information for further reading beyond the primary BoK references. To the extent possible, BoK reference documents are generally accessible and available for public use free of charge; however, in some cases, references may require purchase for access. The BoK is intended to be a living document that may be modified and updated to incorporate new information in form of experience, expertise and lessons learned.

3.1 Systems Engineering

3.1.1 Background

Because one intended outcome of the approach being developed to gain risk insights that can inform nuclear system designers how a reactor design can be made safer, expertise in the area of systems engineering is important. The fundamentals of systems engineering are relevant and applicable throughout each step of the design process. Within the context of safety and risk analyses of advanced reactor designs, the specific concepts of system definition, system decomposition, and the processes of defining requirements, functions, and interfaces are particularly important. Correct application of these concepts is crucial when determining the adequacy of design information to conduct a hazard analysis on a reactor system and when revising a system design using risk insights from safety analyses.

Systems engineering is "the art and science of developing an operable system capable of meeting requirements within often opposed constraints." [1] Systems engineering is a holistic, integrative discipline used to develop a safe and balanced design in the face of competing interests, by effectively combining the contributions of experts from many different fields. Proper systems engineering practices will produce a coherent whole that is not dominated by the perspective of a single discipline [1].

When compared to current risk assessments performed on existing reactor designs, systems engineering is especially relevant to the analysis of new reactor designs because the system design is not yet finalized. Thus, using correct systems engineering practices can ensure that all significant results from the analysis influence the next design iteration. One possible example of this iteration is the use of an assumed subsystem or component reliability rate to derive a requirement for that subsystem or component.

3.1.2 Technical Discussion

3.1.2.1 DOE-STD-1189-2016, DOE Standard on Integration of Safety into the Design Process

This standard [2] provides requirements and guidance for the integration of safety into the design process for high hazard nuclear facilities of the U.S. Department of Energy (DOE) as defined in 10 CFR Part 830, Nuclear Safety Management. It is applied to new nuclear facilities and to modifications of existing facilities. The standard specifies the requirements and responsibilities for project management, engineering and design, safety analysis, and the interactions essential for successful integration of safety into the design and construction phases of the facility life cycle. The standard also specifies key interfaces required for the integration of safety into design.

The project management processes and responsibilities for ensuring proper implementation of the Safety-in-Design concept, required by DOE directives, are presented in Section 3 of the standard. This section identifies requirements for the Safety Design Strategy (SDS), a technical document that provides a roadmap for integration of safety into design and includes several key elements including: philosophies, goal consideration, decision-making, documents, and quality assurance (QA) and configuration management (CM) programs. Additionally, a Code of Record (COR) should be initiated during the conceptual design phase and placed under configuration management to ensure it is updated to include more detailed design requirements, or changes to requirements, as they are identified during maturation of the design.

The design process and criteria to ensure that systems, structures, and components (SSCs) important to safety, specific administrative controls (SACs), and safety management programs (SMPs) are integrated into the design in an effective and efficient way are described. As the design progresses and hazard analyses are performed, the design organization determines appropriate safety features for each phase. A systematic design development process is executed in each project design phase: Pre-Conceptual, Conceptual, Preliminary, Final, Construction, and Transition to Operations. The recommended Safety-In-Design Approach guides the integration of safety into each phase of the design process to ensure the following elements are addressed:

- Identification of Design and Safety Requirements
- Major Safety Functions
- Inherently Safer Design
- Hierarchy of Controls
- Conservatism

- Risk and Opportunity Assessment
- Stakeholder Issues
- Use of Integrated Safety Management Guiding Principles

During the conceptual design phase, alternatives for satisfying the mission need are evaluated in detail to identify the preferred alternative for the preliminary design. The scope of the alternatives analysis should be comprehensive enough to ensure that the selected alternative is best suited from a safety perspective and meets mission needs. Regarding hazard assessment, the standard states that a qualitative evaluation of the potential facility hazards shall be performed for the available alternatives and a more detailed facility-level hazards analysis shall be performed for the preferred alternative. This hazards analysis describes the initial major hazards and other risk areas that could affect project cost and schedule, and identifies significant hazard scenarios and the initial suite of facility design basis accidents (DBAs). This analysis is documented in the Conceptual Safety Design Report (CSDR), which documents the basis for preferred alternative selection, technology readiness, assumptions, and safety-in-design risks/opportunities.

The project is required to implement a Risk Management Plan (RMP) for managing risks and uncertainties affecting safety-in-design and project objectives. Given the potentially significant costs associated with safety decisions, the integration of safety into the design process should include a strong link between the development of safety-in-design and identification of project technical and programmatic risks. Examples of safety-in-design risk factors with potential significant project impact include technology maturity, safety analysis assumptions, design margins, degree of conservatism, and safety classifications of major SSCs and confinement strategy.

Noteworthy Content

The DOE standard provides a “graded approach” process to ensure that the level of analysis, documentation and actions used to comply with a requirement is commensurate with the relative importance to safety, safeguards, and security, the magnitude of hazards involved, life cycle stage and programmatic mission of the facility, and radiological hazards. This concept aligns well with the initial focus on the progression from PHA to PRA as the design matures through the initial design phases.

The appendices are extensive, making up about half the total content of the standard. They provide more details including organizational and process flow diagrams as well as specific examples that flesh out the requirements outlined in the Standard. The level of detail provides useful templates to better facilitate implementation and compliance with the “Safety-in-Design” approach.

3.1.2.2 ANS/ANSI-53.1-2011, American National Standard: Nuclear Safety Criteria and Safety Design Process for Modular Helium-Cooled Reactor Plants

The purpose of the subject standard [3] is to provide criteria applicable to the design of modular helium-cooled reactor nuclear power plants, referred to as "MHR plants" in the standard. To achieve this purpose, this standard provides a process that can be used by advanced reactor developers to:

- Identify safety functions, top-level design criteria, licensing-basis events, design basis accidents, and methods for performing safety analyses;
- Determine safety classification of SSCs;[2]
- Identify safety-related SSC special treatment requirements and defense-in-depth (DID) provisions; and
- Demonstrate the adequacy of DID by applying a risk-informed approach.

The safety design process described in this standard closely follows the risk-informed approach described in the Next Generation Nuclear Plant (NGNP) white papers [4-8], submitted by DOE to the NRC for review and comment, concerning selection of licensing basis events, PRA development, safety classification of SSCs, selection of special treatment requirements, and evaluation of DID adequacy. These white papers in turn provided the starting point for the Licensing Modernization Project white papers for the same topics. The target audience of the standard are developers of modern HTGRs. However, with the exception of some of the material in Chapter 3 and all of Chapter 6, which deal with specific safety issues for HTGRs, the process described in the remaining chapters is generally applicable to other non-LWRs as well as advanced LWRs.

Noteworthy Content

This standard is generally relevant to early stage design criteria development for HTGRs as well as other non-LWRs. However, some aspects of it should be considered before applying the process as follows:

- PHA is not specifically mentioned; however, early stage safety analysis for HTGRs is addressed in Sections 3 and 6 of the standard.
- Examples of licensing basis events for MHRs are provided in the document.

3.1.2.3 NUREG/CR-6065, Systems Analysis of the CANDU 3 Reactor

This NUREG [9] provides an example of a safety assessment developed for an early conversation with regulators about a reactor design that was not yet at a mature stage in the design process. This report contains an independent examination of event sequences, safety systems, and operator actions that might have played a role in any future NRC review of the CANDU 3 for design certification. The results and observations recorded in the report were developed by ORNL and intended to provide the NRC with information that could be used in reaching regulatory decisions for the CANDU 3.

[2] Note: the chapter on SSC safety classification is essentially the same as that described by the IAEA in Reference 16.

Documentation of the CANDU design was obtained by the assessors from the literature and Atomic Energy of Canada Limited (AECL); this information was supplemented by meetings with AECL staff. In order to conduct the analysis of the design, several assessment methodologies were considered including HAZOP, FMEA, and standard fault tree and event tree analysis techniques. Three criteria were used when selecting which assessment methodologies should be used in the study. The first criterion was related to the products required from the project. Because they are typical of products from a PRA of a plant, techniques normally used in PRAs (e.g., event trees and fault trees) were favored. The amount of detail required to implement the methodology effectively was the second criterion to be considered when selecting the approach to be used in this study. Finally, there was the need to provide the NRC with the information in a deterministic format to allow a more consistent review with respect to NRC regulatory criteria. Ultimately, an assessment methodology using a combination of event trees and fault trees was chosen because it best fit the criteria of the program.

A comprehensive list of initiating events (IEs) was developed utilizing experience with US LWRs, US research reactors, and currently operating CANDU power reactors. The goal was to develop a short list of representative initiating events (RIEs) for which event trees would be completed. The IEs selected for this short list were to be representative of the spectrum of CANDU 3 plant responses (i.e., systems that respond to mitigate the IE). The initial set of IEs was parsed into Plant Response Categories (PRCs) which were determined using a Master Logic Diagram, which is provided in the report. The frequency of occurrence of each IE was also estimated, although the report does not describe how this was done.

The next step was to review the PRCs to determine whether any were similar enough to warrant further combination. The guideline for this review was to reduce the level of effort required while maintaining sufficient analysis detail. This step resulted in the selection of seven RIEs that would be evaluated using the fault tree and event tree methodology. Selection of the RIEs was based on PRA analyst experience and operational information for the CANDU 3 plant.

For each RIE, narrative text and an Event Sequence Diagram (ESD) were developed. In addition, the ESDs were used to identify primary and backup systems and systems significant-to-safety in the CANDU 3 design. Based on the plant response information contained in the ESDs, an event tree was prepared for each RIE.

Next, fault trees were used to model the systems and understand how failure of the systems could occur. Only systems categorized by ORNL to be “frontline”, including both primary and backup, were incorporated in the event trees; frontline systems are those systems that act directly to respond to or mitigate an event. A fault tree was developed for each system in the event trees. Support systems are those systems, other than frontline, that provide a support function to the frontline system (electric power is a common one). Because of the lack of design details at this stage, the impact of support systems and components could not be evaluated completely through the use of only event and fault trees. Consequently, additional tools were developed, such as a system dependency matrix (discussed later), to separately track and evaluate these support functions.

The fault trees for each system were solved to determine the failure combinations associated with that system function. The event trees were then solved using the fault tree solutions, and sequence level failure combinations were generated. This information identified the system failure combinations that could contribute to a particular failure sequence in the event tree. This information, along with the IE frequency, was used to classify the event sequences.

To track the dependencies between frontline and support systems, and between support systems themselves, a system dependency matrix was developed. The system dependency matrix was developed to identify support systems whose failure could affect the operation of a frontline system and to identify any dependencies among the support systems themselves.

Noteworthy Content

Numerous event trees, fault trees, and event sequence diagrams are provided in the report with quantitative results. Event sequences are assigned to one of four event classifications depending on their probability, and one of three plant end-states. Systems significant to safety are identified, the methodology for identifying primary and backup systems is elaborated, and significant operator actions are summarized.

Self-described limitations of the PRA are as follows:

- The CANDU 3 design was incomplete so sufficient design detail did not exist to perform in-depth failure analyses.
- The focus of this effort was on systems behavior during power operations. Other plant conditions such as low or zero power operations were not examined. In addition, earthquakes, fires, floods, and common-mode failures associated with such events were not considered in this analysis.
- The main focus of the report is on events that affect the fuel in the reactor core. Event tree and fault tree analyses were not performed for the containment, refueling, and waste storage systems because available information on these systems in the Canadian documentation was sparse.
- The initiating events were obtained from a review of a comprehensive set of sources, including U.S. LWRs and research reactors and Canadian CANDU operating experience. The representative initiating events against which the plant response is gauged are comprehensive, but further analysis and experience could indicate different or additional events that should be analyzed.

3.1.2.4 ANS-30.1, Integrating Risk and Performance Objectives into New Reactor Nuclear Safety Designs

An effort to develop a standard [10] to specify objectives for augmenting deterministic nuclear safety design practices using risk-informed, performance-based (RIPB) methods has been approved by the American Nuclear Society (ANS) and the American National Standards Institute (ANSI) and is currently underway. This standard, ANS-30.1-201x, describes the application of RIPB methods to high level safety criteria selection, nuclear safety function specification, licensing basis event (LBE) selection, equipment classification, and assurance of defense-in-

depth (DID) adequacy. The objective of the standard is to ensure that RIPB-augmentation of nuclear safety design practices is consistently applied for new reactor technologies. The main focus of this standard is to help plant designers ensure acceptance of their advanced reactor designs.

Noteworthy Content

The new draft standard is being issued for comment. As the standard matures, it has the potential to act as an important repository for technical design guidance and best practices in integration of risk insights into the design process. Therefore, progress in development and implementation should be closely tracked to inform updates to this knowledge area.

3.1.3 Summary Observations

A draft ANS standard to integrate risk-based and performance insight into designs is in-process [10]. However, a number of advanced non-LWRs are actively being designed now. As discussed in this sub-section a detailed systems analysis of a non-LWR [9], the CANDU-3, has been performed and the approach and methods used by ORNL to perform that analysis are instructive. On a more comprehensive basis, DOE has developed a technical standard designed to integrate safety analysis into each stage of design, from pre-conceptual options studies, through conceptual and preliminary design phases to final design [2]; general expectations for the content of safety analysis during each phase of design are discussed along with integrating safety deliverables with broader project management. These three standards provide concepts that can assist the designers and safety analysts in their efforts to achieve early integration of safety in design. Additional information and guidance on systems engineering is available in the literature [11─16].

3.1.4 References

1. Hirshorn, S., L. Voss, and L. Bromley. *NASA Systems Engineering Handbook. Rev. 2.* NASA SP-2016-6105. Washington, D.C.: National Aeronautical and Space Administration, 2017.
2. U.S. Department of Energy. *DOE Standard on Integration of Safety into the Design Process*. DOE-STD-1189-2016, Washington, D.C., 2016.
3. ANSI/ANS. *American National Standard: Nuclear Safety Criteria and Safety Design Process for Modular Helium-Cooled Reactor Plants*. ANSI/ANS-53.1-2011. La Grange Park, IL: American Nuclear Society, December 2011.
4. *Next Generation Nuclear Plant Licensing Basis Event Selection White Paper*. Idaho National Laboratory, Idaho Falls, ID: September 2010. Report INL/EXT-10-19521.
5. *Next Generation Nuclear Plant Probabilistic Risk Assessment White Paper*. Idaho National Laboratory, Idaho Falls, ID: September 2011. Report INL/EXT-11-21270.
6. *Next Generation Nuclear Plant Structures, Systems, and Components Safety Classification White Paper*. Idaho National Laboratory, Idaho Falls, ID: September 2010. Report INL/EXT-10-19509.
7. *Next Generation Nuclear Plant Defense-in-Depth White Paper*. Idaho National Laboratory, Idaho Falls, ID: December 2009. Report INL/EXT-09-17139.

8. *Next Generation Nuclear Mechanistic Source Terms White Paper*. Idaho National Laboratory, Idaho Falls, ID: July 2010. Report INL/EXT-10-17997.
9. Wolfgong, J. R., et al. *Systems Analysis of the CANDU 3 Reactor*. NUREG/CR-6065, ORNL/TM-12396. Washington, D.C.: U.S. Nuclear Regulatory Commission, 1993.
10. *Integrating Risk and Performance Objectives into New Reactor Nuclear Safety Designs*. ANS 30.1-201x (New Standard under Development). La Grange Park, IL: American Nuclear Society, 2017.
11. *Basis for the Safety Approach for Design & Assessment of Generation IV Nuclear Systems*. *Revision* 2. GIF/RSWG/2007/002. Generation IV International Forum, Risk and Safety Working Group. November 24, 2008.
12. *Proposal for a Technology Neutral Safety Approach for New Reactor Designs.* IAEA-TECDOC-1570, Vienna (Austria): International Atomic Energy Agency, September 2007.
13. *Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*. *Fourth Edition.* INCOSE-TP-2003-002-04. International Council on Systems Engineering, Hoboken, NJ: John Wiley & Sons, 2015.
14. U.S. Department of Energy. *Content of System Design Descriptions*. DOE-STD-3024-2011. Washington, D.C., August 2011.
15. U.S. Department of Energy. *Managing Design and Construction Using Systems Engineering*. DOE-G-413.3-1, Washington, D.C.: U.S. Department of Energy, September 23, 2008.
16. *Safety Classification of Structures, Systems and Components in NPP*. Safety Standards Series No. SSG-30, Vienna (Austria): International Atomic Energy Agency, 2014.

3.2 Early Stage Safety Analysis and PHA

3.2.1 Background

This section addresses PHA with a focus on the early (pre-conceptual and conceptual) design stages. This section first discusses the Integrated Safety Assessment Methodology (ISAM) developed under the auspices of the Generation IV International Forum (GIF) [1-2], which is intended to encompass safety assessment through all design stages. Next, the HAZOP methodology [8] that is qualitative and suitable for early-stage hazard analysis is discussed, followed by a discussion of a simplified quantitative risk analysis study that was developed for a nuclear facility at DOE's Hanford reservation [10]. The documents are discussed through the lens of how they fit into the need to perform hazard analysis on early-stage reactor designs, where there is limited detail, and build on the initial results as the design matures leading to a PRA suitable to support advanced reactor licensing.

3.2.2 Technical Discussion

3.2.2.1 Generation IV International Forum Integrated Safety Assessment Methodology (ISAM)

The Generation IV International Forum (GIF) prepared a report that describes a methodology called ISAM [1]. The ISAM is intended to support achievement of safety that is "built-in," rather than added on late in design, by influencing the direction of the concept and design development from its earliest stages (this is similar in intent to DOE-STD-1189-2016, discussed in Section 3.1.2.1, above). The ISAM is perhaps best thought of as a tool kit consisting of elements that help to answer different safety-related questions, and provide important safety perspective at the several stages of design development. The value of the tool kit is that it uses interim safety analysis results to actively shape the direction of the design. Subsequently, GIF prepared guidance for implementing ISAM [2] to provide a step-by-step description of how to apply the ISAM by identifying the inputs and outputs of the different tools comprising ISAM and explaining the flow from one step to another. The guidance report also contains several limited, example applications of ISAM.

The ISAM is driven by a defense-in-depth (DID) philosophy which conventionally has five levels: prevention, control, protection, management of severe accidents, and consequence mitigation. The ISAM consists of five tools summarized here.

Qualitative Safety (features) Review (QSR) – QSR is a new tool, developed under ISAM, which provides a systematic means of ensuring and documenting that the evolving designs incorporate the desirable safety-related attributes and characteristics. These attributes and characteristics are identified and discussed in a report entitled *Basis for the Safety Approach for Design and Assessment of Generation IV Nuclear Systems* [3]. It is intended to help ensure that safety truly is built-in, not added-onto. QSR uses a qualitative hierarchical template driven by DID attributes. The result is a hierarchy of "recommendations" to be used in design that is organized into four classes, depending on whether they are generic and technology-neutral or not.

The hierarchy is to be used by comparing the design characteristics of the advanced reactor system to a check list of DID attributes. A characteristic can be rated as favorable, unfavorable, or neutral, with respect to each check list item. An example of applying QSR to part of a reactor system, given in the ISAM report, is 29 pages long; a complete QSR hierarchy would be much larger.

Phenomena Identification and Ranking Tables (PIRT) – PIRT is an established, formalized, and expert-based consensus decision-making tool, which is exhaustive, defendable, and auditable. It allows the evaluation of a concept or design by following the response of a key measurable parameter, called the Figure-of- Merit (FOM), chosen by a panel of experts. The technique helps to systematically identify system and component vulnerabilities and generate a ranked table identifying relative contributions of relevant phenomena to safety and risk.

Objective Provision Trees (OPT) – OPT is another new tool introduced in ISAM to design in and/or to assess safety-related DID of advanced reactors This is done through visual presentation and a systematic inventory of the reactor design provisions that contribute to safety. Its use requires knowledge of the installation characteristics and phenomenology, and the associated risks.

Based on the system being considered, and the phenomenology involved in abnormal situations, the OPT method is a top-down method which for:

- Each level of DID, and
- Each safety objective/function (in general, control of reactivity, removal of heat from the fuel, and confinement of radioactive materials),

Identifies the:

- Possible challenges to the safety function,
- Plausible mechanisms which can lead to these challenges, and
- Provisions included in the concept or design to prevent, control, or mitigate the consequences of the challenges/mechanisms (called a "line of protection").

The result is expressed through a hierarchy of relationships in the form of a tree. More details on OPTs are given in an IAEA report [4]. For the identification of initiating safety events, OPT accomplishes the same functional and analytical objectives as an FMEA or HAZOP study and provides similar results.

Deterministic and Phenomenological Analysis (DPA) – In the context of ISAM, DPA refers to providing quantitative insights that are needed to support the implementation of the PRA. It involves development and implementation of models in areas such as reactor physics, fuel behavior, thermal hydraulic analysis, containment analysis codes, atmospheric dispersion and dose, and structural analysis. More detailed information on DPA can be found in an IAEA report [5] on this subject.

Probabilistic Risk Assessment (PRA)[3] **–** PRA is an industry-standard, rigorous, systematic, and comprehensive tool for identifying and estimating the likelihoods of sequences of events that can result in the loss or damage of complex engineered systems. The essential construct underlying PRA, as discussed in the ISAM, is the potential interaction between technological hazards, potential challenges that create possibilities for those hazards to cause loss or damage, and the effectiveness or reliability of safety provisions that are provided in a system design to prevent or mitigate the potential loss or damage. The discussion of PRA in this report is relatively short because it is an established tool that is comprehensively described in other guides and standards.

[3] GIF and other international entities use the term "Probabilistic Safety Assessment" in lieu of the equivalent "Probabilistic Risk Assessment". For consistency, terminology has been harmonized such that PRA is used throughout this report. Therefore, all discussions in the document summaries refer exclusively to PRA.

Noteworthy Content

The ISAM provides an initial attempt by the international community to address early stage safety analysis of advanced nuclear reactors; as such, it provided an important starting point for the work being performed on this project. Key points in the ISAM report important to transitioning PHA results to support PRA are:

- The ISAM is intended to be an "iterative design process" that ensures "operability, availability, and safety" of the system; however, it is not evident how operability and availability are addressed in the ISAM.
- Both the ISAM and GDI reports contain sections that summarize the inputs and outputs from each of the ISAM tools. Although coverage is uneven from topic to topic (e.g., QSR is given short shrift), these sections do provide useful guidance on the desired results from early stage safety analyses and the potential inputs to PRA.
- No examples of the application of the QSR and OPT tools to an entire advanced reactor system have been identified. Such an application appears to involve substantial resources as the size of QSR and OPT hierarchies appears to increase geometrically with the complexity and extent of the system being analyzed. Future updates of the BoK should monitor and incorporate additional examples of ISAM applications if and when they are identified.
- The LMP PRA report [6] notes that the ISAM approach is generally consistent with the approach to PRA in the LMP report with the following observations:
  - The LMP approach recommends an earlier introduction of PRA than does the ISAM approach in order to capture risk insights early in the design.
  - The PRA presentation in ISAM does not explicitly identify the role of a simplified, early high level safety analysis effort that could be used to guide the preliminary design development.
  - ISAM recognizes the need for technology neutral risk metrics. However, it attempts to redefine core damage frequency (CDF) in a way that applies to all reactors, which could be problematic for some advanced non-LWRs. However, the implied acceptance of a surrogate risk metric is consistent with the LMP report [6] and the Non-LWR PRA Standard [7].
  - A key strength of ISAM is the incorporation of DID considerations at an early stage of design.

3.2.2.2 HAZOP: Guide to Best Practice

This book [8] is the third edition of a seminal document that provides specific guidance for the HAZOP method of performing a PHA[4]. The HAZOP method was pioneered in the early 1960s in the chemical industry and its development in the UK was facilitated by the Chemical Industries Association which published an early guide in 1977. HAZOP has been applied in many different chemical process industries at all life-cycle phases (preliminary design through decommissioning). The HAZOP provides a rigorous, organized, and detailed qualitative hazard analysis which comprehensively evaluates the system under study.

HAZOP studies are in depth analyses of a system, process, or operation and are conducted by a multidisciplinary team of subject matter experts. The guide defines six stages of a project life cycle from concept to decommissioning, and describes the types of hazard studies that are most appropriate for each project stage. The HAZOP is often conducted at the completion of the process development stage,[5] where the development of piping and instrumentation drawings (P&ID) would be available. However, less detailed schematic and process flow diagrams can also be used to evaluate less-mature designs. It is important to document the design information that was used to perform the HAZOP.

When conducting a HAZOP analysis, system parameters such as flow, pressure and temperature, are combined with guidewords such as increased, decreased, no, or reversed, to uncover meaningful[6] deviations from anticipated system operation. The HAZOP team uses these combinations of parameters and guidewords to focus on the deviations from normal operation that could lead to potential hazards to safety, health or the environment. A hazard is described as any physical situation with the potential for human injury, damage to property, damage to the environment, or a combination of these consequences. During the HAZOP analysis, a team identifies unique causes for each deviation. Once the causes have been identified, the team then evaluates the consequences of the deviation, discusses the existing safety systems that could mitigate these consequences, and determines if an action item for change or further investigation is required. The results of this analysis are documented in a written report that is often used as a basis for implementing design changes. Commercial computer software is available to facilitate implementation and documentation of the HAZOP analysis results.

In addition to being used for hazard analysis of new processes, the document discusses application of HAZOP to modification of existing operations, periodic hazard studies of an existing plant, operating procedures, interconnections between systems/plants, commissioning and decommissioning, start-up and shutdown, and construction and demolition.

[4] There are many techniques available for performing a PHA. For a discussion of the techniques and how to select the appropriate technique for a particular application, see Reference 9.

[5] Equivalent to completion of a conceptual design in the sequence of nuclear reactor development.

[6] That is, not nonsensical such as “no temperature”.

Noteworthy Content

Key points in this guide important to transitioning PHA results to support PRA are:

- The guide provides a process for performing a comprehensive hazard assessment of a new system or design.
- A major strength of the HAZOP methodology is the flexibility and adaptability of the results. Because of the creative nature of the deviation generating step of the study, as well as the ability of the team to determine how detailed the discussion of each deviation should be, HAZOP studies can be used to investigate the hazards present in a variety of designs at a range of design maturities.
- Systems important to safe and reliable operation are identified by HAZOP. In addition, a qualitative understanding of the relative importance of each safety system is developed.
- The results of a HAZOP study can contribute significantly to producing information required to perform a PRA:
  - Initiating events for event tree analysis can be obtained from the causes that are identified by the HAZOP team.
  - The consequences discussed for each cause can be useful in the construction of fault trees. The documented consequences could also be helpful in the development of event sequence end states.
  - The safety systems documented for each cause can be a starting point for the development of the pivotal events in event tree analysis.

3.2.2.3 Bechtel River Protection Project Low-Activity Waste Plant Nuclear Safety Model

This study [10] assesses nuclear safety and major asset damage of the Low-Activity Waste (LAW) facility for vitrifying high-level waste at Hanford, based on the documented design as of September 2015. The purpose of this study was to provide perspective on operational safety and the potential for loss of major assets (e.g. the melter) such that both robust and potentially vulnerable areas are identified. The study includes equipment as appropriate for this purpose without regard to whether systems, structures, and components (SSCs) have been previously designated as safety or non-safety related. It resulted in quantitative risk bin and likelihood bin insights about nuclear safety and asset protection. The study yielded a list of suggested safety functions (or controls) application of which would achieve reasonable assurance of adequate protection for workers and public. The study is adjunct to the hazards analysis required by DOE directives.

The LAW Plant Nuclear Safety Model (LPNSM), developed as an output of this analysis, is a comprehensive, plant-wide model of operational event sequences that includes the LAW waste processing equipment and support equipment housed in the LAW vitrification facility and the balance of facilities. Common cause failures and maintenance outage effects on systems are included in the model. It makes no distinction between safety related and commercial equipment. Estimates of equipment reliability rely on well-vetted data sources. Results are provided in terms of both toxicological and radiological material releases for insights into nuclear safety, and in

terms of damage to major assets, such as the melters. There are many parallels between the LPNSM study and the PHA-to-PRA project in terms of objectives, use of tools, and methodology. The Master Logic Diagram for the LAW plant is developed in considerable detail according to the following six levels.

- Level 1: Release of or exposure to toxic or radiological materials.
- Level 2: Sources of toxic or radiological materials.
- Level 3: Barriers between sources and people.
- Level 4: Nuclear safety functions of barriers.
- Level 5: Functional failure mode of barriers.
- Level 6: Initiating events whose event sequences might cause barrier failure.

Noteworthy Content

Key points in this report important to transitioning PHA results to support PRA are:

- This study is an example of a PHA of a facility that includes both chemical/toxicological and radiological hazards, to both the public and facility workers, that leads to a quantitative result (but not a full PRA).
- The major tools employed included the development of detailed Master Logic Diagrams (MLDs) that are used for the systematic identification of events, event sequence diagrams that identify the operational controls that could be employed to mitigate the consequences of the initiating events, and event trees that are quantified to develop order-of-magnitude frequencies for the resulting event sequences. The consequences are evaluated in terms of both chemical/toxicological and radiological effects on plant workers, co-located personnel, and the public offsite.
- The MLD development in this report provides useful guidance on how to organize the information developed in a PHA to support the selection of initiating events and organize the event sequence diagrams and event trees in a PRA.
- Also included in the evaluation are the economic consequences of scenarios involving loss of glass melters. As such, it is an example of a PHA that leads to a simplified high-level PRA and assesses operability concerns as well as safety-related issues.
- There are a number of good examples in this reference on how to document the bases and assumptions behind the PHA and resulting PRA.

3.2.3 Summary Observations

Significant portions of the reports discussed in this section concern early-stage safety analysis techniques such as HAZOP, MLDs, QSR, and PIRT and how the results of these techniques relate to later-stage safety analysis techniques such as event trees, fault trees, deterministic modeling, and ultimately the PRAs that integrate all of the foregoing results. The two ISAM reports explicitly identify information being produced by each upstream tool and needed by each downstream tool, and the uses of information from a HAZOP analysis by downstream tools has been identified.

An approach to doing a simplified quantitative risk analysis was developed in the report on the Hanford LAW facility. Such an approach may be cost-effective at intermediate development stages such as late conceptual design and preliminary design. It may also provide a bridge from qualitative PHA to a full PRA.

The ISAM appears to be a complete and integrated approach to safety assessment. It is claimed to be applicable across the entire development spectrum but some of the initial steps (e.g., QSR, OPT) may somewhat burdensome for early-to-intermediate-stage advanced reactor projects; however, experience with these tools is yet to be developed.

3.2.4 References

1. *An Integrated Safety Assessment Methodology (ISAM) for Generation IV Nuclear Systems. Version 1.1*. Generation IV International Forum, Risk and Safety Working Group. June 2011.
2. *Guidance Document for Integrated Safety Assessment Methodology (ISAM)*. GIF/RSWG/2014/001. Generation IV International Forum, Risk and Safety Working Group. May 12, 2014.
3. *Basis for the Safety Approach for Design & Assessment of Generation IV Nuclear Systems. Revision 1*. GIF/RSWG/2007/002. Generation IV International Forum, Risk and Safety Working Group. November 24, 2008.
4. *Proposal for a Technology-Neutral Safety Approach for New Reactor Designs*. IAEA-TECDOC-1570. Vienna (Austria): International Atomic Energy Agency, September 2007.
5. *Deterministic Safety Analysis for Nuclear Power Plants – Specific Safety Guide*. Safety Standard Series No. SSG-2. Vienna (Austria): International Atomic Energy Agency, 2009.
6. Southern Company Services. *Modernization of Technical Requirements for Licensing of Advanced Non-Light Water Reactors: Probabilistic Risk Assessment Approach*. Draft Report, Revision A. SC-29980-101. (Issued for Collaborative Review) 2017.
7. *Standard for Probabilistic Risk Assessment for Advanced Non-LWR Nuclear Power Plant Applications*. (Trial Use Draft Standard) RA-S-1.4-2013. American Society of Mechanical Engineers/American Nuclear Society, 2013.
8. Crawley, F. and B. Tyler. *HAZOP: Guide to Best Practice, Guidelines to Best Practices for the Process and Chemical Industries*. 3rd Edition. Elsevier, 2015.
9. American Institute of Chemical Engineers, Center for Chemical Processing Safety. *Guidelines for Hazard Evaluation Procedures, Third Edition*. Hoboken, NJ: John Wiley & Sons, 2008.
10. Frank, Michael V., et al. *Low-Activity Waste Plant Nuclear Safety Model. Rev. 0*. 24590-LAW-RPT-NS-15-003. Richland, WA: Bechtel River Protection Project, August 16, 2016.

3.3 PRA Model Development

3.3.1 Background

This section addresses the PRA building blocks that have the potential for benefitting from a PHA. These building blocks include the systematic identification of initiating events, the analysis of the plant response to the initiating events, the development and quantification of event sequence models, and the evaluation of event sequence consequences.

The primary tools used to develop the event sequence models include, Master Logic Diagrams (MLDs), event sequence diagrams, event trees, and fault trees. An event tree is the result of an inductive approach that begins with identification of an undesired initiating event and then develops the potential response of the sequence of plant systems, or functions, that are designed to prevent an undesired consequence (e.g., fuel damage, radionuclide release) from occurring. Qualitative information that is needed to develop an event tree includes knowledge of the plant response to the initiating events and resulting event sequences, identification of the plant safety functions responsible for preventing and mitigating accidents, identification of the SSCs that are responsible for performing these safety functions, success criteria for bringing the plant to a safe and stable end-state, and the success criteria for each modeled safety function.

A system event tree is usually qualitative and the result is often depicted in the form of a branching diagram beginning with the initiating event (e.g., a pipe break) and followed by consideration of a chain of plant features designed to prevent undesirable consequences from occurring. A precursor tool to aid in the definition of event tree top event sequencing and to model the understanding of the plant response, including the implementation of emergency operations and accident management procedures, is the event sequence diagram (ESD). The performance of each plant feature is normally assumed to be binary: either it succeeds in which case the safety function is fulfilled, initiated or it fails in which case the next prevention or mitigation function is considered or the end state and resulting consequences occur. The binary outcome for each modeled SSC performing a safety function leads to the tree-like branching structure.

A fault tree analysis is a deductive analytical technique, whereby an undesired top event is specified and the system is then analyzed in the context of its environment and plant operation to find the credible ways in which the top event can occur. The fault tree itself is a graphic model of the various parallel and sequential Boolean combinations of faults that will result in the occurrence of the top event. The faults can be subsidiary events that are associated with component hardware failures, human errors, or any other pertinent events which can lead to the top event. A fault tree thus depicts the logical interrelationships of primary (bottom-most) and intermediate events that lead to the top event of the fault tree. A fault tree is a qualitative model that can be evaluated quantitatively and often is. An event sequence analysis typically informs selection of the top events in the fault tree. When the event trees and fault trees are logically linked in a PRA model, each pivotal event in the event tree refers to a top event in a corresponding fault tree. There are various schemes used in design of PRA software for quantifying the linked event tree/fault tree logic, but all result in a quantification of each event

tree sequence and a roll up of the frequency for each well-defined end state. In a typical Level 1 PRA model for an LWR there are only two end states of the event tree: successful termination and core damage; however, when considering other reactor designs, there can be any number of different end states, each with a unique outcome and extent of damage.

3.3.2 Technical Discussion

Numerous reports, guides and papers have been written on the development of PRAs for advanced reactors, including the use of event sequence diagrams, event trees and fault trees in PRA. This section will discuss two seminal reports in this regard in the context of PRAs for nuclear reactors and the implications of these reports to advanced reactor design and analysis. The reader may also be interested in the NASA Fault Tree Handbook [1] which is a recent, comprehensive fault tree analysis guide, but addresses non-nuclear issues; it is not discussed below.

3.3.2.1 NUREG/CR-2300, PRA Procedures Guide

Because of an increasing use of PRA techniques within the nuclear industry and the regulatory process after publication of the "Rasmussen" report [2] in 1975, there was an identified need for technical guidance on methods and procedures for performing a PRA. It was this need that led to the creation of this NRC report [3]. Organizations that cooperated on the development of the document include the ANS, the Institute of Electrical and Electronics Engineers (IEEE), the NRC, the DOE, the Atomic Industrial Forum, EPRI, and utilities.

Despite its age, the PRA Procedures Guide remains a very comprehensive compilation of methods to organize, staff, and perform a very broad and full scope PRA of LWRs, many of which were already built and constructed by the time it was issued. The concept of organizing a PRA into the Level 1/Level 2/Level 3 structure that is still in use today for LWR PRAs was introduced in this guide. The scope of the report addressed Levels 1, 2, and 3 as follows.

1. System analysis – definition and quantification of accident sequences, component data, and human reliability.
2. System and containment analysis – subjects covered in Level 1 as well as physical processes or core-melt accidents and radionuclide release and transport.
3. System, containment, and consequence analysis – subjects covered in Levels 1 and 2 as well as environmental transport and consequence analyses.

The majority of the concepts and methods described in this guide are still relevant so it remains a good resource on how to perform a PRA. As PRA has evolved more detailed guidance documents have been developed on a number of specific topics, such as Human Reliability Analysis (HRA), internal fire and flood analysis, seismic PRA, low power and shutdown PRA, generic data sources, and uncertainty analysis[7]. However, another comprehensive guide on all aspects of PRA has not been provided since this report was published. Of particular interest, this

[7] A useful compendium of such guidance documents can be found in Appendix B of the DOE technical standard on development of PRAs [4].

report contains substantial discussion of methods for developing and using system event trees and fault trees in PRAs. These tools have been a key component of previous nuclear reactor PRAs and are a key element of proposed technical requirements for licensing advanced nuclear reactors [5].

Noteworthy Content

Key points in this report important to transitioning PHA results to support PRA include:

- This guide describes the use of Master Logic Diagrams (MLDs) to aid in the systematic search for initiating events for a PRA and to organize the events for initial stages of event tree development. An example MLD and list of initiating events derived from it are presented in this guide. More detailed examples of MLDs are included in the Hanford Low Activity Waste study that is discussed in Section 3.2.2.3. These more detailed examples are for a process plant that exhibits both radiological and toxicological hazards and as such offer more useful guidance for how MLDs may be considered for a molten salt reactor.
- This guide includes detailed instructions on how to develop event trees and fault trees based on system engineering documents and resources, albeit for existing reactors (LWRs).
- The focus of this guide was on developing Level 1 PRAs for existing LWR nuclear power plants, not advanced nuclear reactors; therefore, guidance on developing PRAs for reactors in the earlier design stages (e.g., pre-conceptual and conceptual design) is not included. However, the use of Master Logic Diagrams and systems analyses used to select initiating events is covered.
- The guide conveys important perspective on technical uncertainty and the role that this perspective needs to play in judiciously using PRA results for decision-making.

3.3.2.2 NUREG-0492, Fault Tree Handbook

Since 1975, a short course entitled "System Safety and Reliability Analysis" was presented to NRC personnel and contractors. The Fault Tree Handbook [6] was developed to serve as text for the System Safety and Reliability Course, thereby providing a resource for previously undocumented material on fault tree construction and evaluation.

Noteworthy Content

Key points in this report important to transitioning PHA results to support PRA are:

- Inductive methods are applied to determine what system states (usually failed states) are possible; deductive methods are applied to determine how a given system state (usually a failed state) can occur. Examples of inductive approaches are: PHA,[8] FMEA, Failure Mode Effect and Criticality Analysis (FMECA), Fault Hazard Analysis (FHA), and Event Tree Analysis. However, this reference does not describe how to tailor these analyses (*e.g.*, FMEA) to provide input to FTA.

[8] While the definition of PHA is not explicitly provided and there is some inconsistency in its usage, this BoK assumes a definition consistent with that of the AIChE/CCPS, i.e., encompassing multiple hazard analysis techniques such as HAZOP, What-If, and Checklist.

- While the discussion of inductive methods is not sufficiently detailed to facilitate the performance of an early stage non-LWR safety assessment, the discussion is sufficient to familiarize practitioners with the important concepts in these types of analyses. The inductive methods mentioned in this reference could be used in early stage non-LWR safety assessments.
- This report contains a very complete discussion of how to construct and evaluate fault trees, as well as the underlying probability and logical concepts. This report does seem to imply that inductive techniques such as HAZOP as an inferior substitute for FTA, rather than a complimentary or supporting analysis.
- The computer codes discussed in this reference are almost all obsolete.

3.3.3 Summary Observations

The reports discussed in this section are largely applicable to safety assessments involving PRA and the techniques such as: PRA safety function definition, initiating event selection, system event trees and fault trees, and evaluation of source terms and consequences that support it. The documents can aid practitioners in transitioning from qualitative early-development-stage PHAs (e.g., HAZOP) to quantitative analysis and PRA by indicating the information requirements for the first steps leading to the PRA *per se*, but additional work is needed to establish specific linkages of information needed by PRA building blocks to PHA outputs.

3.3.4 References

1. Stamatelatos, M. and W. Vesely, et al. *Fault Tree Handbook with Aerospace Applications. Version 1.1*. Washington, D.C.: National Aeronautical and Space Administration, August 2002.
2. Rasmussen, Norman C., et al. Reactor Safety Study: *An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants*. WASH-1400 (NUREG-75/014). Washington, D.C.: U.S. Nuclear Regulatory Commission, October 1975.
3. U.S. Nuclear Regulatory Commission. *PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants*. NUREG/CR-2300. Washington, D.C.: Office of Nuclear Regulatory Research, 1983.
4. U.S. Department of Energy. *DOE Standard on Development of Probabilistic Risk Assessments for Nuclear Safety Applications*. DOE-STD-1628-2013, Washington, D.C., 2013.
5. Southern Company Services. *Modernization of Technical Requirements for Licensing of Advanced Non-Light Water Reactors Probabilistic Risk Assessment Approach*. SC-29980-xx. (Draft Report Revision M – Issued for Collaborative Review) 2018.
6. U.S. Nuclear Regulatory Commission. *Fault Tree Handbook*. NUREG-0492. Washington, D.C., January 1981.

3.4 Standards for Achieving PRA Technical Adequacy

3.4.1 Background

Additional perspective in establishing the interfaces between PHA outputs and PRA inputs can be gained by considering references in the BoK that articulate requirements for PRA technical adequacy. The term "technical adequacy" is normally used in lieu of "PRA quality" to distinguish it from "Quality Assurance" requirements that have been developed for designing and constructing nuclear power plant systems. Industry standards for PRA technical adequacy were initially established for operating LWRs by the American Society of Mechanical Engineers and the American Nuclear Society [1] and subsequently endorsed by the NRC [2] for use in risk informed applications. The International Atomic Energy Agency has also published a number of reports that set forth attributes of technically sound PRA, again with a focus on LWRs [3, 4]. More recently, the ASME/ANS Joint Committee on Nuclear Risk Management has issued a trial use PRA standard for advanced non-LWR power plants [5]. This standard uses reactor technology-inclusive risk metrics.

NRC Regulatory Guide 1.200 [2] describes one approach acceptable to the NRC for the determination of the technical adequacy of a Level 1 or a Level 2 PRA to support a risk-informed regulatory activity. This Regulatory Guide can also be viewed as the NRC response to ASME/ANS RA-Sa-2009, the LWR PRA standard [1], as well as the NEI guidance documents concerning PRA review and self-assessments. The purpose of the PHA-to-PRA effort is to demonstrate how the necessary work to build a PRA model can be supported through the performance of process hazard analyses and the use of system engineering tools. If those building blocks of a PRA that are developed follow this guidance, then sufficient confidence in the PRA results is warranted.

Although focused on LWR technology and risk metrics, the topics discussed in this Regulatory Guide are important considerations for stakeholders developing a PRA model that is eventually intended to support an application. Because PHAs and other early activities may be used to inform these PRA activities, topics covered in this Guide (such as source term analysis, initiating event analysis, and level of detail) can play a role in the planning and execution of these early stage analyses as well.

3.4.2 Technical Discussion

A brief review of each of the selected documents that are related to establishing PRA technical adequacy, introduced above, is provided in the following sections.

3.4.2.1 ASME/ANS Probabilistic Risk Assessment Standard for Advanced Non-LWR Nuclear Power Plants

This standard [5] sets forth the requirements for probabilistic risk assessments (PRAs) used to support risk-informed decisions for advanced non-LWR nuclear power plants (NPPs) and prescribes a method for applying these requirements for specific applications. To support application of this standard to PRAs for a diverse set of reactor designs, the requirements in this standard were developed on a reactor technology-neutral basis.

To be effective for a spectrum of advanced non-LWRs, this standard does not use LWR risk metrics such as core damage frequency, but rather technology-neutral metrics such as: frequency vs. offsite dose, individual risk metrics reflected in the NRC safety goal quantitative health objectives (QHOs), as well as user defined metrics that may be suitable for specific reactor types (e.g., sodium boiling for LMFBRs). Because core damage is not used, the Level 1-2-3 PRA framework is also avoided; however, the scope of the PRA requirements in the standard are equivalent to a full scope, all modes and hazards, Level 3 PRA for an LWR.

The technical requirements in this standard are approximately 80% common to the requirements in the supporting LWR PRA Standard [1]. Hence it should not be necessary for advanced non-LWR developers to use both sets of standards. The primary differences between the two standards are as follows:

- PRA event sequence development in the non-LWR PRA Standard is not limited to single reactor end states and includes accident sequences involving releases from one or multiple reactor modules or radiological sources.
- Requirements in the non-LWR PRA Standard are not limited to PRAs on operating plants but support PRA development at any stage of design.
- LWR risk metrics such as core damage frequency are not used, as these are defined in terms of LWR characteristics. This standard uses reactor technology risk metrics such as accident frequency and dose, risk of offsite consequences, and safety goal risk metrics.
- Rather than separating requirements for Level 1, Level 2, and Level 3 PRAs, the non-LWR standard covers event sequence development from initiating events to determination of offsite radiological consequences. This facilitates PRA performance for reactors with different fission product barrier concepts and different safety design approaches.

This standard was issued for trial use in December 2013. During the initial trial use period there were a number of pilot applications that provided useful feedback. The trial use applications included a variety of HTGRs and liquid metal cooled designs. In September 2017, the ASME/ANS Joint Committee on Nuclear Risk Management (JCNRM) approved a plan to extend the trial use period to incorporate insights.

As part of the Southern Company led Licensing Modernization Project (LMP), the NRC staff has indicated its intention to take an active role in the development of the final version of this standard with a view towards endorsing it for use in licensing future advanced non-LWRs. The intended licensing applications envisioned for PRAs developed under this standard include selection of licensing basis events (LBEs), safety classification and development of performance requirements for SSCs, and risk-informed and performance based evaluation of defense-in-depth (DID).

Noteworthy Content

The purpose of the PHA-to-PRA effort is to demonstrate how the work that is necessary to build a PRA model can be supported through the conduct of PHAs and the use of system engineering tools. This standard may be viewed as describing the target set of technical requirements that the resulting PHA and PRAs will need to meet.

The early stages of PRA model building will need to define plant operating states, initiating events, event sequences, success criteria development, and systems analyses (discussed in Sections 4.5.1 through 4.5.5 of the standard). These PRA requirements/information needs will likely have the greatest influence on the requirements for an effective PHA-to-PRA transition.

With regard to initiating event development, the very first technical requirements IE-A1, IE-A2, and IE-A9 call out a role for the use of a structured, systematic process for identifying initiating events that accounts for plant-specific features; the latter two specifically mention HAZOPs and FMEA as methods to be used.

The following elements of the Body of Knowledge are especially relevant to this reference (section cross-references correspond to those in the standard, not this report):

- System Engineering/System Decomposition – See Ref. 5, Section 4.5.5.
- Process Hazard Analysis and Early Stage Safety Analysis – See Ref. 5, Section 4.5.2.
- Event Sequence Diagrams/Event Trees- See Ref. 5, Section 4.5.3.
- Fault Tree Analysis – See Ref. 5, Section 4.5.4.
- Data Collection and Analysis- See Ref. 5, Section 4.5.7.
- Handling of Uncertainties – Each section of the technical requirements in Ref. 5, Section 4.5 has specific requirements for identifying and evaluating uncertainties.
- Operations/Internal Events PRA – See Ref. 5, Section 4.5.6 for HRA, internal events are embedded in the different sections within Ref. 5, Section 4.5.
- Prior Advanced Reactor PRAs – See prior discussion on the pilot PRAs that have used this standard.

3.4.2.2 U.S. NRC Regulatory Guide 1.200, An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities

The purpose of NRC Regulatory Guide 1.200 [2] is to provide guidance to licensees for use in determining the technical adequacy of the base PRA used in a risk-informed regulatory activity, and to endorse standards and industry peer review guidance. The Regulatory Guide provides guidance in four areas, including:

- A definition of a technically acceptable PRA,
- The NRC's position on PRA consensus standards and industry PRA peer review program documents,
- Demonstration that the baseline PRA (in total or specific pieces) used in regulatory applications is of sufficient technical adequacy, and
- Documentation to support a regulatory submittal.

In order to define a technically acceptable PRA, guidance is provided regarding the scope of a PRA, technical elements of a full-scope PRA and their associated attributes and characteristics, level of detail of a PRA, and the development, maintenance, and upgrade of a PRA. The scope of a PRA is determined by its intended use and can be further defined in terms of the metrics used to characterize risk, the plant operating states for which the risk is to be evaluated, and the causes of initiating events (i.e., hazard groups) that can potentially challenge and disrupt the normal operation of the plant. The level of detail of the PRA is also determined by its intended use, and the minimal level of detail is implicit in the technical elements comprising the PRA and their associated characteristics and attributes. Finally, because a PRA is a "living" document that is intended to eventually represent the as-built, as-operated plant[9]. The PRA should be maintained and upgraded to ensure it represents the system as accurately as needed to support the application.

The standards and guidance referenced by the Regulatory Guide include the ASME/ANS RA-Sa-2009 standard [1] and guidance developed by NEI focused on peer review processes. In order to clarify the NRC's position on the content of these documents, the Regulatory Guide addresses each of the requirements given in the ASME/ANS RA-Sa-2009 or the NEI documents and explicitly summarizes the NRC position in one of three categories:

- No objection.
- No objection with clarification. The Staff has no objection to the requirement. However, Staff provides its understanding to requirements that in their view were unclear or ambiguous.
- No objection subject to the following qualification. The Staff has a technical concern with the requirement as written and has provided a path to resolve its concern.

Noteworthy Content

Concerning early stage safety analyses, two high level requirements, both pertaining to the identification and characterization of potential scenario initiators, (HRL-IE-A and HRL-IE-B) are directly applicable. These can be found in ASME/ANS RA-Sa-2009 (p. 41).

HRL-IE-A requires that "the initiating event analysis shall provide a reasonably complete identification of initiating event." Ten supporting requirements (IE-A1 through IE-A10) are associated with this high level requirement (page 42 of ASME/ANS RA-Sa-2009). In summary, they call for a systematic approach to the identification of plant-specific initiators, including the requirement to consider multi-unit site initiators. The Regulatory Guide only has a requirement for 'clarification' for two of the supporting requirements (IE-A5 and IE-A6, pages A-8 and A-9). IE-A5 calls for the systematic evaluation for each system. The Regulatory Guide clarifies that this evaluation 'where necessary' should go down to the subsystem or train level to meet the minimum requirements. To meet 'beyond minimum requirement' (so called Category III), the Regulatory Guide gives the option of "other systematic process(es)" to the ASME/ANS RA-Sa-2009 requirement of performing a failure mode and effects analysis (FMEA).

[9] At early stages, the intent is for the PRA model to reflect the as-designed plant.

HRL-IE-B pertains to how the candidate initiators are to be grouped for further consideration in the PRA to facilitate an "effective but realistic estimation of Core Damage Frequency (CDF)." It has already been noted that the risk metrics embodied in ASME/ANS RA-Sa-2009 may not be optimum or applicable to non-LWR technologies. Five supporting requirements (IE-B1 through IEB5) are associated with this high level requirement. These can be found on page 45 of ASME/ANS RA-Sa-2009. These supporting requirements address detailed considerations when forming groups of initiators that will be represented as having common plant response requirements. Note that supporting requirement IE-B2 calls for a structured and systematic process for grouping initiating events. Specific examples listed are the use of master logic diagrams, heat balance fault trees, or failure modes and effects analysis. The Regulatory Guide listed 'no objections' to the ASME/ANS RA-Sa-2009 supporting requirements for HRL-IE-B.

The expectations described in the Regulatory Guide anticipate that the licensee's description of an application will include the following:

- SSCs, operator actions, and plant operational characteristics affected by the application,
- A description of the cause-effect relationships caused by the change to the above SSCs, operator actions, and plant operational characteristics,
- Mapping of the cause-effect relationships onto PRA model elements,
- Identification of the PRA results that will be used to compare against the applicable acceptance criteria or guidelines and how the comparison is to be made, and
- The scope of risk contributors (hazard groups and modes of operation) included in the PRA to support the decision.

3.4.2.3 IAEA TECDOC-1804, Attributes of Full Scope Level 1 Probabilistic Safety Assessment (PSA) for Applications in Nuclear Power Plants

The expanded use of PRA[10] in the integrated risk informed decision-making process requires that the PRA possess certain features to ensure its technical consistency and quality. This publication [4] aims to further promote the use and application of PRA in IAEA Member States by providing a comprehensive list of PRA applications and describing what technical features (termed 'attributes') of a PRA need to be satisfied to reliably support the PRA applications of interest. Consideration has also been given to the basic set of attributes characterizing a 'base case PRA' that is performed to assess overall plant safety. This publication can support PRA practitioners in appropriate planning of a PRA project taking into account possible uses of the PRA in the future. It can also be used by reviewers as an aid in assessing the quality of PRAs and judging the adequacy of a PRA for particular applications.

This publication supersedes IAEA-TECDOC-1511, "Determining the Quality of Probabilistic Safety Assessment (PSA) for Applications in Nuclear Power Plants" (published in 2006), which provided detailed information on technical features of a restricted scope PRA aimed at analyzing only internal initiating events caused by random component failures and human errors, and accident sequences that may lead to reactor core damage during operation. The new publication

[10] The IAEA and other many other international entities use the term "Probabilistic Safety Assessment" in lieu of the equivalent "Probabilistic Risk Assessment". For consistency, terminology has been harmonized such that PRA is used throughout this report. Therefore, all discussions in the document summaries refer exclusively to PRA.

extends the scope of the PRA to cover a broader range of internal and external hazards, and low power and shutdown modes of nuclear power plant operation. In addition, some PRA aspects relevant to lessons learned from the accident at the Fukushima Daiichi nuclear power plant are also considered.

In 2010 the IAEA published two Safety Guides: SSG-3 "Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants" [3] and SSG-4 "Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants" [6]. These Safety Guides provide a comprehensive, but still high level, set of recommendations on specific features of Level 1 and Level 2 PRA for all types of initiating events and hazards and operating conditions. The Safety Guides were not aimed at providing detailed information on state-of-the-art features of PRA in the view of various PRA applications. The purpose of this TECDOC is to fill those gaps by providing detailed attributes of a PRA that are not explicitly addressed in SSG-3 and SSG-4. The international participants in preparing this TECDOC included several co-authors of ASME/ANS RA-Sb-2013 and ASME/ANS-RA-S-1.4-2013, so there is a certain level of consistency between these documents; however, the TECDOC is expressed in a set of attributes for PRA applications rather than as technical requirements for performing a PRA which was the purpose of the PRA standard.

Noteworthy Content

- The role of this document to the PHA-to-PRA project is similar to ASME/ANS-RA-S-1.4-2013 in that it represents the end goal of the transition in terms of what information is required to support PRA development.
- The attributes in Section 6 regarding initiating events analysis are particularly relevant to the development of Master Logic Diagrams and FMEAs for the selection of initiating events.
- Section 7 on accident sequence analysis is quite relevant to the PRA tasks of event sequence diagram and event tree development.
- Like ASME/ANS-RA-S-1.4-2013, this document supports PRA of multi-unit plants and there are selected attributes throughout the TECDOC for multi-unit PRAs as well as special risk metrics for that purpose in Appendix I.
- A limitation of this resource is that it is focused on PRAs on operating LWRs and, unlike ASME/ANS-RA-S-1.4-2013, has no specific attributes for PRAs performed during design for advanced non-LWRs.

3.4.3 Summary Observations

The documents reviewed in this section identify standards for achieving technical adequacy of PRAs in general as well as PRAs for advanced non-LWRs. It is likely that the requirements in these standards will evolve as risk-informed design and licensing of non-LWRs move forward. However, for the objectives of the P2P Project, understanding the requirements for the resulting PRAs will help identify the key inputs from PHA that will facilitate the development of technically adequate PRAs. The challenge for advanced non-LWRs is for the PRAs to reflect the

most important safety issues for each reactor. Once these issues are identified through such tasks as defining the reactor specific safety functions to be modeled in the PRA, the application of traditional PRA modeling techniques such as event tree and fault tree analysis is expected to be straight-forward.

Note that NRC Regulatory Guide 1.200 references the ASME/ANS RA-Sa-2009, which in turn is focused on LWR technology. In addition to extensive use of LWR terminology, the Guide addresses risk metrics (core damage frequency and large early release frequency) that are not meaningful to some non-LWR technologies.

3.4.4 References

1. Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications. Addendum A to RA-S-2008. ASME/ANS–RA-Sa-2009. American Society of Mechanical Engineers/American Nuclear Society, February 2009.
2. U.S. Nuclear Regulatory Commission. *An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities. Revision 2*. Regulatory Guide 1.200. Washington, D.C., March 2009.
3. *Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants*. IAEA Safety Standards Series No. SSG-3. Vienna (Austria): International Atomic Energy Agency, 2010.
4. *Attributes of Full Scope Level 1 Probabilistic Safety Assessment (PSA) for Applications in Nuclear Power Plants*. IAEA-TECDOC-1804. Vienna (Austria): International Atomic Energy Agency, 2016.
5. *Probabilistic Risk Assessment Standard for Advanced Non-LWR Nuclear Power Plants*. (Trial Use Draft Standard). ASME/ANS RA-S-1.4-2013, American Society of Mechanical Engineers/American Nuclear Society, December 2013.
6. *Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants*. IAEA Safety Standards Series No. SSG-4. Vienna (Austria): International Atomic Energy Agency, 2010.

3.5 Previous Advanced Reactor PRAs

3.5.1 Background

There is well-documented experience with performance of PRAs on some advanced non-LWR designs. This experience spans a period almost as long as LWR PRAs. For example, the PRA that was performed at General Atomics in the 1970s [1] was initiated shortly after the initiation of the Rasmussen study, WASH-1400, on LWRs [2].

This PRA, which was performed on a large 3000MWt prismatic fueled HTGR, was responsible for pioneering work in common cause failure modeling and was the first PRA to address accident sequences initiated by internal fires. However, the most extensive body of work on advanced non-LWR PRAs has been performed on sodium-cooled fast reactors. The molten salt cooled family of reactors has benefitted from the least amount of prior work in PRA

development. The collective body of work on all the advanced non-LWR PHAs and PRAs provides useful guidance for developing PRAs for any type of advanced reactor. This body of work includes specific examples of how the following technical issues in advanced reactor PRA can be addressed:

- Reliability assessment of passive safety systems,
- PRA modeling of accidents involving two or more reactor modules or non-core radionuclide sources,
- PRA database development for reactors with little or no service experience,
- Development of risk metrics appropriate for innovative reactor fuel and radionuclide barrier configurations, and
- Use of the PRA to identify licensing basis events, SSC safety classification and special treatment, and evaluation of defense-in-depth adequacy.

A summary of some selected advanced reactor PRAs and their supporting references are provided in Table 3-1
Summary of selected advanced non-LWR PRAs. Several of these references are reviewed in the following section.

Table 3-1
Summary of selected advanced non-LWR PRAs

Reactor Type	PRA	Applicability
Sodium Cooled Fast Reactor [3]	PRISM – 2017 [4] PRISM – 1986 [5,6]	Pool type SFR similar to EBR-II
	EBR-II – 1991	Pool type SFR
	SAFR- 1988 [7]	Pool type SFR
	CRBR – 1984 [8]	Loop type SFR
High Temperature Gas Cooled Reactor	MHTGR – 1987 [1, 9]	Modular HTGR, Prismatic Fuel
	AIPA – 1978 [10]	Large HTGR, Prismatic Fuel
Molten Salt Reactor	FHR – 2013 [11]	Fluoride salt cooled pebble bed reactor
All Non-LWRs	LMP PRA – 2017 [12]	All non-LWRs with specific examples for MHTGR and PRISM

3.5.2 Technical Discussion

3.5.2.1 PRISM PRA 2017, Development of Advanced Non-LWR PRAs

In 2015, GE-Hitachi Nuclear Energy (GEH) teamed with Argonne National Laboratory (ANL) to perform Research and Development (R&D) of next-generation Probabilistic Risk Assessment (PRA) methodologies for the modernization of an advanced non-LWR PRA. This effort,

discussed in [4], built upon a PRA developed in the early 1990s for GEH's Power Reactor Inherently Safe Module (PRISM) Sodium Fast Reactor (SFR). The work had four main tasks: internal events development, modeling the risk from the reactor for hazards occurring at-power internal to the plant; an all hazards scoping review to analyze the risk at a high level from external hazards, such as earthquakes and high winds; an all modes scoping review to understand the risk at a high level from operating modes other than at-power; and risk insights to integrate the results from each of the three phases above.

To achieve these objectives, GEH and ANL used and adapted proven PRA methodologies and techniques to build a modern non-LWR, all hazards/all modes PRA. The teams also advanced non-LWR PRA methodologies, which is an important outcome from this work. This report summarizes the project outcomes in two major phases. The first phase presents the methodologies developed for non-LWR PRAs. The methodologies are grouped by scope, from Internal Events At-Power (IEAP), to hazards analysis, to modes analysis. The second phase presents details of the PRISM PRA model which was developed as a validation of the non-LWR methodologies. The PRISM PRA was performed in detail for IEAP, and at a broader level for other hazards and modes.

The two phases were strategically linked to maximize the combined impact. The project built upon what was a state-of-the-art PRA for its era, and brought it in-line with current expectations of a modern PRA. This was done by advancing the non-LWR methodologies, by adapting Advanced Light Water Reactor (ALWR) methods, by addressing issues required by the trial use ASME/ANS PRA standard for advanced non-LWRs [13], and by creating new PRA tools. These two project objectives were accomplished through an engagement between industry (GEH) and the Department of Energy (DOE) laboratories (ANL). In addition to contributing methodologies, this project developed risk insights applicable to non-LWR PRA, including focus-areas for future R&D, and conclusions about the PRISM design.

Noteworthy Content

What is particularly noteworthy about this reference is the fact that it was performed, in part, to pilot the non-LWR PRA standard (ASME/ANS-RA-S-1.4-2013), and lessons learned from this pilot and other pilots are being used to revise the standard for full endorsement by the American National Standards Institute. Although details of this PRA are covered in proprietary reports, there are a number of technical aspects of the study presented at two recent international conferences as indicated below.

Five papers presented at the American Society of Mechanical Engineers 24th International Conference on Nuclear Engineering (ICONE 24), Charlotte, NC, June 26-30, 2016:

- ICONE24-60749, "A Methodology for the Integration of Passive System Reliability with Success Criteria in a Probabilistic Framework for Advanced Reactors," Acacia J. Brunett, Dave Grabaskas, Matthew Bucknor, and Stefano Passerini, Argonne National Laboratory.
- ICONE24-60759, "A Methodology for the Integration of a Mechanistic Source Term Analysis in a Probabilistic Framework for Advanced Reactors," Dave Grabaskas, Acacia J. Brunett, and Matthew Bucknor, Argonne National Laboratory.

- ICONE24-60760, "A Methodology for the Development of a Reliability Database for an Advanced Reactor Probabilistic Risk Assessment," Dave Grabaskas, Acacia J. Brunett, and Matthew Bucknor, Argonne National Laboratory.
- ICONE24-61199a, "Development of Non-LWR PRA Methodologies for an Advanced Non-LWR Technology Using a Risk-Informed Framework, Matt Warner," Jonathan Li, and Jordan Hagaman, GE-Hitachi.
- ICONE24-61199b, "Demonstration of a Non-LWR Success Criteria Methodology in a Probabilistic Framework for Advanced Reactors," Jonathan Li and Jordan Hagaman, GE-Hitachi.

One paper presented at the 13th International Conference on Probabilistic Safety Assessment and Management (PSAM 13), Seoul, Korea, October 2-7, 2016:

- PSAM13-A-651, "PRISM Internal Events PRA Model Development and Results Summary," Matthew Warner, Jonathan Li, Jordan Hagaman, Gary Miller, and Dennis Henneke, GE-Hitachi.

These public domain references highlight noteworthy aspects of the PRA. The summary report provides guidance for how to treat several issues common to many advanced reactor technologies including:

- Reliability treatment of passive systems that includes a quantitative evaluation of passive phenomena,
- Developing a PRA database relevant to a particular technology,
- Methodology for screening hazards,
- Methodology for modeling multi-module event sequences, and
- Mechanistic source term development.

3.5.2.2 Modernization of Technical Requirements for Licensing of Advanced Non-Light Water Reactors: Probabilistic Risk Assessment Approach

This report [12] represents a key element in the development of a framework for the efficient licensing of advanced non-light water reactors (non-LWRs). It is the result of a Licensing Modernization Project (LMP) led by Southern Company and cost-shared by DOE. The project builds on best practices as well as previous activities through DOE and industry-sponsored advanced reactor licensing initiatives.

The LMP objective is to assist the NRC in developing regulatory guidance for licensing advanced non-LWR plants. In this paper, the LMP is seeking:

- NRC's approval of the proposed technology-inclusive probabilistic risk assessment (PRA) approach for incorporation into appropriate regulatory guidance for advanced non-LWRs, and
- Identification of any issues that have the potential to significantly impact the use of risk insights derived from the PRA in the selection and evaluation of Licensing Basis Events (LBEs) and safety classification of systems, structures, and components (SSCs).

This report outlines the approach to develop a PRA for advanced non-LWR plants in support of Risk-Informed, Performance-Based (RIPB) applications including:

- Evaluation of design alternatives and incorporation of risk insights into early and continuing development of the design,
- Input to the selection of LBEs, and
- Input to the safety classification of SSCs.

The PRA approach described in this report is specifically designed to be reactor technology-neutral so that it can be used to support all the reactor technologies currently under development. Additional papers under development as part of the LMP address how the PRA is used to support additional risk-informed decisions including:

- Selection of performance requirements for the capabilities and reliabilities of SSCs in the prevention and mitigation of anticipated transients and accidents (the proposed application of special treatment is based on the method of defining risk significance as described in this paper), and
- Risk-informed and performance-based evaluation of defense-in-depth adequacy.

The applications envisioned for the PRA within the LMP framework help define the PRA capabilities and also the useful outputs of the PHA that will be required. Current regulatory requirements require the development of a PRA. The vision of the LMP is to introduce the PRA at an early stage of design to maximize the return on the PRA investment.

Future advanced non-LWR license applications will include a design-specific PRA that is capable of supporting the above listed applications. When introduced at an early stage of the design, the PRA is expected to result in a more efficient risk management process. As described herein, the PRA is introduced at an early stage in the design, and subsequently upgraded in terms of scope and level of detail at various design and licensing stages as the design matures and the design and siting details are defined. At each stage of the design/PRA development process, information from the PRA will be available to support decisions on the selection and evaluation of design options and to help formulate requirements on the capability and reliability of SSCs in the prevention and mitigation of accidents.

Key elements discussed in this report include the PRA scope and objectives, regulatory guidance used in the formulation of these objectives, and the methodology for factoring the objectives into the proposed technology-inclusive PRA framework. These PRA elements are first described in terms of a technology-inclusive framework supplemented with examples of PRA models for specific non-LWR designs including a modular high temperature gas-cooled reactor and a pool-type sodium-cooled fast reactor.

Noteworthy Content

The noteworthy content in this reference is highlighted in the following:

- The paper describes a reactor technology-neutral (i.e., technology-inclusive) approach to development of a PRA model based on a systematic identification and evaluation of radionuclide sources, barriers to release of these sources, safety functions that protect the barriers and serve to prevent and mitigate release of radioactive material.
- The PRA approach to establishing technical adequacy is tightly tied to the ASME/ANS *PRA Standard for Advanced Non-LWR Nuclear Power Plants* (ASME/ANS RA-S-1.4-2013) [13].
- The approach to PRA uses technology-neutral risk metrics such as frequency and dose, individual risks as defined in the NRC Safety Goal Quantitative Health Objectives, as well as user defined metrics that make sense for specific reactor types.
- Guidance is provided for development of a PRA model at an early stage of design with interfaces to systems engineering and process hazards analyses that are part of the reactor design process. PHA is identified as one of the analytical tools that are used to help select initiating events and develop event sequences for the PRA. A key concept advanced in the report is the recommendation to introduce the PRA development at an early stage of design and control the scope and level of detail of the PRA models to the level of design, operation, and siting information available at that stage of design. Risk-informed decisions supported by the PRA are then revisited as the design, scope, and detail of the PRA mature.
- Example PRA developments are presented to illustrate the approach using the MHTGR and PRISM reactors. The report includes guidance for development of event sequence diagrams and event trees and discusses the question of how to develop a PRA database for reactors with limited or no service experience (with an emphasis on the treatment of uncertainties) with references to examples from MHTGR and PRISM.
- The PRA development for modular reactor designs includes the definition of event sequences involving one as well as two or more reactor modules or radiological sources. Event frequencies are expressed in terms of events per (multi-module) plant year. This is to ensure that the designer address the potential for multi-module accidents at an early stage.
- A technology-inclusive approach to defining risk significance of licensing basis events and SSCs is defined in this report and refined further in companion LMP papers on SSC safety classification and evaluation of defense-in-depth adequacy.
- The NRC staff is reviewing the LMP framework. Documentation of this review and potential endorsement is expected in the form of a NUREG report.

3.5.3 Summary Observations

It is very useful to understand how previous non-LWR PRAs were performed, even if the reactor technology is substantially different that that being developed. All non-LWRs share many of the same types of technical issues such as how to address passive system reliability, plant designs with multiple reactor modules, lack of operational data to support PRA database development, and how to structure the PRA. Of all the non-LWR PRAs performed to date, the PRISM 2017 PRA [4] is the only one that addresses the requirements in the ASME/ANS *PRA Standard for Advanced Non-LWR Nuclear Power Plants* [13]. This PRA provides guidance for how to address these technical issues that practically all the advanced reactor technologies share.

3.5.4 References

1. *Probabilistic Risk Assessment for the Standard Modular High Temperature Gas-Cooled Reactor. Vol. 1 and 2*. Rev. 3. DOE-HTGR-86-011. GA Technologies, Inc., San Diego, CA: January 1987.
2. Rasmussen, Norman C., et al. *Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants*. WASH-1400 (NUREG-75/014). Washington, D.C.: U.S. Nuclear Regulatory Commission, October 1975.
3. Grabaskas, D. *A Review of U.S. Sodium Fast Reactor PRA Experience*. 12th International Conference on Probabilistic Safety Assessment and Management (PSAM 12), Honolulu, Hawaii, June 22 – 27, 2014.
4. Henneke, Dennis and James Robinson. *Final Scientific/Technical Report: Development of Advanced Non-LWR PRAs*. DOEGEHH08325. GE-Hitachi Nuclear Energy Americas LLC, March 2017.
5. *PRISM - Preliminary Safety Information Document*. GEFR-00793 UC-87Ta, GE Nuclear Energy, Advanced Nuclear Technology, San Jose, CA: November 1986.
6. U.S. Nuclear Regulatory Commission. *Pre-application Safety Evaluation Report for the Power Reactor Innovative Small Module (PRISM) Liquid Metal Reactor*. NUREG-1368, Washington, D.C., 1994.
7. U.S. Nuclear Regulatory Commission. *Pre-application Safety Evaluation Report for the Sodium Advanced Fast Reactor (SAFR) Liquid-Metal Reactor*. NUREG-1369. Washington, D.C., 1999.
8. *Clinch River Breeder Reactor Plant Probabilistic Risk Assessment*. CRBRP-4. Technology for Energy Corp., Knoxville, TN: 1984.
9. U.S. Nuclear Regulatory Commission. *Draft Pre-application Safety Evaluation Report for the Modular High Temperature Gas-Cooled Reactor*. NUREG-1338. Washington, D.C., March 1989.
10. *HTGR Accident Initiation and Progression Analysis Status Report - Phase II Risk Assessment*. General Atomic Company, San Diego, CA: April 1978. Report GA-A15000.
11. *Fluoride-Salt-Cooled, High-Temperature Reactor (FHR) Subsystems Definition, Functional Requirement Definition, and Licensing Basis Event (LBE) Identification White Paper*. University of California, Berkeley, CA: August 2013. Report UCBTH-12-001.

12. Southern Company Services. *Modernization of Technical Requirements for Licensing of Advanced Non-Light Water Reactors: Probabilistic Risk Assessment Approach*. Draft Revision A. SC-29980-101. (Issued for Collaborative Review) 2017.

13. *Probabilistic Risk Assessment Standard for Advanced Non-LWR Nuclear Power Plants*. (Trial Use Standard) ASME/ANS RA-S-1.4-2013, American Society for Mechanical Engineers/American Nuclear Society, December 2013.

3.6 Data Collection and Analysis and Treatment of Uncertainties

3.6.1 Background

It is often questioned how one can perform a PRA on a new reactor technology that has not yet gained significant operational experience. A similar question was raised before the first LWR PRA was performed. This question appears to confuse the methods of probabilistic risk assessment (PRA) and statistical analysis.

PRA is an investigation of rare events for which direct statistical data is insufficient to characterize risks. There is a role for statistical analysis to support a PRA, but it is performed at the level of component failures and other causes of accidents and not the overall plant risk. The first major PRA of nuclear reactor accidents in the U.S. was the Rasmussen study [1] which was completed in 1975 before there had been a significant accumulation of service experience. The risk models and their quantifications employed in this study did not use *any* statistical analysis of LWR service experience; rather, the estimates of event frequencies, accident causes, and component failure rates were based exclusively on information from non-nuclear industries. The results of the Rasmussen study -- among them the identification of the risk significance of small loss of coolant accidents (LOCAs), human errors, and support system faults -- had a major impact on the understanding of nuclear safety issues, despite not having benefitted from the accumulation of appreciable service experience.

There are three major categories of advanced non-LWRs being considered today, including: high temperature gas-cooled reactors, liquid metal-cooled fast reactors, and molten salt reactors. PRAs have been in development and application for the first two categories of reactors for more than 40 years, and recently, efforts to develop PRAs for MSRs have been initiated. In contrast with the challenges faced by Rasmussen in the 1970’s, these advanced reactor PRAs benefit (to a degree) from using many components and systems that are common to operating reactors and, therefore, benefit from the operating reactor service experience which has been responsible to reduce uncertainties in estimating PRA component level data. These advanced non-LWR technologies have produced designs that are less complex and contain fewer systems and components than operating reactors. This is because the essential safety functions are performed using inherent or passive means, rather than complex engineered systems using active components. Hence the scope of the PRA data requirements in performing advanced reactor PRA may be less demanding than the data challenges faced by Rasmussen. For components unique to each advanced reactor, there is evidence to support the estimation of failure data from research and test reactors, and non-reactor facilities that have service conditions similar to those in the reactors.

The primary justification for introducing PRA technology to risk-inform the design and safety/licensing bases is that PRA is an available and proven technology that has the capability to identify potential accident sequences in a systematic, exhaustive, and reproducible way. PRA also has a well-established capability of identifying sources of uncertainty in analyzing reactor behavior during accidents, and for treating uncertainties in an objective, quantitative manner. The design basis accidents for the current fleet were derived using expert judgments, prior to the availability of significant operating experience and were subsequently amended as service experience was accumulated. Following the advent of PRA, the analysis of uncertainties in reactor behavior became more systematic, complete, and less reliant on subjective judgments. The premise that one cannot do a PRA until there is a lot of service experience reflects a fundamental misunderstanding of the nature of PRA and its relationship to statistics.

There is an excellent summary of PRA database development for SFRs in the PRISM 2017 PRA [2]. Data collected from gas-cooled reactor service experience and other sources to support HTGR PRAs are summarized in the MHTGR 1987 PRA [3]. Data from the process industry [4] and experience with experimental reactors is also available to support PRAs on molten salt reactors. When the PRA process for incorporating our state of knowledge is understood, the goal is to collect the evidence on SSC performance that transcends statistical data and includes all forms of expert information. The key question is whether the assessment of uncertainties in the estimation of PRA parameters adequately accounts for the state of knowledge.

In his 1990 journal article, S. Kaplan [5] presents a method of utilizing evidence to enhance expert knowledge in support of performing a PRA. Essentially, the approach focuses on establishing the set of evidence relevant to a particular parameter for which a quantitative estimate is to be determined. The experts identify this evidence after the context of the parameter is made clear. Establishing a probability curve that expresses the evidence in total is the task of the PRA analyst, although this step is performed with the expert group. More common “expert opinion” approaches call on the experts to express estimates of this probability curve, or merely give point estimates. The Kaplan “expert information” approach, by insisting on focusing on the available evidence, reduces the chance that individual experts might have different understanding of the context of the parameter of interest. This approach is particularly relevant to the estimation of parameters (such as failure rates) in systems that have insufficient operating experience to determine the parameters directly and statistically (such as advanced non-LWRs).

3.6.2 Technical Discussion

3.6.2.1 Guidelines for Process Equipment Reliability Data (with Data Tables)

The primary purpose of this reference [4] is to provide engineers and risk analysts with failure rate data needed to perform a Chemical Process Quantitative Risk Analysis (CPQRA). The reference contains accessible data in the CCPS Generic Failure Rate Data Base, information on several available generic data resources, and procedures to develop failure rate data using information from the plant and process being studied. Another objective of the reference is to present an approach that coordinates the collection of raw plant data, their conversion into plant-specific failure data, and their storage using a Chemical Process Inventory (CPI) oriented taxonomy. This approach is intended to allow future data generated by chemical process facilities to be added to the CCPS Generic Failure Rate Data Base. The reference also provides specifications for the transfer of data in hopes that the approach and standardization will

stimulate the chemical processing industry to generate and transfer failure rate data to CCPS for industry use. Finally, the reference is written to help engineers and analysts develop an understanding of the derivation, usefulness, and limitation of failure rate data so they can form better judgements about the use of data.

The data presented in the book are characterized as equipment failures per 10^6 operating hours for time-related failure rates and failures per 10^3 demands for demand-related failure rates. These rates are given for some common CPI equipment. In preparing the book, the CCPS Subcommittee tried to review all published sources of available generic equipment reliability and failure rate data, including reliability studies, published research works, reliability data banks, or government reports that contained information gathered from chemical process, nuclear, offshore oil, and fossil fuel industries around the world. An industry survey was conducted to solicit unpublished data.

Noteworthy Content

- Explanation of the meaning of generic and plant-specific data, the difference between time-related and demand-related failures, issues of confidence and tolerance, what is captured as an equipment failure, the failure model used, and the role of the taxonomy.
- Explanation of the CCPS taxonomy, including the rationale and process for its development and the factors considered in its construction.
- Summary of several generic data resources available to risk analysts and process engineers in the CPI, including a discussion of the resource search and selection process and the presentation format for the information on resources.
- Tables of generic process equipment reliability data that are structured by the CCPS Taxonomy.
- A discussion of the selection, treatment, and presentation of the data in the Tables.
- Description of the type of data required and their treatment to develop a plant-specific data set suitable for use or aggregation with other data.
- A form to facilitate the transfer of plant-specific data to the CCPS Data Base or to combine it with other generic data.
- A collection of references that describe data collection, analysis, and application techniques but, in general, do not contain reliability data.
- A list of data resources that were identified too late for review.

3.6.2.2 IAEA-TECDOC-478, Component Reliability Data for Use in Probabilistic Safety Assessment

In response to the needs of member states conducting or planning to initiate probabilistic safety assessments (PSA is IAEA term for PRAs), the IAEA carried out a compilation of component reliability data from the publicly available literature [6]. The IAEA Data Base Version 1.0 consists of about 1000 records compiled from 21 different data sources (listed in Appendix 1) and includes all data for nuclear power plant components usually modeled in PRAs. No attempt

was made to interpret or adapt the information contained in the original sources. Therefore, the records of the IAEA Data Base are established directly from the information provided by the sources surveyed. A peer review was conducted at the end of the compilation and all records have been verified.

Appendix 2 to the report provides detailed descriptions and definitions of the major generic failure modes considered during compilation of the Data Base. Two appendices provide listings of the component groups and types together with associated codes. These appendices help the user in selecting the most appropriate components according to codes. Finally, all Data Base records are listed in the last Appendix, sorted in alphabetical order of component.

Components in the IAEA data base can be divided into four major categories:

- Mechanical components (*e.g.*, piping and heat exchangers);
- Electrical equipment (*e.g.*, transformers and relays);
- Instrumentation and control equipment; and
- Emergency power sources.

There is an important section that addresses challenges associated with component reliability databases, including inconsistencies in terminology and inconsistencies in environmental conditions under which data has been collected from various sources. The document also discusses difficulties in collecting in-plant reliability data from maintenance work orders and logbooks. Both sources can suffer from failure to document relevant events.

Noteworthy Content

Reliability data is an essential part of a PRA, and the quality of the data can have a significant effect on the quality of the study as a whole. The IAEA Data Base compiles component reliability from many different publications to facilitate the use of generic data from existing literature, since reliance on failure data originating from the specific plant being analyzed is rarely possible. This report describes in detail the IAEA Data Base format, including the record form and associated coding system. It also describes each data source surveyed and briefly qualifies special features of each. Challenges connected with data bases found in literature are also highlighted in the report. However, the most valuable aspect of the IAEA document is the ~200-page compendium of raw component reliability data organized by component.

The utility of the component reliability data in this document is enhanced by two separate reports on component reliability prepared at about the same time as the subject report [7, 8]. The first report compares reliability data for similar components from various sources in graphical form to give some perspective on data uncertainties. The second report constitutes the proceedings of an IAEA technical committee meeting focused on the role of reliability data, data bases in member states, data management and analysis, and aspects deserving special attention by those collecting and using reliability data.

3.6.2.3 'Expert Information' versus 'Expert Opinions'- Another Approach to the Problem of Eliciting/Combining/Using Expert Knowledge in PRA

The "expert information" approach advocated in the paper by Kaplan [5] puts the emphasis on direct knowledge that can be used to estimate a parameter for a PRA, rather than on the ability to process or encode this knowledge into estimates of a parameter of interest. The approach attempts to develop a very clear written statement of a "total body of evidence" containing all evidence relevant to a parameter that has been collected, fully discussed, and clarified to the extent that a group of experts is willing to agree that the body of evidence constitutes the total evidence of the group relevant to the parameter. By eliciting this experience and information from the expert group, rather than simply opinions regarding the value of the parameter, issues of bias and honesty (conscious or unconscious) can be addressed. Thus, the body of evidence that is developed can be used to construct a consensus state-of-knowledge (probability) curve for the parameter that can be used for PRA activities.

Following a description of the method, examples are given where the approach has been used to support PRA. First, real-world example involving the quantification of design-specific initiators from the High Flux Isotope Reactor (HFIR) PRA is presented. HFIR is a high power density research reactor, utilizing aluminum encased fuel. The coolant channels are very narrow, leading to the potential for flow blockage, and that could lead to fuel damage. Individual initiator categories were identified that depended on the source region and type of blocking material. Reactor design experts, safety analysts, and the PRA team systematically quantified the frequency (including uncertainty) of the initiator categories. The other two examples concern the reliability of successive generations of helicopter equipment and analysis of 'near miss' launch failures in the space shuttle.

Noteworthy Content

Expert elicitation is as structured process to facilitate understanding and quantification of technical parameters by technical experts. Typically, the process focuses on direct estimation of the parameter of interest such as the probability curve for a particular adverse consequence for use in a PRA, i.e., for the experts to reach consensus to estimate the parameter of interest. Such an approach poses challenges because it requires the experts to translate their accumulated knowledge into the particular form of the parameter of interest, which may be unfamiliar to the experts. This document proposes an alternative elicitation process in which the central activity is to form an expert consensus on the evidence (body of technical knowledge) relevant to determining the parameter of interest. Once this consensus is achieved, translating it to the parameter of interest is more straightforward. By focusing on facts, this approach avoids asking experts to do unfamiliar things, which reduces uncertainties as well as the potential for personality-driven disagreements about the relationship between the opinions of individual experts and their relationship to the parameter of interest. Since the analysis of advanced reactor designs is likely to involve parametric uncertainty, better understanding of the nature and use of expert opinion will be important to the analyst.

3.6.2.4 NUREG-1855, Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decision-making[11]

This document [9] provides guidance on how to treat uncertainties associated with probabilistic risk assessment (PRA) in risk-informed decision-making. The objectives of this guidance include fostering an understanding of the uncertainties associated with PRA and their impact on the results of PRA and providing a pragmatic approach to addressing these uncertainties in the context of the decision-making.

This NUREG focuses on epistemic uncertainty (i.e., uncertainties related to the lack of knowledge) and the guidance provided in the document includes acceptable methods of identifying and characterizing the different types of epistemic uncertainty and the ways that those uncertainties are treated. The different types of epistemic uncertainty are completeness, parameter, and model uncertainty.

- Completeness Uncertainty – Guidance is provided on how to address one aspect of the treatment of completeness uncertainty (i.e., missing scope) in risk-informed applications. This guidance describes how to perform a conservative or bounding analysis to address items missing from a plant's PRA scope.
- Parameter Uncertainty – Guidance is provided on how to address the treatment of parameter uncertainty when using PRA results for risk-informed decision-making. This guidance addresses the characterization of parameter uncertainty, propagation of uncertainty, assessment of the significance of the state-of-knowledge correlation, and comparison of results with acceptance criteria or guidelines.
- Model Uncertainty – Guidance is provided on how to address the treatment of model uncertainty. This guidance addresses the identification and characterization of model uncertainties in PRAs and involves assessing the impact of model uncertainties on PRA results and insights used to support risk-informed decisions.

The ASME/ANS LWR PRA standard [10] (as endorsed by the NRC) provides requirements that need to be satisfied to understand what sources of uncertainty are associated with a PRA. The guidance developed in NUREG-1855 provides an acceptable approach for meeting the ASME/ANS LWR PRA standard with regard to the requirements on uncertainty. The non-LWR PRA Standard, ASME/ANS –RA-S-1.4-2013, has many technical requirements to address sources of uncertainty in all of the PRA technical elements.

<u>Noteworthy Content</u>

- Guidance is provided on addressing the different types of uncertainties and focuses on the type of uncertainty that need to be accounted for in the decision-making.
- This NUREG is the primary reference being used in PRAs for operating reactors as guidance for meeting the uncertainty related requirements.
- For early stage analysis and transition to PRA this guidance should be reviewed to be aware of different types of uncertainty that will need to be addressed. Addressing the specific sources of uncertainty is a key task for the early stage safety analysis.

[11] NUREG-1855 presents the word decision-making as an unhyphenated, compound word.

3.6.3 Summary Observations

The review of the references summarized in this section provides insights into the differences between PRA data analysis and statistical analysis of service data. PRA involves modeling and quantifying the frequencies and consequences of rare events. Treatment of uncertainty and incorporating the available evidence in characterizing the state of knowledge about PRA parameters is the focal point of PRA data analysis. The scope of the data parameters that need to be developed include estimates of initiating event frequencies, component failure rates, frequency and duration of maintenance activities, common cause failure rates and associated parameters, and phenomenological parameters. The goal is to quantify our estimates of these parameters in a manner that fully captures the state of knowledge and resulting uncertainties. When failure rates (or other parameters) are not readily available for an advanced reactor PRA from existing operating experience, use of Kaplan's "expert information" approach to estimate the parameter may be more straightforward to justify than the commonly used "expert opinion" approach.

3.6.4 References

1. Rasmussen, Norman C., et al. *Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants*. WASH-1400 (NUREG-75/014). U.S. NRC, October 1975.
2. Grabaskas D., A. Brunett, and M. Bucknor. "A Methodology for the Development of a Reliability Database for an Advanced Reactor Probabilistic Risk Assessment," American Society of Mechanical Engineers 24th International Conference on Nuclear Engineering (ICONE 24), Charlotte, NC, June 26 – 30, 2016. Paper No. ICONE24-60760.
3. *Probabilistic Risk Assessment for the Standard Modular High Temperature Gas-Cooled Reactor. Vol. 1 and 2. Revision 3*. GA Technologies, Inc., San Diego, CA: January 1987. Report DOE-HTGR-86-011.
4. American Institute of Chemical Engineers, Center for Chemical Processing Safety. *Guidelines for Process Equipment Reliability Data (with Data Tables)*. Hoboken, NJ: John Wiley & Sons, 1989.
5. Kaplan, S. "Expert Information' versus 'Expert Opinions. Another Approach to the Problem of Eliciting/Combining/Using Expert Knowledge in PRA," *Reliability Engineering and System Safety*, Vol. 35, pp. 61-72 (1992).
6. *Component Reliability Data for Use in Probabilistic Safety Assessment*. IAEA-TECDOC-478, Vienna (Austria): International Atomic Energy Agency, 1988.
7. *Survey of Ranges of Component Reliability Data for Use in Probabilistic Safety Assessment*. IAEA-TECDOC-508. Vienna (Austria): International Atomic Energy Agency, 1989.
8. *Evaluation of Reliability Data Sources*. IAEA-TECDOC-504. Vienna (Austria): International Atomic Energy Agency, 1989.
9. U.S. Nuclear Regulatory Commission. *Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decision-making. Revision 1*. NUREG-1855. Washington, D.C., March 2017.

10. *Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications. Addendum A to RA-S-2008*. ASME/ANS–RA-Sa-2009. American Society of Mechanical Engineers/American Nuclear Society, February 2009.

3.7 General and Miscellaneous

3.7.1 Background

The documents reviewed as part of the general and miscellaneous section present perspectives advocating application of several safety processes to the design and operation of nuclear facilities. Unlike the previous sections of this report, the topics discussed in the references covered in this section are applicable to multiple steps of the safety assessment process or to the process in general.

The IAEA TECDOC from the International Conference on Topical Issues in Nuclear Installation Safety Conference [1] provides a compendium of talks presented at the IAEA nuclear installation safety conference in 2013 specifically focused on the defense-in-depth (DID) approach to safety. The objective of the conference was to foster the exchange of information on the latest advances in the implementation of DID in operating nuclear installations, including nuclear power plants, research reactors, and fuel cycle facilities. In addition to focusing on the challenges associated with implementing DID, the conference also covered how lessons learned from operating experience and recent events (such as the accident at Fukushima Daiichi) have been used to enhance the safety of nuclear installations. Because DID is fundamental to the safety of nuclear installations and should be implemented during all stages of the installation life cycle, the concepts covered under this topic are related to the PHA-to-PRA approach discussed in this report. More specifically, the hazard and risk analyses discussed as a part of this process can be used to evaluate if a reactor design provides multiple levels of protection so that potential failures are compensated for in a manner that ensures the protection of the workers, the public, and the environment.

Because safety related terms (such as passive and inherent safety) have been widely used with respect to advanced nuclear reactors, and sometimes have definitions inconsistent with each other, the overall purpose of IAEA TECDOC 626 [2] is to present a technical description of safety related terminology to achieve a better understanding and consensus on the meaning and proper use of terms. The intent of this descriptive glossary approach is to help:

- Eliminate confusion and misuse of the terms by members of the nuclear community, rendering the terms more meaningful, and thereby improving communication within the technical community,
- Clarify technical thinking regarding safety terms used in connection with efforts to enhance safety and thereby to help bring about improvements in future designs, and
- Future acceptance of nuclear power by giving precisely described technical meanings to terms commonly used in public discourse.

With respect to the PHA-to-PRA process as applied to advanced reactors, the consistent use of the definitions contained within this document when discussing the safety approach of a reactor design can minimize confusion regarding the documentation that records the results of different analyses (such as PHAs).

NRC NUREG/CR-1278 [3] is a handbook that presents methods, models, and estimated human error probabilities to enable qualified analysts to make quantitative or qualitative assessments of occurrences of human errors that may affect the availability or operational reliability of engineered safety features and components in nuclear power plants. This NUREG provides most of the modeling and information necessary for the performance of human reliability analysis as part of a PRA for nuclear power plants. Although advanced nuclear reactors may have decreased reliance upon human actions for mitigating accidents, the proper treatment of human error will still be needed for the development of a PRA of significant detail and can produce insights towards the development of training and operational procedures.

3.7.2 Technical Discussion

3.7.2.1 IAEA-TECDOC-CD-1749, Defense-in-Depth – Advances and Challenges for Nuclear Installation Safety

Defense-in-depth (DID) is defined by IAEA as "a hierarchical deployment of different levels of diverse equipment and procedures to prevent the escalation of anticipated operational occurrences and to maintain the effectiveness of physical barriers placed between a radiation source or radioactive material and workers, members of the public, or the environment, in operational states and, for some barriers, in accident conditions." The IAEA conference [1] explored four topical issues involving DID that apply to different states and phases of a nuclear facility: (1) advances and challenges in the implementation of DID in siting, design, and construction, (2) advances and challenges in the implementation of DID in commissioning and operation, (3) advances and challenges in the implementation of DID in accident management and emergency preparedness and response, and (4) cross-cutting issues in the implementation of DID (e.g. safety culture, regulatory oversight, human factors, etc.). In addition, the IAEA TECDOC contains the entirety of each paper presented at the conference. Several overarching conclusions were presented in the closing session and are captured in the reference.

Noteworthy Content

The following conclusions are relevant to the topic of applying DID, as well as the improvement of other safety processes:

- DID is not only relevant for the design of new installations, but should also be maintained/improved by periodic safety reviews over the entire life of installations.
- While DID remains an essential tool for safety and should continue to be applied, further development and guidance are required on several subjects such as:
  - Consistent application of design basis definitions at the international level,
  - Postulation of multiple failures in reactor design,
  - Practical use of deterministic and probabilistic approaches,
  - Assessment of independence and reliability of different levels of DID,

  - Approach to be adopted for very low probability events leading to very large health and safety consequences, and
  - Tools to be based on already developed methodologies to ensure that safety provisions are comprehensive enough to ensure DID.
- Hazards, as well as combinations of hazards, to be taken into account in relation to DID need further work and international guidance.
- IAEA concluded that DID is a proven approach to assess the safety of nuclear installations; however, enhancements to other methods of evaluating safety are necessary, including improved hazard and probabilistic analyses. Specifically, they advocated further development and guidance on the application of multiple safety tools. The IAEA further concluded that safety assessment processes should be active throughout the entire life of a nuclear facility, from design to and through the operating life. This suggestion advocates the use of a safety assessment approach that can be updated and enhanced as more design detail or operating experience is available. PHA methods (such as HAZOP) are designed to provide a systematic approach to comprehensive identification of hazards early in design, while also being amenable to iteration as more information becomes available.

3.7.2.2 IAEA-TECDOC-626 Safety-Related Terms for Advanced Nuclear Plants

This short document [2] contains definitions for the following list of terms relevant to nuclear reactor safety based on the outcomes of a workshop in 1991:

- Inherent safety characteristics,
- Passive component,
- Active component,
- Passive system,
- Active system,
- Fail-safe,
- Grace period,
- Foolproof,
- Fault-/error-tolerant,
- Simplified safety system, and
- Transparent safety.

The criterion for inclusion of each term in this document was whether the term is already in fairly common, widespread use, not whether such use is desirable.

The descriptions of the terms were developed to conform to the broad, general, common-sense understanding of each term by the public, as well as by the technical community. Since many of the terms are also used in nonnuclear technologies, the descriptions were also developed to be consistent with reasonable usages in these other technologies. Another important criterion used in developing the definitions was clarity and ease of application.

Noteworthy Content

These terms addressed in this report have been widely used, often with respect to advanced reactors, and sometimes without adequate understanding of what they mean or what they may imply. The intent of the descriptive glossary in IAEA-TECDOC-626 is not to promote wider use of these terms, but rather to clarify their meaning. An important aspect of the report is an appendix on distinctions between active and passive functions, and that this is more a spectrum rather than a dichotomy.

3.7.2.3 NUREG/CR-1278, Handbook of Human Reliability Analysis

The primary purpose of the NRC Handbook of Human Reliability Analysis [3] is to present methods, models, and estimated human error probabilities (HEPs) to enable qualified analysts to make quantitative or qualitative assessments of occurrences of human errors in nuclear power plants that affect the availability or operational reliability of engineered safety features and components. A second purpose of the handbook is to enable the analyst to recognize error-likely equipment design, plant policies and practices, written procedures, and other human factors problems so that improvements can be considered. The handbook provides much of the modeling and information necessary for the performance of human reliability analysis as a part of PRA of nuclear power plants (NPPs).

Part I of the handbook consists of three chapters. Chapter 1 describes the purpose, scope, and organization of the handbook. Chapter 2 defines many of the relatively new terms useful for HRA and PRA (a glossary defines all of the technical terms). Chapter 3 presents a general model of human performance for HRA/PRA, which serves as the background for the more specific models elsewhere in the handbook. This chapter also discusses many of the factors that influence human performance in NPPs and similar complex man-machine systems.

Part II presents methods for analysis and quantification of human performance in six chapters. The topic of Chapter 4, Man-Machine Systems Analysis, is the basic approach used by human factors personnel to identify the potential for human errors in a system and to make some qualitative judgment as to the relative importance of each error in the system. Chapter 5 presents a HRA technique used in PRAs of nuclear power plant operations in the U.S. and in Europe. Chapter 6 describes the major problem for HRA, which is the relatively small amount of human error data that can be used to estimate HEPs for NPP tasks. Chapter 7 presents some interim methods for treatment of distributions and uncertainty bounds of HEPs until data-based models can be derived. Chapter 8 provides guidance in selecting the appropriate method for psychological scaling in using expert judgment for this purpose. Finally, Chapter 9 discusses the use of HEPs to estimate the probability of component unavailability resulting from human error and provides some examples of unavailability calculations.

Part III includes Chapters 10 through 19 which present human performance models and estimated HEPs with their estimates of uncertainty to be used in performing HRAs for input to PRAs. The goal in modeling human performance for PRA is to develop descriptive models to predict (within wide limits) how well people will perform what they are supposed to do in normal and abnormal situations in nuclear power plant operations.

Noteworthy Content

- This document conveys the importance of accounting for human factors in nuclear reactor PRA and to evaluate the impact of plant personnel on the risk for various plant operational states. Human factors are important because many studies have indicated that in complex man-machine systems, human error has often been the overriding contributor to actual or potential system failures.
- The concepts and approaches described in the handbook are as relevant today as when they were documented for the NRC.
- However, the handbook was written at a time (1983) when PRA was just beginning to be used for complex engineered systems such as nuclear reactors. As a consequence, it does have limitations that need to be considered when using it in to perform contemporary HRAs. Primary among the limitations is the small amount of human error data available at the time. An analysis of contemporary HRA guidance can be found in [4].

3.7.3 Summary Observations

The content presented at the IAEA conference (documented in [1]) almost exclusively focuses on DID as it relates to LWRs. Although the PHA-to-PRA process covered in this report is closely related to the subject of the first topical session at the conference (Implementation of DID in Siting, Design, and Construction), and the intention of DID is the same for non-LWRs, development is still ongoing regarding application of DID to advanced non-LWRs.

Based on experience, including lessons learned from the Fukushima Daiichi accident, in addition to refining processes such as DID, application of more comprehensive safety tools for the entire life cycle of a nuclear facility is advocated. NRC supports the use of preliminary hazard assessment tools in order to develop robust PRA analyses.

Documentation of detailed guidance exists for evaluating human behavior in nuclear power plants for use in PRA development as well as PRA development in general.

3.7.4 References

1. *International Conference on Topical Issues in Nuclear Installation Safety: Defense in Depth – Advances and Challenges for Nuclear Installation Safety*. IAEA-TECDOC-CD-1749. Vienna (Austria): International Atomic Energy Agency, 2013.
2. *Safety Related Terms for Advanced Nuclear Plants*. IAEA-TECDOC-626. Vienna (Austria): International Atomic Energy Agency, 1991.
3. U.S. Nuclear Regulatory Commission. *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*. NUREG/CR-1278. Washington, D.C., 1983.
4. U.S. Nuclear Regulatory Commission. *Evaluation of Human Reliability Analysis Methods Against Good Practices*. NUREG-1842. Washington, D.C., 2006.

4
PRELIMINARY PHA-TO-PRA METHODOLOGY

A PRA will ultimately be needed for any advanced nuclear reactor for two reasons. First, a PRA is a *de facto* component of a license to build a test, demonstration, or commercial reactor. Second, it provides focus and structure to the reactor development and design effort in terms of identifying failure mechanisms and necessary mitigating safety features. However, the input to a complete PRA requires the results of a relatively mature reactor development and design program. While having the results of a PRA at the outset of the process for developing and designing a new reactor concept would be ideal, the reality is that the detailed information (and likely the resources) necessary to perform a complete PRA are not available in the early development stages. The reactor design is often no more than a summary-level flowsheet with major components in the primary loop and postulated temperatures and pressures based on literature data. As reactor development and design proceed, the additional details necessary to inform a PRA gradually emerge culminating in a substantially complete PRA in the later development stages. Nevertheless, it is important that the fundamental elements of a PRA, such as the hazards presented by the reactor and plant/facility design and features that mitigate the hazards, be qualitatively identified at the earliest stages of design development.

The foregoing reality leads to the need to identify and use an approach to qualitatively evaluate hazards and mitigating features in any new reactor concept to provide focus for early design development efforts and to inform maturing design and alternative assessment studies. Such an approach should also produce information that is directly useful in developing increasingly detailed and quantitative PRAs for the reactor concept. The purpose of this section is to identify a methodology for a qualitative evaluation process to identify hazards and mitigating features in new reactor concepts and to demonstrate how the resulting information flows into an evolving PRA.[12] The methodology is described below in two parts. First, a qualitative evaluation process to determine the hazards and mitigating features of early-stage designs is selected from available approaches based on factors such as the amount and quality of information available and the timing of the hazards assessment in the design process. Then, the results of the qualitative evaluation approach are described in terms of how they relate to the inputs required to perform a PRA. Finally, an approach to demonstrating the methodology is presented.

4.1 Approach to Qualitatively Assess Hazards and Mitigating Features

In general, approaches to qualitatively evaluate hazards and mitigating features are collectively referred to as process hazards analysis or PHA. In the chemical industry, a PHA or hazard evaluation is defined as “an organized effort to identify and analyze the significance of hazardous situations associated with a process or activity. PHA studies have been used to

[12] Because PRA was developed and applied retroactively to LWRs after the first units began operating and a large commercial fleet had been established, detailed design and operational information was readily available. Therefore, formalized methods to develop and feed information into the PRA was not needed.

pinpoint weaknesses in the design and operations of facilities that could lead to accidental chemical releases, fires, or explosions" [1]. In NUREG-1513, the NRC describes an approach known as an Integrated Safety Analysis (ISA) and describes how PHA techniques should be applied to nuclear fuel cycle facilities (uranium conversion, uranium enrichment, fuel fabrication) in order to address the special hazards present at such facilities, such as their potential for criticality incidents, radiological releases, and certain chemical releases [2]. The NRC has recognized that ISAs, which are dependent upon PHAs, have been successful in identifying potential accident sequences, designating design features and system responses to mitigate them, and describing management measures to be applied to assure reliability and availability of these systems [3]. As previously mentioned, PHAs have also been identified as a suitable method to meet these objectives for advanced nuclear reactor designs [4, 5].

The NRC recognizes the AIChE *Guidelines for Hazard Evaluation Procedures* [1] as an authoritative and comprehensive source of information on common PHA methods and as a resource for practitioners of hazard analysis [2]. The AIChE guidelines describe twelve (12) different PHA methods that provide a spectrum of processes available to perform industry-standard PHA efforts. Choosing among these options is based on the nature of the system being analyzed, the amount and detail of design information available for the evaluation, and the intended use of the results. Three methods are recommended for systems in which the risk of potential accident sequences is believed to be high [1]:

- What-If/Checklist,
- Hazards and Operability (HAZOP), and
- Failure Modes and Effects Analysis (FMEA).

In a previous hazard analysis of an advanced reactor design [6], the What If approach was chosen by EPRI due to the relative immaturity of the reactor design being analyzed at the time of the study, along with the limited time and funding available for the study.

However, both the HAZOP and FMEA methods are more systematic than the What-If analysis approach [7] and provide more comprehensive information to support development and implementation of PRA. Accordingly, case studies employing either the HAZOP or FMEA method will be used in this report to illustrate the proposed PHA-to-PRA methodology.

With respect to major differences between HAZOP and FMEA, the HAZOP method is better suited to comprehensively identify hazards and is capable of analyzing combinations of failures in the context of both safety and operations [8, 9]. Meanwhile, FMEA is better suited for producing safety-related insights with a higher level of detail than those of a HAZOP study.

The references cited in this section provide extensive guidance on performing HAZOP and FMEA evaluations, and commercial software that facilitates implementation is widely available. This information will not be repeated here.

4.2 Application of PHA Results to Meet PRA Input Needs

This section explains how the products of PHA performance can be shaped to support the input needed for the development of the PRA model. The relationship of the PHA results to the generic information needs for a PRA are shown in Figure 4-1 and elaborated in Table 4-1. The

figure and table are followed by discussions of how the PHA results characterize the systems being analyzed and the manner in which they are used in PRA model development.

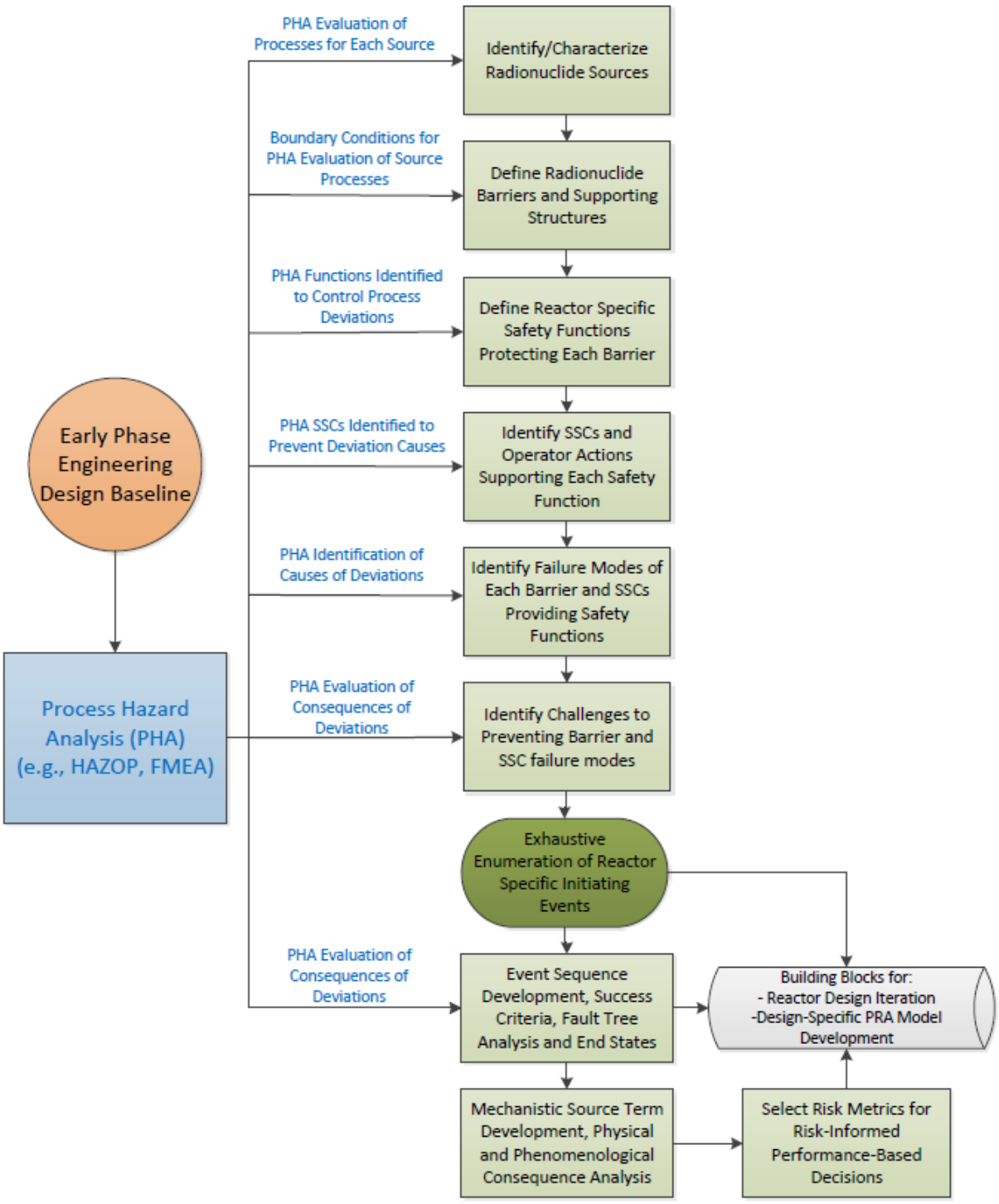


Figure 4-1
Integration of safety-in-design: Sample iteration of PHA-to-PRA inputs

Table 4-1
Relationship of PHA outputs to PRA inputs

PRA Step	Needed PRA Input	PHA Output Meeting PRA Input Need	Comments
1	Identification and characterization of hazardous material that could be released	PHA characterization of process flowsheet for analysis Identification of system hazards (e.g., list of HAZOP parameters to be used for analysis)	Level of detail consistent with current design maturity Qualitative identification (or quantitative characterization at later stages of design) of materials that could be released, as well as other system hazards Example parameters and consequences of interest: temperature, pressure, flow, radioactivity, nuclear reactivity
2	Barriers to hazardous material release	Identification of barriers to the release of hazardous material Taken from PHA characterization of flowsheets for systems/processes that contain hazardous materials	Barriers can include pipes, vessels, containment, filters, etc. The number of barriers that can be identified for each inventory of hazardous material will likely depend on design maturity
3	Reactor-specific safety functions protecting each barrier	List of functions that control process deviations for each subsystem or process analyzed (taken from PHA flowsheet characterization) List of safety functions identified during PHA study to prevent hazardous material release	A “deviation” is an undesirable off-normal condition such as “high pressure”, “increased nuclear reactivity”, etc. List contains functions (e.g., remove decay heat) rather than subsystems/components (e.g., Residual Heat Removal system)
4	Structures, systems, and components (SSCs) and operator actions supporting each safety function	Components performing each function can be identified using design information that includes specific SSCs and/or actions The “Safety Systems” output of a PHA study identifies SSCs and/or actions that prevent causes or mitigate consequences of deviations identified in the study	Features are characterized with respect to the degree of automation PHA “Action Item” outputs may identify additional needs to develop, improve, or understand SSCs and/or operator actions

Table 4-1 (continued)
Relationship of PHA outputs to PRA inputs

PRA Step	Needed PRA Input	PHA Output Meeting PRA Input Need	Comments
5	Failure modes for each SSC and operator action supporting a safety function	List of failure modes taken from PHA "Causes" that have been identified to have deviations that result in failures of specific SSCs and/or actions The PHA "Consequences" output will identify SSC and operator failures leading to barrier failure and potential for hazardous material release	At early stages of design, the list of failure modes may be more functional in nature As more detailed design information is available, a more detailed list of failure modes can be developed using a highly detailed PHA technique (e.g., FMEA)
6	Challenges in preventing SSC and operator failures	Identification (during analysis) of weaknesses in SSCs and operator interventions designed to prevent barrier failure Inadequate mitigation features evident (qualitatively) by comparison of "Consequences" and "Safety Systems" identified for a given failure/deviation	PHA "Action Item" outputs may help identify how to enhance mitigation features
7	Exhaustive enumeration of reactor-specific initiating events	Structured identification of deviation "Causes" Taken from structured and comprehensive PHA evaluation of deviations	Includes generic (pressure, temperature) and concept-specific (radioactivity, nuclear reactivity) deviations A more structured PHA technique (e.g., HAZOP) forces a more exhaustive consideration of deviations
8	Event sequence development including end states and success criteria	Structured identification of deviation "Causes" and "Consequences" Individual sequences can be developed based on the success/failure of "Safety Systems" identified Taken from structured and comprehensive PHA evaluation of deviations	Determination of end states and success criteria may require consequence analysis (see PRA Step 10) Master Logic Diagrams provide a useful way to organize the list of initiating events for event sequence model development

Table 4-1 (continued)
Relationship of PHA outputs to PRA inputs

PRA Step	Needed PRA Input	PHA Output Meeting PRA Input Need	Comments
9	Fault tree development	Structured identification of "Safety Systems" mitigating specific "Consequences" Taken from structured and comprehensive PHA evaluation of deviations	As more detailed design information is available, a more detailed fault tree model can be developed using a highly detailed PHA technique (e.g., FMEA)
10	Mechanistic hazardous material source term development and physical and phenomenological consequence analysis	Structured identification of deviation "Consequences" can prioritize specific scenarios to be analyzed PHA "Action Items" output may identify scenarios that must be analyzed before the "Consequences" can be fully determined	The results of these analyses may inform the next iteration of PHA and provide inputs to the maturing design

4.2.1 System Characterization

Identification of Material at Risk. Important factors to consider when identifying sources of radionuclide and hazardous chemical material at risk include the physical form of the hazardous material, locations of the material, and barriers to the release of the material. The form (e.g., physical state or chemical composition) and amount of hazardous material will affect the severity of the consequences associated with the release of a given inventory of hazardous material, and sources with different forms can require different approaches to model the behavior of the material. Similarly, the location of the material (in relation to the entire system and/or the public) can determine what barriers or functions are used to prevent a release of the material, and event sequences that involve the failure or success of the same barriers or functions can often be grouped together in an initial PRA model [4]. The amount of material present at each location is usually not known for new advanced reactor concepts in the early stages of development but increasingly accurate inventory estimates should become available as the design matures, and such information is a necessary input to mechanistic modeling of hazardous material source terms and event consequences.

Sectioning the System. In order to conduct a PHA, it will be necessary to subdivide the advanced reactor design into analyzable sections or "nodes". The proper definition of these sections contributes to effective analysis, as there are problems associated with choosing either too small or too large a section [10]. If the section being analyzed is too small, there is the possibility of initiating events and/or effects being overlooked because they occur outside of the section boundary. If a section is too large, the function of the design intention can become imprecise or very complicated making it difficult to determine all significant effects that occur due to a failure or deviation from normal operation. Although there is no universal method recommended to divide the design into sections, there are some important concepts from systems engineering that will be utilized to ensure the results of the PHA study readily facilitate the development of a PRA model.

The first concept that will be applied while dividing the reactor design into sections is to ensure that each section has one major function, and that multiple sections do not perform the same function (with the exception of designed-in redundancy). This concept is consistent with the functional decomposition concept that is central to sound systems engineering practices [11, 12]. Furthermore, because the failure to perform a given function is a pivotal event on an event tree, it is desirable to be able to analyze the causes and effects of each failed function within the study of a single section. Since the results of the PHA are intended to inform quantitative risk assessment, it will also be beneficial to structure the section boundaries such that similar operating conditions such as working fluid or pressure exist within each section. Such an approach facilitates the use of component reliability data because failure rate information is often grouped using such attributes (for example, see [13-16]). Finally, when defining the sections, it is valuable to completely document all interfaces between sections because these interfaces are potential routes for propagating a deviation or event sequence from one section to another. Managing and analyzing interfaces can often help highlight important underlying issues much earlier than would otherwise be revealed [15].

Parameter Identification. One final required task that will be performed during system characterization for a PHA study is listing the system parameters that will be considered during the analysis. This list of parameters should represent those indicators and phenomena, necessary to maintain normal operations and to identify the onset of operational abnormalities. Generic parameter lists (e.g., temperature, flow, pressure) are available [10]. In the case of new advanced reactor concepts, these lists will need to be supplemented with parameters unique to nuclear systems such as radioactivity and nuclear reactivity.

In a HAZOP study, these parameters are combined with guidewords to generate the deviations used to analyze the system [1, 10]. In an FMEA, although the parameters are not used explicitly, consideration of the list of important parameters during the study can help ensure a more complete identification of all hazardous scenarios causing or resulting from a failure [17]. Because the relevant parameters that could indicate or cause hazardous scenarios may vary from section to section, care is required to ensure that the design intention of each section and the overall system is carefully considered. It is possible that some parameters that apply to one section may not apply to every section, and new parameters of interest may be identified during the PHA study [11]. The preferred procedure is to establish an inclusive list of parameters for the system and then label irrelevant parameters in a particular section as being "not applicable" to ensure that deviations have been comprehensively considered.

4.2.2 Considerations for Using PHA Results

As discussed, HAZOP studies and FMEAs are recognized as the most systematic PHA methods. Therefore, this discussion will focus on using the results of these PHA methods in a PRA.

Ensuring Comprehensiveness. During recent PHA studies of MSR systems [18, 19], it was found that comprehensively documenting the unmitigated effects of a deviation (for instance, the coupling of a system parameter such as pressure and an upset condition such as "too high") within a section was beneficial to the process of translating HAZOP results to the construction of event trees. Thus, time spent exhaustively brainstorming causes and effects of deviations during a HAZOP study helps to ensure comprehensiveness in hazard identification and evaluation. Similarly, systematically assessing the consequences of the deviation/cause combination at each section interface ensured that the event sequence could be fully analyzed using HAZOP results from multiple sections. Because the goal is to eventually construct quantitative fault trees to estimate the probability of event tree pivotal events and event sequences, it is also helpful to differentiate between automatic system responses and anticipated operator actions in response to system indications. This differentiation will aid in the incorporation of estimates of human error within a PRA model. Finally, a key to performing a consistent PHA is ensuring that the effects of all deviations or equipment failures are analyzed using consistent assumptions and that these assumptions are documented during the evaluation [1].

Event Trees and PHA. Event trees model potential event sequences that occur after an initiating event. Event Tree Analysis assumes that the initiating event occurs and then represents each success or failure to respond to the initiating event as a pivotal event. Each event sequence is a path through pivotal events with an associated end state. When the event tree is quantified using the results from fault tree analysis (see below), it provides probability of occurrence. Master Logic Diagrams provide a useful way to organize the list of initiating events for event sequence model development. The deviations evaluated during the HAZOP study provide inputs to the

identification of initiating events. The comprehensive identification of causes and consequences for initiating events assists in laying out the branches of the event tree; information from several sections/systems may be combined to fully structure the event tree. The modeling of the responses of safety systems, identified during the HAZOP, will assist in distinguishing end states.

The results of the HAZOP studies and FMEAs on an advanced reactor design are qualitative; however, these PHA results will next be used to create models that can then be quantified to estimate the failure probability or frequency associated with a reactor design. It is standard practice to model the progression of nuclear reactor accidents and the end state resulting from event sequences using event trees. Some of the causes of deviations identified during the HAZOP study will represent initiating events in the event trees. Additionally, the pivotal events that determine the different event sequences in event tree analysis will be captured as safety systems mitigating the deviation in the HAZOP results. Finally, the end state of the event sequence will be related to the consequences determined for relevant deviations during the PHA.

In order to maximize the efficiency and effectiveness of using PHA results in quantitative risk analysis, it will be necessary for the event tree models to be built using a consistent set of end states. If the end states are appropriately selected, the sum of frequencies of relevant event sequences that produce a similar, undesired consequence will be a meaningful result. Although the non-LWR PRA approach suggested by the LMP [20] utilizes radiological dose at the site boundary as the risk surrogate or "risk metric" of choice, calculations to estimate these doses can be complicated and have a high degree of uncertainty due to complexities and variability involved in transport of the hazardous material from the source to the receptor. This issue is often addressed by using a surrogate end state such as the amount of hazardous material released from failed barriers. This approach is consistent with the approach advocated in the ASME/ANS non-LWR PRA standard [4] and the US DOE PRA standard [21].

Fault Trees and PHA. The frequency of each pivotal event in an event tree can be evaluated using fault tree analysis, if this information is not readily available from standard references (e.g., references [13], [15]). Fault tree analysis is a deductive approach that starts with the top-level event of concern and decomposes that event into sequences that contribute to its occurrence until the fundamental fault causes (known as "basic events") are identified. These basic events include equipment failures, human response errors, etc. Fault trees are quantified using component reliability data and the frequency of the basic events to estimate the probability of the top-level event. Fault trees model plant systems in detail, informing the PRA modeler of combinations of component failures that prevent the desired response to the initiating event. PRA modeling uses fault trees to represent the combination of individual component failures that will result in each pivotal event in an event tree.

For the case study to be performed on the Molten Salt Reactor Experiment (MSRE), fault trees will be built using the results of HAZOP studies. These fault trees will be developed by looking at the relationship between different causes that have consequences producing the failure of the same component, subsystem, or function. For complex subsystems, a HAZOP study may not produce results that are detailed enough to structure the fault tree on an individual component

basis. In these cases, an FMEA is particularly useful, since the results of an FMEA are organized at the component level. These failures will then represent basic events in the fault trees. The PHA method (or methods) to be used on the pilot study will be tailored to the status of design and safety analysis information available for the advanced reactor design selected.

4.2.3 Design Insights from PHA-to-PRA

Safety systems are those systems which the design depends on to monitor important parameters and provide alarms or protective actions. The identification of safety systems is a fundamental feature of HAZOP studies and FMEAs. This feature allows for the qualitative assessment of which systems are identified most frequently or are associated with mitigating more severe consequences. This in turn provides an initial indication of systems that are important for safe and reliable operation of a system and the overall design. The consequences themselves are a primary output of the PHA, as they will assist in identifying and characterizing hazards. Also, as deviations and failure modes are being evaluated, the PHA team is required to document outstanding technical questions or analyses that are suggested by their assessments. These are generically referred to as "actions." One of the concluding steps of the HAZOP study or the FMEA is to ensure that these actions are assigned to lead individuals on the project team for resolution.

As PHA results are used to develop event and fault tree models, the analyst gains an understanding of how the performance of each subsystem or component contributes to the progression of the event sequences from event trees. A deeper appreciation is developed of the interaction between subsystems and components in accomplishing the anticipated system function. Further, the combination of responses that leads to varying levels of system failure can be obtained by developing the fault tree logic.

The insights obtained from the PHA and the subsequent event and fault tree models are also used to identify the needed safety systems and their functional design criteria for the reactor concept under development.

4.3 Demonstrating the Methodology

4.3.1 Case Study on the MSRE

To provide an initial demonstration of the draft methodology for transitioning from PHA to PRA, an initial case study will be performed. To select an advanced non-LWR design to evaluate, the team took into consideration the fact that PRAs have been performed in the past on liquid-metal fast reactors and high-temperature gas reactors. Therefore, it was decided that it would be most beneficial to perform the case study evaluation on a different advanced reactor concept, a molten salt reactor (MSR). Many current MSR designs have published high-level descriptions of their designs, but detailed design information is either proprietary or not yet developed. This led the team to assess the potential use of the Molten Salt Reactor Experiment (MSRE), operated by the Oak Ridge National Laboratory from 1965-1969. The MSRE does not have a PRA or safety analysis done consistent with current standards. However, during a joint ORNL-Vanderbilt University project in 2017 [22], it was determined that there was sufficient design information available to support a PHA and subsequent event and fault tree analyses that

constitute the core of a PRA. Preliminary HAZOP analyses of selected MSRE subsystems has been completed, including initial development of an MSR-specific component reliability database to support quantitative risk assessment [23]. Scope for the complete MSRE case study activities includes:

- **Pre- HAZOP Work/System Characterization**
  - Decomposition of the MSRE into sections for the HAZOP work.
  - Identification of MSRE-relevant phenomena (system parameters) to consider during hazard assessment, along with the rationale for their selection.
  - Development of a preliminary risk metric (i.e. the conceptual equivalent of "core damage frequency" in a LWR system) that could be applied for the MSRE risk assessment.
- **MSRE HAZOP Study**
  - Use of the HAZOP process to systematically evaluate the MSRE system sections, developed above. At least three separate sections will be studied, including one subsystem pertaining to the main sources of radioactive inventory in the MSRE, the fuel salt loop.
  - Identification and documentation of significant system deviations (*e.g.*, Anticipated Operational Occurrences), consequences, safety systems, and actions.
- **Quantitative Risk Assessment of Selected Initiating Events**
  - Development of fault and event tree analysis specific to MSRE to allow comparison of the frequency and consequence of event sequences.
  - Identification and documentation of the most important significant system deviations.

4.3.2 Pilot Application on an Advanced Reactor Design

This third phase of the project will use the methodology and information from the case study as the basis for a pilot PHA-to-PRA study for a yet-to-be-determined system important to an advanced reactor design team (and ideally of importance to the class of reactors which the particular design represents). This pilot study is intended to be aligned with the resources, needs, and priorities of the reactor design team. Because specific design information will be involved in this phase of the project, proper information control, export control, and safeguard and security practices will be required.

4.4 Summary

In this section, a draft methodology has been proposed for transitioning the early stage safety analyses of advanced reactor designs to the quantitative analysis and ultimately PRA. This has been done by initially presenting a simplified, three-step description of the methodology: (1) preparing for the PHA, which involves selecting a PHA methodology appropriate for the present stage of the design and goals of the evaluation; (2) conducting the PHA in accordance with available industry-standard guidelines and "keeping the end in mind" as the analysis unfolds; and (3) using tools such as event tree analysis and fault tree analysis to build the models of the

system that are at the core of a PRA. The methodology will be further developed during the case study and pilot study phases of this project. In particular, the case and pilot studies will include an effort to document the details of the PHA-to-PRA process to provide insights for subsequent application and advancement of the methodology for use in new advanced reactor design.

4.5 References

1. American Institute of Chemical Engineers, Center for Chemical Processing Safety. *Guidelines for Hazard Evaluation Procedures, Third Edition.* Hoboken, NJ: John Wiley & Sons, 2008.
2. U.S Nuclear Regulatory Commission. *Integrated Safety Analysis Guidance.* NUREG-1513. Washington, DC: Office of Nuclear Materials Safety and Safeguards, 2001.
3. U.S Nuclear Regulatory Commission. *A Comparison of Integrated Safety Analysis and Probabilistic Risk Assessment*. Staff Report. Washington, D.C.: Office of Nuclear Materials Safety and Safeguards, 2011.
4. *Probabilistic Risk Assessment Standard for Advanced Non-LWR Nuclear Power Plants* (Trial Use Draft Standard). ASME/ANS RA-S-1.4-2013. American Society of Mechanical Engineers/American Nuclear Society, 2013.
5. *An Integrated Safety Assessment Methodology (ISAM) for Generation IV Nuclear Systems*. *Version 1.1*. Generation IV International Forum, Risk and Safety Working Group, June 2011.
6. *Technology Assessment of a Molten Salt Reactor Design: The Liquid-Fluoride Thorium Reactor (LFTR).* EPRI, Palo Alto, CA: October, 2015. Report 3002005460.
7. Khan, F. and S. Abbasi. "Techniques and Methodologies for Risk Analysis in Chemical Process Industries," *Journal of Loss Prevention in the Process Industries*. Vol. 11, No. 4: pp. 261-277 (1998).
8. Popović, V. and B. Vasić. "Review of Hazard Analysis Methods and Their Basic Characteristics," *FME Transactions*. Vol. 36, No. 4: pp. 181-187 (2008).
9. Nolan, D.P. "Objective and Description of PHA, What-If, and HAZOP Reviews," In *Safety and Security Review for the Process Industries. Fourth Edition,* Gulf Publishing Company. Chapter 3: pp. 8-13 (2015).
10. Crawley, F. and B. Tyler. *HAZOP: Guide to Best Practice, Guidelines to Best Practices for the Process and Chemical Industries*. *Third Edition*. Elsevier, 2015.
11. Hirshorn, S., L. Voss, and L. Bromley. *NASA Systems Engineering Handbook. Revision 2.* NASA SP-2016-6105, Washington, D.C.: National Aeronautical and Space Administration, 2017.
12. International Council on Systems Engineering. *Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*. *Fourth Edition.* INCOSE-TP-2003-002-04. Hoboken, NJ: John Wiley & Sons, 2015.
13. American Institute of Chemical Engineers, Center for Chemical Processing Safety. *Guidelines for Process Equipment Reliability Data, with Data Tables,* Hoboken, NJ: John Wiley & Sons, 1989.

14. Blanchard, A. and B.N. Roy. *Savannah River Site Generic Data Base Development. Revision 1.* Aiken, SC: Westinghouse Savannah River Company, Aiken, SC: 1998. Report WSRC-TR-93-262.

15. *Component Reliability Data for Use in Probabilistic Safety Assessment.* IAEA-TECDOC-478. Vienna (Austria): International Atomic Energy Agency, 1988.

16. Eide, S., S. Chmielewski, and T. Swantz. *Generic Component Failure Data Base for Light Water and Liquid Sodium Reactor PRAs*. Idaho National Laboratory, Idaho Falls, ID: 1990. Report EGG-SSRE-8875.

17. Stamatis, D. *Failure Mode and Effect Analysis: FMEA from Theory to Execution. Second Edition.* Milwaukee, WI: American Society for Quality – Quality Press, 2003.

18. Chisholm, B., S. Krahn, P. Marotta, A. Croff. "Preliminary Risk Assessment of a Generalized Molten Salt Reactor Off-Gas System," *Transactions of the American Nuclear Society*. Vol. 117. pp. 221-224 (2017).

19. Chisholm, B., S. Krahn, A. Afzali, and E. Harvey. "Application of a Method to Estimate Risk in Advanced Nuclear Reactors: A Case Study on the Molten Salt Reactor Experiment," 14th International Conference on Probabilistic Safety Assessment and Management Conference (PSAM 14), Los Angeles, CA, September 16-21, 2018.

20. Southern Company Services. *Modernization of Technical Requirements for Licensing of Advanced Non-Light Water Reactors: Risk-Informed Performance-Based Guidance for Non-Light Water Reactor Licensing Basis Development.* SC-29980-xx. (Working Draft Report, Revision N) 2018.

21. US DOE. *DOE Standard on Development of Probabilistic Risk Assessments for Nuclear Safety Applications.* DOE-STD-1628-2013. Washington, D.C., 2013.

22. Chisholm, B., G. Flanagan, S. Krahn, G. Mays. "Licensing Basis Event Selection Case Study: The Molten Salt Reactor Experiment." Paper presented at the ORNL Molten Salt Reactor Workshop 2017, Oak Ridge, TN, October 3 - 4, 2017.

23. Chisholm, B., S. Krahn, A. Croff, P. Marotta, A. Sowder, N. Smith. "Preliminary Hazard Assessment and Component Reliability Database for the Molten Salt Reactor Experiment," 2018 International Congress on Advances in Nuclear Power Plants (ICAPP 18), Charlotte, NC, April 8 – 11, 2018.

5
MOVING FROM EARLY SAFETY ANALYSIS TO PRA

The methodology outlined in Section 4 for integration of safety analysis early in advanced reactor design draws on and builds upon a collection of established methods and practices for the safety analysis of industrial processes and facilities worldwide. With respect to application in the nuclear domain, the proposed PHA-to-PRA methodology complements and is consistent with many existing elements of safety analysis that have been exercised and endorsed by the NRC [1, 2] and the DOE [3, 4] for reactor and other nuclear facilities.

The result is a flexible, progressive, iterative and structured approach for the application of qualitative and semi-quantitative process hazard analysis tools and methods that should provide a seamless front-end for more quantitative risk assessment methods. Figure 5-1 illustrates the relationship among various representative methods and supporting elements (shown in blue) and the notional progression from more qualitative methods on left, i.e., PHA, to more quantitative evaluations, e.g., PRA on right (shown in purple).

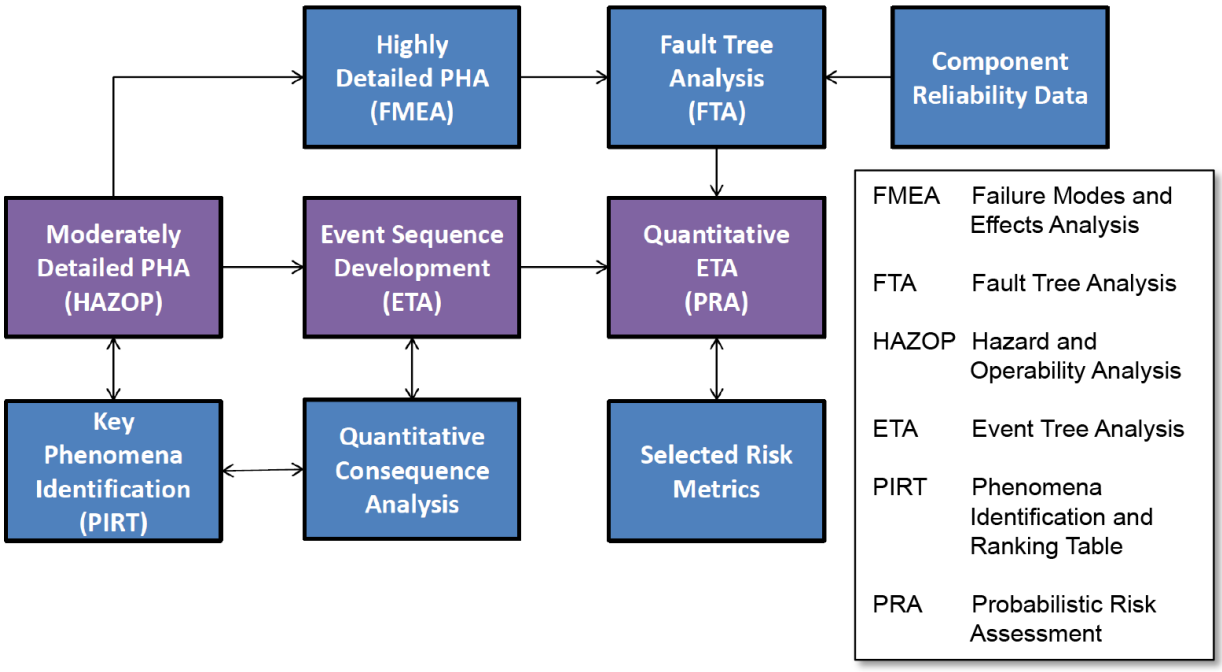


Figure 5-1
Visualized scheme for progression from early safety analysis to PRA

- The methodology commences at the earliest practical point in design when subject matter experts determine that the level of documentation of design information can be analyzed using an established PHA method. This step encourages early development of a relationship between the engineering and design technologists and safety analysts. It can also help enhance early discipline in engineering baseline documentation [5], setting and exercising project systems, and standards for documentation configuration management [6].
- In the PHA-to-PRA process, the HAZOP technique has been chosen as the representative early design safety analysis method. This analysis method is depicted in Figure 5-1 as the starting step and is characterized as a "moderately detailed PHA." The information and documentation required to perform a HAZOP study (or other suitably selected PHA method, see [7]) provides structure that supports multiple philosophies of good design practice endorsed by industry, including systems engineering, configuration management, and safety-in-design. The structures of the various PHA techniques are particularly suited to the analysis of systems while assigning proper priority towards consideration of the interfaces between systems. In addition, proper execution of PHA methods requires rigorous tracking and accounting of assumptions, consistent with good configuration management practices [6]. Further, the conduct of PHA methods involves participation and interaction of both safety and design technologists, helping to establish design and safety interfaces early in the design project life [8]. In this way, the PHA-to-PRA method lays a practical working foundation for safety-in-design.
- The PHA-to-PRA process is likely to begin by focusing on subsets of systems (or subsystems) that have been selected on the bases of available information and projected relative importance to safety risk, performance risk, cost and schedule to develop, and cost to change.
- The PHA-to-PRA process utilizes all relevant information that is developed in the design and safety analysis process when it becomes available. The use of other powerful tools in the suite of safety analysis techniques is encouraged and may be necessary at times. As shown in Figure 5-1, a HAZOP study is capable of producing insights and lines of inquiry necessary for supporting development and execution of a Phenomena Identification and Ranking Table (PIRT) analysis. These lines of inquiry would likely be captured as "Action Items" identified during the study, and could include scenarios that must be further demonstrated to fully understand the consequences of a specific deviation. Furthermore, a PIRT analysis could inform a HAZOP on the nature of hazards to be considered and the relative magnitude of deviations involving different physical phenomena. Although not depicted explicitly in Figure 5-1, the PIRT and the HAZOP can also inform the safety and design technologists of the need for particular areas for technology development, bench-top testing, or scale testing regarding physical and phenomenological behavior that cannot be predicted solely through existing models.
- The deviations identified in early iterations of PHA can be used to qualitatively develop initial event tree models. By developing a set of specific event sequences for which an end state must be known, these initial models would inform the performance of quantitative consequence analysis of accident sequences. The relationship between ETA and consequence analysis is two-way in nature, since the results of the consequence analysis are captured in

the event tree models. In addition to design information, results of analyses would be used in iterations of PIRT and PHA to fine tune results. Finally, results of physical tests and experiments would be used to provide the rationale for modeling assumptions in calculations for the quantification of accident progression and consequence.

- As the design of the system being analyzed and the understanding of accident phenomena in the system mature, more detailed PHA methods (such as FMEA) are enabled. FMEA exercised early enough in design can be used to set design targets for the performance of new sub-systems [9]. The output of an FMEA is structured and comprehensive enough to be used for constructing qualitative fault trees. These fault trees can then be quantified with component reliability data to be used to estimate the failure frequency of sub-systems and design-specific safety functions. Depending on the complexity of design and the nature of available design information, this quantitative FTA, combined with the initial ETA, may enable the beginning of limited quantitative ETA.
- In multiple places along this iterative and evolving design process, the early implementation of safety-in-design will allow the safety and design technologists to identify when and where studies for design alternatives should be considered in order to avoid design complexity or high levels of technical uncertainty, for example. Further, quantitative ETA models can give rise to early insights into comparative risk. These insights regarding relative likelihood and severity of event sequences could then be used to adjust design schedule priorities or to consider design alternatives.
- The PHA-to-PRA methodology continues to be exercised as more information regarding system and sub-system design becomes available. It is imperative to give appropriate attention to the interfaces between subsystems to ensure that consequences are not overlooked if they occur in a different subsystem than the cause of the deviation. Critical to the success of such an iterative process is the foundation established in the first iteration for rigorous configuration management of engineering and safety documentation and comprehensive tracking of design assumptions in safety analyses [6]. As design detail increases and changes, a system needs to be in place to re-evaluate prior safety inputs to a system design, particularly those that could be impacted by changes to interfacing systems.
- As accident sequence and progression are better understood, consideration of risk surrogates or figures of merit for safety analysis may be developed to facilitate analysis and to identify the systems that are most important to safety design. Use of these values can then be defended and incorporated into consequence analysis and quantitative ETA. It is possible that these risk metrics could serve a role in the reactor licensing basis as the safety case for the design continues to develop [10]. As designs begin to solidify, these units of quantitative ETA can be viewed more clearly as specific building blocks of the formal reactor PRA model.
- At later stages of design, when systems and sub-systems have been individually analyzed and system interfaces have been evaluated, the design project can begin to integrate the building blocks of the PRA into the detailed tool that is used to quantify overall facility integrated risk.

In summary, the full suite of the safety analysis process organized around the PHA-to-PRA methodology would include the following:

- Comprehensive identification of physical and chemical phenomena important to safety, including efficient and timely identification of the need for test and experiments.
- Early and iterative utilization of PHA (e.g., HAZOP and/or FMEA) and quantitative consequence analysis to identify risk-informed design strategies including safety system functional requirements, design alternatives, and needs for technical development.
- An incremental development of PRA building blocks with documented ties to component reliability data, safety analysis data, and the engineering baseline to facilitate required PRA integrated risk estimations.
- Identification of technology-relevant risk metrics to facilitate safety analysis, risk analysis, licensing approval, and maintenance of the licensing basis during operations.
- Early establishment of a working interface between safety and engineering technologists.
- Early institution of systems engineering in order to perform hazards analysis of systems, sub-systems, and their interfaces using industry-standard PHA methods.
- Early establishment of engineering and safety documentation interfaces and configuration management.

5.1 References

1. U.S. Nuclear Regulatory Commission. *Integrated Safety Analysis Guidance*. NUREG-1513. Washington, D.C.: Office of Nuclear Materials Safety and Safeguards, 2001.
2. U.S. Nuclear Regulatory Commission. *PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants*. NUREG/CR-2300. Washington, DC: Office of Nuclear Regulatory Research, 1983.
3. U.S. Department of Energy. *DOE Handbook on Chemical Process Hazards Analysis*. DOE-HDBK-1100-2004. Washington, D.C., 2004.
4. U.S. Department of Energy. *DOE Standard on Development of Probabilistic Risk Assessments for Nuclear Safety Applications*. DOE-STD-1628-2013. Washington, D.C., 2013.
5. U.S. Department of Energy. *DOE Standard on Content of System Design Descriptions*. DOE-STD-3024-2011. Washington, D.C., 2011.
6. U.S. Department of Energy. *DOE Standard on Configuration Management*. DOE-STD-1073-2016. Washington, D.C., 2016.
7. American Institute of Chemical Engineers, Center for Chemical Processing Safety. *Guidelines for Hazard Evaluation Procedures, Third Edition.* Hoboken, NJ: John Wiley & Sons, 2008.
8. U.S. Department of Energy. *DOE Standard on Integration of Safety into the Design Process*. DOE-STD-1189-2016. Washington, D.C., 2016.

9. Stamatis, D. *Failure Mode and Effect Analysis: FMEA from Theory to Execution, Second Edition*. Milwaukee, WI: American Society for Quality – Quality Press, 2003.
10. Southern Company Services. *Modernization of Technical Requirements for Licensing of Advanced Non-Light Water Reactors: Risk-Informed Performance-Based Guidance for Non-Light Water Reactor Licensing Basis Development.* SC-29980-xx. (Working Draft Report, Revision N) 2018.

A
RESUMES OF PROJECT TEAM MEMBERS

Resumes for key project team members are provided on the following pages.

Andrew G. Sowder, Ph.D., CHP

Professional Experience

Electric Power Research Institute (EPRI), Technical Executive, Nuclear Sector, Advanced Nuclear Technology Program (2007 – Present) - leads new EPRI strategic focus area on advanced nuclear energy systems to support technology assessment, development of owner/operator requirements, and RD&D prioritization. Dr. Sowder also serves as the EPRI Innovation Scout for advanced nuclear energy systems. His previous responsibilities at EPRI included:

- Leading international engagement on accident tolerant fuel RD&D (2012 – 2015);
- Leading U.S industry technical support (via EPRI – NEI – INPO action plan) for early event analyses of spent fuel pool issues at Fukushima Daiichi (2011-2012);
- Leading for advanced nuclear fuel cycle assessment program for development of in-house expertise and assessment tools (2011-2015);
- Establishing and expanding EPRI-led Extended Storage Collaboration Program (ESCP) to coordinate global RD&D activities and technical engagement for used fuel management (2009-2011); and
- Leading EPRI's independent performance assessment program on Yucca Mountain for the permanent disposal of commercial used fuel in the United States (2007-2009).

U.S. Department of State, Bureau of International Security and Nonproliferation, Office of Nuclear Energy, Safety and Security, Physical Scientist and Foreign Affairs Officer (2003 – 2007) - coordinated U.S. policy for implementation of international radiological security and physical protection of nuclear material among DOE, NRC, DHS, and other U.S. agencies; developed and executed successful strategies for advancing U.S. nuclear safety and radiological security agenda abroad within the G-8, IAEA, and other bilateral and multilateral contexts; and provided technical policy oversight of U.S. assistance for the Chernobyl Shelter and other international nuclear safety programs.

The University of Georgia, Savannah River Ecology Laboratory and Medical University of South Carolina, Marine Biomedicine and Environmental Sciences Program Assistant research scientist/postdoctoral researcher and visiting scientist (2001-2003 & 1998-2000) - coordinated and conducted interdisciplinary research on microbial toxicity and uranium/heavy metal biogeochemistry in riparian and wetland ecosystems on U.S. DOE Savannah River Site. Responsibilities also included supervision of laboratory staff, planning and execution of sediments sampling within radiologically controlled areas, and the procurement, installation, operation, and repair of analytical instruments.

U.S. Environmental Protection Agency, Office of Radiation and Indoor Air, American Association for the Advancement of Science (AAAS) Science & Technology Policy Fellow (2000 – 2001) - coordinated intra- and inter-agency (EPA, DOE, NRC) environmental modeling initiatives; provided independent technical review of EPA documents and publications; conducted independent radiological survey of uranium-contaminated homes and lands on the Navajo Nation in conjunction with U.S. EPA Region IX Superfund removal action; and participated in radiation risk communication and education outreach on the Navajo Nation.

Education

Ph.D., Environmental Engineering and Science, Clemson University, 1998; B.S., Optics, University of Rochester, 1990; Certified Health Physicist, American Board of Health Physics, 2006.

Sowder, cont.

Publications

B. Chisholm, S. Krahn, A. Croff, P. Marotta, A. Sowder, N. Smith. *A Technology Neutral Safety Assessment Tool for Advanced Nuclear Reactors: Preliminary Hazard Assessment and Component Reliability Database for the Molten Salt Reactor Experiment*. ICAPP 2018. Charlotte, NC. April 8-11, 2018.

B. Burkhardt, S. Krahn, T. Ault, A. Croff, A. Sowder, N. Irvin. 2016. *Technology Assessment of an Advanced Reactor Design – A Case Study on a Molten Salt Reactor (MSR)*. ICAPP 2016. San Francisco, CA. April 17-20, 2016.

A. Sowder, B. Burkhardt, S. Krahn, N. Irvin. 2016. *Expanding the Concept of Flexibility for Evaluating Advanced Nuclear Energy Systems as Future Commercial Options*. ICAPP 2016. San Francisco, CA. April 19, 2016.

Technology Assessment of a Molten Salt Reactor Design - The Liquid Fluoride Thorium Reactor (LFTR). EPRI, Palo Alto, CA. 2015. 3002005460.
https://www.epri.com/#/pages/product/3002005460/

B. Smith, S. Krahn, A. Croff, J. Clarke, A. Machiels, A. Sowder. 2015. *Comparison of Radioactive Waste Volumes from Single Used Nuclear Fuel Recycling and the Once-Through Nuclear Fuel Cycle*. International High-Level Radioactive Waste Management Conference, Charleston, SC, USA. April 12-16, 2015.

A. Gardiner, S. Krahn, T. Ault, A. Croff, B. Burkhardt, J. Clarke, L. Fyffe, A. Machiels, A. Sowder. 2015. *Development and Testing of a Decision Framework and Decision Tool for Determining Fuel Cycle Preferences*. International High-Level Radioactive Waste Management Conference, Charleston, SC, USA. April 12-16, 2015.

Radiological Risks and Waste Management Impacts of a U.S. Transition from a Once-Through to a Modified Open Nuclear Fuel Cycle: A Quantitative Comparative Risk Analysis. EPRI, Palo Alto, CA: 2014. 3002003156.
https://www.epri.com/#/pages/product/3002003156/

S. Krahn, A. Croff, B. Smith, J.H. Clark, A. Sowder, and A. Machiels. 2014. *Evaluating the Radiological Risk to Workers from the U.S. Once-Through Nuclear Fuel Cycle*. Nuclear Technology. 185: 192-207.

S. Krahn, A. Resch-Gardiner, T. Ault, A. Croff, B. Smith, J. Clarke, A. Machiels, A. Sowder, 2014. *Decision Analysis Tool to Support Decision-Making for Development of Nuclear Fuel Cycle Technologies*. ANS 2014 Winter Meeting, November 9-13, 2014, Anaheim, California.

S. Krahn, A. Sowder, A. Machiels, R. Jubin, A. Croff, T. Ault, 2014. *Nuclear Fuel Cycle Technology Readiness Metrics Level Determination: The Results of a Focused Expert Review*. ICAPP 2014, April 6-9, 2014, Charlotte, NC.

A.G. Sowder, A.J. Machiels, A.A. Dykes, D.H. Johnson. 2013. *A Decision Analysis Framework to Support Long-Term Planning for Nuclear Fuel Cycle Technology Research, Development, Demonstration and Deployment*. Global 2013, September 29 – October 3, 2013, Salt Lake City, UT.

EPRI Framework for Assessment of Nuclear Fuel Cycle Options. EPRI, Palo Alto, CA: 2013. 1025208.
http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000000001025208

Dr. Steven L. Krahn

Professional Experience

Vanderbilt University, Professor of the Practice of Nuclear Environmental Engineering, Department of Civil & Environmental Engineering (Present) - teaches three (3) graduate-level courses in Nuclear Environmental Engineering and performs research in the field of the nuclear fuel cycle, risk assessment and systems engineering. He is Principal Investigator (PI) on risk analysis and advanced nuclear reactor safety analysis research projects with the Electric Power Research Institute (EPRI), involving quantitative radiological risk assessment of present and future nuclear technology. He leads Vanderbilt research in the area of nuclear and chemical safety for DOE-EM. In addition, Dr. Krahn provides nuclear systems engineering and risk management consulting to the U. S. nuclear industry.

U. S. Department of Energy, Deputy Assistant Secretary for Safety, Security, and QA Office of Environmental Management (6/09 – 11/10) - led the Safety, Security and QA Program for DOE's Office of Environmental Management (EM), the largest nuclear program in the U.S.; he was the technical approval authority for this $6.5B/year program on matters associated with nuclear safety, risk analysis, radiological safety, quality assurance, and security matters. Dr Krahn was selected by the Under Secretary as a member of DOE's Risk Assessment Working Group, a top-level, technical advisory panel which oversaw the Department's implementation of Quantitative Risk Assessment. Further, Dr. Krahn chaired the EM Technical Authority Board (TAB) - the top-level, technical review for engineering & safety issues, reporting directly to the Assistant Secretary; he also served as the Deputy Chair of the DOE Nuclear Safety R&D Committee, which provided direction to nuclear safety research performed by DOE. He received the DOE Career Meritorious Service Award.

U. S. Department of Energy, Director, Office of Waste Processing (8/07 – 6/09) - directed the engineering and technology research to identify, advance, develop, and implement engineering concepts, technologies, and practices that improved the performance of DOE nuclear chemical processing projects. Dr Krahn performed technical reviews of a spectrum of facilities, including: the Waste Treatment Plant at Hanford, the Salt Waste Processing Facility at SRS, the Plutonium Preparation/Pit Disassembly and Conversion Facility Project at SRS.

Perot Systems Government Services (PSGS), Senior Vice President/Consultant (4/00 – 8/07) - directed and provided and technical consulting services to DOE, commercial nuclear companies and NASA in the areas of nuclear safety, systems engineering, quality assurance and risk management. He has provided nuclear system engineering consulting to DOE's Y-12 Complex in Oak Ridge, TN; technical and nuclear safety advice to the Nuclear Materials Technology Division at the Los Alamos National Laboratory; safety management, system engineering and risk management consulting for NASA's Office of Safety & Mission Assurance after the loss of the space shuttle Columbia; nuclear safety and technical consulting to the High-Level Waste (HLW) Tank Farms at Hanford; and engineering and nuclear safety consulting to a nuclear fuel cycle facility, regulated by the NRC. Dr Krahn played pivotal roles in several major technical reviews including: the independent investigation of a major fire in a plutonium fabrication facility at Rocky Flats in 2005; also he had leadership roles in the pre-operational reviews for the Spent Nuclear Fuel Project (Hanford) and the start-up of a nuclear test reactor (Sandia). Also, Dr. Krahn chaired the Senior Safety Review Board, providing independent technical and nuclear safety oversight for the HLW Tank Farms at the Hanford from 2001-2006 and also chaired the Independent Safety Review Board for the Metropolis Technical Works, an NRC-regulated fuel cycle facility from 2005 -2007.

PricewaterhouseCoopers LLP (PwC), Principal Consultant (9/98 to 3/00) - During his work with PwC, Dr. Krahn provided systems engineering and nuclear safety consulting services to DOE Management & Operating contractors (similar to those described above).

Krahn, cont.

U. S. Defense Nuclear Facilities Safety Board (DNFSB) Deputy Technical Director (3/97 to 9/98) – provided technical leadership for the DNFSB. During this time, Dr. Krahn led the technical review of DOE's storage of a highly hazardous isotope of uranium (U-233); the review assessed the risks present in storage & the stability of the chemical/physical configurations of U-233, systematically assessed the uses for the isotope, and provided an engineered set of solutions based on overall risk. He also led several high-priority reviews of weapons-related issues. Dr Krahn was awarded the DNFSB Meritorious Service Award in 1998.

DNFSB, Assistant Technical Director for Nuclear Weapons Programs (10/92 to 3/97) - was the lead DNFSB technical staff member for the implementation of major revisions to DOE'S technical standards and processes for assuring the safety of operations involving nuclear explosives; worked with DOE officials for 3 years to enhance safety management system used for assembling, disassembling and testing nuclear explosive devices; these changes brought modern risk management (e.g., risk-informed methods, formality of operations, hazards assessment) into in the nuclear weapons complex. In 1997, Dr. Krahn was the inaugural winner of the John W. Crawford Award for technical achievement at the DNFSB.

DNFSB, Rocky Flats Program Manager (5/91 to 9/92) - led technical and nuclear safety review of operations in 2 plutonium processing facilities supporting of defense missions.

Orion International Technologies, Inc., DOE Office of New Production Reactors, Principal Engineer (7/90 to 5/91) - led the system-based reengineering of the research and development program to support the design review of several new reactors.

Integrated Systems Analysts, Inc., Navy Maintenance Division, Division Manager, (9/87 to 7/90) - led the technical development of reliability-centered maintenance (RCM) program to increase safety and operational availability of surface ships.

U.S. Navy, Engineering Duty Officer, (12/78 to 11/1987) - was a senior project manager for 4+ years at a naval shipyard, directing both nuclear and non-nuclear work. Previously, Dr. Krahn was selected by Admiral Rickover for duty on his staff as a Nuclear Engineer; he reviewed and approved all modifications and design changes to the reactor plant fluid systems aboard three classes of submarines and two land-based prototypes. Dr. Krahn was one of the youngest engineers ever granted "signature authority" by Admiral Rickover.

Education

Doctorate, Public Administration, Univ. of Southern California, 2001; **MS, Materials Science,** Univ. of Virginia, 1994; **BS, Metallurgical Engineering,** Univ. of Wisconsin, 1978; **Certificate, Management & Leadership,** Massachusetts Institute of Technology, 2009; **Certificate, Nuclear Engineering,** Bettis Reactor Engineering School, U.S. Department of Energy, 1980.

Recent Pertinent Publications

- "Application of a Method to Estimate Risk in Advanced Nuclear Reactors: A Case Study on the Molten Salt Reactor Experiment," B. Chisholm, **S. Krahn**, A. Afzali, A. Sowder, accepted for presentation at the Probabilistic Safety Assessment and Management Conference (PSAM 14), September 2018, Los Angeles, CA
- "Estimating Worker Collective Doses from a Revised Approach to Managing Commercial Nuclear Fuel," B. Burkhardt, **S. Krahn**, A. Croff, A. Sowder, Radwaste Solutions, Volume 22, No. 1, pp (January/June 2015)
- "Comparative Assessment of Thorium Fuel Cycle Radiotoxicity," A. Croff & **S. Krahn**, Nuclear Technology, Vol. 194, pp 271-280 (May 2016)

Krahn, cont.

- "Evaluating the Radiological Risk to Workers from the U.S. Once-Through Nuclear Fuel Cycle," **S. Krahn**, A. Croff, B. Smith, J. Clarke, A. Sowder, A. Machiels, Journal of Nuclear Technology, Volume 185, Number 2, pp 192-207 (February 2014)
- "A Preliminary Analysis of Key Issues in Chemical Industry Accident Reports," L. Fyffe, **S. Krahn**, J. Clarke, D. Kosson, J. Hutton, Safety Science, Vol.82, pp 368-373 (February 2016)

Allen G. Croff

Professional Experience

Nuclear Waste Technical Review Board, Member (2015 to present) - evaluates the technical and scientific validity of U.S. Department of Energy activities related to managing and disposing of spent nuclear fuel and high-level radioactive wastes.

National Academy of Sciences' Committee on Supplemental Treatment of Low-Activity Waste at the Hanford Nuclear Reservation, Vice Chairman (2017 to present) - reviewing the Department of Energy=s plans for supplemental processing and immobilization of low-activity waste at the Hanford Site.

Vanderbilt University Department of Civil and Environmental Engineering, Adjunct Professor (2011 to present) - lecturing and participating in research and development projects for the Department of Energy and the Electric Power Research Institute in areas related to nuclear energy, the nuclear fuel cycle, and radioactive waste management.

Blue Ribbon Commission on America's Nuclear Future, Senior Technical Advisor (2010 to 2012) - provided technical support to the Commissioners and Commission staff members in the form of technical reviews, background papers, and verbal explanations concerning nuclear energy and the nuclear fuel cycle.

U.S. Nuclear Regulatory Commission (NRC), Vice Chairman of the Advisory Committee on Nuclear Waste and Materials (2004 to 2008) - Vice-chairman of a committee of five independent technical advisors to the NRC Commissioners concerning the activities of NRC staff in the areas of waste disposal, nuclear fuel cycle activities, nuclear materials, and transportation until the Committee's merger with the Advisory Committee on Reactor Safeguards. Subsequently a consultant to the Nuclear Regulatory Commission from 2008 to 2010 concerning licensing of the proposed repository at Yucca Mountain, Nevada.

National Council on Radiation Protection (NCRP), Member and Committee Chairman (1998 to present) - Elected as one of about 70 Council members for three six-year terms and now a Distinguished Emeritus Member. The NCRP provides authoritative information to concerning radiation protection and radiation measurements, quantities and units, to the U.S. government agencies and the public. Chairman of a NCRP committee (1993 to 2003) that produced a report providing the scientific foundation for a unified system of classifying wastes as a basis for addressing problems such as the inconsistencies between management of radioactive and chemical wastes and the need to determine the concentration of hazardous materials below which they can be neglected.

Oak Ridge National Laboratory (ORNL) (1973 to 2003) – employed in progressively more responsible technical, line management, and program management positions concerning waste management, nuclear fuel cycle, and nuclear materials research and development (R&D). Technical accomplishments at ORNL include:

- Creation of the ORIGEN2 computer code used world-wide to calculate the radioactive characteristics of nuclear materials for use in nuclear material and waste. characterization, risk analyses, and nuclear fuel cycle analysis.
- Developing and evaluating comprehensive, risk-based waste classification systems, including changing the boundary defining transuranic waste from 10 to 100 nCi/g and numerous technical reports and papers on this subject.
- Performing technical, economic, and systems analyses of current and advanced nuclear fuel cycles from uranium mining through waste disposal.

Croff, cont.

- Conceiving, analyzing, and reviewing actinide partitioning-transmutation (P-T) concepts beginning with the first comprehensive analysis of P-T from 1976 to 1980 through subsequent cycles of renewed interest in the concept.
- Participating in over ten committees plus the Nuclear Radiation Studies Board of the National Academy of Sciences.

Management accomplishments at ORNL include:

- Environmental Technology Program Development, Manager (2000 to 2003) - Responsible for creating or identifying new opportunities for ORNL research staff to provide R&D solutions concerning environmental management and waste disposal to meet the needs of U.S. Department of Energy (DOE) and other sponsors.
- Chemical Technology Division, Associate Director (1993 to 2000) – line management of a 300-person, $60M+/year technical organization conducting nuclear and non-nuclear R&D activities ranging from lab/desktop scale to demonstration scale.

Nuclear Development Committee of the Nuclear Energy Agency (NEA), Chairman (1992 to 2002) - Elected chairman of a standing international committee of the NEA the mandate of which includes the breadth of nuclear technology. Function of the Committee is to initiate specific studies related to nuclear energy and publish the results in internationally recognized consensus reports.

Nuclear Energy Research Advisory Committee, Member (1998 to 2005) -: Appointed by the Secretary of Energy to three successive two-year terms on an independent advisory committee to DOE's Office of Nuclear Energy (1998 to 2005).

Education

Nuclear Engineer Degree, Massachusetts Institute of Technology (1974); **Bachelor of Science Degree in Chemical Engineering**, Michigan State University (1971); **Master of Business Administration Degree**, University of Tennessee (1981).

Pertinent Publications

- "Estimating Worker Collective Doses from a Revised Approach to Managing Commercial Nuclear Fuel", B. Burkhardt, S. Krahn, **A. Croff**, A. Sowder, Radwaste Solutions, Volume 22, No. 1, pp (January/June 2015)
- "Comparative Assessment of Thorium Fuel Cycle Radiotoxicity", **A. Croff** & S. Krahn, Nuclear Technology, Vol. 194, pp 271-280 (May 2016)
- "Evaluating the Radiological Risk to Workers from the U.S. Once-Through Nuclear Fuel Cycle", S. Krahn, **A. Croff**, B. Smith, J. Clarke, A. Sowder, A. Machiels, Journal of Nuclear Technology, Volume 185, Number 2, pp 192-207 (February 2014).
- "Risk-Informed Radioactive Waste Classification and Reclassification", **A. Croff**, Health Physics, 91(5), 449-460 (2006).
- "Risk-Based Waste Classification of Radioactive and Hazardous Chemical Wastes", **A. Croff** (Committee Chairman), Report No. 139 of the National Council on Radiation Protection and Measurements (December 2002).
- "ORIGEN2: A Versatile Computer Code for Calculating the Nuclide Compositions and Characteristics of Nuclear Materials", **A. Croff**, Nucl. Tech. 62(3), 335 (September 1983).
- "Nuclear Waste Partitioning and Transmutation", J.O. Blomeke & **A. Croff**, Nucl. Tech. 56(2), 361 (February 1982).

Paul J. Marotta, PhD., P.E., BCEE

Professional Experience

Vanderbilt University, Department of Civil & Environmental Engineering 2017 – Present
Research Engineer

Dr. Marotta performs research in the field of risk assessment and systems engineering supporting advanced nuclear reactor safety analysis research projects with the Electric Power Research Institute (EPRI), involving quantitative radiological risk assessment of present and future nuclear technology.

AquAeTer Inc., Brentwood, TN 2012–Present
Technical Director

Efforts are focused on close client interaction developing and providing solutions and managing projects from the strategic level through to implementation. The spectrum of projects ranges from wastewater and air pollution, to Merger & Acquisition, litigation support, to quantifying project financial risk for nuclear decommissioning projects valued at $1billion. Participate as an active member of the Board of Directors.

AquAeTer Inc., Brentwood, TN 2001–2012
Operations Manager

Responsible for managing the overall operations of a $3 million engineering consulting firm with 14 direct reports (scientists and engineers). Project director and technical expert in biological wastewater treatment and air pollution control. Roles include project manager, mentor for junior staff and business development leadership. Participate as an active member of the Board of Directors.

International Paper, Corporate Technology, Cincinnati, OH 1996 – 2001
Senior Staff Engineer

Provided technical leadership for capital projects with environmental impacts and participated as the technology specialist for the corporate multi-disciplinary Merger/Acquisition team for the Champion International ($7.3 billion) and Union Camp deals ($5.0 billion) . The scope of major capital projects technical review was approximately 100 projects per year in the $1million to $100 million range.

International Paper, Liquid Packaging, Kansas City, KS 1994 – 1996
Plant Manager

Primary responsibilities were overall business P&L and directing the lead team for a packaging manufacturing facility with 150 employees. Focus areas included capital project development, developing and initiating an employee training program, customer satisfaction and quality management.

International Paper, Folding Carton, Clinton, IA 1992 – 1994
Manufacturing Manager

Responsible for all manufacturing related activities and directing the senior manufacturing team managing over 800 employees. Focus areas included facilitating the development of a high performance work team environment with annual operating savings of over $2 million per year, and capital upgrade projects for two printing presses ($1.8 million), a new glue line ($0.5 million) and a new electron beam dryer ($1.2 million).

International Paper, Corporate Headquarters, Memphis, TN 1992 – 1992
Corporate Environmental Manager

Provided direct support to multiple paper mills and manufacturing facilities with environmental regulatory compliance challenges. Transitioned to the Environmental Manager for the Folding Carton Division during this time, which lead to the position as manufacturing manager in Clinton, Iowa.

Marotta, cont.

International Paper, Ticonderoga Paper Mill, Ticonderoga, NY **1990 – 1992**
Environmental Compliance Leader

Directly responsible for overall mill environmental regulatory compliance including air emissions, wastewater discharge, solid waste, hazardous waste and water treatment. Provided regulatory guidance to the mill lead team, process area leaders and interfaced with internal/external council and federal, state and local regulators.

International Paper, Ticonderoga Paper Mill, Ticonderoga, NY **1989 – 1990**
Capital Project Engineer

Responsible for developing and implementing large capital projects in the power plant area including a 35 MW GE (multiple extraction) steam turbine rotor replacement, boiler super heater replacement and major annual shutdown repair projects.

General Electric, Knolls Atomic Power Laboratory, Niskayuna, NY **1981 – 1988**
New Prototype Concept Team Design Engineer

Focused on developing new prototype reactor plant design concepts for advanced emergency core cooling systems.

Brittle Fracture Prevention Design Engineer

Developed finite element models of reactor pressure vessels including a new 3-dimensional finite element model of the reactor nozzle/vessel intersection. This model was the first of its kind used to set operating limits.

Prototype Field Engineer (Kesselring Site)

Supervised construction activities and developed test procedures for installation and testing of emergency core cooling systems similar to post-TMI upgrades required for commercial facilities. Primary interface with the system design group to modify designs as required for installation, and directed skilled trades.

Thermal/Hydraulic Design Engineer

Responsible for performing extensive design basis accident transient analyses utilizing complex computer simulation models. The initial stages of the analysis process required obtaining an expert level understanding of each accident transient and a complete understanding of reactor dynamics and the relationships between major components such as reactor coolant pumps, pressurizers, steam generators, turbines and condensers.

Education and Certifications

Paul earned a Bachelor of Science degree from Siena College in Applied Mathematics, a Bachelor of Engineering degree from Manhattan College, a Master's degree in Engineering from Union College and a PhD. from the University of Tennessee, all in Mechanical Engineering. He has also completed the Manufacturing Executive Program at the University of Michigan, the Knolls Atomic Design Power School and is a Board Certified Environmental Engineer. He is also an adjunct Assistant Professor at the University of Tennessee Space Institute where he teaches graduate level courses in conduction and radiation heat transfer and thermodynamics.

Marotta, cont.

Pertinent Publications

Marotta, P., Steam Reheat in Nuclear Power Plants. PhD diss., University of Tennessee, 2012.

Marotta, P., High Temperature Gas Reactor Steam Reheat. American Nuclear Society Annual Meeting. Atlanta, GA, 2013. Vol. 108: p. 619-620.

Marotta, P., and Antar, B., Small Modular Reactor Thermal Performance Improvement with Addition of a High Temperature Gas Reactor Superheater, in ASME 2014 Small Modular Reactors Symposium. 2014, American Society of Mechanical Engineers: Washington, DC. p. v001T01A007.

Marotta, P., Moeller, T., Antar, B. and Ruggles, A., Thermal Radiation Heat Transfer Analysis for High Temperature Steam. American Nuclear Society Winter Meeting. Washington D.C., 2013. Vol. 109: p. 1720-1721.

Marotta, P., Antar B. and Krahn, S., Optimizing Nuclear Energy at a Refinery. Transactions of the American Nuclear Society Winter Meeting, 2015. 113: p. 912-914.

Marotta, P., Antar B. and Krahn, S., All Nuclear Superheater Design Method. Transactions of the American Nuclear Society Annual Meeting, 2016. 114: p. 603-606.

Brandon M. Chisholm

Relevant Experience

Vanderbilt University, Ph.D. Candidate and Graduate Research Assistant, Department of Civil & Environmental Engineering (Present) - performs research in the field of the nuclear fuel cycle, risk assessment, and systems engineering. Involved in specific projects focusing on risk analysis and advanced nuclear reactor safety analysis research projects with the Electric Power Research Institute (EPRI), involving quantitative radiological risk assessment of present and future nuclear technology. He also contributes Vanderbilt research in the area of nuclear and chemical safety for DOE-EM. Brandon's dissertation topic is the development of a technology-neutral methodology to analyze risks associated with advanced reactor designs and demonstrate this methodology on the Molten Salt Reactor Experiment (MSRE).

Oak Ridge National Laboratory (ORNL), Higher Education Research Experiences (HERE) Graduate Intern, Reactor & Nuclear Systems Division (06/17-09/17) – became thoroughly immersed in the design and operating details of the MSRE by reviewing design and safety basis documentation, consulting with subject matter experts, and physically inspecting the facility. Brandon then used this knowledge to apply a newly developed methodology to identify licensing basis events for molten salt reactors (MSRs) and investigate the applicability of this methodology. The results of this effort were presented at the ORNL MSR workshop and documented in an ORNL technical report.

North Carolina State University, Nuclear Regulatory Commission (NRC) Licensed Test Reactor Operator, Nuclear Reactor Program (01/14-05/16) – qualified, became licensed, and operated the PULSTAR test reactor and performed various facility maintenance responsibilities. Knowledge gained during qualification and operating provided Brandon with an extensive knowledge regarding nuclear reactor theory and operating behavior.

Education

MS, Environmental Engineering, Vanderbilt University, 2018

BS, Nuclear Engineering, North Carolina State University, 2016

Recent Pertinent Publications

- "Application of a Method to Estimate Risk in Advanced Nuclear Reactors: A Case Study on the Molten Salt Reactor Experiment," B. Chisholm, S. Krahn, A. Afzali, E. Harvey, accepted for presentation at the Probabilistic Safety Assessment and Management Conference (PSAM 14), September 2018, Los Angeles, CA
- "Licensing Basis Event Selection Case Study: The Molten Salt Reactor Experiment," B. Chisholm, G. Flanagan, S. Krahn, G. Mays, Presented at the ORNL 2017 MSR Workshop, October 2017, Oak Ridge, TN.
- "Preliminary Hazard Assessment and Component Reliability Database for the Molten Salt Reactor Experiment," B. Chisholm, S. Krahn, A. Croff, P. Marotta, A. Sowder, and N. Smith. International Congress on Advances in Nuclear Power Plants (ICAPP 2018) Proceedings pp 513-522, April 2018, Charlotte, NC
- "Preliminary Risk Assessment of a Generalized Molten Salt Reactor Off-Gas System," B. Chisholm, S. Krahn, P. Marotta, A. Croff. Transactions of the American Nuclear Society, 2017. Vol. 117, pp 221-224.

Karl N. Fleming

Professional Experience

KNF Consulting Services LLC, President (Present) – Performs consulting services in the fields of reliability engineering and risk assessment of complex engineered systems. He is an internationally recognized expert in probabilistic risk assessment and risk management of nuclear reactor systems. He is a member of the ASME/ANS Joint Committee on Nuclear Risk Management, a co-author of the ASME/ANS PRA Standard, a principal author of the ASME/ANS PRA Standard for Advanced non-LWRs, as well as hundreds of reports, papers, and peer reviewed articles on the development and application of PRA technology to nuclear reactor safety. His 45 years of experience includes more than 25 years in light water reactor (LWR) PRA technology, more than 15 years in high temperature gas-cooled reactor (HTGR) PRA, and extensive experience in applying PRA technology to the aerospace, process, and chemical industries in risk-informed applications. Mr. Fleming is the Chairman of the ASME/ANS Joint Committee on Nuclear Risk Management Writing Group responsible for the PRA Standard on Advanced non-LWRs. This group was responsible for a trial use version of that standard ASME/ANS-Ra-S-1.4-2013 and is currently developing an ANSI version to reflect feedback from extensive pilot PRAs.

Mr. Fleming's major accomplishments include the following: He is the lead author of an International Atomic Energy Agency Safety Report on PRA of multi-unit sites. As an extension of this effort, he organized and was the technical chairman of an international workshop on multi-unit PSA sponsored by the Canadian Nuclear Safety Commission. Mr. Fleming has take the lead role in developing technical guides and standards for multi-unit and multi-reactor module PRAs. On this topic, Mr. Fleming has participated in an NRC Commissioners Briefing in 2011 and has presented his work on multi-unit PRA to the National Academy of Sciences. Mr. Fleming is a key author of the Licensing Modernization Project (LMP) white papers and guidance documents for the risk-informed and performance-based licensing of advanced non-LWRs. He was the lead author of the LMP white papers on selection and evaluation of licensing basis events, safety classification and performance requirements for SSCs, and PRA development for advanced non-LWRs. He was a contributing author to the white paper on evaluation of defense-in-depth adequacy and the LMP Guidance Document that is currently being used to inform an NRC regulatory guidance for licensing advanced non-LWRs. These documents are built on a similar series of documents that were developed to support the licensing of PBMRs and the Next Generation Nuclear Plant project and authored or co-authored by Mr. Fleming. Mr. Fleming is also a co-author of ANS 53.1, the design standard for advanced helium cooled reactors which is based on the NGNP white papers, and the Department of Energy PRA Standard for non-reactor facilities.

ERIN Engineering and Research, In. Vice President of PWR Technology (1995-2001). Mr. Fleming established and managed the Southern California office of ERIN. While at ERIN was the principal investigator of EPRI's Risk Informed In-service Inspection (RI-ISI) project and lead author of the EPRI Topical Report on that topic which was reviewed and approved by the NRC. He lead a team that performed 22 reactor plant applications of the RI-ISI methodology which was responsible for significant cost and radiation exposure reductions associated with meeting inservice inspection requirements. While at ERIN, he was responsible for the publication of EPRI guidelines and pipe failure rate data reports for the performance of internal flooding and high energy line break PRAs.

Fleming, cont.

Pickard, Lowe, and Garrick, Inc; Vice President Nuclear Energy Systems (1981-1995). He was responsible for business development and project management of PRA projects on nuclear power plants including Seabrook, South Texas Project, Beaver Valley, and Kernkraftwerk Goesgen. During the Seabrook he led the effort to resolve emergency planning issues and performed the first full scope PRA of multi-unit accidents. He was a co-author of the EPRI PSA Applications Guide and the PRA Procedures Guide (NUREG/CR-2300). His contributions to PRA technology include the development of methods for common cause failure analysis in PRA including the Beta Factor, Multiple Greek Letter, and contributing author of the Alpha Factor method, methods for predicting the reliability of piping systems, for estimating the influence of inspections on pipe rupture frequencies, pioneering work in internal fire and internal flooding PRA, PRA of events initiated during low power and shutdown, PRA of multi-unit accidents, PRA database development, probabilistic treatment of severe accident phenomena in Level 2 PRA, and risk-informed applications including in-service inspection of piping systems and technical specifications.

General Atomics Inc., Senior Engineer (1974-1981). Mr. Fleming developed the Beta Factor Method of Common Cause Failure Analysis and was the principal investigator of the Department of Energy's Accident Initiation and Progression Analysis project which produced a PRA for a high temperature gas-cooled reactor.

Education

Master of Science, Nuclear Science and Engineering, Carnegie-Mellon University 1974;

B.S. Physics, Penn State University. Cum Laude, 1969

Recent Pertinent Publications

Fleming, K.N. and M.K. Ravindra, "Technical Approach to NuScale Multi-Module Seismic PRA", Report developed by KNF Consulting Services LLC for Nuscale Power, June 12, 2015

Fleming, K.N., "On The Risk Significance Of Seismically Induced Multi-Unit Accidents", paper presented at PSA-2015 Sun Valley 2015

Fleming, K.N, et al, "Technical Approach to Multi-Unit Probabilistic Safety Assessment (MUPSA)", International Atomic Energy Agency Report, SSR-8.5, 2018

Fleming, K.N., and B.O.Y. Lydell, Pipe Rupture Frequencies for Internal Flooding PRAs, Revision 4. EPRI, Palo Alto, CA: 2018. 3002000079.

Fleming, K.N., and B.O.Y. Lydell, Guidelines for Performance of Internal Flooding Probabilistic Risk Assessment. EPRI, Palo Alto, CA: 2009. 1019194.

Fleming, K. N., "Markov Models for Evaluating Risk Informed In-Service Inspection Strategies for Nuclear Power Plant Piping Systems", Reliability Engineering and System Safety, Vol. 83, No. 1 pp.:27-45, 2004.

Fleming, Karl N., "Markov Models for Evaluating Risk Informed In-Service Inspection Strategies for Nuclear Power Plant Piping Systems", Vol. 83 No. 1 Reliability Engineering and System Safety, Jan 2004. pp. 27-45

Fleming, Karl N., "Issues and Recommendations for Advancement of PRA Technology for Risk Informed Decision Making", prepared by Technology Insights for U.S. NRC Advisory Committee on Reactor Safeguards, NUREG/CR-6813, January 2003

Fleming, Karl N. and Fred A. Silady, "A Risk Informed Framework for Defense in Depth for Advanced and Existing Reactors", Reliability Engineering and System Safety, Elsevier Publishing Company, 78 (2002) pp. 205–225

Dr. David Heywood Johnson

Professional Experience

Dr. Johnson currently the lead of the Nuclear Safety and Security Unit of the **B. John Garrick Institute for the Risk Sciences at UCLA**. Current projects include supporting interdisciplinary teams building a foundation for new advanced nuclear power systems. These include investigating the relationship of process hazard analyses and probabilistic risk analyses for unique designs (EPRI); informing the test reactor plan for a new reactor concept to reduce the licensing risk for the commercial design (Southern); and, participating as Vice Chair in the development of ANS Standard 30.1, a design standard for new non-LWR reactors. Previously while at **ABS Consulting (Vice President – Quantitative Risk Analysis, 2000–2017)** he recently led the risk analysis activities on a multidisciplinary team integrating physics-based analyses in support of a risk-informed solution to a long standing generic safety issue for commercial nuclear power plants (GSI-191). He was also a key contributor in developing a multi-attribute decision framework supporting the evaluation of future nuclear fuel cycle strategies for EPRI's Future of Nuclear Power initiative.

While at **EQE International (1997–2000)** and **PLG, Inc. (1980–1997)**, Dr. Johnson served as project manager for the Defense Threat Reduction Agency's (formerly the Defense Special Weapons Agency) "START III Active Stockpile/Inactive Stockpile" Study. Study provides a technical basis for the Inactive Stockpile inventory, considering aging, testing, and repair, in support of the START III Treaty. Dr. Johnson served as project manager for the Defense Special Weapons Agency (DSWA) (formerly the Defense Nuclear Agency) B 52 Electrical Study performed to identify and evaluate the hazard scenarios associated with the exposure of the B 52H weapon system to electrical environments that could lead to special nuclear material dispersal. The analysis addressed all potential abnormal electrical environments that may occur during activities associated with peacetime stockpile to target sequence operation. Key technical contributor to the DSWA Fire Resistance Enhance (FRE) study. Provided technical analyses and oversight for the evaluation of the needs, benefits, and costs associated with introductory FREs to selected weapons. Principal Investigator for the B 52H Weapons System Safety Assessment. Developed methodology that breaks the stockpile to target sequence into logical groups for a detailed study of the overall risk related to B 52H force generation. Dr. Johnson served as key technical contributor to the NRC BETA project to develop the Kalinin PRA (Russia) as well as training and procedures for future PRAs to be conducted in Russia and was co-author of PRA procedures developed for use in former Soviet Union and Eastern European countries. He received training on VVER technology and operations in Russia.

Dr. Johnson served as project manager for the High Flux Australian Reactor PSA. Project manager and key technical contributor to the DOE High Flux Isotope Reactor PRA and the Health Physics Research Reactor PRA. Key contributor to the shutdown events PRA of the Dodewaard nuclear plant and the assessment of operator actions in support of the Surry Shutdown PRA. Technical lead for the Level 1/Level 2 interface consulting that ABS Consulting (formerly PLG) for Electricité de France. Project manager of ABS Consulting's evaluation of the environmental hazards PRA of BNL's High Flux Beam Reactor.

For more than 25 years, he has provided PRA services to the Tennessee Valley Authority. He served as principal investigator for the Multi Unit Browns Ferry PRA and the BFNU2M and BFNU3M PRAs. He served as technical project leader for TVA's IPEs performed on Browns Ferry Unit 2, Sequoyah, and Watts Bar Nuclear Power Plants. He served as project manager and one of the principal investigators for the Browns Ferry Unit 1 PRA; also primary focal point of ABS/TVA technology transfer efforts. Dr. Johnson served as project manager in the Phase I Bellefonte Unit 1 PRA. He served as key participant in Pilgrim Safety Enhancement Program and probabilistic containment response analysis. He made technical contributions to Vermont Yankee Containment Safety Study. He made significant technical contributions to the Nine Mile Point Unit 1 limited scope probabilistic safety assessment, the Hatch Integrated Plant Risk Model, and the DOE/TVA sponsored integrated probabilistic public health risk, plant damage, and

Johnson, cont.

economic model for the Sequoyah Nuclear Plant, among others. Dr. Johnson served as project manager for PSA support and update for the Browns Ferry Extended Power uprate system. He served as project manager for the Browns Ferry Severe Accident Mitigation Alternatives (SAMA) Analyses. He served as project manager of Browns Ferry PSA to support restart of Unit 1.

International Atomic Energy Agency (IAEA) Technical Expert missions to Bulgaria in support of the Kozloduy PSA. IAEA IPERS team member for review of PRA for Petten Research Reactor in the Netherlands. Dr. Johnson performed oversight and review for the analysis of programmatic risks associated with the Viability Assessment of the Yucca Mountain Project. Invited participant, Conference on Managing Risk In and Around Airports, Amsterdam, 1994.

Member, Committee on Review and Evaluation of the Army Chemical Stockpile Disposal Program, National Research Council, 2001-2004. Member, Committee on Review of Army Planning for the Disposal of M55 Rockets at the Anniston Chemical Agent Disposal Facility, National Research Council, 2003. Invited participant in National Research Council workshop to Reduce Space Science Research Mission Costs. Invited reviewer of National Research Council's "Tooele Chemical Agent Disposal Facility: Update on National Research Council Recommendations," 1999, and Integrated Design of Alternative Technologies for Bulk Only Chemical Agent Disposal Facilities, 2000. Associate Editor of Risk Analysis: An International Journal, Society for Risk Analysis, 1991 1998; Editorial Board, 1999 - 2008. Instructor, University of California at Irvine, Extension School, "Risk Analysis and Management," 1999.

Previously (1979-1980), as an **Advisory Committee on Reactor Safeguards Fellow**, assisted Committee members in reviewing and evaluating the potential hazards associated with nuclear facilities. Also provided independent assessments of selected topics of concern to the members. These topics included the advisability of review of industry operating experience and the development and implications of candidate quantitative risk acceptance criteria.

Education

Sc.D., Nuclear Engineering, Massachusetts Institute of Technology, Cambridge, 1979

M.S., Nuclear Engineering, Massachusetts Institute of Technology, Cambridge, 1976

Research Assistant, 1977 1978. General Electric Foundation Fellowship, 1976 1977.Teaching Assistant, 1974 1976

B.S. with High Honors, Nuclear Engineering, University of Florida, Gainesville, 1974

Relevant Recent Publications

Johnson, D.H., M.A. Linn and C.T. Remsey, "Identification and Quantification of Risk Scenarios for a Unique Nuclear Reactor – a Historical Example," proceedings of the 14th International Probabilistic Safety Assessment and Management (PSAM 14), Los Angeles, CA, September 2018.

Morton, D., B. Letellier, J. Tejada, **D. H. Johnson**, et al., "Sensitivity Analyses for a High Order Simulation Used in the STP GSI-191 Risk Informed Resolution Project," proceedings of the International Conference on Nuclear Energy (ICONE22), Prague, Czech Republic, July 7–11, 2014.

Johnson, D. H., A. A. Dykes, A. G. Sowder, and A. J. Machiels, "Programmatic Assessment of RG-MOX Utilization Following Participation in the DOE Surplus Plutonium Disposition Program," proceedings of the 12th International Probabilistic Safety Assessment and Management Conference (PSAM 12), Honolulu, Hawaii, June 2014.

The Electric Power Research Institute, Inc. (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety and the environment. EPRI members represent 90% of the electric utility revenue in the United States with international participation in 35 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; and Lenox, Mass.

Together...Shaping the Future of Electricity

Programs:

Technology Innovation

Nuclear Power

Advanced Nuclear Technology

© 2018 Electric Power Research Institute (EPRI), Inc. All rights reserved. Electric Power Research Institute, EPRI, and TOGETHER...SHAPING THE FUTURE OF ELECTRICITY are registered service marks of the Electric Power Research Institute, Inc.

3002011801

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com