Development of a Technology-Inclusive Methodology to Analyze the Environmental, Safety, and Health Risks Associated with Advanced Nuclear Reactor Designs as Demonstrated on the Molten Salt Reactor Experiment

By

Brandon M. Chisholm

Dissertation

Submitted to the Faculty of the

Graduate School of Vanderbilt University

in partial fulfillment of the requirements

for the degree of

DOCTOR OF PHILOSPHY

in

Environmental Engineering

May 8, 2020

Nashville, Tennessee

Approved:

Steven L. Krahn, D.P.A.
David S. Kosson, Ph.D.
Mark D. Abkowitz, Ph.D.
James H. Clarke, Ph.D.
Askin Guler Yigitoglu, Ph.D.

To Mom, Nick, and Dad, for making me who I am today

and

To Lauren, for inspiring me to never give up

ACKNOWLEDGEMENTS

Honestly, there are so many people without whom I would have never been able to achieve what I have so far; I don't even know where to begin to express my gratitude.

First of all, I'd like to thank my family for setting me up for success. Mom, words cannot describe how much your relentless care and hard work means to me. Nick, you've been the best right-hand man that anyone could ever ask for. Dad, thank you for sending me down the path to be an engineer and for giving me the motivation to always do better. GramHoney and Pa, your love and support has allowed me to follow my passion. To the rest of the Chizners, thank you for always being there when I need you and for always making me laugh and laughing with me (sometimes at me). I also want to thank all the friends who have been a part of my life so long that you're a part of my family too: Mr. Lloyd and Miss Rita, Zach, Conner, Stroudly, the rest of the Rhodes family, Erik, Charles, Aaron, and so many others. You'll never know how much you have helped me along the way, and how thankful I am.

Dr. Krahn, thank you for all of your guidance during my graduate studies and for the opportunities and doors that you have opened up for me. I sincerely appreciate the foundation that you have helped develop for me as I begin my professional career.

Thank you to everyone else at Vanderbilt who has helped me out since I got to Nashville. To my committee members, your feedback and encouragement has been instrumental in making this dissertation a success. Allen, Paul, Megan, Carole, Bethany, and Tim, this work wouldn't have been possible without your guidance and technical assistance. Jack, Bowen, Yanqing, Peng, Chris, and Chelsea, thank you for always helping to put a smile on my face. Charity, Bev, Karen Fuller, Karen Page, and Jackie, I owe you each quite a few favors for always helping me figure out how to get things done.

Thank you to all of the organizations (and the people in the organizations) that made this project possible and helped shape both this research and my future. Thank you to the US Department of Energy and the Nuclear Energy University Programs. Your fellowship support has permitted me to dream big and tackle some important problems that I may have not had the opportunity to address otherwise. I would especially like to thank George, Gary, Askin, David, Zack, Tommy, and Anita at ORNL; Lauren, Irvin, Amir, Smith, and Lance at Southern; Andrew and Cristian at EPRI; and the B. John Garrick Institute for the Risk Sciences at UCLA. Karl and Joe, thank you also for your help over the past 4 years.

Last, but certainly not least, I'd like to thank the two beautiful souls that dealt with me pretty much every day and got me through the toughest moments of the work for this dissertation. Hattie, thank you for napping next to me while I stared at a computer screen for hours on end, all the while never forgetting to remind me when it was time for your dinner. Lauren, thank you for constantly putting up with my nonsense and making all the hard work worthwhile. I'm so excited for the next chapter of our lives together as a family.

Disclaimers

This material is based upon work partially supported under a Department of Energy, Office of Nuclear Energy, Integrated University Program Graduate Fellowship. As such, this report was prepared in part as an account of work sponsored by an Agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof.

The research in this dissertation was also partially supported by the Electric Power Research Institute (EPRI) Agreement #10007945, "Vanderbilt University Support for Developing Best Practices for Integrating Safety Assessment in the Advanced Reactor Design (PHA to PRA)." As such, this report was prepared in part as an account of work sponsored by EPRI. Neither EPRI nor any of their employees makes any warranty, expressly or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of the information contained herein.

TABLE OF CONTENTS

Page

LIST OF TABLES ... xi

LIST OF FIGURES ... xii

LIST OF ABBREVIATIONS ... xv

DEFINITIONS ... xvii

GLOSSARY OF RELEVANT NUCLEAR ENGINEERING TERMS ... xix

Chapter

1. Introduction and Motivation ... 1
   - 1.1. Background ... 1
   - 1.2. Research Objectives ... 5
   - 1.3. Key Questions and Dissertation Structure ... 6
   - 1.4. Dissertation Scope ... 8
2. Literature Review of Relevant Risk Assessment and Safety-in-Design Approaches and Prior Efforts ... 11
   - 2.1. Industry-Standard Approaches for Quantitative Risk Assessment ... 11
   - 2.2. PHA and Early Stage Safety Analysis ... 15
   - 2.3. Safety-in-Design and Risk-Informed Frameworks for Safety Assessment ... 18
   - 2.4. Prior Safety and Risk Assessments of Liquid-Fueled Molten Salt Reactors ... 21
     - 2.4.1. Original Safety Basis for the MSRE ... 21
     - 2.4.2. Recent LF-MSR Safety Assessment Efforts ... 25
   - 2.5. Summary ... 34
3. Overview of a Technology-Inclusive Methodology to Analyze ES&H Risks associated with Advanced Reactor Designs ... 38
   - 3.1. Overall Methodology Structure ... 38
   - 3.2. Analysis Tools and Interfaces between Methods ... 41
     - 3.2.1. Hazard Identification ... 41
     - 3.2.2. Operating Experience and Stylized Accidents ... 42
     - 3.2.3. Hazards and Operability (HAZOP) Study Method ... 42
     - 3.2.4. Key Phenomena Identification and Ranking ... 47

3.2.5. Exhaustive Identification of Initiators 47
3.2.6. Event Sequence Development 48
3.2.7. Quantitative Consequence Analysis 49
3.2.8. Failure Modes and Effects Analysis (FMEA) 50
3.2.9. Fault Tree Analysis (FTA) 50
3.2.10. Component Reliability Data 51
3.2.11. Quantitative Event Tree Analysis (ETA) 52
3.2.12. Selection of Appropriate Risk Metrics 52
3.3. Summary of Interfaces between Methodology Elements 53
3.4. Observations from Methodology Development 65
4. Hazard and Operability Studies of the Molten Salt Reactor Experiment 66
4.1. Overview of MSRE Design and Inventories of Radioactive Material 68
4.2. Preparing for MSRE HAZOP Studies 75
4.3. Conducting MSRE HAZOP Studies 77
4.4. Results of MSRE HAZOP Studies and Related Design Insights 79
4.4.1. MSRE Fuel Salt Loop 79
4.4.2. MSRE Fuel Salt Processing System 81
4.4.3. MSRE OGS and CCS 84
4.5. Relationships between MSRE HAZOP Studies and Other Analyses 86
5. Identification of Postulated Initiating Events for the MSRE Design 87
5.1. Approach for Identifying MSRE PIEs 88
5.2. Master Logic Diagram for the MSRE 96
5.3. Identification of MSRE PIEs 104
5.4. Observations from PIE Identification 107
6. Analysis of MSRE Freeze Valve Failure Rates and Evaluation of Design Insights 110
6.1. MSR Freeze Valve Literature 112
6.1.1. MSRE Freeze Valve Design Information 112
6.1.2. Experience with MSRE Freeze Valves 120
6.1.3. Recent MSR Freeze Valve Analysis and Testing Efforts 122

6.2. PHA studies of an MSRE Freeze Valve 126
6.2.1. Overview of Approach 127
6.2.2. Conduct of MSRE Freeze Valve PHA Studies 128
6.2.3. Qualitative Hazard, Risk, and Performance Insights 133
6.3. MSRE Freeze Valve Reliability Estimates 135
6.3.1. Constructing and Evaluating Freeze Valve System Fault Trees 136
6.3.2. Failure Rate of FV-103 to Thaw on Demand 137
6.3.3. Failure Rate for a Spurious Thaw of FV-103 139
6.3.4. Failure Rate Sensitivity Study 141
6.4. Observations from Freeze Valve Studies 142
7. Event Tree Analysis of MSRE Off-Gas System 145
7.1. Analysis Approach 147
7.2. ETA and FTA Development 149
7.2.1. Initiating Event: Release of Radioactive Material to Reactor Cell 152
7.2.2. Pivotal Event 1: Fuel Salt Drain 155
7.2.3. Pivotal Event 2: Isolation of Cell Exhaust Flow 156
7.3. Quantitative ETA Results 157
7.4. Discussion of Event Sequence Consequences 159
7.5. Risk-Informed Evaluation of MSRE OGS Safety and Design 162
7.6. Observations from OGS Risk Assessment 166
8. Conclusions 169
8.1. Lessons Learned from Methodology Demonstration 170
8.1.1. Risk Assessment during Pre-conceptual Design 174
8.1.2. Risk Assessment during Conceptual Design 175
8.1.3. Risk Assessment during Preliminary Design 176
8.1.4. Risk Assessment during Final Design and Beyond 176
8.2. Methodology Demonstration Challenges 177
8.2.1. Resource Constraints 177
8.2.2. Quantitative Consequence Analysis 178

8.2.3. Selecting a Risk Metric ... 178
8.2.4. Modeling Challenges ... 179
8.3. Other Observations Concerning the Effective Implementation of the Methodology ... 180
8.4. Potential Areas for Future Work ... 181
8.5. Reflections and Concluding Remarks ... 183
REFERENCES ... 185
Appendix
A. Background on Fluid-Fueled Nuclear Reactors ... 201
A.1. Early Aqueous Homogeneous Reactor Research ... 203
A.2. Fluid-Fueled Reactor Research at Los Alamos ... 204
A.2.1. The First Homogeneous Reactors ... 204
A.2.2. The Los Alamos Power Reactor Experiments (LAPRE-I and -II) ... 208
A.2.3. Los Alamos Molten Plutonium Reactor Experiment (LAMPRE-I) ... 210
A.3. The Homogenous Reactor Program at ORNL ... 212
A.4. The Aircraft Nuclear Propulsion Program at ORNL ... 215
A.5. The Molten Salt Reactor Program at ORNL ... 216
A.5.1. The Molten Salt Reactor Experiment ... 217
A.5.2. Conclusion of the MSRP at ORNL ... 218
References for Appendix A ... 219
B. HAZOP Results Used to Support MSRE ETA ... 221
C. Quality Assurance Considerations for the MSRE HAZOP Studies ... 229
References for Appendix C ... 230
C.1. Resumes of MSRE HAZOP Team Members ... 231
D. Fault Tree Models and Basic Event Data Used to Estimate Failure Rates for FV-103 ... 243
D.1. Fault Tree and Basic Event Data for Spurious Thawing of FV-103 ... 243
D.2. Fault Tree and Basic Event Data for Failure of FV-103 to Thaw on Demand ... 260
References for Appendix D ... 264
E. Fault Tree Models and Basic Event Data Used in MSRE OGS ETA ... 265

E.1. Fault Tree and Basic Event Data for Initiating Event – Release of Radioactive Material from OGS to Reactor Cell 265

E.2. FT and Basic Event Data for Pivotal Event #1 – Fuel Salt Drain 272

E.3. FT and Basic Event Data for Pivotal Event #2 – Isolation of Cell Evacuation Flow 279

References for Appendix E 287

F. Calculations to Estimate Radioactivity of Gaseous Flow into MSRE OGS 288

References for Appendix F 290

LIST OF TABLES

Table Page

1. Overview of GIF advanced nuclear systems.... 2
2. LFTR PIEs identified by Geraci [2017] 28
3. MSFR PIE families identified by Gèrardin et al. [2019] 29
4. FUJI 233-Um PIEs identified by Pyron [2016].... 31
5. Summary of prior LF-MSR hazard and risk assessment efforts.... 35
6. Summary of interfaces between methodology elements 54
7. Major Plant Operating States (POSs) of the MSRE.... 91
8. Interfaces and barriers for radioactive material in the MSRE fuel salt loop during normal operations.... 101
9. Interfaces and barriers for radioactive material inventory in the main MSRE OGS during normal operations 102
10. MSRE PIE categories with applicable inventories of radioactive material.... 105
11. Excerpt of MSRE freeze valve FMEA results 132
12. Calculated freeze valve failure rates, MSRE as designed.... 138
13. Sensitivity study - modified freeze valve failure rates assuming no redundant cooling gas isolation valve.... 141
14. Summary of event sequences in OGS ETA 158
15. Elements of DID identified for the MSRE OGS during analysis of OGS-2.... 166
16. Summary of information available at a given design stage and useful tools for generating ES&H risk insights.... 173
17. Correlations between stages in reactor design process and TRLs 174
18. Excerpt of HAZOP study results used to help construct ET model 221
19. Basic event data used in fault tree for spurious thaw of FV-103.... 255
20. Basic event data used in fault tree for failure of FV-103 to thaw on demand 262
21. Basic event data used in fault tree for release of radioactive material from OGS to reactor cell 269
22. Basic event data for fault tree of fuel salt drain 277
23. Basic event data for fault tree of failure to isolate cell exhaust flow.... 285
24. Estimated radioactivity of OGS flow in Line 522 288

LIST OF FIGURES

Figure Page

1. Elements of developed methodology and associated dissertation chapters ... 9
2. Simple example of a fault tree linked to an event tree ... 14
3. Overview of methodology ... 39
4. Basic steps in a HAZOP study ... 46
5. Example of relationship between HAZOP study results and ETA ... 49
6. Elevation view of MSRE building ... 70
7. Flowsheet of the major components in the MSRE design ... 71
8. Detailed view of MSRE fuel salt and coolant salt systems ... 72
9. Schematic of MSRE fuel salt loop ... 80
10. Schematic of MSRE fuel processing system ... 82
11. Schematic of MSRE OGS ... 85
12. Schematic of barriers to release of radioactivity for MSRE fuel salt loop during normal operations ... 93
13. Schematic of barriers to release of radioactivity for MSRE main OGS during normal operations ... 94
14. Schematic of barriers to release of radioactivity for MSRE fuel processing system during fluorination ... 95
15. Levels 1-4 of the MSRE MLD ... 99
16. Example of Levels 4-9 of the MSRE MLD for the radioactive material in the off-gas during normal operations ... 100
17. Example of freeze valve subsystem ... 113
18. Example of freeze valve piping ... 114
19. Schematic of freeze valve layout with siphon pots ... 115
20. Location of MSRE freeze valves ... 117
21. Schematic of MSRE FV-103 layout ... 118
22. Schematic of MSRE FV-103 subsystem ... 129
23. Process for selecting and evaluating Licensing Basis Events (LBEs) ... 146
24. Frequency-Consequence (F-C) target suggested by LMP for evaluation of LBEs ... 147
25. MSRE OGS and CCS instrument application diagram ... 150
26. Event sequence diagram for a release of radioactive material from the main OGS to the reactor cell during normal operations ... 151
27. Flowsheet including major CCS and OSG components ... 153
28. Schematic diagram of MSRE containment and ventilation systems ... 154
29. Event tree developed for MSRE OGS ... 158
30. Decomposition of safety functions for MSRE OGS LBEs ... 163

31. Framework for evaluating LBEs using layers of defense concept adapted from IAEA 165
32. Relationship between safety analysis tools and design development 172
33. Schematic of a Light Water Reactor (LWR) nuclear power plant 201
34. Structure of an LWR fuel assembly 202
35. Schematic of a Liquid-Fueled Molten Salt Reactor nuclear power plant concept 203
36. Cross section of LOPO design 205
37. Picture of a "Water Boiler" reactor at Los Alamos 206
38. Schematic diagram of North Carolina State R-1 reactor 207
39. Schematic of LAPRE-I reactor 209
40. LAPRE-II core assembly with heat exchanger (upper section) and baffle that enclosed critical region (bottom section) 210
41. Cutaway view of the LAMPRE-I reactor 211
42. Schematic of HRE design 213
43. Cutaway view of the HRT core vessel 214
44. Photo of the HRT core vessel 214
45. Elevation section of the ARE core 216
46. Fault tree for spurious thaw of FV-103 (Page 1 of 12) 243
47. Fault tree for spurious thaw of FV-103 (Page 2 of 12) 244
48. Fault tree for spurious thaw of FV-103 (Page 3 of 12) 245
49. Fault tree for spurious thaw of FV-103 (Page 4 of 12) 246
50. Fault tree for spurious thaw of FV-103 (Page 5 of 12) 247
51. Fault tree for spurious thaw of FV-103 (Page 6 of 12) 248
52. Fault tree for spurious thaw of FV-103 (Page 7 of 12) 249
53. Fault tree for spurious thaw of FV-103 (Page 8 of 12) 250
54. Fault tree for spurious thaw of FV-103 (Page 9 of 12) 251
55. Fault tree for spurious thaw of FV-103 (Page 10 of 12) 252
56. Fault tree for spurious thaw of FV-103 (Page 11 of 12) 253
57. Fault tree for spurious thaw of FV-103 (Page 12 of 12) 254
58. Fault tree for failure of FV-103 to thaw on demand (Page 1 of 2) 260
59. Fault tree for failure of FV-103 to thaw on demand (Page 2 of 2) 261
60. Fault tree for release of radioactive material from OGS to reactor cell (Page 1 of 4) 265
61. Fault tree for release of radioactive material from OGS to reactor cell (Page 2 of 4) 266
62. Fault tree for release of radioactive material from OGS to reactor cell (Page 3 of 4) 267
63. Fault tree for release of radioactive material from OGS to reactor cell (Page 4 of 4) 268
64. Fault tree for fuel salt drain (Page 1 of 7) 272
65. Fault tree for fuel salt drain (Page 2 of 7) 273
66. Fault tree for fuel salt drain (Page 3 of 7) 274
67. Fault tree for fuel salt drain (Page 4 of 7) 274

68. Fault tree for fuel salt drain (Page 5 of 7).......... 275
69. Fault tree for fuel salt drain (Page 6 of 7).......... 276
70. Fault tree for fuel salt drain (Page 7 of 7).......... 276
71. Fault tree for failure to isolate cell exhaust flow (Page 1 of 7).......... 279
72. Fault tree for failure to isolate cell exhaust flow (Page 2 of 7).......... 280
73. Fault tree for failure to isolate cell exhaust flow (Page 3 of 7).......... 281
74. Fault tree for failure to isolate cell exhaust flow (Page 4 of 7).......... 282
75. Fault tree for failure to isolate cell exhaust flow (Page 5 of 7).......... 282
76. Fault tree for failure to isolate cell exhaust flow (Page 6 of 7).......... 283
77. Fault tree for failure to isolate cell exhaust flow (Page 7 of 7).......... 284

LIST OF ABBREVIATIONS

ACRS: Advisory Committee on Reactor Safeguards
AEC: Atomic Energy Commission
AIChE: American Institute of Chemical Engineers
ANS: American Nuclear Society
AOO: Anticipated Operational Occurrence
ASME: American Society of Mechanical Engineers
BDBE: Beyond Design Basis Event
CCF: Common-Cause Failure
CCPS: Center for Chemical Process Safety
CCS: (MSRE) Component Cooling System
CDF: Core Damage Frequency
CFSRS: (TMSR-LF) Core Fuel Salt Release System
DBA: Design Basis Accident
DID: Defense-in-Depth
DOE: Department of Energy
EPRI: Electric Power Research Institute
ES&H: Environmental, Safety, and Health
ET: Event Tree
ETA: Event Tree Analysis
FFMEA: Functional Failure Modes and Effects Analysis
FHR: Fluoride-salt-cooled High-temperature Reactor
FMEA: Failure Modes and Effects Analysis
FT: Fault Tree
FTA: Fault Tree Analysis
GFR: Gas-cooled Fast Reactor
GIF: Generation IV International Forum
HAZOP: Hazards and Operability (study)
HRA: Human Reliability Analysis
IAEA: International Atomic Energy Agency
IE: Initiating Event
ISA: Integrated Safety Analysis
ISAM: Integrated Safety Assessment Methodology
LBE: Licensing Basis Event
LERF: Large Early Release Frequency
LF-MSR: Liquid-Fueled Molten Salt Reactor
LFR: Lead-cooled Fast Reactor

LFTR: Liquid Fluoride Thorium Reactor
LMP: Licensing Modernization Project
LWR: Light Water Reactor
MCA: Maximum Credible Accident
MLD: Master Logic Diagram
MSBR: Molten Salt Breeder Reactor (specific LF-MSR design concept)
MSR: Molten Salt Reactor
MSRE: Molten Salt Reactor Experiment (specific LF-MSR design)
MSRP: (ORNL) Molten Salt Reactor Program
NASA: National Aeronautics and Space Administration
NEI: Nuclear Energy Institute
NGNP: Next Generation Nuclear Plant (specific advanced reactor design concept)
NRC: Nuclear Regulatory Commission
OGS: Off-Gas System
OPT: Objective Provision Tree
ORNL: Oak Ridge National Laboratory
ORO: (AEC) Oak Ridge Operations (office)
PHA: Process Hazards Analysis
PIE: Postulated Initiating Event
PIRT: Phenomena Identification and Ranking Table
POS: Plant Operating State
PRA: Probabilistic Risk Assessment
PrHA: Preliminary Hazards Analysis
QSR: Qualitative Safety features Review
R&D: Research and Development
RIPB: Risk-Informed and Performance-Based
RM: Radioactive Material
RORC: (ORNL) Reactor Operations Review Committee
RSWG: (GIF) Risk and Safety Working Group
SAR: Safety Analysis Report
SCWR: SuperCritical Water-cooled Reactor
SFR: Sodium-cooled Fast Reactor
SiD: Safety in Design
SR-SSCs: Safety-Related Structures, Systems, and Components
SSCs: Structures, Systems, and Components
TMSR: Thorium Molten Salt Reactor (development project)
TMSR-LF: Thorium Molten Salt Reactor, Liquid-Fueled (specific LF-MSR design concept)
VHTR: Very High-Temperature gas-cooled Reactor

DEFINITIONS

The terms on this page are often used in a variety of contexts, and sometimes the meanings of these terms can slightly differ for different applications and/or industries. For clarity, the definitions of these terms for the purposes of this dissertation are provided, as follows.

Hazard: a potential condition that can possibly result in undesired consequences [Ericson, 2011]. A *hazard* is a factor or condition that might operate against *safety* [International Atomic Energy Agency (IAEA), 2019].

Node: a section of a *system* (or process) being analyzed during a Process Hazards Analysis or similar study [Crawley and Tyler, 2015]. A study *node* is typically defined as having a single major function and can be a *subsystem* or a smaller grouping of components.

Plant Operating State (POS): a standard arrangement of a system during which conditions are relatively constant and are distinct from other configurations in ways that impact *risk*. [ASME/ANS, 2013]

Reliability: the probability of an item to perform a desired function under stated conditions for a specified period of time [US Department of Defense (DoD), 2005].

Risk: a measure of potential future events that could occur and result in outcomes with undesirable consequences [Ericson, 2011]. *Risk* involves three parameters: (1) a potential future event, (2) the likelihood of the event occurring, and (3) the potential consequences from the event when it occurs [Kaplan and Garrick, 1981].

Risk-Informed: a nonprescriptive approach to decision-making in which insights from *hazard* and *risk* assessments are considered, along with other sources of insights [Nuclear Energy Institute (NEI), 2019]. "Risk-based" is a commonly used term with a similar definition [Ericson, 2011].

Safety: the condition of being protected against physical harm or loss [Ericson, 2011]. It is noted that safety itself is not a device; it is a state of being safe or an activity working toward creating a safe state.

Subsystem: a subset of a *system*; a smaller *system* that is part of a larger *system* [Ericson, 2011]. In this dissertation, a *subsystem* represents a coherent and somewhat independent portion of a larger *system* and typically is characterized by fewer and/or more specific functions than a *system*. For example, the components that have the function of controlling the air temperature within the cabin of a car represent one of many *subsystems* that compose the larger *system* of the car.

System: an integrated composite of components that provides function and capability to satisfy a stated need or objective [Ericson, 2011]. A *system* is a holistic unit that is functionally greater than the sum of its parts.

Technology-Inclusive: is applicable to a variety of different technologies and/or *system* designs, without needing significant alteration. Other commonly used terms with similar definitions include "technology-neutral" and "design-agnostic."

GLOSSARY OF RELEVANT NUCLEAR ENGINEERING TERMS

Activation Product: an unstable (i.e., radioactive) isotope of an element created by neutron bombardment. An example of an activation product is carbon-14 resulting from the absorption of a neutron by carbon-13 in the structural material of a reactor (e.g., steel). [Wood, 2007]

Control Rod: a device used to absorb neutrons so that the chain reaction in a reactor core may be slowed or stopped by inserting them further or accelerated by withdrawing them. [Wood, 2007]

(Reactor) Coolant: the material that absorbs and removes the heat produced by nuclear fission and maintains the temperature of the *fuel* within acceptable limits. The absorbed heat can then be applied so as to drive electricity-generating turbines. A coolant can also be a *moderator*; water is used in this dual way in most nuclear reactors. [Nuclear Energy Agency (NEA), 2012]

Criticality: the stage of a nuclear reactor when enough neutrons are created by fission to make up for those lost by leakage or absorption, such that the number of neutrons produced in fission remains constant. [NEA, 2012]

Enriched material: material in which the percentage of a given isotope present in the material has been artificially increased, so that it is higher than the percentage of that isotope naturally found in the material. For example, enriched uranium contains more of the fissile uranium-235 than the naturally occurring percentage (0.7%). [Atomic Energy Commission (AEC), 1969]

Fast neutron: a neutron released during fission, travelling at very high velocity (20,000 km/s) and having high energy (~2 MeV). Fast neutrons can cause fission in *fissile* materials, but the probabilities are less than that for *thermal neutrons*. However, the number of isotopes that can fission increases as the energy of the neutron increases. [Wood, 2007]

Fast reactor: a nuclear reactor with little or no *moderator* and hence utilizing *fast neutrons*. A fast reactor normally burns plutonium while producing *fissile* isotopes in *fertile* material (such as depleted uranium or thorium). [Wood, 2007]

Fertile: capable of becoming *fissile* by capturing neutrons, possibly followed by radioactive decay. Examples of fertile isotopes include uranium-238 and plutonium-240. [Wood, 2007]

Fissile: capable of capturing a *thermal neutron* and undergoing nuclear fission. Examples of fissile isotopes include uranium-235, uranium-233, and plutonium-239. [Wood, 2007]

Fission Products: the fragments resulting from the splitting of a nucleus during fission. When a nucleus undergoes fission, it generally splits into two fragments while releasing neutrons and energy. The resulting fragments may be stable or unstable (i.e., radioactive). The term "fission products" can also refer to the daughter nuclide resulting from the radioactive decay of the unstable fission fragments. [NEA, 2012; Wood, 2007]

Fissionable: capable of undergoing fission. *Fissile* isotopes are fissionable by *thermal neutrons*. [Wood, 2007]

Fuel: the part of a nuclear reactor that contains the *fissionable* material. [NEA, 2012]

Moderator: used to slow *fast neutrons* down to the *thermal* energy range to increase the likelihood that they cause fission. The moderator must be a light material that will allow the neutrons to slow down efficiently from collisions with lighter nuclei without there being a high probability of the neutrons being absorbed. Usually, ordinary water is used; an alternative is graphite (a form of carbon). [NEA, 2012; Wood, 2007]

Reactivity: a measure to express the departure of a reactor from *criticality*. A positive reactivity addition indicates a move towards supercriticality (power increase). A negative reactivity addition indicates a move towards subcriticality (power decrease). *Control rods* are an example of a component used to control reactivity. [NEA, 2012]

Source Term: the amount and isotopic composition of material released (or postulated to be released) during an accident. [Wood, 2007]

Thermal neutrons: are those with a low kinetic energy, less than 1 electron volt (eV). Thermal neutrons have the greatest probability of causing fission in uranium-235 and plutonium-239. [NEA, 2012]

Thermal reactor: a nuclear reactor in which the fission chain reaction is sustained primarily by *thermal neutrons* and hence requiring a *moderator* (as distinct from a *fast reactor*). [Wood, 2007]

CHAPTER 1, INTRODUCTION AND MOTIVATION

In the efforts to reduce greenhouse gas emissions and limit the severity of global climate change, nuclear power represents a time-tested electricity generation technology that can reduce climate mitigation costs [Pehl et al., 2017; Socolow and Glaser, 2009]. Nuclear power also minimizes other threats to the environment and human health; for example, compared to other energy sources, nuclear power offers smaller plant footprints, a better worker and user safety record, and significantly lower emissions of environmental pollution [Rhodes, 2018; Rhodes and Beller, 2000].

Because of modern advancements in areas such as materials, supercomputing, and modular construction, recent interest has significantly increased towards the development of "advanced" nuclear reactor designs. These reactors offer the potential for enhanced safety, efficiency, and economics when compared to currently operating commercial nuclear reactors, and the deployment of these advanced technologies can help hedge the risk of high climate mitigation cost [Generation IV International Forum (GIF), 2014b; Lehtveer and Hedenus, 2015]. However, the design of an advanced nuclear reactor, along with the environmental, safety, and health (ES&H) hazards associated with such designs, can differ substantially from that of current commercial reactor designs -- and from that of other advanced reactors.

The development of a flexible methodology to comprehensively identify the hazards and determine the most significant risks associated with the operation of these new designs is required in order to systematically assess the safety of advanced nuclear reactors, along with their potential for environmental insult. Additionally, integration of appropriate safety and risk assessment methods into the design process can provide valuable insights and feedback early in the systems development process, when changes are less costly to make. As such, the research presented in this dissertation was conducted in order to define and exercise a hazard and risk assessment methodology applicable to early stage advanced nuclear power designs, particularly those based on alternatives to present, dominant Light Water Reactor (LWR) technology.

1.1. Background

There are a variety of advanced nuclear technologies under development that have made different selections regarding reactor fuels, coolants, moderators, and heat transfer system designs. The Generation IV International Forum (GIF) is a cooperative international endeavor that was set up to carry out the research and development (R&D) needed to establish the feasibility and performance capabilities of the next generation of nuclear energy systems. The six advanced reactor systems defined by GIF include the gas-cooled fast reactor (GFR), lead-cooled fast reactor (LFR), molten salt reactor[1] (MSR), sodium-cooled fast reactor (SFR), supercritical water-cooled reactor (SCWR), and very high temperature gas-cooled reactor (VHTR) [GIF, 2014b]. The various designs of the Generation IV systems feature thermal and fast neutron spectra, as well as a wide range of reactor sizes from very small to very large; the main characteristics of these systems are summarized in Table 1. Even between individual designs of a given next generation reactor system design details (including the form of the fuel and the fuel cycle) can be substantially different. For example, the VHTR has two typical configurations (i.e., the pebble bed type and the prismatic block type), and at least one concept is being developed for each configuration [GIF, 2014b].

Table 1: Overview of GIF advanced nuclear systems
(adapted from [World Nuclear Association (WNA), 2019] and [GIF, 2013])

	Neutron Spectrum (fast/thermal)	Coolant	Temperature (°C)	Pressure
GFR	Fast	Helium	900-1000	High
LFR	Fast	Lead or Pb-Bi	480-570	Low
MSR (liquid-fueled)	Thermal or fast	Halide salts (w/ dissolved fuel)	700-800	Low
MSR (solid-fueled)[2]	Thermal	Fluoride salts	750-1000	Low
SFR	Fast	Sodium	500-550	Low
SCWR	Thermal or fast	Water	510-625	Very high
VHTR	Thermal	Helium	900-1000	High

Due to the variation amongst design details and operating conditions in these reactor systems, the hazard profile associated with each of these technologies varies, and the most risk-significant accident for a given reactor type may be prevented or mitigated by a fundamental design feature of another. For example, an undesirable occurrence that can lead to the melting of the solid fuel and potential release of radioactivity in current LWR designs is an exothermic oxidation of the metal fuel cladding by high-temperature steam in the water coolant [Cheng et al., 2016]. However, VHTR designs use helium as coolant, which avoids the possibility of this particular hazard since the inert gas does not chemically interact with the graphite fuel cladding [GIF, 2014b].

The US Nuclear Regulatory Commission (NRC) has explicitly expressed the desire not to prioritize one single advanced reactor technology when considering how to develop a method

[1] Including both liquid-fueled and solid-fueled design variants

[2] Solid-fueled MSRs are sometimes also referred to as Fluoride High-temperature Reactors (FHRs).

to assess the safety of advanced reactors in order to license them [NRC, 2008]. In order to allow for an ES&H risk assessment approach to be beneficial to the most stakeholders, a flexible approach to identify hazards and assess risk in a variety of nuclear reactor designs is necessary. The long history of events that has led to the maturation and deployment of the LWR commercial power industry has produced a tailored set of standards and practices that may not be ideally suited for advanced technologies, especially those at an early stage of the design process. Many, if not most, of today's safety analysis methods, standards, and tools have been developed and applied specifically for deployed LWR nuclear power technology. As such, they are not applicable to advanced reactor systems or very early stages of design without significant modifications. The NRC has also identified the need to develop the ability to review advanced technologies (including non-LWRs) and to identify and resolve technology-inclusive policy issues that impact safety and regulatory reviews of next generation nuclear power plants [NRC, 2018b]. Ongoing nuclear electricity generation industry-led initiatives have the goal of working with regulators and constructing a relationship that is beneficial to both parties [Cowan, 2016]. Conversations involving reactor developers and regulators regarding the hazard and risk assessment approaches for advanced reactors will likely reduce the uncertainty surrounding environmental and safety aspects of licensing these reactor designs for both sides.

Therefore, there is a clear need for a technology-inclusive methodology to assess the risks of advanced reactors and achieve Safety-in-Design (SiD) for commercial reactor designs. A more risk-informed approach for investigating potential risk-significant scenarios is needed to identify those accidents that should be of greatest priority to the designers and regulators of advanced reactors, to assist in verifying that the reactor design meets the public health risk safety goals of the NRC. Furthermore, if the applicable hazards of a reactor design can be identified, and the risk significance can be assessed systematically at an early stage of design, the analysis can lead to design decisions that will help minimize the risk associated with postulated accident scenarios. Because most contemporary safety assessment approaches have evolved alongside regulatory frameworks addressing the existing fleet of operating LWRs, guidance for and understanding of their application to less mature or novel technologies that employ different coolants and operate in different pressure and temperature regimes is lacking. It is particularly important for the developed methodology to be technology-inclusive, along with being practical and effective in the early stages of the design process. Thus, this dissertation attempts to define and demonstrate an approach that allows designers and ES&H analysts of any advanced nuclear system to assess their design, incorporate insights into the design, incrementally build a rigorous safety case, and, if desired, begin an early conversation with regulators.

This effort draws from the SiD guidance from the US Department of Energy (DOE) [2016], and is consistent with SiD approaches endorsed domestically by the NRC [NRC, 2008] and the joint American Society of Mechanical Engineers (ASME) and American Nuclear Society (ANS) draft Probabilistic Risk Assessment (PRA) Standard for Advanced Non-Light Water Reactor Nuclear Power Plants [ASME/ANS, 2013]. Furthermore, this approach is also consistent with international SiD approaches, such as the GIF's Integrated Safety Assessment Methodology (ISAM) [GIF, 2011], and the safety assessment approach suggested by the International Atomic Energy Agency (IAEA) [IAEA, 2002]. As mentioned by the NRC in its Policy Statement on the regulation of advanced reactors [NRC, 2008], early SiD has important benefits, some of which could impact success or failure in the ultimate deployment of a technology. In particular, early SiD encourages the practice of sound systems engineering principles and provides a structure for hazard identification and documentation that incentivizes participation across a variety of technical disciplines in the design organization.

A phased approach to integrating SiD from the conceptual stage of design through final design is advantageous, as continuous and growing awareness of identified hazards early in design allows for effective improvements while there is still flexibility in the design to make changes and minimize economic impacts [US DOE, 2016]. Furthermore, early SiD also allows a design organization to continuously rank and prioritize safety design issues, associated technological uncertainty, and the need for research and analysis. A systematic approach to early SiD helps to ensure that safety concerns are identified as early as possible, allowing for sufficient time to plan efficient and well-formulated methods to reduce the severity of such concerns, including test and demonstration programs.

In addition to being conducive to early SiD, another fundamental objective of the methodology developed and demonstrated in this dissertation is to identify hazards and risks, incrementally and iteratively increasing in detail and complexity, to ultimately produce a safety case supported by a PRA model. PRA[3] is an endpoint that has become expected as a part of the safety analysis for next generation advanced nuclear power reactors [NRC, 2008]. The use of PRA has been initiated for some advanced reactor technologies, including VHTRs [GA Technologies, 1987] and SFRs [Grabaskas, 2014]. However, Liquid Fueled MSRs (LF-MSRs) are an example of an advanced nuclear technology that lacks a significant body of quantitative risk assessment case studies, since most LF-MSRs have not surpassed a relatively immature stage of design development, as noted by the B. John Garrick Institute for the Risk Sciences [Southern Company, 2019a]. This lack of experience -- coupled with the fact that multiple LF-MSR

[3] PRA is sometimes referred to in the nuclear industry (especially internationally) as Probabilistic Safety Assessment (PSA).

developers have formally notified the NRC of their intent to engage in regulatory interactions [NRC, 2019a] -- highlights the benefit that could be gained from the demonstration of a method to identify hazards and analyze the risks inherent in an LF-MSR design.

Additionally, LF-MSRs have a hazard profile that is particularly dissimilar to those of other reactor technologies. In current commercial reactor designs (including LWRs and Heavy Water Reactors) and most advanced reactor types (such as GFRs, LFRs, SCWRs, SFRs, VHTRs, and even Fluoride-cooled High-temperature Reactors[4]), the nuclear fuel and radioactive fission products are secured within multiple structures of relatively small volume (e.g., fuel pellets, spheres, or rods). In an LF-MSR, the fuel and fission products (as well as any activation products) are dissolved and circulating throughout a much larger volume. This larger volume may have penetrations for draining the fuel or the handling of volatile fission products, meaning that physical or chemical changes of the fuel (e.g., temperature or redox conditions) can result in the transport of radioactive material due to changes in properties like solubility. Due to the integrated nature of hazards such as high temperature and radioactive material, in addition to the lack of significant operating experience of LF-MSRs,[5] a solid basis to identify and evaluate risk-significant accidents on a prescribed, deterministic basis (such as that developed for LWRs over the past five decades) does not exist. Instead, a flexible and comprehensive approach to identify hazards and analyze their significance in a reactor design represents a more robust method to assess the safety of these reactor designs. Thus, in this dissertation, the developed ES&H risk assessment approach is demonstrated using a LF-MSR design in order to illustrate its flexibility and help contribute to the development of experience in the area of LF-MSR risk assessment.

1.2. Research Objectives

In an effort to fill a current knowledge gap, the objectives of the research presented in this dissertation are:

1. To identify, integrate, adapt, and deploy the best available and emerging industry practices in a technology-inclusive manner in order to establish a method to evaluate and confirm Safety-in-Design (SiD) for advanced reactors -- beginning at early stages of development; and,

---

[4] FHRs are sometimes considered a subset of MSRs because they utilize molten salt as coolant. However, FHRs have small, discrete, solid fuel elements in contrast to the dissolved fuel of LF-MSRs.

[5] A more thorough discussion on nuclear reactors operating with fluid fuel is provided in Appendix A of this dissertation.

2. To demonstrate an ES&H hazard and risk assessment methodology applicable to early stage advanced nuclear power designs, particularly those based on alternatives to present, dominant LWR technology.

The sub-objectives of the methodology demonstration are to (i) provide insights for subsequent application and advancement of the methodology for use in new advanced reactor design and (ii) contribute to the base of knowledge for LF-MSR designs. Risk-informed results from application of the methodology to the MSRE that may be useful to stakeholders in the LF-MSR industry include prioritized research topics and design considerations, as well as identification of potentially risk-significant operational occurrences and/or design decisions.

1.3. Key Questions and Dissertation Structure

In this dissertation, a novel methodology is defined and demonstrated that is intended to be useful to begin the process of ES&H risk assessment for early stage advanced reactor designs. Considerations for transitioning early stage hazard analyses to more quantitative risk analysis are also discussed and demonstrated. In this dissertation, the array of best available safety design and analysis practices from the nuclear power generation and other industries was considered. It was then determined how these tools could be used to support a methodology that is systematic, rigorous, and adaptable to advanced reactor concepts. The intended benefits of such a methodology include the following:

- The availability of a technique that is not entrenched in established LWR technology and, therefore, does not inappropriately emphasize (or de-emphasize) hazards that may or may not apply to other technologies.
- Demonstrating a risk assessment approach that can be effectively integrated with early stages of design and advance along with design development.
- Demonstrating the importance of early integration of SiD for new technologies for the purpose of identifying and prioritizing risk-significant design issues and technical uncertainty. This early integration 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, scale testing, etc.).
- The demonstration of an early stage risk assessment technique that could support a more risk-informed and performance-based licensing framework and could be used in an incremental step-wise approach to building the safety case for licensing (thereby reducing schedule and scope uncertainty). Such a methodology could be used to produce the building blocks for a PRA model, for instance.

The methodology defined and demonstrated in this dissertation was developed and refined during its application to a specific LF-MSR design. In particular, this demonstration of how the process can be applied emphasized efforts to document the details of the developed process and provide insights for subsequent application and advancement of the methodology for use in new advanced reactor design. The lessons learned during this application of the developed methodology are discussed in this dissertation to maximize the usefulness of the methodology to potential future users in the fields of advanced reactor design and ES&H risk assessment.

In order to achieve the benefits discussed above, a series of interrelated questions regarding the assessment of risks for advanced reactor designs must be answered. The research presented in this dissertation was conducted in order to answer the following questions:

- What tools commonly used in engineering disciplines (e.g., systems engineering and chemical process engineering) are available to identify and evaluate hazards and risks associated with an advanced nuclear reactor design?
    - What attributes are most important to consider when selecting a specific hazard/risk assessment method?
- How can relevant ES&H hazards for a system in an early stage of design be identified in a technology-inclusive, systematic, and comprehensive fashion?
- What insights can be gained from the use of industry-standard Process Hazards Analysis (PHA) methods applied to early-stage advanced nuclear reactor designs?
- How should ES&H risks be characterized early in the design of advanced nuclear reactors?
    - How can potentially risk-significant occurrences be identified and evaluated?
    - How can the likelihood of failure be estimated, especially for functions, systems, subsystems, and/or components that may not have significant industrial operational experience?
    - How can the consequences of occurrences and/or failures be identified and evaluated?
- What considerations can be made to conduct a hazard analysis in a way that facilitates the transition of the results into industry-standard quantifiable risk analyses?
- What insights can be gained from the results of preliminary quantitative risk assessment of a particular advanced nuclear reactor?
    - What results may be of particular interest to reactor designers?
    - What results may be of particular interest to regulators?

To answer the foregoing questions, this dissertation begins with a general explanation of the developed methodology and then discusses the demonstration of the methodology using the

Molten Salt Reactor Experiment (MSRE), a specific early design and experimental implementation of LF-MSR technology. The demonstration begins with a qualitative hazard evaluation of the portions of the system that contain significant inventories of radioactive material and concludes with an example of a limited scope, semi-quantitative evaluation of design-specific risk-significant scenarios.

A literature review to identify current commercial nuclear power generation industry-standard risk assessment approaches and some proposed frameworks for the safety assessment of advanced reactor designs is presented in Chapter 2, as well as a characterization of prior LF-MSR safety and risk assessment efforts. The developed methodology that is demonstrated in this dissertation is represented graphically in Figure 1; this methodology, the tools that support it, and the interfaces between the various analyses are discussed in Chapter 3. In Chapter 4, the MSRE design is introduced and discussed, and the preparation for, conduct of, and results from PHA studies on portions of the MSRE design are detailed. Chapters 5-7 each provide a demonstration of a different portion of the developed methodology, as indicated in Figure 1. Chapter 5 demonstrates how the results of the inductive MSRE PHA studies can be used in combination with a deductive analysis to systematically identify potential initiators of design-specific, risk-significant scenarios. A detailed analysis of possible component failures is used to develop a model to quantitatively estimate the likelihood of an important initiator related to a unique feature of LF-MSR system designs in Chapter 6, and design considerations for improving reliability are discussed. In Chapter 7, the transition from qualitative PHA results to a semi-quantitative evaluation of the risk-significance associated with selected occurrences and design decisions is demonstrated. Finally, conclusions and overarching observations are presented in Chapter 8.

1.4. Dissertation Scope

The development and demonstration of the methodology in this dissertation is intended to provide useful insights on the initial stages of ES&H risk assessment of early-stage advanced reactors for use by designers. Industry standards, such as [ASME/ANS, 2013], provide requirements for the development of a full scope PRA that would be required to support the licensing process of the NRC; however, few advanced reactor design concepts are at a sufficient maturity to support the development of a PRA that would fully satisfy the requirements for exhaustiveness and fidelity of analysis. In this dissertation, the analysis focuses on the treatment of internal hazards from basic events, such as operational system upsets and both single and common cause failures (CCFs) of systems, structures, and components (SSCs). Limited analysis of hazards related to human errors or external events (such as aircraft crashes or natural phenomena) is presented in this work.[6] Additionally, the hazards present in the system during normal operating conditions are prioritized, consistent with recommendations for the graded approach to development of risk assessments [ASME/ANS, 2013].

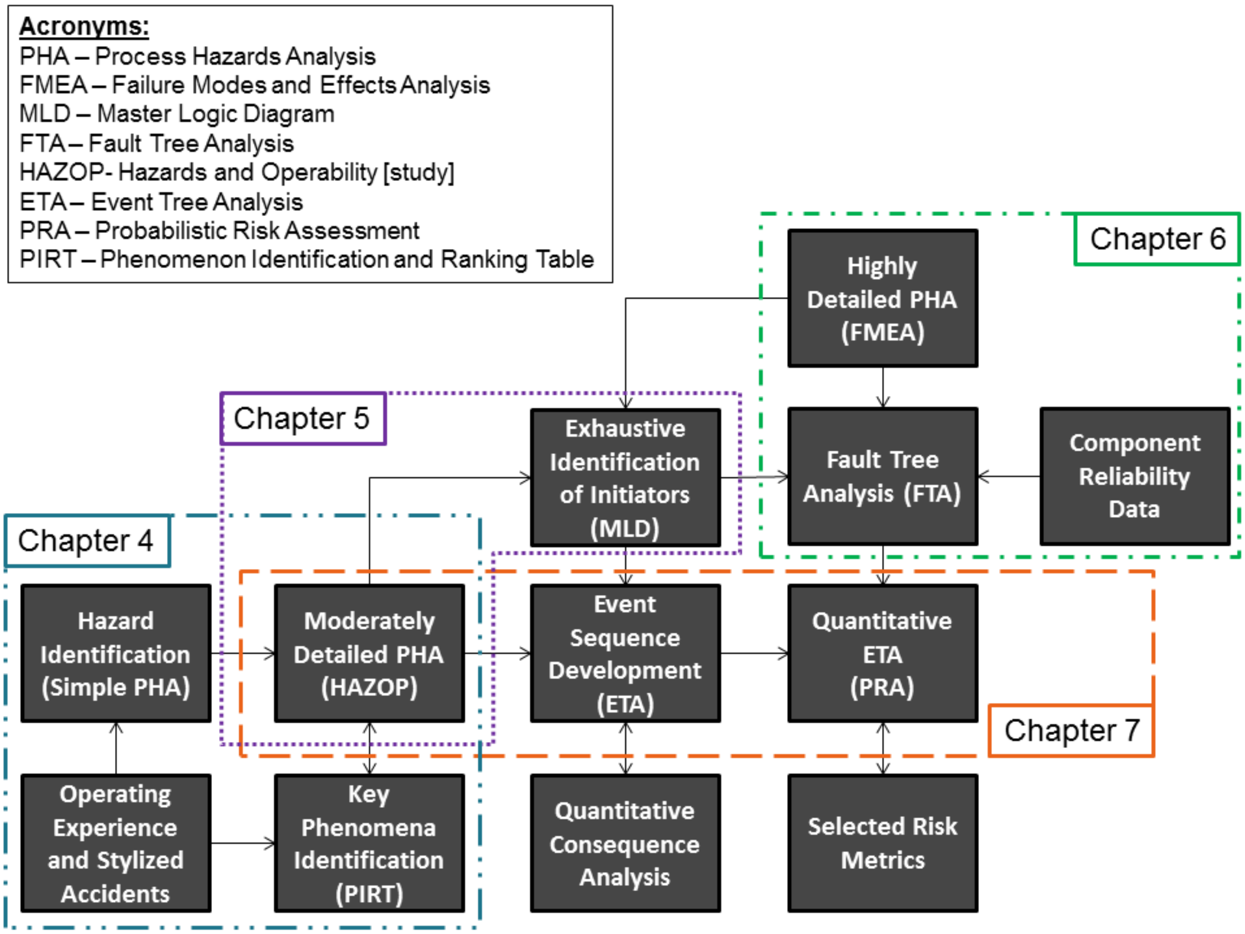


Figure 1: Elements of developed methodology and associated dissertation chapters

The risk assessment performed in this research has focused on the radiological hazards associated with LF-MSRs and is not intended to demonstrate how the risks associated with chemical hazards could be minimized. The LF-MSR designs currently under consideration employ a variety of molten salt chemistries, which have their own distinctive chemical hazards. Therefore, in an effort to make the results generally useful to the LF-MSR community, it was decided to focus this initial work on radiological hazards; however, the systematic risk

[6] Similarly, deliberate acts that are intended to cause harm are outside of the scope of this dissertation since these types of events typically fall under the category of nuclear security [Gupta and Bajramovic, 2017]

assessment methodology developed is equally applicable to identifying and assessing inventories of hazardous chemicals.

An important aspect of risk assessments is the understanding and characterization of uncertainty [Ericson, 2011]. As such, the uncertainty associated with the quantitative estimates of likelihood and/or consequences in this research is quantified when possible. However, due to the relative immaturity of many technical aspects of LF-MSR design and operation, quantification of uncertainty in the models was not always possible, which is typical and representative of early stages of design development for any technology. In these instances, further research activities that would allow for a more thorough treatment of uncertainty will be identified. This treatment is characteristic of early SiD efforts, and effective application of the methodology can lead to prioritization and characterization of research that is necessary to resolve risk-significant technical uncertainty.

As discussed further in Chapter 4, the MSRE design was selected for the demonstration of the ES&H risk assessment methodology because it is associated with perhaps the most detailed collection of LF-MSR design and operational information that is publicly available. However, the MSRE design was a small scale research reactor that was designed and operated as a proof of concept, instead of having the objective to generate electricity. Some of the most notable differences between the MSRE and modern commercial LF-MSR concepts that are currently under development are: the intended power level of the reactor system, an absence of online fuel processing in the MSRE, and the lack of a steam generator and balance-of-plant equipment in the MSRE design. Accordingly, some of the risk insights presented will be specific to the MSRE design, and may not be applicable to all LF-MSR designs currently under development. Further analysis of the specific design differences would be required to fully understand the relevance of the MSRE risk insights discussed in this dissertation for any other given advanced reactor design.

CHAPTER 2, LITERATURE REVIEW OF RELEVANT RISK ASSESSMENT AND SAFETY-IN-DESIGN APPROACHES AND PRIOR EFFORTS

2.1. Industry-Standard Approaches for Quantitative Risk Assessment

Quantitative risk assessment (known in the nuclear and aerospace industries as PRA) is a method designed to help evaluate risk and overall system safety and to identify areas for cost-effective risk reduction [Center for Chemical Process Safety (CCPS), 2010]. Risk quantification uses the risk triplet as a set of three questions that can be used to define risk [NRC, 2016b]. The idea of risk as a triplet was introduced by Stan Kaplan and B. John Garrick to diminish confusion surrounding public decision making involving risk [Kaplan and Garrick, 1981]. These three questions that make up the risk triplet[7] are:

1. What can go wrong?
2. How likely is it?
3. What are the consequences?

A related fourth question that can be asked is, "what are the uncertainties in addressing each of these questions using PRA?" In their paper, Kaplan and Garrick [1981] also establish an explicit manner to incorporate uncertainty into the definition of risk, which allows for an objective comparison of risk in two different systems.

The advantages of PRA in uncovering design and operational weaknesses are due to its logical, systematic, and comprehensive approach. PRA has shown that it is important to examine not only single low-probability and high-consequence mishap events, but also scenarios that can emerge as a result of the occurrence of multiple high-probability and low consequence events [National Aeronautics and Space Administration (NASA), 2011]. In the nuclear power generation industry, PRA is used to support risk-informed decision-making and to enhance assurance that reactor designs will meet the public health safety goals set by the NRC [ASME/ANS, 2013; Keller and Modarres, 2005].

A PRA model presents a set of scenarios, frequencies, and associated consequences, developed in such a way as to inform decisions regarding how resources should be allocated to prevent or mitigate accidents [NASA, 2011]. The quantification of uncertainty is also an integral part of this modeling. Generally speaking, a scenario begins with an initiating event (IE) and then proceeds through one or more pivotal events that ultimately lead to an end state. An IE is typically a

[7] Using this definition, "hazard" can be defined as a doublet, consisting of questions 1 and 3 [Kaplan and Garrick, 1981].

deviation from normal operating conditions that requires a response from systems or operators. The pivotal events include the successes or failures of the subsequent responses to the IE, or possibly the manifestation (or absence) of external conditions. The end state of a given event sequence[8] depends upon the combination of pivotal events and generally represents the kind and/or severity of the consequences that result from the event sequence.

PRA models quantify "risk metrics." A risk metric is a probabilistic performance measure that might appear in a decision model, such as the frequency or probability of consequences of a specific magnitude or expected consequences [NASA, 2011]. Figures of merit such as "system failure probability" can be used as risk metrics, but the phrase "risk metric" normally suggests a higher-level, more consequence oriented, figure of merit. For example, in the commercial nuclear industry, risk for the current generation of LWRs is commonly expressed in terms of two risk metrics: core damage frequency (CDF) and large early release frequency (LERF) [NRC, 2007b]. CDF is defined as the sum of the frequencies of those accidents that result in the uncovering and heat-up of the reactor core, at which point severe fuel damage is anticipated [NRC, 2009]. LERF is defined as the sum of the frequencies of those accidents leading to rapid, unmitigated release of airborne fission products to the environment occurring before the effective implementation of offsite protective actions [NRC, 2009]. While these risk metrics have been demonstrated to be useful surrogates for the NRC's public health safety goals[9] in LWR designs, the maximum quantitative values set for CDF and LERF, and even the consequences associated with the metrics, may not be applicable to advanced non-LWRs [NRC, 2007b].

PRA models in the nuclear industry are typically represented using specific techniques. Event trees model the possible event sequences that can occur after an IE [NRC, 2018c]. Event Tree Analysis (ETA) assumes that an IE occurs, and then represents each success or failure to respond to the IE as a top event. Each event sequence is a path that has an associated end state and probability of incidence, which is determined by the product of the frequencies of the pivotal events (also known as "top events") that the event sequence follows. In PRA, Fault Tree Analysis (FTA) is a method often used to represent IEs and pivotal events and can be used to estimate their frequency of occurrence [NASA, 2011]. FTA is a deductive approach that starts with the top event of concern and decomposes it into more specific events, such as enabling conditions and the failure of mitigating measures, that contribute to the manifestation of the top event until the fundamental fault causes (known as "basic events") are identified [CCPS, 2008; Vesely et al., 1981]. These basic events include equipment failures, human response errors, and

[8] An event sequence is a unique combination of pivotal events after the occurrence of an IE.

[9] The qualitative safety goals and the quantitative objectives used in determining achievement of the safety goals were published by the NRC in 1986 [NRC, 1986].

the like [US DOE, 2004]. By incorporating component reliability data, it is possible to estimate the frequency of the basic events and, using the Boolean logic of the fault tree (FT) structure, the top-level event. With respect to PRA activities, FTs model plant systems in detail so that analysts can identify all possible combinations of component failures that prevent the desired response to the IE. FTA often includes special attention to the evaluation of human errors (through the use of Human Reliability Analysis, HRA) [Swain and Guttmann, 1983] and problems that can cause the failure of more than one component at a time (i.e., CCFs) [NRC, 2016a].

In practice, ETA is typically used to portray progressions of events over time, while FTA best represents the logic corresponding to the failure of complex system. The process of combining ETA with FTA is known as linking, and is displayed conceptually in Figure 2. Although the link shown in Figure 2 is an example of a standard PRA technique where the top event in the FT corresponds to the failure of a specific pivotal event, it is not necessary to develop a FT for every top event in ETA. If applicable probabilistic data is available from another model or testing, this data can be assigned directly to the top events without further modeling [NASA, 2011].

The ASME/ANS Non-LWR PRA Standard [ASME/ANS, 2013] sets forth the requirements for PRA used to support risk-informed decisions for advanced non-LWR nuclear power plants and describes a method for applying these requirements for specific applications. This standard was issued for trial use in December 2013. During the initial trial use period, there were a number of pilot applications, including a variety of VHTR and SFR designs. In September 2017, the ASME/ANS Joint Committee on Nuclear Risk Management approved a plan to extend the trial use period to incorporate insights developed during the pilot 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-inclusive basis. For example, this standard does not use LWR risk metrics (such as CDF or LERF, discussed above) and instead encourages the use of more general metrics, such as: frequency vs. offsite dose, individual risk metrics reflected in the NRC safety goal quantitative health objectives, as well as user defined metrics that may be suitable for specific reactor types (e.g., sodium boiling for SFRs). Overall, the technical requirements in the Non-LWR PRA Standard are approximately 80% common to the requirements in the supporting LWR PRA Standard [ASME/ANS, 2009].

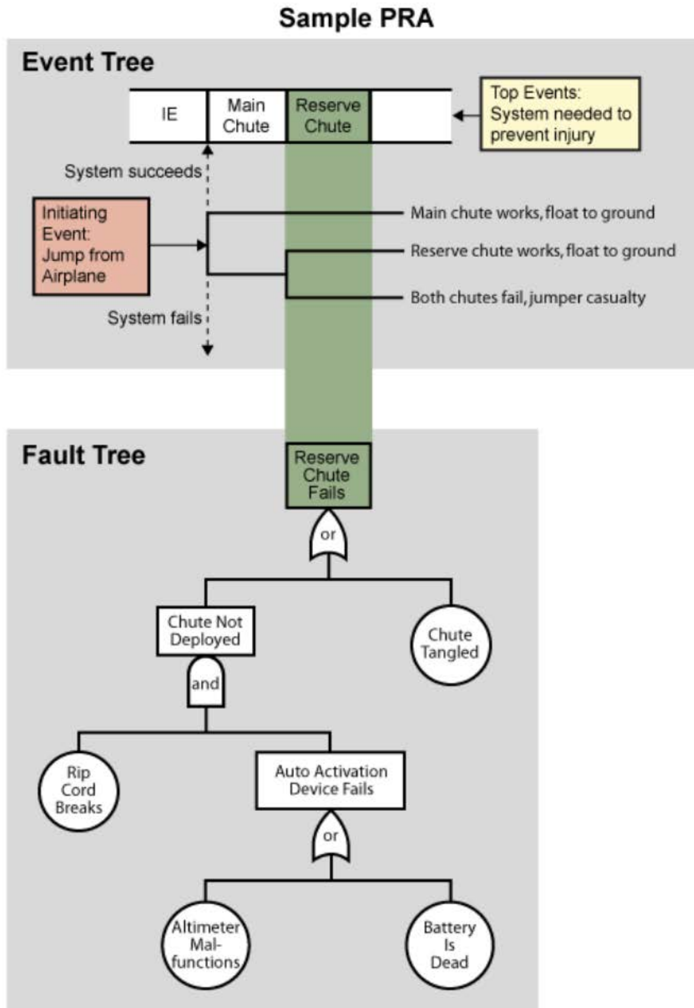


Figure 2: Simple example of a fault tree linked to an event tree [NRC, 2018a]

One objective of the research presented in this dissertation was to demonstrate how the use of system engineering tools and the conduct of PHAs can be used to form the building blocks of a PRA model. The Non-LWR PRA Standard is useful to identify the target set of technical requirements that the PHA studies (as discussed below) and PRA building blocks will need to meet. According to the standard, the early stages of PRA model building will need to define Plant Operating States (POSs), IEs, event sequences, success criteria, and systems analyses. The requirements for these tasks in the standard were helpful to determine which tools can best support the transition from qualitative hazard analyses and more quantifiable risk assessment models. For example, the technical requirements for IE development call for the use of a structured, systematic process to identify IEs that accounts for plant-specific features and specifically mentions Failure Modes and Effects Analysis (FMEA) and Hazard and Operability

(HAZOP) studies as examples of such tools. This recommendation informed the approach for identification of Postulated Initiating Events (PIEs) for the MSRE design presented in Chapter 5.

2.2. PHA and Early Stage Safety Analysis

In the foregoing section, the discussion assumes that a system designer and/or regulator requires, or can benefit from, the eventual construction of a complete PRA model. For a large nuclear reactor intended for commercial operation, the methodology defined and demonstrated in this dissertation is intended to incrementally and iteratively produce elements that will evolve with a maturing design into the building blocks of the final full-facility PRA. However, the approach is also intended to be flexible enough that it can be tailored to support the design of facilities and apparatus, in general; for example, a single test loop that may not contain radioactive material but may contain hazardous chemical materials. Whether or not a full-scope PRA is the desired or necessary endpoint, the present methodology is rooted in a rigorous, systematic identification and analysis of potential hazards. Experience gained during the execution of the research presented herein consistently reinforced the principle that the root of a valid safety analysis is a thorough identification of potential hazards. The efforts presented in this dissertation support that, for nuclear facility safety analysis, a reliable method to achieve sufficiently thorough hazard identification is through the disciplined application of a proven hazard analysis/evaluation tool.

In the chemical process industry, a PHA is defined as "an organized effort to identify and analyze the significance of hazardous situations associated with a process or activity. Specifically, PHA studies are used to pinpoint weaknesses in the design and operations of facilities that could lead to accidental chemical releases, fires, or explosions." [CCPS, 2008] 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 CCPS, an applied research group within the American Institute of Chemical Engineers (AIChE) [CCPS, 2008]. This benchmark technical standard continues to be updated and used widely in industry.

PHA methods are also recognized in the nuclear industry as useful tools to support PRA model development. In NUREG-1513, the NRC describes an approach known as an Integrated Safety Analysis (ISA) and discusses how PHA techniques should be applied to nuclear fuel cycle facilities in order to address the special hazards present at such facilities, as well as their potential for causing criticality incidents and radiological releases, in addition to certain chemical releases [NRC, 2001]. 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 [NRC, 2011]. As previously mentioned, PHAs have also been identified as a suitable method to analyze these same concepts in advanced nuclear reactor designs [ASME/ANS, 2013; GIF, 2011].

PHA techniques have historically been used to support the risk assessments of LWR designs [Shopsky, 1977]. Similarly, for some advanced reactors, including GCRs and SFRs, the technical information provided by a PHA had to be generated in some manner before PRA development [IAEA, 2000; King et al., 1991]. As noted above, PHA techniques (such as HAZOP studies) have been recognized as useful tools for the systematic identification of initiating events for PRA. In addition, PHA studies have been used in the design development process. For example, the HAZOP method was used to help guide the development of control systems and control setpoints for the Pebble Bed Modular Reactor project [Joubert et al., 2009].

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 [Southern Company, 2019a]. Further, as noted in the NRC's draft guidance document DG-1353 [NRC, 2019c], which endorsed the process described in the LMP White Paper:

> *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 of early initiation of these types of analyses 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 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 model for advanced reactor technologies and designs. Therefore, the research presented in this dissertation investigated broader application of PHA methods to support the development of PRA models early in system design, especially for new reactor technologies and design variants that do not have an established history or prior PRA development and application, like LF-MSRs. It is important to note that PHA studies are not performed in isolation from other design and safety analysis efforts, however. This subject is discussed further in Chapter 3 of this dissertation, which illustrates how the developed methodology integrates PHA methods (like HAZOP studies and FMEA) with other established elements of safety analysis, such as mechanistic calculation of accident phenomena and consequences.

PHA techniques are well-exercised in the nuclear power generation, US DOE non-reactor facilities, chemical process, and oil industries. They represent an array of associated tools that can be used depending upon the stage of design, degree of detail, and specific objectives of the analysis being performed. The methodology in this dissertation utilizes PHA methods that are considered suitable for assessment of hazardous processes and facilities in varying stages of design and operations. These methods are explicitly referenced by both the NRC [2013] and US DOE [2013, 2016] for hazard analysis of new and modified nuclear facilities and processes. The six PHA methods explicitly recognized by the CCPS include the following:

- 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)

This collection of techniques, described in detail by guidelines published by the CCPS [2008], provides 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. A more thorough discussion of select PHA methods, important aspects to consider when selecting a PHA method, and potential relationships between various analysis tools is presented in Chapter 3 of this dissertation.

As previously noted, it is entirely possible that not all nuclear systems will require a PRA as comprehensive as envisioned in industry standards. Other aspects that should be considered when selecting an appropriate hazard or risk assessment approach include the type and amount of hazardous material present in a given design. For example, NRC non-reactor licensees who plan to possess special nuclear material are compelled to meet the safety assessment requirements set out in 10 CFR 70. One of these requirements is that the licensees are required to perform an ISA on the facility, part of which involves using existing PHA methods to make qualitative or semi-quantitative estimates of risk for the facilities.

The SHINE Medical Radioisotope Production Facility is a non-power reactor being built for the production of Mo-99 for medical use. The SHINE facility is licensed by the NRC and performed an ISA as part of its safety analysis [SHINE Medical Technologies Inc., 2015]. In order to identify potential design basis accidents, the SHINE facility applied the HAZOP and preliminary design hazard analysis (PrHA) methods to identify and document potential hazards, initiating events, and controls for the preliminary design of the radioisotope production facility.

Similarly, the Northwest Medical Isotopes Radioisotope Production Facility is a radioisotope separation and processing facility for the production of Mo-99 which performed an ISA as part of its licensing under NRC [Northwest Medical Isotopes LLC, 2017]. In its ISA, the Northwest Medical Isotopes Radioisotope Production Facility used a combination of PHA methods (What-If, HAZOP, and FMEA) and traditional nuclear accident analysis methods (ETA and FTA) as part of its accident analysis methodology. The facility initially used PHA methods to identify events and qualitatively evaluate the risk for such events. FTA and ETA were then used to demonstrate that the items relied on for safety would be capable of reducing the risk of each event to an acceptable level.

2.3. Safety-in-Design and Risk-Informed Frameworks for Safety Assessment

The concept of incorporating SiD from the earliest stages of the design process of a nuclear facility was pioneered by the US DOE. DOE-STD-1189-2016 [US DOE, 2016] is a useful reference that provides requirements and guidance for the integration of safety into the design process for high hazard nuclear facilities of the US 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 between these functions 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. Examples of SiD 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.

Regarding hazard assessment, [US DOE, 2016] states that a comprehensive 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). Most notably, the standard provides a "graded approach" process to ensure that the level of analysis, documentation and actions used to comply with a requirement are 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.

In the U.S. commercial nuclear power industry, a broadly applicable, NRC-accepted, risk-informed, performance-based (RIPB) licensing framework has long been desired. Incremental advances, accelerated recently by increased interest in licensing and building advanced nuclear reactors and congressional interest, have resulted in the commercial nuclear generation industry viewing now as an opportune time to pursue NRC endorsement of a RIPB framework. Accordingly, the NRC has been engaged by the LMP, which is a nuclear industry project being led by Southern Company, coordinated by the Nuclear Energy Institute (NEI), and cost-shared by the US DOE. The LMP's objective is to develop technology-inclusive, RIPB safety analysis guidance for licensing non-LWRs to be considered by the NRC for possible endorsement. For example, as part of the LMP, the NRC staff indicated its intention to take an active role in the development of the final version of the Non-LWR PRA Standard [ASME/ANS, 2013], with a view towards endorsing it for use in licensing future advanced reactors. The intended applications envisioned for PRA models developed under this standard and LMP guidance include selection of licensing basis events (LBEs), safety classification and development of performance requirements for SSCs, and RIPB evaluation of defense-in-depth (DID).

NRC staff has reviewed four LMP white papers[10] and, after sending feedback to the LMP as well as a series of public meetings, industry issued its consolidated LMP document, as NEI 18-04, on September 28, 2018.[11] This report outlines an approach for use by reactor developers to select LBEs, classify SSCs, determine special treatments and programmatic controls, and assess the adequacy of a design in terms of providing layers of DID [NEI, 2019]. The NRC staff and industry representatives briefed the Advisory Committee on Reactor Safeguards (ACRS) Future Plant Subcommittee on the LMP twice in 2018, and the ACRS full committee in 2019. The NRC then published draft regulatory guide DG-1353, "Guidance for a Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of

[10] The LMP White Papers were published by Southern Company and covered the following topics: development of a PRA model [2019a]; evaluation of Defense-in-Depth adequacy [2019b]; safety classification of SSCs [2019c]; and selection and evaluation of Licensing Basis Events [2019d].
[11] A revision to NEI 18-04 was submitted to the NRC in August 2019; this revision is the NEI report referenced in this dissertation (i.e., [NEI, 2019]).

Applications for Licenses, Certifications, and Approvals for Non-Light Water Reactors," in the Federal Register on May 3, 2019, for public comment [NRC, 2019c]. This proposed new regulatory guide endorses, with clarifications, the principles and methodology in NEI 18-04 as one acceptable method for determining the appropriate scope and level of detail of the safety case that will be used in applications for licenses, certifications, and approvals for advanced reactors, including non-LWRs. The draft guide and the methodology described in NEI 18-04 provide a general approach for identifying an appropriate scope and depth of safety basis information to be provided in applications to the NRC for advanced reactors.

At a high level, the discussion in [NEI, 2019] describes a process to inform the safety design approach for a reactor design, and this safety design approach is then applied to demonstrate compliance with the regulations and requirements applicable to a reactor design. The relevant questions stemming from existing requirements and their implementation guidance, which are directly related to the methodology developed and demonstrated in this dissertation, are as follows:

- What are the plant IEs and event sequences that are associated with the design and site?
- How do the SSCs in the proposed design respond to IEs and event sequences?
- Is the philosophy of DID adequately reflected in the design and operation of the facility?

Various components of LMP process have been employed in previous US DOE and industry initiatives. For examples, demonstration projects were performed with X-energy [Waites et al., 2018] and General Electric Hitachi [Hicks et al., 2018], which were the first opportunities to implement the process in the context of the draft LMP Guidance Document. The efforts in this dissertation applied parts of the LMP approach to inventories of radioactive material in an LF-MSR design. Thus, the results presented herein help support the idea that the LMP approach outlined in NEI 18-04 can be used to produce RIPB ES&H risk design insights for an LF-MSR at an early, pre-operational stage of design.[12] Analyzing the MSRE at this early level of design maturity allowed for the investigation of how a designer might use tools such as PHA studies to initiate the first iteration of the LMP process.

An international approach that also attempts to encourage SiD while simultaneously supporting the development of an RIPB safety assessment is the Integrated Safety Assessment Methodology (ISAM), which is described in a report by the GIF Risk and Safety Working Group (RSWG) [2011]. The ISAM is intended to support achievement of safety that is “built-in,” rather

[12] i.e., a Technology Readiness Level (TRL) of ~4-5. For more information on the concept of TRLs, see [US DOE, 2011] and [EPRI, 2017].

than added on late in the design process, by influencing the direction of the concept and design development from its earliest stages (similar to the intent in [US DOE, 2016]). 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 [GIF, 2014a], 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.

Overall, 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 relevant to the work presented in this dissertation include:

- The ISAM is intended to be an "iterative design process" that ensures "operability, availability, and safety" of the system; however, it is not readily evident how operability and availability are addressed in the ISAM.
- The GIF reports on ISAM contain sections that summarize the inputs and outputs from each of the individual tools. Although coverage is uneven from topic to topic (e.g., Qualitative Safety Features Review is only covered briefly), these sections do provide useful guidance on the desired results from early stage safety analyses and the potential inputs to an eventual PRA model.
- The LMP White Paper on PRA development [Southern Company, 2019a] notes that the ISAM approach is generally consistent with the approach to PRA in the LMP report.

2.4. Prior Safety and Risk Assessments of Liquid-Fueled Molten Salt Reactors

2.4.1. Original Safety Basis for the MSRE

As discussed in Section 2.2, there exists history of PRA development for some advanced non-LWR technologies, such as VHTRs and SFRs. Meanwhile, there is little or no legacy PRA work to build upon for the evaluation of LF-MSRs. The only LF-MSR focused on civilian applications[13] that has been licensed and operated is the MSRE[14] [Singh et al., 2017]. Because authorization to construct and operate the MSRE was issued by the Atomic Energy Commission (AEC)[15] in the 1960s, a PRA model was not required and thus was not developed for the MSRE. In fact, PRA was not brought to the forefront of nuclear engineering thought until the late 1960s, and the first project to develop a PRA model for a nuclear plant was not initiated until the 1970s [Keller and Modarres, 2005].

In its early years, the AEC licensed a wide variety of non-LWRs, mostly using customized safety reviews based on engineering experience and expert judgement. Since the 1970s, no commercial non-LWRs have been licensed. In the early days, the safety assessment for reactors began with a Preliminary Hazards Analysis (PrHA). This PrHA formed the basis for a reactor design's safety analysis and was reviewed by the AEC Regulatory Division for commercial licensing; however, experimental and test reactors, such as the MSRE, followed a less prescriptive pathway [Flanagan, 2017]. The PrHA and Safety Analysis Report (SAR) were reviewed by the ACRS. In the SAR, the applicant proposed a postulated Maximum Credible[16] Accident (MCA), which was believed to bound all other accident consequences and was used to determine offsite radiological dose consequences. This MCA was used in a manner similar to what would later be called a "design basis accident"[17] in the safety analysis and system design processes.

Regarding the safety assessment of experimental, research, and test reactors at Oak Ridge National Laboratory (ORNL), such as the MSRE, each reactor design was reviewed by an independent group of experts from various disciplines within ORNL reporting to the Laboratory Director, known as the Reactor Operations Review Committee (RORC). Reviews began at the conceptual design stage and continued through construction and operation. The PrHA and safety analysis documentation were prepared by the ORNL project team and reviewed by the RORC. ORNL also usually set up an independent review committee comprised of outside consultants. Results of the ORNL review of the PrHA and SAR, along with the actual documents, were then presented to the AEC Oak Ridge Operations (ORO) office for review and comment.

---

[13] The Aircraft Reactor Experiment (ARE) was operated in November 1954 at ORNL with a $NaF\text{-}ZrF_4\text{-}UF_4$ fuel for a total thermal power production of 96 MW-hr; however, this sodium cooled reactor was designed to investigate aircraft nuclear propulsion rather than civilian power production [Bettis et al., 1957]. Appendix A contains further discussion of the ARE.

[14] The MSRE design is discussed in detail in Chapter 4 of this dissertation.

[15] The AEC managed the development, use, and control of atomic (nuclear) energy for military and civilian applications from 1946 until it was abolished in 1974 and succeeded by the NRC and the Energy Research and Development Administration (now part of the US DOE) [NRC 2019b].

[16] In this context, "credible" means useful as a bounding analysis, but not necessarily mechanistic.

[17] i.e., accidents that form the design basis for engineered safety features

The ORO Review results, along with the ORNL documents, were sent to the program office at AEC Headquarters. In the case of the MSRE, the Reactor Technology Development Office was the program office, and AEC Headquarters was the authoring organization. The PrHA and SAR were reviewed by the program office and the ACRS; if these analyses were approved, these groups made a recommendation to the AEC, and the AEC then could grant a construction permit for the reactor. The same process was then repeated for the MSRE operating license. Finally, an Operational Readiness Review was conducted by ORO and the project office at AEC headquarters prior to startup.

The PrHA and the SAR for the MSRE were based on previous ORNL experience with fluid-fueled reactors, more specifically the Aircraft Nuclear Reactor Experiment and two aqueous homogeneous reactor experiments [Rosenthal, 2010]. A more thorough discussion of fluid-fueled reactors is provided in Appendix A of this dissertation. MSRE PrHA was first published in 1960 and reissued in 1962 [Beall, 1962], with some supporting safety analyses published separately [Haubenreich and Engel, 1962].

The MSRE PrHA was a barrier analysis [Flanagan, 2017], since the safety approach taken by the MSRE designers was to surround each component of the system that contained fuel or fission products by at least 2 barriers. In the PrHA, events were identified that could partially damage a single barrier but produce no release if the second barrier remained undamaged. Events that might damage two barriers were considered to be very unlikely to occur but were thought to potentially contribute to off-site consequences (today these might be considered Beyond Design Basis Events, BDBEs). The identified events were then analyzed as part of the safety analysis to provide detailed information regarding impacts on the radiological material in the fuel salt and the challenges to the structures containing it.

In the MSRE SAR [Beall et al., 1964], the following nuclear reactivity events were analyzed using analog computers and an early digital computer code[18]:

- Fuel pump failure
- Cold fuel slug accident
- Fuel salt filling accident
- Loss of structural graphite from the core (i.e., filling the empty space with fuel salt)
- Fuel anomalies (i.e., precipitated fuel circulating in core or non-mixed fuel lumps circulating in core)

[18] i.e., MURGATROYD [Nestor Jr., 1962a], which was later renamed ZORCH [Nestor Jr., 1962b]

- Uncontrolled control rod withdrawal
- Ramp and step additions of reactivity

The results indicated that the consequences associated with these events were benign [Beall et al., 1964]. Some internal damage to structures from high temperatures could result from three events: extreme cold slug accidents, premature criticality during refueling, and uncontrolled withdrawal of control rods. However, these events could only result from compound failure of protective devices. In each case, the analysts concluded that there existed effective corrective actions, independent of the credited safety function, such that damage was considered to be unlikely.

In addition to reactivity events, the final SAR of the MSRE investigated the following scenarios:

- Loss of flow
- Loss of heat sink
- Loss of decay heat removal
- Criticality of fuel salt in drain tanks
- Freeze valve and flange structural failures
- Excessive system wall temperatures
- Corrosion
- Salt spillage
- Beryllium release from a leak

The SAR [Beall et al., 1964] describes the most probable accident for the MSRE as a small leak of fuel salt into the secondary container.[19] In this scenario, radiation monitors were designed to shut down the reactor and alarm the operators. Airborne activity that had been released into the cell could then be pumped from secondary containment and through charcoal beds (to allow for decay of volatile radionuclides) and filters (to retain radioactive particulates) before being released up the stack. The calculations in the SAR indicated that the dose consequences associated with this scenario did not exceed maximum permissible dose on-site.

The Maximum Credible Accident (MCA) for the MSRE was considered to be either a break in the 3.8-cm (1.5-in.) fuel salt drain line or a break in a 13-cm (5-in) fuel salt circulation line. The calculations in the SAR assumed that the entire inventory of molten fuel salt (i.e., 4536 kg or 10,000 lbs) would be released to the secondary containment vessel in less than 370 sec. The

[19] For the fuel salt loop, the secondary container was the reactor cell, which was a seal-welded, carbon steel containment vessel [Robertson, 1965].

calculations also assumed a simultaneous spillage of water from installed cooling systems into the secondary containment to maximize pressure in the seal-welded cell (calculated to be 758 kPag or 110 psig without venting). The rupture disk in the vapor condensing system was designed to open at 138 kPag (20 psig); accordingly, the calculations estimated the maximum pressure in the reactor cell after venting to the vapor condensing system would be 269 kPag (39 psig). This internal pressure was not considered to be high enough to cause the cell to fail.

Assuming a 1% leakage of the contents from the cell at 269 kPag (39 psig), the dose offsite (i.e., 3000 m from the MSRE building) under the worst meteorological conditions was calculated to be approximately 0.06 Sv (6 rem) from iodine [Beall et al., 1964].[20] Due to the relatively immature status of the technical knowledge surrounding LF-MSRs, a thoroughly vetted source term calculation does not exist for the purposes of estimating dose consequences associated with the material in the MSRE. The bases for the assumptions in the MSRE SAR calculation have not been confirmed, and, as will be discussed more thoroughly in Chapter 7, quantitative LF-MSR dose estimates currently contain significant and unquantifiable uncertainty. A reactor developer would likely use such early results to identify and prioritize technical uncertainties that need to be the subject of later tests and/or experiments before proceeding with more rigorous analysis.

2.4.2. Recent LF-MSR Safety Assessment Efforts

Several years after the MSRE concluded operation in 1969, the Molten Salt Reactor Program (MSRP) at ORNL was terminated by the AEC [LeBlanc, 2010]. Between the early 1970s and the early 2000s, very little funding worldwide was directed towards R&D of LF-MSR technology. However, the selection of MSRs as one of the six Generation IV reactors by GIF in 2002 was responsible for an increased interest in LF-MSR designs [LeBlanc, 2010]. Although many LF-MSR design concepts are still in the early stages of the design process, a handful of preliminary efforts to evaluate risk and safety associated with LF-MSR designs have been initiated.

A few high-level studies have made attempts to qualitatively evaluate the safety of the LF-MSR concept, without focusing on a single design variant [Elsheikh, 2013; Mohsin et al., 2019]. In general, these studies view LF-MSRs very favorably, making statements that "MSRs are safer and more stable" than current LWR designs [Elsheikh, 2013] or that the "safety concept of MSRs practically eliminates the possibility of [radioactive] release" [Mohsin et al., 2019]. However,

---

[20] The SAR states that the calculations assumed that 10% of the total inventory of iodine, 10% of the particulates, and 100% of the noble gases were released. Further, for the SAR calculations, Beall et al. [1964] assumed that 50% of the iodine released subsequently plated out on secondary container surfaces and stated, "based on experiments in which the solubility of the fuel salt in water was measured, much less iodine is expected to be released."

these conclusions seem to be predicated upon the idea that the only inventory of radioactive material that should be considered as possibly contributing to the ES&H risk profile of an LF-MSR is the radioactive material dissolved within the fuel salt. For example, the only DBAs considered by Elsheikh [2013] are a power increase accident (or reactivity initiated accident), a fuel salt flow decrease accident, or a fuel salt leak accident. Further, Elsheikh [2013] notes that the "chance of radiation exposure by gaseous fission products is smaller due to their continuous removal from fuel salt, and the danger of piping rupture is also very low." Similarly, Mohsin et al., [2019] states that there "is still a potential for the fission products to leak out from places other than the [fuel salt] loop but designing against such release is easier because of lower driving forces."

As will be discussed in Chapters 4, 5, and 7 of this dissertation, the MSRE design had multiple unique radioactive material inventories that were of different forms and compositions and were intended to be contained by a variety of barriers. Furthermore, among modern LF-MSR design concepts, there is no truly "representative" design. Different developers have made a number of different design decisions that affect the hazard and risk profiles of each LF-MSR concept, including the chemical composition of the fuel salt, the neutron spectrum of the core, and the method of fission product separation [Holcomb, 2017]. Each design decision affects what can go wrong, the associated consequences, and how likely it is. For this reason, a risk-informed analysis of the hazards inherent to a specific reactor design seems more appropriate than blanket statements regarding the overall safety of the LF-MSR concept based on generic assumptions.

A recent workshop was held at ORNL with the objective of identifying PIEs for a generic LF-MSR design, with participants including representatives from 7 prospective reactor vendors, nuclear industry organizations, US and Canadian regulators, US and Canadian national laboratories, and the academic community [Holcomb et al., 2019]. To facilitate a brainstorming exercise, summary high-level design information for several subsystems, taken from the MSRE and the concepts for both the Molten Salt Demonstration Reactor (MSDR) and the Molten Salt Breeder Reactor (MSBR)[21], was briefly presented.

For each of the subsystems, the participants of the workshop were asked to brainstorm "what could go wrong?" and the answers were recorded [Holcomb et al., 2019]. The structure of the study to brainstorm PIEs that could pertain to inventories of radioactive material other than the

[21] Conceptual designs for the MSDR and the MSBR were developed at ORNL before the termination of the Molten Salt Reactor Program in the mid-1970s; however, the publicly available design information for these plants was not particularly detailed, especially for so-called "auxiliary" and support systems, including systems intended to handle significant volumes of radioactive gases (e.g., off-gas systems).

fuel salt represents an improvement in comprehensiveness over other studies that focus mostly on the fuel salt system; however, the 140 PIEs listed in the report were not organized in any fashion. Furthermore, the brainstorming evaluation at the workshop was not as systematic as other industry-standard approaches (such as a HAZOP study), and it is noted by Holcomb et al. [2019] that the list of PIEs "is intended to support the IE identification process." As such, the list of PIEs in the report represents the results of an inductive analysis of PIEs that can be used to supplement design-specific deductive and inductive studies.

An example of a recent study focusing on a specific modern commercial LF-MSR design is documented by Geraci [2017]. The objective of the paper was to identify key PIEs for Flibe Energy's Liquid Fluoride Thorium Reactor (LFTR) conceptual design. A list of PIEs was compiled by surveying generic lists of LWR PIEs [IAEA, 1993], NRC reports [Eide et al., 2007; Mackowiak et al., 1985; NRC, 1990; Poloski et al., 1999], and Master Logic Diagrams (MLDs) being developed for FHRs [Mei et al., 2014; Zuo et al., 2016], and then identifying PIEs from these sources that related to the hazards identified by the What-If analysis of the LFTR design conducted by Vanderbilt for the Electric Power Research Institute (EPRI) [2015]. Table 2 lists the 18 PIEs that were identified, with 10 PIEs determined to be similar to those typically considered for LWRs and 8 determined to be "unique to the LFTR design." However, the analysis by Geraci does not explicitly mention hazards or PIEs that could potentially result in release of radioactive material from the off-gas system (OGS); further, the PIEs identified in the thesis that relate to radioactive material inventories other than the fuel salt are either: generically defined (e.g., operator error), related to external events (e.g., seismic events), or are internal events that potentially impact many plant functions simultaneously (e.g., fire within the plant or loss of offsite power without scram). Because the only LF-MSR-specific reference surveyed for this PIE analysis was a What-If analysis, which is not a comprehensive PHA method [CCPS, 2008], a more comprehensive study of hazards and potential initiators is likely warranted to provide confidence that important PIEs were not missed.

Perhaps the most systematic and comprehensive effort to identify and evaluate PIEs for a specific LF-MSR design to-date is the analysis published by Gèrardin et al. [2019]. The authors set out to develop an initial list of PIEs for normal operating conditions of the Molten Salt Fast Reactor (MSFR) conceptual design, which is being developed in the European Union, through use of the MLD approach and Functional FMEA (FFMEA) [Burge, 2010]. The list of PIEs is intended to be used as input for successive deterministic safety analyses. The results of the functional analysis on the MSFR were also used to consider open questions about the design, procedures, operating conditions, and important phenomena.

Table 2: LFTR PIEs identified by Geraci [2017]

PIEs shared in common with LWRs
1. Operator Error
2. Rod control interlock failure
3. Instrumentation and control circuitry or protective logic failure
4. Seismic events
5. Fire within the plant
6. Loss of instrument air
7. Loss of AC or DC control power
8. Continuous rod withdrawal casualty
9. Core geometry failure
10. Loss of off-site power without Scram
PIEs determined to be unique to the LFTR design
11. Improper handling of graphite tubes during maintenance or inspection
12. Chemical processing plant failure
13. Loss of fuel salt flow
14. Loss of coolant salt flow
15. Fuel salt channel blockage
16. Drain tank cooling mechanism design deficiency
17. Freeze valve design deficiency
18. CO_2 / Intermediate Coolant Salt Heat Exchanger Failure

Combining the results of both analyses, the 13 "families" of PIEs displayed in Table 3 were identified by grouping together PIEs that resulted in similar consequences, and at least one "representative event" was identified for each family of PIEs. The representative PIEs were assumed to envelope all similar PIEs in terms of radiological consequences. Based on the list of PIEs, Gèrardin et al. [2019] concluded that PIEs were identified for the MSFR that had not previously been identified for LWRs, such as "loss of fuel flow." The next step in the MSFR safety assessment work will be to investigate the Defense-in-Depth (DID) of the MSFR design [Uggenti et al., 2017].

Regarding the PIE identification approach, Gèrardin et al. [2019] concluded that, in general, the results of the MLD and FFMEA methods agreed well, but some events were identified by only one method and not the other. In particular, the inductive method of the FFMEA was determined to have provided more detail on the systems or procedures used for detection, prevention, and mitigation, while the MLD offers a more convenient graphical tool to present hazards and understand logical connections between different hazards [Gèrardin et al., 2019]. These conclusions support the idea that the combination of a deductive analysis (such as MLD) combined with an inductive analysis (such as an FFMEA or a HAZOP study) is an effective way to systematically and comprehensively identify PIEs for a design that does not benefit from extensive prior safety assessment information or operating experience. However, the MSFR MLD only considers PIEs for normal operations. As will be discussed in Chapter 5 of this dissertation, it is possible that for some LF-MSR designs, the composition and physical location of the major inventories of radioactive material will vary for different Plant Operating States (POSs). Accordingly, the challenges to the barriers that are intended to prevent the release of radioactive material (and the safety functions protecting the barriers) may need to be evaluated separately for each inventory and for each POS to ensure a comprehensive enumeration of PIEs for LF-MSR designs.

Table 3: MSFR PIE families identified by Gèrardin et al. [2019]

F1: Reactivity insertion
F2: Loss of fuel flow
F3: Increase of heat extraction/over-cooling
F4: Decrease of heat extraction
F5: Loss of fuel circuit tightness
F6: Loss of fuel composition/chemistry control
F7: Fuel circuit structures over-heating
F8: Loss of cooling of other systems containing radioactive materials
F9: Loss of containment of radioactive materials in other systems
F10: Mechanical degradation of the fuel circuit
F11: Loss of pressure control in fuel circuit
F12: Conversion circuit leak
F13: Loss of electric power supply

The most extensive and quantitative evaluation of risk associated with a specific LF-MSR design was conducted by Pyron [2016]. In this thesis, Pyron uses the RIPB process developed by the Next Generation Nuclear Plant (NGNP) Project[22] to identify and evaluate LBEs for Thorium Tech Solution Inc.'s FUJI-233Um conceptual design [IAEA, 2007]. As a part of the safety assessment of the FUJI-U233m reactor, Pyron [2016] documented the following work:

- Identification of IEs using the MLD method
- Development of event sequence diagrams and analysis of parameter evolutions and potential consequences
- Construction of an LF-MSR-specific database for component failure rates

[22] The LBE selection approach described by the LMP [NEI, 2019; Southern Company, 2019b] and endorsed by the NRC [2019c] builds upon the LBE selection approach developed by the NGNP Project [Idaho National Laboratory (INL), 2010] by incorporating lessons learned from NRC and ACRS reviews of NGNP approach and by considering its application in a technology-inclusive manner.

- Construction of FTs, event trees (ETs), and quantification of a preliminary PRA model
- Identification of safety weaknesses; and
- Identification of Safety-Related SSCs (SR-SSCs) and DBAs

The PIEs identified for the FUJI-U233m design are displayed in Table 4. The PIEs resulting from the MLD analysis were compared by Pyron to a list of FHR PIEs [Allen et al., 2013] and typical examples of events analyzed in LWR PRAs [NRC, 2007a; Schweizerische Eidgenossenschaft, 2009], and then grouped into 8 categories. All of the categories but one (i.e., the "MSR-specific category") were derived based upon the categories of Anticipated Operational Occurrences (AOOs) and postulated accidents recommended in the NRC Standard Review Plan for LWRs [NRC, 2007a].

Although Pyron's MLD includes the consideration of PIEs for the release of radioactive material inventories other than those related to the inventory of fuel salt, there is a disparity between the resolution of the PIE decomposition that could lead to the release of fuel salt and that of PIEs that could lead to the release of material from other inventories. For example, "release of core material/core damage" is decomposed into 7 different hazards that could result in a transport of fuel salt through the first barrier to its release, while "off-gas system failure" is not decomposed any further in the MLD. Therefore, as demonstrated in Chapters 4 and 5 of this dissertation, use of an inductive analysis tool, such as a HAZOP study, can be used to increase the understanding of functional and/or subsystem failures that could contribute to a release of radioactive material from an LF-MSR OGS.

Out of the 24 PIEs in Table 4 that were modeled using quantitative ETA and/or FTA, only one (i.e., "off-gas system failure") deals with an inventory of radioactive material other than the fuel salt. Pyron [2016] estimates the probability of a leak from the OGS using a FT model of low fidelity, comprised only of basic events corresponding to external leakage from the individual OGS components. It is possible that this approach overlooks possible failures of SSCs that perform functions that prevent challenges to barriers intended to contain the volatile radioactive material in the OGS. Further, Pyron [2016] notes that "it is suggested to study the off-gas system as another system apart from the reactor." As demonstrated in Chapters 4, 5, and 7 of this dissertation, PHA studies can be used to develop comprehensive ETA and FTA models to evaluate the ES&H risks associated with a wide variety of radioactive material inventories.

Table 4: FUJI 233-Um PIEs identified by Pyron [2016]
(PIEs that are analyzed using quantitative FTA and/or ETA are in *italics*)

Increase in heat removal by the secondary system
Secondary salt flow increase
Cooling flow increase (feedwater system malfunction and steam pressure regulator system failure)
Inadvertent opening of a steam generator relief or safety valve
Decrease in heat removal by the secondary system
One / Two loop(s) secondary pump trip
Turbine trip
Inadvertent closure of Main Steam Isolation Valve (MSIV) (+CCF MSIVs)
Loss of condenser vacuum
Total loss of feedwater
Partial loss of feedwater
Feedwater pipe rupture
Secondary pipe leak
Steam generator tube rupture
Decrease in primary loop system flowrate
One / Two loop(s) primary pump trip
Loss Of Offsite Power (LOOP)
Reactivity and power distribution anomalies
Graphite loss
Control rod(s) drop
Malfunction in He bubbles injection
Cold loop startup
Salt control failure: excessive fuel addition
Salt control failure: cold fuel salt injection
Oxygen / Moisture ingress: fissile precipitation
Off-gas system plugged (loss of removal of poisons - e.g., xenon)
Fissile penetration to graphite and release
Increase in primary salt inventory
Salt control failure
Heat eXchanger Tube Rupture (HXTR)
Decrease in primary salt inventory
Freeze valve failure
Leak from reactor vessel
Leak from the primary circuit
Radioactive release from a subsystem or component
Off-gas system failure
Decay container leakage
Fresh fuel container leakage
Drain tank leakage
MSR-specific category
Graphite fire
Malfunction of the containment heating system

Pyron's approach for developing an LF-MSR-specific database of IE frequencies and component failure rates was to collect these rates for IEs and components that were judged to be sufficiently similar in other reactor types. Some rates, such as "loss of feedwater flow" or "loss of condenser vacuum," are likely to be fairly similar across many different reactor types due to the relative maturity of BOP system design and operation. However, for SSCs that are unique to LF-MSRs, assuming that their failure rates can be modeled using SSCs from other reactor types may result in a less accurate estimate of failure likelihood. For example, in the absence of any failure rate data specifically available for a freeze valve system, Pyron's analysis simply assumed that the failure rate of a freeze valve could be approximated using the failure rate of either a generic solenoid valve or the failure rate of a solenoid valve used in an SFR for the control of liquid sodium. However, it was concluded by Pyron [2016] that a major uncertainty in the presented analysis of LBEs is this lack of failure rate data for an MSR-specific freeze valve system and that "a better evaluation of the freeze valve reliability would result in a lower value [of uncertainty]." Chapter 6 of this dissertation demonstrates how one can use PHA studies to develop a more design-specific estimate of a failure rate for unique SSCs or functions that do not yet have a vast amount of operating experience.

Ultimately, Pyron [2016] used the NGNP Project's RIPB approach to identify a list of SR-SSCs for the design, which includes the auxiliary OGS, the OGS cell, and the drain tank cooling system. Pyron's other conclusions that are most relevant to this dissertation are as follows:

- An RIPB approach to evaluating environmental and nuclear safety risks associated with design lends itself to a thorough identification of risk-significant occurrences and design decisions.
- In an LF-MSR, radioactive material inventories other than the fuel salt (such as off-gas) should be evaluated for its contribution to a design's risk profile.
- Development of LF-MSR-specific SSC failure rates would reduce uncertainty associated with quantitative models of risk for LF-MSR designs.
- Due to the fundamental differences between LF-MSRs and other reactor types, it is possible that hazards and phenomena that are not considered for other reactor designs need to be evaluated for their significance in LF-MSR designs before they can be dismissed.

A more focused quantitative analysis was performed by Qun et al. [2017] to evaluate the significance of equipment reliability and human error in accident sequences affecting the liquid-fueled Thorium Molten Salt Reactor (TMSR-LF), being developed in China. In this study, FTA was used to estimate the probability of a failure of the special core fuel salt release system (CFSRS) to discharge fuel salt to drain tanks when demanded. The analysis was performed to identify possible design shortcomings of the system and help uncover possible solutions. The CFSRS model included two freeze valves, one valve in each line from the core vessel to each of two drain tanks. The failure rates for the components comprising the freeze valve system were then retrieved from LWR-specific component reliability databases, but no quantitative failure probability for the freeze valve function is provided. Qun et al. [2017] concluded that human error is the dominant contributor to failure of the CFSRS, and that addition of a redundant pipe heating subsystem might improve reliability of the subsystem. However, relevant to the discussion in Chapter 6 of this dissertation, Qun et al. [2017] also mention that more accurate results would be possible if LF-MSR-specific failure rates were available for certain SSCs, including freeze valves.

A limited-scope quantitative evaluation of risk in the MSRE was conducted by Chisholm et al. [2018c]. The objective of the study was to assess the applicability of the RIPB process for identifying LBEs described by the LMP [Southern Company, 2019d] to LF-MSR designs. A preliminary search for MSRE PIEs was conducted by surveying the scenarios discussed in the MSRE PrHA [Beall, 1962] and SAR [Beall et al., 1964], and quantitative ETA and FTA was used to estimate the probability of possible event sequences resulting from 3 different PIEs. The analysis identified that a post-construction modification actually increased the risk of a release of radioactive material from the MSRE system. More importantly, Chisholm et al. [2018c] identify that it was necessary to make significant (and conservative) simplifying assumptions in order to evaluate the LBEs identified using the frequency-consequence criteria suggested by the LMP. Quantitative results with significant uncertainties and/or uncertainty that is not well characterized are not useful for risk-informed decision-making; accordingly, Chisholm et al. [2018c] suggest that it might be beneficial to use a simpler consequence measure than off-site dose to reduce the uncertainty associated with quantitatively estimating risk associated with an LF-MSR design.

Finally, Chisholm et al. [2018c] note that although the MSRE PrHA [Beall, 1962] was helpful to identify some PIEs and important system responses for the quantitative ETA used to evaluate LBEs, contributions from a more comprehensive hazards assessment approach would have been useful to develop a more accurate understanding of risk. The safety analysis developed prior to operation of the MSRE was much more thorough in identifying hazards and mitigating SSCs and design features for the fuel salt system than for the other inventories of radioactive material, such as those present in the OGS and fuel processing systems. Chisholm et al. [2018c] conclude that using modern PHA methods to identify PIEs would likely allow for the grouping of these PIEs in a more technology-inclusive manner. This conclusion is made because modern PHA studies focus on a broad range of possible deviations from nominal operating conditions, rather than limiting the safety analysis to those scenarios that are typically considered for more familiar reactor designs.

2.5. Summary

In the commercial nuclear industry, a probabilistic approach to quantify risk is currently used to assess the safety of mature reactor designs and to verify that they will meet safety goals set by the regulator (i.e., the NRC in the US). However, the implementation of PRA to evaluate the safety of LWRs has been significantly informed by prior operating experience. As such, a truly technology-inclusive methodology to perform a systematic and comprehensive evaluation of a nuclear reactor design without a substantial body of commercial operating experience has not been defined. Furthermore, since the incorporation of PRA into the commercial nuclear safety assessment approach, the benefits of using risk and hazard evaluations starting at an early stage of design for risk-informed decision-making and incorporation of safety into the design process is now understood and gaining momentum.

The methodology defined and demonstrated in this dissertation is predicated upon the concept that execution of a formal assessment of ES&H risks at an early stage will: (1) maximize the incorporation of SiD; (2) incrementally contribute elements to a reproducible and risk-informed safety basis; and (3) assist in the identification and prioritization of potential R&D tasks. The methodology also recognizes that for relatively immature technologies, a fully quantitative characterization of risk may not be possible, and for some systems, a fully quantitative characterization of risk may not be necessary. Accordingly, qualitative industry-standard PHA methods can be used as the starting point for a methodology that achieves the aforementioned objectives.

Table 5 displays a brief summary of the prior LF-MSR hazard and risk assessment efforts reviewed in Section 2.4.2. It can be seen that although quantitative evaluations of risk associated with LF-MSR designs have been initiated, most studies are focused on the fuel salt loop during normal operations. However, as illustrated in Section 4.1 using the MSRE design, other significant inventories of radioactive material can exist in LF-MSR systems. The research in this dissertation fills existing gaps in the approach to ES&H risk assessment of advanced reactors by exploring how risk can be effectively characterized for radioactive material inventories other than the fuel salt being circulated in the fuel salt system during normal operations in a technology-inclusive, systematic, and comprehensive way.

Table 5: Summary of prior LF-MSR hazard and risk assessment efforts

Reference	Focus of Study	Task(s) Performed	Method(s) Used	Insights Gained and Used for Methodology Development
[Holcomb et al., 2019]	Normal operations of select subsystems from MSRE, MSBR, and Molten Salt Demonstration Reactor	PIE identification	Brainstorming (i.e., Hazard Identification)	• An exhaustive search for PIEs should consider occurrences outside of the fuel salt loop • Categorization of PIEs will facilitate transition to more quantifiable models of risk (e.g., ETA)
[Geraci, 2017]	Normal operations of LFTR fuel salt loop	PIE identification and grouping	Survey of PIE lists for other reactor technologies and What-If analysis ([EPRI, 2015])	• A systematic and comprehensive hazard analysis is a beneficial precursor to an exhaustive search for PIEs
[Gèrardin et al., 2019]	Normal operations of MSFR fuel salt loop	PIE identification and grouping	FFMEA and MLD	• Gèrardin et al. [2019] notes that using both an inductive analysis and a deductive analysis increases the exhaustiveness of a search for PIEs • Grouping PIEs by plant response required to mitigate consequences would facilitate transition to analysis of event sequences

Reference	Focus of Study	Task(s) Performed	Method(s) Used	Insights Gained and Used for Methodology Development
[Pyron, 2016]	Normal operations of FUJI U233-Um (fuel salt loop and OGS)	Identification of PIEs, SR-SSCs, DBAs, and safety weaknesses	MLD, event sequence diagrams, ETA, and FTA (preliminary PRA model)	• An RIPB approach to evaluating risks associated with design lends itself to a thorough identification of risk-significant occurrences and design decisions • It is possible that hazards and phenomena that are not considered for other reactor designs need to be evaluated for their significance in LF-MSR designs before they can be dismissed • Pyron [2016] notes that there is a need for a methodology that can assess the risk associated with "auxiliary" systems containing radioactive material (e.g., OGS) • Pyron [2016] also indicates that development of LF-MSR-specific SSC failure rates would reduce uncertainty associated with quantitative models of risk for LF-MSR designs
[Qun et al., 2017]	TMSR-LF special core fuel salt release system	Evaluation of subsystem reliability	FTA and HRA	• Qun et al. [2017] notes that development of LF-MSR-specific SSC failure rates would reduce uncertainty associated with quantitative models of risk for LF-MSR designs

Reference	Focus of Study	Task(s) Performed	Method(s) Used	Insights Gained and Used for Methodology Development
[Chisholm et al., 2018c]	MSRE fuel salt and off-gas during normal operations	Identification and grouping of PIEs; identification of LBEs and design-specific safety functions	Survey of MSRE PrHA ([Beall, 1962]), ETA, and FTA	• Chisholm et al. [2018c] suggest that event sequences resulting in the release of radioactive material from "auxiliary" systems in LF-MSRs (e.g., an OGS) can be risk-significant • A more comprehensive hazards analysis would help identify PIEs for inventories of radioactive material other than the fuel salt during normal operations

CHAPTER 3, OVERVIEW OF A TECHNOLOGY-INCLUSIVE METHODOLOGY TO ANALYZE ES&H RISKS ASSOCIATED WITH ADVANCED REACTOR DESIGNS

The following guiding principles assisted the definition of the methodology described in this chapter:

- The approach is not entrenched in established LWR technology; however, it does build on techniques developed and implemented to support safety analysis of the existing fleet of LWRs.
- It uses existing, proven, industry-standard safety analysis techniques in a technology-inclusive manner.
- Rooted in systematic and thorough hazards identification techniques and using well-exercised methods for frequency and consequence determination, the methodology supports RIPB approaches to safety assessment and design.
- It begins at the earliest feasible stages of concept development, adapting tools and techniques to the amount and maturity of the data available.
- It can advance incrementally and iteratively with the maturing design, developing the elements for the safety case of a design, in addition to delivering results that are useful for prioritizing technical issues requiring resolution.
- Using both qualitative and quantitative techniques, the methodology can be readily tailored to support SiD for systems of various scales and applications, including: experimental apparatus, test reactors, demonstration reactors, and full-scale reactors.

3.1. Overall Methodology Structure

Figure 3 provides a pictorial representation of a single iteration of the safety assessment methodology. For a full-scale reactor design, the depicted process is intended to incrementally and iteratively produce elements that will evolve with a maturing design into the building blocks of the final full-scope facility PRA. However, the process can be readily tailored to support other design-related facilities and apparatus, such as a single test loop that may not contain radioactive material but may contain hazardous chemical materials.

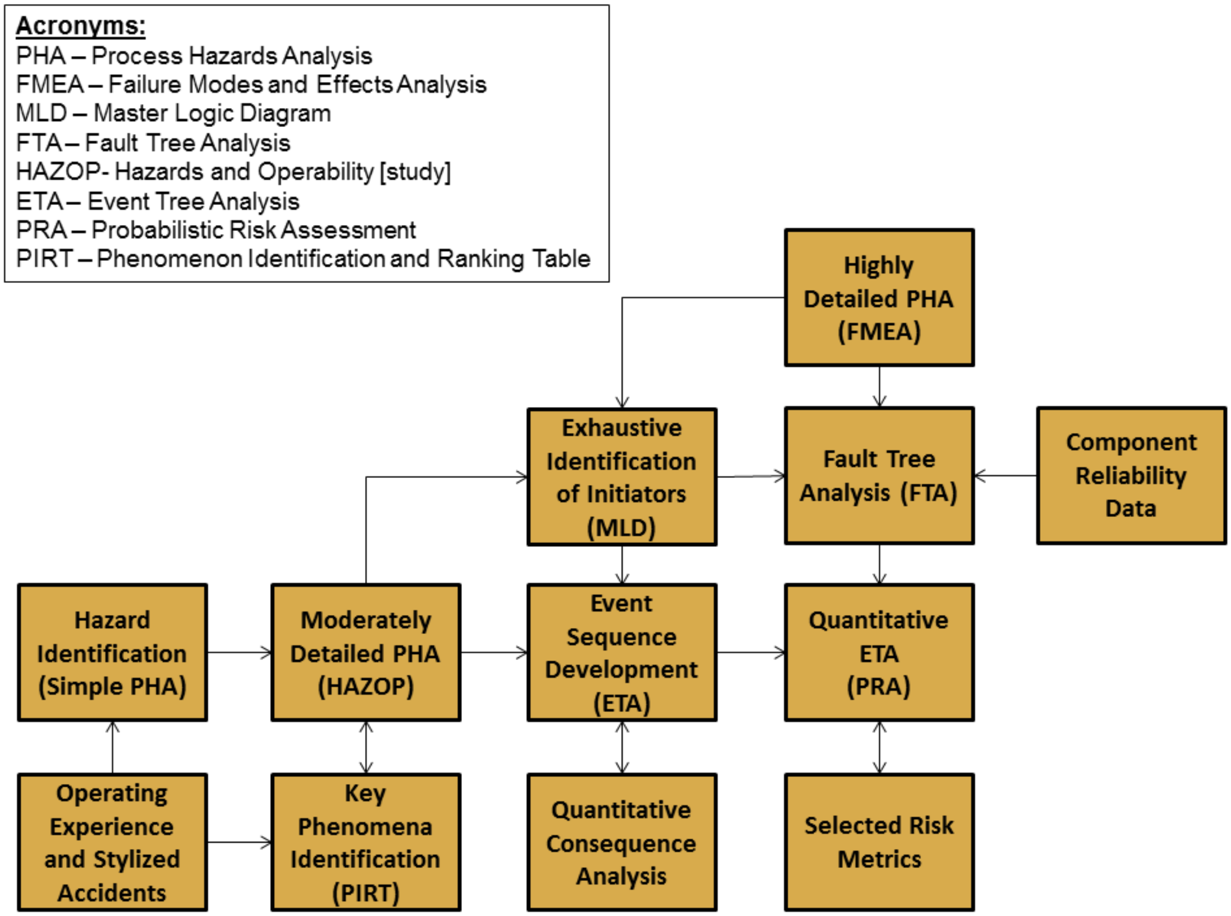


Figure 3: Overview of methodology[23]

The starting point for the methodology is the performance of an industry-standard PHA study, indicated by the upper boxes in the first and second columns in Figure 3. The NRC [2001] and US DOE [2004] recognize that the Guidelines published by the CCPS [2008] represent perhaps the most clear and comprehensive reference to provide information on common PHA study methods, in addition to being well-suited to experienced practitioners of hazard analysis. The Guidelines describe 12 different PHA methods, and the choice between 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 [CCPS, 2008]. However, three methodologies, including What-If/Checklist, HAZOP study, and FMEA, represent the entire list of choices recommended for the study of a system in which the perceived risk of potential accident sequences is high [CCPS, 2008].

[23] Earlier versions of this flowchart were published by EPRI [2018, 2019], Krahn et al. [2018a], and Chisholm et al. [2019].

The maturity of the design to be analyzed is an important consideration when selecting an appropriate PHA process to begin the methodology. 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. These kinds of early PHA studies can be used to identify: (1) hazards that may result in deviations from nominal system operation, (2) the potential consequences if the deviation is not mitigated, and (3) the specific design features or safety functions relied upon to mitigate the consequences. The initial list of hazardous scenarios can be supplemented using a literature survey of operating experience documented for similar systems or stylized accidents required to be analyzed by a regulator (e.g., DBAs such as a large break loss of coolant accident [National Research Council, 2014]).

As the design of the system being analyzed and the understanding of accident phenomena in the system mature, more detailed PHA methods become appropriate [NRC, 2001]. Typically, as design advances to the conceptual stage, sufficient information becomes available to support application of the HAZOP method. The results of a HAZOP study are typically more comprehensive than those of a What-If study, and can be used for applications such as developing initial event sequence diagrams that form the basis of models for qualitative ETA [NRC, 1983]. By providing a set of specific PIEs and event sequences for which an end state must be known, these initial models can additionally provide an informed basis for the formulation of accident sequences to be evaluated for early quantified estimates of consequences. The use of other tools, such as MLD, augments the HAZOP in surfacing additional observations and findings (as discussed further in Chapter 5). HAZOP analysis can also be useful to identify gaps in existing knowledge surrounding a design or a technology, especially regarding hazards or phenomena that are not well understood. These results can inform R&D efforts and/or developer test plans [EPRI, 2019].

The more design information that is available, the more relevant and meaningful the PHA results become. Eventually, the design will mature sufficiently to enable the use of a PHA method like FMEA that can produce outputs that are structured and comprehensive enough to support the development of qualitative FTs. The FTs can then be quantified with component reliability data to estimate the failure frequency of SSCs and to identify design-specific safety functions. Then, quantitative FTA can be linked to the initial ETA and enable the beginning of limited quantitative ETA, which is a building block towards the eventual preparation of a complete PRA model [ASME/ANS, 2013]. At later stages of design, when systems and subsystems have been individually analyzed and system interfaces have been defined, the design project can begin to integrate the building blocks of the PRA into the process for assessing overall facility integrated risk, if desired. When the PRA is sufficiently mature, meaningful quantitative risk metrics can be identified to better understand the risk profile of various potential scenarios and design decisions [NRC, 2019c].

3.2. Analysis Tools and Interfaces between Methods

In this section, each element depicted in Figure 3 will be discussed, including an overview of industry-standard approaches and a discussion of how the elements interface with each other.

3.2.1. Hazard Identification

As indicated in Figure 3, this methodology was defined in such a way that the rigorous consideration of hazards is encouraged to begin as early as possible in the design process – perhaps even earlier than safety analysts may deem that PHA method as structured as a HAZOP study can be performed. Even in the absence of detailed system design information, designers and safety analysts are able to answer the question "what can go wrong?" and document the results. A simple tool for identifying potential hazardous interactions among specific parameters (such as materials, energy sources, environmental conditions, etc.) is an interaction matrix [CCPS, 2008]. Checklist Analysis is another example of a structured approach to identify potentially hazardous situations that are applicable to specific processes or inventories of hazardous materials [CCPS, 2008]. Although these approaches will not necessarily identify every potential hazard in a design, significant hazards that are identified can inform future safety assessment and design efforts. Additionally, hazard identification results can lay the groundwork for more advanced safety analyses, such as providing insight regarding parameters and guidewords to be used as part of a HAZOP study (see Section 3.2.3).

In the pre-conceptual phase of a design process, it is also possible to perform a limited qualitative evaluation of system consequences related to hazards that have been identified. Examples of studies to perform such an analysis include tools like a PrHA or a What-If study [CCPS, 2008]. For instance, in a previous LF-MSR hazard analysis, the What If method was chosen to analyze the Liquid Fluoride Thorium Reactor (LFTR) conceptual design 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 [EPRI, 2015]. These tools can provide initial qualitative insights regarding potential safety concerns, as well as a rough relative ranking of those concerns. As discussed in the following subsection, these less comprehensive PHA methods can benefit by the incorporation of insights gained from prior related operating experience and/or any applicable stylized accidents that have been evaluated for similar designs. In the What-If study of the LFTR design, for example, the SAR for the MSRE design [Beall et al., 1964] was used to identify hazards and develop postulated hazardous scenarios to be evaluated [EPRI, 2015].

3.2.2. Operating Experience and Stylized Accidents

Relevant operating experience from similar systems can be a valuable tool to identify hazards. Undesirable consequences that have occurred in the past can demonstrate where hazards exist, while good experience can demonstrate that hazards have been adequately controlled and how this was done [CCPS, 2008]. For example, the hazards evaluated in the MSRE PrHA [Beall, 1962] were based upon ORNL's previous experience with other liquid-fueled nuclear reactor designs [Flanagan, 2017]. Prior experience with hazards is also an input to activities that rank hazards to be considered in a design and the relative magnitude of deviations involving different physical phenomena, such as Phenomena Identification and Ranking Table (PIRT) analyses (see Section 3.2.4); additionally, an understanding of the existing body of knowledge surrounding each hazard is needed to characterize the associated uncertainty.

Another source of information to be consulted in the earliest stages of hazard evaluation, especially for nuclear reactor designs, is historical guidance on hypothetical risk-significant events. For example, regulators have previously required the analysis of DBAs (such as Anticipated Transients without Scram and Station Blackouts) to protect plants against "unknown unknowns." [Apostolakis, 2016; Nourbakhsh et al., 2018] These high-consequence and low-probability events do not reflect operating experience or modern understanding [Apostolakis, 2016], but can provide insight about hazardous scenarios of concern to the regulator. Thus, a comprehensive assessment of ES&H risk should at least consider these hypothetical risk-significant events, even if an RIPB methodology does not prescribe a thorough analysis of the stylized scenario.

3.2.3. Hazards and Operability (HAZOP) Study Method

Once the design of the system that is being analyzed and the understanding of accident phenomena relevant to the system reach sufficient maturity, more systematic and comprehensive PHA methods can be used to evaluate hazards. Because the hazard assessments of the MSRE presented in the following chapters of this dissertation were intended to be as comprehensive as possible, both the HAZOP and FMEA methods were used. Both of these PHA approaches are more systematic than the What-If methodology [Khan and Abbasi, 1998]. The major differences in application between the HAZOP and FMEA methodologies are that, although an FMEA can produce results with a higher level of detail than those of a HAZOP study, a HAZOP study is better suited to comprehensively identify hazards and is capable of analyzing a combination of failures [Nolan, 2015; Popović and Vasić, 2008]. Based on these differences, the methodology demonstrated in this dissertation relies most heavily upon HAZOP studies to generate risk insights regarding hazardous events and their progression through the system over time. The reason is that HAZOP studies, with the proper groundwork and preparation, are highly effective at comprehensive hazards assessment and can be applied at a fairly early stage in design development [Crawley and Tyler, 2015]. The FMEA methodology (discussed in Section 3.2.8) was used to complement a HAZOP study in situations that the HAZOP approach did not produce results with sufficient resolution (see Chapter 6). The HAZOP method is recognized in industry standards as a method that provides sufficiently detailed results to directly support quantitative risk assessment (i.e., PRA) efforts [ASME/ANS, 2013; IAEA, 2010; US DOE, 2013]. The next few paragraphs discuss the structure of a HAZOP evaluation, drawing from industry guidelines [Center for Chemical Process Safety (CCPS), 2008; Crawley and Tyler, 2015; Nolan, 2015; Product Quality Research Institute (PQRI), 2015].

The HAZOP approach is the most comprehensive of the primarily non-quantitative PHA methods [CCPS, 2008] and is based on the principle that a focused team of subject matter experts, with varied backgrounds, can "interact in a creative, systematic fashion and identify more problems when working together than when working separately and combining their results" [NRC, 2011]. A HAZOP study is unique in this sense because other PHA techniques could, theoretically at least, be performed by a single person. The method has been successfully used on projects in early design phases to inform the design process on an iterative basis [McDermid et al., 1995; PQRI, 2015]. In order to be able to identify situations outside of the intended operational range of the system or subsystem - referred to as "deviations" in a HAZOP study - the team conducting the HAZOP begins with the development of an understanding of the specific system or subsystem to be analyzed and how it is intended to function during normal operation. The system under review is described in detail (descriptions of equipment in each subsystem, materials, operating conditions, as well as the means of control), with references to design documents, so that a later user of the results would be able to understand the approach and information used by the HAZOP team.

The parsing of the system being studied into analyzable "nodes" is a critical step in the preparation for a HAZOP study that warrants careful consideration and the willingness to make adjustments even after the elicitation process begins, if necessary. If the study node is too tightly defined, it is possible that hazards or PIEs could be overlooked because they occur outside the node boundary [Crawley and Tyler, 2015]. Conversely, if the node is too broadly defined, the functions of the intended design can be too complicated to recognize all significant consequences due to a failure or deviation from normal operating conditions within the node. Useful guiding principles for node definition include:

- Each node should be limited to one major design function.
- Node definition should be such that multiple nodes do not perform the same function (with the exception of redundancy by design).

- Node boundaries should be structured such that similar operating conditions (such as working fluid or pressure) exist within each node. Component failure rate data is often grouped according to such attributes.
- The interfaces between nodes should be thoroughly documented in order to better account for the propagation of a deviation or event sequence from one node to another.

Once the study team understands the design and intended normal operation of the study node, the hazard analysis can begin with the generation of potential deviations from the defined normal operation, by coupling a guideword and a parameter. "Guidewords" are action words or phrases such as "no," or "reduced," that describe how parameters within the system could change in relation to their values during normal operation. An example set of guidewords for a chemical processing plant is as follows [Crawley and Tyler, 2015]:

- No (not, none): None of the design intent is achieved
- More (more of, higher): Quantitative increase in a parameter
- Less (less of, lower): Quantitative decrease in a parameter
- As well as (more than): An additional activity occurs
- Part of: Only some of the design intention is achieved
- Reverse: Logical opposite of the design intention occurs
- Other than (other): another activity takes place OR an unusual activity occurs or uncommon condition exists

Although general recommendations are available regarding applicable guidewords to consider during a HAZOP study, the list of parameters to be paired with the list of guidewords is not as straightforward. The selection of parameters is a task each study team must address for the system being studied [Crawley and Tyler, 2015]. While examples of typical parameters that are used in HAZOP reviews are available (for examples, see [CCPS, 2008; Crawley and Tyler, 2015; Nolan, 2015]), the list of parameters used for each study should be supplemented or tailored to meet the needs of that system. As previously mentioned, the results of prior hazard identification efforts on the design being analyzed can also identify parameters that should be considered as part of the HAZOP study; for example, the MSRE PrHA [Beall, 1962] was used to develop the list of guidewords used for the HAZOP studies of the MSRE (see Chapter 4). Also, because the set of guidewords and parameters is intended for examination of several different subsystems, not all combinations may produce a meaningful deviation in each subsystem. For example, a deviation such as "no temperature" does not have a physical meaning. The purpose of the brainstorming done during this deviation generating stage of the HAZOP is to explore the possible guidewords that generate significant deviations [CCPS, 2008].

Once a meaningful deviation is identified, the next step in the HAZOP process is to identify the potential cause, or causes, of the deviation. Specificity is helpful when describing the cause(s) to ensure each different cause, with any unique consequences, is considered separately. As demonstrated in Chapter 6 of this dissertation, causes of deviations that are identified during a HAZOP study can represent PIEs that may contribute to later analyses, such as MLDs or ETA. Once possible causes for a particular deviation have been identified and discussed, the consequences of each cause are evaluated to determine qualitatively whether they take the system outside of the intended range of operation. Consequences should be identified as completely as available design and operational information permit. These consequences can include the initial response of the system, as well as potential secondary responses that may affect the overall impact to the system (e.g., a temperature increase that also increases pressure). Important information to incorporate into the discussion of the consequences includes the specific parameters that will be monitored to indicate a deviation from normal operation, as well as safety systems[24] that are intended to prevent the cause or mitigate the consequences. The discussion of relevant safety systems should include documentation of which actions will be manual (i.e., procedural) rather than automatic (i.e., engineered) [CCPS, 2008].

It is also possible that, for some causes, the discussion may result in a recommended action item that can increase the accuracy of the results or resolve uncertainty, for instance, by the performance of a more detailed analysis outside of the HAZOP study [Crawley and Tyler, 2015]. To conclude the discussion for a particular deviation, any actions agreed upon by the team should be recorded. Generally, the study team will recommend a solution to a problem only if they have clearly agreed upon a recommendation; thus, cases will exist where the team needs to defer potential problems for further investigation or the development of an engineering or procedural solution to a problem. Action items from a HAZOP study can also include scenarios that must be further assessed to fully understand the consequences of a specific deviation; these insights and lines of inquiry can support the development and execution of a PIRT exercise to inform R&D or the development of analytical tools, as discussed in the following subsection.

Once the information for a specific deviation has been recorded, the team proceeds to generate the next deviation. In other words, another guideword is combined with the parameter currently under review. Once all significant guidewords for a given parameter have been identified, the HAZOP team considers the next parameter of interest, and repeats the analysis

[24] In the chemical process industry, these prevention and mitigation features are often referred to as "safeguards." In this dissertation, the term "safety system" has been used to avoid confusion with the distinct field of nuclear safeguards.

process, as illustrated by the flowchart in Figure 4. The examination of a system or subsystem is completed when no further important parameters remain [CCPS, 2008; Crawley and Tyler, 2015].

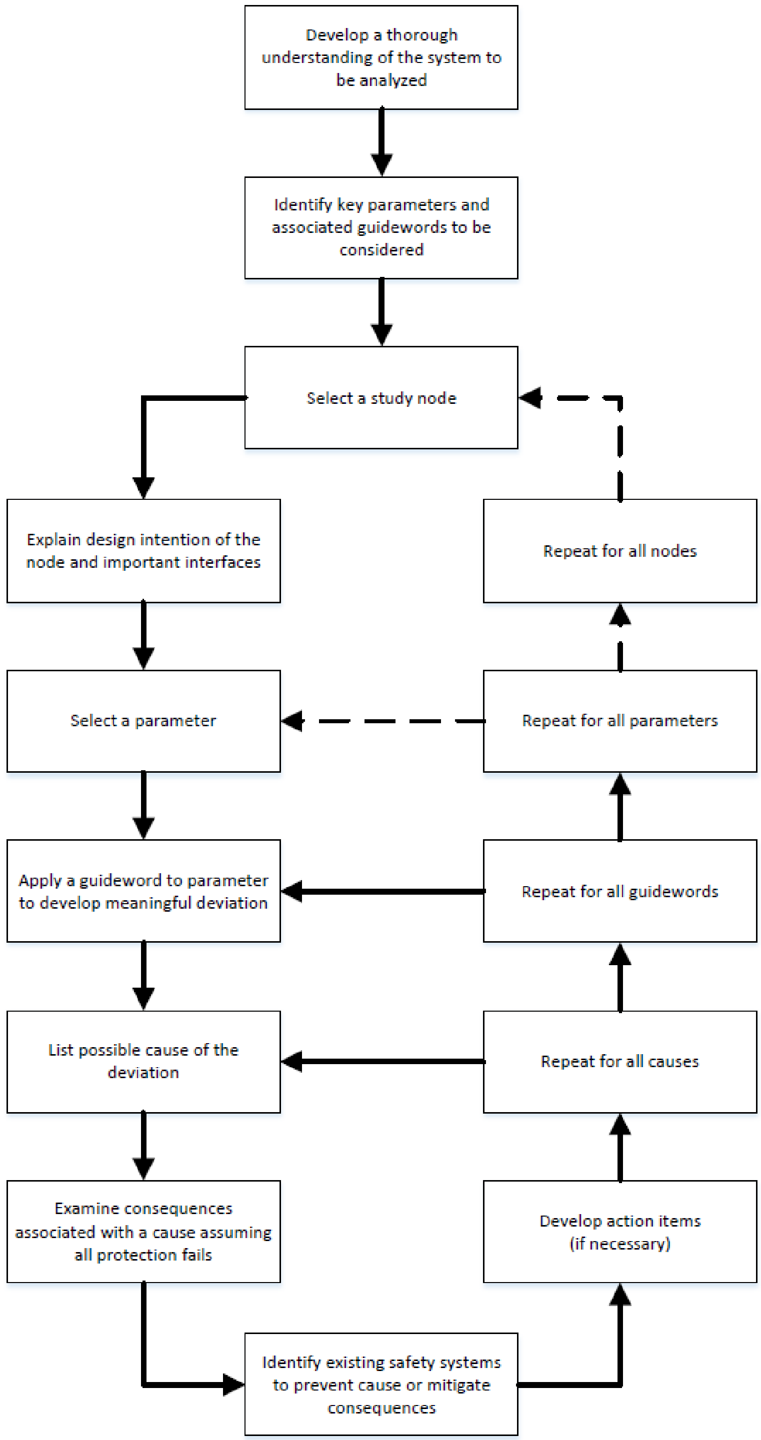


Figure 4: Basic steps in a HAZOP study (adapted from [CCPS, 2008])

Documenting the HAZOP study is focused on capturing the conversations in a tabular format while reporting the results of the review and describing how action items (discussed above) that have been identified will be addressed. The tabular structure organizes pertinent information related to each postulated scenario and also allows the responsible individuals to place the issues that have been identified in their proper context [CCPS, 2008; Crawley and Tyler, 2015]. As will be discussed in Section 3.2.6, the tabular results of a HAZOP study also lend themselves to the structuring of event sequence diagrams and initial qualitative ET models.

3.2.4. Key Phenomena Identification and Ranking

The PIRT technique is an approach that has been used in the nuclear industry since the late 1980s. It is a systematic way of gathering information from experts on a specific subject and ranking the importance of the information in order to meet a desired objective [Diamond, 2006]. For example, a PIRT exercise was recently conducted to understand the modeling needs for codes to simulate the fuel salt systems of LF-MSRs [Diamond et al., 2018]. In the context of risk nuclear reactor risk assessment, the phenomena of interest are hazards and other challenges to plant safety. An important part of the PIRT process is the estimation of uncertainty in the ranking, which is usually done by scoring the knowledge base for each phenomenon [Diamond, 2006].

A PIRT analysis can be used to inform a HAZOP (or other PHA) study on the nature of hazards to be considered and the relative magnitude of deviations involving different physical phenomena, especially in designs for which hazard identification has not been conducted. For systems that were previously analyzed thoroughly using a hazard identification approach, like those discussed in Section 3.2.1, a PIRT exercise may simply be an extension or update to the hazard identification study. Additionally, although not depicted explicitly in Figure 3, results of hazard identification, PHA studies, and/or a PIRT exercise can inform 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 and tools. Finally, as mentioned in the previous section, insights generated by PHA studies related to hazards and important phenomena can inform the construction of any subsequent PIRT exercises.

3.2.5. Exhaustive Identification of Initiators

An important starting point for a quantitative safety assessment is a comprehensive and systematic analysis of possible occurrences that have the potential to result in undesirable consequences within the system (i.e., design-specific answers to the question "what can go wrong?). In general, these occurrences are called IEs. However, the IAEA [2019] recommends the term "*postulated* initiating event" when used during the consideration of hypothetical events at the design stage. Identification of PIEs is acknowledged as one of the first steps for evaluating risk associated with system designs in many industries [Modarres, 2006], including the aerospace [NASA, 2011], chemical process [CCPS, 2010], and commercial nuclear industries [IAEA, 2010; NRC, 1983]. A commonly cited tool to facilitate the identification of PIEs is the MLD [IAEA, 1993; Modarres, 2006; NASA, 2011; NRC, 1983]. MLD is a deductive (i.e., top-down) analysis that resembles a fault tree but is almost exclusively qualitative and is generally less rigorously structured than the latter [Papazoglou and Aneziris, 2002]. MLD analysis begins with a single undesired consequence, and this event is then logically decomposed down into simpler contributing events that could lead to the top event [Papazoglou and Aneziris, 2002]. The decomposition continues with a concerted effort to consider all physically possible phenomena until a sufficient level of detail is reached.

The MLD approach can be useful to determine elementary failures (or combinations of elementary failures) that could challenge normal operations; however, use of MLD alone does not provide sufficient confidence that PIEs have been comprehensively identified [IAEA, 2010]. The combination of a deductive analysis (such as MLD) with an inductive analysis to determine hazardous physical and/or chemical reactions has been found to be particularly effective to ensure completeness of PIE identification and design improvement, including reduction of uncertainty [Nagel and Stephanopoulos, 1995]. The variety of industry-standard inductive analyses include semi-structured PHA methods (e.g., What-If analysis), structured PHA methods (e.g., HAZOP studies), and structured analysis of failure modes (e.g., FMEA) [CCPS, 2015]. An example of an effort using FFMEA and MLD analysis to identify PIEs for a conceptual LF-MSR design was published by Gèrardin et al. [2019] (see Section 2.4.2), and discussion of how HAZOP studies and MLD analysis were used to identify PIEs for the MSRE design is presented in Chapter 5 of this dissertation.

3.2.6. Event Sequence Development

ETA was introduced in Section 2.1 of this dissertation as an industry-standard approach to model the response of a system to a PIE through a number of pivotal events (representing the success or failure of SSCs to perform preventative or mitigating functions) to depict the end state of the system for each unique event sequence. A simplified example of how the results of HAZOP studies can support the development of initial event tree models is displayed in Figure 5. The causes of deviations can represent PIEs (or families of similar PIEs that have been grouped together). As discussed in the previous section, PIEs can also be identified through use of additional tools, such as MLD. Many consequences documented in a HAZOP study are related to the end state of an event sequence, as they can identify challenges to barriers that prevent or mitigate release of hazardous material; however, some consequences may only be related to operability concerns that ultimately do not result in safety-significant consequences.

The safety systems documented in the HAZOP results can help identify pivotal events to be modeled in the ETA, in addition to informing the proper ordering of these pivotal events in the model. While constructing an event tree model, it is important to review all related results to ensure a comprehensive understanding of the event sequences of interest. The following subsection will discuss considerations for how consequence analysis can be used to calculate quantitative values associated with a given end state, while the quantification of ET models by linking to fault trees is the topic of Sections 3.2.9 through 3.2.11.

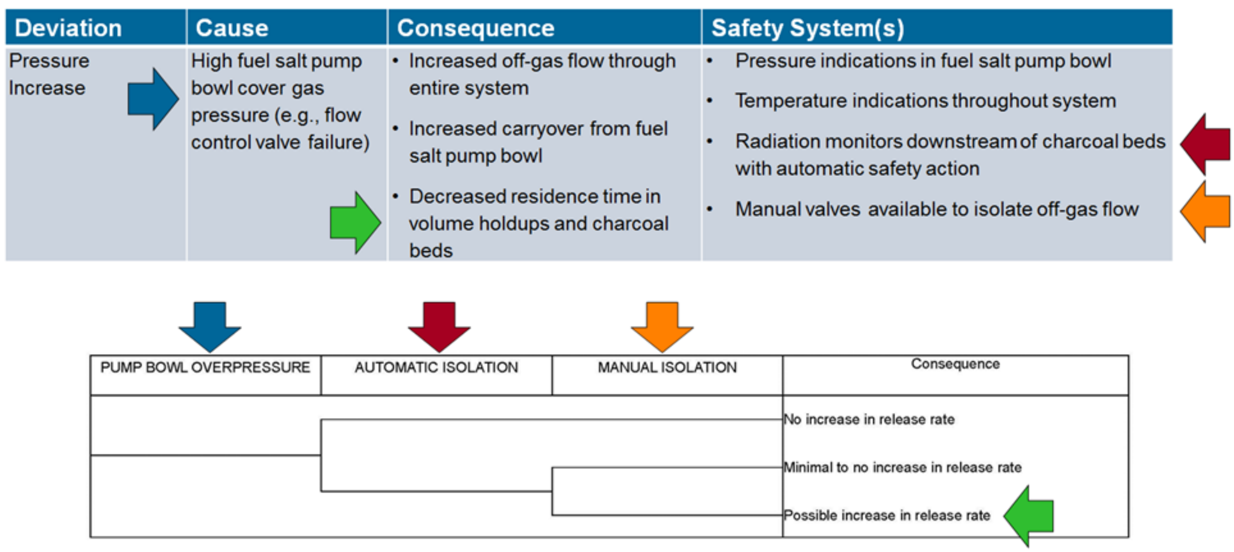


Figure 5: Example of relationship between HAZOP study results and ETA [Chisholm et al., 2018a]

3.2.7. Quantitative Consequence Analysis

Estimates of the consequences associated with each event sequence and/or end state in the ET models for a design will likely increase in fidelity as the maturity of the information regarding system design increases. At an early stage of design, design detail and/or analysis capabilities may only support a qualitative description of an event sequence's end state. Factors that will facilitate comparison and prioritization of event sequences include the form and composition of the inventories of hazardous material involved, whether hazardous material is transported through any barriers, and any conditions that may affect this transport.

Once sufficient data exists to reasonably estimate the amount and form of the hazards for a given inventory of material (e.g., activity, chemical compound, and/or physical form of radioelements), it is possible to increase the fidelity of the consequence analysis. Results of this caliber could be used to estimate consequences such as accident risks to workers and/or capital loss. As system design reaches the latter stages of development, sufficient information regarding safety system design and performance, as well as siting characteristics, will become available to support the development of analyses that estimate impact to the public, such as radiation dose to members of the public. These detailed calculations will likely be performed as the design is being finalized, and they may also support licensing and/or other applications.

3.2.8. Failure Modes and Effects Analysis (FMEA)

In order to quantitatively estimate risk, it is necessary to build a model that represents the various combinations of possible failures that can occur in a system and lead to an undesired event. In subsystems or processes of low-to-moderate complexity, the results of a HAZOP study are typically detailed enough to inform the creation of such a model. However, the FMEA method is capable of providing additional insight into system behavior while concentrating on one particular system failure at a time [Stamatis, 2003]. Due to this capability of FMEA, it may be necessary during the risk assessment process to perform an FMEA in addition to a HAZOP study for particularly complex systems or systems that have not previously been analyzed in great detail.

An FMEA is performed in a deliberate, systematic manner to reduce the possibility of omissions and to enhance the completeness of the study [CCPS, 2008]. The study is performed by examining each individual component or subsystem, one at a time, and then listing all credible failure modes associated with the equipment type and operating conditions. When considering a given failure mode for a specific component, the effects of the failure on the system as well as any safety systems mitigating the likelihood or consequence of the effects are recorded, similar to the "consequence" and "safety system" analysis for a HAZOP study. The key to performing a rigorous FMEA is ensuring that the effects of all equipment failures are analyzed using consistent assumptions [CCPS, 2008]. The FMEA analysis proceeds systematically until all the credible failure modes for each component in the system have been considered and the results have been recorded.

As previously mentioned, FMEA can identify PIEs in the form of specific failure modes of SSCs in the design that lead to a given, undesired consequence. The following subsection discusses how the results of a sufficiently detailed FMEA can be useful to help structure FT models that will eventually be used to quantitatively estimate the likelihood of failure for various SSCs and functions.

3.2.9. Fault Tree Analysis (FTA)

In Section 2.1, FTA was introduced as a deductive approach that decomposes a top event of concern into more specific events, until the fundamental fault causes (such as specific equipment failures or human response errors) are identified [CCPS, 2008; US DOE, 2004; Vesely et al., 1981]. In PRA models, FTA is often used to represent PIEs and pivotal events in ETA, and can be used to estimate their frequency of incidence [NRC, 1983].

The results of PHA studies can be somewhat helpful to structure FT models, provided that the results contain a sufficient level of detail. For example, in HAZOP study results, multiple different causes that have the same (or similar) consequences could represent basic events that are grouped under the same intermediate event in a fault tree. However, it is possible that a HAZOP study may not document the results at a detailed enough level to comprehensively capture the basic events that can contribute to the top event of the fault tree. However, FMEA is particularly useful to document component failure modes that represent basic events, as well as the larger system or functional failures to which these failure modes can contribute. When developing FT models, the causes and consequences from the results of a HAZOP study can be used to identify the top event of a fault tree and to structure the logic of the intermediate events at the higher levels of the tree. Then, the failure modes and consequences from FMEA results can be used to populate the basic events at the lower level and help maximize the comprehensiveness and thoroughness of the analysis. The following subsection will discuss how qualitative FT models can be quantified using component reliability data.

3.2.10. Component Reliability Data

In order to quantify FT models to calculate a quantitative estimate of likelihood for the top event, it is necessary to assign a failure probability to each basic event in the model [CCPS, 2010; Vesely et al., 1981]. In a system with many electrical and mechanical components, a large number of the basic events are likely to be failures of components; thus, an essential aspect of quantifying models of system risk is component reliability data. Generic component reliability databases do exist for the commercial nuclear industry (e.g., [Eide et al., 1990; Gertman et al., 1989; IAEA, 1988]), but because this data was gathered for the current fleet of commercial LWRs, models to analyze advanced reactors may need failure rates for components that are not represented in these databases.

Options for determining a failure rate include estimating a failure rate for a component based upon R&D activities; using component reliability that has been collected for a similar component from another industry (e.g., non-nuclear) under similar operating conditions; and/or eliciting expert opinion to estimate the component failure rate. The selection of which option is most appropriate depends on how much data exists for the component or for similar components, as well as the intended use of the quantitative results. Factors to consider when evaluating the similarity of two components include function, operating environment, and size/scale. R&D activities that can produce preliminary estimate of failure rate include component development tests, separate effects tests, and integrated effects tests. If the intention is to use the quantitative fault tree results for design applications, expert opinion may be an efficient option for estimating failure rates; however, modern regulatory applications may require more empirical approaches to collecting component reliability data. Interestingly, according to a report published by the NRC [2016b] that documents historical knowledge and primary source information from a participant in the first nuclear reactor PRA study (i.e., WASH-1400)[25], the accuracy of WASH-1400 did not suffer from lack of data or experiments, even though it was conducted in the 1970s, when the commercial nuclear industry was still quite young.

3.2.11. Quantitative Event Tree Analysis (ETA)

In order to provide quantitative relative risk insights by comparing the likelihood and consequence associated with various event sequences, estimates of frequency and consequence are required for each event sequence that is modeled in the ETA. The likelihood of each PIE and pivotal event are calculated in the ETA by linking the events to the appropriate corresponding quantitative FT model, and the frequencies of the event sequences are determined by the "failure or success" logic set in the ET model [CCPS, 2010]. These quantitative estimates of likelihood and consequence for each PIE and event sequence are building blocks for the PRA model, and will eventually be combined to contribute to the full-scope PRA model of the design as the fidelity and comprehensiveness of the quantitative ETA increases [NRC, 1983].

3.2.12. Selection of Appropriate Risk Metrics

Finally, at later stages of design, when systems and subsystems have been individually analyzed and system interfaces have been thoroughly evaluated, the safety assessment can integrate the building blocks of the PRA into a detailed tool that is used to quantify overall facility integrated risk. At this point, industry guidance (such as [ASME/ANS, 2013]) can be used to ensure the technical adequacy of the full-scope PRA model for the entire system.

As accident sequences and their progression are better understood, consideration of risk surrogates or figures of merit for ES&H risk assessment may be developed to facilitate safety analysis and to identify the systems and scenarios that are most risk-significant. Use of these metrics can then be defended and incorporated into quantitative ETA and consequence analysis. 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 [NEI, 2019]. As discussed in Section 2.1, the

[25] WASH-1400, "Reactor Safety Study" (also known as the "Rasmussen Report"), issued in October 1975, was the first full-scope use of PRA techniques in commercial nuclear industry and contributed greatly to the development of the quantitative approach to risk-informed and performance-based regulations [NRC 2016b].

most familiar example of a risk metric currently used in the commercial nuclear industry is Core Damage Frequency (CDF).

3.3. Summary of Interfaces between Methodology Elements

Table 6 displays a summary of the major interfaces between each element in the developed methodology (shown in Figure 3).

Table 6: Summary of interfaces between methodology elements

Element	Input(s) from Other Element(s)	Output(s) to Other Element(s)	Notes/Comments
Hazard Identification	• Hazard-related insights gained from prior related operating experience • Applicable stylized accidents previously evaluated for relevant technologies/systems	• Preliminary list of applicable hazards (and/or hazardous phenomena) • Framework for downstream analyses (e.g., insights regarding parameters and/or guidewords for a HAZOP study)	• Insights to inform next stage of design (e.g., limited qualitative evaluation of safety functions) can also be generated during hazard identification • The simple PHA methods used for identification of hazards (e.g., What-If and PrHA) are typically not as systematic or comprehensive as "Moderately Detailed PHA" methods

Element	Input(s) from Other Element(s)	Output(s) to Other Element(s)	Notes/Comments
Operating Experience and Stylized Accidents	• N/A	• Undesirable consequences during prior operations can help identify hazards • Positive operating experience can demonstrate how hazards can be adequately controlled • Hypothetical, stylized (i.e., high-consequence and low-probability) events to be considered during hazard identification • Prior experience with hazards can assist in ranking the relative magnitude of physical phenomena and qualitatively assessing uncertainty	• Prior operating experience can also be helpful to identify parameters and/or guidewords for HAZOP studies

Element	Input(s) from Other Element(s)	Output(s) to Other Element(s)	Notes/Comments
Moderately Detailed PHA	• Results of prior hazard identification efforts can help ensure exhaustive consideration of relevant hazards (e.g., parameters for HAZOP study) • Existing rankings of hazards/phenomena can be used to prioritize PHA studies	• Hazard analysis studies can identify occurrences that represent potential initiators of safety-significant scenarios • Identification of consequences of deviations from intended operating conditions and related safety systems (or functions) is useful for development of event sequence end states and pivotal features • Consideration of consequences associated with various phenomena can help rank the severity of relevant phenomena, and can identify areas of uncertainty	• If a PHA study is performed in early stages of system design, the results can be used to help set functional requirements for safety systems • Insights to inform next stage of design (e.g., identification of how a safety-significant scenario could be detected by instrumentation) can also be generated during hazard identification • "Action items" for additional detailed analyses (e.g., simulation development) can be produced during PHA studies

Element	Input(s) from Other Element(s)	Output(s) to Other Element(s)	Notes/Comments
Key Phenomena Identification/Ranking	• Prior experience with hazards can assist in ranking the relative magnitude of physical phenomena and qualitatively assessing uncertainty • For systems that were previously analyzed using a hazard identification approach or PHA study, a PIRT exercise may simply be an extension or update to this analysis	• Results can inform subsequent PHA studies on the nature of hazards to be considered and the relative magnitude of deviations involving different phenomena • Results of a PIRT exercise can identify the need for and/or prioritize development efforts of experiments, models, analyses, and/or technology regarding physical and phenomenological behavior that cannot be satisfactorily predicted using existing knowledge and tools	• As adequate data and simulation tools are developed for a specific technology, the results of earlier phenomena identification/ranking exercises should be updated accordingly

Element	Input(s) from Other Element(s)	Output(s) to Other Element(s)	Notes/Comments
Exhaustive Identification of Initiators	• Moderately detailed PHA studies can identify functional PIE groups • Highly detailed PHA studies can identify specific PIEs (e.g., failures of different components that would belong to the same PIE group)	• PIEs (or PIE groups) are the starting point for event sequence models • PIE groups can be represented using fault tree models. Use of FTA allows for the eventual quantitative estimation of PIE (or PIE group) likelihood	• Many PHA studies utilize inductive approaches to identify PIEs; thus, the use of a deductive analysis (such as MLD) can be helpful to increase the exhaustiveness of a search for initiators • By extension, an exhaustive search for PIEs also benefits from consideration of prior operating experience, stylized accident scenarios, and hazard identification efforts

Element	Input(s) from Other Element(s)	Output(s) to Other Element(s)	Notes/Comments
Event Sequence Development	• PIE groups (or PIEs) are the starting point for event sequence models • Pivotal events in event sequence models can be identified as safety systems (or functions) in PHA studies • The end state associated with each event sequence can be qualitatively identified as a consequence in the results of a PHA study • Quantitative consequence analysis can be required to develop a more detailed understanding of end states	• The likelihoods of event sequences can be quantitatively estimated by linking quantitative fault tree models to initiating events and pivotal events • Identification of event sequences for which consequences have not previously been evaluated can influence the development of consequence analysis models/tools	• Both event sequence diagrams and qualitative event tree models can be used to display qualitative or semi-quantitative event sequence models

Element	Input(s) from Other Element(s)	Output(s) to Other Element(s)	Notes/Comments
Quantitative Consequence Analysis	• Event sequence models can be used to prioritize the scenarios and/or end states for which quantitative consequence analysis should be performed • Results of PIRT exercises can help determine the appropriate fidelity of consequence analysis for a given stage of design and/or desired use of results	• Quantitative consequence analysis can be used to develop a more detailed understanding of the end states associated with event sequences • As adequate data and simulation tools are developed for a specific technology, the results of earlier phenomena identification/ranking exercises should be updated accordingly	• As a system design and associated simulation tools mature, both the accuracy of quantitative consequence analyses and the understanding of associated uncertainties will increase

Element	Input(s) from Other Element(s)	Output(s) to Other Element(s)	Notes/Comments
Highly Detailed PHA	• Generic component reliability databases can be helpful to identify commonly considered failure modes for individual components	• Highly detailed PHA methods can produce results that are sufficiently detailed to contribute to the construction of fault tree models • Highly detailed PHA studies, such as FMEAs, can identify specific PIEs (e.g., failures of different components that would belong to the same PIE group)	• "Highly" detailed PHA studies can require a higher fidelity of design information than "moderately" detailed PHA methods (e.g., Piping and Instrumentation Diagrams, P&IDs vs. Process Flow Diagrams, PFDs)

Element	Input(s) from Other Element(s)	Output(s) to Other Element(s)	Notes/Comments
Fault Tree Analysis	• An exhaustive search for accident initiators can identify top events that can be decomposed and represented by fault tree models • Highly detailed PHA methods can produce results that are sufficiently detailed to contribute to the construction of fault tree models • Component reliability data can be used to quantitatively estimate the likelihood of basic events in a fault tree model	• Fault tree models can quantitatively estimate the likelihood of pivotal events and/or initiating events in event tree (or event sequence) models	• Human Reliability Analysis (HRA) can also be useful to quantify fault tree models

Element	Input(s) from Other Element(s)	Output(s) to Other Element(s)	Notes/Comments
Quantitative Event Tree Analysis	• The likelihood of event sequences can be quantitatively estimated by linking quantitative fault tree models to initiating events and pivotal events in the event tree (or event sequence) model • Cumulative risk insights can be generated by summing the frequencies of event sequences with end states corresponding to a particular risk metric	• The fidelity of existing models of system risk will inform what risk metrics can be reliably assessed and useful, given the current understanding of the design and relevant phenomena	• For technologies with sufficient operating experience, it may be possible to quantitatively estimate the frequency of initiating events and/or pivotal events based on historical data, without linking to fault tree models
Risk Metric Selection	• The fidelity of existing models of system risk will inform what risk metrics can be reliably assessed, given the current understanding of the design and relevant phenomena	• Cumulative risk insights can be generated by summing the frequencies of event sequences with end states corresponding to the selected risk metric	• Selection of appropriate risk metrics can also be informed by regulations and associated stylized events

Element	Input(s) from Other Element(s)	Output(s) to Other Element(s)	Notes/Comments
Component Reliability	• N/A	• Component reliability data can be used to quantitatively estimate the likelihood of basic events in a fault tree model	• Expert opinion can be used in the absence of sufficient relevant operating experience • Information from related industries with similar operating conditions can be of use for this element

3.4. Observations from Methodology Development

The methodology illustrated in Figure 3 was defined in such a way that its use during the design process of advanced nuclear reactors (or other systems containing significant inventories of hazardous material) is intended to benefit designers, safety analysts, and regulators alike. Industry-standard tools, such as PHA methods, offer flexible, systematic, and comprehensive approaches to answer the questions in the risk triplet at a level of depth that is commensurate with the current state of knowledge surrounding the design and the associated technology. By assessing the ES&H hazards and risks at an appropriate level iteratively through the design process, risk insights can be used to maximize the amount of safety that is built into the system design. Additionally, as demonstrated in Chapters 4-7 of this dissertation, qualitative PHA studies produce results that are sufficiently detailed to facilitate the transition from early-stage hazard assessments to more mature and quantitative assessments of risk in an incremental fashion. Finally, conducting the structured elements that comprise the methodology will also identify important knowledge gaps that can be used to prioritize R&D efforts.

CHAPTER 4, HAZARD AND OPERABILITY STUDIES OF THE MOLTEN SALT REACTOR EXPERIMENT

In order to demonstrate the technology-inclusive methodology discussed in Chapter 3, and to develop insights based on its implementation, a viable candidate advanced reactor technology was needed. As previously mentioned, LF-MSR technology was selected for multiple reasons; first and foremost of which was the lack of any prior PRA development efforts for LF-MSR technology. All of the other candidate advanced non-LWR concepts have a history of PRA development, including VHTRs and SFRs, but the application of an RIPB approach to evaluate an LF-MSR design would allow for the effort to generate first-of-a-kind results. Another advantage of selecting LF-MSR technology was the availability and proximity to a sufficient amount of publicly available design information and documentation. For example, MSBR and MSRE documentation has been publicly released and is retrievable,[26] and the source organization, ORNL, was available to collaborate on document retrieval as well as technology familiarization.

Once the decision was made to use LF-MSR technology, an early stage design needed to be found. Many current MSR designs[27] have published high-level descriptions of their design concepts, but detailed design information is either proprietary or not yet developed. The unfinished MSBR conceptual design [Robertson, 1971] may have been a candidate, as an early exploration of the application of PHA studies to the OGS of an LF-MSR [Chisholm et al., 2017] had allowed for familiarization with the design. The limited-scope MSBR hazard assessment exercises demonstrated the importance, from an ES&H risk perspective, of attention to the auxiliary systems. The intended presence of significant inventories of hazardous material beyond the fuel salt loop during normal operation supported the notion that proper nodalization and the use of flexible, industry standard hazard assessment tools were important for the comprehensive identification of potential pathways and scenarios for the inadvertent release of hazardous material. As may have been expected, the majority of detailed MSBR information focused almost exclusively on the fuel salt system, as opposed to the auxiliary SSCs performing functions to protect barriers for inventories of hazardous material other than the fuel salt. In contrast, due to its several years of operating history, considerably more information was available for the SSCs associated with the MSRE design -- notably, the OGS and fuel processing system. It was decided, therefore, that use of the MSRE would provide more opportunities in the learn-by-doing approach taken during this dissertation research.

---

[26] The publicly available MSRE documentation is available through the US DOE's Office of Scientific and Technical Information (OSTI) database, accessible at https://www.osti.gov/

[27] For example, see [Elysium Industries USA, 2018; Gèrardin et al., 2017; TerraPower LLC, 2019; ThorCon, 2018].

As discussed in Section 2.4.1, the MSRE does not have a safety analysis performed consistent with modern standards, nor has PRA been used to quantitatively analyze its risk profile. However, during a joint ORNL-Vanderbilt University effort in 2017 [Chisholm et al., 2018c], it was determined that there was sufficient design information available to support the application of detailed PHA methods, such as HAZOP studies and FMEA, as well as the eventual transition to quantitative FTA and ETA that constitute the core building blocks of a PRA. Further, it was determined that the available design information would be suitable for a simulation of an early design stage – as the design of both the OGS and fuel processing evolved considerably during the operating life of the MSRE.

The MSRE was designed, built, and operated for research. Had the MSRP at ORNL continued further past the conclusion of MSRE operations, more experience and data would have been collected in support of MSR technology. Logically, therefore, the technology was not fully developed and ready for deployment in a commercial application. Thus, from a safety perspective, the MSRE can be characterized by a Technology Readiness Level (TRL)[28] of 4 or 5 and, from a commercial facility design perspective, viewed to be in early design status. For purposes of methodology demonstration, the analyses considered that the facility was not yet operational and simulated this early design stage by using the available pre-operational design information documentation as a stand-in (or proxy) for the MSRE design team that would be represented on a team participating in team-based PHA efforts, such as HAZOP studies. Then, the MSRE operational data and the published safety documentation were used to help evaluate the developed methodology. In certain cases, the hazards and risks identified and characterized by the efforts presented in Chapters 4-7 were able to be compared to the hazards identified, characterized, and addressed by the original MSRE program to evaluate the benefits of systematic and comprehensive approach to hazard assessment.

The following lists provide a brief overview of some important references that were used to facilitate the system familiarization and the ES&H risk assessment of the MSRE design.

[28] A detailed discussion of TRLs and their application to advanced nuclear reactors is available in a report documenting a joint Vanderbilt-EPRI project published by EPRI [2017].

Reports written before operation of the MSRE:[29]

- Part I, Description of Reactor Design (ORNL-TM-728) [Robertson, 1965]: This report was written to discuss the design of the reactor. It contains thorough discussion of the design details and it contains the original design flowsheets for each MSRE subsystem.
- Part IIA, Nuclear and Process Instrumentation (ORNL-TM-729A) [Tallackson, 1968]: This report details the design and intended function of the MSRE safety system (i.e., most of the automatic responses of the system).
- Part III, Nuclear Analysis (ORNL-TM-730) [Haubenreich et al., 1964]: This report discusses the calculations made to characterize the nuclear behavior of the MSRE.
- Part VI, Operating Safety Limits for the MSRE (ORNL-TM-733) [Beall and Guymon, 1964]: This report describes the operating safety limits for the MSRE that are intended to protect the safety and health of the public, the safety of the operators, and the safety of the system against a severe and disabling accident.
- Part VIII, Operating Procedures (ORNL-TM-908, Vol. II) [Guymon, 1966]: This report contains the written operating procedures for the system. Volume I of ORNL-TM-908 discusses the nuclear aspects of operation, the operation of auxiliary systems, and startup checklists for the auxiliary systems.

Reports written after the conclusion of MSRE operations:

- Fission Product Behavior in the MSRE (ORNL-4865) [Compere et al., 1975]: This report contains much of the data taken during and after MSRE operations regarding the behavior of fission products in the system, as well as interpretation of the data.
- MSRE Systems and Components Performance (ORNL-TM-3039) [Guymon, 1973]: This report contains some high-level schematics for the final configurations of some systems and a detailed discussion of MSRE operating experience.
- MSRE Design and Operations Report – Part IIB, Nuclear and Process Instrumentation (ORNL-TM-729B) [Moore, 1972]: This report contains a thorough discussion of the instrumentation for almost all of the MSRE systems, as well as detailed drawings documenting the final configuration of each system.

4.1. Overview of MSRE Design and Inventories of Radioactive Material

Documentation of design details and operating experience for the MSRE are available in the references listed above. A high-level schematic of the major systems of the MSRE is shown in Figure 7; Figure 6 and Figure 8 provide views of the layout of the MSRE building and system.

---

[29] Each of the reports in this first list was an individual document published as a part of a series, and their title begins with the words "MSRE Design and Operations Report," which have been omitted here for clarity.

The approximately 8 MWth test reactor was designed, constructed, and operated at ORNL between 1965 and 1969. The reactor was fueled with UF_4 dissolved in a carrier molten fluoride salt. Heat from fission was generated in the fuel salt as it passed through the graphite channels of the reactor vessel, and then transferred to the molten fluoride coolant salt in the heat exchanger. Fission product gases were removed continuously from the circulating fuel salt by spraying a portion of the salt into the cover gas above the liquid in the fuel pump tank. From this space, the radioactive gas was swept out by a low flow purge of helium into the OGS. The coolant salt was circulated through a heat exchanger and radiator, where air was blown axially across the tubes to remove the heat. The air was then exhausted to the atmosphere via a stack. The MSRE was equipped with drain tanks for storing the fuel and coolant salts when the reactor was not operating. The salts were drained by gravity and transferred back to the circulating system by pressurizing the tanks with helium. The MSRE also included a simple processing facility for the offline treatment of fuel salt batches for removal of oxide contamination and for recovering the uranium. Additional auxiliary systems included:

- a helium cover-gas system with treatment stations for oxygen and moisture removal;
- two closed-loop oil systems for lubricating the bearings of the fuel and coolant pumps;
- a closed loop component cooling system (CCS) for cooling in-cell components using 95% N_2 and less than 5% O_2;
- several cooling water systems;
- a ventilation system for contamination control; and
- an instrument air system.

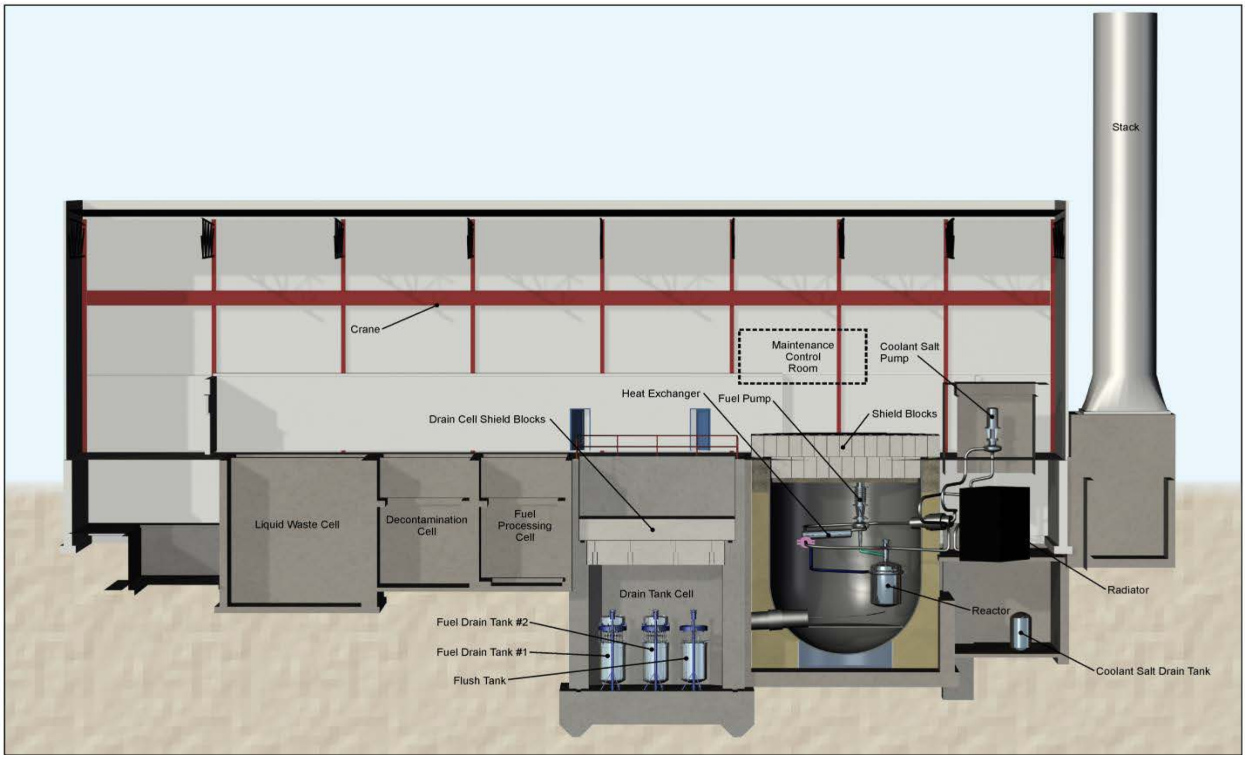


Figure 6: Elevation view of MSRE building [UCOR, 2016]

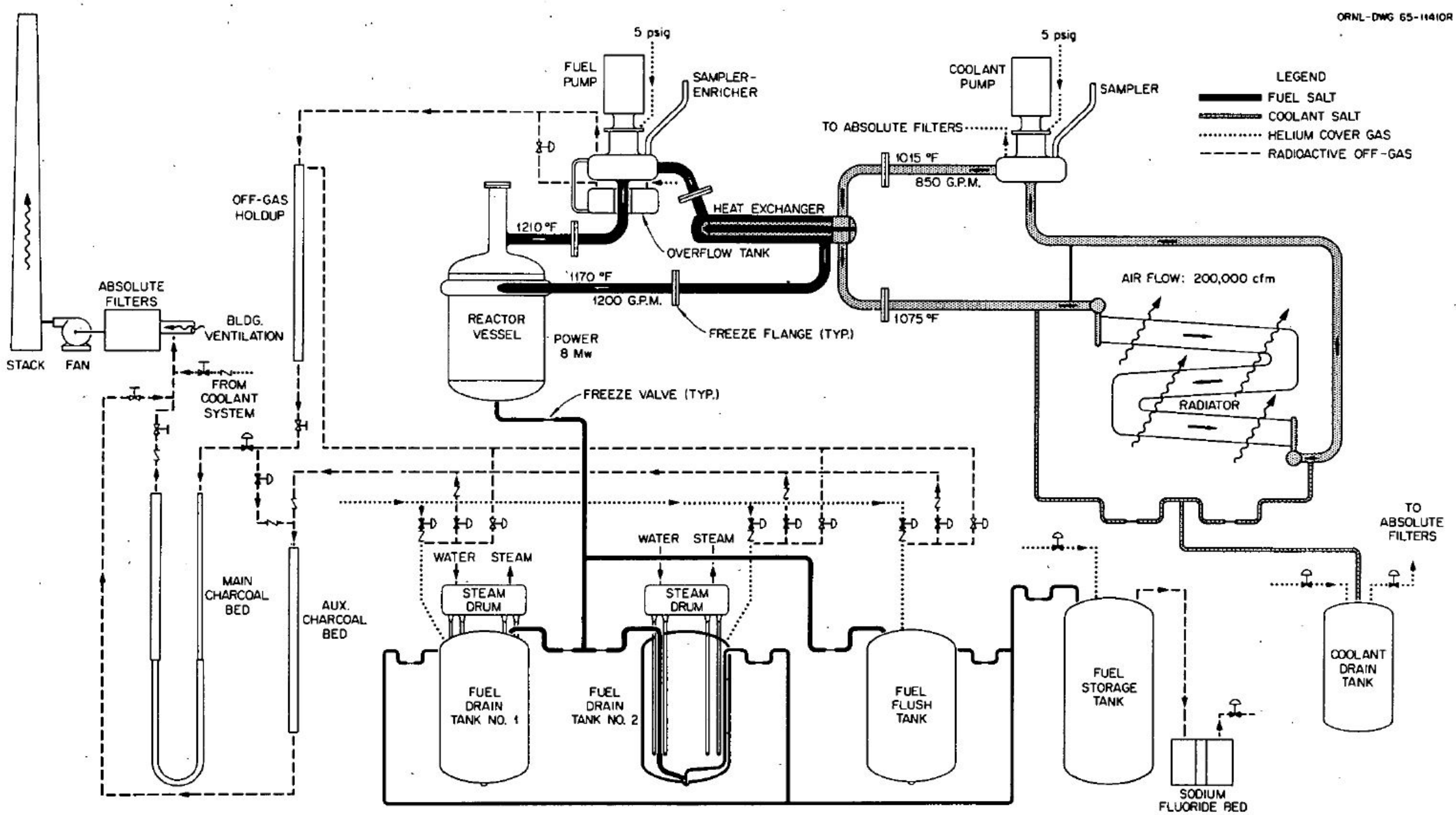
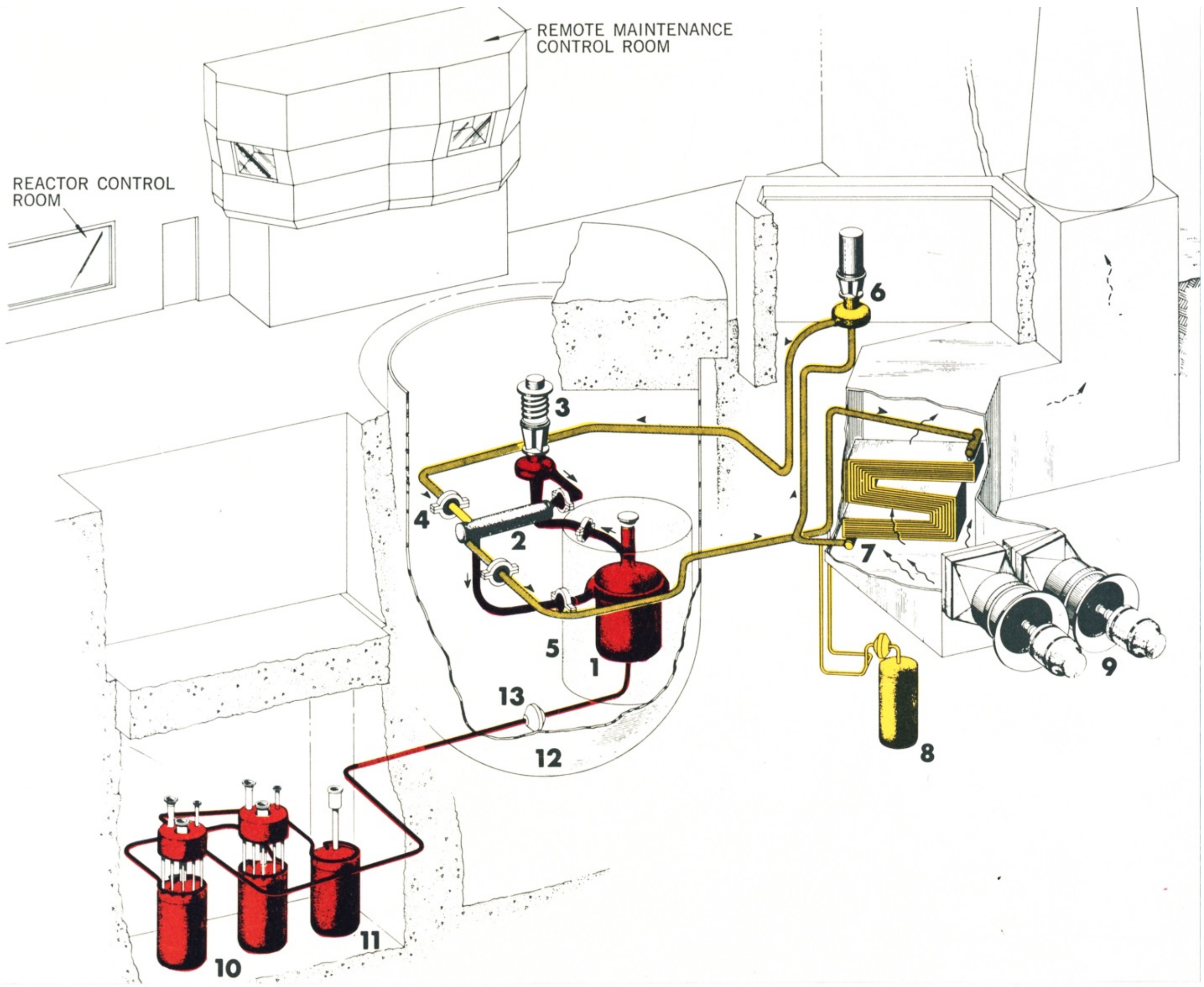


Figure 7: Flowsheet of the major components in the MSRE design [Guymon, 1973]



1. Reactor Vessel, 2. Heat Exchanger, 3. Fuel Pump, 4. Freeze Flange, 5. Thermal Shield, 6. Coolant Pump, 7. Radiator, 8. Coolant Drain Tank, 9. Fans, 10. Fuel Drain Tanks, 11. Flush Tank, 12. Containment Vessel, 13. Freeze Valve.

Figure 8: Detailed view of MSRE fuel salt and coolant salt systems [Robertson, 1965]

The preparation to conduct a technology-inclusive, RIPB approach for evaluating hazards in a design requires the identification and characterization of the different inventories of hazardous material that are present in a system design [NEI, 2019]. The distribution and movement of radioactive materials in the MSRE required the consideration of materials existing in different forms and different concentrations, which were contained by an array of different barriers to release. Review of the MSRE design information revealed that unique inventories could be defined on the basis of fundamental criteria, such as chemical composition and barriers to release.

The molten fluoride-based fuel salt had fission products and transuranics dissolved within it. During normal operations, the fuel salt was circulated around the fuel salt loop by the fuel salt pump; however, the approach to ensure subcriticality of the fuel and shut down the MSRE was to allow the fuel salt to drain via gravity from the fuel salt loop and into at least one of two fuel salt drain tanks. The fuel salt was kept in the fuel salt loop by a frozen plug of salt in a narrowed section of pipe (called a "freeze valve", see Chapter 6) during normal operations, and this plug was thawed to enact a fuel salt drain and reactor shutdown. Each drain tank had a dedicated freeze valve in which a plug of salt could be frozen to isolate the vessel from the fill/drain line once the fuel salt had drained to the tank(s).

When salt was being circulated by the fuel salt pump, a portion of the salt in the pump bowl was sprayed out of holes in a distributor ring, which allowed the noble gas fission products (mostly xenon and krypton) to vent from the salt [Robertson, 1965]. A helium sweep gas was introduced to the pump bowl to carry an estimated 10.36 TBq (280 Ci) each second out of the fuel salt loop and into the so-called "main" OGS. The main OGS was designed to provide holdup time to allow for the decay of all radioactive isotopes to insignificant amounts -- with the exception of ^{85}Kr, ^{131m}Xe, and ^{133}Xe. Volume holdups were used to allow for the decay of short-lived radioisotopes, while water-cooled charcoal beds were designed to provide average residence times of 90 days for xenon and 7.5 days for krypton [Robertson, 1965]. After being held up for this decay, the effluent of the off-gas disposal system was exhausted to the atmosphere after passing through filters (to retain solids) and after being massively diluted.

An "auxiliary" OGS was also provided to handle the intermittent, relatively large flows of helium, containing significant amounts of radioactive gases and particulates that were produced during salt transfer operations. Unlike the main OGS, the auxiliary OGS did not contain any volume holdups; however, the auxiliary OGS did have a charcoal bed that was located in the same water-filled cell as the main charcoal beds. The effluent of the auxiliary charcoal bed flowed into the same line as the effluent of the main charcoal beds before passing through the stack filters and being diluted and exhausted via the stack. Lines were provided to flow the off-gas from the fuel salt drain tanks to both the main OGS and the auxiliary OGS, with isolation valves in the lines that could be opened and closed to direct the gas flow.

Other significant inventories of radioactive material in the MSRE design would have been present at times in the fuel processing and handling equipment in the fuel processing cell and adjacent adsorber cubicle. It is important to note that because the MSRE did not perform online fuel salt processing, fuel salt would not have been in the fuel salt system and the fuel processing system at the same time. Although the radionuclides entered the fuel processing cell in the form of fuel salt, during fluorination (for recovery of U), many elements were volatilized out of the fuel salt. Thus, the salt remaining in the storage tank after uranium recovery, the off-gas from the fluorination process (including the volatilized UF_6), and the radionuclides removed from this off-gas by various components during processing were all forms of hazardous material that were present during batch processing of fuel, but were not present anywhere else in the MSRE system.

The material described above represents a significant majority of the total radioactivity that was in the MSRE plant; however, there were several other smaller distinct inventories of radioactive material. For completeness, these inventories are discussed in Section A.5.1 (of Appendix A).

The above discussion has focused exclusively on characterizing the inventories of radioactive material because the analysis in this dissertation is interested in assessing the risk associated with a release of radioactive material from the MSRE building to the environment. However, a number of other occupational hazards can be identified for the MSRE system. First and foremost, common industrial hazards such a poor ergonomics, trips/falls, noise, electricity, and movement of heavy or bulky materials would have been present for any MSRE worker. Because the melting point of the MSRE fuel salt was about 840°F (449°C), the operating temperature of the fuel salt system was well above this temperature, around 1200°F (649°F) [Guymon, 1973]; thus, heat would be another occupational hazard, and any water that makes contact with molten salt at this temperature may turn to steam with explosive effect. Molten salts in general create the hazard of a continuous ignition source for combustibles in their vicinity [Allen and Janz, 1980]. Individual components of the MSRE salt also introduce a variety of hazards including toxicity and corrosiveness [McFarlane et al., 2019]. In particular, BeF_2 is particularly hazardous, as beryllium is a highly toxic element and additional damaging effects can be added due to the production of HF resulting from hydrolysis [Allen and Janz, 1980]. Furthermore, F_2 gas was used at the MSRE for the removal of uranium (as UF_6) from the fuel salt; fluorine gas is very corrosive and toxic, and UF_6 can react vigorously with water [McFarlane et al., 2019].

However, as discussed in Section 1.4, the present research is not intended to demonstrate how the risks associated with chemical hazards could be analyzed and/or minimized. For LF-MSR designs, future efforts may be warranted to explore: (1) how chemical hazards are integrated, as necessary, into the overall facility risk profile characterized by the facility PRA model, and (2) how chemical consequences may need to be incorporated into LBE scenarios and their associated acceptance criteria.

4.2. Preparing for MSRE HAZOP Studies

As discussed in Section 3.2 of this dissertation, a starting point for developing a RIPB model to analyze ES&H risks in a reactor design, especially one at an early stage of design, can be the performance of a qualitative PHA study using one of several PHA methods that are recommended by both the nuclear [ASME/ANS, 2013] and chemical process industries [CCPS, 2008]. Due to the level of detail available regarding the MSRE design, and the intention to continue on to quantitative risk assessment, the HAZOP method was selected as the first PHA method used in this demonstration, as consistent with guidance in [ASME/ANS, 2013]. The objectives of the HAZOP analysis included the gathering of qualitative insights about risks associated with the MSRE design and to support the development of more quantifiable models of risk. In order to conduct a HAZOP study, it is necessary to divide the reactor design into analyzable sections or "nodes." [CCPS, 2008; Crawley and Tyler, 2015] Based on a review of MSRE design information, the following 21 nodes were identified based on primary function and nominal operating conditions:

- Fuel salt loop
- Fuel salt drain/fill system
- Fuel salt processing equipment
- Coolant salt loop
- Coolant salt drain/fill system
- Sampler-enricher system
- Cover gas system
- Leak detection system
- Fuel salt off-gas system
- Coolant salt off-gas system
- Containment ventilation system
- Component cooling system
- Secondary component cooling system
- Instrument air system
- Treated cooling water system
- Tower cooling water system
- Vapor condensing system
- Liquid waste system
- Drain tank afterheat removal system
- Salt pump lube oil system
- Electrical system

Due to funding and time constraints, it was not possible to conduct a complete HAZOP study on each node; accordingly, it was necessary to select the nodes of the MSRE that were of highest priority to be the subject of a HAZOP study. Some of the nodes identified in the MSRE do not differ substantially from systems with significant industrial experience (e.g., tower cooling water system, instrument air system) and others of the nodes may not be common to modern commercial MSR designs (e.g., the sampler-enricher). Additionally, because PRA models are typically developed for a specific combination of radioactive material inventory, POS, and hazard group [ASME/ANS, 2013], an important step of system characterization was to develop an understanding of which nodes would contain or interface with the significant inventories of radiological materials within the MSRE design. Performing a PHA on these nodes will likely help assess the ES&H hazards and risks of most interest to LF-MSR designers and regulators, since the consequences of event sequences associated with the failure of barriers in these nodes have the potential to be more severe than those associated with the failure of barriers in other nodes. Based on the above considerations, the MSRE nodes selected to be analyzed using the HAZOP method were the main MSRE OGS, the fuel salt processing equipment, the fuel salt loop, and the CCS.

The first three of these systems are home to the major inventories of radioactive material described in Section 4.1. Although the MSRE CCS did not contain a significant radioactive material inventory during normal operations, the system performed functions that will likely need to be addressed in most or all MSR designs, was integral to safe operation of the MSRE, and had not been the subject of detailed prior hazard evaluations or risk assessments. In the MSRE design, the CCS interfaced with the reactor cell atmosphere, which could become contaminated if radionuclides from the fuel salt loop or OGS were transported past the first barrier to their release. The MSRE CCS also had a direct interface with the MSRE stack and the environment.

Also discussed in Section 3.2, another task that is performed during the preparation for a PHA study is the identification of system parameters to be considered during the study. During a HAZOP analysis, these parameters are combined with guidewords to generate the deviations used to analyze the system [CCPS, 2008; Crawley and Tyler, 2015]. 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 as an effect of a failure. Because the relevant parameters that could indicate or cause hazardous scenarios will vary based on specific design details, care should be taken to ensure that the design intention of each node and the overall system is carefully considered [Crawley and Tyler, 2015].

The relevant top-level phenomena considered during the study of the MSRE were (in no particular order):

- Temperature
- Pressure
- Flow
- Level/weight
- Reactivity
- Radiological Inventory
- Chemical/Physical property changes

The first four items on the foregoing list are common process parameters that are typically measured in real time and provided to system operators to indicate system condition and performance. Trends in these variables could indicate off-normal situations and lead to damage of components. Reactivity and radiological inventory were included based on the NRC's discussion of how to conduct PHAs for fuel cycle facilities [NRC, 2001]. Criticality (due to reactivity transients) and radioactive material can produce other hazards (e.g., heat and radiation dose) that should be considered during the analysis of a nuclear system. Finally, chemical and physical property changes were identified as important phenomena to consider during the operation of an LF-MSR. For example, the chemical composition of LF-MSR fuel salt can affect the transport of heat, corrosion rates, and the solubility of certain fission products. This final parameter was determined by review of molten salt literature as well as hazard assessments of other advanced reactor technologies [Southern Company, 2019a].

4.3. Conducting MSRE HAZOP Studies

The HAZOP studies of the MSRE were performed by a team of subject matter experts[30] that spanned a broad range of relevant technical expertise and included engineering and ES&H risk assessment experts with a thorough understanding of the system design. Additionally, various members were selected for the team based on their extensive knowledge and experience in fields including: nuclear engineering and physics, chemical process engineering, materials science, power plant maintenance and operations, mechanical engineering, and health physics. The objective of the team was to comprehensively and systematically analyze the MSRE design information to identify possible off-normal scenarios of safety significance.

The first step of the HAZOP study once the team was assembled was to ensure that each member of the team had a full understanding of the node to be analyzed. It was helpful to start

[30] Brief resumes of the MSRE PHA team members are displayed in Appendix C of this dissertation.

each study meeting with a presentation that educated or refreshed the study participants on details including node boundaries, function, components, operating parameters, and intended approach to operations and safety. This presentation also allowed for team members to ask for clarifications about certain aspects of the node. Once the details of the node had been reviewed, the study facilitator reviewed with the team the scope of the study, as well as the parameters and guidewords that had been identified to be used for the study.[31] Once the group was comfortable with the node, parameters, and guidewords, the facilitator began to lead the group systematically through the HAZOP study process. The structure of a HAZOP study was discussed thoroughly in Section 3.2.3 of this dissertation. The HAZOP analyses of the MSRE were aided by an assigned group scribe using an off-the-shelf software program [Lihoutech, 2014]. The study team had design information, such as flowsheets, schematics, and specifications, readily accessible during the study. Visual aids such as process flow diagrams and/or system schematics were particularly useful to help the team brainstorm potential causes of deviations. After identification, each cause was discussed individually by the group. The facilitator helped lead the team to a consensus on the consequences of each cause, the safety systems that would prevent or mitigate the cause, and any resulting action items from the discussion of the cause.

During the MSRE HAZOP studies, it was found that comprehensively documenting the unmitigated effects of a deviation within a section was particularly beneficial to the subsequent process of translating HAZOP results to ET models. 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 nodal interface ensured that the event sequence could be fully analyzed using HAZOP results tables from more than one node. Because the goal of the research conducted for this dissertation was to eventually construct quantitative fault trees to estimate the probability of event tree pivotal events and event sequences, it was also helpful to differentiate between automatic system responses and anticipated operator actions in response to system indications. This differentiation facilitated the incorporation of Human Reliability Analysis (HRA) [Swain and Guttmann, 1983] within the models of quantitative risks. Finally, a key to performing a consistent PHA was ensuring that the effects of all deviations or equipment failures were analyzed using consistent assumptions and that these assumptions were thoroughly documented during the evaluation.

---

[31] At times, the need for expansion, contraction, or other adjustment to nodes, parameters, or guidewords was revealed over the course of the study. Subsequent changes were made with the consensus of the group, and once a decision had been made to make a change, it was reviewed for its impact on any previous analysis results.

The documentation of the HAZOP study results took the form of a table; an excerpt of the MSRE OGS HAZOP study results is provided in Appendix B of this dissertation. By its nature, a PHA is a design and safety analysis tool, not a final product. As previously discussed, it is a precursor to the selection of potential risk-significant scenarios as well as the construction of quantifiable models of risk (e.g., event trees). A PHA exercise is focused, and can be efficient and relatively fast-paced, so the documentation of the results can be somewhat abbreviated and are intended to be of greatest benefit to the design and operations personnel who were major participants in the study. Any attempt to document the details of all the group's rationales for the table contents would be voluminous and overly time-consuming, and would be a distraction. The quality assurance measures taken to assure the validity of the MSRE HAZOP study results can be found in Appendix C.

4.4. Results of MSRE HAZOP Studies and Related Design Insights

4.4.1. MSRE Fuel Salt Loop

A representative schematic of the MSRE fuel salt loop is provided in Figure 9. The performance of the HAZOP study of the MSRE fuel salt loop benefitted from the fact that it was chronologically executed after the HAZOP studies of the OGS, CCS, and fuel processing system;[32] thus, the HAZOP team was most familiar with the study procedure and details of the MSRE design during the HAZOP study of this node. Even so, the tight coupling of certain nuclear physics in a liquid fuel made it difficult for the team to conclusively determine consequences associated with some deviations without additional calculations and/or models.

For example, in the case of increased heat removal by the coolant salt system in the heat exchanger, the negative temperature coefficient of the fuel salt would result in an increase in reactor thermal power to match the demand from the coolant salt loop as the cold fuel salt entered the reactor vessel. This increased heat generation would then produce an increase in the temperature of the fuel salt exiting the reactor vessel. Safety systems that were intended to protect the fuel salt loop from the consequences associated with high power and/or temperature included a high outlet temperature reactor scram and fuel salt pump trips associated with high and low level trips in the fuel salt bowl; however, the relevance of these safety systems and their usefulness depend on the exact magnitude and timescale of the competing phenomena (i.e., temperature decrease vs. power increase vs. temperature increase). Therefore, for certain

[32] The discussion of the MSRE fuel salt loop HAZOP study is presented here first because (as discussed in Section 2.4) there have been other LF-MSR safety assessment efforts focused on the radioactive material inventory in fuel salt loops; thus, the author considers the results of this HAZOP study to be "less interesting" than the others.

deviations, it was difficult to anticipate the MSRE system response with a high level of certainty.

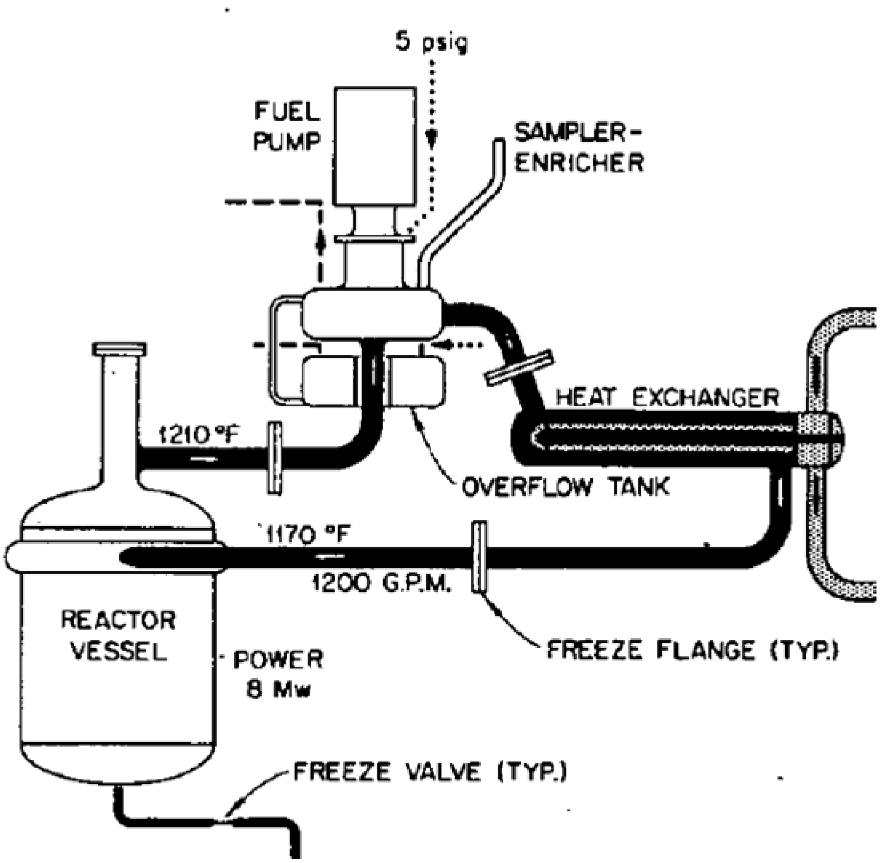


Figure 9: Schematic of MSRE fuel salt loop [Guymon, 1973]

A total of 66 deviations were evaluated and documented for the fuel salt loop. One unique aspect regarding the fuel salt loop is that all of the transients and accidents evaluated in the original MSRE Preliminary Hazards Report [Beall, 1962] and Safety Analysis Report [Beall et al., 1964] related to the inventory of the radioactive material in the fuel salt loop. Consequently, the HAZOP study results for the fuel salt loop identified more deviations that had already been considered by the MSRE team in the original ORNL documentation -- compared to the results from the studies on any of the other nodes. However, the HAZOP study team did identify a number of potentially risk-significant deviations concerning the fuel salt loop that had not been previously covered in the MSRE documentation.

For example, an interface with the CCS node was identified to be capable of propagating effects from a deviation in the CCS node to the fuel salt loop. A loss of component cooling gas flow could compromise the ability to maintain a frozen plug of salt in the main freeze valve below the reactor vessel. The heat conducted into the valve body from the pipeline heaters and the circulating fuel salt could melt the plug, which would result in an unscheduled drain of the fuel salt loop. Although the drain tanks were designed to have geometry such that the concern of criticality in the drain tank would be limited, the fuel salt would be at a high temperature and the decay heat would be at a maximum if the reactor was drained from full power [Guymon, 1973]. Because of the potential risk-significance of this failure, the reliability and safety associated with proper functioning of the MSRE freeze valve is evaluated in Chapter 6 of this dissertation. Additionally, any cause of increased heat removal by the CCS could increase the size of the frozen salt plug in the freeze valve, and this would increase the amount of time needed to thaw the freeze valve in the case that the reactor needed to be drained.

Finally, in an LF-MSR design, it is likely that the fuel salt chemistry will play a significant role in system performance, and the HAZOP study of the MSRE fuel salt loop identified that it could also be the cause of system deviations or upsets that could challenge barriers. For example, deposition of materials from the fuel salt onto surfaces in the system could affect the ability to transfer heat, change the redox conditions of the salt and increase corrosion rates, foul sensors and prevent an accurate indication of process conditions, and plug small lines. One chemistry-related issue experienced by the MSRE was the leakage of lubricating oil from the fuel salt pump into the fuel salt in the pump bowl. This lubricating oil broke down in the pump bowl and caused plugging of the off-gas line from the pump bowl [Guymon, 1973]. Another more serious chemistry-related deviation that was postulated, but not observed during operation, was oxygen contamination of fuel salt that was significant enough to alter redox conditions such that uranium precipitation would be possible [Beall and Guymon, 1964].

4.4.2. MSRE Fuel Salt Processing System

A representative schematic of the MSRE fuel processing system is provided in Figure 10. It is worth noting that the fuel processing system only performed the full process of fluorinating a batch of salt two times. The system design that was analyzed in the HAZOP study was the design that resulted after the system shakedown tests, and the schematic in the figure incorporates changes detailed by Lindauer [1969] that were made from the original system design (presented in [Lindauer, 1967]). A total of 88 potential deviations were identified and evaluated for the components involved in the fluorination of MSRE fuel salt for the recovery of uranium. The MSRE Preliminary Hazards Report [Beall, 1962] and SAR [Beall and Guymon, 1964] did not contain the discussion of any hazards relating to inventories of radioactive material in the fuel processing system. The only publicly available document containing any discussion of hazards during operation of the fuel processing equipment is a small section in a separate report by Lindauer [1967]. Thus, almost all of the deviations discussed and analyzed during the MSRE HAZOP study represented hazards that were not covered in the original MSRE documentation.

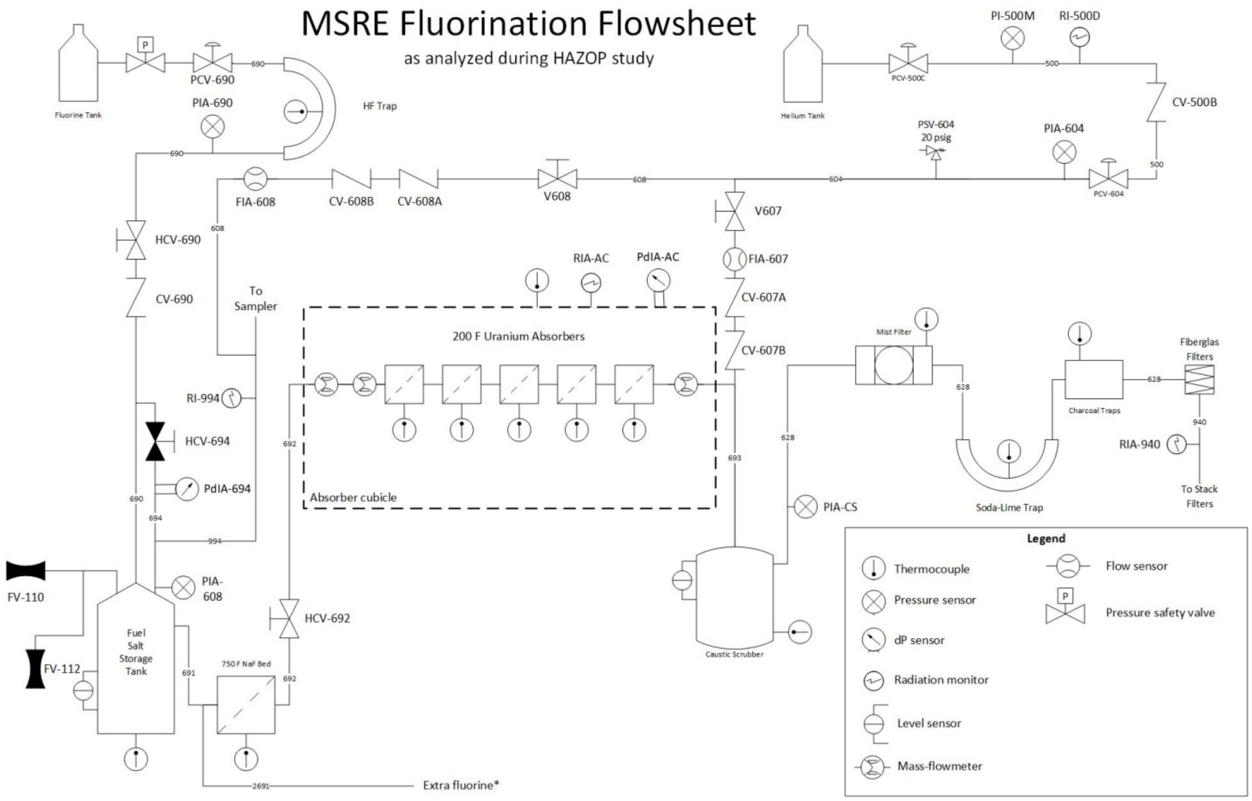


Figure 10: Schematic of MSRE fuel processing system

A major issue experienced during the operation of the fluorinating equipment identified by the MSRE team was corrosion [Lindauer, 1969]. The high concentration of fluorine in the gas stream attacked the Hastelloy-N[33] structural material and increased the amount of impurities (such as NiF_2, FeF_2, and CrF_2) in the fuel salt. Additionally, fluorination in the fuel salt storage tank allowed for the formation of MoF_6, which is volatile and therefore was carried out of the fuel salt storage tank along with the other volatile species (such as UF_6). Two important deviations identified during the HAZOP study of this node pertain to corrosion concerns. Increased fluorine concentration in the fuel salt storage tank could be caused by a failure of the fluorine control valve. If no corrective actions were taken, this increase in fluorine concentration would likely increase the corrosion rate in the fuel salt storage tank, which would increase the production rate of MoF_6. This MoF_6 in the process gas stream could compete with UF_6 for absorption in the uranium absorbers [Lindauer, 1967] or produce hydrated oxides of Mo that

[33] The MSRE literature refers to this material as INOR-8; however, when the material was licensed to Haynes International the trade name for the material became Hastelloy N®. This material is also sometimes referred to as UNS 10003 or Alloy N.

could cause an obstruction in lines downstream of the caustic scrubber [Lindauer, 1969]. Additionally, because Mo has a similar heat capacity to U, the accuracy of the mass-flowmeters used to monitor the uranium content of the gas stream entering and exiting the absorbers could be negatively impacted [Lindauer, 1969].

The second deviation related to increased corrosion rates could be caused by a loss of helium flow in the gas flow upstream of the caustic scrubber. This loss of helium flow would likely increase the rate of corrosion in the dip tubes of the caustic scrubber. Although means to monitor plugging was provided, plugging of the dip tube lines was experienced during operation of the fluorination equipment despite redundant lines [Lindauer, 1969]. It is possible that increased corrosion rates in the dip tubes could result in plugging significant enough to produce reverse flow through the uranium absorbers. This reverse flow was identified during the HAZOP study to be a possible cause of disrupted process flow and the possible desorption of UF_6 or other radionuclides that were previously deposited in the absorbers.

During the study, multiple deviations regarding the temperature parameter were identified to possibly affect the inventories of radioactive material in different components in the node. Decreased heat removal from the uranium absorbers could reduce the amount of UF_6 removed from the process stream by the absorbers, since the capacity of NaF for UF_6 varies inversely with temperature [Lindauer, 1967]. Additionally, decreased heat addition to the NaF bed could lead to deposition of UF_6 in the bed, which does not have mass-flowmeters upstream to allow for indication of UF_6 removed from the process stream by this component. Thus, the only indication to the operators that UF_6 is being absorbed in the NaF bed would be indication of temperature in the bed. Furthermore, an action item developed during the HAZOP study was to investigate how criticality is prevented in the NaF bed and the uranium absorbers. While the caustic scrubber contains a soluble neutron poison [Lindauer, 1969], there is no discussion of other design features to prevent criticality in the bed or the absorbers.

One potentially risk-significant source of hazardous material that was identified during the HAZOP study was the caustic solution in the scrubber. Due to the changes made to the system before operation, the scrubber became the main component responsible for the capture of iodine and fluorine [Lindauer, 1969]. Because these changes were made after the system was originally designed, there is limited information regarding analysis of the contents of this component. Multiple deviations that could result in a release of the material from the scrubber to the fuel processing cell were identified during the study, including violent reactions in the scrubber or decreased heat removal from the scrubber. It is possible that the release of this material to the fuel processing cell could volatilize iodine (which could pose a radiological hazard) or fluorine (which could pose a chemical exposure hazard).

Finally, as mentioned above, the role of fuel salt chemistry in the safe and reliable performance of an LF-MSR system highlights the value of online sampling. The MSRE did not have the capability to analyze the conditions of the salt during operations and relied on batch samples taken from the system and analyzed in another ORNL facility. As an alternative to online salt chemistry measurements, the MSRE team used surrogate measurements, and the HAZOP study of the MSRE fuel processing system identified deviations that could affect the efficacy of these surrogates to adequately indicate system conditions. For example, incorrect calibration of the mass-flowmeters used during fluorination could lead to material accountability errors when calculating how much uranium has been removed from the fuel salt.

4.4.3. MSRE OGS and CCS

A representative schematic of the MSRE OGS/CCS is provided in Figure 11. During the HAZOP studies, a total of 35 potential deviations were identified and evaluated for the MSRE OGS, and a total of 40 deviations were identified and evaluated for the CCS. Although the CCS does not contain a significant radioactive material inventory during normal operations, the system: performs functions that will likely need to be addressed in most or all MSR designs, was integral to safe operation of the MSRE, and has not been the subject of detailed prior hazard evaluations or risk assessments. The OGS and CCS were not the subject of much discussion in the original MSRE Preliminary Hazards Report [Beall, 1962] or SAR [Beall et al., 1964]. Most of the deviations identified in the HAZOP study results were not covered in the original ORNL MSRE documentation; however, some of them are informed by documentation of MSRE operational experience [Guymon, 1973].

Unlike the MSRE fuel salt loop, a portion of the boundary of the OGS during normal operations was formed by a functional barrier. Rather than providing a structural barrier to prevent transport of any material through the charcoal beds, the activated carbon retained radionuclides for an extended period of time via adsorption, and this residence time allowed for the decay of radionuclides (such as Kr and Xe). The results of the HAZOP study identified many deviations from normal operating conditions that would decrease the effectiveness of this functional barrier. For example, ignition of the activated carbon due to volatile organic materials in the off-gas stream or a rapid expansion of water vapor due to an inleakage of cooling water could lead to a reduction in the effectiveness of the carbon bed and lead to an increased rate of transport of radioactive material past the normal OGS boundary [Zerbonia et al., 2001]. In addition, any cooling water that leaks into the bed has the potential to react with any remaining fluorine from the fuel salt and produce HF, which is toxic and corrosive. The scenario of water intrusion into the charcoal beds poses a possible occupational hazard as well as a method to damage components important to the control of radioactive material.

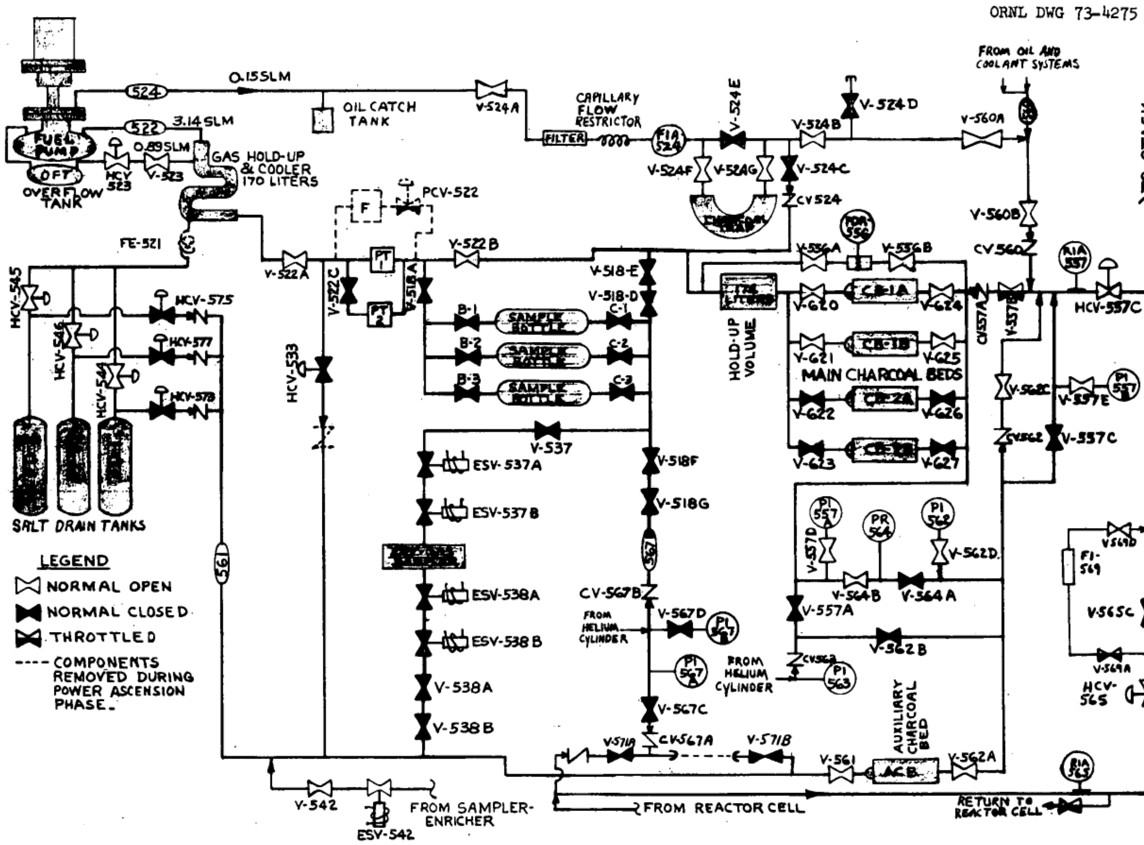


Figure 11: Schematic of MSRE OGS [Guymon, 1973]

Over the course of all the MSRE HAZOP studies, several deviations were identified that suggested that interfaces between gas and salt pose potentially hazardous conditions that could challenge functions intended to protect barriers of hazardous material. MSRE operational experience suggested that the corrosion rate at these surfaces could be significantly higher than corrosion rates encountered elsewhere in the system [Guymon, 1973], and it is also possible that the deposition rate of impurities from the salt on structural materials could be higher at these locations. The MSRE team also had a significant number of complications related to fuel salt “aerosol” or “mist,” which was caused by bubbling and splashing around the interface between the fuel salt and the cover gas in the fuel salt pump bowl. This mist could potentially cause an increased rate of material transport from a fuel salt system to an off-gas system, which could result in plugging of small-diameter off-gas lines. Another scenario that was experienced during MSRE operation was thermal expansion of the fuel salt that was significant enough to allow fuel salt to overflow into the off-gas system in the fuel salt pump bowl [Guymon, 1973]. Because the coefficient of thermal expansion for the salts considered for use in MSRs is high, increases in level due to thermal expansion represent another potential cause of plugging in lines (especially small diameter off-gas lines). If a thermal expansion transient is significant enough, it is possible that any seals located above a salt/gas interface (e.g., fuel salt pump shaft seal) could be at risk of being compromised by the hot, radioactive salt.

Based on observations during MSRE operations, deviations that affect void fraction can have effects on the reactivity in the core [Guymon, 1973]. This interaction places a higher significance on the interface between the OGS node and the fuel salt loop. Any scenario that can increase or decrease the amount of volatile fission gases removed from the fuel salt, including plugging in the off-gas line, plugging of the stripping spray rings in the pump bowl, or high cover gas supply pressure, could also affect reactor power level, pressure, and temperatures in the fuel salt loop.

The discussion of the performance of the OGS system, throughout the four years of MSRE operations, indicated that the system experienced frequent plugging. Modifications made to the system after the initial design included the removal of an automated pressure control valve and addition of a particle trap to reduce particulates entrained in the effluent from the fuel salt pump bowl. Several methods were developed to unplug lines, including using heat and back pressure as well as mechanical methods. In addition, the system design featured a number of sample ports, which provided ready access to the system, if needed.

4.5. Relationships between MSRE HAZOP Studies and Other Analyses

As evident in Figure 1, the results of the MSRE HAZOP studies are used as inputs for the other elements of the methodology demonstrated in this dissertation. The HAZOP study results of the fuel salt loop, the OGS, and the fuel processing system identified initiators of potentially risk-significant event sequences that are used to contribute to a comprehensive and systematic search for PIEs in Chapter 5. The results of the HAZOP study on the CCS and (to a lesser extent) the fuel salt loop are used to inform the assessment of freeze valve performance and reliability presented in Chapter 6. Finally, event sequences associated with a group of PIEs associated with the radioactive material inventory in the main OGS are analyzed in Chapter 7; the results from the HAZOP studies of the OGS and the CCS were fundamental to the building of the models used.

CHAPTER 5, IDENTIFICATION OF POSTULATED INITIATING EVENTS FOR THE MSRE DESIGN

As introduced in Section 3.2, an important effort that must be undertaken to gain a complete understanding of the risk profile of a design is a comprehensive and systematic search for occurrences that have the potential to initiate scenarios that may result in undesirable consequences within the system. Within the risk assessment community, these occurrences are referred to as "initiators" or "initiating events (IEs)." In the building of models to quantitatively evaluate risk, IEs are used in event sequence[34] modeling and ETA to support efforts to characterize the risk associated with event sequences of interest. However, because the definition of risk also involves defining consequences of interest, the specific scope of what is considered to be an initiating event can vary among different industries. In the most general sense, an IE is a deviation from normal conditions that could, if not responded to in a correct and timely manner, lead to a consequence of concern [CCPS, 2015; Modarres, 2006]. In the analyses presented in this chapter, the consequence of concern is the transport of radioactive material through a barrier that is intended to prevent its release. This work will use a definition based upon the definition used in the Non-LWR PRA Standard [ASME/ANS, 2013]; an IE is "a perturbation to the plant that challenges plant control and safety systems whose failure could potentially lead to an undesirable end state and/or radioactive material release." However, the IAEA [2019] notes that the term "initiating event" is often used in relation to event reporting and analysis, while "*postulated* initiating event" is more appropriate during the consideration of hypothetical events at the design stage. As such, the events identified in the present work for the MSRE are considered to be postulated initiating events (PIEs).

Because of the extensive operating experience associated with LWRs, generic IE lists are available for LWRs (e.g., [IAEA, 1993; Mackowiak et al., 1985; McClymont and Poehlman, 1982]). By contrast, the LF-MSR is an example of an advanced reactor technology that could benefit from a comprehensive identification of PIEs. No commercial LF-MSRs have been operated, and very little work has been conducted in the area of LF-MSR safety assessment even when compared to other non-LWR technologies -- such as VHTRs [GA Technologies, 1987; NRC, 1989] and SFRs [GE Hitachi Nuclear Energy, 2017; NRC, 1994]. The current body of knowledge documenting LF-MSR safety assessments was discussed in Section 2.4 of this dissertation. Some preliminary searches for LF-MSR PIEs have been based upon prior operating experience [Beall, 1962], literature surveys [Geraci, 2017], and loosely-structured brainstorming approaches [Holcomb et al., 2019]. The PIE identification efforts that have employed the use of

[34] An event sequence is comprised of an IE, the plant response to the IE (which includes a sequence of successes and failures of mitigating systems) and a well-defined end state [NEI, 2019].

more structured, systematic methods to identify PIES (e.g., the MLD approach or FFMEA) focused only on initiators that were applicable to the inventory of radioactive material in the fuel salt loop during normal operations [Gèrardin et al., 2019; Pyron, 2016].

As previously discussed, LF-MSR designs have the potential to have multiple significant inventories of radionuclides that are in forms not commonly experienced in other commercial nuclear reactor designs; these forms include soluble fission products dissolved in molten salt and volatile radionuclides in off-gas streams. Because these inventories of hazardous material present unique challenges to the barriers that are intended to prevent their release from the system, a thorough identification of PIEs could find occurrences that have not previously been considered for other reactor technologies. Thus, the objective of the analysis presented in this chapter is to systematically identify PIEs for the Molten Salt Reactor Experiment (MSRE). First, the methodology for the analysis of MSRE PIEs is defined. Then, the results of the MSRE PIE search are discussed, including the discussion of a MLD for MSRE PIEs. Finally, conclusions regarding these results and insights regarding the identification of PIEs in an LF-MSR design are presented.

5.1. Approach for Identifying MSRE PIEs

The approach to identify PIEs for the MSRE draws from guidance on PRA development [NEI, 2019; Southern Company, 2019a] and US nuclear industry standards [ASME/ANS, 2013]. Because this study is the first step towards a comprehensive evaluation of PIEs for the MSRE, the present analysis focuses only on the identification of internal PIEs (e.g., SSC failures) and does not enumerate PIEs that might be related to external events (such as flooding or seismic events). This prioritization of internal events in early safety analysis is consistent with international guidance [Wielenberg et al., 2017] and the Non-LWR PRA Standard [ASME/ANS, 2013]. The identification and evaluation of external events would need to be covered for a full scope risk assessment of a more mature design; however, this analysis is intended to demonstrate a tool that can be used to analyze a reactor design at a conceptual stage of design.

The development of an exhaustive enumeration of reactor specific PIEs begins with the identification and characterization of the different inventories of hazardous material that are present in a system design [ASME/ANS, 2013]. However, review of the MSRE design information in preparation for the HAZOP studies (see Chapter 4) suggested that unique inventories could be defined for different POSs of the MSRE on the basis of fundamental criteria, such as chemical composition and barriers to release. As such, consistent with guidance in the Non-LWR PRA Standard [ASME/ANS, 2013], an analysis of POSs[35] was performed for the MSRE as a prerequisite to a comprehensive search for PIEs.

According to MSRE design documentation [Tallackson, 1968], the following five POSs (referred to in the MSRE documentation as "operational modes") were defined for the MSRE control system:[36]

1. Off: The reactor is shut down, with control rod withdrawal prohibited. The fuel salt is secured in the drain tanks.
2. Prefill: Salt transfers among the drain tanks or to/from the Fuel Storage Tank (FST) in the fuel processing system are permitted during Prefill. The fuel salt loop is maintained empty.
3. Operate: Fuel salt is being transferred from one of the drain tanks to the fuel salt loop via the fuel salt drain/fill line.
4. Operate-Start: Operate-Start is when the reactor loop has been filled to the correct level and the reactor drain valve is frozen; however, reactor power is below 1.5 MW.
5. Operate-Run: This mode is obtained when conditions requisite for operation at power levels greater than 1.5 MW have been met, and it is mutually exclusive from Operate-Start.

The status of the fuel processing system is not covered by Tallackson [1968], but it was discussed by Lindauer [1967]. Additionally, as part of the development of PIEs for FHRs[37], [Allen et al., 2013] analyzed several different operating modes and states that are applicable to a more comprehensive analysis of the MSRE. These reactor modes and states are distinct from the foregoing POSs in how the systems are arranged and how they operate (including control interlocks, valve positions, etc.). Accordingly, the following additional POSs can be defined for the MSRE:

6. Maintenance
    a. Purposeful disruption of the second barrier to release to allow for maintenance procedures. For remote handling equipment to reach some of the components in the reactor or drain tank cells, it may be necessary to remove the concrete roof shielding plugs. In this POS, the fuel salt system is most likely in the Off state; however, the containment ventilation may be in an off-normal arrangement

[35] The definition of Plant Operating State for the purposes of this dissertation is presented in the Glossary of Relevant Nuclear Engineering Terms.
[36] More comprehensive descriptions of the MSRE POSs are given by Tallackson [1968].
[37] i.e., solid-fueled, molten salt-cooled reactors

during maintenance operations (e.g., air being exhausted from the reactor or drain tank cells to cause a down-flow of air through the openings in the cell roof).

7. Fuel processing
    a. Recovery of uranium (i.e., Fluorination): To volatilize and remove the uranium from the fuel/flush salt (in addition to other fission and activation products), the salt in the fuel salt storage tank can be fluorinated. The resulting UF_6 is then captured on NaF absorbers outside of the fuel processing cell.
    b. Removal of oxides: The fuel or flush salt in the fuel storage tank can be treated by a mixture of H_2 and HF to remove oxides in the fuel that result from contamination by moisture or oxygen. This POS is considered distinct from the recovery of uranium because (1) different chemicals are used to treat the salt in the storage tank and (2) different chemical compounds are volatilized from the salt (and then enter the process line).
8. Experimental
    a. Fuel salt sampling: Because the MSRE was a test reactor, the system was intended to be operated (often temporarily) in operating modes that may only adjust the configuration or control scheme slightly from the other POSs described above. One such operating state was the process of obtaining a fuel salt sample from the bowl of the fuel salt pump using the sampler-enricher. Because this sampler-enricher penetrated both the first and second barriers to the release of fuel salt, the process of taking a sample would change which two barriers in the sampler-enricher component are actively performing the first and second barrier functions. Additionally, the potentially radioactive off-gas from the sample collection process is vented to the auxiliary OGS.

Table 7 provides an overview of the major unique POSs identified for the MSRE and the associated inventories of radioactive material. The table does not cover Operate-Start because the only major difference from Operate-Run is the power level of the reactor. Additionally, fuel salt sampling and fuel salt transfers (i.e., Prefill) are not included in the table because the barriers to release can change during different procedures occurring during these POSs; thus, these POSs require further decomposition.

Table 7: Major Plant Operating States (POSs) of the MSRE

Plant Operating State (POS)	Major Inventories of Radioactive Material	Minor Inventories of Radioactive Material	Status of Selected Barriers	Notes
Operate-Run (Normal Operations)	Fuel salt in fuel salt loop Volatile radionuclides in main OGS line	Fuel salt heel in drain tank Liquid waste storage Tritium	Fuel salt: FV-103 frozen, FV-105 and FV-106 thawed OGS: main charcoal beds	Safety system response triggers thawing of FV-103 (drain to drain tank via gravity)
Operate (Fuel salt loop filling)	Fuel salt in Drain Tank, fill/drain line, and fuel salt loop Volatile radionuclides in auxiliary OGS line	Liquid waste storage Tritium	Transfer FVs frozen, FV-103 thawed OGS: auxiliary charcoal bed	He pressure used to fill system Coolant salt loop filled
Off (Shutdown)	Fuel salt in Drain Tank(s) Volatile radionuclides in auxiliary OGS line	Heel/deposits in fuel salt loop Deposits in main OGS line/components Liquid waste storage Tritium	Transfer FVs, FV-104 and FV-105 frozen OGS: auxiliary charcoal bed	Heat removal by Afterheat Removal System; fuel salt can be in 1 DT or 2

Plant Operating State (POS)	Major Inventories of Radioactive Material	Minor Inventories of Radioactive Material	Status of Selected Barriers	Notes
Fuel salt processing (Fluorination)	Fuel in Fuel Storage Tank (FST) Volatile process flow in fuel processing line/components	Heel/deposits in fuel salt loop Heel in fuel salt DT(s) Deposits in OGS lines/components Liquid waste storage Tritium	Processing FV frozen Volatile radionuclides: processing charcoal trap	N/A
Maintenance	Fuel salt in Drain Tank(s) Volatile radionuclides in auxiliary OGS line	Heel/deposits in fuel salt loop Deposits in main OGS line/components Liquid waste storage Tritium	Similar to "Shutdown" Confinement barriers may change System may be opened	Fuel salt loop likely cold

The information displayed in Table 7 illustrates that the inventories of radioactive material that have the potential to be released are different for different POSs of the MSRE. Thus, in order to understand how the material could be released, the form and composition of each inventory needs to be evaluated and characterized. Once an understanding of the material has been developed, the barriers and supporting structures intended to prevent the release of the material must be defined [NEI, 2019]. The safety approach taken by the MSRE designers was to ensure that each inventory had two levels of independent barriers between the material and the environment [Beall et al., 1964]. A characterization of the inventories and discussion of the first level of barriers intended to prevent their release was presented in Section 4.1, above. A visual summary of this information for the radioactive material inventories in the fuel salt loop (during normal operations), the main OGS (during normal operations), and the fuel processing system (during fluorination) is depicted in Figure 12, Figure 13, and Figure 14, respectively.

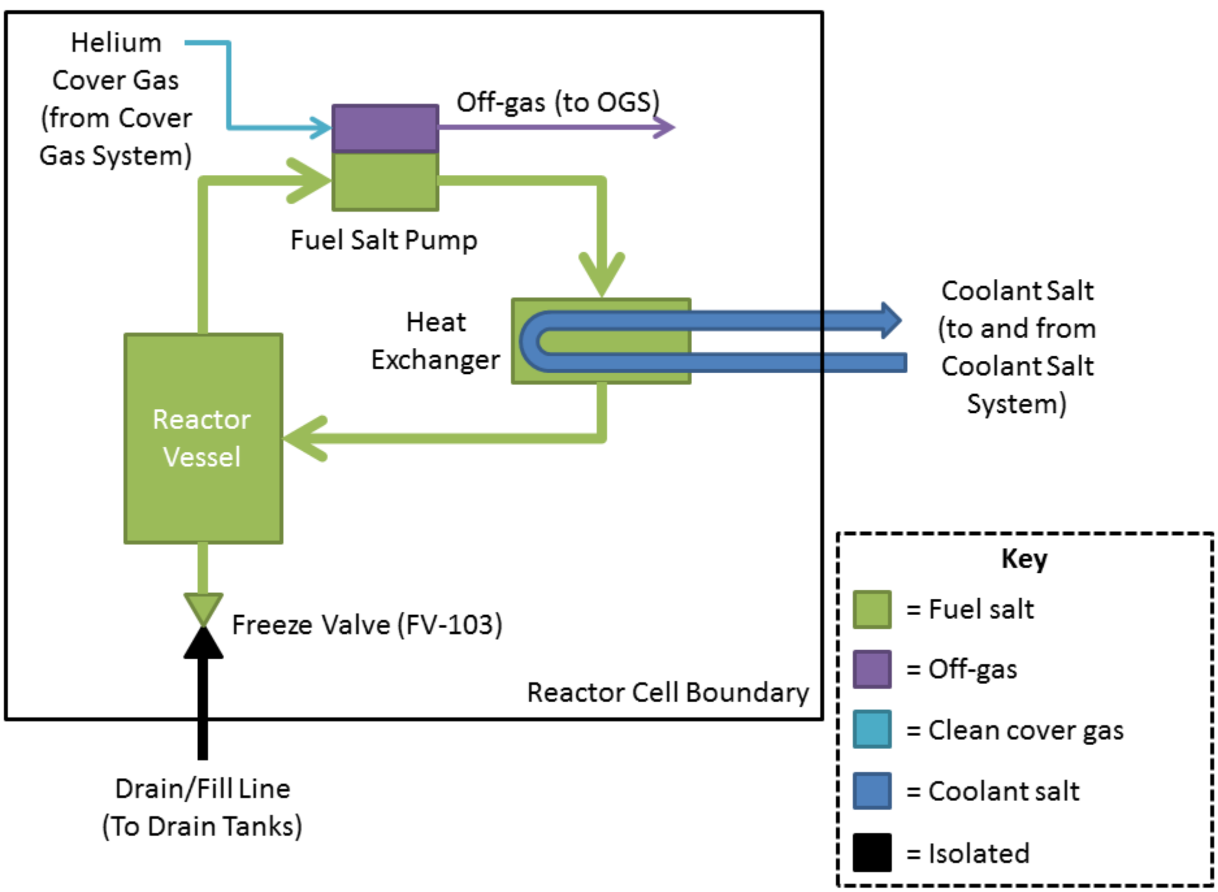


Figure 12: Schematic of barriers to release of radioactivity for MSRE fuel salt loop during normal operations

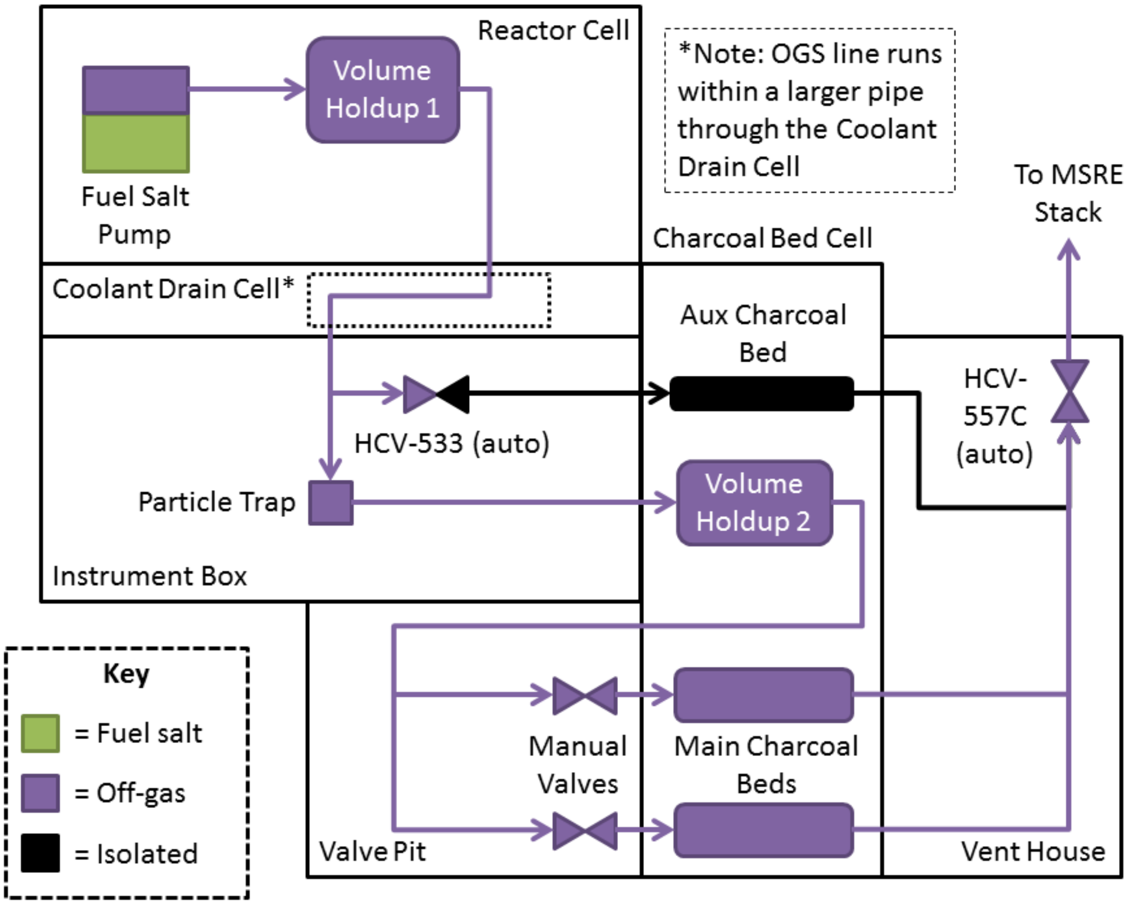


Figure 13: Schematic of barriers to release of radioactivity for MSRE main OGS during normal operations

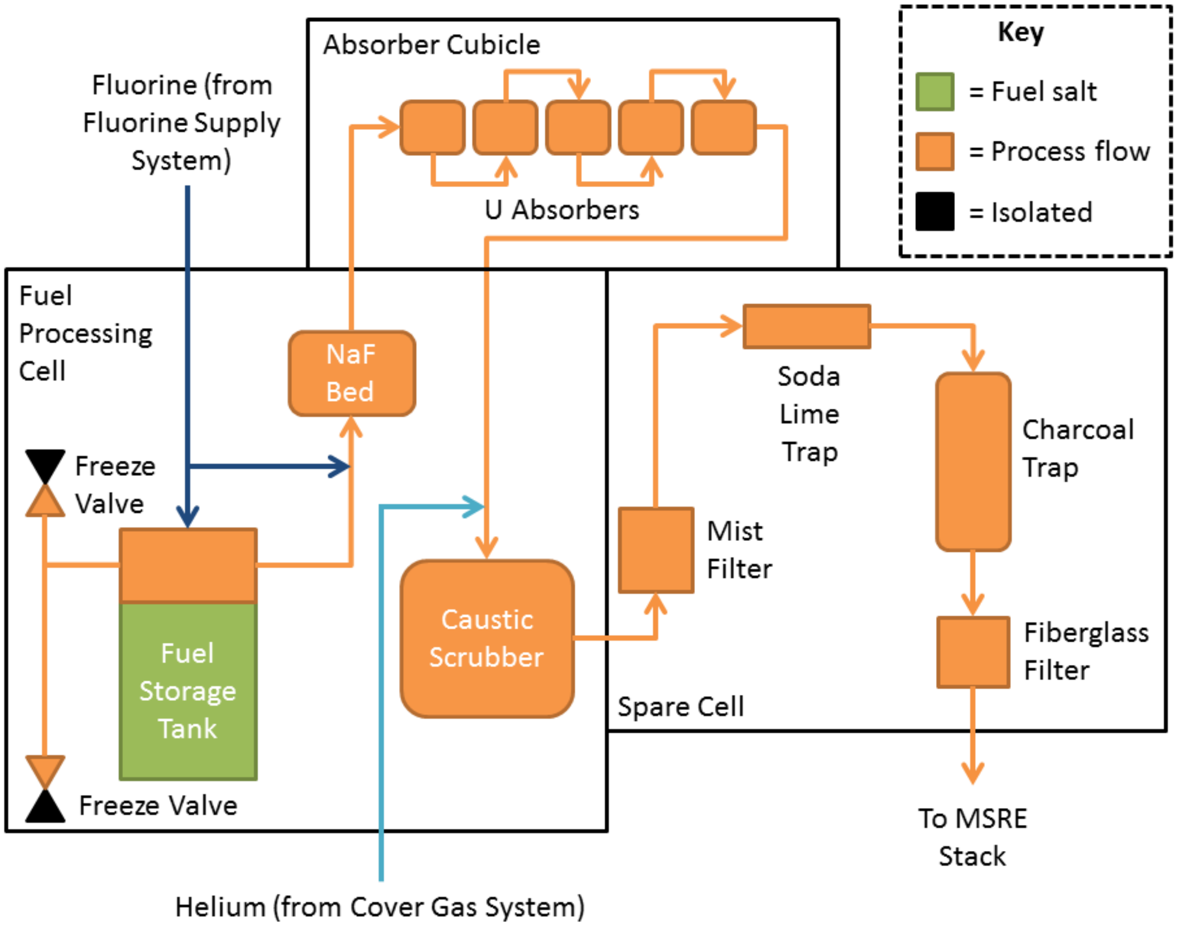


Figure 14: Schematic of barriers to release of radioactivity for MSRE fuel processing system during fluorination

Once the barriers intended to prevent the release of radioactive material have been defined, the search for PIEs can be conducted by identifying the failure modes of the barriers, and the challenges or initiators that will produce these failure modes [NEI, 2019]. A frequently cited tool to facilitate the identification of PIEs is the MLD approach [IAEA, 1993; Modarres, 2006; NASA, 2011; NRC, 1983]. MLD can be useful to determine elementary failures (or combinations of elementary failures) that could challenge the success of barriers; however, use of MLD alone does not provide sufficient confidence that PIEs have been comprehensively identified [IAEA, 2010]. The combination of a deductive analysis (such as MLD) with an inductive analysis to determine hazardous physical and/or chemical reactions of concern to a design has been found to be particularly effective to ensure completeness of PIE identification and resolution of uncertainty surrounding design quality [Nagel and Stephanopoulos, 1995]. The technical requirements for IE development in the Non-LWR PRA Standard specifically mention HAZOP studies as an example of a structured, systematic process to identify IEs that accounts for plant-specific features [ASME/ANS, 2013].

Thus, the HAZOP approach was used to identify PIEs in the MSRE design; many of the HAZOP results discussed in Section 4.4 identify potentially hazardous scenarios that could lead to the failure of barriers intended to contain radioactive material. In addition to the HAZOP studies of the MSRE design, the MLD approach was used to identify any PIEs that may have been overlooked by the inductive HAZOP method, in addition to providing a visual tool to organize the PIEs that were identified.

5.2. Master Logic Diagram for the MSRE

The MLD approach was used to analyze the same inventories of radioactive material that were studied using the HAZOP method (i.e., the fuel salt during normal operations, the off-gas during normal operations, the process flow during fluorination, and the fuel salt during fluorination). The highest levels of the MSRE MLD can be seen in Figure 15, and an example of the breakdown to Level 9 for the radioactive material in the off-gas during normal operations is shown in Figure 16. The "top event" of the MSRE MLD is the release of radioactive material. The MLD analysis was conducted by logically decomposing the top event down into simpler contributing events that could lead to it. The decomposition of intermediate events continued until a sufficient level of detail was reached and no additional physical phenomena could be identified. The basic events that could not be further separated into sub-events represented PIEs for the MSRE design. For more general information on the MLD approach, the reader is referred to [Papazoglou and Aneziris, 2002].

In general, the MLD for the identification of MSRE PIEs was developed according to the following levels:

- Level 1: Release of radioactive material (overall event of interest)
- Level 2: POS during which the release occurs
- Level 3: Inventory of radioactive material with potential for release
- Level 4: Level of barrier between inventories and the public/environment
- Level 5: Interface where barrier fails
- Level 6: Acute vs. latent failures of barrier
- Level 7: Challenge leading to failure of barrier
- Level 8: Functional failure leading to challenge
- Level 9: Occurrence contributing to functional failure
- Levels 10+: Specific system/component failures with similar system consequences

Industry guidance on PRA development [NEI, 2019] provides some suggestions for considerations that can be used to organize the logical decomposition in the MLD. For example, reactor-specific PIEs can be grouped based on which inventory of radioactive material they could cause to be released. However, the MSRE HAZOP studies and the analysis in the previous section demonstrated that the barriers in the MSRE that are intended to prevent the release of a single inventory of material can vary for the different MSRE POSs. In the MLD, Level 2 is the MSRE POSs and Level 3 is the major inventories of radioactive material that could be released during each POS. Since the safety approach in the MSRE design was to ensure that each inventory had at least two levels of independent barriers between the material and the environment [Beall et al., 1964], Level 4 continues the decomposition by the level of the barrier that fails to contain radionuclides. As discussed further in the following section, the barriers that are intended to contain radionuclides in LF-MSRs are not always structural barriers that prevent the transport of all materials. For example, the MSRE processing system consisted of a variety of functional barriers (including NaF traps, a caustic scrubber, and activated charcoal traps) that were intended to contain certain radionuclides but allow helium cover gas to flow fully through the system and be exhausted to the atmosphere via the MSRE stack.

PIEs with similar consequences that require similar responses by plant systems are often grouped together in risk assessments [ASME/ANS, 2013]. In the MSRE, the plant responses that are important to mitigate the consequences of a barrier failure are dependent upon where the radioactive material is transported following the failure. For example, different system responses would be required if the main charcoal beds failed in such a way that radioactive material was released to the Charcoal Bed Cell or if OGS Volume Holdup 1 failed in such a way that radioactive material was released to the Reactor Cell, even though both the main charcoal beds and Volume Holdup 1 constitute part of the first barrier to release of radioactive material in the OGS. Thus, Level 5 of the MSRE MLD decomposes the PIEs based upon the interface through which a specific barrier failure allows the radioactive material to be transported. An overview of the interfaces and barriers for the radioactive material inventories in the MSRE fuel salt loop and main OGS during normal operations are displayed in Table 8 and Table 9, respectively.

Level 6 of the MLD separates the challenges to individual barriers based on whether they would lead to a rapid failure of a barrier (i.e., "acute") or contribute over time to the failure of a barrier (i.e., "latent"), and Level 7 is the specific challenge that leads to the failure of the barrier. In general, a structural failure of a barrier can be due to (1) overpressure, (2) underpressure, (3) corrosion, (4) erosion, (5) external loading, (6) high temperature, or (7) vibration [Papazoglou and Aneziris, 2002]. Because some of the barriers in the MSRE are functional, causes leading to underperformance of these functions are also included in the MLD. Level 8 of the MLD distinguishes the functional failure that presents the challenge to the barrier, and Level 9 contains the occurrence that represents the functional failure. Finally, any decomposition past

Level 9 in the MSRE MLD displays specific system/component failures that would have similar consequences to contribute to the occurrence shown in Level 9.

For the first level of barriers, the occurrences in Level 9 can be considered PIEs for the MSRE; however, some of the occurrences in Level 9, such as those pertaining to barriers in the second level or beyond (such as the barriers in the CCS), represent pivotal events that occur after a PIE in an MSRE event sequence. The unique combination of successes and/or failures of these mitigating systems determine the end state of the plant at the conclusion of event sequences.

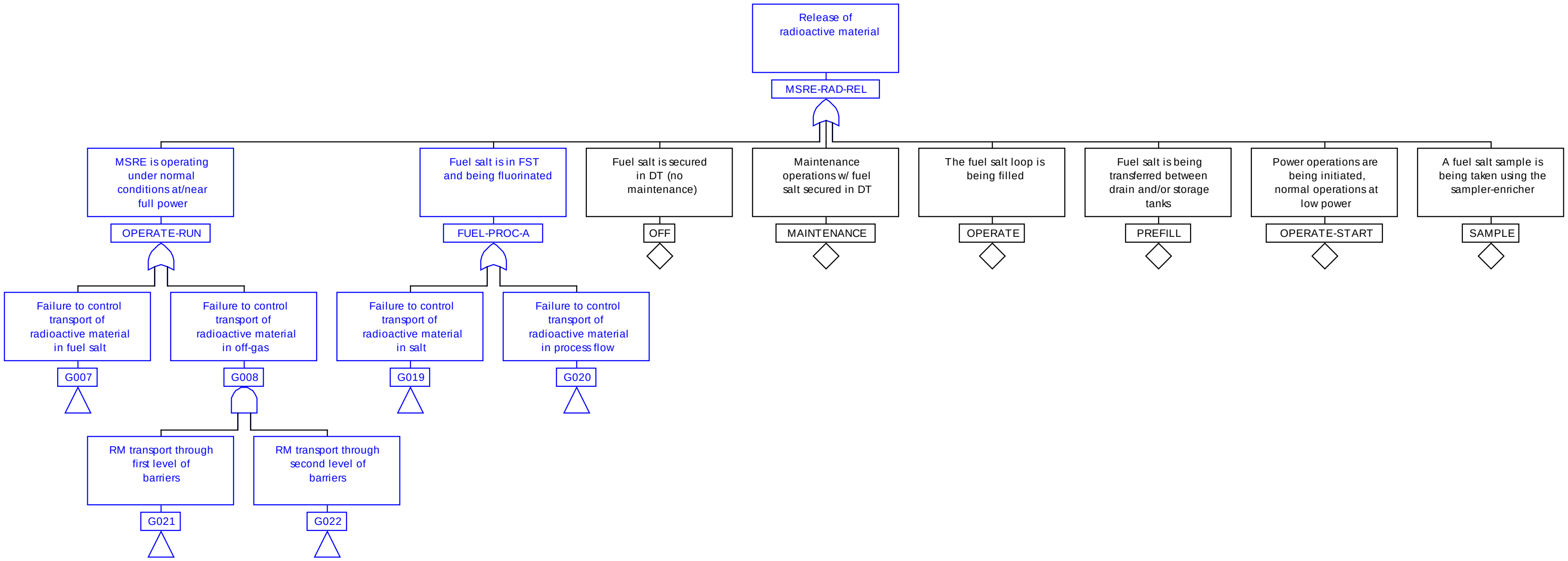


Figure 15: Levels 1-4 of the MSRE MLD

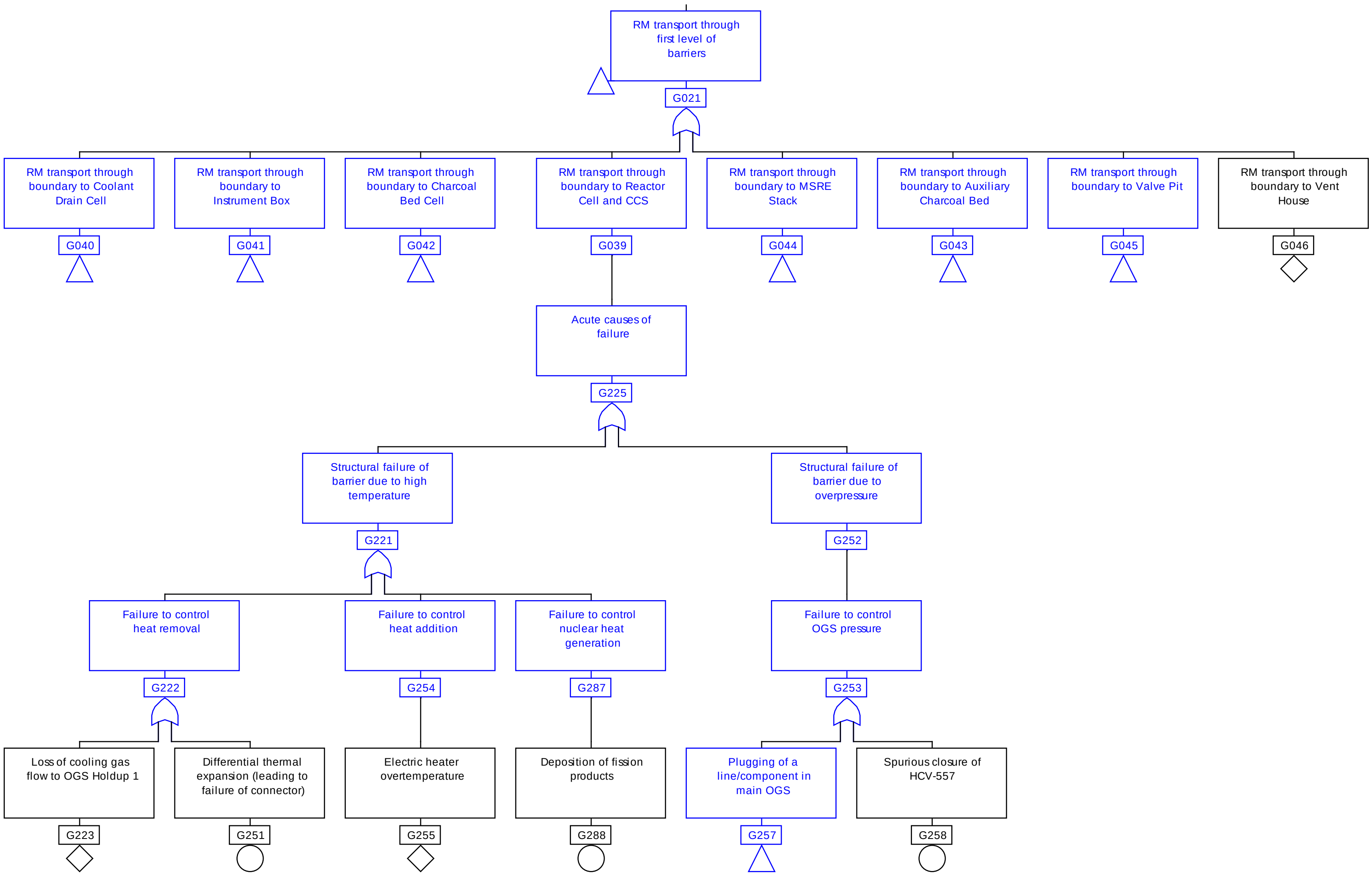


Figure 16: Example of Levels 4-9 of the MSRE MLD for the radioactive material in the off-gas during normal operations

Table 8: Interfaces and barriers for radioactive material in the MSRE fuel salt loop during normal operations

Radioactive Material (RM) Inventory Boundary (First Barrier)	Interface (Second Barrier to RM Release)	Third Barrier to RM Release	Notes
Fuel salt piping, reactor vessel, fuel salt pump bowl, heat exchanger shell, freeze flanges	Reactor Cell and CCS	MSRE Building and Ventilation System	N/A
Heat exchanger tubes	Coolant Salt System	Coolant Cell / MSRE Building and Ventilation System (Coolant Cell not maintained at negative differential pressure like Reactor Cell and Drain Tank Cell)	Transfer of material could be from Coolant Salt into Fuel Salt or from Fuel Salt out to Coolant Salt
Gas/liquid interface in fuel salt pump bowl	Off-Gas System	Reactor Cell and CCS / MSRE Building and Ventilation System	Transfer of only volatile radionuclides from fuel salt pump bowl to OGS during normal operations
Fuel salt pump bowl	Cover Gas System	Reactor Cell / Special Equipment Room / MSRE Building and Ventilation System	Transfer of material from cover gas to fuel salt pump bowl only during normal operations
Freeze Valve FV-103	Fuel Salt Drain/Fill System	Drain Tank Cell and CCS	N/A

Table 9: Interfaces and barriers for radioactive material inventory in the main MSRE OGS during normal operations

Radioactive Material (RM) Inventory Boundary (First Barrier)	Interface (Second Barrier to RM Release)	Third Barrier to RM Release	Notes
Fuel salt pump bowl, OGS piping and connections, Volume Holdup 1	Reactor Cell and CCS	MSRE Building and Ventilation System	Off-gas could potentially flow from fuel salt pump bowl into cover gas system piping
OGS piping and connections in Coolant Drain Cell	Concentric OGS Pipe	Coolant Drain Cell / MSRE Building and Ventilation System	Coolant Drain Cell is not kept at a negative differential pressure like Reactor Cell
OGS piping and connections in Instrument Box	Instrument Box	Vent House	N/A
Volume Holdup 2, Main Charcoal Beds, Auxiliary Charcoal Beds (structural integrity)	Charcoal Bed Cell (water-filled)	N/A	Charcoal Bed Cell is located underground next to MSRE building
HCV-533 (closed)	Auxiliary Charcoal Bed (functional)	N/A - See Note	During normal operations, flow is isolated from Auxiliary Charcoal Bed by closing of HCV-533
Main Charcoal Beds (functional)	MSRE Stack (atmosphere)	N/A	HCV-557C is designed to automatically isolate flow to MSRE stack upon high levels of radiation
OGS piping and connections in Valve Pit	Valve Pit	N/A	Valve Pit is located next to MSRE building
OGS piping and connections in Vent House	Vent House	N/A - See Note	If Main Charcoal Beds function as intended, gas stream should have low concentration of radioactive material

The MSRE MLD highlights the idea that many phenomena in an LF-MSR are very closely coupled. For instance, in the fuel salt loop, the magnitude of the reactivity effects due to a change in fuel salt loop operating pressure is affected by the temperature of the fuel salt [Beall et al., 1964]. Additionally, pressure transients in the fuel salt loop have multiple (sometimes competing) reactivity effects, including void fraction and poison concentration [Beall et al., 1964]. The complicated nature of these relationships can make it somewhat difficult to determine the "basic event" that results in a barrier failure. For example, plugging in the off-gas outlet from the fuel salt pump bowl would increase the pressure of the MSRE fuel salt loop; however, the plugging of this line may also increase the concentration of soluble poisons in the fuel salt because they are not able to be swept into the plugged off-gas line. Therefore, for the radioactive material in the fuel salt during normal operations, the "basic event" of a plug in the off-gas outlet from the fuel salt bowl can be identified as a possible contributor to the structural failure of a barrier due to overpressure as well as a possible contributor to the structural failure of a barrier due to high temperature due to a failure to control nuclear heat generation.

In comparison to the HAZOP method, the MLD approach was better suited to identify latent phenomena contributing to barrier failure. Examples of such phenomena include excessive radiation damage, thermal fatigue, and erosion rates. The MLD approach also identified pre-existing deficiencies that could contribute to barrier failures, such as: an insufficient seal in a freeze flange (leading to leakage or rupture of the flange) or an insufficient frozen plug of salt in a freeze valve (leading to leakage or spurious thawing of a freeze valve). Another advantage of the MLD method over the HAZOP approach is that the visual representation of the MLD can be easier to understand quickly than are the tabular results of the HAZOP study.

The MLD approach was able to identify some failures and phenomena that were not identified during the HAZOP study; however, the HAZOP results identified a higher number of PIEs, including ones that would not have been readily identified by the decomposition of the MLD alone. The HAZOP approach was more useful to examine the MSRE due to the room for creativity and flexibility during the brainstorming of deviation causes. In contrast to the rigid structure of the MLD, the use of parameter/guideword combinations such as "high temperature" and "high pressure" were particularly useful to identify system and component failures that could potentially lead to the failure of a barrier intended to contain radionuclides.

Finally, perhaps the most significant difference between the MLD and HAZOP approaches is simply the amount of information documented during the analysis of PIEs. While the results of the MLD do convey information including where radioactive material could be transported due to a failure of a given barrier and what function certain systems or components perform, the tabular HAZOP results contain much more information that could be used to support the development of more quantifiable models of risk, such as ETA. Examples of details captured in the HAZOP results that would be useful towards a further analysis of risks associated with a design include: (1) discussion of consequences that affect operability or could contribute to the failure of a barrier in another subsystem; (2) discussion of safety systems that would allow for prevention or mitigation of undesired consequences; and (3) important interfaces between subsystems.

5.3. Identification of MSRE PIEs

The 26 categories of PIEs identified using the HAZOP study results and the MSRE MLD are listed in Table 10 along with the inventories of radioactive material to which each category is applicable. Since a complete HAZOP study of the entire MSRE plant design was not completed (as discussed in Chapter 4), the results presented in this section are applicable to the study nodes that were analyzed. Nevertheless, it can be seen in the table that 5 of the categories are applicable to more than one inventory and none of the categories are applicable to more than two inventories.

Compared to the prior efforts that have identified and grouped PIEs in LF-MSRs discussed in Section 2.4.2, the categories of MSRE PIEs are different due to the identification of a number of new functional failures for the removal and/or retention of volatile nuclides. For example, a PIE identified for the MSRE off-gas during normal operations is the ignition of the activated carbon in the main charcoal bed, perhaps due to the presence of volatile organic material. This failure to control heat generation from a chemical reaction in the charcoal bed could decrease the efficiency of the adsorption reaction and reduce the time that volatile radionuclides like krypton and xenon decay before leaving the component. Thus, this PIE belongs to the category "increased radioactive material concentration in effluent to MSRE Stack" and would require a plant response in order to mitigate the consequences of an increased rate of radioactive release from the MSRE Stack. The implication associated with the identification of this type of PIE is that a barrier can fail to perform the intended function of preventing transport of radioactive material without failing structurally. Similar PIEs were identified for the inventory of radioactive material in the process flow during fluorination, including insufficient charge in the caustic scrubber and loss of helium supply flow. Either of these PIEs could have potentially led to a release of radioactive material via the MSRE Stack if actions were not taken by the operators and/or plant systems.

Table 10: MSRE PIE categories with applicable inventories of radioactive material

PIE Category	Normal Operations – Fuel Salt	Normal Operations – Off-gas	Fluorination – Process Flow	Fluorination – Fuel Salt
Release of radioactive material to Reactor Cell	X	X		
Leak of fuel salt material into coolant salt	X			
Ingress of coolant salt into fuel salt	X			
Increase in radioactive material transfer to OGS	X			
Leakage or spurious drain of fuel salt to drain tank	X			
Contamination of helium cover gas system	X		X	
Reactivity transients with forced fuel salt flow	X			
Reactivity transients without forced fuel salt flow	X			
Release of radioactive material in Coolant Drain Cell		X		
Leakage through or inadvertent opening of HCV-533		X		
Release of radioactive material to Instrument Box		X		
Release of radioactive material to valve pit		X		
Release of radioactive material to Charcoal Bed Cell		X		
Increased radioactive material concentration in effluent to MSRE Stack		X	X	
Release of radioactive material to vent house		X		
Pressure feedback transient to fuel salt pump bowl		X		
Contamination of Fluorine Supply System			X	X
Release of radioactive material to Fuel Processing Cell			X	X
Release of radioactive material to Absorber Cubicle			X	
Unintended criticality			X	
Release of radioactive material to Spare Cell			X	
Leakage of radioactive material through transfer freeze valve			X	
Unintended flow of radioactive material to Waste Storage Tank			X	
Pressure feedback transient to Fuel Storage Tank			X	
Fuel salt flow into process line				X
Fuel salt flow into transfer line				X

Multiple MSRE PIE categories were identified for scenarios in which radioactive material did not pass through a structural barrier, but instead flowed from one system to another. Associated with this transport of radioactive material through system boundaries is a change in the systems and functions that prevent the further release of the transported material. For example, a spurious drain of the fuel salt to the fuel salt drain tank does not pose an immediate challenge to any of the barriers preventing release of this material to the Reactor Cell; however, certain responses of systems in the Drain Tank Afterheat Removal System are required to ensure that decay heat is adequately removed from the salt to prevent the barriers in the Fuel Salt Drain/Fill system from being challenged by excessive temperature.

Another interesting observation made based on the MSRE PIEs identified is that a failure to control pressure was identified multiple times as the functional failure contributing to the challenge of a barrier. Over-pressurization was identified as a possible cause of failure for multiple different barriers, including the fuel salt pump seal, OGS piping and connections, and salt processing piping and components. Additionally, the driving force for the off-gas flow is the cover gas supplied to the fuel salt pump bowl and the driving force for the fluorination processing flow is the fluorine gas supplied to the FST. Thus, a blockage of flow at many different points downstream could contribute to the pressurization and potential failure of multiple components upstream. For example, plugging of the OGS piping immediately downstream of the outlet of fuel salt pump bowl could initiate a pressure transient that does not pose a challenge to any barriers in the main OGS but that challenges barriers to the radioactive material in the fuel salt. However, the responses necessary to mitigate the consequences of this PIE would likely involve the radioactive material in the off-gas (i.e., providing an alternative flowpath around the blocked line). Accordingly, the MSRE PIE categories for pressure feedback transients were created to capture these kinds of PIEs.

One category of PIEs that is commonly considered for LWRs [NRC, 2007a], and has been identified for both the FUJI 233-Um [Pyron, 2016] and the MSFR [Gèrardin et al., 2019] conceptual designs, is a decrease in heat extraction from the primary system (i.e., fuel salt in the case of LF-MSRs). However, calculations made by the MSRE team indicated that, due to inherent feedback in the MSRE fuel salt, a complete loss of load at 10 MWth resulted in a mild temperature transient with no core pressure surge [Beall et al., 1964]. Additionally, the analysis of MSRE PIEs identified that an over-temperature malfunction of the electric heaters for the fuel salt loop could possibly affect the heat balance of the loop in a similar way. Because no analysis was found that illustrated a concern of barrier failure related to either a decrease in fuel salt loop heat extraction or an increase in fuel salt loop heat addition, these PIEs were grouped under the MSRE PIE category of "reactivity transients with forced fuel salt flow."

Another commonly identified PIE category for LF-MSRs is a decrease in fuel salt flow rate [Gèrardin et al., 2019; Pyron, 2016]. In LWRs, PIEs that result in a decrease in Reactor Coolant System flow rate represent a failure of the heat removal function [NRC, 2007a]. In LF-MSRs, however, fuel salt flow is related to both heat removal and heat generation. A decrease in fuel salt flow immediately increases the number of fissions caused by delayed neutrons released in the core, in addition to decreasing the rate of heat removal, which increases the temperature at the core outlet [Beall et al., 1964]. However, in response to increase fuel salt temperature, the heat generation rate in the fuel salt decreases substantially. Accordingly, the PIEs associated with decreases in fuel salt flow rate, such as a fuel salt pump trip, were included in the MSRE PIE category "reactivity transients without forced fuel salt flow." This grouping recognizes that the timescale of the system response necessary to mitigate challenges to barriers is different for reactivity transients that occur with the fuel salt under natural convection, as opposed to forced flow, but acknowledges that the barrier challenges associated with a decrease in fuel salt flow are related to the reactivity balance rather than the heat balance.

Finally, each of the PIEs identified by Pyron [2016] and Gèrardin et al. [2019] can be grouped into one of the categories of the MSRE PIE categories listed in Table 10. However, due to the tight coupling of phenomena in LF-MSRs, the MSRE PIE categories identified in this work seem to lend themselves more readily for further evaluation using traditional risk assessment methods (such as ETA). An example from Gèrardin et al. [2019] is the comparison of the following two PIEs: (1) an undetected deviation of the chemical composition and (2) a rupture of the gas processing unit with a leak of processing fluid. Although both of these PIEs are considered to belong to the same PIE families (i.e., "Loss of fuel composition/chemistry control"), the plant response would be different for an event sequence in which radioactive material has been transported past a barrier (i.e., Scenario 2) than it would for an event sequence in which no barrier has failed yet (i.e., Scenario 1). By contrast, both a rupture of MSRE OGS piping and a rupture of MSRE fuel salt piping belong to the same MSRE PIE group from Table 10 (i.e., "Release of radioactive material to the Reactor Cell"). Although the composition of the radioactive material release to the cell may be different, the functions required to contain the release to the reactor cell would be similar for these two PIEs.

5.4. Observations from PIE Identification

The work reported in this chapter represents an in-depth initiation of a safety assessment -- a systematic and comprehensive answer to the question "what can go wrong?" for a given system design. The MLD and HAZOP approaches were used together to identify and consider PIEs for the MSRE in a way that is conducive to the analysis of an advanced nuclear reactor design at an early design stage. Identifying the PIEs for a reactor design that is at a conceptual or preliminary stage of design facilitates the incorporation of risk insights into the next iteration of the design process and allows for the early establishment of more quantifiable risk assessment models, such as ETA.

Using the HAZOP and MLD methods to identify how radioactive material could be transported through barriers intended to prevent their release identified 26 categories of PIEs for 4 inventories of radioactive materials in the MSRE across 2 different POSs. Compared to previous efforts to identify PIEs for LF-MSR designs, the present work identified new functional failures in which radioactive material was not necessarily released due to the structural failure of a component, but the material was still transported through a boundary that would likely initiate a plant response to mitigate consequences. One example is the overheating of the main charcoal beds in the OGS during normal operations (possibly due to loss of cooling or to chemical reactions in the bed) that would reduce the effectiveness of the activated carbon to adsorb volatile radionuclides, thus increasing the concentration of radioactive material to the next step in the process and potentially leading to radioactivity in the MSRE stack effluent above desired levels.

The results demonstrate that the concepts of hazardous material inventories and the barriers to the release of this material are fundamental to the identification of PIEs for LF-MSRs. Significant inventories of radioactive material may exist outside of the fuel salt that is undergoing fission in the core (e.g., volatile radionuclides in the OGS and the separation of radionuclides via processing of the fuel salt), and the barriers that are designed to retain this material may be different for different POSs. Additionally, the safety functions that are intended to prevent failure may be different for different sets of barriers and radioactive material inventories. Therefore, an exhaustive identification of PIEs for an LF-MSR design should consider the challenges to the barriers for each unique arrangement of material inventories.

The results also suggest that not all functional categories of PIEs that are often considered for LWRs will necessarily be relevant for the safety assessment of LF-MSRs. For example, due to inherent feedback mechanisms, a loss of load for the MSRE design did not represent a significant challenge to the barriers intended to contain radionuclides. This observation emphasizes the need to focus on the major inventories of hazardous materials and the failure of barriers intended to prevent the release of the material when using the MLD methodology for the analysis of PIEs for an LF-MSR design, rather than simply basing the functional decomposition upon the MLD structure for other nuclear reactor designs.

Additionally, categorizing PIEs based upon the interfaces through which radioactive material will be transported in the case of a barrier failure appears to be an appropriate manner to meet the objectives of IE analysis prescribed by industry standard approaches [ASME/ANS, 2013], especially for early stage designs. In other efforts, LF-MSR PIEs have sometimes been grouped functionally (e.g., "radioactive release from a subsystem or component"). However, the system responses in an LF-MSR design that are important to mitigate the consequences may be different depending on where the radioactive material is released. For example, consider the first layer of barriers intended to prevent the release of radioactive material in the OGS during normal operation shown in Figure 13. The response necessary to mitigate the consequences of a release of radioactive material from the components in the reactor cell would be different than the response necessary to mitigate the consequences of a release from the components in the charcoal bed cell. Grouping the PIEs based upon the interface through which radioactive material is transported can also help minimize the number of redundant event sequences (e.g., "increase in heat removal by coolant salt" vs. "loss of electric fuel salt pipeline heater") that will need to be modeled when developing more quantifiable models of risk, such as event sequence diagrams or ETA.

It is worth noting again that the present identification of internal initiators represents the first step of the PIE analysis for the MSRE. For a full scope risk assessment of the MSRE design (or other LF-MSR designs), the analysis of PIEs would need to be expanded to include identification of external hazard scenarios and the consideration of correlations between internal and external hazards and PIEs for each POS [Wielenberg et al., 2017]. Additionally, it is possible that consideration of PIEs that could lead to other undesirable consequences other than release of radioactive material (such as release of hazardous chemicals or loss of investment) may be of interest to LF-MSR stakeholders. In particular, the use of an interaction matrix may be useful to ensure comprehensive understanding of potential chemical reactions that could occur and their associated consequences.

CHAPTER 6, ANALYSIS OF MSRE FREEZE VALVE FAILURE RATES AND EVALUATION OF DESIGN INSIGHTS

One key technical challenge that has long been identified for MSRs is the design of valves having adequate performance and reliability [Spiewak, 1958]. When the design and construction of the MSRE began at ORNL in the early 1960s, a mechanical valve design that had been proven reliable for use in molten salt systems had yet to be demonstrated [Guymon, 1973]. Therefore, as an alternative, the MSRE design team made the decision to utilize a "freeze valve." A freeze valve[38] includes a flattened section of salt-filled piping that can be cooled when desired to establish a short "plug" of frozen salt to block salt flow, and heated when desired to melt the plug and allow salt flow through the pipe. As such, an MSR freeze "valve" requires the support of auxiliary subsystems to allow for cycling of the valve – namely, a means to heat the plug and a means to cool the plug. In this sense, describing a "freeze valve" as an individual component is a misnomer. The freeze valve function is actually achieved by a system of components, and assessment of freeze valve subsystem capabilities and performance must include comprehensive consideration of the components necessary for its proper functioning.

Additionally, the operation of a freeze valve is often cited as an example of a passive approach to safety in MSR designs [Elsheikh, 2013]. Yet, this sort of characterization does not adequately consider the active auxiliary subsystems that must continue to operate to enable the performance of the freeze valve function. An in-depth analysis of the MSRE freeze valve subsystem design can help ensure that the reliability of this feature, and the associated impact on the risk profile of the overall MSRE system, is represented appropriately.

The MSRE PHA studies (see Chapter 4) highlighted the fact that the MSRE control rods were not designed to be capable of providing absolute reactor shutdown under all conditions. Due to the negative temperature coefficient of the liquid fuel, the shutdown worth in the rods could be lost if the fuel salt in the core vessel was sufficiently cooled [Tallackson, 1968]. Instead of utilizing the traditional nuclear safety approach of ensuring subcriticality of the fuel by inserting sufficient negative reactivity using control rods (i.e., a reactor "scram"), transference of the fuel salt to the drain tanks (i.e., a fuel salt drain) was the intended method of obtaining safe shutdown in the MSRE. A fuel salt drain was initiated by the thawing of a freeze valve in the fuel salt drain line, which allowed the fuel salt to drain to tanks via gravity. Thus, a failure of this freeze valve to thaw on demand represents a failure of an important safety system, since fuel salt that remained critical in the fuel salt loop for an extended period of time during an accident scenario could ultimately threaten the integrity of barriers in the fuel salt loop and

[38] Sometimes called a "freeze plug"

potentially result in release of hazardous material [Beall et al., 1964]. A quantitative evaluation of the likelihood that the freeze valve in the MSRE drain line fails to thaw on demand will likely be needed for evaluation of a variety of event sequences (for example, see Chapter 7).

Another scenario of interested identified during the HAZOP study of the MSRE fuel salt loop is an unanticipated thaw of the freeze valve in the drain/fill line during operation of the MSRE at full power. In the absence of cooling, the temperature rise of the fuel salt due to decay heat from dissolved fission products would be higher if the salt was in the drain tanks than if it was trapped in the fuel salt loop [Beall et al., 1964]. Thus, a spurious thawing of the freeze valve in the drain line represents an initiator for a potentially risk-significant event sequence, and was identified as a PIE for the MSRE design (see Chapter 5). Designers of contemporary MSR systems would also be interested in the possibility of a spurious thawing of a freeze valve in general, since experience at MSRE revealed the refilling the fuel salt loop after a fuel salt drain to be a time-consuming operation; the return to power operations after a drain at MSRE could take an hour or more, depending on troubleshooting and any repairs that may have been necessary [Guymon, 1973]. As such, even if it does not produce a challenge to barriers intended to contain hazardous material, an unanticipated fuel salt drain at a minimum represents an example of an operational upset in an LF-MSR system.

At the conclusion of the 4-year span of MSRE operation, the ORNL team qualitatively described the operation of the freeze valves as "quite satisfactory" [Guymon, 1973]. However, detailed review of the freeze valve operational experience discussed in the MSRE documentation reveals failures and other incidents that appear to contradict the subjective pronouncement of satisfactory performance and reliability. As there is no other documented body of evidence to rely on, it is possible that current MSR stakeholders may assume a greater degree of reliability and performance for freeze valve subsystems than is justified. Examples of MSR conceptual designs that rely upon freeze valves to isolate the flow of salt during operations and to drain the fuel salt in an upset condition include the Thorium Molten Salt Reactor (TMSR) [Xu, 2013] and the Molten Salt Fast Reactor (MSFR) [Tiberga et al., 2019].

No specific reliability estimates have been identified in the open literature for freeze valves. Recent work has investigated the thermodynamics associated with salt plug freezing and melting [Giraud et al., 2019; Makkinje, 2017; Shafer, 2018; Swaroop, 2016; van Tuyll, 2016]; however, there has not been analysis conducted to evaluate freeze valve safety and/or reliability. Therefore, a thorough review of freeze valve operating experience has been recently conducted, and an original quantitative reliability assessment has been developed. In addition to producing quantitative estimates of freeze valve failure likelihood that can be used in subsequent quantitative risk assessment efforts, this work provides insights and reveals nuances related to the design and operation of freeze valves that are likely to be of interest to MSR stakeholders, especially designers.

6.1. MSR Freeze Valve Literature

Examples of different freeze valves assembled and tested as part of the MSRP at ORNL in the 1960s are shown in Figure 17 and Figure 18. Each of the two narrowed sections of pipe in the freeze valve assembly shown in Figure 18 is referred to as a “freeze valve body,” while the wider pipe sections on either end of the freeze valve assembly are “siphon pots.” The freeze valve shown in Figure 17 depicts a more complete picture of the entire “freeze valve subsystem.” In order to achieve the “freeze valve function” of thawing and freezing a plug of salt inside the pipe on demand, heaters were provided as a source of heat, a flow of cooling gas across the body of the valve was provided as a means to remove heat, and thermocouples were located on the valve assembly to provide an indication of the condition of the freeze valve.

6.1.1. MSRE Freeze Valve Design Information

<u>MSRE Freeze Valve Overview</u>

In the final MSRE system design, there were a total of 12 freeze valves, with six installed in 3.8 cm (1.5-in.) lines and six in 1.3 cm (0.5-in.) lines. All of the freeze valves, except for FV-103 in the fuel salt drain line, were oriented horizontally. Line 103 and FV-103 were pitched at about 3° to facilitate the draining of the fuel salt from the fuel salt loop to the fuel salt drain tanks via gravity [Robertson, 1965]. The general arrangement of the freeze valves other than FV-103 is illustrated in Figure 19. One major difference from earlier freeze valve assemblies tested at ORNL was the addition of a shroud (evident in Figure 17) used to direct the flow of cooling gas around the freeze valve body and improve the heat removal capability. The shroud also prevented the gas from unintentionally impinging on nearby heated surfaces. Short vertical lengths of larger, 10 cm (4-in.) piping were placed on either side of some freeze valve bodies to provide siphon breaks and ensure that a sufficient volume of salt would remain in the valve body after a salt transfer so that a full and solid frozen plug was formed during re-freezing.

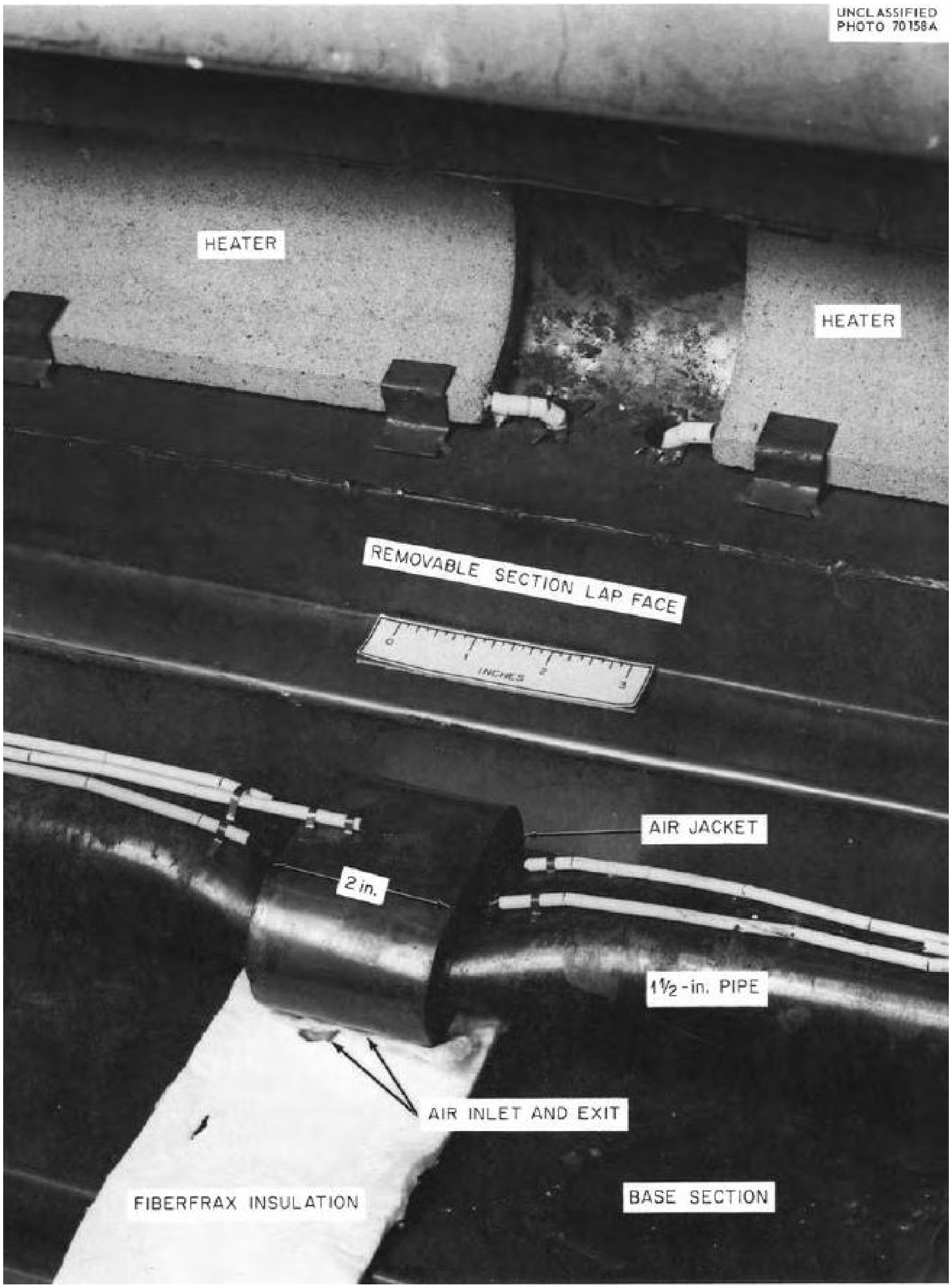


Figure 17: Example of freeze valve subsystem (with cylindrical shroud around valve body) [Briggs, 1964]

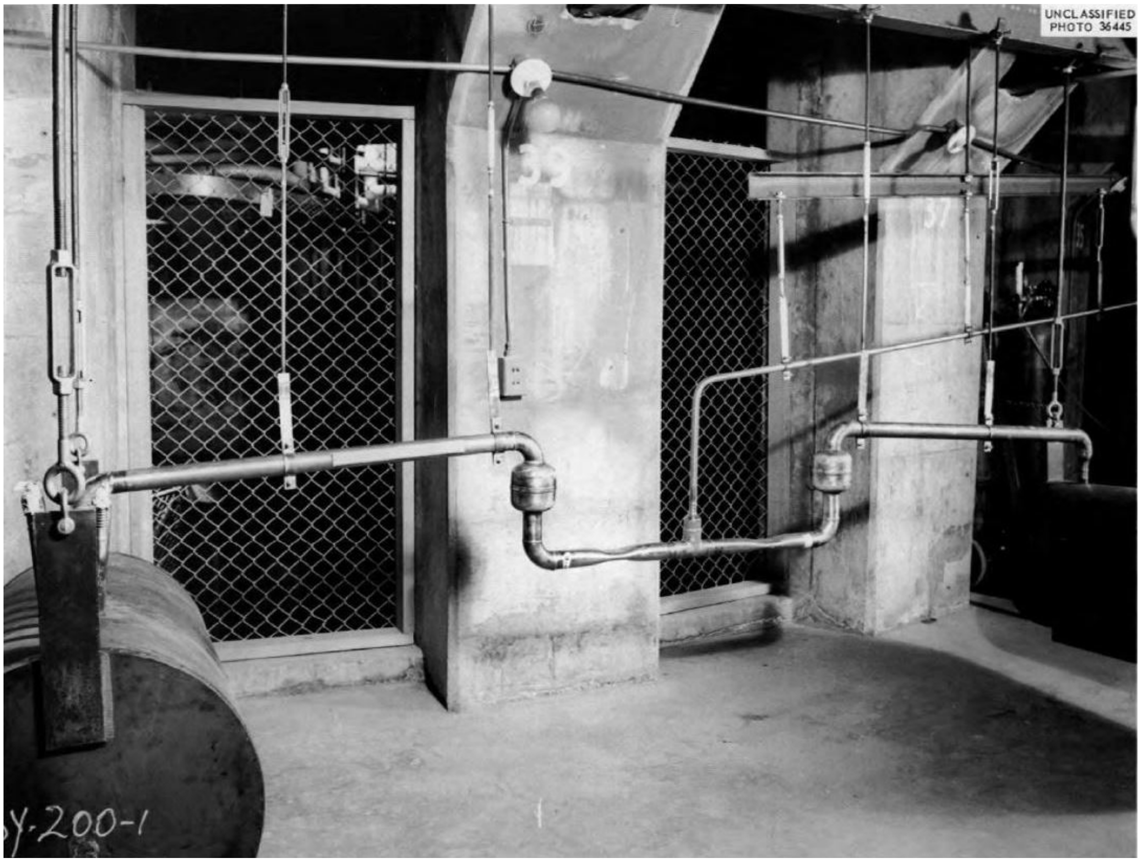


Figure 18: Example of freeze valve piping [Briggs, 1961]

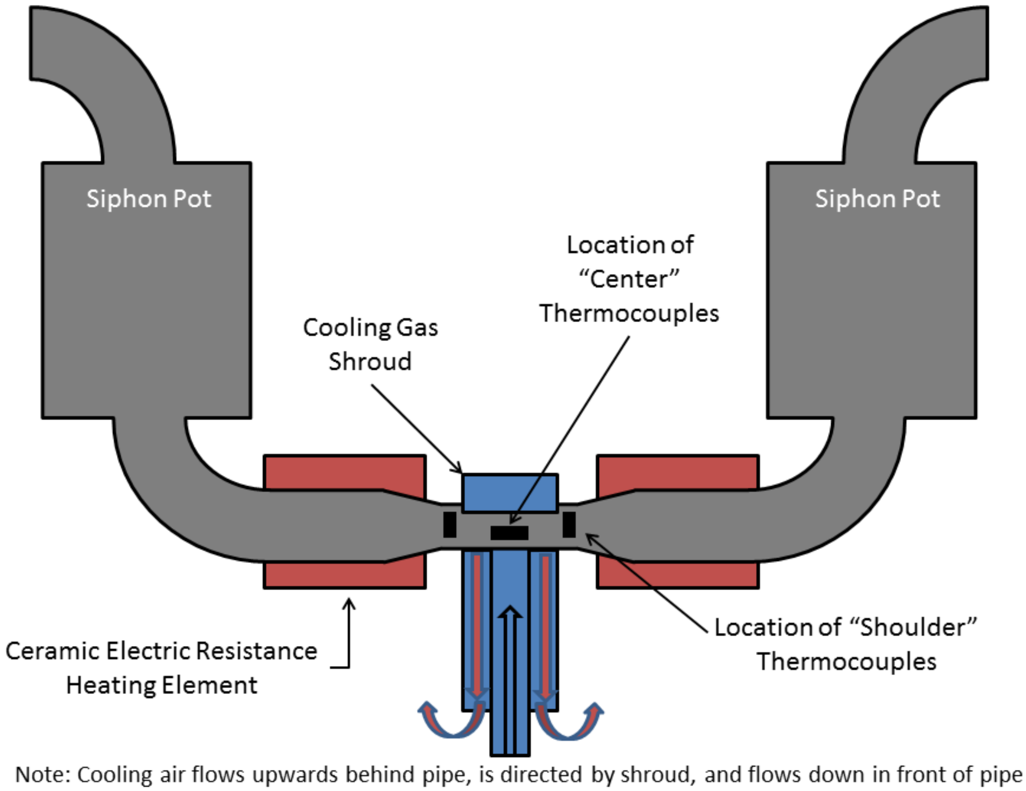


Figure 19: Schematic of freeze valve layout with siphon pots (profile view, adapted from [Robertson, 1965])

Thermocouples were installed on each freeze valve, providing coverage of the valve body and both "shoulders" (i.e., the transitions between the pipe and the flattened area), as illustrated in Figure 19. If the temperature at the center section of a freeze valve body rose above 700°C (1300°F), or fell below a set value, an alarm was sounded in the control room; however, there were no associated automatic system responses. The operating modes of the MSRE freeze valve subsystems were defined as follows:

- Deep Frozen: The salt plug was frozen, and would remain so for an extended period of time, even upon loss of electric power and cooling gas supply. The freeze valve heaters were off, and may also have been off on adjacent piping. The cooling gas may or may not have been supplied to the valve body, based on the specific heat balance for each freeze valve.
- Frozen: Freeze valve heaters were off, the heaters on adjacent piping were on, and the salt plug remained frozen due to the cooling action of the gas stream. The frozen salt

plug would thaw in a specified amount of time if the electrical power failed (and caused a loss of cooling gas flow) and remain thawed for at least 20 minutes.[39]

- Thawed: Electric heaters on adjacent piping and/or in the freeze valve subsystem were on; the cooling gas flow was off. If electric power failed, the salt in the valve would remain thawed for at least 30 minutes.[40]

Figure 20 illustrates the location of the freeze valves in the MSRE. One freeze valve (FV-103) was provided in the fuel salt drain/ fill line; this valve was frozen to keep salt circulating in the fuel salt loop. There was another freeze valve in series between this freeze valve and each of the fuel salt drain tanks (i.e., a total of two freeze valves) to allow for drain tank isolation during scheduled fuel salt drains; these freeze valves were both kept thawed during normal operations. Another freeze valve was provided in series between FV-103 and the fuel flush salt tank (used for special evolutions) and kept in the "deep frozen" condition during normal operations to isolate this vessel. The coolant salt system had two parallel freeze valves that were frozen to keep salt circulating in the coolant salt loop and thawed to allow the coolant salt to drain to the two coolant salt drain tanks. The remaining six freeze valves were used only during shutdown periods for salt transfers and additions; these valves were kept deep-frozen during normal MSRE operations. Only FV-103, the freeze valve in the fuel salt drain line, is discussed further in this section to provide information relevant to the PHA studies and fault tree analysis (FTA) presented in Sections 6.2 and 6.3.

[39] A freeze valve design that could form a frozen salt plug while salt was flowing through the valve body was not discussed in the MSRE literature; however, Robertson [1965] does not specify what assumptions were made regarding salt flow when determining the time that a valve was required to remain open after a loss of electric power.

[40] The specific design details of each freeze valve in the MSRE system resulted in unique operational approaches and control setpoints for each freeze valve subsystem. Robertson [1965] and Moore [1972] present detailed discussions of the exact configurations, heat balances, and operational adjustments/fine tuning needed for each MSRE freeze valve.

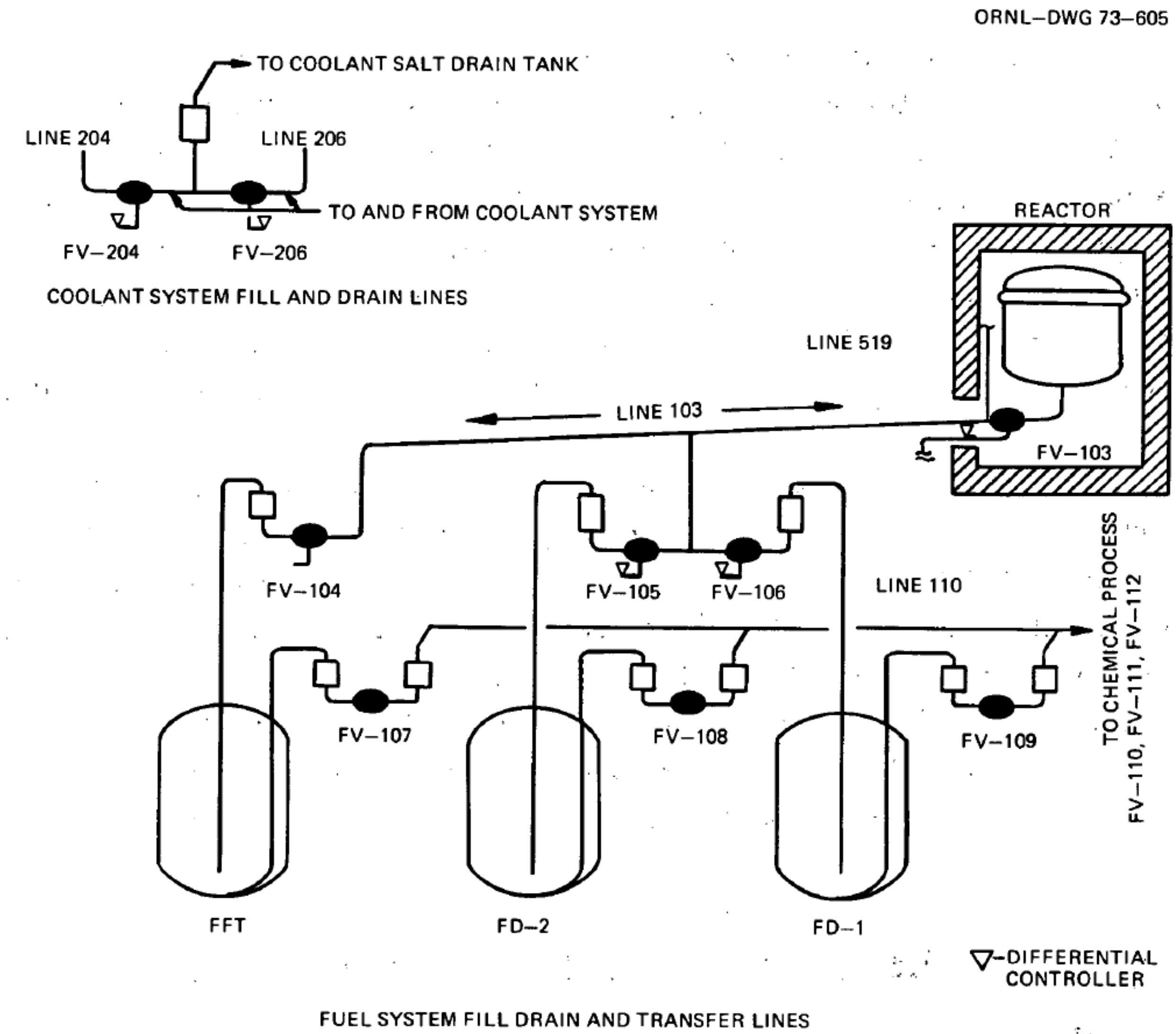


Figure 20: Location of MSRE freeze valves [Guymon, 1973]

MSRE Freeze Valve FV-103

The specific arrangement around FV-103 (the freeze valve in the fuel salt drain line) is illustrated in Figure 21. The MSRE design team determined that a dedicated heating element was not needed for the thawing of this freeze plug because sufficient heat was supplied by nearby heaters for the reactor vessel and adjacent components.[41] FV-103 was kept in the frozen operating mode while salt was in the MSRE fuel salt loop by an automatic control subsystem. The control subsystem operated as follows:

[41] However, a heating element was included in the design to prevent the pipe from becoming too cool in the vicinity of the electrical connection for the resistance heating of the drain/fill line (Line 103) [Robertson, 1965].

- The salt plug in the valve was frozen by a 107 Nm^3/hr (68 scfm) jet of cooling gas (referred to as "blast" air flow) in less than 30 minutes.[42]
- As the valve cooled, the cooling gas flow was reduced to a "holding" flow rate of about 24 Nm^3/hr (15 scfm) when the temperature at the shoulders of the valve reached a "high" setpoint.
- If the valve continued to cool, the cooling gas flow was cut off entirely when the shoulder temperatures reached a "low" setpoint. Once the valve temperatures rose back above the "low" setpoint, the holding air would be resumed.
- If the temperatures of the valve exceeded the "high" setpoint, the higher "blast" air flow was reinitiated automatically.

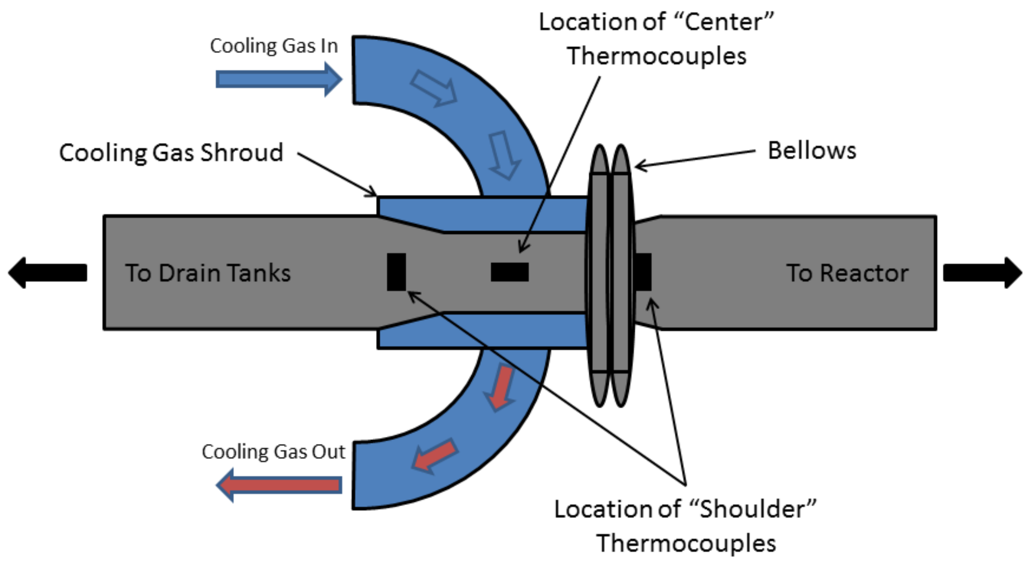


Figure 21: Schematic of MSRE FV-103 layout (top view, adapted from [Robertson, 1965])

An important insight from reviewing the discussion of freeze valves in Robertson [1965] is that the design of each freeze valve assembly utilized in the MSRE design differed slightly depending on the desired function of the valve subsystem and its exact physical location within the MSRE design. Additionally, it is possible that current, improved electronic components would allow for a more flexible approach to freeze valve control instead of the "blast-hold-off" approach to controlling the cooling gas in the MSRE design.

---

[42] As previously mentioned, the valve could not be frozen if liquid salt was flowing through the valve body.

Moore [1972] provides detailed descriptions of the MSRE process instrumentation and the electrical control and alarm circuitry. The following paragraphs summarize the instrumentation and control of the freeze valve in the fuel salt drain line (i.e., FV-103).

The reactor cell (the containment vessel surrounding the MSRE fuel salt loop) was penetrated with process lines for helium, air, and water. To ensure the integrity of the containment, the MSRE design team used block valves to automatically seal off these penetrations when potential hazards were detected by the MSRE safety system [Tallackson, 1968].[43] Since it was considered essential that FV-103 be able to thaw regardless of the state of confinement isolation, special restrictor valves were utilized on the air supply to the pneumatic freeze valve cooling gas isolation valves so that cooling gas flow could be secured regardless of the position of the block valves in the line.

The condition of FV-103 was determined by measuring the temperatures at the center and on both shoulders of the valve body. The frozen plug of salt in a freeze valve body was assumed to be thawed when the temperature of the salt was slightly above 450°C (850°F) and frozen when the temperature was slightly below 450°C (850°F). Temperature switches operated to automatically control the cooling air supply valves, and position indicator lamps, operational interlocks, and annunciators were provided. The position of the cooling gas isolation valves could also be controlled by operation of a manual switch in the control room.

A notable characteristic of the approach to the control of FV-103 was the "fail-safe" configuration of the circuits for the solenoid valves that supplied air to open the pneumatic valves controlling the flow of cooling gas. The operation of the circuits was such that the solenoid valve would close and shut off the cooling air supply to the valve body (thus allowing the valve to thaw) in the case that power to the control circuit failed or a solenoid coil burnt out. This arrangement supported the MSRE design assumption that draining the fuel salt to critically-safe, cooled drain tanks was the safest configuration for the MSRE under upset conditions.

The geometry of the MSRE fuel salt drain tanks and lack of nearby neutron moderator supported the design philosophy that it would be safer to drain the fuel salt (rather than leave it in the fuel salt loop) during upset conditions. However, it should be noted that block valves were required to close in order for the MSRE Afterheat Removal System to function properly

[43] Section 1.2.3.1 of [Tallackson, 1968] provides a detailed discussion of the safety requirements associated with the components performing the function of containing radioactive material that could be released to/from the reactor cell.

and allow removal of heat from the salt once it is in the drain tank [Tallackson, 1968]. In the absence of sufficient cooling, significant heating of the fuel salt could occur in the drain tank due to decay heat from dissolved fission products [Beall et al., 1964]. Additionally, although there is redundancy in the freeze valve subsystem, the pneumatic valves that isolate the cooling gas to the freeze valve must close to allow thawing of the freeze valve before the fuel salt can be drained via gravity. Thus, based on the International Atomic Energy Agency definition of a passive component, neither the thawing of the freeze valve nor the securing of the fuel salt in the drain tank, as executed in the MSRE design, would qualify today as a "passive" operation because the closing of the solenoid and pneumatic valves was not achieved using stored energy [IAEA, 1991].

6.1.2. Experience with MSRE Freeze Valves

As previously mentioned, operation of the freeze valves was qualitatively described by MSRE staff as "quite satisfactory." [Guymon, 1973] The 12 freeze valves were collectively cycled through the freezing and thawing processes a total of almost 600 times over the duration of MSRE operations from 1965-1969; however, the MSRE operations plan did not incorporate specific experiments focused on evaluating freeze valve performance, and the number of cycles per valve subsystem varied substantially. FV-103 in the fuel salt drain line was cycled a total of 91 times, accounting for approximately 16% of all freeze valve cycles. The normal thaw time without power for FV-103 was 9-11 minutes, and each thaw of FV-103 that occurred while salt was in the fuel salt loop resulted in a full drain and fill cycle for the fuel salt loop. Although the time required to freeze FV-103 was not documented, the shortest period quoted for the freeze valves used to isolate the fuel salt drain tanks (FV-104, FV-105, and FV-106) to reach the salt freezing point was 36 minutes with no salt flowing through the pipe. Because these freeze valve assemblies were further away from the fuel salt loop (thus more thermally insulated) than was FV-103, it does not seem likely that FV-103 could be frozen in a shorter period of time than the drain tank isolation freeze valves could.

FV-103 was desired to melt in less than 15 minutes when demanded, even without power. As such, during normal MSRE operations, FV-103 was maintained in the "frozen" condition. Based on the MSRE literature, it does not seem that the designers were particularly concerned about the potential of over-pressurization of freeze valves being thawed from the "frozen" condition. However, it is discussed by Guymon [1973] that it required approximately 8 hours to bring a freeze valve out of the "deep-frozen" condition into the frozen condition. Heat was required to be applied in a controlled manner to ensure that the salt was melted progressively from either end toward the center of the freeze valve body. This approach was taken to avoid having molten salt trapped between frozen salt plugs and the associated possible danger of pipe over-pressurization leading to a rupture. This phenomenon is relevant to a failure of a modern test freeze valve discussed in the following subsection.

One difficulty noted by the MSRE team related to the performance of the freeze valves was the operation of the modules that made up the installed alarm monitoring subsystem [Guymon, 1973]. The setpoints drifted, double trip points occurred, and failures to respond to alarm signals were encountered. Further complicating the operation of the modules was occasional improper setpoint adjustments performed by MSRE operators. Failures and malfunctions of the modules were traced to quality issues with components and corrosion or oxidation at the printed circuit board contacts. These faults were eliminated by replacement of faulty components, gold-plating all module contacts, and minor circuit changes. When considering the design of a modern freeze valve subsystem, it is likely that improvements in circuitry and sensors since the 1960's would offer improved performance and reliability compared to those used in the MSRE.

FV-103 did not have a dedicated heating element associated with its performance, as sufficient ambient heat to thaw the valve (provided the cooling air was secured) was supplied by nearby heaters. Since the setpoints for the shoulder temperature control modules were premised for a balanced heat distribution, difficulty maintaining the valve temperatures within the module limits was encountered. To alleviate these difficulties, individual heater controls were added to permit separate control of the heat to each shoulder, but control issues associated with this solution also occurred.

Guymon [1973] stated that once appropriate control setpoints were established, FV-103 operated reliably except for one unscheduled drain. This drain was caused by an upward drift of one freeze valve control module setpoint coupled with an incorrect administrative change of another control module setpoint.[44] However, when examining the complete list of interruptions to MSRE operations in [Guymon, 1973] in more detail, two additional unscheduled fuel salt drains can be attributed to failures of components that were required for proper functioning of the freeze valve subsystem. These two events were both due to failures of the operating blower that was supplying cooling gas for the freeze valve while the standby blower was unavailable.

[44] The administrative change was based on an untested theory that the valve should be adjusted on the reactor inlet salt temperature rather than the outlet. Due to the change, there was little if any warning to the operator prior to the freeze plug melting. In addition, the upward drift of the control module had occurred prior to the previous freezing operation, which caused a shorter plug of salt to be formed in the valve body than normal. These two factors, combined with an adjustment to decrease the cooling gas flow because the fuel salt was at a reduced temperature, resulted in the melting of the plug and an unanticipated fuel drain [Guymon, 1973].

Without the ability to provide cooling gas to maintain the frozen salt plug in FV-103, the fuel salt loop had to be drained and the blowers had to be repaired. An unanticipated transference of fuel salt from the fuel salt loop to the drain tank a short period of time after the reactor was operating at full power represents a potential safety concern. The fact that the failure of a blower can result in the failure of the freeze valve subsystem reinforces the idea that it is important to comprehensively evaluate the component failures that can result in the failure of the freeze valve function, even if the components are not physically located near the freeze valve assembly.

One significant underlying concept evident from the MSRE experience with freeze valves is that the heat balance that must be maintained to keep the salt plug in a freeze valve body just below the melting point is difficult to precisely control. It is possible that modern components could reduce failures such as drifting setpoints; however, thermal transients that affect the heat sources and sinks around the valve may still result in undesired thermal cycles in the freeze valve subsystem, as shown by detailed review of MSRE operating experience.

6.1.3. Recent MSR Freeze Valve Analysis and Testing Efforts

<u>Molten Salt Fast Reactor (MSFR) Freeze Valves</u>
As previously discussed in Section 2.4.2, an on-going project with sponsorship across Europe is the development of the MSFR design, which is an adaptation of the MSRE and Molten Salt Breeder Reactor (MSBR) concepts; however, the MSFR does not have a solid moderator in the core and thus operates in the fast neutron spectrum. The reference configuration is a 3000 MWth reactor operating on a thorium fuel cycle [Gèrardin et al., 2017]. In 2015, the SAMOFAR (Safety Assessment of a MOlten salt FAst Reactor) project was launched to deliver experimental and analytical insights regarding the reactor's key safety features. The publications summarized below have contributed to the project's efforts regarding development of freeze valves.[45]

The reference configuration of the MSFR includes a vertically-oriented freeze valve assembly at the base of each of the sixteen fuel loops in the reactor core. The salt plug in the valve body is kept frozen with the use of cooling fans; however, the melting of the plug is intended to be achieved using the decay heat from the liquid fuel in the reactor core. According to Shafer [2018], an MSFR freeze valve subsystem design is desired that achieves the following functions:

[45] In the SAMOFAR literature, freeze valves are referred to as "freeze plugs."

- In the event of an accident (e.g., power loss), the plug of frozen salt must melt in time to allow the reactor to drain before the temperature of structural materials reaches 1473 K.[46]
- The plug must not melt or fall out unless an accident occurs. This means that it must withstand the pressure in the reactor and potential velocity and temperature fluctuations without failing.

In order to achieve these requirements, the SAMOFAR work on the MSFR freeze valve has considered both a single-plug design, which contains one plug of frozen salt occupying the full width of the draining pipe (similar to the MSRE design), and a multi-plug design, which consists of several smaller plugs of frozen salt contained in a metal plate. The single-plug design was originally studied by Swaroop [2016], who specifically considered how heat transfer to the freeze plug is affected by convection in the draining pipe above it. It was found that significant thermal stratification could be expected in the draining pipe above the freeze plug, such that the decay heat in the core would be overwhelmingly transported to the plug by conduction. Thus, the efficiency of a single-plug configuration may be limited since the fuel salt has a low conductive heat transfer coefficient. Consequently, the freeze plug would have to be located in close proximity to the reactor core in order to melt as quickly as desired from the decay heat in the fuel.

Several other studies considered a freeze plug concept consisting of multiple cylindrical plugs in a metal plate (i.e., a multi-plug design). These studies supposed that using multiple plugs inside a plate could accelerate melting[47] by reducing the total volume that needs to be melted and by increasing heat transfer through the sides of the plugs.[48] However, the most recent studies by Shafer [2018] and Tiberga et al. [2019] suggest that the single freeze plug is recommended over a multi-plug design due to the inefficient melting of the thin frozen layer of salt above the copper plate in the multi-plug design.[49] Another conclusion from their analysis is that, for the MSFR reference configuration, a freeze plug that relies on decay heat from the core

---

[46] According to Tiberga et al. [2019], this time is estimated to be between 480s and 1340s.

[47] Makkinje [2017] found that increasing the spacing between freeze plugs speeds up melting until the space between plugs reaches approximately 1/2 the freeze plug diameter, after which gains in melting times become insignificant.

[48] Deuvorst [2017] found that the melting times could be further reduced by introducing vertical heat fins to the top of the plate to conduct decay heat from the core, while van Tuyll [2016] found that incorporating a more conductive material like copper into the Hastelloy-N grate could also reduce melting times by improving heat transfer.

[49] Enhanced modeling capabilities are necessary for a definitive assessment of the feasibility of the multi-plug design, and Shafer [2018] and Tiberga et al. [2019] note that a model that accounts for the continuous sinking of the frozen salt layer due to the hydrostatic pressure in the reactor would likely estimate melting times that are more comparable to (but still longer than) those of the single-plug.

to melt is not feasible unless the freeze plug is located within 0.01 m of the core. This small distance between the frozen plug and the molten salt core could be undesirable, however, because the likelihood of an unanticipated thaw of the plug due to temperature oscillations in the liquid fuel increases as the distance decreases. Therefore, it is not a foregone conclusion that MSR designers can rely solely upon core decay heat to thaw a freeze plug.

Experimental data collected from the Forced Fluoride Flow for Experimental Research (FFFER) and Salt at Wall: Thermal excHanges (SWATH) facilities to improve the accuracy of the SAMOFAR analysis detailed by Giraud et al. [2019] have corroborated Tiberga et al.'s conclusion that the MSFR freeze valve should be thermally isolated from the heat in the core to maximize stability of the heat balance in the plug and the subsystem control setpoints.[50] The SWATH freeze valve design[51] included the addition of a copper plate into the design to enhance the heat transfer towards the salt plug during melting and away from the plug during freezing [Giraud et al., 2019]. Although copper has better heat transfer properties than frozen salt, Giraud et al. noted that copper would not be suitable for high temperature use because of its mechanical properties. Another modification made to the reference MSFR freeze valve subsystem design, based upon the operating experience of the FFFER and SWATH freeze valves, is the addition of mechanical valves to improve the control of cooling gas flow and salt during freeze valve operations. Giraud et al. [2019] note, however, that the addition of these valves will notably increase the size and complexity of the MSFR freeze valve subsystem.

Although the initial design intention of the SAMOFAR research was to develop a simple system to perform the freeze valve function in the MSFR design, the analytical and experiment results suggest that such simplicity may not be achievable. The addition of mechanical valves to the design eliminates the concept of a freeze plug that operates passively and introduces new components that could contribute to the failure of the freeze valve to successfully perform its intended function. Furthermore, the decision to incorporate a dissimilar metal into the design to facilitate heat transfer will need to be evaluated regarding how it may adversely affect the materials and mechanical performance of the freeze valve subsystem.

---

[50] The heat balance of the freeze valve subsystem in the FFFER loop was significantly altered by heat transferred from nearby lines containing flowing salt. Thus, small alterations in the physical configuration of the FFFER loop resulted in significant changes in the operational setpoints and performance of the freeze valve [Giraud et al., 2019].

[51] The SWATH experiment did not involve salt flowing in the vicinity of the freeze valve assembly in an effort to reduce the number of heat sources that must be balanced in order to control the heat balance of the salt plug [Giraud et al. 2019].

Thorium Molten Salt Reactor (TMSR) Freeze Valves

The Chinese TMSR project was launched in 2011 and is being led by the Shanghai Institute of Applied Physics (SINAP). The TMSR project adopts the technical route of developing the solid-fuel and liquid-fuel TMSR designs (TMSR-SF and TMSR-LF, respectively) in parallel [Zhang et al., 2017]. Early experiments at SINAP to gather data that would support freeze valve simulations were conducted using a nitrate salt and a simple geometry[52] to generate initial data [Aji et al., 2018].

To research molten salt coolant technology as a part of the TMSR project, a high-temperature molten salt loop with 5-cm (2-in.) piping was constructed at SINAP and began operation in 2013, with FLiNaK as the working fluid [Li et al., 2014]. Mechanical valves on the loop experienced failures to operate in the salt environment, including leaking and jamming. Although the thawing and freezing of the freeze valve on the loop took more time than the opening and closing of a manual valve, the freeze valve did not experience the same failures to operate as the mechanical valves [Li et al., 2014]. However, one notable failure of the loop freeze valve did occur during commissioning; this failure was a crack in the freeze valve body resulting from the expansion of liquid salt between frozen plugs of salt at both ends of the freeze valve [Kong et al., 2018]. In order to reduce the likelihood of this failure occurring again, additional heaters were added to both ends of the freeze valve body [Fu, 2016]. The rupture of the freeze valve body on the SINAP salt loop suggests that designers of a freeze valve subsystem should follow the lead of the MSRE design team (discussed in the previous subsection) and take care to ensure that the frozen salt plugs are melted in such a way that minimizes the likelihood of trapping liquid salt in between masses of frozen salt.

Approximations for MSR Freeze Valve System Failure Rates

As discussed in Section 2.4.2, Pyron [2016] initiated the construction of a preliminary PRA model for a the FUJI-233Um conceptual design. While identifying initiating events for the model, Pyron indicated that the failure of a freeze valve (i.e., inadvertent thawing of a freeze valve) should be analyzed for its contribution to the risk profile of the reactor system. In the absence of any failure rate data specifically available for an LF-MSR freeze valve subsystem, Pyron simply assumed that the failure rate of a freeze valve could be approximated using the failure rate of either a generic solenoid valve or the failure rate of a solenoid valve used in a SFR for the control of liquid sodium. However, it was concluded by Pyron [2016] that the main uncertainty in the presented analysis of licensing basis events (and the associated risk profile) is

[52] More specifically, various metal rods were used to melt a frozen layer of salt using heat conducted from liquid salt, through the metal rod, and into the frozen salt [Aji et al., 2018].

this lack of failure rate data for an MSR-specific freeze valve subsystem and that "a better evaluation of the freeze valve reliability would result in a lower value [of uncertainty]."

Quantitative risk assessment was also used to estimate the probability of a failure of the TMSR-LF special core fuel salt release system (CFSRS) to discharge fuel from the core to drain tanks when demanded [Yang et al., 2017]. The CFSRS model included two freeze valves, one valve in each line from the core vessel to each of two drain tanks. In the FTA, the failure of a freeze valve to melt is represented as the failure of a resistive heater to function; the failure of an electromagnetic heater to function; or the failure of a switchboard, bus, or relay to provide power to the heaters. The fact that multiple independent component failures could result in a failure of the freeze valve function supports the concept that an MSR is a subsystem rather than a single component. The failure rates for the electrical components comprising the freeze valve subsystem were then retrieved from LWR-specific component reliability databases, but no quantitative failure probability for the freeze valve function is provided by Yang et al. [2017]. It is unclear if the TMSR freeze valve design is such that active cooling would need to be secured in order for the freeze valve to thaw on demand, as no failure associated with an active freeze valve cooling subsystem is modeled in the FT shown by Yang et al. [2017] for the failure of the freeze valve.

6.2. PHA studies of an MSRE Freeze Valve

Although freeze valves are present in many MSR designs, and many modern LF-MSR designers have chosen to use the draining of the fuel salt from the reactor core to the drain tanks as a safety system response to certain potential system upsets, the literature discussed in the foregoing section represents the major insights that can be obtained from publicly-available design, analysis, and experimental information related to MSR freeze valves that currently exists. The summation of this reported research does not directly support a reliability estimate for the freeze valve function.

If an LF-MSR designer chooses to take a similar approach to safety as the MSRE program, and rely upon the thawing of a freeze valve as the ultimate method to ensure subcriticality of the fuel salt, a failure to thaw the frozen salt plug on demand represents an important safety concern. Fuel salt that remains critical in the fuel salt loop for an extended period of time during an accident scenario could threaten the integrity of the fuel salt loop and potentially result in release of hazardous material from the loop. Furthermore, a spurious thawing of a freeze valve resulting in an unanticipated drain of fuel salt during power operations represents at least an operational upset, since the evolution to refill the fuel salt loop and return to power could be cumbersome and time-consuming. However, the scenario in which sufficient cooling is not available to remove the decay heat from the fuel salt after it has been drained to the drain tanks from full power represents another potential safety-related concern.

6.2.1. Overview of Approach

As evident from the foregoing discussion, no research has been conducted to specifically estimate the reliability of MSR-specific freeze valve designs or how their reliability impacts the risk profile of a design. It was apparent based on the review of ORNL MSRE literature that the MSRE design team assessed that the freeze valve subsystem was adequately functional and reliable for its use in a small-scale experiment reactor; however, the failures of the freeze valve subsystem experienced during MSRE operations indicate that the MSRE freeze valve designs would need to be evaluated to ensure they possess sufficient reliability for use in a modern commercial power reactor. Thus, PHA studies were conducted on an MSRE freeze valve design to gain qualitative insights about how the reliability and performance of a freeze valve might affect the overall operability and safety of an LF-MSR.

It became apparent during the review of the MSRE design information that multiple individual components contributed to the performance of the freeze valve function. As such, a number of individual component failures have the potential to impact the reliability of the freeze valve function, and the term "freeze valve component" is a misnomer. The freeze valve design is more accurately modeled as its own subsystem, rather than a single component. The review of the MSRE design details also suggested that FV-103, the freeze valve in the fuel salt drain line, likely had the most significant impact on the safety and operability of the MSRE system. FV-103 was kept in the "frozen" condition during normal operation of the MSRE, but it was designed to thaw in less than 15 minutes to support an emergency drain. Additionally, although each MSRE freeze valve had unique requirements, design characteristics, and control strategies, the design and operation of FV-103 is reasonably typical of the general approach to freeze valve subsystem design as executed in the MSRE.

The HAZOP studies of the MSRE fuel salt loop and CCS were the first step in the assessment of FV-103 and the associated risk. However, as discussed further in the following subsection, a Failure Modes and Effects Analysis (FMEA) was performed to supplement the HAZOP studies. The PHA studies were conducted consistent with industry-standard practice [CCPS, 2008] and regulatory guidance [ASME/ANS, 2013; GIF 2011; US DOE 2016], including the US Nuclear Regulatory Commission's recommendations in NUREG-1513 for applying PHA techniques to nuclear fuel cycle facilities [Milstein, 2001; NRC, 2011].

The results of the PHA studies were then used to structure FT models that were quantified using component reliability data and human reliability estimates to ultimately produce quantitative failure rates for the FV-103 design.[53]

6.2.2. Conduct of MSRE Freeze Valve PHA Studies

In order to conduct a PHA study on a reactor design, it is necessary to subdivide the design into analyzable sections or "nodes." The proper definition of these nodes contributes to effective analysis, as there are problems associated with choosing either too small or too large a section [Crawley and Tyler, 2015]. One consideration that is useful while dividing a system into nodes is to thoroughly document the interfaces between nodes, as these interfaces may be capable of propagating a potential accident from one node to another [Crawley and Tyler, 2015]. This consideration proved particularly critical for the study of the MSRE freeze valve subsystem, since it is composed of components from several nodes, including the MSRE fuel salt loop, CCS, electric heat system, and instrument air system.

Based on a review of the MSRE design information [Guymon, 1973; Moore, 1972; Robertson, 1965], 21 unique nodes were defined based on primary function and nominal operating conditions. These nodes and the HAZOP studies of the MSRE nodes containing significant inventories of hazardous material are discussed in Chapter 4 of this dissertation. The components that constitute the MSRE freeze valve subsystem are displayed schematically in Figure 22. This schematic was developed to organize all the components that can contribute to the success or failure of the freeze valve to properly perform its intended function. The data and information used to create the schematic was derived from several different figures and technical descriptions in pertinent MSRE design and operations reports.

[53] One of the FT models was ultimately used to estimate the frequency of a pivotal event modeled in the MSRE ETA presented in Chapter 7 of this dissertation.

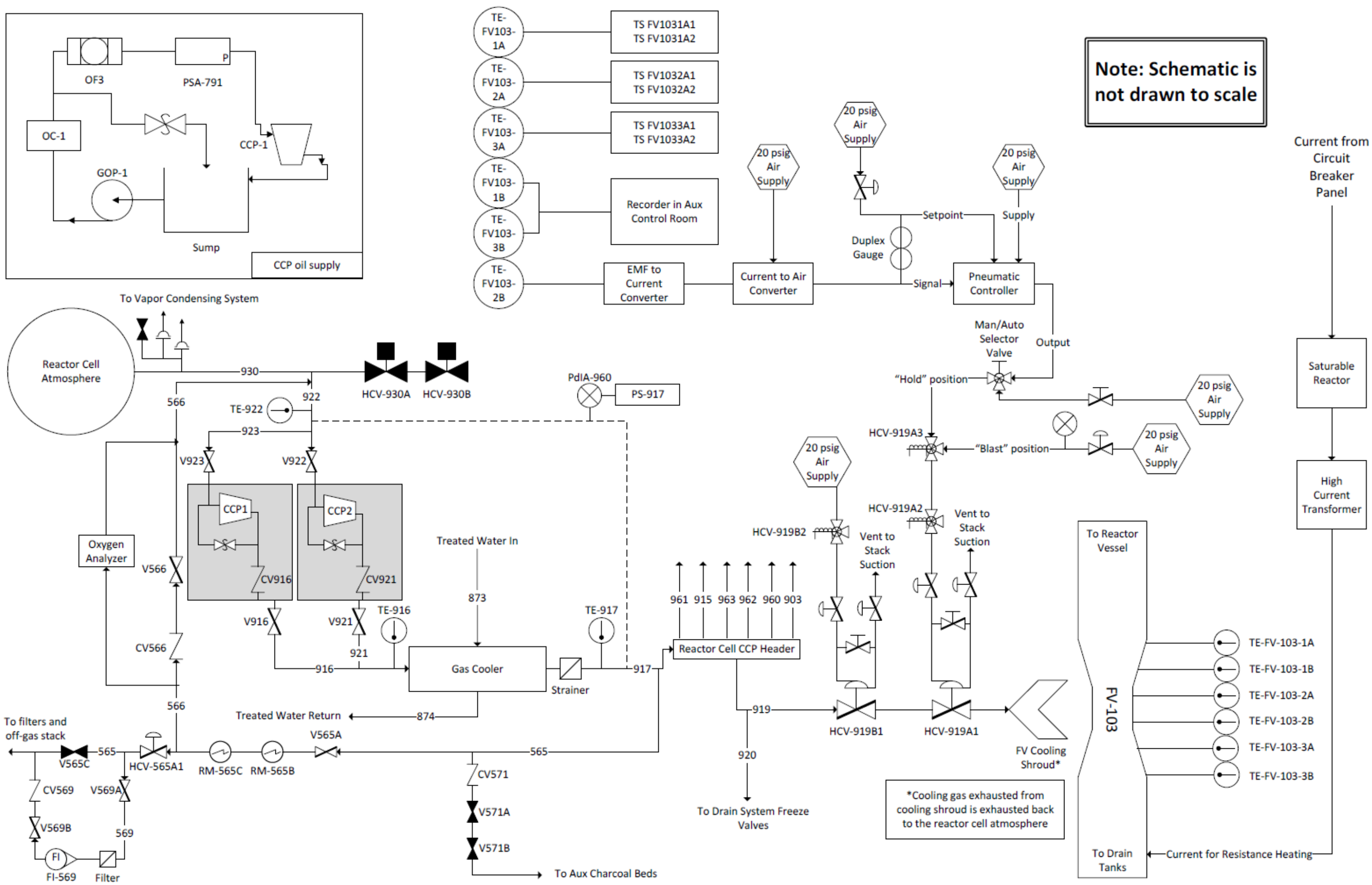


Figure 22: Schematic of MSRE FV-103 subsystem[54]

[54] Earlier versions of this schematic were published by Chisholm et al. [2018a, 2018b].

The results of the HAZOP study conducted on the MSRE CCS provide insights that are directly relevant to the freeze valve subsystem; the contribution of these results with respect to understanding freeze valve design and performance will be discussed in the following subsection. However, when the HAZOP approach was used to evaluate the components related to the control of the pneumatic valves in Line 919, it was somewhat difficult to ensure that the study was comprehensively capturing credible failure modes for all the components. Accordingly, FMEA was selected as an analysis tool to complement the HAZOP study in order to fully detail how individual component failures would relate to freeze valve function and performance, since the guiding principle of an FMEA is to evaluate and document the consequences associated with each failure mode for each component being analyzed [Stamatis, 2003]. FMEA was also selected for the analysis of the freeze valve subsystem because the components being studied were exclusively mechanical or electrical in nature [Milstein, 2001]. Finally, as demonstrated in Section 6.3, the consideration of specific effects associated with individual component failure modes allows the results of the FMEA to be more readily translated into basic events for FTA.

For the FMEA, the freeze valve subsystem was divided into two separate sections based on primary functions. The first section was composed of the CCS components, since this section has a single working fluid (i.e., reactor cell atmosphere gas) and its primary function, in the context of freeze valve performance, is to supply cooling gas to the freeze valve body. The second section was composed of the instrumentation and controls associated with the two pneumatic valves that determine the flow rate of cooling gas blown on the freeze valve body. The main working fluid in the control section is instrument air that is supplied at 140 kPa (20 psig).

As introduced in Section 3.2.8, an FMEA is performed by examining each component, one at a time, and then listing the credible failure modes associated with the equipment type and operating conditions. For the FMEA of the MSRE freeze valve subsystem, industry-standard component reliability databases (e.g., [Blanchard and Roy, 1998; CCPS, 1989; Eide et al., 1990]) were consulted to help ensure that no credible component failure modes were overlooked. When considering a given failure mode for a specific component, the effects of each failure were initially evaluated on a worst-case basis by assuming that any design features in the subsystem providing redundancy and/or diversity to mitigate the failure did not function properly. In the FMEA of FV-103, these effects were recorded and then the components or design features that might provide mitigation of consequences or reduction in likelihood were also documented. The FMEA analysis then proceeded systematically until all failure modes for each component in the subsystem had been considered and the results were recorded.

Approximately 220 failure modes were considered and documented during the FMEA of the FV-103 subsystem. An excerpt of the result is shown in Table 11. When compared to the HAZOP results, the FMEA results were more focused, and single rows of the results table did not generally describe entire event sequences. For the CCS components that had previously been analyzed using the HAZOP methodology, the FMEA did not contribute much new information regarding physical failures because only a few failure modes were relevant for each component. For example, a normally open manual valve could only fail to close or have an external leakage/rupture. However, the FMEA allowed for the evaluation of human errors that had not previously been addressed, such as the mispositioning of a manual valve. Further, the FMEA was particularly helpful to analyze the effects of the control components, such as the switches, sensing elements, and transmitters. Because the performance of the cooling gas control subsystem could be affected in different ways depending on the specific failure mode (e.g., a temperature switch spuriously opens/closes or fails to open/close), the FMEA proved to be a valuable tool to build the FT models that included these components.

Table 11: Excerpt of MSRE freeze valve FMEA results

Identification/ Description	Failure Mode	Effect	Safety Systems
"Supply" block valve for HCV-919B1 (normally open)	Spuriously closes	Closes HCV-919B1, isolates cooling gas flow to FV	Operator alarm on high freeze valve temperature, indication of freeze valve condition
Solenoid valve HCV-919B2	Spuriously closes	Closes HCV-919B1, isolates cooling gas flow to FV	Operator alarm on high freeze valve temperature, indication of freeze valve condition
Temperature switch TS-FV103-1A2	Spuriously opens	De-energizes HCV-919B2 and HCV-919A2, isolates cooling gas flow to FV	Operator alarm on high freeze valve temperature, indication of freeze valve condition
Thermocouple TE-FV103-1A	Failure (indicates lower temp than actual)	First, close TS-1A1 Then, open TS-1A2	Redundant temperature indication (TE-FV103-1B) displayed on recorder in aux control room

6.2.3. Qualitative Hazard, Risk, and Performance Insights

The following four failure modes were identified for the freeze valve subsystem: (1) spurious thawing; (2) spurious freezing, (3) failure to freeze on demand; and (4) failure to thaw on demand. Each of these failures is represented by unique initial and intended final configurations of components contributing to the functioning of the freeze valve. Additionally, the first two failures are represented quantitatively by failure rates per unit time, while the second two failure rates are per demand.

The HAZOP study results reinforced the safety concern posed by a failure of FV-103 to thaw when a fuel salt drain is desired, thereby preventing a drain of the fuel salt from the reactor vessel to the drain tank. The shutdown worth of the MSRE control rods could be lost if the fuel salt in the core vessel was sufficiently cooled due to the negative temperature coefficient of the liquid fuel [Tallackson, 1968]. Thus, a failure of FV-103 to thaw on demand could produce a scenario in which fuel salt remains critical in the fuel salt loop for an extended period of time. In this case, it is possible that conditions could be produced such that the physical integrity of the fuel salt boundary could be threatened and radioactive material could be released from the fuel salt loop [Beall et al., 1964].

The HAZOP analysis also suggested that a spurious thawing of FV-103 with the MSRE operating at full power should be further evaluated as a Postulated Initiating Event (PIE) of interest for the MSRE design. As discussed in Section 6.1, review of the MSRE operating experience revealed that this scenario did occur more than once during less than four full years of MSRE operations. In the case that sufficient means were available to remove decay heat from the fuel salt drained to the drain tank, an unanticipated fuel salt drain from full power represents an example of an operational upset, since the return to power operations after a drain could take an hour or more, depending on trouble-shooting and any repairs that may have been necessary [Guymon, 1973]. However, in the absence of sufficient drain tank cooling, the temperature rise of the fuel salt due to decay heat could be higher if the salt was in the drain tanks than if it remained in the fuel salt loop [Beall et al., 1964]. Thus, for the MSRE design, the event sequence in which FV-103 spuriously thaws at full power and the Drain Tank Afterheat Removal System fails to function represents a potentially risk-significant event sequence. This specific accident scenario was not considered in the MSRE Safety Analysis Report because the Afterheat Removal System was originally intended to function passively [Beall et al., 1964]. However, in the final MSRE design, drain valves in the Afterheat Removal System were required to actively close in order for it to function properly [Tallackson, 1968].

The results of the FMEA of the freeze valve components provided some qualitative insights regarding possible causes and effects of freeze valve failures. Overall, there was more redundancy regarding components enabling the MSRE freeze valve design to thaw than there was in the components that caused the valve to remain frozen. For example, if one of the pneumatic valves in the cooling gas supply line (Line 919) failed to close on demand, there was a redundant valve in series that would still isolate cooling gas flow if it succeeded to close. Conversely, the spurious closure of either of these valves would isolate cooling gas from the freeze valve body and subsequently initiate the thawing of the frozen plug of salt in the freeze valve. This insight supports the design philosophy stated by the MSRE design team, as the freeze valves were intended to fail in the "thaw" position to ensure the ability to enact a reactor drain in order to shut down the reactor when desired [Tallackson, 1968].

The FMEA results also suggested that, due to the design of the instrumentation and control for the MSRE freeze valve subsystem, the failure of many individual components would have been indistinguishable to the operator from the failure of other components. For example, all of the following component failures would have been indicated to the operator only by an increase in the indications of <u>all</u> freeze valve temperatures (due to insufficient "hold" cooling gas flow):

- Drifting of thermocouple TE-FV103-2B
- Malfunction of EMF-to-Current converter
- Malfunction of Current-to-Air converter
- Malfunction of Pneumatic controller
- Failure of pneumatic valve HCV-919A1 to change position

Because it would have been difficult for the operators to tell exactly which component had failed, many of the failures evaluated that would have resulted in a lack of cooling flow (to maintain a frozen valve) would have been difficult to distinguish in time to prevent an unanticipated thawing of the freeze valve (and subsequent draining of the fuel salt from the reactor vessel to the drain tanks).

Another example of insufficient instrumentation was that the low differential pressure alarm across the component cooling pump (CCP) was the only alarm that would immediately notify operators of low cooling gas flow to FV-103 before the temperature of the valve was substantially affected. Further, this annunciator sounded in the auxiliary control room rather than the main control room, which would reduce the likelihood that the condition would be noticed, correctly diagnosed, and corrected in less than 15 minutes -- before the plug in the freeze valve melted.

Similarly, the failure of a component downstream of the CCP differential pressure indication would only be indicated when 2 out of 3 temperature indications on the freeze valve exceeded their limits and triggered an alarm to notify the MSRE operators. Thus, the operators would have a short amount of time (or no time at all) to observe that alarm, diagnose the problem, and correct the situation before the freeze valve melted. Examples of failures that would fall under this category include failures of the pneumatic valves that modulate cooling gas to FV-103 and failures of the solenoid valves that control the position of the pneumatic valves.

6.3. MSRE Freeze Valve Reliability Estimates

Industry-standard reliability databases are commonly used by system designers and safety analysts to estimate failure rates for systems, subsystems, and components. These databases are composed of failure datasets collected from operational experience gained from sufficiently appropriate applications. For advanced nuclear reactor designs, reliability databases from applications other than commercial nuclear power generation, such as nuclear fuel cycle facilities and/or the chemical industry, can sometimes also be useful to help estimate failure rates for systems and components without significant commercial nuclear industry operating experience. However, because freeze valves are unique to MSRs, they represent an example of a system that has very little operational experience; thus, failure rate estimates for freeze valves cannot be found in generic databases. Because freeze valves perform flow isolation functions similar to mechanical valves (and because of the prevalence of the misnomer "freeze valve component"), MSR designers or safety analysts may be tempted to assume that the failure rates of freeze valves might be approximated using those of mechanical valves. However, an important conclusion from the analysis presented in this chapter is that freeze valves are notably different in design and operation from a solenoid valve or a pneumatic valve.

Thus, quantitative FTA was used to estimate failure rates for the FV-103 design from the MSRE. FTA is a deductive approach that starts with the top-level failure of concern and decomposes that event into failures that contribute to its manifestation until the fundamental causes of the fault (known as "basic events") are identified. These basic events include equipment failures and human response errors [CCPS, 1989; Milstein, 2001]. The impetus behind quantitative FTA of the components contributing to the proper functioning of the MSRE freeze valve subsystem is two-fold:

- The freeze valve function was important to the safety and operability of the MSRE, and an estimated failure rate is needed for any quantitative estimate of risk in the MSRE; and
- The developed MSRE freeze valve failure rates might provide a starting point for the analysis of MSR designs intending to use a similar freeze valve system design and control strategy to that used at MSRE.

The failure rates developed for the MSRE's FV-103 should be considered as starting points, rather than generic freeze valve failure rates, for a few reasons. First, there was no such thing as a "standard freeze valve subsystem design" in the MSRE, as discussed in Section 6.1.1. Any design differences between freeze valve subsystem designs should be fully evaluated for their potential impact on failure rates. Second, the failure rates modeled in the present analysis consider the failure of the MSRE freeze valve under normal operating conditions. The presence of accident conditions may affect the actual failure rate. Finally, the FTA in this work attempts to approximate the freeze valve failure rates using publicly-available generic component failure rates due to lack of operational experience. The most accurate estimate of component and system failure rate will result from compilation and analysis of a sufficient size of specific testing and operational data, once it is available.

6.3.1. Constructing and Evaluating Freeze Valve System Fault Trees

In the FT models for the MSRE freeze valve subsystem, the overall top event is the failure of interest for the freeze valve function being addressed. As previously mentioned, a spurious thawing of FV-103 during operation at power represents at least an operability concern for the MSRE, while a failure of the freeze valve to thaw on demand represents a safety concern. In the MSRE HAZOP study and FMEA, the results for different study nodes are listed in separate tables. As such, the highest level of intermediate events in the freeze valve FT models separates the basic events by the node of the MSRE in which the failure occurred. The remaining events were populated using the "Safety Systems" and "Effects" columns of the FMEA results.

During the construction of the FT for spurious thawing of FV-103 it was assumed that a failure in the components controlling the position of the pneumatic valves in the freeze valve cooling gas line would not be reversed by operator action in time to prevent draining of the fuel salt, due to the limited amount of information available to the MSRE operators (as discussed in Section 6.2.3). Additional assumptions used when constructing the models included:[55]

1. Minor cooling gas temperature transients (e.g., reduced heat removal in the gas cooler) would not produce a spurious thaw;
2. Spurious operation of manual valves did not occur; and
3. Common cause failures (CCFs) for a group size of two components could be approximated using a generic beta factor (i.e., $\beta = 0.024$) [Mosleh et al., 1998].

[55] Failure of the freeze valves due to loss of power supply or complete loss of instrument air supply were not included in the models; this treatment is consistent with the boundaries used in industry-standard component reliability databases [CCPS, 1989; Eide et al., 1990].

One known limitation of the present analysis is the assumption of a binary, "success or failure" of the freeze valve system. Based on the available analysis, the use of FTA was a necessary simplification; however, the possibility of a partial thaw or an imperfect freeze of a salt plug was not modeled. Therefore, there are more paths to freeze valve failure than are represented in this study. Full accounting of all freeze valve scenarios would need to be captured by PRA of the MSRE. Furthermore, because failures of the freeze valve function depend on thermodynamics and can be time dependent, it is possible that tools other than traditional FTA would be useful to develop a more complete understanding of freeze valve failures.

The FT models were generated using EPRI's Computer-Aided Fault Tree Analysis (CAFTA) software [EPRI, 2014]. The probabilities of basic events were obtained by a review of the available literature and incorporated into the model. This basic event data is displayed in Appendix D. The cutsets for each FT were calculated using CAFTA's built-in cutset generator, and EPRI's UNCERT software was used to estimate the failure probability of the top event including the uncertainty associated with the basic event probabilities [EPRI, 2014]. The UNCERT analysis was a Monte Carlo simulation with 100,000 runs (i.e., $N = 100{,}000$). The error factors for the freeze valve failure rate distributions were assumed to follow a lognormal distribution since it is commonly used in the nuclear industry to represent component failure behavior; thus, for each failure rate the error factor was calculated as the ratio of the 95th percentile estimate to the median value calculated by the UNCERT analysis.

6.3.2. Failure Rate of FV-103 to Thaw on Demand

In the construction of the FT model, it was assumed that the failure of FV-103 to thaw occurred after the MSRE operator initiated a manual "emergency drain" using a switch in the control room, consistent with MSRE operating procedures [Guymon, 1966]. The FT model reflects the assumptions that the freeze valve would not thaw if the cooling gas blowing across the valve assembly is not isolated or if the resistance heating of the drain/fill line (Line 103) fails. The cooling gas could be isolated by either of the two pneumatic valves in the FV-103 cooling gas supply line (Line 919). The arrangement of the control system to close these pneumatic valves is identical; the initiation of the drain demand by the operator de-energizes solenoids (HCV-919A2 and B2) to isolate the instrument air that keeps the pneumatic valves open. In the event that the control air to the pneumatic valves is not isolated by the solenoid valves, it would be possible for the operator to close a manual valve in the MSRE instrument air system to allow the pneumatic valves to close.

The fuel salt drain/fill line (Line 103) was heated by passing an electrical current through the pipe walls [Robertson, 1965]. Control of the current was provided by passing current from a circuit breaker panel through a saturable reactor[56]; the output of the saturable reactor was then passed through a special transformer to deliver the current to Line 103 [Robertson, 1965]. A failure of the resistance heating of the line could be due to a failure of either of these two components.

As shown in Table 12, the mean estimated failure rate of FV-103 to thaw on demand is 2.50E-05/demand. The FT model used to obtain this value is displayed in Appendix D. A review of the ORNL MSRE literature revealed no failures of FV-103 to thaw when demanded either manually by the operator or automatically by the MSRE safety system [Guymon, 1973]; however, the total number of times that this freeze valve was demanded to thaw was limited. Although it is indicated by Guymon [1973] that FV-103 experienced a cumulative total of 91 freeze/thaw cycles over the 4 years of MSRE operations, all but 26 of the 91 cycles were indicated to be scheduled shutdowns. "Normal" (i.e., scheduled) shutdowns of the MSRE were distinct from emergency (i.e., unscheduled) shutdowns, and the operators used different operating procedures and control schemes depending on the type of shutdown [Guymon, 1966]. Since an emergency drain was only demanded a total of 26 times over the entire duration of MSRE operation, a quantitative estimate of a failure to thaw after a manual emergency drain demand based upon the operational experience cannot be made without significant uncertainty.

Table 12: Calculated freeze valve failure rates, MSRE as designed

Failure Mode	Mean Failure Rate	Units	Error Factor (Lognormal Distribution)
Failure to Thaw on Demand	2.50E-05	/demand	8.14
Spurious Thaw (Failure to Remain Frozen during Normal Operations)	2.23E-01	/year	2.39

Because all that is required for successful thawing of the freeze valve is isolation of cooling gas and supply of heat to the drain line, there are only 8 cutsets from the FT model for failure of FV-103 to thaw on demand. Additionally, due to the redundancy of valves in the system, the only cutsets with estimated frequencies greater than 1E-6/demand involve either failures of the

[56] A saturable reactor is a special form of inductor that provides a simple means to remotely and proportionally control alternating current (AC); the AC is roughly proportional to the direct current (DC) through the control winding of the component.

components used for the resistance heating of the line (i.e., the saturable reactor or the transformer) or CCFs of the valves associated with isolation of the cooling gas (i.e., HCV-919A1/B1 or HCV-919A2/B2).

6.3.3. Failure Rate for a Spurious Thaw of FV-103

At the same depth of analysis, there are more basic events that contribute to the failure mode of a spurious thawing of FV-103 than for the failure of FV-103 to thaw on demand. There are some failures in the CCS that could be diagnosed by the operator and corrected by starting the standby CCP blower. These failures include failures of the operating blower or blockages in the lines associated with the operating blower. Subsequent failures that could prevent flow from being restored could result from a failure of the operator to correctly diagnose the problem, a failure to initiate the starting of the standby blower, or a failure that prevents the standby blower from running. Failures in the CCS that could not be corrected by starting the standby blower include blockages that would isolate the cell exhaust flow from reaching the MSRE stack (via Line 565) because these failures would increase the pressure in the reactor cell and trigger the response from the MSRE safety system to close the valves that allow cooling gas to flow to the freeze valve [Tallackson, 1968]. These valves would also be closed if a rupture in the cell exhaust line dramatically decreased the pressure in the CCS [Tallackson, 1968].

Other failures that could allow an inadvertent thawing of FV-103 include failures that would close either pneumatic valve that allows cooling gas to flow to the freeze valve (HCV-919A1 or B1). These valves could be closed due to any of the following failures:

- Failure of the pneumatic valve itself;
- Failure of the solenoid valve supplying instrument air to keep the pneumatic valve open;
- Failure of the temperature switch energizing the solenoid valve; or
- Failure of the temperature sensor energizing the temperature switch.

In the case of the throttled cooling gas pneumatic supply valve (HCV-919A1), the possibility also exists for the controllers that set the position of the pneumatic valve to fail and cause the pneumatic valve to reduce the cooling gas flow discharged onto the freeze valve assembly.

It was assumed that the heaters affecting the heat balance of the plug in FV-103, including the resistance heating of Line 103 and the reactor furnace heaters, were operated at capacity; therefore, an over-temperature of the heaters was not considered to be a valid cause of a spurious thaw.

As shown in Table 12, the mean estimated likelihood of a spurious thawing of FV-103 is 2.23E-01/year. The FT model used to obtain this value is displayed in Appendix D. Assuming that FV-103 would be required to remain frozen during normal operations for 24 hours a day, 365 days a year, this result estimates a failure rate of 2.54E-05/hr. This assumption does not reflect the actual operations at MSRE,[57] but likely reflects the desired operability for a commercial MSR.

Over the course of 21,788 total hours of fuel salt circulations, the MSRE team mentioned three inadvertent drains of the fuel salt [Guymon, 1973], which averages out to 1.38E-04 spurious operations per hour (1.21 spurious operations per year). Considering the short duration of MSRE operations, the less than one order of magnitude difference between this value and the estimated failure rate for FV-103 suggests the FT model is in relatively good agreement with the operating experience. The individual causes of the inadvertent drains observed at the MSRE were as follows:

- A mechanical failure of the operating blower (CCP1) while the standby blower (CCP2) was secured for maintenance;
- An oil leak in the operating blower (CCP1) while the standby blower (CCP2) was secured for maintenance; and
- A failure of both temperature switches to close with the throttled cooling gas supply valve (HCV-919A1) not sufficiently open.

All three of the above scenarios are represented by cutsets in the FT model. Combined, these cutsets have an estimated frequency of 4.75E-3/year, which is approximately 2% of the overall estimated frequency of a spurious thaw. However, review of the MSRE operating experience revealed that one basic event that contributed to HCV-919A1 not being sufficiently open during the third failure in the above list was an incorrect adjustment of a control setpoint by an operator [Guymon, 1973]. Operator errors such as this were not included as basic events in the FTA of FV-103; thus, a more comprehensive Human Reliability Analysis (HRA) and addition of operator errors to the FT models could reduce the difference between the estimated failure rate and the failure rate observed during MSRE operations.

An interesting insight from the FTA results is that 4 of the 6 cutsets with estimated frequencies greater than 1E-2/year are single failures of components in the CCS that are not in close physical proximity to FV-103. This result demonstrates that many of the component failures that are likely to produce a spurious thawing of the freeze valves occur in components that would not

[57] Over its 4 years of operation, the MSRE only had salt circulating in the fuel salt loop for a total of 21,788 hours [Guymon, 1973].

normally be mentioned as part of the "freeze valve component." The implication for designers and analysts of modern freeze valve subsystems is that it is important to thoroughly understand and document all components that contribute to, or interface with, the proper functioning of a system as complex as the MSR freeze valve.

6.3.4. Failure Rate Sensitivity Study

As mentioned in Section 6.1, the intent of the MSRE designers was for FV-103 to fail in the open (i.e., thawed) position in order to allow the fuel salt to be secured in the drain tanks in the case of an accident at MSRE. Considering the qualitative insights gained from PHA studies of the freeze valve system regarding the number of components providing redundancy to ensure that FV-103 would thaw on demand, it is possible that designers of a freeze valve subsystem may face a design trade-off between the likelihood of a failure to thaw on demand and the likelihood of a spurious thaw during normal operation. More specifically, it is possible that the addition of redundant means to isolate cooling gas flow when desired could result in the addition of components that could fail and isolate cooling gas flow unintentionally.

In order to evaluate the extent to which the redundancy in the cooling gas control subsystem affected the failure rates estimated for FV-103, a sensitivity study in the form of additional FTA was conducting assuming that pneumatic valve HCV-919B1 and all components solely associated with its operation (i.e., HCV-919B2 and the associated "supply" block) were not included in the design for the FV-103 system. The control strategy for pneumatic valve HCV-919A1 was assumed to remain the same, and CCFs related to the removed valves were not included in the new FTA. The failure rates estimated by this FTA are displayed in Table 13.

Table 13: Sensitivity study - modified freeze valve failure rates assuming no redundant cooling gas isolation valve

Failure Mode	Mean Failure Rate	Units	Error Factor (Lognormal Distribution)
Failure to Thaw on Demand	3.02E-04	/demand	10.76
Spurious Thaw (Failure to Remain Frozen during Normal Operations)	2.09E-01	/year	2.45

As expected, by removing the basic events associated with closing of HCV-919B1, the estimated failure rate of FV-103 to thaw on demand was increased by approximately an order of magnitude. This result supports the qualitative conclusion from the FMEA that the redundancy of the freeze valve system to isolate cooling gas flow suppresses the likelihood that the valve will not thaw on demand.

However, modifying the FT model for a spurious thawing of FV-103 not to include the basic events associated with the functioning of pneumatic valve HCV-919B1 only decreased the estimated failure frequency by about 6%. Similar to the results discussed in Sect. 4.3, the 4 cutsets with the highest probability were due to failures of components that contributed to the function of supplying cooling gas rather than failures of components in the valves controlling and isolating the flow of cooling gas across the body of FV-103. Collectively, these 4 cutsets represented about 67% of the overall estimated spurious thaw failure rate. Taken together, these FTA results suggest that a reduction in redundant means to isolate cooling gas has only a marginal (if any) impact on the expected frequency of a spurious thaw; however, due to the specifics of the MSRE CCS, a more substantial improvement to reliability could be made by altering the design, controls, and operation of the subsystem delivering the cooling gas. Moreover, because no failures of CCS components were identified that would lead to a failure of FV-103 to thaw on demand, it is suggested that modern designers basing their freeze valve system designs on the MSRE freeze valve system design could reduce the likelihood of a spurious failure without decreasing the likelihood of a failure to thaw on demand by additional attention to the design of the subsystem that supplies cooling gas to the freeze valve.

6.4. Observations from Freeze Valve Studies

The freeze valve continues to be widely adopted in MSR design efforts because a mechanical valve that can tolerate the corrosive and high-temperature environment in a molten salt system has not yet been demonstrated. Freeze valve systems were incorporated into the MSRE design for an array of functions, including isolation of the fuel salt loop during normal operations, performing a safety function during accident scenarios, and for use in non-power and maintenance evolutions. At first glance, the simplicity of the freeze valve body seems to have been a solution for the problems associated with the active portions of a mechanical valve, but it also necessitated the reliability of several auxiliary subsystems and numerous components. First, active cooling of the frozen salt plug in the freeze valve body was necessary during normal operations. Additionally, active isolation of the cooling gas flow and a targeted application of heat, including detailed consideration of the localized heat balance, was necessary to enact a thawing of the plug to allow the fuel salt to drain.

Recently, research has restarted on freeze valve design and operations; however, the most extensive source of freeze valve information still comes from the team that designed and operated the MSRE at ORNL in the 1960’s. In the MSRE, the success of the freeze valve to thaw on demand or remain frozen during power operation depended on two subsystems comprised of power-operated sensors, mechanical valves, and other active components. Accordingly, as executed at the MSRE, the freeze valve system was not a fully passive safety feature.

Although the performance of the freeze valves was described by the MSRE team as "satisfactory," this characterization was evidently based on the lack of a failure to thaw when requested and there were design details that resulted in the operability being less than optimal. Examples of such features included complicated indications of freeze valve condition to the operators and unreliable temperature switch setpoints that contributed to three unscheduled drains of the fuel salt system over the course of 21,788 hours of salt circulation due to failures of FV-103.

Recent operating experience on salt loops, including the catastrophic failure of a freeze valve body during testing in China, has shown that operation of a freeze valve remains a considerable technical challenge and supports the observation from the MSRE team that substantial configuration-specific testing and as-installed adjustment is required to develop a control strategy for these valves. Furthermore, recent thermodynamic analyses suggest that the feasibility of a freeze valve that melts due to decay heat in an MSR design may not be as readily available as envisioned by some. Finally, tests in small scale salt loops have indicated that freeze valve system performance is highly dependent on physical configuration of nearby heat sources and sinks. The current understanding of freeze valve performance is only a small piece of the technical understanding needed for design, however, and the design issues are complicated; they depend on scale, heat balances, and other particulars of MSR concept implementation.

Original work was presented in this dissertation in which FT models were constructed to estimate preliminary failure rates for the MSRE freeze valve design. PHA methods (including HAZOP studies and FMEA) were particularly useful to structure the trees and also provided qualitative insight to freeze valve subsystem design. One such insight, among many, was that the MSRE design included significantly more redundancy to allow the freeze valves to thaw, than to remain frozen. Therefore, as MSR developers advance the maturity of their freeze valve system designs, it will be essential to conduct analyses to evaluate how design decisions affect reliability and safety. The quantitative results presented in Section 6.3 suggest that the reliability of the MSRE freeze valve system to remain frozen during normal operations could be enhanced by improving the design of the subsystem supplying cooling gas to the freeze valve body, and that these design changes should have minimal negative influence on the reliability of the freeze valve system to drain on demand.

Future efforts should include modeling additional freeze valve system failure modes to be used in analyses of MSR risk assessment activities. For example, a failure of the freeze valve to freeze on demand represents a PIE during the filling evolution of an MSR. Additionally, as evident from the operating experience from the MSRE and the TMSR FLiNaK test loop, freeze valve body ruptures have occurred. MSR designers and safety analysts would benefit from an estimate of the likelihood of this type of failure and identification of design and/or control approaches that would minimize the risk associated with this failure. Research towards characterizing and assuring the quality of the frozen salt plug (e.g., size, density, homogeneity, etc.) will be necessary, especially for valves that a required to perform in safety-significant scenarios.

Finally, thorough evaluation of freeze valve design, performance, and analysis experience to-date suggests that the design of a freeze valve system for use in a modern MSR is not an insignificant exercise. Designers should not dismiss the possibility of using other technical approaches for molten salt flow isolation. For instance, alternatives to a freeze valve system like that used in the MSRE include the combination mechanical-freeze valve concept conceived at ORNL after conclusion of MSRE operations [Bettis et al., 1972] and the possibility of modifying off-the-shelf valves for use in molten salt systems [Howard et al., 2019]. Especially because the technical maturity of all solutions to isolate salt flow in LF-MSR application is relatively low, it will be important for MSR stakeholders to advance the state of knowledge surrounding freeze valve systems, and other alternatives under consideration, through a combination of physical tests, computational simulations, and design-related studies.

CHAPTER 7, EVENT TREE ANALYSIS OF MSRE OFF-GAS SYSTEM

As evident from the review of prior safety assessment efforts for LF-MSR designs presented in Section 2.4.2, a quantitative assessment of the risk associated with an LF-MSR OGS has not performed to-date. A quantitative estimate of the frequency and consequences of event sequences that could result in the release of hazardous material from an LF-MSR could allow for a comparison of the risk inherent to the fuel salt loop (which contains the inventory of radioactive material on which nuclear reactor designers commonly focus) to the risk inherent to the OGS (which contains an inventory of radioactive material that is not commonly the focus of reactor designers). Additionally, the quantitative Event Tree Analysis (ETA) and Fault Tree Analysis (FTA) needed to produce a quantitative estimate of risk represent fundamental building blocks towards a comprehensive PRA model of an LF-MSR design. Finally, a quantitative evaluation of risk associated with various event sequences and Structures, Systems, and Components (SSCs) in a design can be used to develop risk insights regarding the safety approach for a system or subsystem.

An example of an NRC-endorsed technology-inclusive approach to risk-inform the design and safety assessment processes for advanced nuclear reactors is described by the Licensing Modernization Project (LMP) [NEI, 2019; NRC, 2019c]. The information flow between various tasks in this approach is depicted in Figure 23. The process described by the LMP is intended to select Licensing Basis Events (LBEs)[58] in an RIPB manner and help reactor developers identify Required Safety Functions (RSFs), Safety Related SSCs (SR-SSCs), and evaluate Defense-in-Depth (DID) for their design. Fundamental to an RIPB approach to these tasks is the use of a quantitative Frequency-Consequence evaluation correlation (or "F-C target") that is based on insights gained from a review of existing regulatory safety goals; the LMP F-C target is depicted in Figure 24. In short, if event sequences that result from a PIE (or group of PIEs) that have potential consequences that include the release of radioactive material from the MSRE OGS, it will be possible to utilize the LMP process to identify which functions and SSCs in the MSRE are the most important to the safety case. In order to minimize the overall risk associated with a design, these RSFs and SR-SSCs would require special treatment to ensure they possess high reliability and performance.[59]

---

[58] LBEs are the entire collection of event sequences considered in the design and licensing basis of a nuclear power plant [NEI, 2019].

[59] The risk-informed categorization and treatment of SSCs for nuclear power plants is covered in 10 C.F.R. § 50.69.

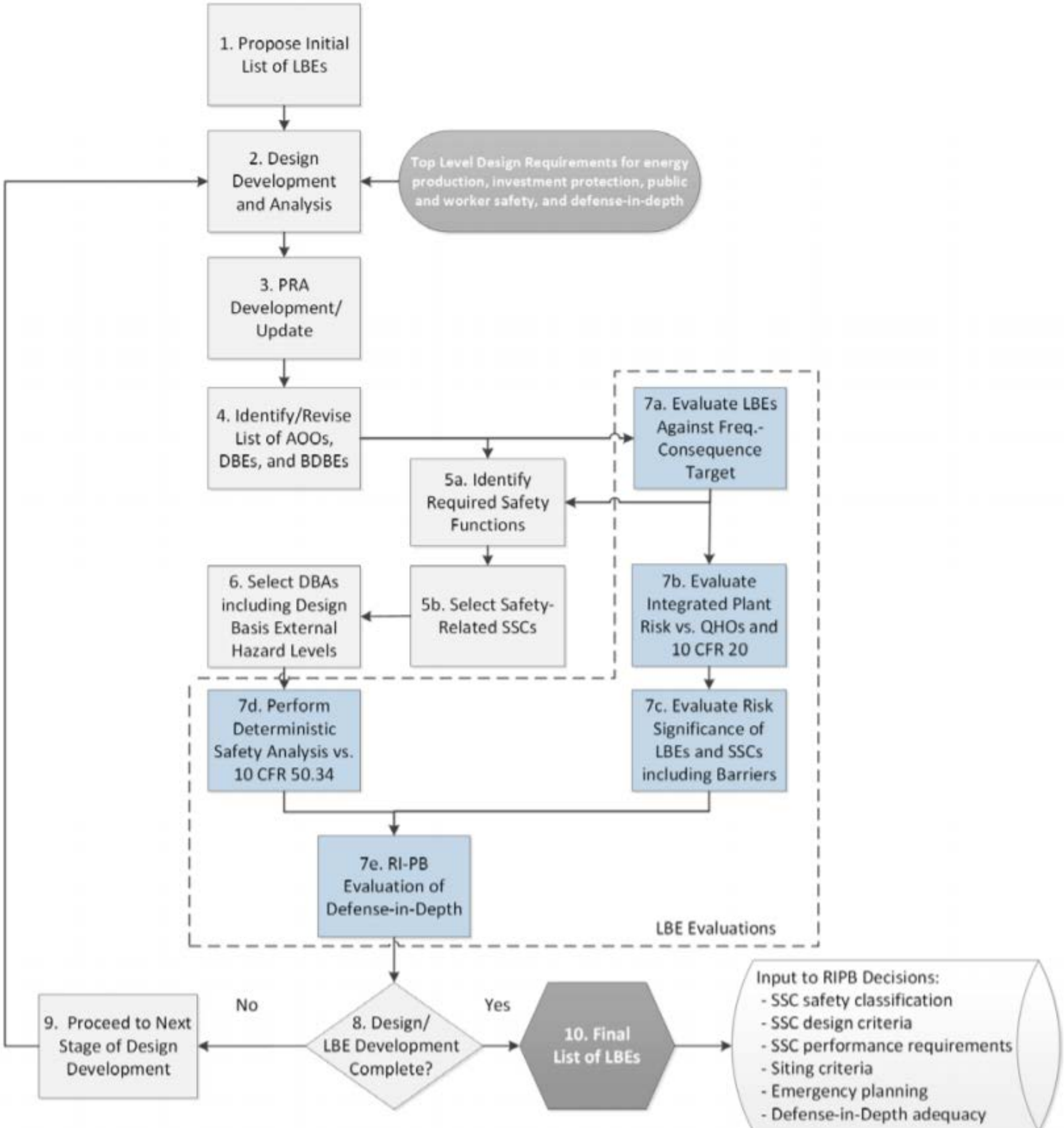


Figure 23: Process for selecting and evaluating Licensing Basis Events (LBEs) [NEI, 2019]

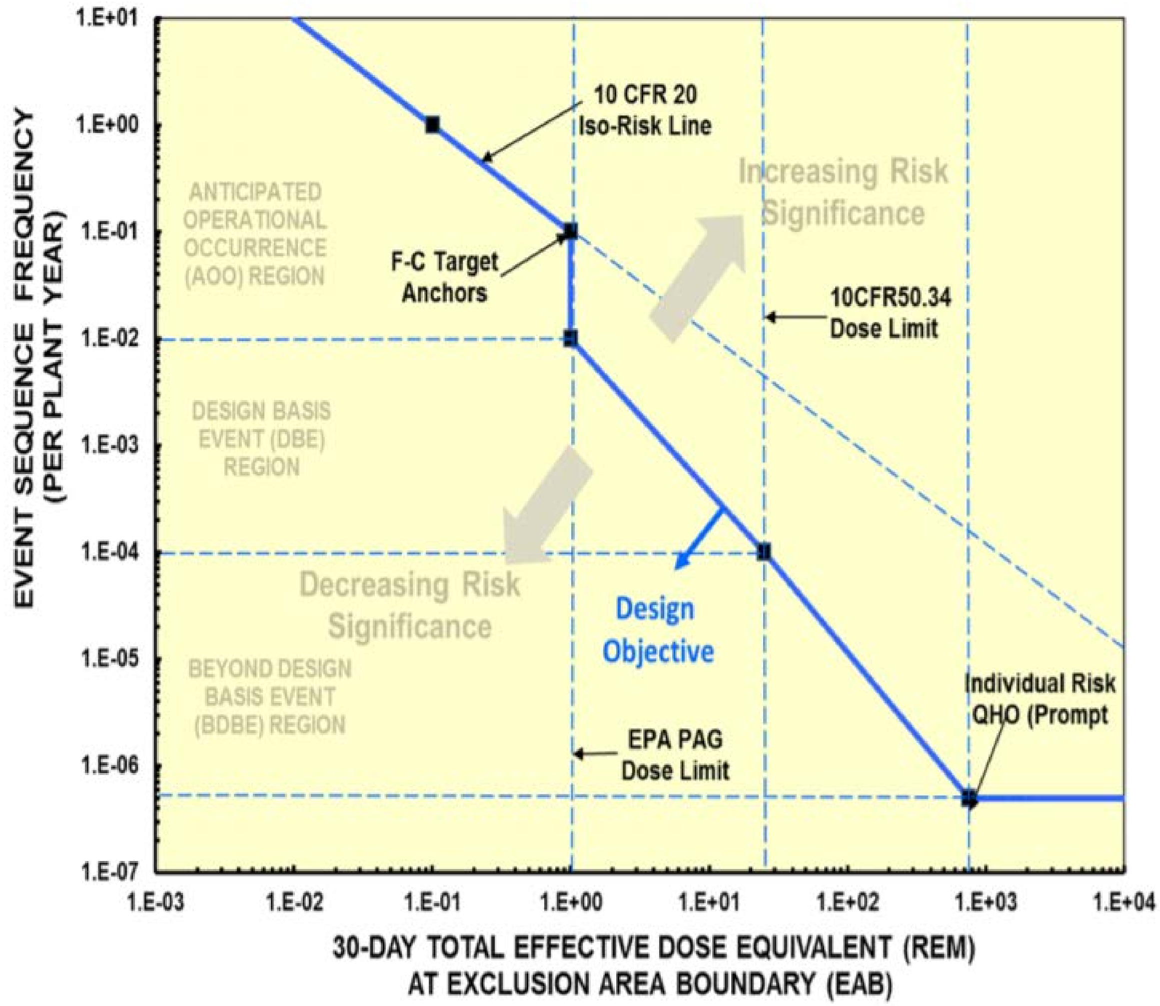


Figure 24: Frequency-Consequence (F-C) target suggested by LMP for evaluation of LBEs [NEI, 2019]

7.1. Analysis Approach

Chapter 4 discusses the inventories of radioactivity in the MSRE design that were identified and characterized to prepare for HAZOP studies of 4 different nodes in the MSRE: the fuel salt loop, the OGS, the fuel processing system, and the CCS. This characterization was used to down-select the radioactive material inventory in the MSRE OGS during normal operations (i.e., the Operate-Run POS) as the focus of the limited-scope quantitative risk analysis summarized in this chapter. As discussed in Chapter 5, the results of the HAZOP studies were combined with the development of an MLD to identify and group PIEs for the inventories of radioactive material analyzed during the HAZOP studies, including the OGS. From the results of the search for PIEs, one group of PIEs that were identified during the HAZOP studies to have the potential of resulting in the release of radioactive material from the OGS to the atmosphere was selected to be modeled using ETA.

The HAZOP results (supplemented by original MSRE design and operations information when necessary) can be used to identify the pivotal events that structure the ET model and ultimately discern between individual event sequences and their associated end states. Each pivotal event can then be represented by linking it to a FT model, which can be constructed using the results of the HAZOP studies and additional information from the original MSRE design information. Using the developed ET and FT models, the frequencies of event sequences can be estimated by using component reliability data and estimates for human reliability for quantification. Uncertainties in the frequency estimates can be included in the models and characterized using EPRI's CAFTA and UNCERT Software [EPRI, 2014].

Once the frequency of the modeled OGS event sequences has been estimated, each event sequence can be classified as one of three possible categories of LBEs, as suggested by the LMP and endorsed by the NRC [NEI, 2019; NRC, 2019c]. The three categories of LBEs are as follows [NEI, 2019]:

- Anticipated Operational Occurrences (AOOs) - Anticipated event sequences expected to occur one or more times during the life of a nuclear power plant, which may include one or more reactor modules. Event sequences with mean frequencies of 1×10^{-2}/plant-year and greater are classified as AOOs.
- Design Basis Events (DBEs) - Infrequent event sequences that are not expected to occur in the life of a nuclear power plant, which may include one or more reactor modules, but are less likely than AOOs. Event sequences with mean frequencies of 1×10^{-4}/plant-year to 1×10^{-2}/plant-year are classified as DBEs.
- Beyond Design Basis Events (BDBEs) - Rare event sequences that are not expected to occur in the life of a nuclear power plant, which may include one or more reactor modules, but are less likely than a DBE. Event sequences with mean frequencies of 5×10^{-7}/plant-year to 1×10^{-4}/plant-year are classified as BDBEs.

Using the LBEs identified, the application of the LMP approach [NEI, 2019] will then be explored to illustrate how an advanced reactor developer at an early stage of design might conduct a preliminary iteration of tasks such as identification of RSFs, classification of SR-SSCs, and evaluation of DID. The final analysis that will need to be performed to develop a quantitative estimate of risk associated with the MSRE OGS LBEs is an initial quantitative estimate of the consequences associated with the end state for each event sequence. To allow for the performance of the tasks in the LMP process, the consequence metric used would be 30-day total effective dose equivalent at the MSRE Exclusion Area Boundary (EAB) (as shown on the x-axis in Figure 24). The EAB for the MSRE is defined as 3000m from the MSRE building [Beall et al., 1964], and a preliminary dose consequence will be calculated for an assumed maximally exposed individual.

7.2. ETA and FTA Development

An overview of the MSRE OGS was given in Chapter 4, and a schematic of the major OGS components was shown in Figure 11. A more detailed diagram (including relevant instrumentation) is shown in Figure 25. The event sequence diagram developed for the OGS is shown in Figure 26, and the rows of the MSRE HAZOP study results that were helpful in structuring the model are displayed in Appendix B. The following subsections will discuss the development and quantification of the FT models that were used to estimate the frequency of each event sequence. The FT models and basic event data used to quantify them are shown in Appendix E.

The IE in the ET model is a leak from one of the off-gas components within the reactor cell, which is the portion of the OGS that contains gaseous radionuclides that are at their highest concentration. This IE represents the OGS PIE group "release of radioactive material to the reactor cell" identified in Chapter 5. Once this radioactive material is released from the OGS to the reactor cell atmosphere, the MSRE system is designed such that this contaminated atmosphere will be drawn into the CCS by the operating component cooling pump (CCP) blower. A portion of this gas flow is continuously being checked by process radiation monitors, and after passing through the monitors, it is exhausted to the atmosphere via the MSRE stack. If either of the two monitors detects excess radioactivity in the gas flow, multiple automatic system responses are initiated by the MSRE control system. First, a drain of the fuel salt system is initiated. Once the fuel salt has been successfully drained and secured in the drain tanks, the off-gas would be routed to the auxiliary charcoal bed, bypassing the failed portion of the OGS, which would terminate the leak of OGS flow to the reactor cell atmosphere [Guymon, 1966]. Secondly, a pneumatic valve downstream of the radiation monitors in the cell exhaust line is intended to close to prevent contaminated cell atmosphere from being exhausted to the stack [Tallackson, 1968]. Successful isolation of this flow would prevent the radioactive material from being exhausted to the environment.

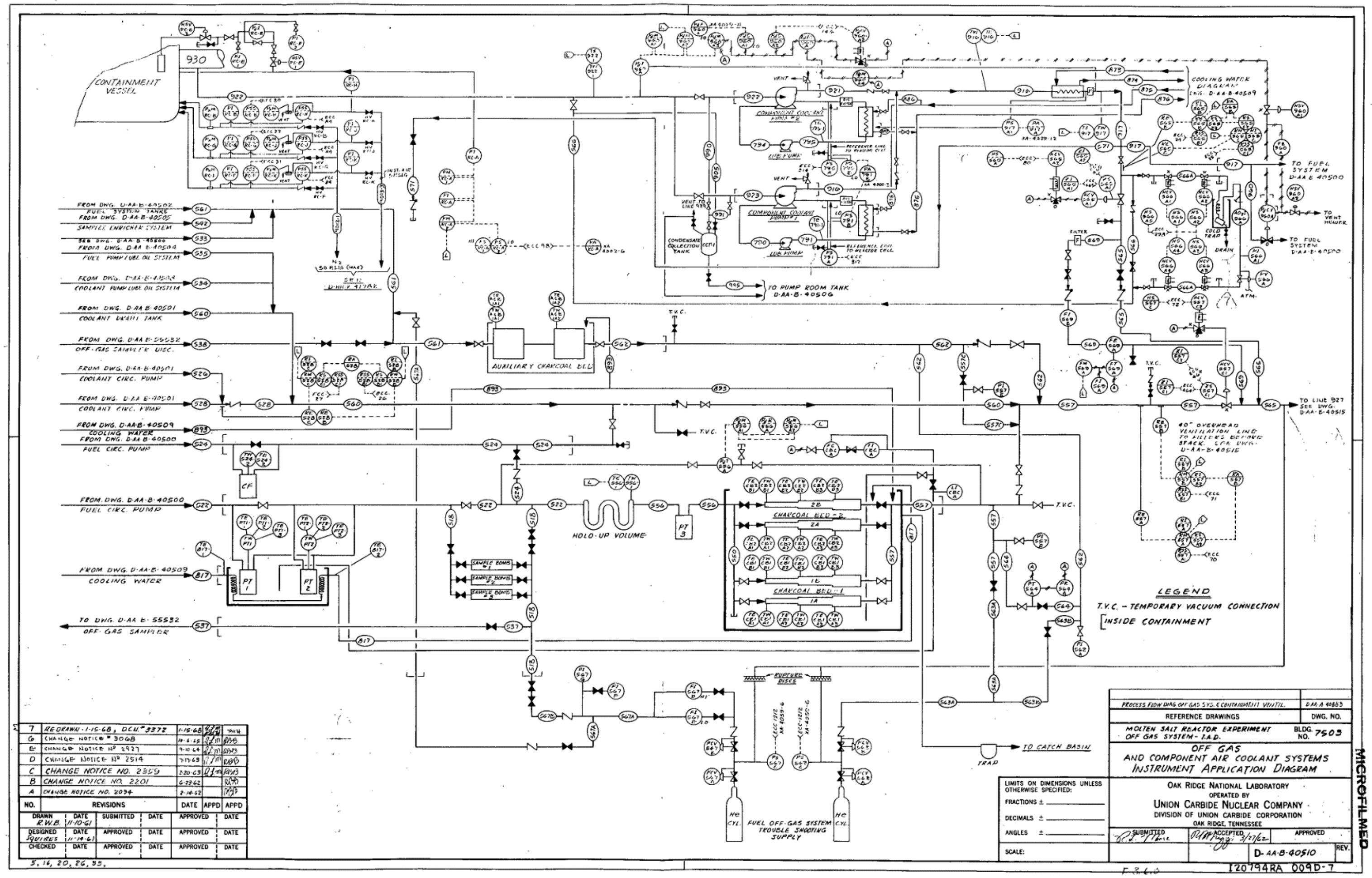


Figure 25: MSRE OGS and CCS instrument application diagram [Moore, 1972]

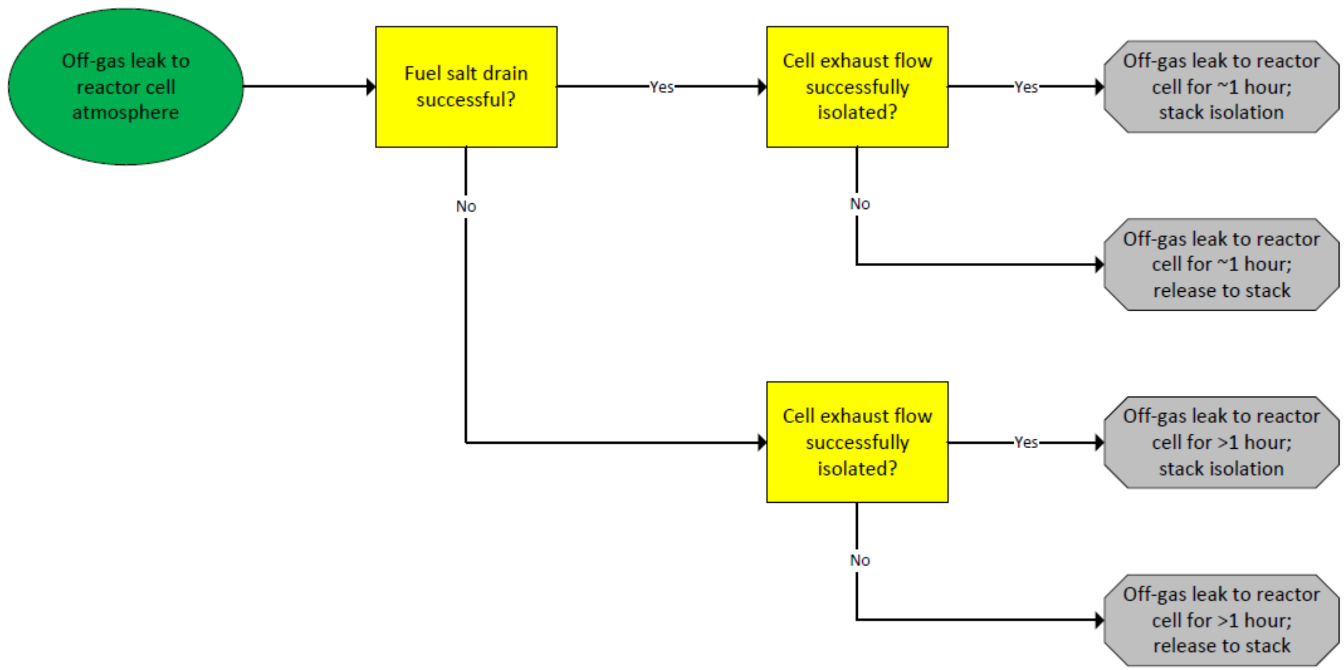


Figure 26: Event sequence diagram for a release of radioactive material from the main OGS to the reactor cell during normal operations

7.2.1. Initiating Event: Release of Radioactive Material to Reactor Cell

A leak from one of the off-gas components within the reactor cell was chosen as the IE for the OGS ET model because this portion of the off-gas line will contain gaseous radionuclides that are at their highest radioactivity. Also, a detailed understanding of occurrences that could result in a failure of the MSRE CCS to prevent a release of material from the reactor cell to the atmosphere was developed through the performance of the HAZOP study on the CCS (see Chapter 4) and through the development of the MSRE MLD (see Chapter 5). The portion of the OGS line within the reactor cell contained a 91 cm- (3 ft.-) long "jumper" section of 1.3 cm (½ in.) ID, type 304 stainless flexible hose, an O-ring flange on each side of the jumper, 21 m (68 ft.) of 10 cm (4 in.) stainless steel pipe, and another mechanical connection to connect the 4 in. pipe to ½-in. pipe before exiting the reactor cell [Compere et al., 1975]. The purpose of this run of 10 cm (4 in.) pipe was to provide at least 45 minutes of delay time for the short-lived fission products exiting the gas space of the fuel salt pump bowl, especially the noble gases.

The fault tree for the IE of leakage from Line 522 can be seen in Section E.1 of Appendix E. Originally, three independent phenomena were identified using the MSRE HAZOP results that could result in leakage (or rupture) of Line 522:

1. A failure of a component that constitutes a part of the pressure boundary under normal operating conditions;
2. A pressure increase in the line due to a blockage downstream in the OGS; or
3. Leakage at one of the connections due to differential thermal expansion/contraction.

However, upon review of the design information, differential thermal expansion/contraction was eliminated from the FT model for multiple reasons. First, the differential expansion or contraction would have to result from a heating or cooling deviation in Line 522. The design documentation [Robertson, 1965] did not discuss a heater that was used to add heat to Line 522 during normal operations, and heat was removed from the volume hold-up piping by gas flow from the CCS, which failed multiple times during MSRE experience without causing a leak [Guymon, 1973]. More importantly, it was assumed that the design of the jumper section would allow for the thermal expansion/contraction associated with temperature changes in the portion of the MSRE OGS piping considered for this FT.

Leakage during normal operation could occur in any of the three piping connections, the flexible "jumper" section of Line 522, or the 10 cm (4 in.) holdup section of pipe. Regarding failures downstream that could increase the pressure in Line 522, the FT model assumes that the pressure buildup due to a blockage downstream would result in leakage from the portion of Line 522 inside the reactor cell and that the reactor operators would not be able to take corrective action to prevent the failure, due to limited pressure and flow indication in the OGS. Additional assumptions made include (1) that spurious closure is not a valid failure mode for manual valves and (2) the plugging of a single charcoal bed would not produce a pressure transient significant enough to cause a leak/rupture, due to the existence of a parallel pathway for flow through the other (unplugged) charcoal bed.

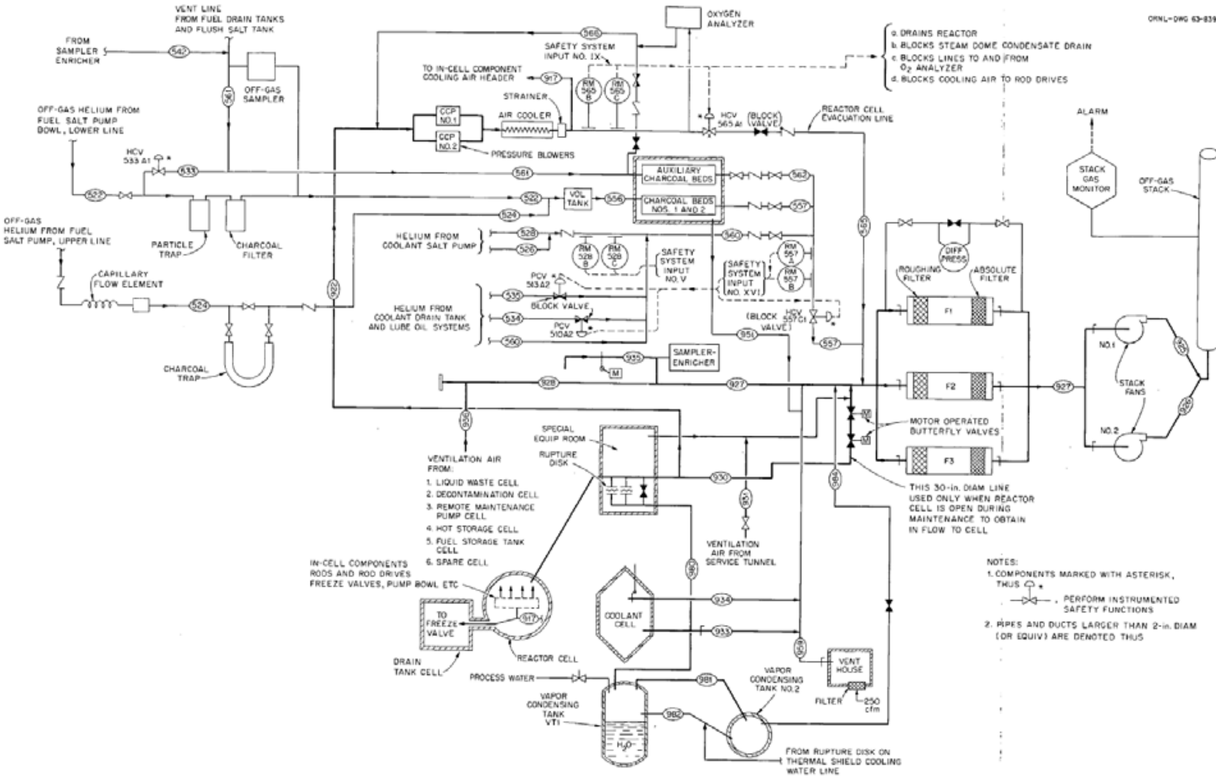


Figure 27: Flowsheet including major CCS and OSG components [Tallackson, 1968]

Once the leak in the off-gas piping begins releasing radioactive material to the reactor cell atmosphere, the MSRE system is designed such that this cell atmosphere (containing radionuclides intended to be handled by the OGS) would be drawn into the CCS by the operating CCP blower. Important components of the CCS and OGS can be seen in Figure 27. The function of the CCS is to distribute this gas elsewhere within the reactor and drain tank cells; however, a portion of this gas flow is continuously being exhausted to atmosphere via the MSRE stack, after being monitored by radiation monitors and flowing through a metallic filter in a 0.64 cm (¼ in.) line. This flowpath can be seen in Figure 28. If either of the two monitors detects excess radioactivity in the gas flow, multiple system responses[60] are initiated by the MSRE control system [Tallackson, 1968].

[60] See also Figure 1.5.2 of [Tallackson, 1968]

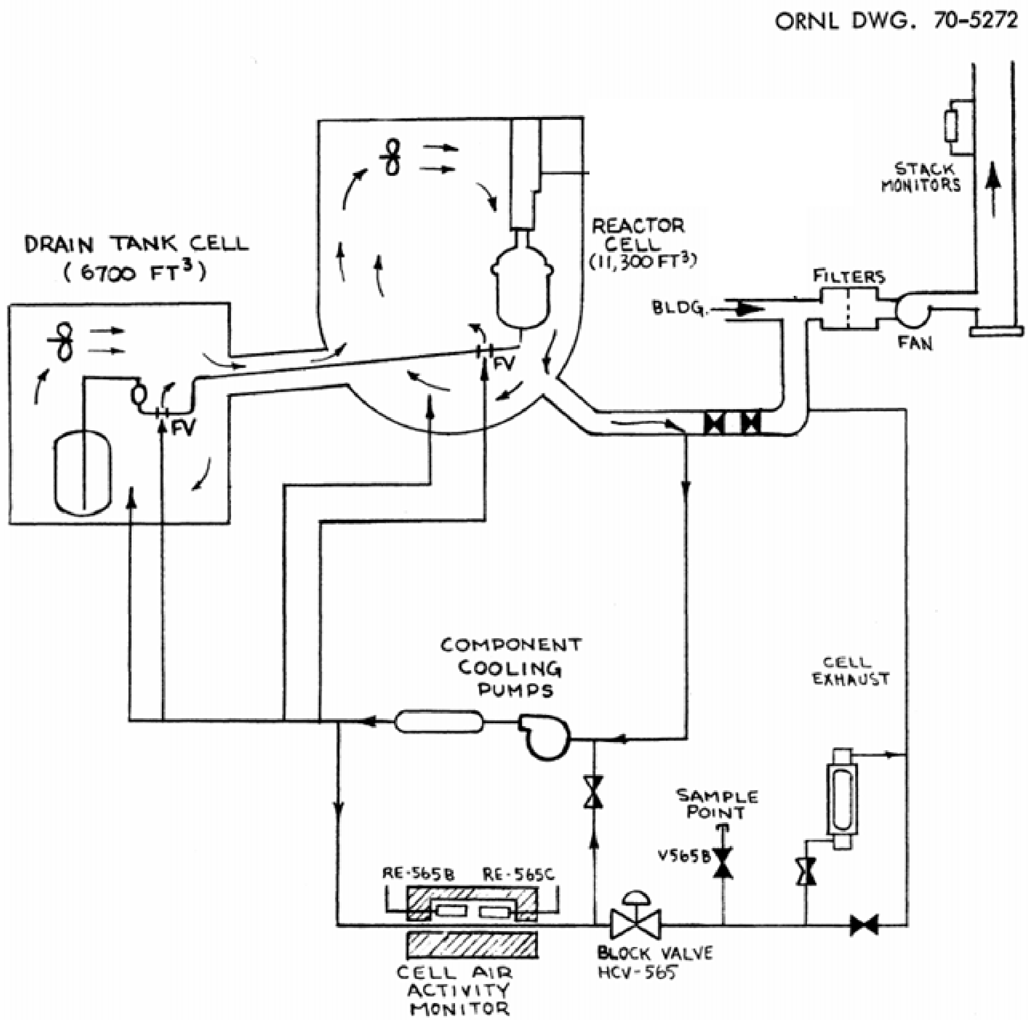


Figure 28: Schematic diagram of MSRE containment and ventilation systems [Guymon et al., 1970]

The following two MSRE control system actions are immediately relevant to the termination of the off-gas leak and mitigation of further release of the radionuclides to the reactor cell:

1. A drain of the fuel salt system is initiated. This action is important because radioactive off-gas will continue to enter Line 522 (and leak into the reactor cell) as long as the cover gas, being supplied to the gas space in the fuel salt pump, is in contact with fuel salt. As shown in Figure 27, once the fuel salt is secured in the drain tanks, the off-gas can be routed through Line 561 to the Auxiliary Charcoal Bed (ACB) and bypass the failed portion of Line 522.
2. A pneumatic valve downstream of the radiation monitors (HCV-565-A1, in the cell exhaust line) is closed to prevent cell atmosphere from being exhausted to the atmosphere (via the stack).

7.2.2. Pivotal Event 1: Fuel Salt Drain

As shown in Figure 29, the first pivotal event after a leak from Line 522 is the initiation and execution of a reactor drain. The fault tree for failure to drain the fuel salt from the fuel salt loop after a leak from Line 522 to the reactor cell can be seen in Section E.2 of Appendix E. In order to calculate a failure probability for components with hourly failure rates, it was assumed in the model that the components would need to successfully perform their intended function[61] for 1 hour to allow for a full drain of the fuel salt loop.[62]

An emergency drain may be initiated automatically or manually [Moore, 1972]. Guymon [1973] reveals that tests of the draining system demonstrated that the fuel salt would drain to the drain tanks via gravity regardless of the positions of the helium pressure equalizing valves in the drain tank system; therefore, failures related to these valves were not included in the FT model. Furthermore, this analysis assumes that at least one of the freeze valves to the fuel salt drain tanks is thawed,[63] such that the only failure of an MSRE system that would prevent the fuel salt from draining to the drain tanks would be a failure of the main freeze valve (FV-103) to thaw (even if one of the valves was erroneously frozen, either drain tank has sufficient volume to accept a full fuel salt system drain [Robertson, 1965]). The failure rate of FV-103 to thaw on demand was thoroughly analyzed in Chapter 6.

If either radiation monitor on the cell evacuation line (RE-565B or RE-565C) detected radiation levels higher than 0.2 mSv/hr (20 mrem/hr), the MSRE control system was designed such that a switch (RSS-565) would open. Upon the opening of this switch, contacts in the control logic of FV-103 would open to isolate the cooling gas that was maintaining the cooling gas flow to maintain the frozen plug of fuel salt in the freeze valve [Tallackson, 1968]. It is assumed in the present analysis that the resistance heating of Line 103 would be required during the entire time period that it would take for the fuel salt to drain from the fuel salt loop into the drain tanks, and that a failure of either of the components controlling this heating would lead to a failure of the fuel salt to drain.

In parallel, the high radiation levels detected by the monitors are also intended to sound an annunciator in the control room. The MSRE operating procedures [Guymon, 1966] instruct the operator to initiate a draining of the reactor if the safety system has not already done so. This drain could be initiated by the turning of a manual switch (Switch S3) in the control room [Moore, 1972].

---

[61] Also referred to as "mission time"

[62] A period of one hour is based upon operational observations discussed by Guymon [1973] and consists of an assumed 10 minutes for the drain signal to be initiated, 10 minutes for the freeze valve in the drain line to melt, and 40 minutes for a fuel salt drain.

[63] Operating procedures required both valves to be thawed during MSRE operations [Guymon, 1966].

Other assumptions in the model depicted in the FT for a failure to drain the fuel salt from the fuel salt loop to the drain tanks include:

- The generic failure rate obtained from the literature is appropriate to describe the scenario in which the radiation detectors do not detect high radiation, and this failure does not trigger the safety system response;
- Human response errors were modeled using best estimate data, based upon the method in NUREG/CR-1278 [Swain and Guttmann, 1983]; and
- The failure rates in the literature for solenoid valves describe mechanical failures, and it is not redundant to explicitly include control failures in the model.

7.2.3. Pivotal Event 2: Isolation of Cell Exhaust Flow

The next pivotal event after draining the fuel salt to the drain tanks is to isolate the cell evacuation flow in Line 565 from the stack. Successful isolation of this flow will contain the activity that is released from Line 522 within the reactor cell and CCS piping and prevent it from being exhausted to the atmosphere via the stack. The FT model representing a failure to isolate the cell exhaust flow from the stack can be seen in Section E.3 of Appendix E. Similar to the previous FT, it was assumed that the components would need to perform for 1 hour to allow for a full drain of the fuel salt loop.

As mentioned above, the MSRE control system was intended to automatically shut valve HCV-565-A1 upon high radiation levels detected by either of the monitors on the cell exhaust line. A physical failure of the valve to shut or a failure of the control system to initiate this closing would prevent the cell exhaust flow from being isolated. However, the operator could also manually isolate the flow using manual switch HS-565-A1. Since the annunciator for high radiation levels in the cell exhaust flow is controlled by the same circuit that automatically initiates the closing of the valve, it would be necessary for the operator to observe high levels of radiation in the stack exhaust [Moore, 1972]. It is assumed in the FT model that the activity from Line 522 would be detected either by the beta-gamma detector or the iodine detector in the stack, but not by the alpha detector.[64] The indicating instruments for these stack monitors are located in the auxiliary control room. The alarm detection equipment associated with this instrumentation provides a local annunciation of the alarm from any of the detection channels and transmits the alarm signal to ORNL's Waste Monitoring Control Center [Tallackson, 1968].

[64] See Section 2.11 of [Tallackson, 1968] for a detailed discussion of how these detectors were intended to operate.

The FT model assumes that a failure in the stack monitoring channels would prevent both the local alarm and the alarm at the Waste Monitoring Control Center.[65]

7.3. Quantitative ETA Results

The ET model developed for the OGS is shown in Figure 29. The FT models used to estimate the likelihood of the IE and each pivotal event were quantified using component reliability data and estimates of human reliability; this FTA and basic event data can be seen in Appendix E. The generic beta factor to model CCFs for a group size of two components was $\beta = 0.024$ [Mosleh et al., 1998]. The FT models were linked to the ET model in EPRI's CAFTA software, and the frequency of each event sequence was calculated [EPRI, 2014]. Using EPRI's UNCERT software, the uncertainty due to the probability distribution of the component failure rates was calculated with a Monte Carlo analysis with a sample size of N = 100,000. The quantitative frequency results for the ET model in Figure 29 are shown in Table 14.

[65] It is possible that the predicted failure rate to detect high stack radiation levels may be a bit lower if the alarm signal to the Control Center was sent by a different channel; however, due to lack of specific details regarding the instrumentation design and the Control Center (e.g., staffing and monitoring procedures), it was assumed that a failure to respond to the alarm in the auxiliary MSRE control room was the dominant failure in this scenario.

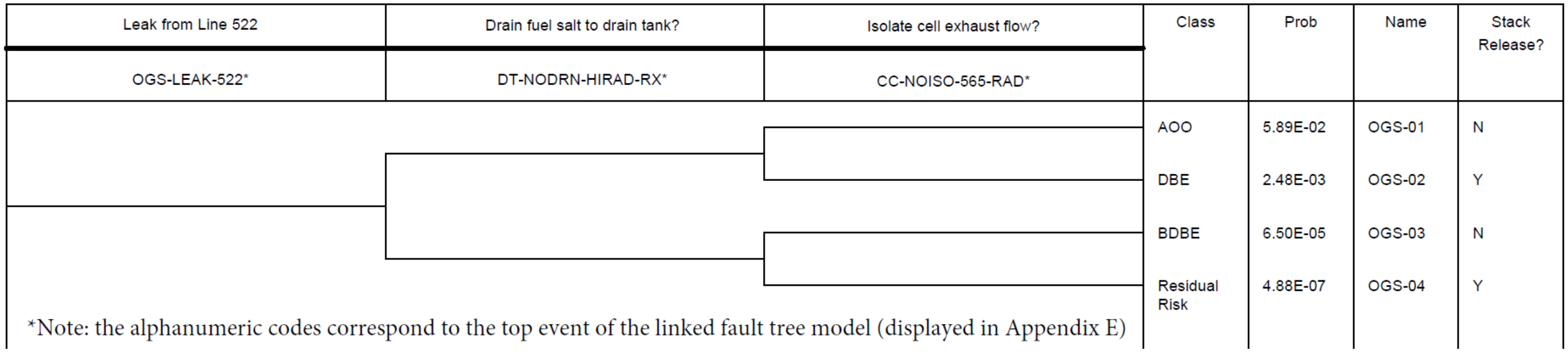


Figure 29: Event tree developed for MSRE OGS

Table 14: Summary of event sequences in OGS ETA
(N = 100,000 for uncertainty analysis)

Sequence Name	Mean [reactor-yr^{-1}]	Classification	Qualitative End state	Point Estimate [reactor-yr^{-1}]	Median [reactor-yr^{-1}]	5% [reactor-yr^{-1}]	95% [reactor-yr^{-1}]
OGS-01	5.89E-02	AOO	Off-gas leak to Rx cell for ~1 hour, stack isolation	5.90E-2	4.31E-02	1.78E-02	1.45E-01
OGS-02	2.48E-03	DBE	Off-gas leak to Rx cell for ~1 hour, release to stack	2.74E-03	7.94E-04	6.55E-05	9.66E-03
OGS-03	6.50E-05	BDBE	Off-gas leak to Rx cell for >1 hour, stack isolation	4.39E-05	1.70E-05	2.45E-06	2.06E-04
OGS-04	4.88E-07	Residual Risk	Off-gas leak to Rx cell for >1 hour, release to stack	3.31E-08	4.71E-09	1.28E-10	3.81E-07

Using the event sequence names displayed in Figure 29, a brief summary of each sequence identified for the radioactive material in the OGS is as follows:

- OGS-1 is the scenario in which a leak/rupture occurs in the OGS piping and radioactive off-gas flows from the OGS into the reactor cell. In response to the elevated levels of radioactivity in the cell atmosphere, both a drain of the fuel salt and isolation of the cell exhaust flow are successful.
- For OGS-2, the fuel salt is successfully drained and the leak is terminated, but the cell exhaust flow containing radioactive material is not successfully isolated from the MSRE stack. Similar to the events in OGS-1, the securing of the fuel salt in the drain tank terminates the leak of radioactive material into the reactor cell. Unlike in OGS-1, however, the contaminated atmosphere in the cell has a flowpath to the environment through the CCS and MSRE stack.
- In OGS-3, the cell exhaust flow is able to be secured, but the fuel salt is not successfully drained and secured in the drain tanks. In this scenario, the duration of the OGS leak to the reactor cell is longer than in OGS-1 or OGS-2.
- OGS-4 represents the event sequence in which the fuel salt is unable to be drained and the cell exhaust flow is not isolated.

Using the LMP definitions [NEI, 2019], the ETA model identifies 1 AOO, 1 DBE, and 1 BDBE. The remaining event sequence is below the frequency threshold for consideration as an LBE; thus, it is considered to be "Residual Risk." It is worth noting that in order to use the frequency definitions for LBEs from the LMP, it was assumed that the MSRE operated at full power for 24 hours a day, 7 days a week, 365 days a year. Because the MSRE was a first-of-a-kind test reactor, both planned maintenance and unplanned shutdowns reduced the availability of the system; thus, assuming a capacity factor of 100% is an overestimation.[66]

7.4. Discussion of Event Sequence Consequences

In order to compare the events identified in the MSRE case study to the F-C target shown in Figure 24, and to fully execute the tasks depicted in Figure 23, a radiation dose at the EAB associated with each MSRE LBE must be calculated. As discussed in Section 4.1, the inventory of radioactive material handled by the OGS included the collection of volatile fission products, mostly the noble gases Kr and Xe. However, this inventory of radioactive material was not specifically modeled in any of the publicly-available MSRE documentation, including the

[66] Between the beginning of the first run of the MSRE (01/09/1965) and the end of the last run (11/20/1969), salt was circulating in the fuel salt loop for a total of 21,788 hours [Guymon, 1973], which is only 51% of the time period between these two dates.

Preliminary Hazards Report [Beall, 1962] and the Safety Analysis Report [Beall et al., 1964]. Furthermore, very little research in the area of fission product volatility in LF-MSR systems has been documented. Thus, the MSRE design and operating documentation was thoroughly reviewed to evaluate whether an accurate model of the off-gas composition could be generated.

During normal operating conditions, some concentration of these isotopes would exist dissolved in the fuel salt, but the introduction of helium into the fuel salt in the bowl of the fuel salt pump was designed to strip a significant portion of these noble gases from the fuel salt (~38%, according to Bell [1970]). As fuel salt was sprayed out of holes in a distributor in the pump bowl, the stripped noble gases were drawn into the OGS [Robertson, 1965]. The OGS included a piping run to provide hold-up time for the radioactive gases to decay (~two hours), water-cooled beds of activated charcoal to adsorb noble gases, roughing filters and particle filters, and a stack to dilute any radionuclides remaining when the resulting effluent was exhausted to the atmosphere. One aspect that could complicate the tracking of these radionuclides throughout the MSRE OGS was that certain fission products would transition between groups according to their respective decay paths. For example, ^{137}Xe was stripped out of the fuel salt as a noble gas, so a significant amount of ^{137}Cs (a daughter product of ^{137}Xe) could be found in the OGS rather than in the fuel salt, even though ^{137}Cs was considered a salt seeker.

In ORNL calculations made before MSRE operation, the radioactive gas (mixed with helium carrier gas) in the OGS was estimated to remove about 10 TBq (280 curies) each second from the pump bowl into the off-gas line [Robertson, 1965]. In the charcoal beds, the residence time of Xe was designed to be at least 90 days, and the residence time for Kr was at least 7.5 days. During this time, almost all of the fission product gases decayed to stable elements. However, because some of the daughters in the decay chains of the fission produce gases were particulates (e.g., ^{89}Sr, ^{137}Cs, ^{140}Ba), deposits in the charcoal beds, filters, and piping retained these daughters. By the time that the gas left the charcoal bed, the only radioactive isotopes that were calculated to exist in any significant amount[67] were ^{85}Kr, ^{131m}Xe, and ^{133}Xe [Robertson, 1965].

The LBEs identified by the MSRE OGS ETA were related to the gas flow immediately downstream of the outlet of the fuel salt pump bowl. The most comprehensive available data concerning the composition of the radioactive gas leaving the gas space of the fuel salt pump bowl is available in [Houtzeel and Dyer, 1972]. Section 7.5.1 of that report discusses the result of gamma spectroscopy measurements that were taken on the off-gas line with the MSRE

[67] These radioisotopes were calculated to have activity concentrations on the order of 3.7E-2 Bq/cm^3 (1E-6 μCi/cm^3); all other radioisotopes were estimated to have activity concentrations no greater than 3.7E-4 Bq/cm^3 (1E-8 μCi/cm^3). See Table 12.1 of [Robertson, 1965] for more detail.

operating at full power. Houtzeel and Dyer [1972] present the estimated average activity of individual radionuclides in the off-gas line and analyze the results; however, they suggest that these activities contain significant uncertainty and may be a factor of 10 to 50 too high. Possible explanations by Houtzeel and Dyer [1972] for this overestimation include errors by the computer program used during the experiment and longer than normal residence time for certain radionuclides (e.g., adsorption or deposition on the OGS piping).

As previously mentioned, the pre-operational calculations estimated approximately 10 TBq/sec (280 curies/sec) in the off-gas flow from the pump, but an estimated radionuclide makeup of this gas stream is not provided by Robertson [1965]. This data is contained in ORNL documents (ORNL CF-57-7-17 and ORNL-MSR-61-101) that are currently in the process of external review for release at ORNL and were not available for use in this work. Using the measurements in [Houtzeel and Dyer, 1972] as a basis, 83.6 TBq (2260 curies) were estimated to be flowing into the off-gas line per second from the gas space of the fuel salt pump. The estimated radioactivity for the OGS flow in the pipe at the effluent of the gas space of the fuel salt pump bowl is displayed by isotope in Appendix F.

One radioelement off-gas concentration with a particularly high level of uncertainty involved in the dose calculations is iodine. According to Compere et al. [1975], the gamma spectrometer studies strongly suggest that iodine left the fuel salt via off-gas; however, neither gas samples nor examinations of OGS components were able to support such a loss path. Compere et al. [1975] concluded that "of the order of one-fourth to one-third of the iodine has not been adequately accounted for" in their fission product material balance. Additionally, the chemical form of this iodine is not well-characterized in existing literature. Houtzeel and Dyer [1972] did conclude, based upon spectroscopy studies of the MSRE system following a shutdown, that iodine activity could be detected due to the decay of I-precursors that deposited on surfaces in the system; however, iodine itself was determined to have remained largely with the fuel salt. Recent thermodynamic calculations to predict the behavior of iodine in liquid-fueled MSRs predict negligible presence of the elemental gases (i.e., I and I_2) as well as for the gaseous IF_x compounds [Capelli et al., 2018].

The identification of the above sources of uncertainty demonstrates that the developed ES&H risk assessment methodology can help prioritize research needs in addition to design insights. In order to increase the confidence in calculations to estimate the quantitative consequences of event sequences involving the radioactive material inventories handled by LF-MSR OGS designs, additional experiments and/or better modeling techniques are required. Furthermore, if these results were obtained during the analysis of a system during the design process, considerations for redesign to eliminate the postulated release paths and/or release scenarios should also be considered by the design team.

7.5. Risk-Informed Evaluation of MSRE OGS Safety and Design

In the process described by the LMP [NEI, 2019], the quantitative results from LBE analysis are intended to be used for other purposes, including: identifying Required Safety Functions (RSFs), selecting Safety-Related Structures, Systems, and Components (SR-SSCs), and evaluating Defense-in-Depth (DID) adequacy. The relationship between these tasks is displayed in Figure 23. Although a comprehensive list of LBEs pertaining to the inventory of radioactive material in the MSRE OGS has not yet been identified, and a full quantitative analysis of the associated risk is not yet possible, the following paragraphs will explore how a reactor developer at an early stage of design might use preliminary qualitative and semi-quantitative analysis (i.e., the results of the analyses described in the previous sections in combination with the qualitative results discussed in Chapters 4-6) to begin the first iteration of these tasks.

Even without a comprehensive identification of LBEs for the inventory of radioactive material in the OGS, the results of the HAZOP studies performed on the MSRE OGS and CCS, coupled with the MSRE MLD developed in Chapter 6, can be used to help demonstrate how a designer could use the LMP approach to determine the safety functions used in the prevention and mitigation of the OGS LBEs and the SSCs that perform these functions. As an initial step, Figure 30 displays a hierarchical representation of the safety functions for the MSRE OGS, starting with the broad safety functions applicable to nuclear power plants in general (highest level) and ending with the specific safety functions employed by the MSRE OGS to prevent and/or mitigate LBEs (lowest level).

Levels 1 and 2 of Figure 30 correspond to the highest levels of the safety function decompositions for the X-Energy reactor design [Waites et al., 2018] and the Modular High Temperature Gas Reactor design [GA Technologies, 1987]. The boxes in the third level of the tree represent the major sources of radionuclides in the MSRE design during the Operate-Run POS (i.e., normal operations), discussed in detail in Section 4.1 of this dissertation.[68] The fourth level of the tree distinguishes between the need to control the transport of radioactive material and to control direct radiation. Because the consequence of interest suggested by the LMP is radiation dose at the EAB, the functions supporting control of direct radiation are not further discussed.

---

[68] As discussed in Section 4.1, major inventories of radioactive material were present in the MSRE Fuel Salt Processing System during certain POSs; however, due to the batch nature of the salt processing, these inventories were not applicable to normal operations.

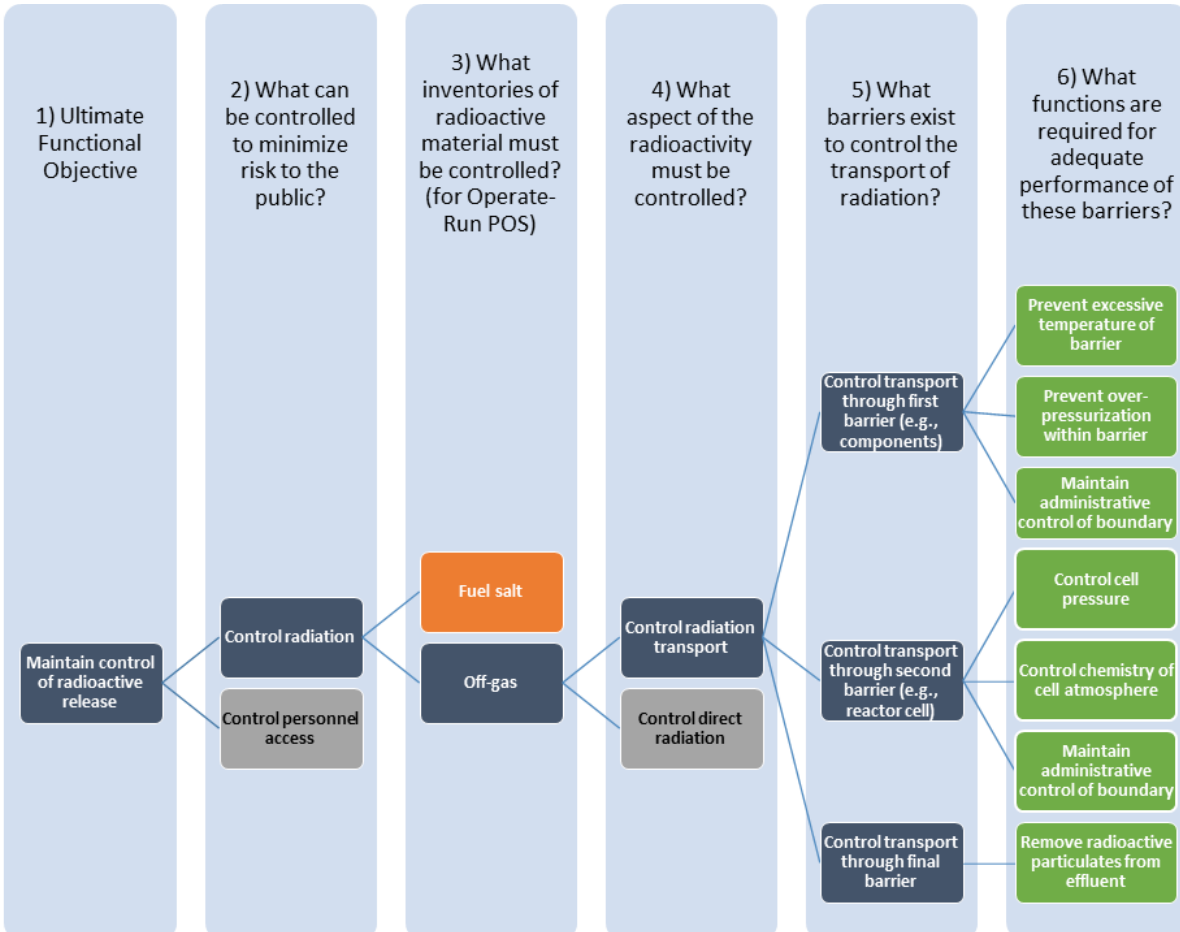


Figure 30: Decomposition of safety functions for MSRE OGS LBEs

The fifth level of Figure 30 divides the safety functions for the OGS based upon which barrier they are intended to protect. From the PHA results, it was determined that there are three distinct levels of barriers to the release of radioactive material from the MSRE OGS. The first barrier is comprised of physical boundaries of OGS piping and components, as well as the functional barriers provided by certain components (e.g., the main charcoal beds). From the "Consequences" and "Safety System" columns of the HAZOP study results, it was determined that two phenomena could lead to transport of radioactive material through this barrier: excessive heat or excessive pressure. The MLD identified that a failure of administrative control (i.e., inadvertent opening of HCV-533) could also result in a transport of radioactive material past this first level of barriers.

As discussed in Chapter 5, if radioactive material from the OGS is released through the first barrier, the second barrier intended to prevent release of the material consists of several different smaller structures in different locations around the MSRE building. For the LBEs identified in the MSRE OGS ETA, this second level of barriers consists of the reactor cell and the CCS piping/components.[69] The MSRE system is designed such that elevated levels of radioactivity in the CCS should trigger actions that isolate the cell exhaust flow to the MSRE stack without operator action, but the HAZOP study of the CCS and the MLD identified functions that must be performed to ensure that the barriers perform as designed. Finally, the ultimate barrier to release of certain radioactive materials from the MSRE OGS is comprised of the filters in the MSRE ventilation system. It is worth noting that this barrier would not be effective at confining all radionuclides, as noble gases would pass through the filters unmitigated. However, the "absolute" stack filters were intended to retain more than 99.9% of the particulates in the cell exhaust flow.[70]

Finally, Table 15 lists elements of DID that were identified for the MSRE OGS during the analysis of OGS-2, which was the only DBE identified by the ET model. The information in this table is not intended to be a comprehensive list of all the provisions that contribute to DID for all LBEs that can occur involving the radioactive material in the OGS; rather, the list is intended to illustrate the approach suggested by the LMP to evaluate LBEs using the layers of defense concept. The DID provisions in the table were able to be identified using the MSRE FTA/ETA, as well as the PHA results. The success criteria from [NEI, 2019] are displayed in Figure 31, and were useful in determining the layer to which each provision belonged. It is important to note that some of the Plant Capabilities in Table 15 would also involve Programmatic aspects of DID. Additionally, because the MSRE design as analyzed was at an early stage of design (i.e. a Technology Readiness Level of ~4-5), there was not much information available regarding Layer 5 of DID.

[69] Although a HAZOP study has been conducted on the CCS, comprehensive PHA results are not available for the MSRE reactor cell.

[70] As previously mentioned, the MSRE was a research reactor that was authorized for construction and operation in a regulatory environment unlike the current regulatory environment for current reactor designs (especially commercial designs). It seems unlikely that a modern LF-MSR would have a similar effluent path for radionuclides.

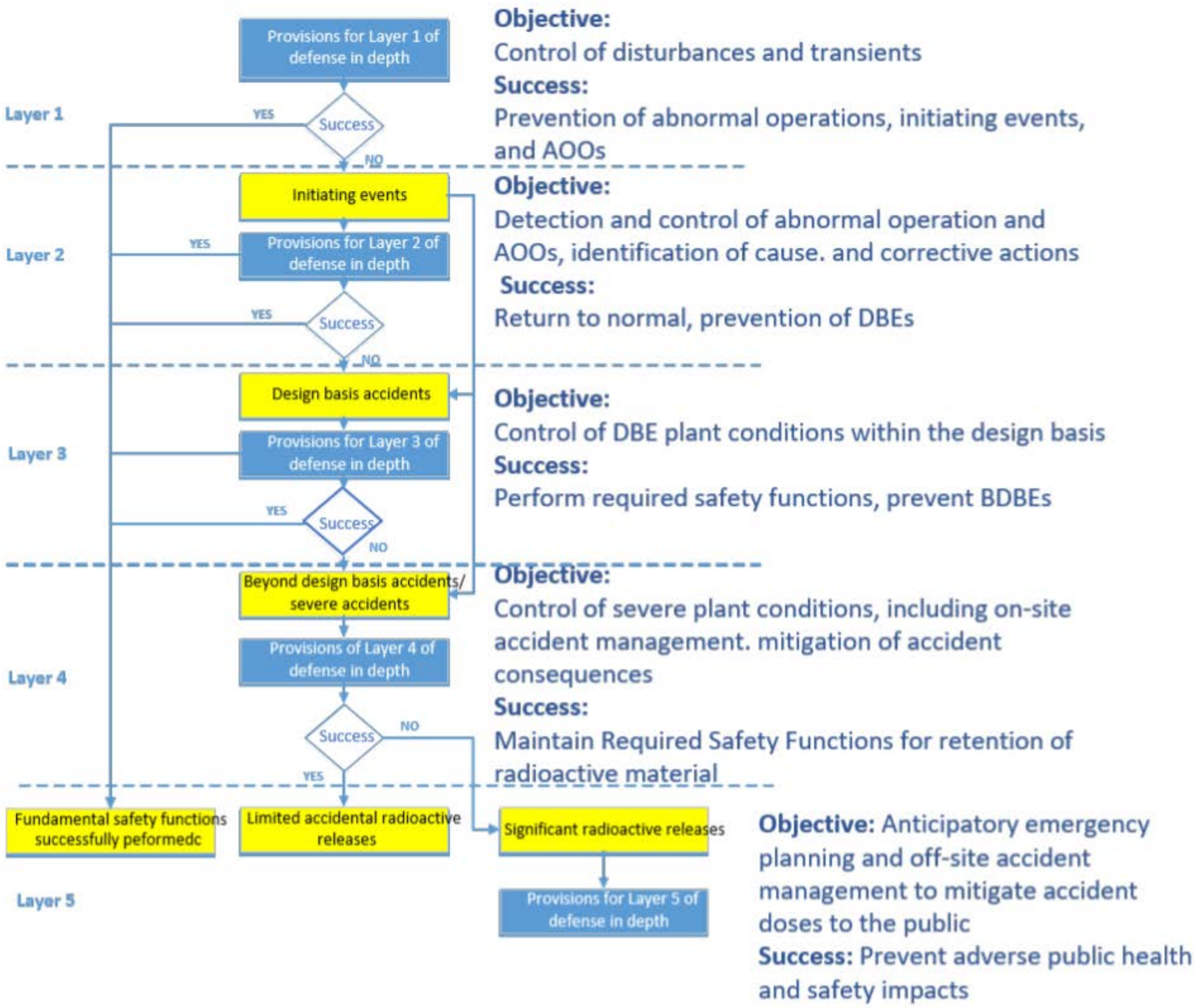


Figure 31: Framework for evaluating LBEs using layers of defense concept adapted from IAEA [NEI, 2019]

Table 15: Elements of DID identified for the MSRE OGS during analysis of OGS-2

Provision	Objective	Plant Capability*/ Programmatic DID	Layer (from [1])
Robustness of OGS piping (Line 522)	Prevent leak of OGS flow	Plant Physical Capability	Layer 1
Design of OGS valves and filters	Prevent plugging in OGS	Plant Physical Capability	Layer 1
Valve lineups in OGS	Prevent unintended path for off-gas flow	Programmatic	Layer 1
Fuel salt pump bowl pressure indications	Notify operator to prevent over-pressurization in OGS	Plant Functional Capability	Layer 2
OGS pressure indications and alarms	Notify operator to prevent over-pressurization in OGS	Plant Functional Capability	Layer 2
Availability of standby charcoal bed	Allow for bypassing of plugged charcoal bed, prevent over-pressurization in OGS	Plant Functional Capability	Layer 2
Cell exhaust radiation indications and alarms	Notify operator to prevent release of radioactive material to atmosphere	Plant Functional Capability	Layer 3
Cell exhaust isolation (HCV-565-A1)	Isolate cell exhaust flow from MSRE stack (prevent release of radioactive material)	Plant Functional Capability	Layer 3
Fuel salt drain	Minimize duration of OGS leak from Line 522 (minimize release of radioactive material)	Plant Functional Capability	Layer 4
Stack radiation monitors	Notify operator of radioactive material release (minimize release of radioactive material)	Plant Functional Capability	Layer 4
ORNL monitoring of stack radiation monitors	Redundant means to notify operators in order to minimize duration of release of radioactive material	Plant Functional Capability	Layer 4
Cell exhaust filter	Retain radioactive material in cell exhaust flow to stack (minimize release)	Plant Functional Capability	Layer 4
Stack HEPA filters	Retain radioactive particles in flow to MSRE stack (minimize release)	Plant Functional Capability	Layer 4

***Note:** It is possible that some of these plant capabilities would also involve programmatic aspects of DID

7.6. Observations from OGS Risk Assessment

ETA and FTA of the main OGS of the MSRE were completed for selected event sequences during normal operations. Quantitative estimates of frequency were developed for event sequences involving the radioactive material inventory handled by the main OGS of the MSRE during normal operations. However, significant, unresolvable uncertainties prevented the calculation of quantitative dose consequence estimates associated with this inventory of radioactive material. Nonetheless, using the LBEs identified, tasks from the RIPB approach to safety basis development described by the LMP [NEI, 2019] were explored to illustrate how an advanced reactor developer could initiate the first iteration of tasks such as identification of reactor-specific safety functions and evaluation of DID, even at an early stage of design. Semi-quantitative estimates of risk, coupled with the qualitative results of PHA studies, proved useful to provide an example of how to initiate these tasks. Obviously, a quantitative estimate of consequences would aid the development of a more mature understanding of system risk, which would in turn support more definite conclusions about LBEs and/or overall plant risk.

The results of the analysis presented in this chapter also suggest that, for advanced reactors that have several distinct inventories of radionuclides, the LMP process for selecting and evaluating LBEs (shown in Figure 23) will need to separately consider each inventory of radioactive material. The MSRE was a research reactor authorized for operation on a US DOE site in the 1960s, and the safety analysis requirements for a modern commercial nuclear reactor would be very different from those under which the MSRE was authorized. Accordingly, risk assessment of modern LF-MSR designs should include consideration of release frequency and consequence to the environment from each inventory, instead of simply focusing on the inventory of the fuel salt loop during normal operations.

As evident in Figure 3, quantitative consequence analysis is not considered in the developed risk assessment methodology to be a fixture of very early SiD. Meaningful consequence analyses need to be informed by fairly mature event sequence development, a good understanding of the various inventories of hazardous material and their characteristics under accident conditions, as well as reasonably mature system design description. Without these pieces of input, important characteristics of potential material releases will be missing and attempts at quantified dose calculations, such as dose to a public receptor, could be too uncertain to be meaningful. In such a case, the time and resources for an early assessment of safety can be put to more productive use in the development of qualitative consequence assessments focusing on the pre-cursors of postulated releases to the environment. For example, early screening for risk-significant events and design decisions can be performed using semi-quantitative event tree analysis that combines quantitative frequency estimates from fault tree analysis with qualitative consequence estimates.

As early designs mature and the nature and extent of possible paths to environmental release are better understood, quantitative consequence analysis may be a reasonable pursuit in the case where bounding calculations using simplified conservative assumptions are deemed to be useful [IAEA, 2009; Krahn et al., 2018b]. These analyses should be accompanied by characterization (and quantification) of the analysis uncertainties [IAEA, 2008] and an assessment of the cost-benefit of the research and model development required for uncertainty reduction. Especially for novel fuel materials, plant configurations, and operating conditions, model development for better-estimate consequence determination may require new research and testing. While potentially sophisticated model development may be required for best-estimate risk characterization, system designers should not postpone their best efforts to eliminate and/or prevent releases to the environment until these tools are completely developed.

CHAPTER 8, CONCLUSIONS

In this dissertation, a novel methodology that is intended to be useful to begin the process of ES&H risk assessment for early stage advanced reactor designs was defined and demonstrated. It was important for the developed methodology to be technology-inclusive, and it was the objective of this dissertation research to consider the array of best available safety design and analysis practices, from the nuclear power generation and other industries, and determine how they can be used to support such a methodology that is technically rigorous and technologically applicable to advanced reactor concepts, including non-LWR technologies. The review, vetting, and compilation of best available practices for such a process led to the definition of a risk assessment methodology based upon the adapted application of well-exercised industry-standard safety analysis techniques. The methodology also supports an incremental and iterative approach, beginning early in design and advancing in detail as design matures.

The methodology developed in this dissertation is intended to allow designers and ES&H analysts of any advanced nuclear system to assess system design, incorporate safety-related insights into the design, and incrementally build a rigorous safety case. Further, in this dissertation, the developed risk assessment approach was demonstrated using a LF-MSR design, an advanced reactor design with minimal historical safety analysis documentation, in order to illustrate its flexibility and contribute to the development of experience in the area of LF-MSR ES&H risk assessment.

The application of the methodology to evaluate the MSRE design has demonstrated its use to effectively identify hazards for advanced reactor technologies, such as those currently under development by the US Government and a number of private sector entities. Although the methodology was only demonstrated in this dissertation using an LF-MSR design, the nature of the tools selected for the execution of the defined elements allows for analysis of a wide variety of systems and hazards. In particular, designers and/or analysts of other advanced reactor technologies that have not benefitted from significant prior risk-informed safety assessment efforts could benefit from the use of the developed methodology and the incorporation of its results into the system design process. For example, early-stage FHR and/or SCWR designs could be evaluated to identify PIEs and important safety systems that should be considered as reactor developers progress through the Pre-conceptual and Conceptual stages of the design process. Additionally, use of the developed methodology could be beneficial to designers and stakeholders in industries other than the commercial nuclear electricity generation industry, including the chemical process or oil and gas industries. More specifically, the methodology could be helpful to stakeholders in these industries that desire to develop a more quantitative assessment of system risk. Because the methodology is based upon commonly-used PHA methods, the methodology could facilitate the transition to a more quantitative assessment without the need to start the safety assessment from scratch.

Overall, the research presented in this dissertation investigated broader application of PHA methods to support the development of the building blocks for PRA models early in system design, especially for new reactor technologies and design variants that do not have an established history or prior PRA development and application. The efforts presented in this dissertation support that, for nuclear facility safety analysis, a reliable method to achieve sufficiently thorough hazard identification is through the disciplined application of a proven hazard analysis/evaluation tool. The technical work performed has provided evidence that the use of PHA, even in early stages of design and technology development, provides a more comprehensive and systematic approach to accident scenario development than the use of historical research and propagation of past deterministic approaches to safety by themselves.

8.1. Lessons Learned from Methodology Demonstration

The discussion of the methodology in Chapter 3 mostly focused on the use of the hazard, risk, and safety analysis tools in a one time through manner, starting with the application of a hazard identification or hazard evaluation method to identify hazards and advancing through the use of the various tools depicted in Figure 3, depending upon the level of available data. During the demonstration of the methodology using the MSRE design, emphasis was placed on understanding the applicability of these techniques at early stages of design, since it has been more common in the past to do these sorts of studies in a back-fit fashion for completed design of an operating facility. However, the methodology defined and demonstrated in this dissertation is intended to be exercised iteratively throughout the design process, and perhaps even extending into the operating life of a facility. This intention raises the following two questions:

1. When can the use of the methodology begin for a given system design?
2. How often and when does it make sense to be applied during the design process?

Given that the impetus for the methodology stems not only from the desire to characterize environmental and nuclear safety risks associated with a given design, but also to incorporate SiD, the results of the analysis discussed in Chapter 4 illustrates that PHA methods can be gainfully employed in the early stages of Pre-conceptual Design. Even before the design is formally documented in significant detail, PHA is a tool that facilitates the structured gathering of the key design disciplines in a collaborative manner [US DOE, 2016] – the benefits of which will be: (1) a firming up of the common understanding of the design, (2) a potential tool for qualitatively evaluating design options, (3) a reasoned and organized partition of the facility for analysis, and (4) an integrated inter-disciplinary discovery of design factors important to safety.

The second question regards when and how often the iterations of the methodology should occur. The answer to this question is likely to vary according to the circumstances associated with the project to which the methodology is applied. For example, as discussed in Section 2.2., the number and type of methodology iterations performed while conducting a facility design program would be specific to the nature and maturity of the technology and the specific details of the design approach. Based on the experience gained by exercising the methodology on the MSRE design, a concept anchored in fundamental Systems Engineering approaches [International Council on Systems Engineering (INCOSE), 2015] is depicted in the spiral diagram shown in Figure 32. This figure conveys the idea that the methodology can be performed in progressive degrees of risk analysis detail that align with Pre-conceptual Design, Conceptual Design, Preliminary Design, and Final Design.[71] Additionally, it conveys that the methodology is a tool that can be made integral to the design process, continuously used throughout the stages of design development to reduce and manage risk and to produce the justification for safe operations that is necessary for final regulatory approval.

The subsections below discuss lessons learned during the demonstration exercises of the developed methodology regarding what information is available about a given technology at different stages of the design process, as well as how information availability can affect which industry-standard tools can generate meaningful risk insights. These conclusions are also summarized in Table 16. In addition to the experience gained during the research performed as a part of this dissertation, the discussion below also draws on research performed by Vanderbilt for EPRI (and published by EPRI [2017]) about the information available as each design stage is completed. Because EPRI [2017] also structures discussion of the design process using Technology Readiness Levels (TRLs) [US DOE, 2011], Table 17 displays the relationship between commonly defined qualitative design stages (i.e., Pre-conceptual, Conceptual, Preliminary, Final, and Operating) and TRLs for test, demonstration, and commercial nuclear reactor designs.

[71] This idea is consistent with the approach advocated (but not explained in great detail) in [US DOE 2016].

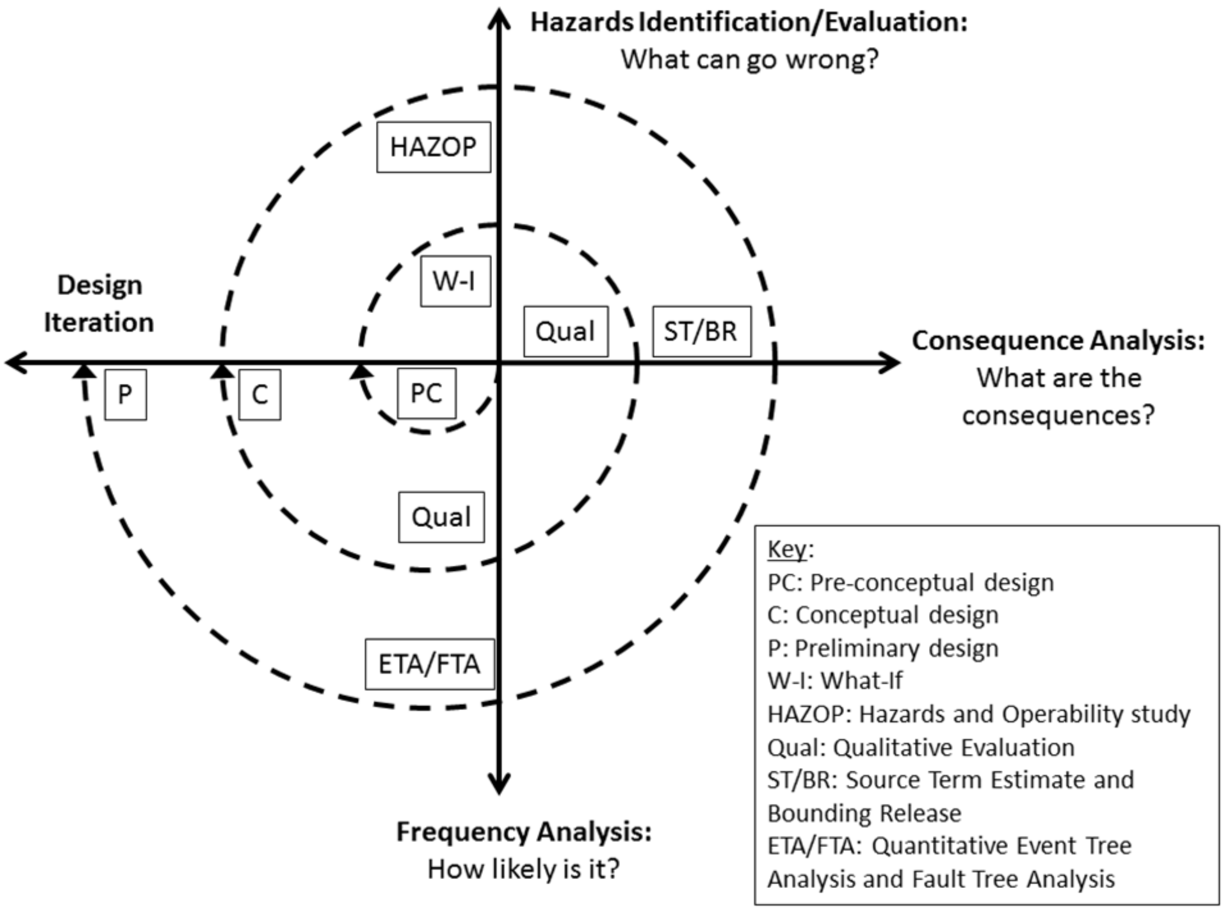


Figure 32: Relationship between safety analysis tools and design development [Chisholm et al., 2019]

Table 16: Summary of information available at a given design stage and useful tools for generating ES&H risk insights

Design Stage	Example of Information Available	Useful Tools for Risk Insights
Pre-conceptual	• Preliminary user requirements and constraints • Candidate layouts for major subsystems (e.g., Process Flow Diagrams) • Some components functionally identified • Some results of bench-scale experimental work	• Preliminary Hazards Analysis (PrHA) and/or What-If analysis • Qualitative consideration of likelihood and potential consequences associated with various phenomena • Qualitative ranking of hazards (e.g., PIRT analysis)
Conceptual	• Process, block, and engineering flow diagrams for subsystems • Process simulations and material and energy balances • Bench-scale tests in a realistic environment using radioactive materials	• Moderately-detailed PHA methods, including HAZOP study • Event sequence diagrams and/or qualitative event trees • Early quantitative consequence analysis, such as calculations of bounding releases
Preliminary	• Detailed Piping and Instrumentation Diagrams (P&IDs) • Process equipment specifications, process parameters, and specifications of automation systems • Considerable technical data to support refined understanding of system behavior and operational limits	• Highly detailed PHA methods, including FMEA • Quantitative fault trees • Semi-quantitative and/or quantitative event trees
Final (and beyond)	• Information of extensive detail to facilitate siting, licensing, construction, and operation of a reactor system	• When complete, the elements of the developed methodology allow for the construction of the nuclear safety case to support facility licensing and operation

Table 17: Correlations between stages in reactor design process and TRLs [Chisholm et al., 2019; EPRI, 2017]

TRL (from EPRI [2017])	Test Reactor	Demonstration Reactor	Commercial Reactor
1 – Basic Research	--	--	--
2 – Concepts Formulated	Pre-conceptual Design	Pre-conceptual Design	Pre-conceptual Design
3 – Proof of Concept	Pre-conceptual Design	Pre-conceptual Design	Pre-conceptual Design
4 – Component Validation: Bench-Scale	Conceptual Design	Pre-conceptual Design	Pre-conceptual Design
5 – Subsystem Validation: Bench-Scale	Preliminary Design	Conceptual Design	Conceptual Design
6 – Subsystem Validation: Engineering-Scale	Final Design	Preliminary Design	Conceptual Design
7 – Test Reactor	Operating test reactor	Final Design	Preliminary Design
8 – Demonstration Reactor	--	Operating demonstration reactor	Final Design
9 - Commercialization	--	--	Operating commercial reactor

8.1.1. Risk Assessment during Pre-conceptual Design

During the pre-conceptual stage of design, preliminary user requirements and constraints for the system are identified. Candidate layouts for the “major” subsystems (e.g., heat generation, heat transfer, and heat rejection) are identified, generally in the form of high-level Process Flow Diagrams (PFDs). Some components for these systems have been functionally identified, but it is possible that detailed information has not yet been produced regarding system/component specifics, such as materials of construction. Design information for auxiliary subsystems is likely not developed in much detail and may be represented using functional and/or placeholder data. Candidate geometries and chemical forms for the fuel may be identified, as well as estimates of coolant, fuel, and other material inventories. Regarding experimental data, some results of bench-scale experimental work in a functional environment and low-fidelity configuration using mostly non-radioactive materials may be available.

Given the relatively low fidelity and completeness of the design information that exists during Pre-conceptual Design, performance of the more detailed elements of the methodology is not feasible. For example, construction of event and fault trees is likely inaccessible during this design stage since the safety system and/or control philosophy for the plant may not be developed much past generic requirements. However, basic tools, such as PrHA and What-If analysis, can be used to produce meaningful results for pre-conceptual system designs; these more loosely structured analyses can provide a documented answer to the question "what can go wrong?" for a given system. Although the understanding of a given technology may not yet be sufficient to allow for a comprehensive quantitative assessment of risk, qualitative consideration of the likelihood and potential consequences associated with various hazardous phenomena can produce insights that can be used to influence the development plan for Conceptual Design. For example, the documented results of hazard identification studies can impact design decisions and design trade studies. Additionally, qualitatively ranking the magnitude of the severity and uncertainty associated with various hazardous phenomena (e.g., using an expert-driven PIRT analysis) can inform future decisions to perform additional research, such as prioritization of bench-top experiments to be run.

8.1.2. Risk Assessment during Conceptual Design

During the conceptual stage of design, details are developed for the entire system. This includes the development of process, block, and engineering flow diagrams for subsystems, and supplementation of these diagrams with the results of process simulations and material and energy balances. Bench-scale test results in a realistic environment and using radioactive materials are used when feasible to optimize subsystems and to plan for engineering-scale testing. Additionally, experimental results are used to validate analytical models that represent subsystem performance.

During Conceptual Design, sufficient design detail is available to perform a "moderately detailed PHA," such as a HAZOP study. Results of these analyses can be used to begin the process of identifying SSCs important to safety, in addition to supporting the development of preliminary cost estimates and early strategies for nuclear safeguards. It is also possible that the results of PHA studies can be used to identify event sequences of interest, which can be modeled qualitatively with event sequence diagrams and/or event trees. These types of models can be used to define preliminary accident scenarios that may eventually establish functional design criteria for engineered safety systems and associated operating safety limits. As a Conceptual Design develops, a firmer understanding of the characteristics of the hazardous material inventories under normal, abnormal, and accidental conditions is acquired and advances the safety design basis; these developments support beginning the formal preparation of licensing analyses and documentation. Early exercises in quantitative consequence analysis, including initial calculations of bounding releases, may reveal a need for applied research and testing to develop reasonable and defensible quantitative estimates.

8.1.3. Risk Assessment during Preliminary Design

During Preliminary Design, system and subsystem design information is defined in significant detail. Detailed Piping and Instrumentation Diagrams (P&IDs) are produced, supplemented by details such as: process equipment specifications (e.g., size, functionality, operational environmental conditions, etc.); sizing of process support like feed preparation, process utilities, building utilities, and spaces; and specifications of the automation systems (i.e., degree and level). Isometric and 3D installation drawings may also be developed, along with installation specifications. Considerable technical data is produced by experiments to support a refined understanding of system behavior under steady-state and transient conditions, as well as reactor operational responses and limits.

During this stage of the design process, the greater level of design detail increases the benefits gained from the utilization of highly detailed PHA methods, such as FMEA, and quantifiable models, such as fault trees. As demonstrated in Chapters 4-7 using the MSRE, the existing data and design detail during Preliminary Design should support the utilization of almost all of the tools in the developed methodology. Quantitative ETA and FTA efforts can be used to support the development of quantitative risk insights related to specific design decisions, and these analyses may reveal the need for design modifications or further modeling/analysis or experimentation/testing (e.g., to reduce uncertainty). By updating and expanding the scope of the risk assessment efforts performed during early stages of the design process, many building blocks should be in place to begin construction of a preliminary PRA model for the design. The need for further iterations of the risk assessment methodology in the subsequent stages of the design process would be a function of several characteristics, including: the stability of the design; the nature of design refinements or new changes; and the expectation of the regulators.

8.1.4. Risk Assessment during Final Design and Beyond

During Final Design, information of extensive detail is produced to facilitate the siting, licensing, construction, and operation of a reactor system. For the Final Design of a commercial reactor, the design is optimized using lessons learned from the operation of prior systems (i.e., test reactors and/or demonstration reactors). Because the design used to demonstrate the developed methodology in this dissertation was that of the MSRE, the research in this dissertation did not fully explore the implementation of the methodology through the Final Design of a commercial nuclear reactor system. However, Vanderbilt preliminarily explored this subject in [EPRI, 2017].

Once the final design is established, the methodology should have been exercised sufficiently to produce all the elements necessary for a model of safety and risk that supports the nuclear safety case used for facility licensing and operation. A sufficiently complete evaluation of risk can involve fully quantitative answers to the questions of the risk triplet, along with a quantified characterization of the associated uncertainty. As previously mentioned, the iterative nature of the methodology is intended to facilitate the incremental advancement of the system's risk assessment model at each stage of the design process by building upon the results produced during each previous iteration.

8.2. Methodology Demonstration Challenges

During the demonstration of the developed risk assessment methodology on the MSRE, a complete assessment of risk associated with all hazardous material inventories during each POS was not developed. Notable challenges experienced during the demonstration activities are briefly discussed in the following subsections; these challenges help to frame future research opportunities.

8.2.1. Resource Constraints

A comprehensive assessment of hazards for even just a single POS of the MSRE would require a PHA study (e.g., a HAZOP study) to be performed on each subsystem; however, these types of studies are moderately time-consuming and resource-intensive. Because it was not feasible to perform a PHA study on every subsystem of the MSRE as part of the research for this dissertation, the subsystems containing major inventories of radioactive material during two specific POSs (i.e., normal operations and uranium recovery) were prioritized to be analyzed using the HAZOP method. The intention behind this structure was to demonstrate how to identify a number of different PIEs (and groups of PIEs) that could lead to event sequences that could potentially result in the release of radioactive material to the environment; the MSRE MLD also reflects this intention by only being fully decomposed to identify PIEs relevant to the same 4 inventories of radioactive material. As such, it is possible that additional PIEs and/or event sequences of interest to LF-MSR designers, safety analysts, and regulators may be identified for the MSRE design by the performance of a rigorous hazard assessment for the remaining study nodes.

Similarly, although overall phenomena of interest to operating the MSRE were identified as part of the HAZOP study effort, a rigorous effort to rank phenomena relevant to LF-MSR technology was not performed due to limitations on time and resources. While the results of the analyses performed to demonstrate the developed methodology identified hazardous phenomena and could also help characterize the uncertainty associated with these phenomena, these insights were only qualitatively addressed. Use of tools such as a PIRT analysis [Diamond, 2006] could generate semi-quantitative results that may be of interest to LF-MSR stakeholders. More specifically, scoring criteria could be used to rank phenomena based on a figure of merit in order to achieve various objectives, such as prioritization of experimental data collection and/or analytical model development.

8.2.2. Quantitative Consequence Analysis

The event sequences analyzed using ETA in Chapter 7 were related to the gas flow immediately downstream of the outlet of the fuel salt pump bowl, because that portion of MSRE OGS contains the gaseous radionuclide hazard that is at its highest concentration. However, as discussed in Section 7.4, an accurate estimate of consequences associated with the end states of these event sequences could not be developed due to the conflicting nature of the existing body of knowledge. The following are examples of some questions that would likely need to be answered in order to allow for an accurate quantification of consequences associated with event sequences related to the radioactive material in the MSRE OGS:

1. Other than the initial list of radionuclides discussed by Houtzeel and Dyer [1972], what radionuclides exist in the OGS flow?
2. In what chemical form do the radionuclides in the OGS flow exist?
3. Are the radionuclides in the OGS flow, in the chemical form determined above, readily transported out of the reactor cell?
4. To what degree do phenomena like filtration in the ceramic filter and plating out in piping affect the transport of radionuclides from the reactor cell atmosphere to the environment?

Similar questions also exist for the radioactive material inventories in the fuel salt loop during normal operations and in the fuel salt processing system during fluorination. Accordingly, fully quantitative answers to the questions of the risk triplet cannot be developed for many event sequences of the MSRE until better analytical models of LF-MSR source terms are developed and/or additional experimental data is collected.

8.2.3. Selecting a Risk Metric

The Non-LWR PRA Standard [ASME/ANS, 2013] states:

> *"Although intermediate risk metrics or surrogate risk metrics similar to core damage are not specifically called out in this standard, such metrics may be used to help define event sequences, event sequence families, and release categories. Such an approach may involve structuring of event sequences in the Event Sequence Analysis in a manner similar to a Level 1/Level 2 PRA for an LWR."*

Thus, it was originally desired during the analyses presented in this dissertation to explore the development of a preliminary risk metric; i.e., a conceptual equivalent of "Core Damage Frequency (CDF)" in an LWR system. It can be extremely resource-intensive to rigorously calculate dose consequences, and significant uncertainties within these estimates can exist for reactor systems under accident conditions, especially for technologies at low levels of maturity. If a surrogate could be thoroughly defined, its use could reduce the amount of resources required to develop valuable insights regarding relative severity of the consequences associated with different initiating events and event sequences modeled in the initial event tree models.

The risk metric proposed was defined as "an unanticipated significant increase of radionuclide transport through the first barrier intended to prevent release of radioactive material." In an LF-MSR, the barriers could be defined for the reactor system as a whole (e.g., fuel salt flowing into the off-gas system would not be considered as violating a barrier) or individually defined for each inventory of hazardous material (e.g., fuel salt inadvertently flowing into the Off-Gas System would violate the barrier for the fuel salt system). With this metric, it was hoped that event sequences resulting in significant, undesirable consequences within or close to the system would be captured. Therefore, it was considered that this metric could be used to support the early SiD objective to eliminate and/or prevent environmental release, if at all possible.

However, the risk metric used to investigate qualitative risk at an early stage of design may be different from the risk metrics used to analyze quantitative risk in a more mature design. Nevertheless, at early design stages, safety assessment efforts, such as current efforts for LF-MSR technology, are not yet mature enough to allow for the selection of a meaningful, broadly applicable risk metric that can serve as a regulatory metric – especially considering the challenge with quantifying source terms described in Section 8.2.2.

8.2.4. Modeling Challenges

Some challenges were experienced during the MSRE demonstration related to the tendency of industry-standard quantitative risk assessment tools, such as fault and event trees, to express functional or subsystem success or failure as a purely binary condition. For example, the implication of the Boolean logic used in the fault tree model discussed in Section 6.3.2 is that the freeze valve either thaws completely as designed or fails to thaw entirely; however, because the functioning of the freeze valve relies upon the phase change of the frozen salt plug in the valve body, it is possible that the valve could "partially function," i.e., function in a degraded fashion. For example, the frozen plug of salt in the valve body could thaw at a slower rate than intended, or the plug could partially melt, which would reduce the rate at which the fuel salt is able to be drained from the fuel salt loop to the drain tank.

While it is possible that advanced tools, such as Dynamic Probabilistic Risk Assessment (DPRA) approaches, may be able to more accurately handle subsystems and components in advanced reactor designs that can potentially function in a partial manner (including passive components), a large amount of information must be gathered to do a proper dynamic analysis [Metzroth, 2011]. Such work was beyond the scope of the research in this dissertation, but it provides food for thought moving forward.

8.3. Other Observations Concerning the Effective Implementation of the Methodology

In addition to the methodological insights discussed in the previous two sections, the demonstration of the developed risk assessment methodology also produced valuable information regarding how to maximize the efficiency of the transition between the elements depicted in Figure 3 (and summarized in Table 6).

During the conduct of the MSRE HAZOP studies, the importance of understanding and documenting the interfaces between nodes was emphasized. Because of the tightly coupled nature of phenomena in LF-MSRs, PIEs that occur in one node (or subsystem) could result in consequences that propagate to another node (or subsystem). For example, a pressure transient in the main fuel salt OGS could affect the operating pressure of the fuel salt loop during normal operations. In order to capture these interactions, it was found that listing the consequences of a given deviation at each nodal interface facilitated the analysis of each PIE and/or event sequence using HAZOP results from multiple different nodes.

Although it is possible to conduct a HAZOP study while holding the assumption that some of the safety systems intended to mitigate the consequences associated with a given cause are successful in their response to the deviation, it was found during the MSRE demonstration activities to be helpful to comprehensively document the unmitigated effects of a scenario. Assuming the failure of the intended safety systems particularly facilitated the construction of event sequence models in which responses from plant systems were not successful and the identification of the end states associated with these sequences.

Experience during the conduct of the FMEA identified that using a list of common failure modes and/or human errors was particularly helpful to maximize the transition between FMEA results and a fault tree model. Using this approach meant that each row of the FMEA results table functioned as a basic event in a fault tree model. Similarly, because the intention was to use the FMEA results to help construct quantitative fault tree models, it was also helpful to differentiate between automatic system responses and actions that would be required by operators in response to system indications. This differentiation aided in the treatment of human error within the quantitative models of risk associated with the MSRE.

Finally, as discussed in Chapter 5, grouping PIEs based on the plant response that would be required to mitigate the associated consequences was particularly useful during the transition to the development of event sequences. Specifically, this approach reduced the number of redundant event sequences that were identified. As a corollary, developing and maintaining a list of the various component failure modes comprising each PIE group facilitated the construction of the fault tree model used to estimate the likelihood of the PIE group.

8.4. Potential Areas for Future Work

Specific observations resulting from the development of the methodology are presented in Section 3.4, and conclusions drawn from the application of different portions of the methodology to assess the safety of the MSRE design are discussed at the end of each chapter summarizing the results. Section 5.4 identifies considerations for a systematic search for potential accident initiators in advanced reactor design, Section 6.4 identifies design insights produced by a detailed analysis of a unique LF-MSR design feature, and Section 7.6 explores how designers of relatively immature systems can maximize the benefit of a RIPB approach to evaluating potential accident scenarios. Based on the efforts to demonstrate the developed methodology using the MSRE design, a few recommendations for broad areas of further research were identified, in addition to several specific potential projects for future work.

Future efforts to improve the comprehensiveness and robustness of an ES&H risk assessment methodology could focus on:

- **Non-radiological chemical hazards** - LWR risk assessment has historically placed emphasis on hazards from postulated accidental releases of radiological material. Any chemical hazards would typically be addressed as part of worker/industrial safety programs, and the risk from chemical hazards is generally considered to be dwarfed by risk from radiological hazards. The nature of some advanced technologies, such as MSRs, may require greater attention to potential hazards from the release and exposure to non-radiological hazards such as toxic or corrosive materials. The MSRE, for instance, could be classified as a chemical processing facility as well as a critical nuclear reactor. The PHA-based methodology defined in this dissertation offers certain advantages in this regard, as PHA methods were originally developed for the chemical processing industry. Although DOE-STD-1189 provides some preliminary guidance on the integration of chemical hazards into nuclear facility safety analysis [US DOE, 2016], more attention may be warranted regarding: (1) how chemical hazards are integrated, as necessary, into the overall facility risk profile characterized by the facility PRA model, and (2) how chemical consequences may need to be incorporated into LBE scenarios and their associated acceptance criteria.

- **Operational modes and facility life cycle** - Because PHA studies can generate large numbers of deviations, the desire for a thorough hazards identification exercise needs to be balanced against the need for manageable study performance and logistics through well-defined boundaries for scope. A reasonably comprehensive PHA at an early stage of design may be limited to the intended full-power operating mode of a reactor facility early in design development, but the risk assessment model needs to eventually comprehensively consider other POSs, as well (e.g., start-up, test configurations, shutdown, maintenance outage, re-fueling, etc.). Further, the ES&H risk assessment should also identify any insights for how the facility will be retired and ultimately dispositioned.
- **Failures and degradations due to latent causes** – PHA methods offer powerful tools traditionally used to identify immediate or acute hazards in a process or system. However, the potential for more chronic and gradual effects such as degradation of materials and components, which can occur over longer timeframes, exists in systems where aggressive physical and chemical environments are expected. The following types of potentially hazardous conditions in a system may not be reliably identified, or can be difficult to assess, by traditional application of PHA tools such as HAZOP analysis: corrosion, erosion, thermal fatigue, mechanical fatigue, and radiation damage. These and other types of latent hazards should be considered for any advanced commercial power reactor. The industry would benefit from the availability of methods and tools to systematically identify and address these hazards as early in design as possible, since material selection requires considerable lead time.

In addition, several opportunities for more focused research projects were identified, including:

- Development of more specific guidance on how to maximize the efficiency of an iterative and incremental approach to ES&H risk assessment. A detailed exploration of which analysis methods are the most useful during each of the well-defined stages of design would enhance the efficiency of the developed methodology for a wider range of system designers and safety analysts.
- Performance of a HAZOP study on MSRE filling and draining procedures. Understanding the potential safety-significant scenarios during POSs other than normal operations could identify PIEs and event sequences not evaluated during the HAZOP studies performed as a part of this dissertation.
- LF-MSR freeze valve engineering development and options analysis. The detailed analysis of the MSRE freeze valve subsystem in this dissertation identified aspects of the

design that could potentially be improved to increase the reliability of a freeze valve. Future efforts could include completion of the FMEA for unanalyzed failure modes of the MSRE freeze valve and investigation of how to optimize the approach for freeze valve control.

- Detailed characterization of the composition and potential for dispersion of LF-MSR radioactive material inventories. A comprehensive quantitative assessment of risks associated with an LF-MSR will not be possible until more accurate models are available for radioactive material inventories other than the fuel salt, such as the off-gas. For example, more information is needed regarding potential deposits on surfaces and components in an off-gas system and any alterations in composition brought about by unique accident conditions. Additional experimental data, such as radionuclide volatility, may be necessary to reduce uncertainty and develop meaningful results.

8.5. Reflections and Concluding Remarks

The most meaningful conclusion underlying the development and demonstration activities conducted as a part of this dissertation research is that understanding and addressing risk requires comprehensive, systematic diligence. A thorough and accurate characterization of risk for a system necessitates consideration of the maturity of the design, anticipated operating modes, and inventories of hazardous material (including the locations and states of reactive, toxic, and radioactive materials); although not explored in any detail in this dissertation, the life cycle phase that a facility is in (e.g., startup, operation, deactivation/decommissioning) will also impact the understanding of risk. Therefore, the work presented here is the "tip of the iceberg" in the full understanding of risk posed by the MSRE and, more generally, LF-MSR technology. Secondly, the incorporation of safety from the earliest stages of design will lead to significant improvements in the *efficiency* of both the safety assessment and design processes. This enhanced efficiency can ultimately lead to *reduced cost* and *improved design*. For example, design changes are less costly at early stages of design, and a more complete understanding of risk can reduce the amount of additional safety margin that must be included in a design (i.e., “over-engineering”). Further, early systematic identification of potential risk in new technologies can be used to optimize the timing and direction of additional research and experimentation. Optimized R&D allows for incorporation of design improvements earlier in design to avoid costly rework in later stages of design or after a facility becomes operational. This is particularly important to new technological approaches to nuclear power, which may have the disadvantage of little to no operating experience and may present hazards (and therefore risks) that are not obvious first glance.

Opportunities to gain additional valuable insights exist in further development and application of the methodology. For example, it will be useful to explore other potential interfaces with such a risk-informed hazard and risk assessment methodology as a system reaches the Final Design stage (and beyond), such as the development of an Environmental Impact Statement and/or the implementation of administrative controls to minimize occupational risk to workers. Ultimately, the true value of the developed hazard and risk assessment methodology is its potential to enable the implementation of advanced nuclear reactors as a piece in the puzzle of addressing growing energy demand in a responsible manner. The current fleet of nuclear power plants have already demonstrated that nuclear energy is an efficient, safe, and clean method to produce electricity; however, advanced nuclear reactors (such as Molten Salt Reactors) look to improve upon the current generation in a way that will yield significant social benefit in the forms of environmental stewardship and energy abundance for generations to come.

REFERENCES

Aji, I.K., Tatsuya, T., Kinoshita, M., and Okawa, T. [2018] An Experimental Study on Freeze Valve Performance in a Molten Salt Reactor. Presented at 26th International Conference on Nuclear Engineering (ICONE26), July 22-26, London, England.

Allen, C.B., and Janz, G.J. [1980] Molten Salts Safety and Hazards: an Annotated Bibliography. Journal of Hazardous Materials, 4, 145-175.

Allen, T., Ball, S., Blandford, E., Downar, T., Flanagan, G., Greenspan, E., Holcomb, D., Hu, L.-W., Matzie, R., McGaha, J., Mears, D., Memmot, M., Peterson, P., Rushton, J., Schleicher, R., Silady, F., Stanculescu, A., Stoots, C., and Wright, R. [2013] Fluoride-Salt-Cooled, High-Temperature Reactor (FHR) Subsystems Definition, Functional Requirement Definition, and Licensing Basis Event (LBE) Identification White Paper. University of California, Berkeley, Integrated Research Project Workshop 1, UCBTH-12-001.

American Society of Mechanical Engineers (ASME) and American Nuclear Society (ANS) [2009] 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 (ASME) and American Nuclear Society (ANS) [2013] Standard for Probabilistic Risk Assessment for Advanced Non-LWR Nuclear Power Plant Applications. ASME/ANS RA S-1.4-2013.

Apostolakis, G. [2016] Risk-Informed Decision Making and Nuclear Power. Presented at The Institute of Energy Economics, Japan, Sept 27, 2016. Available at: https://eneken.ieej.or.jp/data/6987.pdf.

Atomic Energy Commission (AEC) [1969] Nuclear Terms: A Brief Glossary, Second Edition. US AEC, Division of Technical Information.

Beall, S.E. [1962] Molten Salt Reactor Experiment Preliminary Hazards Report. Oak Ridge National Laboratory, CF-61-2-46, Addendum No. 2.

Beall, S.E., and Guymon, R.H. [1964] MSRE Design and Operations Report - Part VI: Operating Safety Limits for the Molten-Salt Reactor Experiment. Oak Ridge National Laboratory, ORNL-TM-733.

Beall, S.E., Haubenreich, P.N., Lindauer, R.B., and Tallackson, J.R. [1964] MSRE Design and Operations Report - Part V: Reactor Safety Analysis Report. Oak Ridge National Laboratory, ORNL-TM-732.

Bell, M.J. [1970] Calculated Radioactivity of MSRE Fuel Salt. Oak Ridge National Laboratory, ORNL-TM-2970.

Benhardt, H.C., Eide, S.A., Held, J.E., Olsen, L.M., and Vail, R.E. [1994] Savannah River Site Human Error Data Base Development for Nonreactor Nuclear Facilities. Westinghouse Savannah River Company, WSRC-TR-93-581.

Bettis, E.S., Cottrell, W.B., Mann, E.R., Meem, J.L., and Whitman, G.D. [1957] The Aircraft Reactor Experiment - Operation. Nuclear Science and Engineering, 2, 841-853.

Bettis, E.S., Alexander, L.G., and Watts, H.L. [1972] Design Studies of a Molten-Salt Reactor Demonstration Plant. Oak Ridge National Laboratory, ORNL-TM-3832.

Blanchard, A., and Roy, B.N. [1998] Savannah River Site Generic Database Development. Westinghouse Safety Management Solution, WSRC-TR-93-262, Rev. 1.

Briggs, R.B. [1961] Molten-Salt Reactor Program Progress Report for Period from August 1, 1960, to February 28, 1961. Oak Ridge National Laboratory, ORNL-3122.

Briggs, R.B. [1964] Molten-Salt Reactor Program Semiannual Progress Report for Period Ending January 31, 1964. Oak Ridge National Laboratory, ORNL-3626.

Briggs, R.B. [1971] Additional Calculations of the Distribution of Tritium in the MSRE. Oak Ridge National Laboratory, ORNL CF-71-7-8.

Burge, S. [2010] The Systems Engineering Tool Box: Functional Failure Modes and Effects Analysis. Version 1.2. Burge Hughes Walsh, Rugby, England.

Cadwallader, L.C. [1998] Selected Component Failure Rate Values from Fusion Safety Assessment Tasks. Idaho National Engineering and Environmental Laboratory (INEEL), Idaho Falls, ID, INEEL/EXT-98-00892.

Capelli, E., Benes, O., and Konings, R.J.M. [2018] Thermodynamics of soluble fission products cesium and iodine in the Molten Salt Reactor. Journal of Nuclear Materials, 501, 238-252.

Center for Chemical Process Safety (CCPS) [1989] Guidelines for Process Equipment Reliability Data with Data Tables. American Institute of Chemical Engineers (AIChE), New York, NY.

Center for Chemical Process Safety (CCPS) [2008] Guidelines for Hazard Evaluation Procedures. 3rd ed. John Wiley & Sons, Inc. and the American Institute of Chemical Engineers (AIChE), New York, NY.

Center for Chemical Process Safety (CCPS) [2010] Guidelines for Chemical Process Quantitative Risk Analysis. 2nd ed. John Wiley & Sons, Inc. and the American Institute of Chemical Engineers (AIChE), New York, NY.

Center for Chemical Process Safety (CCPS) [2015] Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis. John Wiley & Sons, Inc. and the American Institute of Chemical Engineers (AIChE), New York, NY.

Cheng, B., Kim, Y.-J., and Chou, P. [2016] Improving Accident Tolerance of Nuclear Fuel with Coated Mo-alloy Cladding. Nuclear Engineering and Technology, 48, 16-25.

Chisholm, B., Krahn, S., Marotta, P., and Croff, A. [2017] Preliminary Risk Assessment of a Generalized Molten Salt Reactor Off-Gas System. Transactions of the American Nuclear Society, 117, 1, 221-224.

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

Chisholm, B., Krahn, S., Marotta, P., Sowder, A., and Smith, N. [2018b] Preliminary Reliability Analysis of Molten Salt Reactor Experiment Freeze Valves. Transactions of the American Nuclear Society, 119, 1, 195-198.

Chisholm, B., Krahn, S., Harkema, M., Sowder, A., and Leach, C. [2019] Considerations for Early-Stage Safety Assessments for Advanced Reactor Designs. Transactions of the American Nuclear Society, 121, 1, 993-996.

Chisholm, B.M., Flanagan, G.F., Krahn, S.L., and Mays, G.T. [2018c] A New Look at Licensing Basis Events for the Molten Salt Reactor Experiment. Oak Ridge National Laboratory, ORNL/TM-2018/788.

Compere, E.L., Kirslis, S.S., Bohlmann, E.G., Blankenship, F.F., and Grimes, W.R. [1975] Fission Product Behavior in the Molten Salt Reactor Experiment. Oak Ridge National Laboratory, ORNL-4865.

Cowan, P. [2016] NEI Activities in Support of Advanced Non-Light Water Reactors. Nuclear Energy Institute, Washington, D.C., NRC ADAMS No: ML17013A139.

Crawley, F., and Tyler, B. [2015] HAZOP Guide to Best Practice. 3rd ed. Elsevier, Waltham, MA.

Deuvorst, F.R. [2017] Design of the Cooling Fins on the Freeze Plug. Delft University of Technology, Department of Applied Physics, BS Thesis.

Diamond, D.J. [2006] Experience Using Phenomena Identification and Ranking Technique (PIRT) for Nuclear Analysis. Presented at PHYSOR-2006 Topical Meeting, Sept 10-14, Vancouver, British Columbia, Canada.

Diamond, D.J., Brown, N.R., Denning, R., and Bajorek, S. [2018] Phenomena Important in Modeling and Simulation of Molten Salt Reactors. Brookhaven National Laboratory, BNL-114869-2018-IR.

Eide, S.A., Chmielewski, S.V., and Swantz, T.D. [1990] Generic Component Failure Data Base for Light Water and Liquid Sodium Reactor PRAs. Idaho National Engineering Laboratory, EGG-SSRE-8875.

Eide, S.A., Wierman, T.E., Gentillon, C.D., Rasmuson, D.M., and Atwood, C.L. [2007] Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants. Idaho National Laboratory, NUREG/CR-6928.

Electric Power Research Institute (EPRI) [2014] Computer Aided Fault Tree Analysis System (CAFTA), Version 6.0b. Palo Alto, CA, URL: https://www.epri.com/#/pages/product/000000003002000020/.

Electric Power Research Institute (EPRI) [2015] Program on Technology Innovation: Technology Assessment of a Molten Salt Reactor Design -- The Liquid Fluoride Thorium Reactor (LFTR). Palo Alto, CA, EPRI Report 3002005460. URL: https://www.epri.com/#/pages/product/000000003002005460/.

Electric Power Research Institute (EPRI) [2017] Program on Technology Innovation: Expanding the Concept of Flexibility for Advanced Reactors: Refined Criteria, a Proposed Technology Readiness Scale, and Time-Dependent Technical Information Availability. Palo Alto, CA, EPRI Report 3002010479. URL: https://www.epri.com/#/pages/product/000000003002010479/.

Electric Power Research Institute (EPRI) [2018] Program on Technology Innovation: Early Integration of Safety Assessment into Advanced Reactor Design, Preliminary Body of Knowledge and Methodology. EPRI Report 3002011801. URL: https://www.epri.com/#/pages/product/000000003002011801/.

Electric Power Research Institute (EPRI) [2019] Development of a Technology-Neutral Approach to Safety-in-Design for Advanced Nuclear Power: Progress Report, Insights, and Lessons Learned. EPRI Report 3002015752. URL: https://www.epri.com/#/pages/product/000000003002015752/.

Elsheikh, B.M. [2013] Safety assessment of molten salt reactors in comparison with light water reactors. Journal of Radiation Research and Applied Sciences, 6, 2, 63-70.

Elysium Industries USA [2018] Advanced Nuclear Technology to Close the Fuel Cycle. Presented at Institute of Nuclear Materials Management (INMM) Spent Fuel Seminar, Jan 24, Washington, DC.

Ericson, C.A. [2011] Consice Encyclopedia of System Safety: Definition of Terms and Concepts. John Wiley & Sons, Hoboken, NJ.

Flanagan, G.F. [2017] Historical Perspective - MSRE Safety Basis Authorization. Presented at 2017 ORNL MSR Workshop, October 3, Oak Ridge, TN.

Fu, Y. [2016] SINAP loop operations - summary of experience to data. Presented at 2016 ORNL MSR Workshop, Oct 4-5, Oak Ridge, TN.

GA Technologies [1987] Probabilistic Risk Assessment for the Standard Modular High Temperature Gas-Cooled Reactor. San Diego, CA, DOE-HTGR-86-011, Revision 3, Volume 1.

GE Hitachi Nuclear Energy [2017] Final Scientific/Technical Report: Development/Modernization of an Advanced Non-LWR Probabilistic Risk Assessment. Argonne National Laboratory, Report No. DOEGEHH08325.

Generation IV International Forum (GIF) [2011] An Integrated Safety Assessment Methodology (ISAM) for Generation IV Nuclear Systems. Version 1.1. GIF Risk and Safety Working Group (RSWG).

Generation IV International Forum (GIF) [2013] Technology Systems. Accessed Jan 31, 2020. Available at: https://www.gen-4.org/gif/jcms/c_40486/technology-systems

Generation IV International Forum (GIF) [2014a] Guidance Document for Integrated Safety Assessment Methodology (ISAM). GIF Risk and Safety Working Group (RSWG), GIF/RSWG/2014/001.

Generation IV International Forum (GIF) [2014b] Technology Roadmap Update for Generation IV Nuclear Energy Systems. OECD Nuclear Energy Agency.

Geraci, N.C. [2017] Initiating Event Analysis of a Lithium Fluoride Thorium Reactor. Masters of Science (MS) thesis, Engineering Management, Old Dominion University.

Gèrardin, D., Allibert, M., Heuer, D., Laureau, A., Merle-Lucotte, E., and Seuvre, C. [2017] Design Evolutions of the Molten Salt Fast Reactor. Presented at International Conference on Fast Reactors and Related Fuel Cycles: Next Generation Nuclear Systems for Sustainable Development (FR17), Yekaterinburg, Russia.

Gèrardin, D., Uggenti, A.C., Beils, S., Carpignano, A., Dulla, S., Merle, E., Heuer, D., Laureau, A., and Allibert, M. [2019] A methodology for the identification of the postulated initiating events of the Molten Salt Fast Reactor. Nuclear Engineering and Technology, 51, 1024-1031.

Gertman, D.I., Gilbert, B.G., Gilmore, W.E., and Galyean, W.J. [1989] Nuclear Computerized Library for Assessing Reactor Reliability (NUCLARR) Data Manual - Part 3: Hardware Component Failure Data (HCFD). EG&G Idaho, Inc., Idaho Falls, ID, NUREG/CR-4639 (EGG-2458) Volume 5, Part 3, Rev. 1.

Giraud, J., Ghetta, V., Rubiolo, P., and Retamales, M.T. [2019] Development of a cold plug valve with fluoride salt. EPJ Nuclear Sciences & Technologies, 5, 9.

Grabaskas, D. [2014] A Review of U.S. Sodium Fast Reactor PRA Experience. Presented at 12th Conference on Probabilistic Safety Assessment and Management (PSAM12), June 2014, Honolulu, Hawaii.

Gupta, D. and Barjramovic, E. [2017] Security culture for nuclear facilities. AIP Conference Proceedings 1799, 050014. DOI: 10.1063/1.4972948

Guymon, R.H. [1966] MSRE Design and Operations Report - Part VII: Operating Procedures. Oak Ridge National Laboratory, ORNL-TM-908, Vol. II.

Guymon, R.H., Steffy, R.C., and Gabbard, C.H. [1970] Preliminary Evaluation of the Leak in the MSRE Primary System Which Occurred During the Final Shutdown. Oak Ridge National Laboratory, CF-70-4-24.

Guymon, R.H. [1973] MSRE Systems and Components Performance. Oak Ridge National Laboratory, ORNL-TM-3039.

Haubenreich, P.N., and Engel, J.R. [1962] Safety Calculations for MSRE. Oak Ridge National Laboratory, ORNL-TM-251.

Haubenreich, P.N., Engel, J.R., Prince, B.E., and Claiborne, H.C. [1964] MSRE Design and Operations Report - Part III: Nuclear Analysis. Oak Ridge National Laboratory, ORNL-TM-730.

Hicks, T., Warner, M., Miller, G., and Li, J. [2018] PRISM Sodium Fast Reactor Licensing Modernization Project Demonstration. Southern Company, Report SC-29980-201.

Holcomb, D. [2017] Module 2: Overview of MSR Technology and Concepts. ORNL Presentation for US Nuclear Regulatory Commission Staff, Washington, DC, NRC ADAMS No: ML17331B114.

Holcomb, D.E., Huning, A., Yigitoglu, A.G., Muhlheim, M.D., Poore, W.P., and Flanagan, G.F. [2019] Molten Salt Reactor Initiating Event and Licensing Basis Event Workshop Summary. Oak Ridge National Laboratory, ORNL/TM-2019/1246.

Houtzeel, A., and Dyer, F. [1972] A Study of Fission Products in the Molten-Salt Reactor Experiment by Gamma Spectroscopy. Oak Ridge National Laboratory, ORNL-TM-3151.

Howard, T., Holcolmb, D.E., and Robb, K.R. [2019] Assessment on the Practicality of Off-the-Shelf Valves for Use in Molten Salt. Presented at 18th International Topical Meeting on Nuclear Reactor Thermal Hydraulics (NURETH 2018), Aug 18-23, Portland, Oregon.

Idaho National Laboratory (INL) [2010] Next Generation Nuclear Plant Licensing Basis Event Selection White Paper. Idaho Falls, ID, INL/EXT-10-19521.

International Atomic Energy Agency (IAEA) [1988] Component Reliability Data for use in Probabilistic Safety Assessment. Vienna, Austria, IAEA TECDOC-478.

International Atomic Energy Agency (IAEA) [1991] Safety Related Terms for Advanced Nuclear Plants. Vienna, Austria, IAEA-TECDOC-626.

International Atomic Energy Agency (IAEA) [1993] Defining Initiating Events for Purposes of Probabilistic Safety Assessment. Vienna, Austria, IAEA-TECDOC-719.

International Atomic Energy Agency (IAEA) [2000] Heat Transport and Afterheat Removal for Gas Cooled Reactors Under Accident Conditions. Vienna, Austria, IAEA-TECDOC-1163.

International Atomic Energy Agency (IAEA) [2002] Procedures for conducting probabilistic safety assessment for non-reactor nuclear facilities Vienna, Austria, IAEA-TECDOC-1267

International Atomic Energy Agency (IAEA) [2007] Molten Salt Reactor for Sustainable Nuclear Power - MSR FUJI. Status of Small Reactor Designs Without On-Site Refuelling. Vienna, Austria. IAEA-TECDOC-1536, Annex XXX.

International Atomic Energy Agency (IAEA) [2008] Best Estimate Safety Analysis for Nuclear Power Plants: Uncertainty Evaluation. Vienna, Austria, Safety Reports Series No. 52.

International Atomic Energy Agency (IAEA) [2009] Deterministic Safety Analysis for Nuclear Power Plants. Vienna, Austria, IAEA Standards Series No. SSG-2.

International Atomic Energy Agency (IAEA) [2010] Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants. Vienna, Austria, IAEA Standards Series No. SSG-3.

International Atomic Energy Agency (IAEA) [2019] IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection. Vienna, Austria, 2018 Edition.

International Council on Systems Engineering (INCOSE) [2015] Systems Engineering Handbook. Fourth ed. John Wiley & Sons, Inc., Hoboken, NJ. INCOSE-TP-2003-002-04.

Joubert, J., Kohtz, N., and Coe, I. [2009] South African Safety Assessment Framework for the Pebble Bed Modular Reactor. Presented at Fourth International Topical Meeting on High Temperature Reactor Technology, Sept 28 - Oct 1, Washington, DC.

Kaplan, S., and Garrick, B.J. [1981] On The Quantitative Definition of Risk. Risk Analysis, 1, 1, 11-27.

Keller, W., and Modarres, M. [2005] 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, 89, 3, 271-285.

Khan, F.I., and Abbasi, S.A. [1998] Techniques and methodologies for risk analysis in chemical process industries. Journal of Loss Prevention in the Process Industries, 11, 4, 261-277.

King, T.L., Landry, R.R., Throm, E.D., and Wilson, J.N. [1991] Preapplication Safety Evaluation Report for the Sodium Advanced Fast Reactor (SAFR) Liquid-Metal Reactor. US NRC, Washington, DC, NUREG-1369.

Kong, X., Fu, Y., Zhang, J., Lu, H., and Wang, N. [2018] Upgrade and Shakedown Test of a High Temperature Fluoride Salt Test Loop. Presented at 26th International Conference on Nuclear Engineering (ICONE26), July 22-26, London, England.

Krahn, S., Chisholm, B., and Sowder, A. [2018a] A Project to Encourage the Early Integration of Safety Assessment into the Design, License, and Build Process of Nuclear Power Plants - Status Report. Presented at 14th International Conference on Probabilistic Safety Assessment and Managment (PSAM 14), Sept 16-21, Los Angeles, CA.

Krahn, S., Modarres, M., and O'Brien, J. [2018b] Understanding and effectively managing conservatisms in safety analysis. Presented at 28th International European Safety and Reliability Conference (ESREL 2018), June 17-21, Trondheim, Norway.

LeBlanc, D. [2010] Molten salt reactors: A new beginning for an old idea. Nuclear Engineering and Design, 240, 6, 1644-1656.

Lehtveer, M., and Hedenus, F. [2015] How much can nuclear power reduce climate mitigation cost? – Critical parameters and sensitivity. Energy Strategy Reviews, 6, 12-19.

Li, Q., Tang, Z., Fu, Y., Li, Z., and Wang, N. [2014] Preliminary Study of the Use of Freeze-Valves for a Passive Shutdown System in Molten Salt Reactors. Presented at ASME/NRC 12th Valves, Pumps, and Inservice Testing Symposium (NRC2014), June 23-25, Rockville, Maryland.

Lihoutech [2014] HAZOP Manager V7.0. Lihou Technical & Software Services, Birmingham, UK.

Lindauer, R.B. [1967] MSRE Design and Operations Report - Part VII: Fuel Handling and Processing Plant. Oak Ridge National Laboratory, ORNL-TM-907 Rev. 1.

Lindauer, R.B. [1969] Processing of the MSRE Flush and Fuel Salts. Oak Ridge National Laboratory, ORNL-TM-2578.

Mackowiak, D.P., Gentillon, C.D., and Smith, K.L. [1985] Development of Transient Initiating Event Frequencies for Use in Probabilistic Risk Assessments. EG&G Idaho, Inc., Idaho Falls, ID, NUREG/CR-3862.

Makkinje, A. [2017] Design of a Freeze Plug Grate. Delft University of Technology, Department of Applied Physics, BS Thesis.

McClymont, A.S., and Poehlman, B.W. [1982] ATWS: A Reappraisal, Part 3: Frequency of Anticipated Transients. EPRI, Palo Alto, CA, EPRI-NP-2230.

McDermid, J.A., Nicholson, M., Pumfrey, D.J., and Fenelon, P. [1995] Experience with the application of HAZOP to computer-based systems. COMPASS '95: Proceedings of the Tenth Annual Conference on Computer Assurance, June 25-29, pp 37-48.

McFarlane, J., Taylor, P., Holcomb, D., and Poore, W.P. [2019] Review of Hazards associated with Molten Salt Reactor Fuel Processing Operations. Oak Ridge National Laboratory, ORNL/TM-2019/1195.

Mei, M., Shao, S., He, Z., and Chen, K. [2014] Research on initial event analysis for solid thorium molten salt reactor probabilistic safety assessment. Nuclear Techniques, 37, 9, 090601.

Metzroth, K.G. [2011] A Comparison of Dynamic and Classical Event Tree Analysis for Nuclear Power Plant Probabilistic Safety/Risk Assessment. The Ohio State University, PhD Dissertation.

Milstein, R.I. [2001] Integrated Safety Analysis Guidance Document. US NRC, Washington, DC, NUREG-1513.

Modarres, M. [2006] Risk Analysis in Engineering: Techniques, Tools, and Trends. CRC Press, Boca Raton, FL.

Mohsin, M.H., Qureshi, K., and Ashfaq, T. [2019] Safety assessment of MSR concept using INPRO methodology. Progress in Nuclear Energy, 117.

Moore, R.L. [1972] MSRE Design and Operations Report - Part IIB: Nuclear and Process Instrumentation. Oak Ridge National Laboratory, ORNL-TM-729B.

Mosleh, A., Rasmuson, D.M., and Marshall, F.M. [1998] Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment. Idaho National Engineering and Environmental Laboratory, Idaho Falls, ID, NUREG/CR-5485 and INEEL/EXT-97-01327.

Nagel, C., and Stephanopoulos, G. [1995] Inductive and Deductive Reasoning: The Case of Identifying Potential Hazards in Chemical Processes. Advances in Chemical Engineering, 21, 187-225.

National Aeronautics and Space Administration (NASA) [2011] Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practictioners, Second Edition. NASA/SP-2011-3421.

National Research Council [2014] Lessons Learned from the Fukushima Nuclear Accident for Improving Safety of U.S. Nuclear Plants. Committee on Lessons Learned from the Fukushima Nuclear Accident for Improving Safety and Security of U.S. Nuclear Plants; Nuclear and Radiation Studies Board; Division on Earth and Life Studies. National Academies Press, Washington, DC.

Nestor Jr., C.W. [1962a] MURGATROYD -- An IBM 7090 Program for the Analysis of the Kinetics of the MSRE. Oak Ridge National Laboratory, ORNL-TM-203.

Nestor Jr., C.W. [1962b] ZORCH -- An IBM 7090 Program for the Analysis of Simulated MSRE Power Transient with a Simplified Space-Dependent Kinetics Model. Oak Ridge National Laboratory, ORNL-TM-345.

Nolan, D.P. [2015] Safety and Security Review for the Process Industries: Application of HAZOP, PHA, What-If and SVA Reviews. 4th ed. Gulf Professional Publishing, Waltham, MA.

Northwest Medical Isotopes LLC [2017] Chapter 13 - Accident Analysis. Construction Permit Application for Radioisotope Production Facility, Corvallis, OR, NWMI-2013-021, Rev. 3.

Nourbakhsh, H.P., Apostolakis, G., and Powers, D.A. [2018] The evolution of the U.S. nuclear regulation process. Progress in Nuclear Energy, 102.

Nuclear Energy Agency (NEA) [2012] Nuclear Energy Today. Organisation for Economic Co-operation and Development (OECD), NEA No. 6885, 2nd Ed.

Nuclear Energy Institute (NEI) [2019] Risk-Informed Performance-Based Guidance for Non-Light Water Reactor Licensing Basis Development, Report Revision 1. Washington, DC, NEI 18-04, NRC ADAMS No: ML19241A472.

Nuclear Regulatory Commission (NRC) [1983] PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants. Washington, DC, NUREG/CR-2300, Vol. 1.

Nuclear Regulatory Commission (NRC) [1986] Policy statement on safety goals for the operation of nuclear power plants. Fed. Regist., 51 FR 28044; Aug 1986, as corrected and republished at 51 FR 30028.

Nuclear Regulatory Commission (NRC) [1989] Draft Preapplication Safety Evaluation Report for the Modular High-Temperature Gas-Cooled Reactor. Washington, DC, NUREG-1338.

Nuclear Regulatory Commission (NRC) [1990] Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants. Washington, DC, NUREG-1150.

Nuclear Regulatory Commission (NRC) [1994] Preapplication Safety Evaluation Report for the Power Reactor Innovative Small Module (PRISM) Liquid-Metal Reactor. Washington, DC, Final Report, NUREG-1368.

Nuclear Regulatory Commission (NRC) [2001] Integrated Safety Analysis Guidance Document. Washington, DC, NUREG-1513.

Nuclear Regulatory Commission (NRC) [2007a] Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, LWR Edition. Washington, DC, NUREG-0800.

Nuclear Regulatory Commission (NRC) [2007b] Feasibility Study for a Risk-Informed and Performance-Based Regulatory Structure for Future Plant Licensing. Washington, DC, NUREG-1860.

Nuclear Regulatory Commission (NRC) [2008] Policy Statement on the Regulation of Advanced Reactors. Washington, DC, NRC-2008-0237.

Nuclear Regulatory Commission (NRC) [2009] An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities. Washington, DC, RG 1.200, Revision 2.

Nuclear Regulatory Commission (NRC) [2011] A Comparison of Integrated Safety Analysis and Probabilistic Risk Assessment, Revision 1. Washington, DC, NRC ADAMS No: ML110610195.

Nuclear Regulatory Commission (NRC) [2013] Integrated Safety Analysis: Why It Is Appropriate for Fuel Cycle Facilities. URL: http://energy.gov/sites/prod/files/2013/06/f1/NRC_Integrated_Safety_Analysis_Fuel_Recycling_Facilities.pdf.

Nuclear Regulatory Commission (NRC) [2016a] Backgrounder on Probabilistic Risk Assessment. Washington, DC, URL: https://www.nrc.gov/docs/ML0322/ML032200337.pdf.

Nuclear Regulatory Commission (NRC) [2016b] WASH-1400, The Reactor Safety Study: The Introduction of Risk Assessment to the Regulation of Nuclear Reactors. Washington, DC, NUREG/KM-0010.

Nuclear Regulatory Commission (NRC) [2018a] Probabilistic Risk Assessment (PRA). Accessed 19 June 2018. Available at: https://www.nrc.gov/about-nrc/regulatory/risk-informed/pra.html

Nuclear Regulatory Commission (NRC) [2018b] SECY-18-0011: Advanced Reactor Program Status. Washington, DC, NRC ADAMS No: ML17334B199.

Nuclear Regulatory Commission (NRC) [2018c] Tutorial on Probabilistic Risk Assessment (PRA). Accessed May 21, 2019. Available at: https://www.nrc.gov/about-nrc/regulatory/risk-informed/rpp/pra-tutorial.pdf

Nuclear Regulatory Commission (NRC) [2019a] Advanced Reactors (non-LWR designs). Accessed 14 Dec 2019. Available at: https://www.nrc.gov/reactors/new-reactors/advanced.html

Nuclear Regulatory Commission (NRC) [2019b] Glossary - Atomic Energy Commission. Accessed 18 Nov 2019. Available at: https://www.nrc.gov/reading-rm/basic-ref/glossary/atomic-energy-commission.html

Nuclear Regulatory Commission (NRC) [2019c] Guidance for a Technology-Inclusive, Risk-Informed, and Performance-Based Methodology To Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light Water Reactors. Washington, DC, DG-1353.

Papazoglou, I.A., and Aneziris, O.N. [2002] Master Logic Diagram: method for hazard and initiating event identification in process plants. Journal of Hazardous Materials, A97, 11-30.

Pehl, M., Arvesen, A., Humpenöder, F., Popp, A., Hertwich, E.G., and Luderer, G. [2017] Understanding future emissions from low-carbon power systems by integration of life-cycle assessment and integrated energy modelling. Nature Energy, 2, 12, 939-945.

Poloski, J.P., Marksberry, D.G., Atwood, C.L., and Galyean, W.J. [1999] Rates of Initiating Events at U.S. Nucler Power Plants: 1987-1995. Idaho National Engineering and Environmental Laboratory (INEEL), Idaho Falls, ID, NUREG/CR-5750.

Popović, V., and Vasić, B. [2008] Review of hazard analysis methods and their basic characteristics. FME Transactions, 36, 4, 181-187.

Product Quality Research Institute (PQRI) [2015] Hazard & Operability Analysis (HAZOP) Training Guide. PQRI Risk Management Working Group, Washington, DC, URL: http://pqri.org/wp-content/uploads/2015/08/pdf/HAZOP_Training_Guide.pdf.

Pyron, D.A. [2016] Safety Analysis for the Licensing of Molten Salt Reactors. Paul Scherrer Institute, MS Thesis.

Qun, Y., Minghai, L., Jie, H., Zhaozhong, H., and Kun, C. [2017] Application of the Probability-Based Safety Analysis for the Reliability Evaluation of a Special Fuel Salt Release System Design in the Molten Salt Reactor. Presented at ASME 25th International Conference on Nuclear Engineering (ICONE25), July 2-6, Shanghai, China.

Rhodes, R., and Beller, D. [2000] The need for nuclear power. Foreign Affairs, 79, 1, 30-44. DOI: 10.2307/20049612.

Rhodes, R. [2018] Energy: a human history. Simon & Schuster, New York.

Robertson, R.C. [1965] MSRE Design and Operations Report - Part I: Description of Reactor Design. Oak Ridge National Laboratory, ORNL-TM-728.

Robertson, R.C. [1971] Conceptual Design Study of a Single-Fluid Molten-Salt Breeder Reactor. Oak Ridge National Laboratory, ORNL-4541.

Rosenthal, M.W. [2010] An Account of Oak Ridge National Laboratory's Thirteen Nuclear Reactors. Oak Ridge National Laboratory, ORNL/TM-2009/181 (Rev.).

Schweizerische Eidgenossenschaft [2009] Probabilistic Safety Analysis (PSA): Quality and Scope. Guideline for Swiss Nuclear Installations, ENSI-A05/e.

Serp, J., Allibert, M., Beneš, O., Delpech, S., Feynberg, O., Ghetta, V., Heuer, D., Holcomb, D., Ignatiev, V., Kloosterman, J.L., Luzzi, L., Merle-Lucotte, E., Uhlíř, J., Yoshioka, R., and Zhimin, D. [2014] The molten salt reactor (MSR) in generation IV: Overview and perspectives. Progress in Nuclear Energy, 77, 0, 308-319.

Shafer, T.D. [2018] Design and Melting Behavior of the MSFR Freeze Plug. Delft University of Technology, MS Thesis.

SHINE Medical Technologies Inc. [2015] Preliminary Safety Analysis Report. Janesville, WI, NRC-006C, Rev. 1. NRC ADAMS No: ML15342A435.

Shopsky, W.E. [1977] Failure Mode and Effects Analysis (FMEA) of the Emergency Core Cooling System (ECCS) for a Westinghouse type 312, three loop pressurized water reactor. Westinghouse Nuclear Energy Systems, Pittsburgh, PA, WCAP-8977.

Singh, V., Lish, M.R., Chvála, O., and Upadhyaya, B.R. [2017] Dynamics and control of molten-salt breeder reactor. Nuclear Engineering and Technology, 49, 5, 887-895.

Socolow, R.H., and Glaser, A. [2009] Balancing risks: nuclear energy & climate change. Daedalus, 138, 4, 31-44.

Southern Company [2019a] Modernization of Technical Requirements for Licensing of Advanced Non-Light Water Reactors: Probabilistic Risk Assessment Approach. SC-29980-101 Rev 0.

Southern Company [2019b] Modernization of Technical Requirements for Licensing of Advanced Non-Light Water Reactors: Risk-Informed and Performance-Based Evaluation of Defense-in-Depth Adequacy. SC-29980-103 Rev 0.

Southern Company [2019c] Modernization of Technical Requirements for Licensing of Advanced Non-Light Water Reactors: Safety Classification and Performance Criteria for Structures, Systems, and Components. SC-29980-102 Rev 0.

Southern Company [2019d] Modernization of Technical Requirements for Licensing of Advanced Non-Light Water Reactors: Selection and Evaluation of Licensing Basis Events. SC-29980-100, Rev 0.

Spiewak, I. [1958] Component Development. In: Fluid Fuel Reactors. Addison-Wesley Publishing Company, Inc., Reading, MA, pp. Chap. 8, pp. 445-448.

Stamatis, D.H. [2003] Failure mode and effect analysis: FMEA from theory to execution. ASQ Quality Press, Milwaukee, WI.

Swain, A., and Guttmann, H. [1983] Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. US NRC, Washington, DC, NUREG/CR-1278.

Swaroop, P. [2016] Design of a Freeze Plug for the Molten Salt Fast Reactor (MSFR). Delft University of Technology, Department of Sustainable Energy Technology, MS Thesis.

Tallackson, J.R. [1968] MSRE Design and Operations Report - Part IIA: Nuclear and Process Instrumentation. Oak Ridge National Laboratory, ORNL-TM-729A.

TerraPower LLC [2019] TerraPower's Molten Chloride Fast Reactor Technology: Retooling Nuclear for a Changing Energy Sector. Bellevue, WA, URL: https://www.terrapower.com/resources/#group_6799-19.

ThorCon [2018] ThorCon: The Do-able Molten Salt Reactor. Version 1.24, Stevenson, WA, URL: http://thorconpower.com/docs/domsr20180119.pdf.

Tiberga, M., Shafer, D., Lathouwers, D., Rohde, M., and Kloosterman, J.L. [2019] Preliminary investigation on the melting behavior of a freeze-valve for the Molten Salt Fast Reactor. Annals of Nuclear Energy, 132, pp. 544-554.

UCOR [2016] Molten Salt Reactor Experiment Engineering Evaluation and Extended Life Study. URS | CH2M Oak Ridge LLC, Oak Ridge, TN, STJ-02MSRE-D992.

Uggenti, A.C., Delphine, G., Andrea, C., Sandra, D., Elsa, M., Daniel, H., Axel, L., and Michel, A. [2017] Preliminary functional safety assessment for molten salt fast reactors in the framework of the SAMOFAR project. Presented at International Topical Meeting on Probabilistic Safety Assessment and Analysis (PSA2017), Sept 24-28, Pittsburgh PA.

US Department of Defense (DoD) [2005] DoD Guide for Achieving Reliability, Availability, and Maintainability. Washington, DC.

US Department of Energy (DOE) [2004] DOE Handbook: Chemical Process Hazards Analysis, Report. Washington, DC, DOE-HDBK-1100-2004.

US Department of Energy (DOE) [2011] Technology Readiness Assessment Guide. Washington, DC, DOE G 413.3-4A.

US Department of Energy (DOE) [2013] DOE Standard on Development of Probabilistic Risk Assessments for Nuclear Safety Applications. Washington, DC, DOE-STD-1628-2013.

US Department of Energy (DOE) [2016] Integration of Safety into the Design Process. US DOE Office of Environment, Health, Safety, and Security, DOE-STD-1189-2016.

van Tuyll, F. [2016] A new design for the safety plug in a Molten Salt Fast Reactor. Delft University of Technology, Department of Applied Physics, BS Thesis.

Vesely, W.E., Goldberg, F.F., Roberts, N.H., and Haasl, D.F. [1981] Fault tree handbook. US NRC, Washington, DC, NUREG-0492.

Waites, B., Fleming, K., Silady, F., Huning, A., and Redd, J. [2018] High Temperature, Gas-Cooled Pebble Bed Reactor Licensing Modernization Project Demonstration. Southern Company, SC-29980-200 Rev 0.

Wielenberg, A., Alzbutas, R., Apostol, M., Bareith, A., Brac, P., Burgazzi, L., Cazzoli, E., Cizelj, L., and Hage, M. [2017] Methodology for Selecting Initiating Events and Hazards for Consideration in an Extended PSA. European Union, ASAMPSA_E/WP30/D30.7/2017-31 Vol. 2.

Wood, J. [2007] Nuclear Power. The Institution of Engineering and Technology, London, United Kingdom.

World Nuclear Association (WNA) [2019] Generation IV Nuclear Reactors. Accessed Jan 31, 2020. Available at: https://www.world-nuclear.org/information-library/nuclear-fuel-cycle/nuclear-power-reactors/generation-iv-nuclear-reactors.aspx

Xu, H. [2013] Thorium Energy and Molten Salt Reactor R&D in China. Presented at Thorium Energy for the World: Proceedings of the ThEC13 Conference, Oct 27-31, Geneva, Switzerland.

Yang, Q., Li, M., Hou, J., Zhaiozhong, H., and Chen, K. [2017] Application of the Probability-Based Safety Analysis for the Reliability Evaluation of a Special Fuel Salt Release System Design in the Molten Salt Reactor. Presented at ASME 25th International Conference on Nuclear Engineering (ICONE25), July 2-6, Shanghai, China.

Zerbonia, R.A., Brockmann, C.M., Peterson, P.R., and Housley, D. [2001] Carbon Bed Fires and the Use of Carbon Canisters for Air Emissions Control on Fixed-Roof Tanks. Journal of the Air & Waste Management Association, 51, 1617-1627.

Zhang, D., Liu, L., Liu, M., Xu, R., Gong, C., Zhang, J., Wang, C., Qiu, S., and Su, G. [2017] Review of conceptual design and fundamental research of molten salt reactors in China. International Journal of Energy Research, 42, 5, pp. 1834-1848.

Zuo, J., Jing, J., Song, W., and Zhang, C. [2016] The Analysis of Initiating Events in PSA for TMSR. Presented at ASME 24th International Conference on Nuclear Engineering (ICONE24), June 26-30, Charlotte, NC.

APPENDIX A, BACKGROUND ON FLUID-FUELED NUCLEAR REACTORS

A schematic of a typical Light Water Reactor (LWR) nuclear power plant is shown in Figure 33. The nuclear reactor development approach that produced these types of water-cooled designs that are currently operating worldwide assumes that a nuclear reactor is primarily a mechanical engineering device – that the ultimate goal of economically competitive nuclear power can be achieved by simplifying the mechanical design and by making the fuel elements in the core more reliable. The structure of a typical LWR fuel assembly is illustrated in Figure 34. LWR fuel is composed of pellets, which are made of ceramic UO_2. These pellets are stacked on top of each other in a fuel rod, which is a tube made of a zirconium alloy. An array of fuel rods is then grouped together to form a fuel assembly using structural components called spacer grids. An LWR core is composed of hundreds of rigid fuel assemblies, which are held stationary by structural material and cooled using water that is pumped through the core to remove the heat produced by fission and radioactive decay.

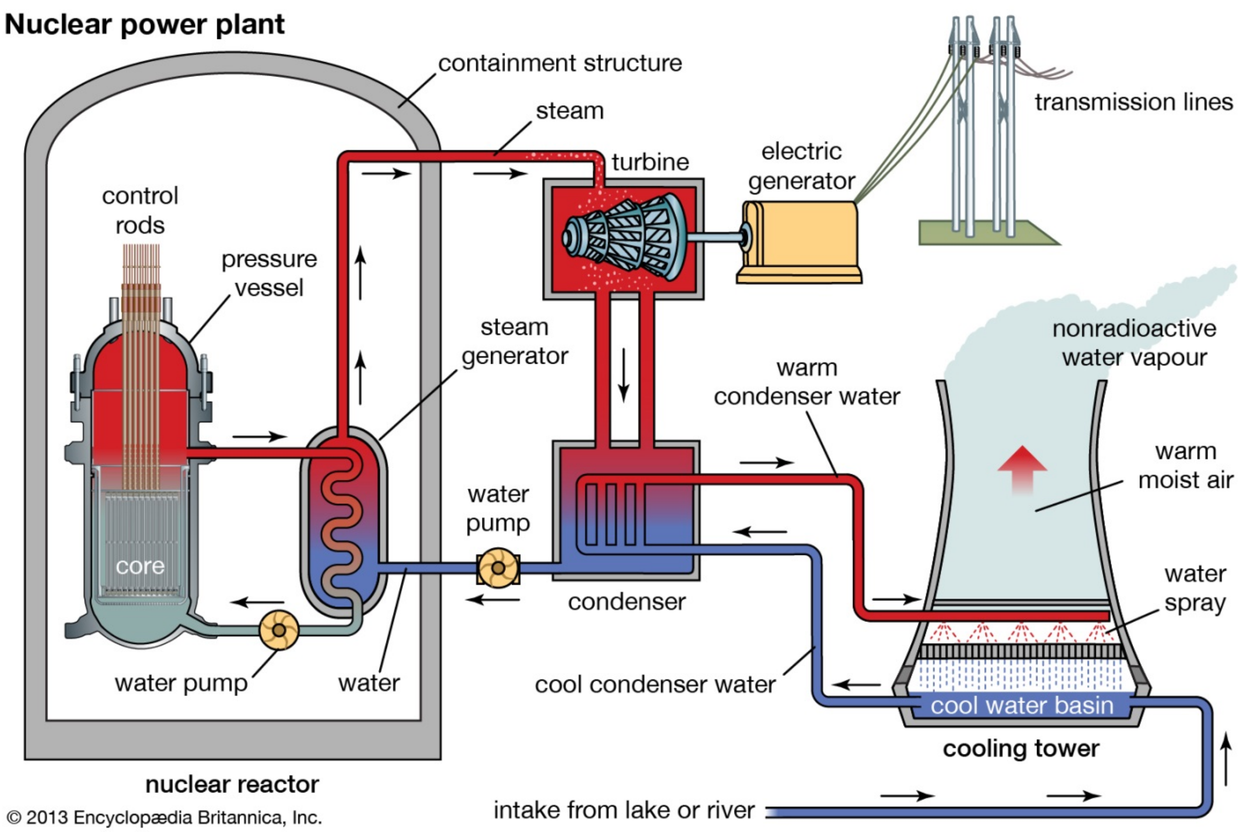


Figure 33: Schematic of a Light Water Reactor (LWR) nuclear power plant [Encylopaedia Britannica]

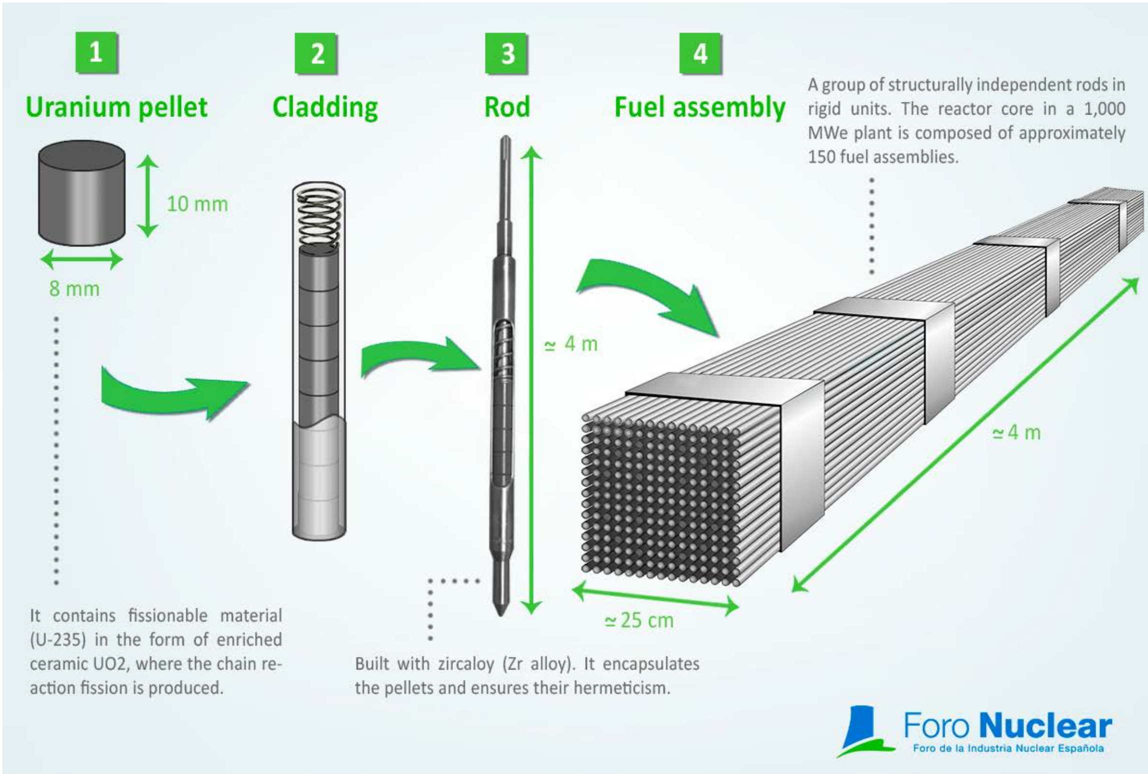


Figure 34: Structure of an LWR fuel assembly [Foro Nuclear, 2018]

However, a fundamentally different view of nuclear reactor design assumes that the economics of a nuclear reactor can be optimized using the methods that have been proven useful in the chemical industry – i.e., the continuous handing of material in liquid form. This approach to design, which holds that reactors are chemical plants, led to the conceptualization and exploration of reactors that operate using fluid fuel. Figure 35 displays a concept for a commercial nuclear power plant that operates using fuel that is made by dissolving fissile material within a molten salt. The fission products and heat produced during fission, as well as the fissile material, are circulated through the fuel salt loop, and the heat is transferred to another fluid by passing the fuel salt through a heat exchanger (or a steam generator). To provide some context for the history behind the development of fluid-fueled reactors, the following subsections of this appendix discuss the early R&D that ultimately led to the Molten Salt Reactor Program (MSRP) at Oak Ridge National Laboratory (ORNL).

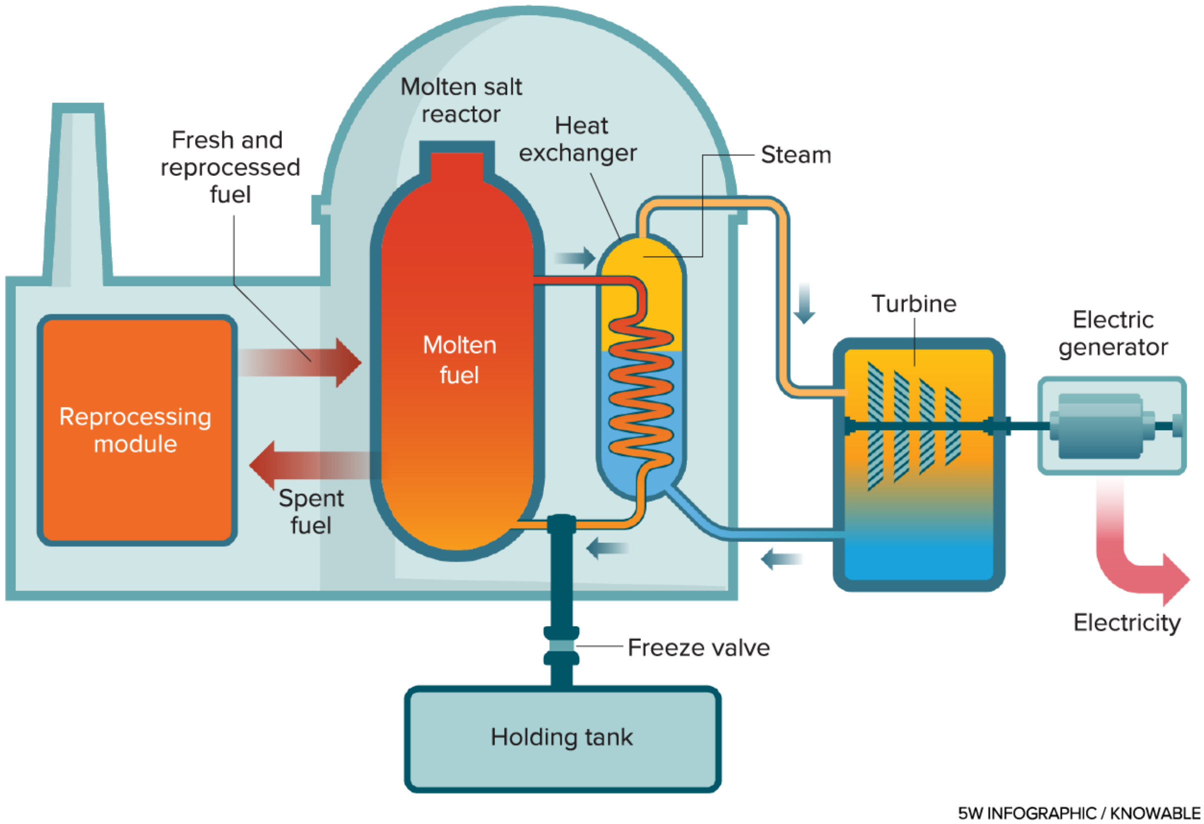


Figure 35: Schematic of a Liquid-Fueled Molten Salt Reactor (LF-MSR) nuclear power plant concept [Waldrop, 2019]

A.1. Early Aqueous Homogeneous Reactor Research

Following the discovery of uranium fission, nuclear reactors fueled with a solution or homogeneous mixture of fuel and moderator were among the first nuclear systems to be investigated experimentally. In 1939, researchers at the Cavendish Laboratory in England had established that a self-sustaining chain reaction of fissions were not possible with natural (i.e., unenriched) uranium and ordinary (i.e., light) water [Bohlmann et al., 1958]. In 1940, it was reported that a homogenous mixture of U_3O_8 powder and heavy[72] water was capable of producing a self-sustaining fission chain reaction; however, after the destruction of the Norwegian Hydroelectric Company's laboratories in 1942, the remaining worldwide inventory of D_2O was not sufficient to allow for the construction of a critical homogeneous nuclear reactor core. Thus, the first successful self-sustaining chain reaction was achieved on December 2, 1942 using solid uranium metal fuel in a heterogeneous lattice arrangement spaced inside graphite blocks. Some interest in developing homogeneous reactors to produce plutonium for the

[72] In comparison to ordinary "light" water, the hydrogen atoms in "heavy water" have an additional neutron. Hydrogen with an extra neutron is often called "deuterium," and heavy water is sometimes referred to as "deuterated water" and abbreviated as D_2O.

Manhattan Project remained at Columbia University and Chicago University, but almost all of this research was discontinued in 1944 due to the successful operation of the plutonium production reactors at Hanford [Bohlmann et al., 1958].

A.2. Fluid-Fueled Reactor Research at Los Alamos

A.2.1. The First Homogeneous Reactors

Thanks to the availability of enriched uranium samples, calculations were performed at Los Alamos in 1943 to design an aqueous homogeneous reactor that used ordinary water instead of heavy water. The fuel consisted of UO_2SO_4 dissolved in water, and the design was nicknamed the "Water Boiler" since the liquid fuel appeared to be boiling due to the splitting of water molecules into hydrogen and oxygen gas by the energetic process of fission [Atomic Heritage Foundation, 2017]. The design of the first Water Boiler, named LOPO (i.e., "low power") because it had essentially zero power output, is depicted in Figure 36, and a picture of a Water Boiler at Los Alamos is shown in Figure 37. The stainless steel sphere that held the fuel was about one foot in diameter. LOPO went critical in May 1944 using only 565 grams of uranium-235; however, this amount was the entire supply of enriched uranium that existed in the US at the time [Atomic Heritage Foundation, 2017].

LOPO was used to perform calculations related to the construction of the atomic bombs, and other theoretical experiments including investigations of: cooling and shielding, the effects of temperature changes on criticality, and the effects of control rod movements. LOPO was dismantled later in 1944, but its operation had allowed for the design of a higher power Water Boiler design, called HYPO (i.e., "high power"), which had a maximum power output of 5.5 kilowatts and began operating in 1949 [Rosenthal, 2010]. The fuel used in HYPO was a solution of uranyl nitrate, and the HYPO fuel vessel contained cooling coils to remove heat produced by fission. The major use of HYPO was as a source of neutrons for a number of experiments at Los Alamos, including measurements of the adsorption characteristics of a number of elements and calibration of equipment to measure gamma ray and neutron intensities at the Trinity test [Atomic Heritage Foundation, 2017].

By the 1950s, HYPO was heavily modified to increase its neutron output; the resulting "super-powered" reactor, named SUPO, had a maximum power output of 35 kilowatts. The major modifications included further enrichment of the uranium fuel, replacement of the beryllium oxide reflector with graphite, and the addition of a gas recombination system to fuse the hydrogen and oxygen gas produced during operation back into liquid water. SUPO operated at Los Alamos for over twenty years, during which it was used for many experiment related to nuclear weapons in addition to a series of experiments on the effects of radiation on live animals (such as mice, rats, rabbits, and monkeys) [Atomic Heritage Foundation, 2017].

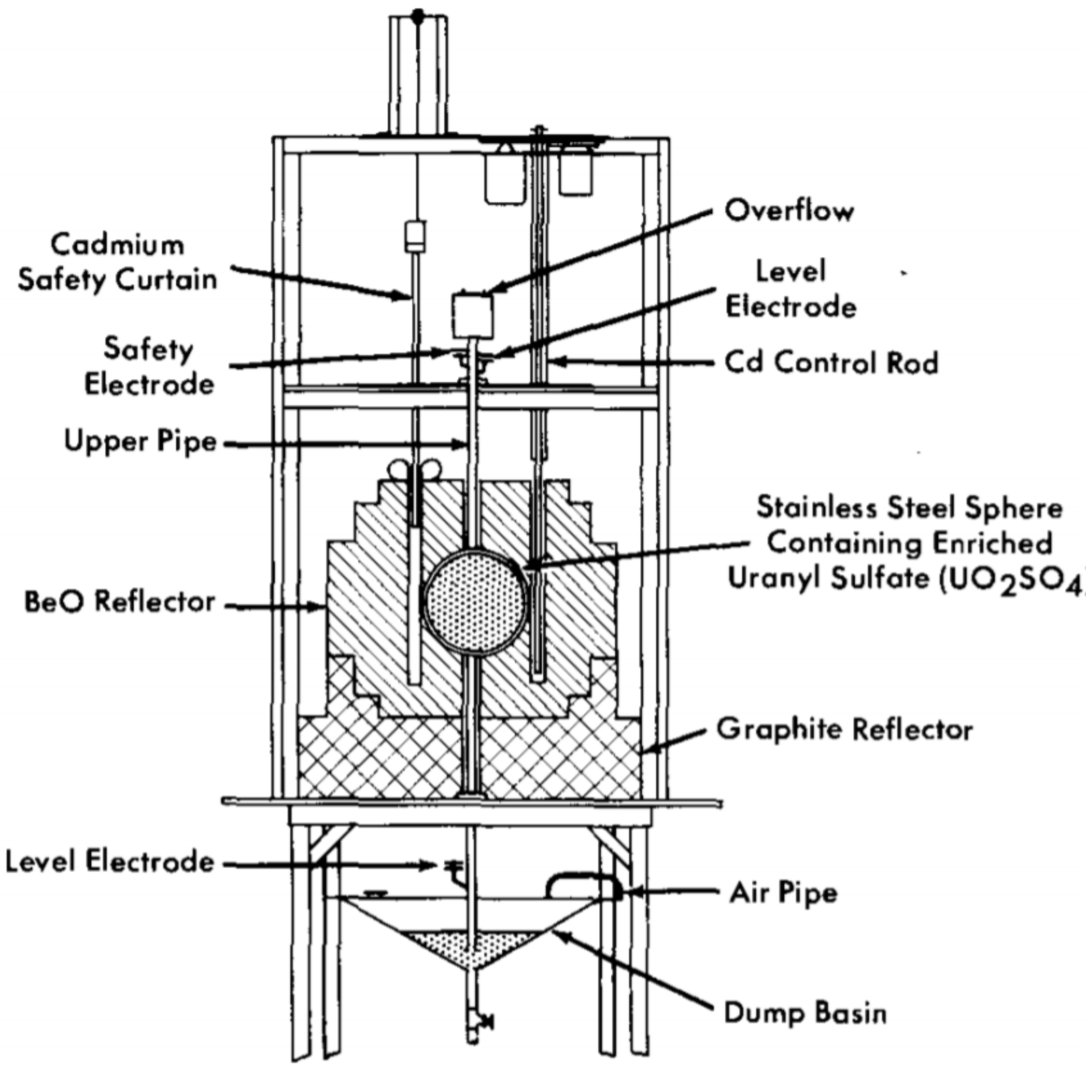


Figure 36: Cross section of LOPO design [Bohlmann et al., 1958]

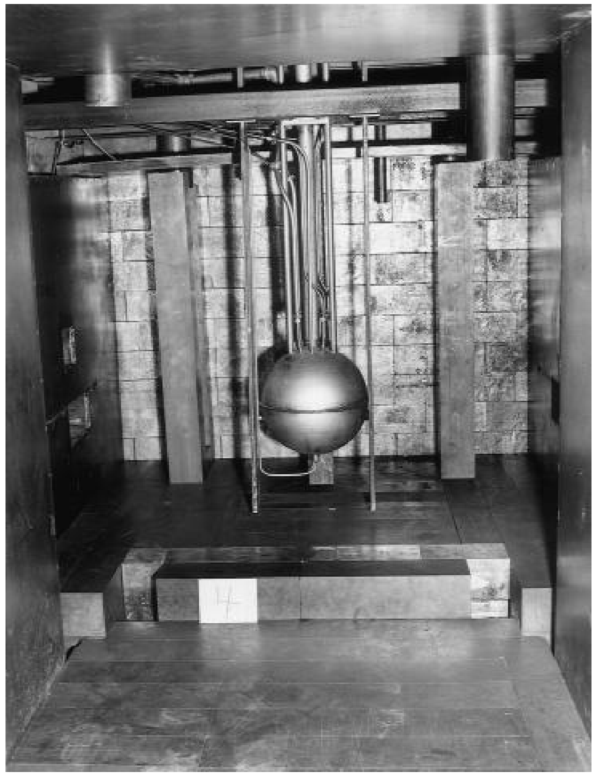


Figure 37: Picture of a "Water Boiler" reactor at Los Alamos [Atomic Heritage Foundation, 2017]

Several design variations based on the Los Alamos “Water Boilers” were constructed and operated at different laboratories across the country. The simplicity of the reactor design made it useful for experimental work with neutrons and gamma rays and for training in reactor operation. The first college-owned nuclear research reactor was called R-1, and it began operations at 10 kilowatts in September 1953 at North Carolina State College (now North Carolina State University).[73] Similar to SUPO, the R-1 fuel was a homogeneous mixture of uranyl sulphate dissolved in water; however, the R-1 fuel container was a cylinder (rather than a sphere) [Bohlmann et al., 1958]. Operations at R-1 ended in June 1955 due to corrosion in the reactor vessel and cooling coils [NC State Nuclear Reactor Program]. After the shutdown of R-1, a new reactor vessel with a hemispherical bottom was constructed and inserted into the original R-1 shielding assembly. This new reactor, which also operated on uranyl sulphate fuel, first went critical in May 1957, with a maximum power level of 500 watts. In December 1958, the R-2 reactor core was moved to a different building on the North Carolina State campus and renamed R-4. The R-4 reactor operated from 1959 to 1961 at a maximum power level of 100 watts [NC State Nuclear Reactor Program].

[73] Notably, North Carolina State is also home to the first nuclear engineering program in the US. [Keller and Modarres, 2005]

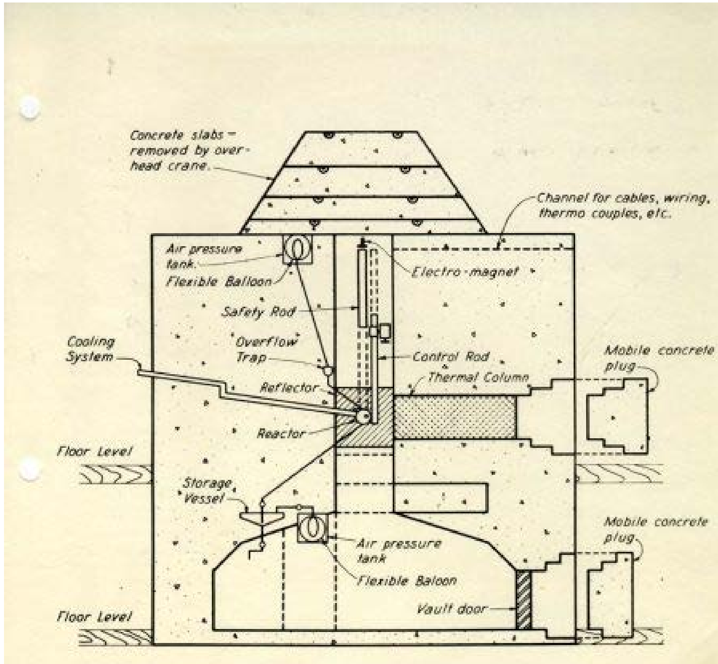


Figure 38: Schematic diagram of North Carolina State R-1 reactor [NC State Nuclear Reactor Program]

Other Water Boilers based on the Los Alamos designs were offered commercially by various companies. The Atomics International Division of the North American Aviation Company (which eventually became part of Rockwell International and is now part of Boeing) built at least 17 such reactors, including the following [Bohlmann et al., 1958; Bunker, 1983]:

- The 1-watt Water Boiler Neutron Source at Downey, California;[74]
- A 5-watt laboratory research reactor (L-47) for Atomic International;
- The 100-watt Livermore Research Reactor at Livermore, California;
- A 5-watt reactor for the Danish Atomic Energy Commission in Denmark;
- The 50-kilowatt Kinetic Experiment for Water Boilers at Santa Susana; and
- A number of other 50-kilowatt reactors for organizations such as:
    - The UCLA Medical Facility;
    - The Armour Research Foundation in Chicago, Illinois;
    - The Japan Atomic Energy Research Institute;
    - The University of Frankfurt;
    - The Institute of Nuclear Research in Germany; and
    - The Politecnico Enrico Fermi Nuclear Study Center in Italy.

[74] The Water Boiler Neutron Source was later moved to Santa Susana and modified to operate at 2 kilowatts.

A.2.2. The Los Alamos Power Reactor Experiments (LAPRE-I and -II)

The work on Water Boilers at Los Alamos led to the design of power reactor concepts that might find application within the military establishment as portable power sources [Bunker, 1983]. Construction of these reactors, which were known as Los Alamos Power Reactor Experiments No. 1 and No. 2 (LAPRE-I and LAPRE-II), started in 1955. The fuel for these reactors was a fuel solution composed of highly enriched UO_2 (93.5 percent U-235) dissolved in concentrated phosphoric acid to enable high-temperature operation at relatively low pressures [Bohlmann et al., 1958]; the reactors were designed to operate as essentially constant-temperature sources of energy [Bunker, 1983].

A schematic of the LAPRE-I design is shown in Figure 39. The reactor first reached criticality in March 1956 and was operated at 20 kilowatts for about 5 hours [Bohlmann et al., 1958]. At that time, radioactivity was noted in the steam system, so the system was shut down and dismantled to be examined. It was discovered that the gold plating on the stainless steel cooling coils had been damaged during assembly, and the phosphoric acid fuel solution had corroded through the stainless steel. After the cooling coils were replaced, operations were resumed in October 1956; however, similar corrosion difficulties were encountered, so the decision was made to permanently discontinue operations [Bohlmann et al., 1958].

Construction of the LAPRE-II reactor was completed in 1958, and a picture of the LAPRE-II core assembly can be seen in Figure 40. In order to prevent the problems related to the design and construction of LAPRE-I, the core design and method of control were different for LAPRE-II [Clark, 1960]. LAPRE-II was successfully operated at a maximum power of 800 kilowatts, and the temperature of the fuel solution and of the superheated steam output was set by the uranium concentration in the fuel and by the position of an adjustable control rod. Although the stainless steel fuel vessel and heat transfer coils had been plated with gold to mitigate the corrosiveness of the high-temperature phosphoric acid in the fuel, persistent difficulties were encountered in achieving absolute integrity of the gold cladding. Thus, the LAPRE program was terminated at Los Alamos in 1960.

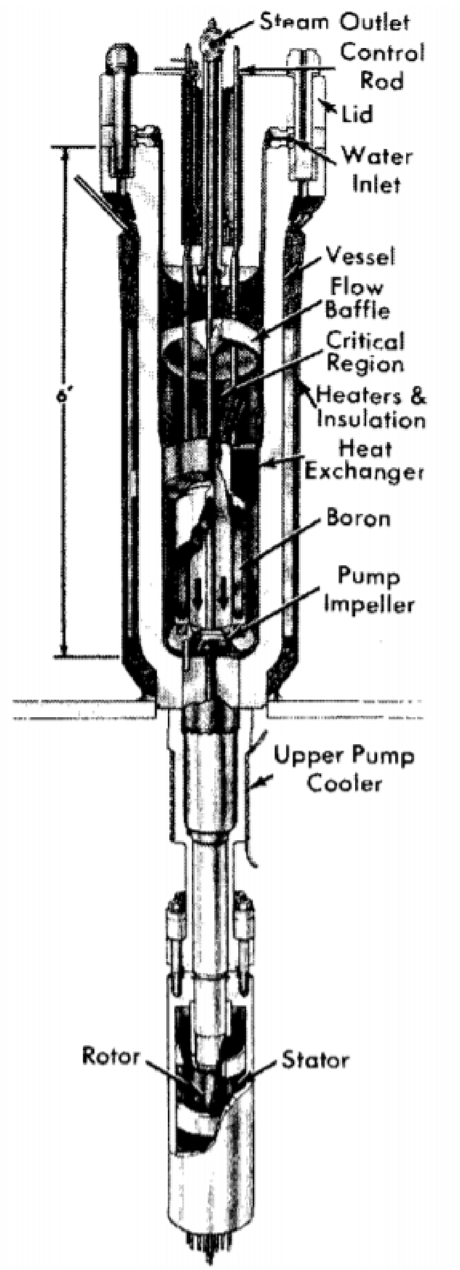


Figure 39: Schematic of LAPRE-I reactor [Bohlmann et al., 1958]

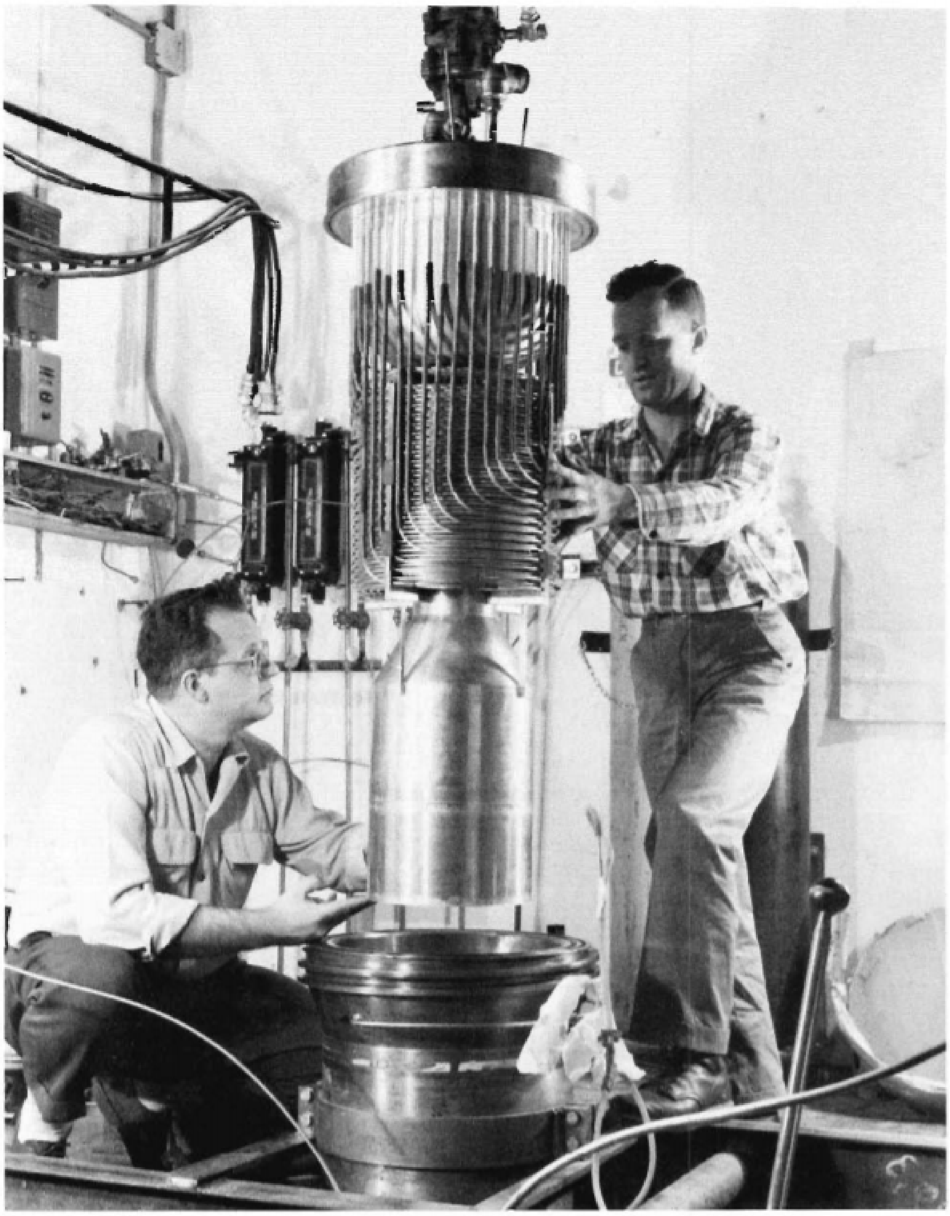


Figure 40: LAPRE-II core assembly with heat exchanger (upper section) and baffle that enclosed critical region (bottom section) [Bunker, 1983]

A.2.3. Los Alamos Molten Plutonium Reactor Experiment (LAMPRE-I)

The Los Alamos Molten Plutonium Reactor Experiment No. 1 (LAMPRE-I) was a slightly different approach to a reactor operating with fluid fuel. A cutaway view of the LAMPRE-I reactor vessel is depicted in Figure 41. The core of the 1-megawatt test reactor contained 199 separate stationary fuel elements, each consisting of a plutonium iron fuel material encased in a tantalum thimble [Bunker, 1983]. The use of plutonium fuel allowed for the reactor to operate in the fast neutron spectrum, and the heat from fission was removed by a molten sodium coolant. The operation of LAMPRE-I was intended to provide much of the materials data needed to develop and construct LAMPRE-II. The LAMPRE-II design was a 20-megawatt reactor fueled by molten plutonium contained in a single connected region and cooled by sodium flowing through tubes welded to the top and bottom plates of a cylindrical container.

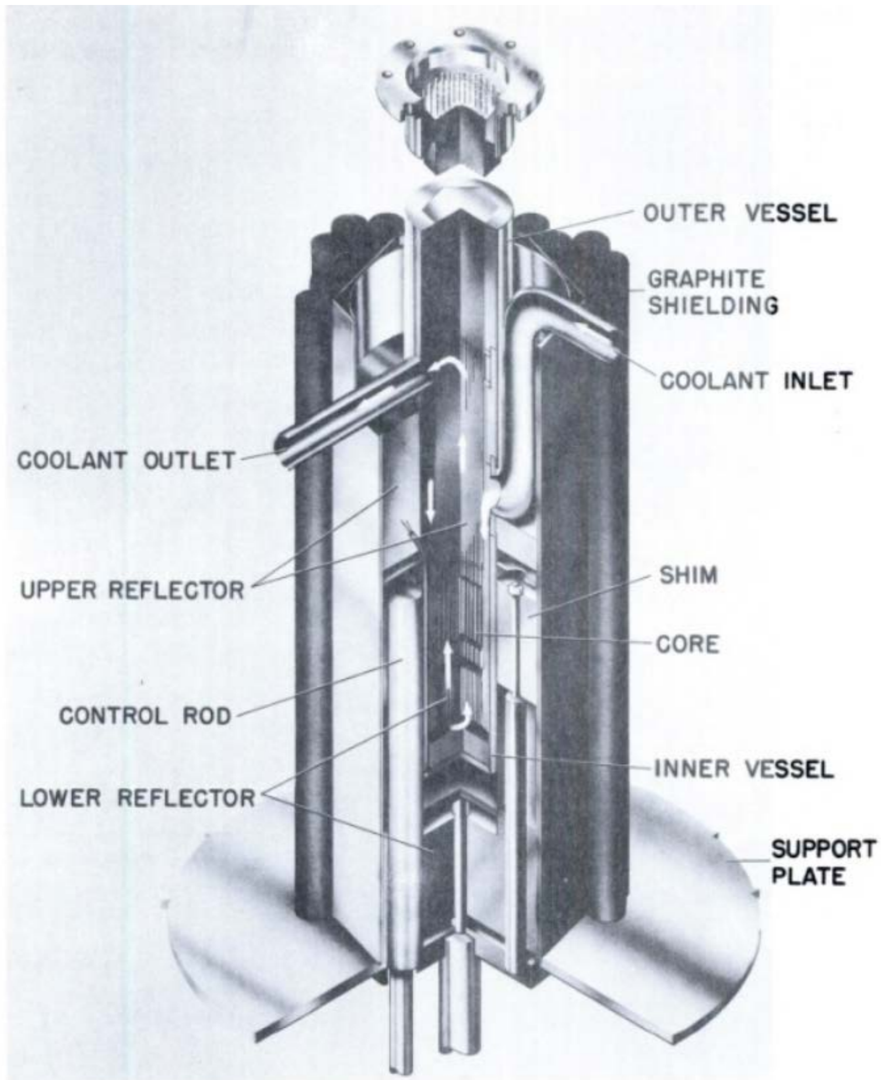


Figure 41: Cutaway view of the LAMPRE-I reactor [Swickard, 1959]

LAMPRE-I first went critical in 1961, and operated successfully for several thousand hours. The performance of the materials was found to be satisfactory (including no leakage from fuel elements after thousands of hours of high-temperature operations); thus, LAMPRE-I operations were concluded in mid-1963 [Bunker, 1983]. The LAMPRE-I sodium cooling loop was also shut down in 1963 after more than 20,000 hours, which represented the most extensive and successful test of a high-temperature sodium cooling loop that had been conducted up to that time. Although LAMPRE-I was considered to be a success, funding for the construction of

LAMPRE-II never materialized because all available resources for the R&D of fast reactors was diverted into the development of uranium oxide fuels [Bunker, 1983].

A.3. The Homogenous Reactor Program at ORNL

Although proposals were developed in 1944 and 1945 at Oak Ridge National Laboratory (ORNL) to build aqueous homogeneous reactors for research and isotope production, funding was not secured for the design and construction of such a reactor until 1949, after LOPO had demonstrated the feasibility of the Water Boiler design [Rosenthal, 2010]. Construction of the Homogeneous Reactor Experiment (HRE) was completed at ORNL in 1952.

A schematic of the HRE system is shown in Figure 42. The fuel was a solution of 93% enriched uranium as uranyl sulfate dissolved in water, and the reactor operated at 250°C and 1000 psi [Bohlmann et al., 1958]. The design power was 1000 kilowatts of heat, but a maximum of 1600 kilowatts was obtained. A pump circulated the fuel solution from the core through a heat exchanger, and the saturated steam produced in the heat exchanger powered a turbine generator. Accordingly, the HRE was the first aqueous homogeneous reactor to produce electricity and feed this electricity to the grid [Rosenthal, 2010].

The HRE was operated for 24 months and the system was dismantled when operations were concluded in 1954. During operations, maintenance tasks on the radioactive parts of the system were performed using long-handled tools, including the replacement or repair of the main circulating pump three times and the diaphragm feed pumps twice [Rosenthal, 2010]. The operation of HRE was considered to have successfully demonstrated the nuclear and chemical stability of a reactor with circulating fuel and a moderately high power density [Bohlmann et al., 1958]. However, the HRE did not demonstrate all of the engineering features of a homogeneous reactor required for continuous operation of a commercial nuclear power plant; thus, a second experimental reactor, the Homogeneous Reactor Test (HRT) was designed and constructed on the HRE site in 1956.

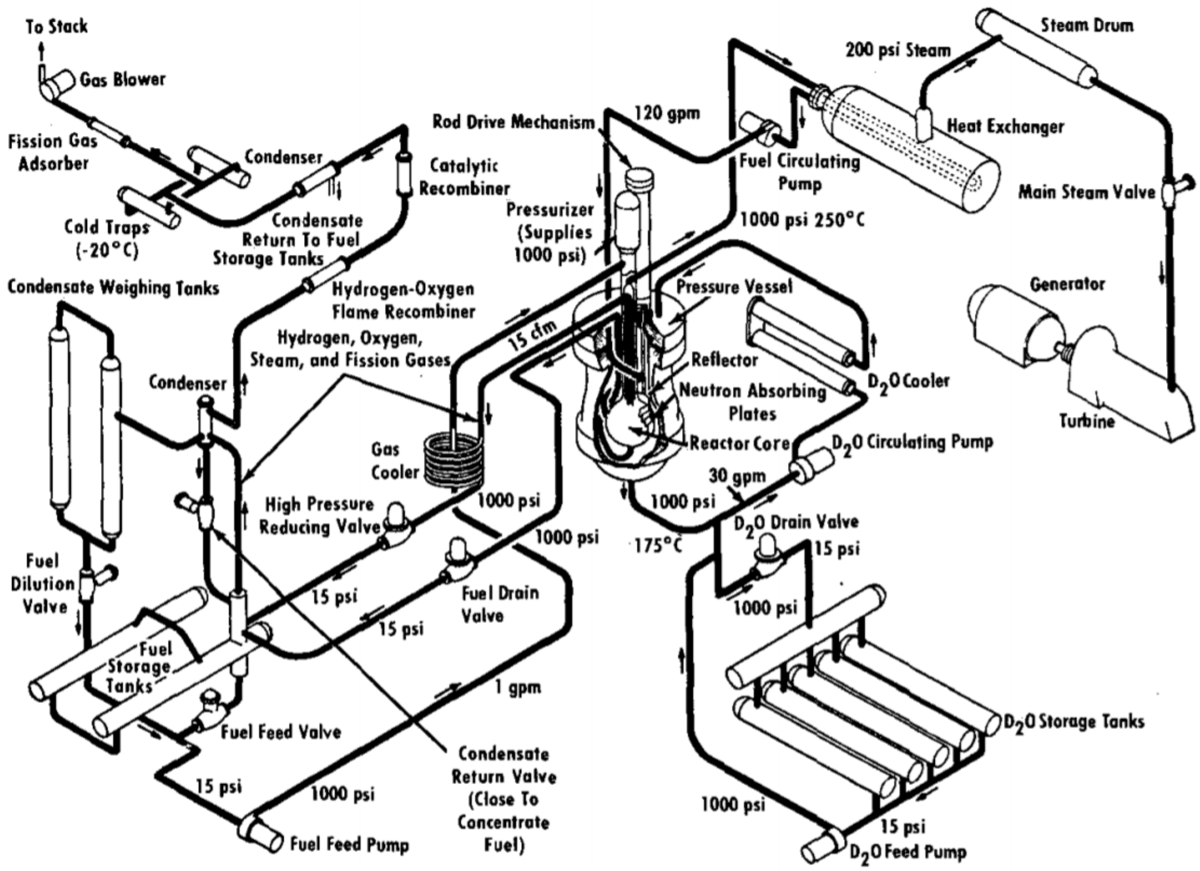


Figure 42: Schematic of HRE design [Bohlmann et al., 1958]

The HRT was intended to test: the reliability of materials and equipment for long-term continuous operation of a homogeneous reactor; remote maintenance procedures; and methods for the continuous removal of fission products and insoluble corrosion products. A schematic representation and a photograph of the HRT core vessel are displayed in Figure 42 and Figure 44, respectively. The diameter of the HRT core was nearly twice that of the HRE core; the HRT operated at a higher temperature than the HRE, and it generated four times the power [Rosenthal, 2010]. The fuel was still uranyl sulfate, but it was dissolved in D_2O (instead of ordinary light water).

The HRT went critical in 1957 and reached full-power operation at 5 megawatts in April 1958. Shortly thereafter, a crack in the core tank allowed fuel solution to leak into the D_2O blanket. After consideration of the nuclear behavior of the reactor with fuel in both the core and the blanket, operation was resumed for about 21 months until another hole developed in the vessel [Bohlmann et al., 1958; Rosenthal, 2010]. Subsequent examinations revealed that the holes were caused by the low velocity of the fuel passing through the core, which trapped solid particles in the core and led to high localized temperatures [Rosenthal, 2010].

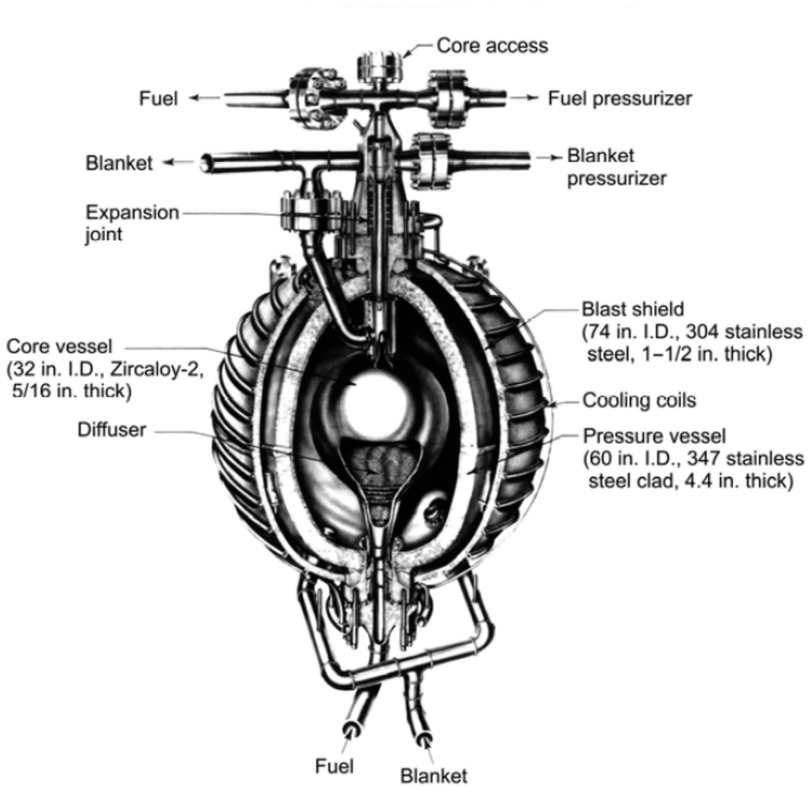


Figure 43: Cutaway view of the HRT core vessel [Rosenthal, 2010]

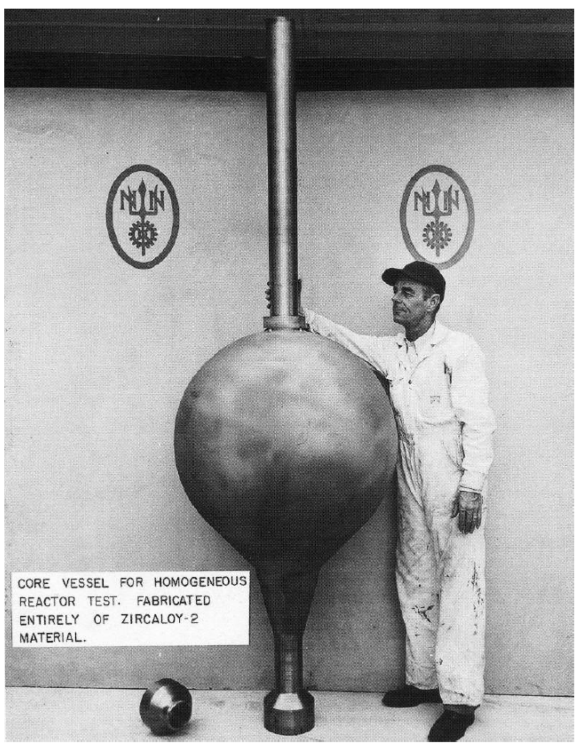


Figure 44: Photo of the HRT core vessel [Rosenthal, 2010]

The holes in the HRT were plugged to limit the leakage of fuel, and the reactor was run for an additional 4 months with no signs of fuel instability. However, when one of the plugs fell out, operation of the HRT was concluded in 1961 [Rosenthal, 2010]. The HRT had shown the feasibility of operating a circulating-fuel reactor, and the techniques and tools used to maintain the HRT provided valuable examples for other radioactive facilities, such as the MSRE. In spite of these positive outcomes, the operational challenges experienced at the HRT (including fuel instability, power excursions, and the holes in the core vessel) ultimately resulted in the conclusion of further aqueous homogenous reactor R&D at ORNL.

A.4. The Aircraft Nuclear Propulsion Program at ORNL

The Aircraft Nuclear Propulsion (ANP) program was started at ORNL in the early years of the Cold War [Rosenthal, 2010]. In the early 1950s, ORNL undertook the objective of developing an indirect cycle to power an aircraft, in which a molten metal would flow through a reactor and then through a heat exchanger, where it would heat air for a jet engine. In order to guide this development program, a small reactor, called the Aircraft Reactor Experiment (ARE) was designed. Due to concerns about the reliability of solid fuel elements at high temperatures, the ARE concept avoided the use of fuel elements by instead using a molten salt that contained a dissolved uranium compound. Ultimately, the choice of carrier salt was a mixture of sodium and zirconium fluorides, into which UF_4 was dissolved [Rosenthal, 2010].

A schematic of the ARE core is depicted in Figure 45. The fuel salt flowed through channels in a stack of hexagonal beryllium oxide blocks that served as the moderating material for the core. Helium removed heat from the salt exiting the core in a finned-tube heat exchanger, and the helium was in turn cooled by water. Heat generated in the beryllium oxide blocks was removed by a molten sodium coolant. The ARE was designed to operate at a power of 1 to 3 megawatts of heat and a fuel salt temperature of about 1300°F [Rosenthal, 2010]. Operation of the ARE began in 1954, with a plan to run the reactor for 100 MW-hours. However, this target was reached after only 9 days of operation at power. Although extending the operations of the ARE was considered, the experiment was concluded on schedule due to a concern about weakness in the fuel salt fill line. Concluding operations at this time proved to be a wise decision, as the line failed 5 days later and released radioactive gas into the reactor compartment [Rosenthal, 2010].

The US Air Force was satisfied with the performance of the ARE, and plans at ORNL were developed to construct a compact 60 megawatt Aircraft Reactor Test (ART). However, the ANP program at ORNL was terminated in March 1961 soon after John F. Kennedy became President [Rosenthal, 2010]. During its 12-year run, the ANP program greatly expanded knowledge of the chemistry and technology of molten salts, and made advances in materials, shield design, and other areas that would be fundamental to the design and operation of the MSRE.

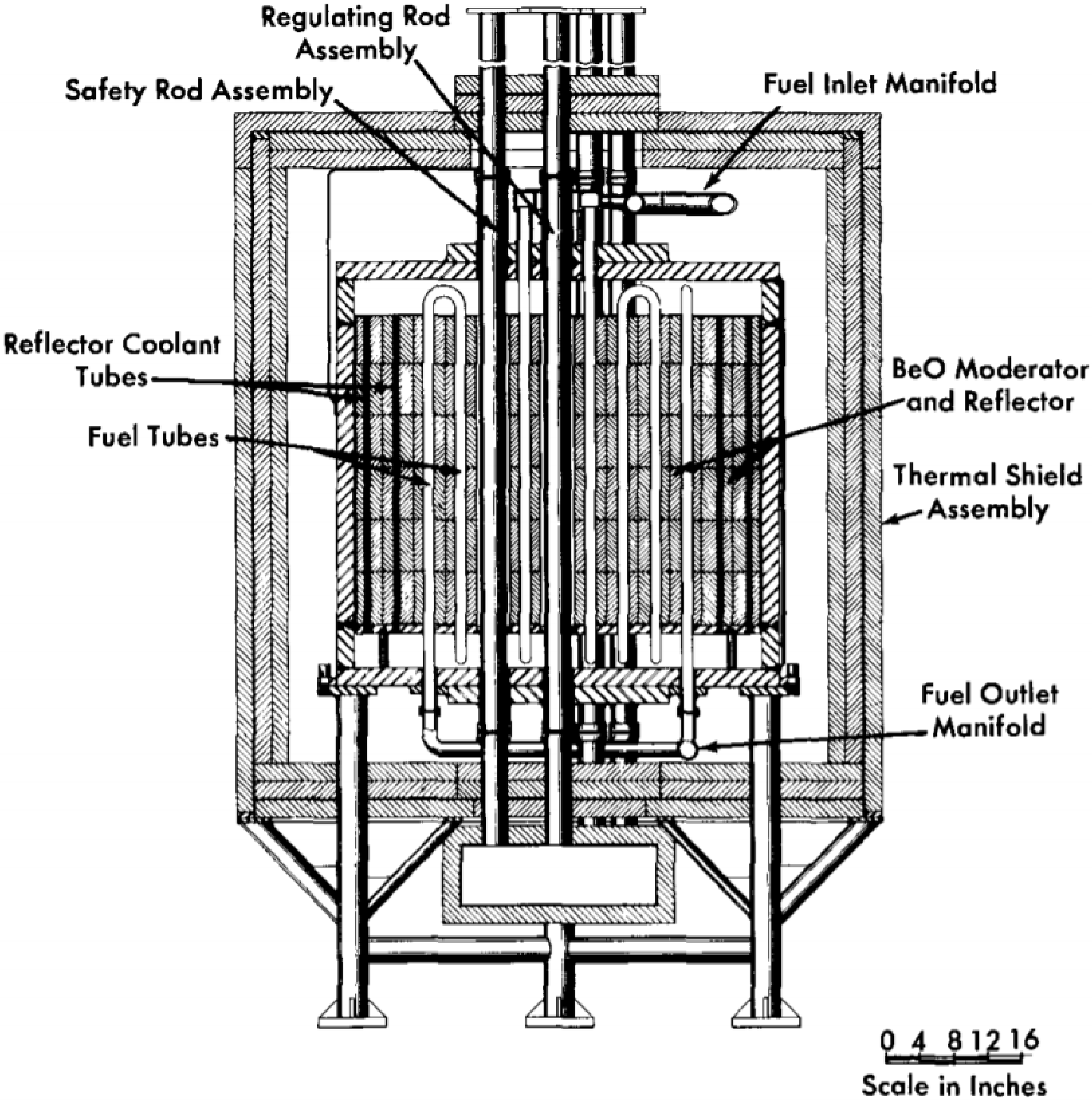


Figure 45: Elevation section of the ARE core [Rosenthal, 2010]

A.5. The Molten Salt Reactor Program at ORNL

With the ARE having shown the feasibility of a nuclear reactor running on molten salt fuel, ORNL asked the Atomic Energy Commission (AEC) for funding to study molten salt reactors for commercial power generation. However, at the time, the AEC was still funding the aqueous homogeneous reactor program and a liquid-bismuth reactor program at Brookhaven National Laboratory. A task force was created to evaluate all three fluid-fueled reactor programs, and concluded that the Molten Salt Reactor (MSR) concept "had the highest probability of achieving technical feasibility. [Rosenthal, 2010]" By the end of 1959, the AEC approved ORNL's proposal for a small reactor that would investigate the technologies needed for civilian power, called the Molten Salt Reactor Experiment (MSRE). This decision by the AEC resulted in the cancellation of ORNL's aqueous homogenous reactor program (discussed in Section A.3) and the Brookhaven Liquid Metal Fueled Reactor program.[75]

A.5.1. The Molten Salt Reactor Experiment

Design of the MSRE began in 1960 and construction started in 1962. Careful provisions were made for maintenance of the MSRE system, based on the prior HRT experience. For example, the design and layouts of components were such that they could be removed from above with long-handled tools [Rosenthal, 2010]. Construction of the MSRE was completed in 1964, and critical experiments began in 1965. The design and normal operations are discussed in detail in Chapter 4 of this dissertation. Approach to full power began in early 1966, but the reactor had to be shut down after a few hours due to plugs that developed at several points in the fuel salt off-gas system (OGS). After three months of investigating and remedying these issues, operation at full power was resumed.

Although the inventories of radioactive material discussed in Chapter 4 represented a significant majority of the total radioactivity that was in the MSRE plant, there were several other smaller distinct inventories of radioactive material. For example, around 2 TBq (55 Ci) of tritium was produced in the MSRE per day, mainly due to neutron interactions with the lithium-6 in the fuel salt), with about half of this tritium carried off in the off-gas of the fuel salt. Some of the tritium was absorbed into the core graphite, and measurable amounts diffused to the cooling air across the radiator and to the reactor cell atmosphere [Briggs, 1971]. Additionally, a heel of approximately 10% of the fuel salt volume was estimated to remain in the drain tanks after the fuel salt loop was filled [Bell, 1970], and fission, corrosion, or activation products could have plated out on or been absorbed into components with sustained contact with fuel salt. Similarly, components in the OGS could contain deposits due to condensation or the decay of volatile radionuclides into solid daughter isotopes. At any given point, there also may have been some amount of radioactive material contained in the liquid waste system in the liquid waste storage tank filters or the associated piping and pumps.

From 1966 to March 1968, the MSRE operated well with the exception of a few interruptions, including the breaking up of one of the main blowers in the heat removal system and the reoccurrence of restrictions in the off-gas lines [Guymon, 1973]. After the March 1968 shutdown,

---

[75] Although a design had been developed for a Liquid Metal Fueled Reactor Experiment (LMFRE-I) to be constructed at Brookhaven, the AEC made its decision to divert funding away from the development project before the reactor could be built [Thompson, 1963].

the uranium-235 in the fuel salt was removed by fluorination in the fuel salt processing system before uranium-233 from a production reactor was added to the salt. In October 1968, the MSRE was taken critical with the uranium-233 fuel salt. Over the next several months, the performance of the MSRE on the U-233 fuel salt was found to be quite stable, and the dynamic behavior closely matched the pre-operational predictions [Rosenthal, 2010]. Before the conclusion of MSRE operations, a small amount of plutonium was added to further demonstrate the fissile-fuel flexibility of LF-MSRs. The final run of the MSRE was terminated in December 1969, so its funds could be diverted to the development of technologies that would enable the design and construction of a commercial MSR. Interestingly, radioactive gas was released to the reactor cell from a leak in the body of a freeze valve during the final drain of the fuel salt system [Guymon, 1973; Rosenthal, 2010]. However, the overall MSRE experience had increased confidence in the performance and practicality of molten salt systems.

A.5.2. Conclusion of the MSRP at ORNL

The favorable experience gained from the MSRE led to the design of a reference commercial LF-MSR design called the Molten Salt Breeder Reactor (MSBR) that was intended to be capable of producing 1000 megawatts of electricity while simultaneously generating (i.e., "breeding)" fissile material [Serp et al., 2014]. To achieve this performance, a complex processing flowsheet was developed to achieve the difficult separation of thorium from fission products dissolved in the fuel salt. In 1972, the Joint Committee on Atomic Energy recommended that the MSR concept be appraised so that a decision could be made about the continuation of R&D and the appropriate level of funding for the MSRP [Sorenson]. A thorough review of fluoride reactor technology was undertaken to prove information for an appraisal, but a subsequent decision was made by the AEC to terminate work on MSRs. In spite of the technical success of the MSRE, the AEC was strongly committed to the development of Sodium-cooled Fast Reactors (SFRs); thus, the MSRP at ORNL was shut down in January 1973 [Rosenthal, 2010].

R&D of LF-MSRs was briefly reinstated from January 1974 to February 1976 [Sorenson]. During this period of time, efforts were focused on the preparation of a detailed plan to facilitate the development of LF-MSRs. Specific areas of emphasis included conceptual design studies and work on materials, fuel and coolant salt chemistry, fission product behavior, and development of LF-MSR components. After the successor to the AEC, the Energy Research and Development Administration, directed the termination of the MSRP in 1976, interest in MSR R&D was extremely sparse for the following three decades. The current increase in interest towards MSR designs was initiated in 2002, when the Generation IV International Forum (GIF) selected the MSR as one of the six Generation IV advanced reactor technologies [LeBlanc, 2010]; however, the MSRE operation in the late 1960s still represents the most recent (and relevant) operating experience for the modern LF-MSR design concepts.

References for Appendix A

Atomic Heritage Foundation [2017] Water Boiler Reactor. National Museum of Nuclear Science & History, Accessed 1 Feb 2020. Available at: https://www.atomicheritage.org/history/water-boiler-reactor

Bell, M.J. [1970] Calculated Radioactivity of MSRE Fuel Salt. Oak Ridge National Laboratory, ORNL-TM-2970.

Bohlmann, E.G., Kasten, P.R., Lane, J.A., McBride, J.P., Thomas, D.G., McDuffie, H.F., McNees, R.A., Segaser, C.L., and Spiewak, I. [1958] Fluid Fuel Reactors. Addison-Wesley Publishing Company, Inc., Reading, MA.

Briggs, R.B. [1971] Additional Calculations of the Distribution of Tritium in the MSRE. Oak Ridge National Laboratory, ORNL CF-71-7-8.

Bunker, M.E. [1983] Early Reactors: From Fermi's Water Boiler to Novel Power Prototypes. Los Alamos Science, Winter/Spring 1983, 124-131.

Clark, R.A. [1960] Los Alamos Power Reactor Experiment No. II: LAPRE II. Los Alamos Scientific Laboratory, Los Alamos, NM, LA-2464.

Encylopaedia Britannica [n.d.] Image: Schematic diagram of a nuclear power plant using a pressurized-water reactor. Accessed 31 Jan 2020. Available at: https://cdn.britannica.com/62/162162-050-586ADA35/diagram-nuclear-power-plant-reactor.jpg

Foro Nuclear [2018] Image: Manufacture of a fuel assembly. For de la Industria Nuclear Española, Madrid, Spain, Accessed 31 Jan 2020. Available at: https://www.foronuclear.org/images/stories/imagenes/infografias/2018/manufacture-fuel-assembly.png

Guymon, R.H. [1973] MSRE Systems and Components Performance. Oak Ridge National Laboratory, ORNL-TM-3039.

Keller, W., and Modarres, M. [2005] 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, 89, 3, 271-285.

LeBlanc, D. [2010] Molten salt reactors: A new beginning for an old idea. Nuclear Engineering and Design, 240, 6, 1644-1656.

NC State Nuclear Reactor Program [n.d.] History of the Nuclear Reactor Program. Accessed 1 Feb 2020. Available at: https://www.ne.ncsu.edu/nrp/about/history/

Rosenthal, M.W. [2010] An Account of Oak Ridge National Laboratory's Thirteen Nuclear Reactors. Oak Ridge National Laboratory, ORNL/TM-2009/181 (Rev.).

Serp, J., Allibert, M., Beneš, O., Delpech, S., Feynberg, O., Ghetta, V., Heuer, D., Holcomb, D., Ignatiev, V., Kloosterman, J.L., Luzzi, L., Merle-Lucotte, E., Uhlíř, J., Yoshioka, R., and Zhimin, D. [2014] The molten salt reactor (MSR) in generation IV: Overview and perspectives. Progress in Nuclear Energy, 77, 0, 308-319.

Sorenson, K. [n.d.] ORNL's Molten-Salt Reactor Program (1958-1976). Thorium Energy, Accessed 2 Feb 2020. Available at: https://energyfromthorium.com/msrp/

Swickard, E.O. [1959] Los Alamos Molten Plutonium Reactor Experiment (LAMPRE) Hazard Report. Los Alamos Scientific Laboratory, Los Alamos, NM, LA-2327.

Thompson, D.H. [1963] Engineering Design Considerations for a Liquid-Metal In-Pile Loop. Iowa State University of Science and Technology, Mechanical Engineering, Ph.D. Dissertation.

Waldrop, M.M. [2019] Nuclear Technology Abandoned Decades Ago Might Give Us Safer, Smaller Reactors. Kalmbach Media Co., Accessed 31 Jan 2020. Available at: https://www.discovermagazine.com/environment/nuclear-technology-abandoned-decades-ago-might-give-us-safer-smaller-reactors

APPENDIX B, HAZOP RESULTS USED TO SUPPORT MSRE ETA

Table 18: Excerpt of HAZOP study results used to help construct ET model

ENTRY #	DEVIATION	CAUSE	CONSEQUENCE	SAFETY SYSTEMS	NOTE
8	Pressure Increase	High fuel salt pump bowl cover gas pressure (e.g. regulator failure)	Increased off-gas flow through entire system (VH-1, particle trap, VH-2, charcoal bed) Increased carryover from fuel salt pump bowl Decreased residence time in VH-1, VH-2, and charcoal beds Increased pressure downstream of pump bowl	Pressure indications in fuel salt pump bowl (PT-522/592) RM-557A radiation monitors downstream of charcoal beds with automatic safety action (RM-557-A/B) Temperature indications throughout system (TE-522-1, TE-524-1, TE-556-1A)	None

ENTRY #	DEVIATION	CAUSE	CONSEQUENCE	SAFETY SYSTEMS	NOTE
16	Flow Decrease	Plugging in reactor cell holdup volume (VH-1 in Line 522)	Pressure increase in reactor pump bowl gas space Pressure increase in gas space of fuel salt overflow tank Reduced off-gas flow through rest of system (Particle Filter, VH-2, CBs) Accumulation of radioactive material in VH-1	Fuel salt pump bowl pressure indications (PT-522 and PT-592)	PCV-522 is shown on some MSRE flowsheets, but was removed during the power ascension phase [ORNL-TM-3039]

ENTRY #	DEVIATION	CAUSE	CONSEQUENCE	SAFETY SYSTEMS	NOTE
17	Flow Decrease	Plugging in charcoal cell holdup volume (VH-2 in line 522)	Pressure increase in VH-1 Pressure increase in reactor pump bowl gas space Pressure increase in gas space of fuel salt overflow tank Reduced off-gas flow through charcoal beds Accumulation of radioactive material in VH-2	Fuel salt pump bowl pressure indications (PT-522 and PT-592) Temperature indication upstream of charcoal cell holdup volume (TE-522-1)	This pressure increase might be slower than the increase due to plugging in VH-1 [ORNL-TM-3039] Methods to clear plugs included: - acetone wash for valve - excess helium (forward blow) - helium back blow - targeted heating - mechanical cleaning

ENTRY #	DEVIATION	CAUSE	CONSEQUENCE	SAFETY SYSTEMS	NOTE
18	Flow Decrease	Plugging in particle trap	Pressure increase in VH-1 Pressure increase in reactor pump bowl gas space Pressure increase in gas space of fuel salt overflow tank Reduced off-gas flow through VH-2 and charcoal beds Accumulation of radioactive material in particle trap	Fuel salt pump bowl pressure indications (PT-522 and PT-592) Temperature indications in particle trap (TE-PT-2YM/2FM/2FF)	None
21	Flow No	Spurious closure of automatically operated valves (e.g. HCV-557C)	Reduced off-gas flow to filters/stack Increased pressure upstream of valve (charcoal beds, VH-2, VH-1, particle trap, fuel salt pump bowl gas space) Reduced helium demand from cover gas system to fuel salt pump bowl	Fuel salt pump bowl pressure indications (PT-522 and PT-592) Cover gas system pressure control and indication (FCV-516, FI-516B) Rupture disks and backflow preventers in cover gas system	Block valve position is indicated on the main control board [ORNL-TM-729B]

ENTRY #	DEVIATION	CAUSE	CONSEQUENCE	SAFETY SYSTEMS	NOTE
22	Flow No	Spurious closure of manually operated valves (e.g. V557B, V562C, V620-V627, V522A, V522B)	Reduced off-gas flow to filters/stack Increased pressure upstream of valve Reduced helium demand from cover gas system to fuel salt pump bowl	Fuel salt pump bowl pressure indications (PT-522 and PT-592) Cover gas system pressure control and indication (FCV-516, FI-516B) Rupture disks and backflow preventers in cover gas system	It is unclear if these valves have any design specific failures that are different than typical manual valves. During startup of the off-gas and cover gas systems, operators performed a checklist that required tagging these valves closed [ORNL-TM-908, V2]
23	Flow As well as	Increased fuel salt carry over into off-gas line (e.g. lines 522 or 523)	Blockage of off-gas lines See blockage deviations evaluated as "flow decreases"	Level indication in fuel salt pump bowl with associated high level trip (LT-593-C, LT-596-B) Fuel salt pump bowl pressure indications (PT-522 and PT-592)	None

ENTRY #	DEVIATION	CAUSE	CONSEQUENCE	SAFETY SYSTEMS	NOTE
24	Flow As well as	Oil contamination of off-gas from fuel salt pump bowl	Possibility for undesirable reactions (e.g. radio-polymerization of oil leading to deposits in off-gas line)	Fuel salt pump bowl pressure indications (PT-522 and PT-592) Procedures to clean off-gas line (blow down, heat up, ream)	Discussed in ORNL-TM-3039 section 8
28	Flow obstruction in charcoal bed (e.g. plugging, compaction)	Reduction in gas flow through charcoal beds Asymmetry of flow through parallel beds Increased back-pressure in upstream OGS components	Pressure drop indication across charcoal beds (PDT-556A) Radiation monitors downstream of beds tied automatic control action (RE-557-A/B) Gas flow can be switched to aux charcoal bed Thermocouples are installed at three locations on each of the main charcoal beds (one thermocouple on aux charcoal bed)	No additional actions identified at this time	None

ENTRY #	DEVIATION	CAUSE	CONSEQUENCE	SAFETY SYSTEMS	NOTE
33	Rad. Inventory Increase	Increased deposition of fission/corrosioN/Activation products in particle filter	Eventual blockage of component Accumulation of radioactive material for potential release Accumulation of fissile material could produce criticality in component	Temperature indications in particle trap (TE-PT-2YM/2FM/2FF) Fuel salt pump bowl pressure indications (PT-522 and PT-592)	None
35	Rad. Inventory Decrease	Leak of off-gas out of system pressure boundary	Release of radioactive material to surrounding area (e.g. reactor cell atmosphere, charcoal bed cell, vent house) Contamination of CCS, see entry 72	See entry 72 Stack radiation monitors (RM-S1A/B/C) Ventilation filters for particulates	None

ENTRY #	DEVIATION	CAUSE	CONSEQUENCE	SAFETY SYSTEMS	NOTE
72	Rad. Inventory Increase	High radioactivity in reactor cell atmosphere (e.g. fuel salt leak)	Increased radioactivity of cell evacuation effluent to stack Potential for increased activity of CCP condensate (and sump discharge) Potential for accumulation of activity in CCP discharge strainer	Cell exhaust radiation indications with automatic safety actions (RM-565-B/C) Stack radiation monitors and alarms (RM-S1A/B/C) CCP condensate is discharged to liquid waste handling system CCP strainer material decontaminated prior to disposal (as LLW)	None

APPENDIX C, QUALITY ASSURANCE CONSIDERATIONS FOR THE MSRE HAZOP STUDIES

It is imaginable that regulators and independent oversight could feel an obligation to find a way to validate the results of a PHA study, especially if they are used as the foundation for a design-specific RIPB safety case.

A HAZOP study can be difficult to independently review in the same way that a radiation dose or chemical exposure calculation can be. The idea behind the PHA approach is that some systems are too large and complex to be fully understood from all technical aspects by one expert. Therefore, a group of experts is called upon to collectively provide the necessary expertise. It then follows that the validity and completeness of the process depends heavily on the participants to collectively provide technical expertise of sufficient breadth and depth. According to the Non-LWR PRA Standard [ASME/ANS, 2013], the peer review process for the PRA model of a nuclear reactor design should be commensurate with the model's complexity and importance to safety. The US DOE [2013] requires that this peer review process be documented in a PRA plan. The PRA plan should identify whether peer reviews will be conducted at intermediate stages during development and conduct of the PRA. The scope of peer review may range from a single subject matter expert to a formal external review, depending on the scope, complexity and intended use of the PRA. Short of replicating a PHA team with an independent set of qualified participants, a complete independent/peer review of a HAZOP study is not practical. There are ways, however, to validate the quality of the process and thus, by construction, the validity of the technical conclusions.

Although the MSRE exercise presented in this dissertation is only intended to serve as a demonstration of a technology-inclusive methodology to evaluate risks in an early stage advanced nuclear reactor design, a review plan was developed to guide the efforts to assure quality in the process. The plan included:

- Since the quality of a HAZOP study depends heavily upon the expertise of the participants, the team member qualifications were reviewed for completeness. See Section C.1 for brief resumes for the members of the MSRE HAZOP study team.
- A HAZOP Study Plan that includes tools such as checklists to document that good practices have been followed in the preparation and conduct of the study. This way, studies were performed in a consistent manner with practices that have been properly vetted through the planning and approval process. A HAZOP study that is governed by a plan can be reviewed for process compliance.
- A HAZOP Study procedure that described expectations for:

    - Engineering documentation for systems
    - Selection of HAZOP study participants and documentation of qualifications
    - Documentation of results
- An independent expert on the system being analyzed and an independent expert on risk analysis were utilized to review the technical background materials and the HAZOP results for technical rigor and consistency. These expert reviewers were present for portions of the studies.

References for Appendix C

American Society of Mechanical Engineers (ASME) and American Nuclear Society (ANS) [2013] Standard for Probabilistic Risk Assessment for Advanced Non-LWR Nuclear Power Plant Applications. ASME/ANS RA S-1.4-2013.

US Department of Energy (DOE) [2013] DOE Standard on Development of Probabilistic Risk Assessments for Nuclear Safety Applications. Washington, DC, DOE-STD-1628-2013.

C.1. Resumes of MSRE HAZOP Team Members (from [EPRI, 2018])

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).

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)

"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.
- 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.

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.

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.

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.

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. Co author of PRA procedures developed for use in former Soviet Union and Eastern European countries. 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 economic model for the Sequoyah Nuclear Plant, among others.

Johnson, cont.

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.

APPENDIX D, FAULT TREE MODELS AND BASIC EVENT DATA USED TO ESTIMATE FAILURE RATES FOR FV-103

D.1. Fault Tree and Basic Event Data for Spurious Thawing of FV-103

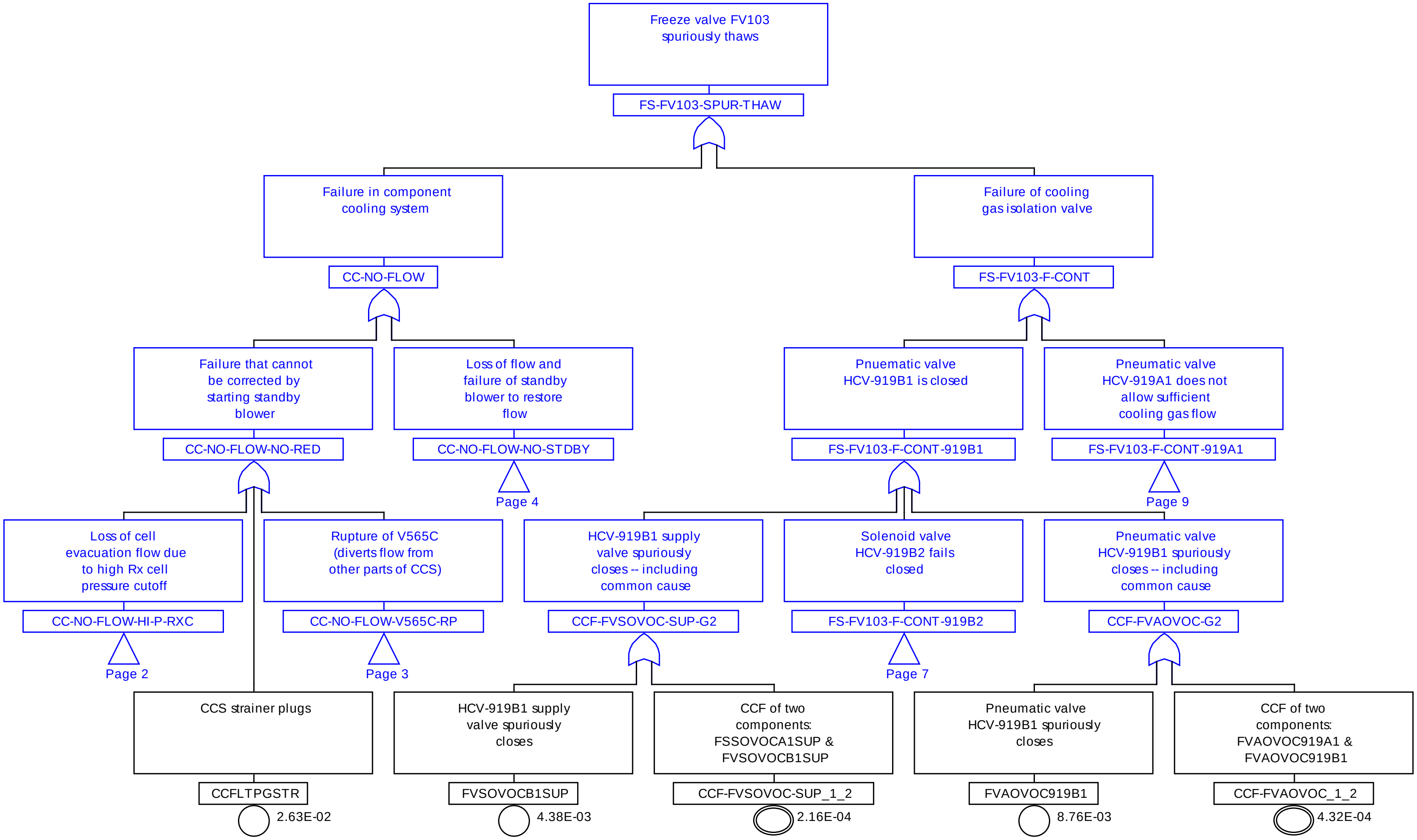


Figure 46: Fault tree for spurious thaw of FV-103 (Page 1 of 12)

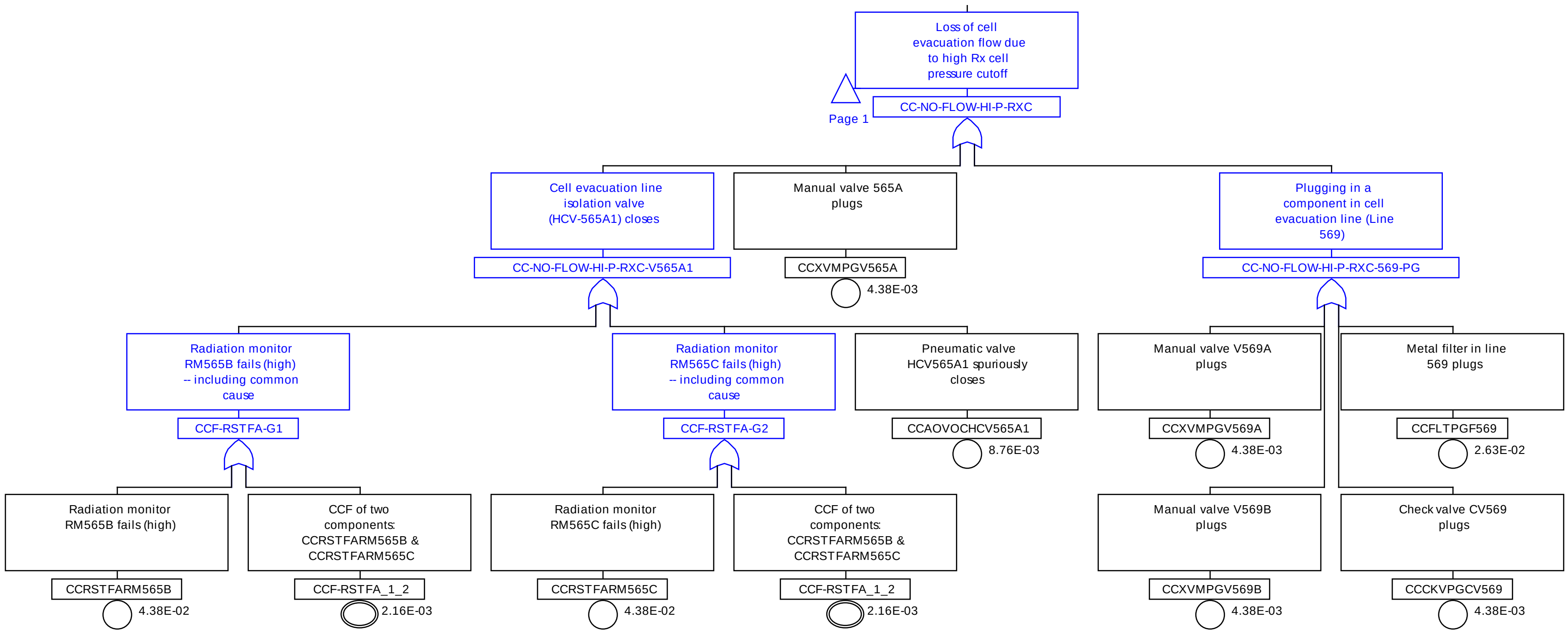


Figure 47: Fault tree for spurious thaw of FV-103 (Page 2 of 12)

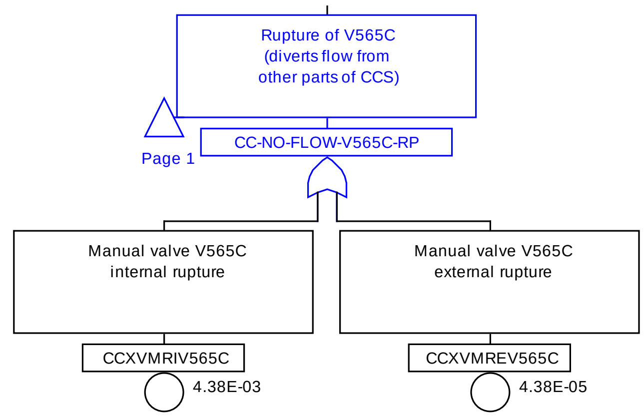


Figure 48: Fault tree for spurious thaw of FV-103 (Page 3 of 12)

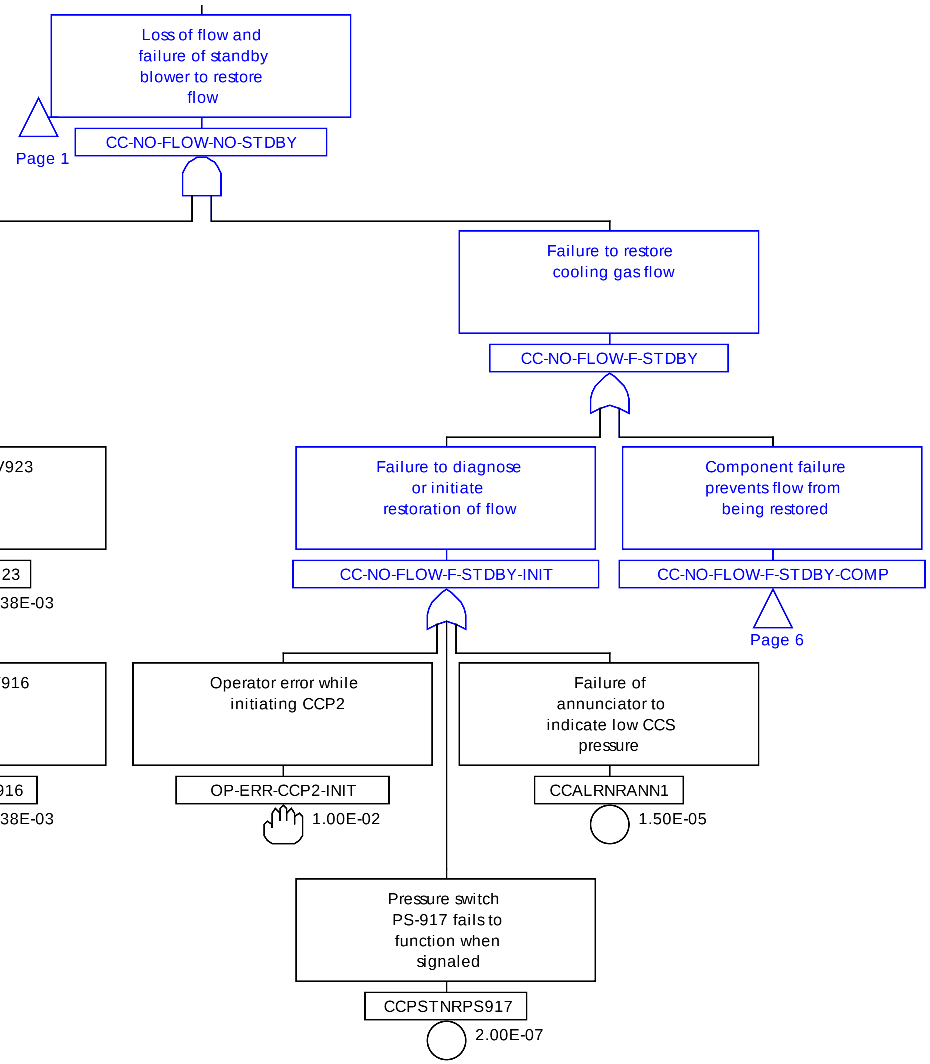


Figure 49: Fault tree for spurious thaw of FV-103 (Page 4 of 12)

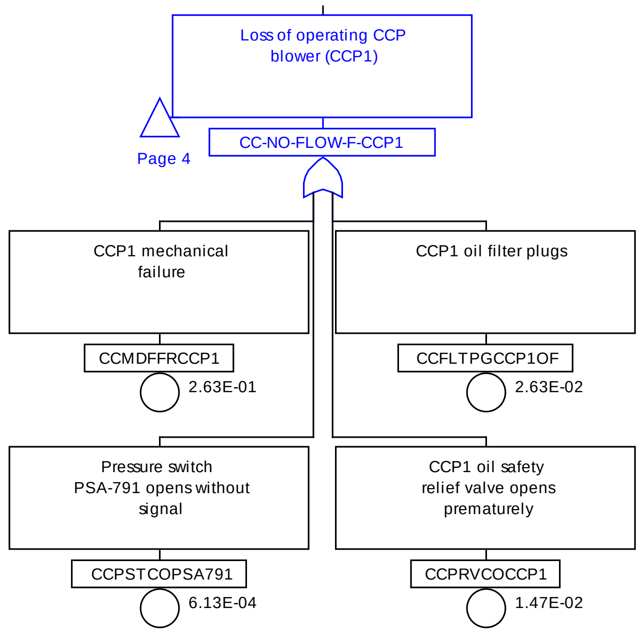


Figure 50: Fault tree for spurious thaw of FV-103 (Page 5 of 12)

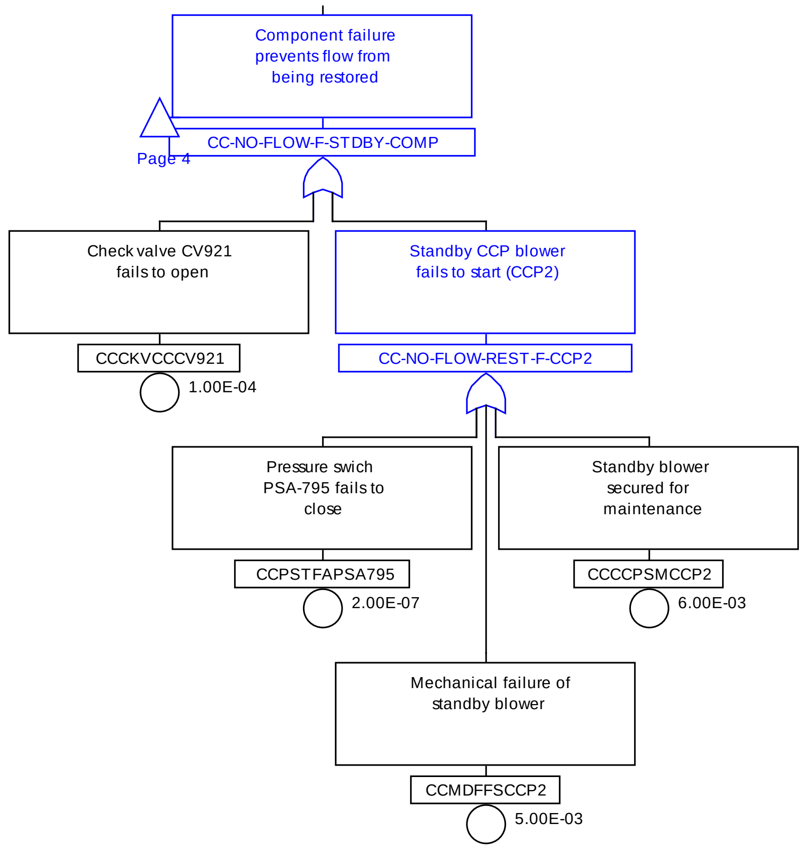


Figure 51: Fault tree for spurious thaw of FV-103 (Page 6 of 12)

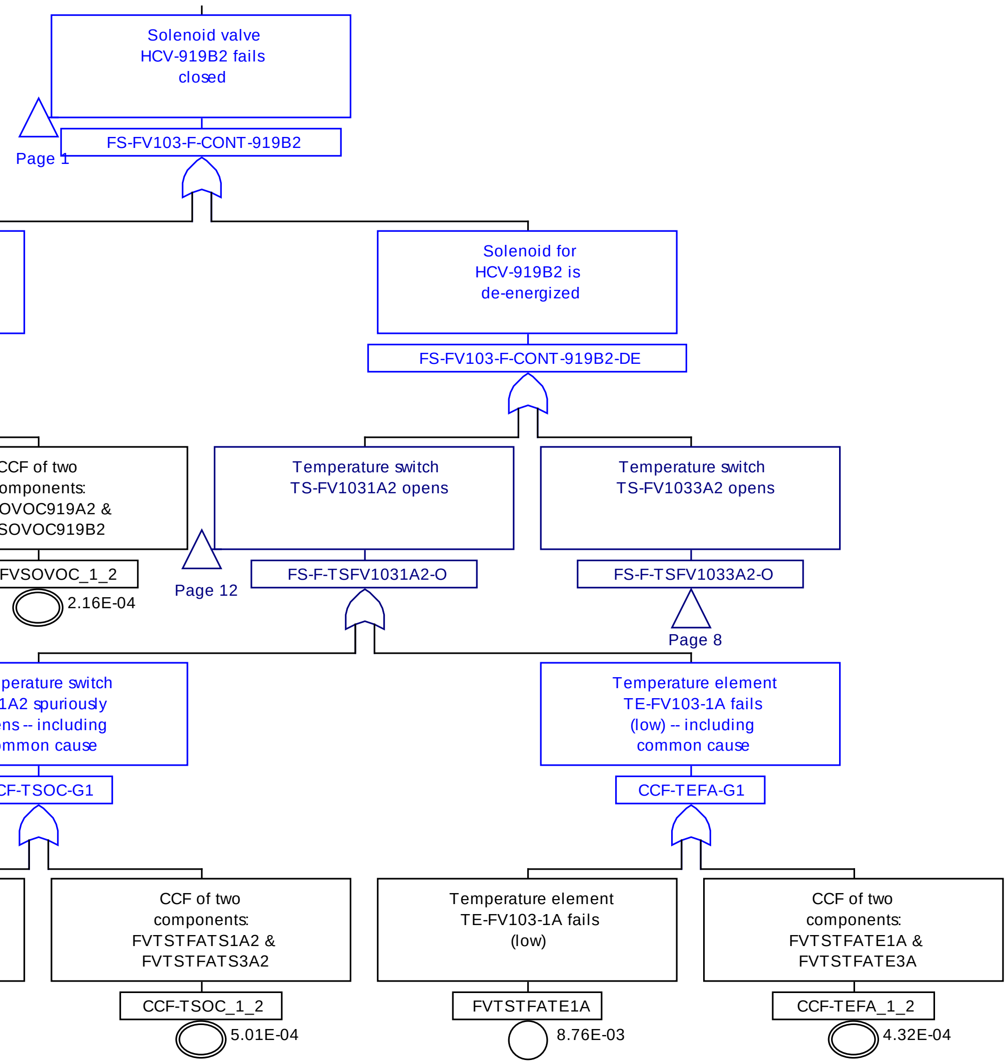


Figure 52: Fault tree for spurious thaw of FV-103 (Page 7 of 12)

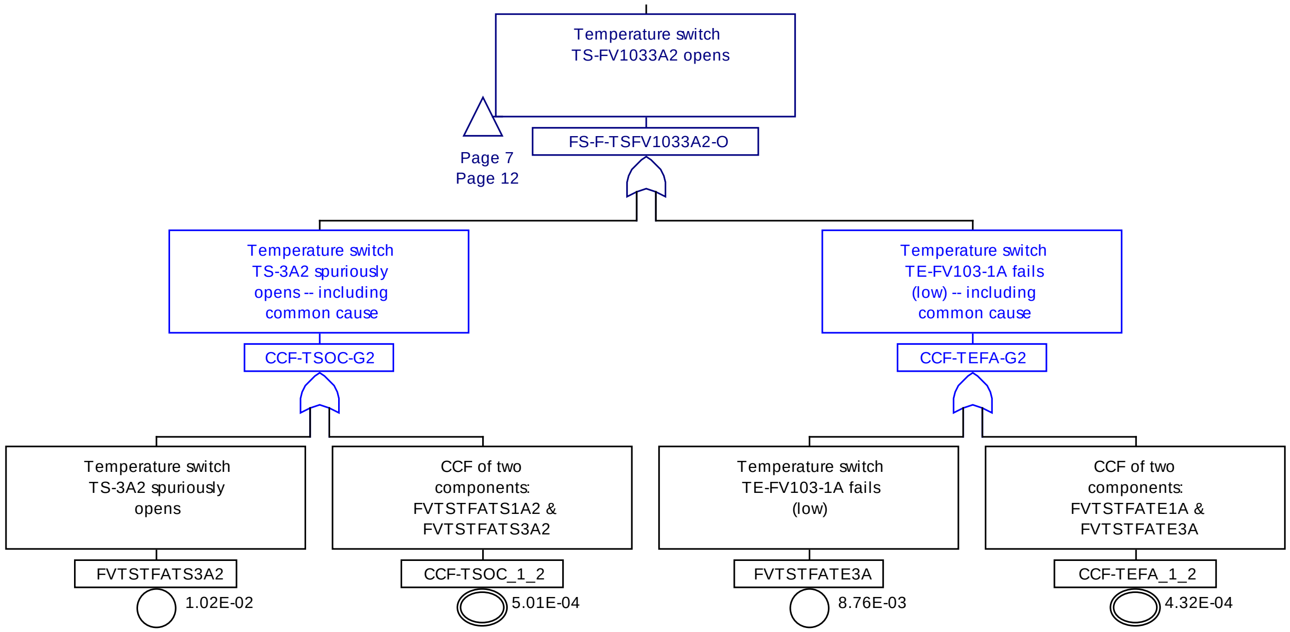


Figure 53: Fault tree for spurious thaw of FV-103 (Page 8 of 12)

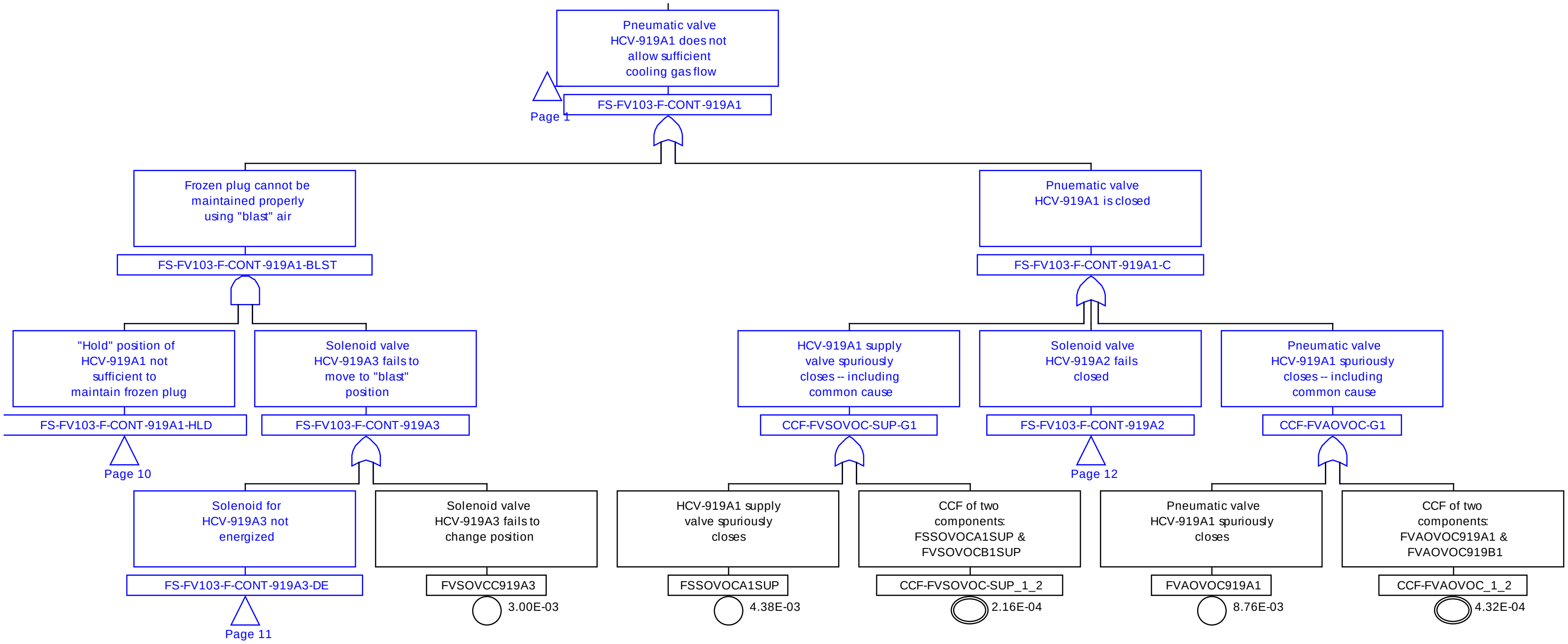


Figure 54: Fault tree for spurious thaw of FV-103 (Page 9 of 12)

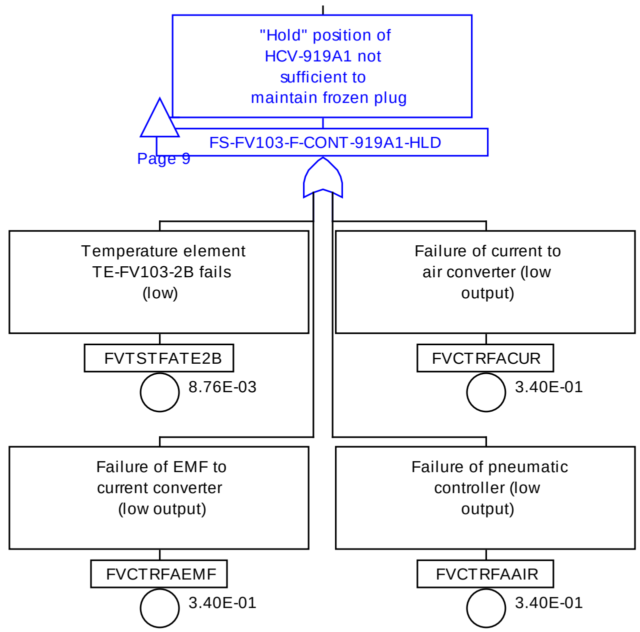


Figure 55: Fault tree for spurious thaw of FV-103 (Page 10 of 12)

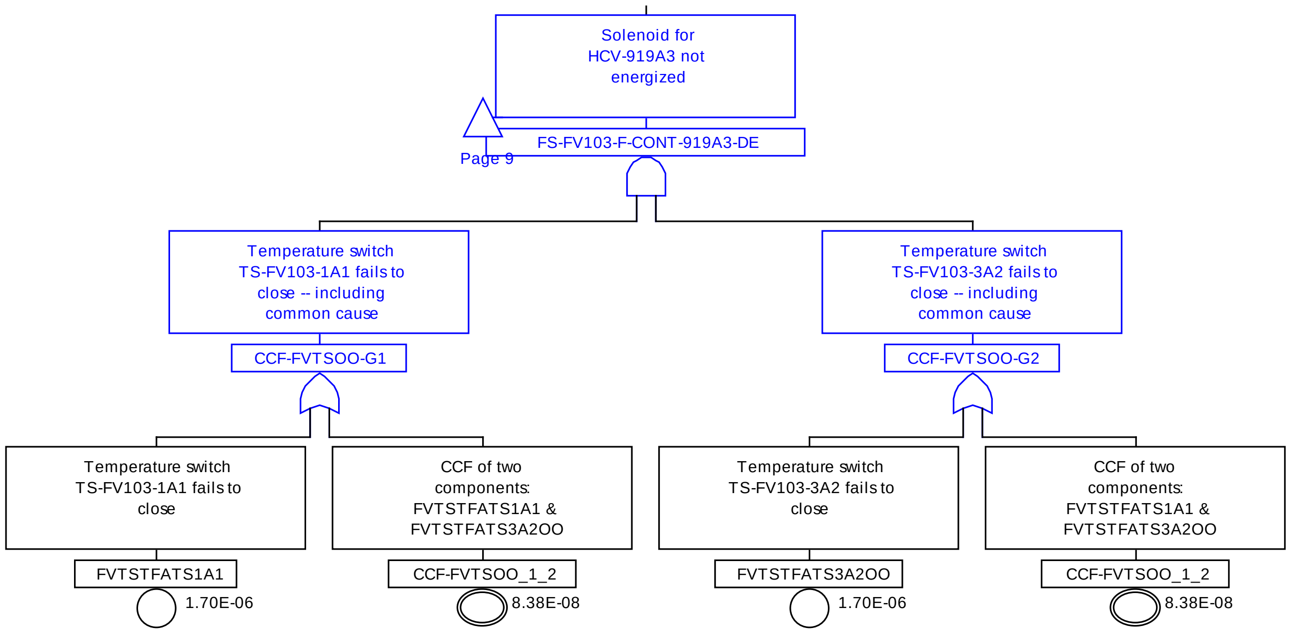


Figure 56: Fault tree for spurious thaw of FV-103 (Page 11 of 12)

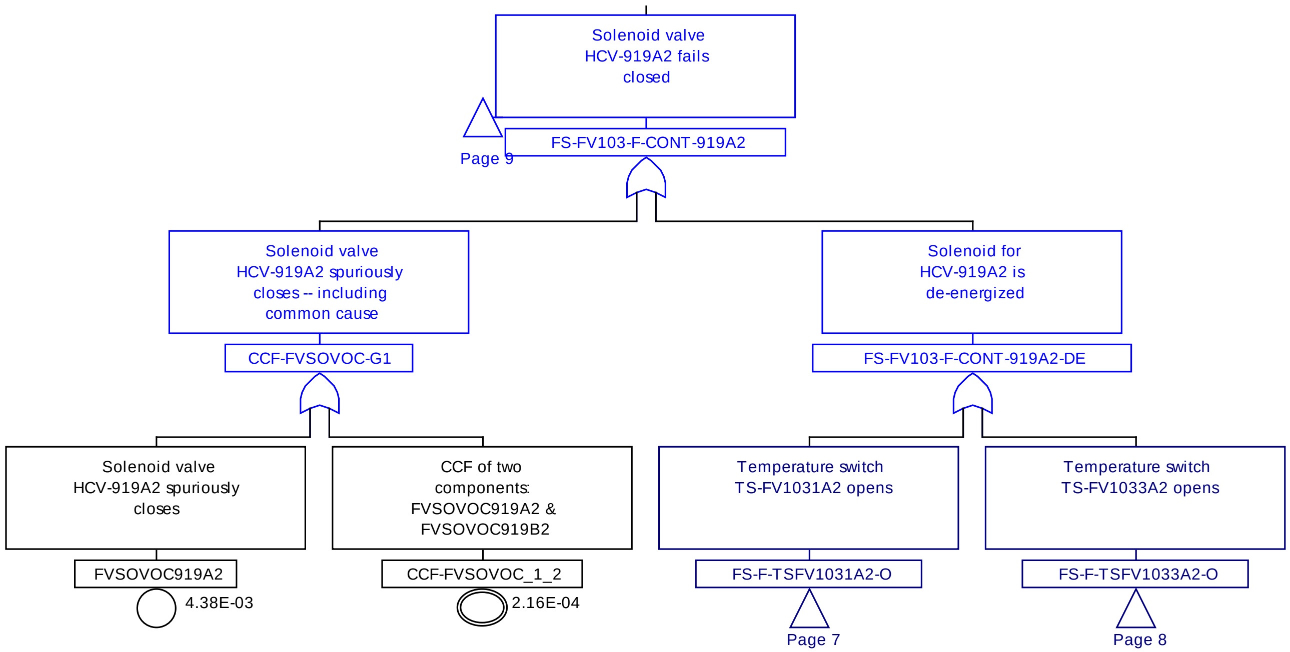


Figure 57: Fault tree for spurious thaw of FV-103 (Page 12 of 12)

Table 19: Basic event data used in fault tree for spurious thaw of FV-103

Event Name	Component Type	Failure Mode	Failure Rate	Units	Multiplier	Error Factor	Source	Source Identifier	Notes
CCRSTFARM565B	Radiation Monitor	Failure	5.00E-06	/hour	8760 hours	5	[Blanchard and Roy, 1998]	RST-FA-I	CCF group: CCF-RSTFA
CCRSTFARM565C	Radiation Monitor	Failure	5.00E-06	/hour	8760 hours	5	[Blanchard and Roy, 1998]	RST-FA-I	CCF group: CCF-RSTFA
CCAOVOCHCV565A1	Pnuematic Valve	Spurious Operation	1.00E-06	/hour	8760 hours	10	[Blanchard and Roy, 1998]	AOV-OC-G	
CCXVMPGV565A	Manual Valve	Plugs	5.00E-07	/hour	8760 hours	10	[Blanchard and Roy, 1998]	XVM-PG-G	
CCFLTPGSTR	Filter	Plugs	3.00E-06	/hour	8760 hours	10	[Blanchard and Roy, 1998]	FLT-PG-G	
CCXVMPGV569A	Manual Valve	Plugs	5.00E-07	/hour	8760 hours	10	[Blanchard and Roy, 1998]	XVM-PG-G	
CCXVMPGV569B	Manual Valve	Plugs	5.00E-07	/hour	8760 hours	10	[Blanchard and Roy, 1998]	XVM-PG-G	
CCFLTPGF569	Filter	Plugs	3.00E-06	/hour	8760 hours	10	[Blanchard and Roy, 1998]	FLT-PG-G	
CCCKVPGCV569	Check Valve	Plugs	5.00E-07	/hour	8760 hours	10	[Blanchard and Roy, 1998]	CKV-PG-G	
CCXVMRIV565C	Manual Valve	Internal Rupture	5.00E-07	/hour	8760 hours	10	[Blanchard and Roy, 1998]	XVM-RI-G	

Event Name	Component Type	Failure Mode	Failure Rate	Units	Multiplier	Error Factor	Source	Source Identifier	Notes
CCXVMREV565C	Manual Valve	External Rupture	5.00E-09	/hour	8760 hours	10	[Blanchard and Roy, 1998]	XVM-RE-G	
CCMDFFRCCP1	Motor Driven Blower	Fails to Run	3.00E-05	/hour	8760 hours	3	[Blanchard and Roy, 1998]	MDF-FR-H	
CCPSTCOPSA791	Electric Pressure Switch	Opens without Signal	7.00E-08	/hour	8760 hours	5	[CCPS, 1989]	2.1.4.1.3	
CCFLTPGCCP1OF	Filter	Plugs	3.00E-06	/hour	8760 hours	10	[Blanchard and Roy, 1998]	FLT-PG-C	Assumed to be similar to chemical process system filter
CCPRVCOCCP1	Safety Relief Valve	Opens Prematurely	1.68E-06	/hour	8760 hours	3	[CCPS, 1989]	4.3.3.2	
CCXVMPGV916	Manual Valve	Plugs	5.00E-07	/hour	8760 hours	10	[Blanchard and Roy, 1998]	XVM-PG-G	
CCXVMPGV923	Manual Valve	Plugs	5.00E-07	/hour	8760 hours	10	[Blanchard and Roy, 1998]	XVM-PG-G	
CCCKVPGCV916	Check Valve	Plugs	5.00E-07	/hour	8760 hours	10	[Blanchard and Roy, 1998]	CKV-PG-G	
OP-ERR-CCP2-INIT	Operator Error	Failure to Initiate Standby CCP Blower	1.00E-02	/demand	1 demand	5	[Benhardt et al., 1994]	3.6.2.3 (Nominal Mean Value)	Assumed to be similar to "Failure to Respond to Compelling Signal"

Event Name	Component Type	Failure Mode	Failure Rate	Units	Multiplier	Error Factor	Source	Source Identifier	Notes
CCPSTNRPS917	Electric Pressure Switch	Fails to Function when Signaled	4.00E-07	/hour	0.5 hours	5	[CCPS, 1989]	2.1.4.1.3	FV-103 assumed to begin thawing within 30 minutes of low cooling gas flow
CCALRNRANN1	Annunciator	Fails to Alarm	3.00E-05	/hour	0.5 hours	10	[Blanchard and Roy, 1998]	ALR-NR-I	FV-103 assumed to begin thawing within 30 minutes of low cooling gas flow
CCCKVCCCV921	Check Valve	Fails to Open	1.00E-04	/demand	1 demand	10	[Blanchard and Roy, 1998]	CKV-CC-G	
CCPSTFAPSA795	Electric Pressure Switch	Fails to Function when Signaled	4.00E-07	/hour	0.5 hours	5	[CCPS, 1989]	2.1.4.1.3	FV-103 assumed to begin thawing within 30 minutes of low cooling gas flow
CCMDFFSCCP2	Motor Driven Blower	Fails to Start	5.00E-03	/demand	1 demand	5	[Blanchard and Roy, 1998]	MDF-FS-H	

Event Name	Component Type	Failure Mode	Failure Rate	Units	Multiplier	Error Factor	Source	Source Identifier	Notes
CCCCPSMCCP2	Motor Driven Blower	Standby Blower Secured for Maintenance	6.00E-03	/demand	1 demand	10	[Guymon, 1973]	Table 4-5	Probability based on 3 days of CCP maintenance over 468 day period
FVSOVOCB1SUP	Solenoid Valve	Spurious Operation	5.00E-07	/hour	8760 hours	10	[Blanchard and Roy, 1998]	SOV-OC-G	CCF group: CCF-FVSOVOC-SUP
FVSOVOC919B2	Solenoid Valve	Spurious Operation	5.00E-07	/hour	8760 hours	10	[Blanchard and Roy, 1998]	SOV-OC-G	CCF group: CCF-FVSOVOC
FVAOVOC919B1	Pnuematic Valve	Spurious Operation	1.00E-06	/hour	8760 hours	10	[Blanchard and Roy, 1998]	AOV-OC-G	CCF group: CCF-FVAOVOC
FVTSTFATS1A2	Electric Temperature Switch	Functioned without Signal	1.16E-06	/hour	8760 hours	5	[CCPS, 1989]	2.1.4.1.4	CCF group: CCF-TSOC
FVTSTFATE1A	Temperature Element	Failure	1.00E-06	/hour	8760 hours	3	[Blanchard and Roy, 1998]	TST-FA-I	CCF group: CCF-TEFA
FVTSTFATS3A2	Electric Temperature Switch	Functioned without Signal	1.16E-06	/hour	8760 hours	5	[CCPS, 1989]	2.1.4.1.4	CCF group: CCF-TSOC
FVTSTFATE3A	Temperature Element	Failure	1.00E-06	/hour	8760 hours	3	[Blanchard and Roy, 1998]	TST-FA-I	CCF group: CCF-TEFA
FVTSTFATE2B	Temperature Element	Failure	1.00E-06	/hour	8760 hours	3	[Blanchard and Roy, 1998]	TST-FA-I	

Event Name	Component Type	Failure Mode	Failure Rate	Units	Multiplier	Error Factor	Source	Source Identifier	Notes
FVCTRFAEMF	EMF to Current Converter	Failure (low output)	6.88E-05	/hour	8760 hours	5	[CCPS, 1989]	2.2.1	Assumed to be similar to controller
FVCTRFACUR	Current to Air Converter	Failure (low output)	6.88E-05	/hour	8760 hours	5	[CCPS, 1989]	2.2.1	Assumed to be similar to controller
FVCTRFAAIR	Pnuematic Controller	Failure (low output)	6.88E-05	/hour	8760 hours	5	[CCPS, 1989]	2.2.1	Assumed to be similar to controller
FVTSTFATS1A1	Electric Temperature Switch	Failed to Function when Signaled	3.40E-06	/hour	8760 hours	5	[CCPS, 1989]	2.1.4.1.4	CCF group: CCF-FVTSOO
FVTSTFATS3A2OO	Electric Temperature Switch	Failed to Function when Signaled	3.40E-06	/hour	8760 hours	5	[CCPS, 1989]	2.1.4.1.4	CCF group: CCF-FVTSOO
FVSOVCC919A3	Solenoid Valve	Fails to Change Position	3.00E-03	/demand	1 demand	10	[Blanchard and Roy, 1998]	SOV-OO-G	
FSSOVOCA1SUP	Solenoid Valve	Spurious Operation	5.00E-07	/hour	8760 hours	10	[Blanchard and Roy, 1998]	SOV-OC-G	CCF group: CCF-FVSOVOC-SUP
FVSOVOC919A2	Solenoid Valve	Spurious Operation	5.00E-07	/hour	8760 hours	10	[Blanchard and Roy, 1998]	SOV-OC-G	CCF group: CCF-FVSOVOC
FVAOVOC919A1	Pnuematic Valve	Spurious Operation	1.00E-06	/hour	8760 hours	10	[Blanchard and Roy, 1998]	AOV-OC-G	CCF group: CCF-FVAOVOC

D.2. Fault Tree and Basic Event Data for Failure of FV-103 to Thaw on Demand

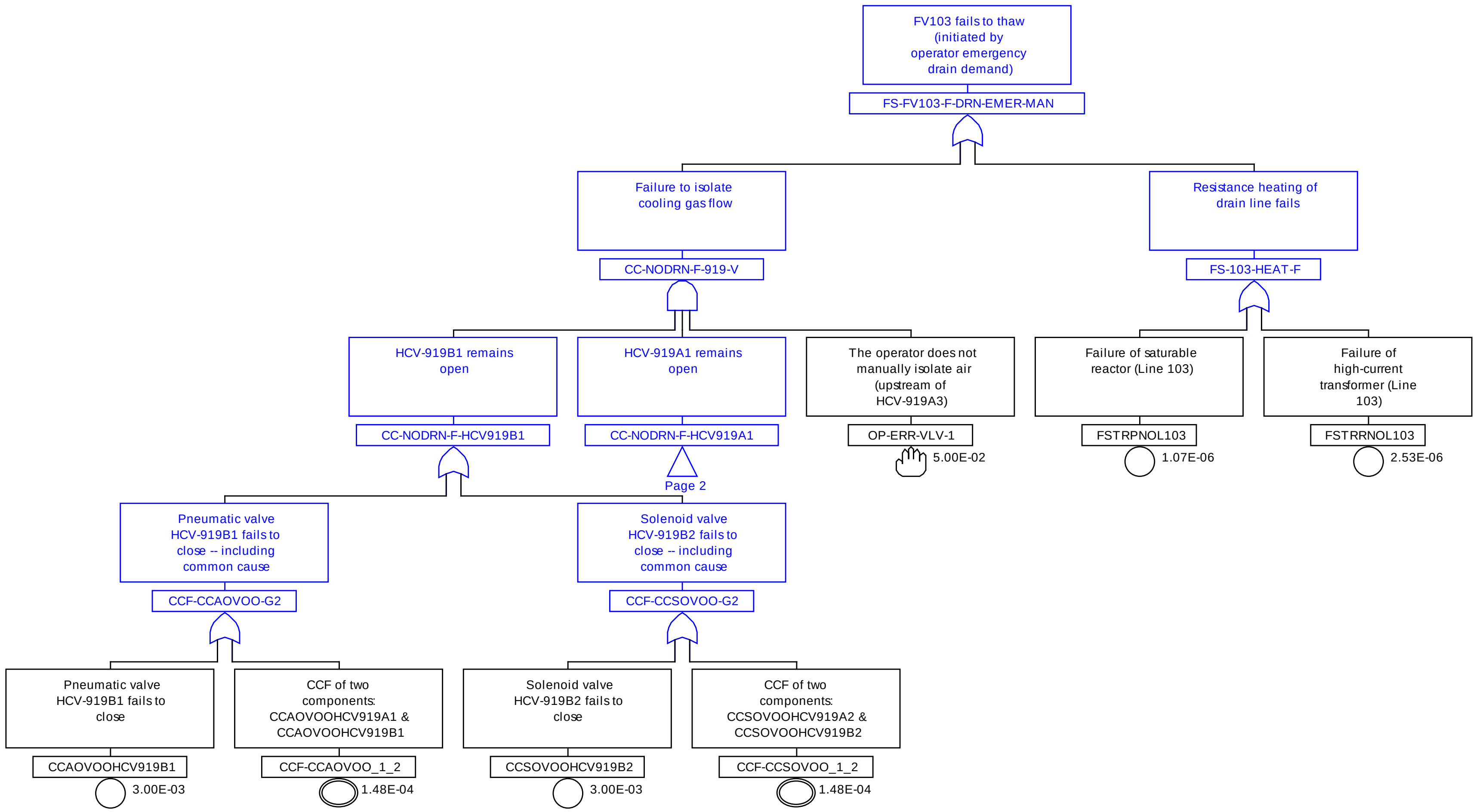


Figure 58: Fault tree for failure of FV-103 to thaw on demand (Page 1 of 2)

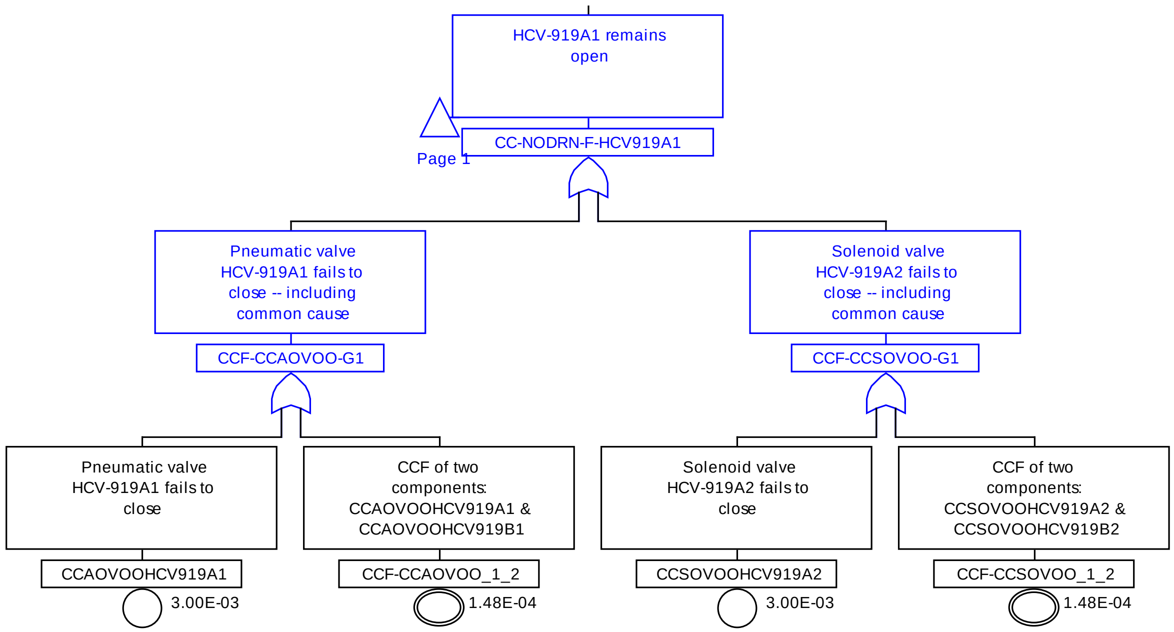


Figure 59: Fault tree for failure of FV-103 to thaw on demand (Page 2 of 2)

Table 20: Basic event data used in fault tree for failure of FV-103 to thaw on demand

Event Name	Component Type	Failure Mode	Failure Rate	Units	Error Factor	Source	Source Identifier	Notes
CCAOVOOHCV919B1	Pneumatic Valve	Fails to Close	3.00E-03	/demand	10	[Blanchard and Roy, 1998]	AOV-OO-G	CCF group: CCF-CCAOVOO
CCSOVOOHCV919B2	Solenoid Valve	Fails to Close	3.00E-03	/demand	10	[Blanchard and Roy, 1998]	SOV-OO-G	CCF group: CCF-CCSOVOO
CCAOVOOHCV919A1	Pneumatic Valve	Fails to Close	3.00E-03	/demand	10	[Blanchard and Roy, 1998]	AOV-OO-G	CCF group: CCF-CCAOVOO
CCSOVOOHCV919A2	Solenoid Valve	Fails to Close	3.00E-03	/demand	10	[Blanchard and Roy, 1998]	SOV-OO-G	CCF group: CCF-CCSOVOO
OP-ERR-VLV-1	Operator Error	Error in Selecting Control or Valve Outside Control Room	5.00E-02	/demand	5	[Benhardt et al., 1994]	3.6.6.3 (High Mean Value)	None
FSTRPNOL103	Saturable Reactor	No Output	1.07E-06	/hour	5	[CCPS, 1989]	1.2.8.3	Assumed to be similar to Rectifier Transformer. Assumed to be required to function for 1 hour for fuel salt drain

Event Name	Component Type	Failure Mode	Failure Rate	Units	Error Factor	Source	Source Identifier	Notes
FSTRRNOL103	High-current Transformer	No Output	2.53E-06	/hour	5	[CCPS, 1989]	1.2.8.1	Assumed to be similar to Power Transformer. Assumed to be required to function for 1 hour for fuel salt drain.

References for Appendix D

Benhardt, H.C., Eide, S.A., Held, J.E., Olsen, L.M., and Vail, R.E. [1994] Savannah River Site Human Error Data Base Development for Nonreactor Nuclear Facilities. Westinghouse Savannah River Company, WSRC-TR-93-581.

Blanchard, A., and Roy, B.N. [1998] Savannah River Site Generic Database Development. Westinghouse Safety Management Solution, WSRC-TR-93-262, Rev. 1.

Center for Chemical Process Safety (CCPS) [1989] Guidelines for Process Equipment Reliability Data with Data Tables. American Institute of Chemical Engineers (AIChE), New York, NY.

Guymon, R.H. [1973] MSRE Systems and Components Performance. Oak Ridge National Laboratory, ORNL-TM-3039.

APPENDIX E, FAULT TREE MODELS AND BASIC EVENT DATA USED IN MSRE OGS ETA

E.1. Fault Tree and Basic Event Data for Initiating Event – Release of Radioactive Material from OGS to Reactor Cell

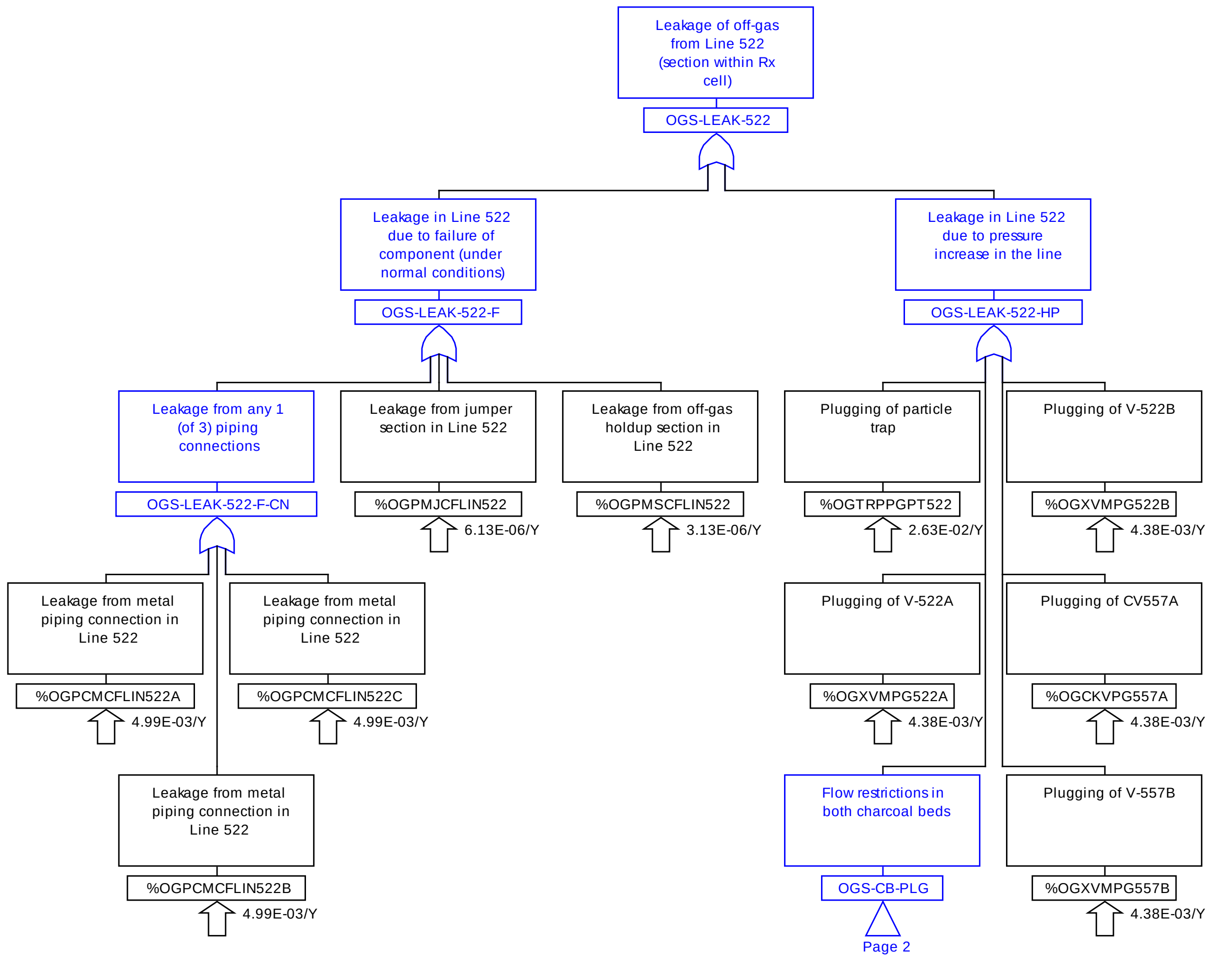


Figure 60: Fault tree for release of radioactive material from OGS to reactor cell (Page 1 of 4)

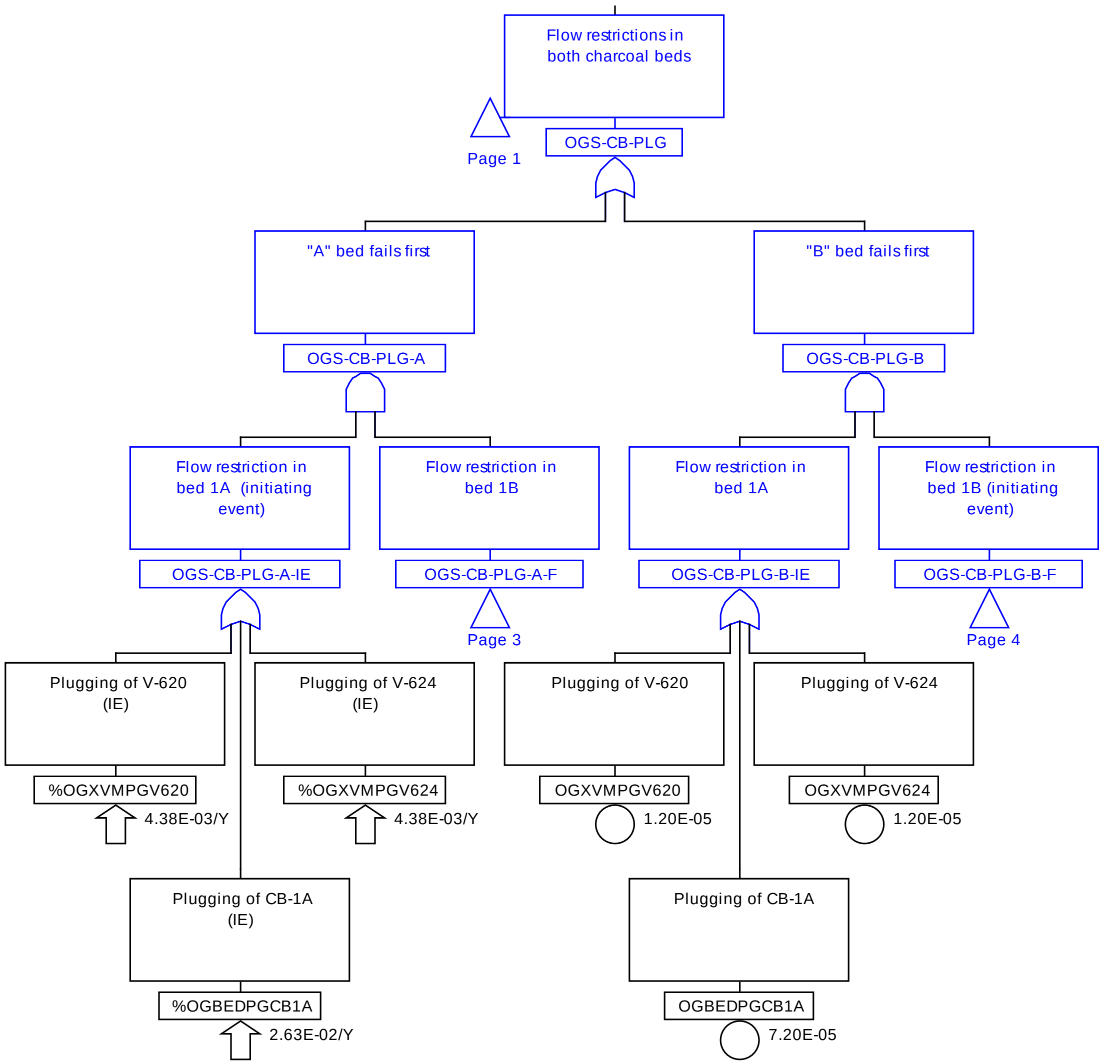


Figure 61: Fault tree for release of radioactive material from OGS to reactor cell (Page 2 of 4)

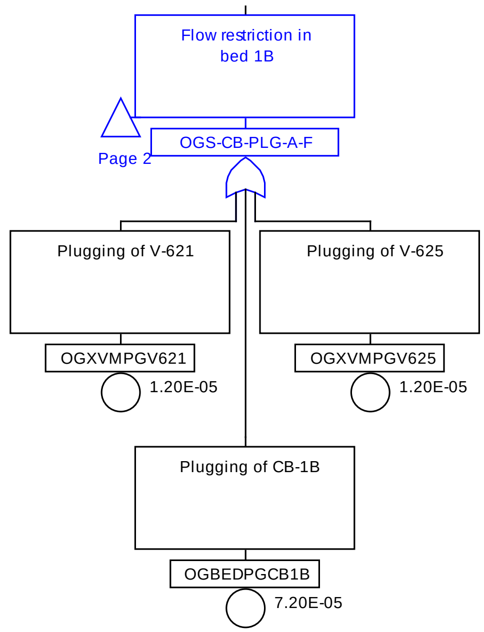


Figure 62: Fault tree for release of radioactive material from OGS to reactor cell (Page 3 of 4)

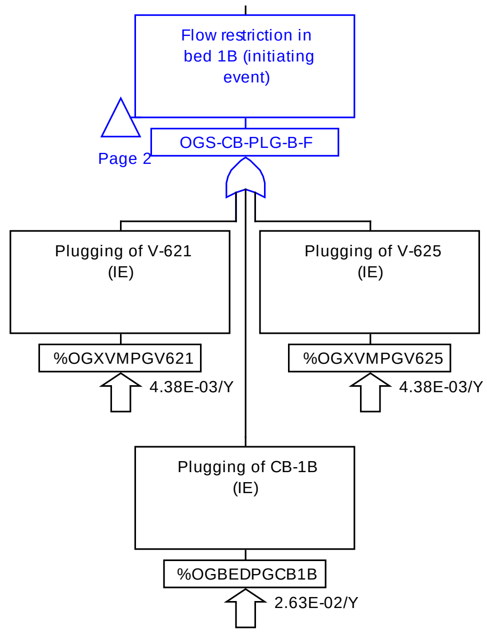


Figure 63: Fault tree for release of radioactive material from OGS to reactor cell (Page 4 of 4)

Table 21: Basic event data used in fault tree for release of radioactive material from OGS to reactor cell

Event Name	Component Type	Failure Mode	Failure Rate	Units	Error Factor	Source	Source Identifier	Notes
%OGPCMCFLIN522 A	Piping connection	Leakage/rupture	4.99E-03	/reactor -year	5	[CCPS, 1989]	3.2.1.4	
%OGPCMCFLIN522B	Piping connection	Leakage/rupture	4.99E-03	/reactor -year	5	[CCPS, 1989]	3.2.1.4	
%OGPCMCFLIN522C	Piping connection	Leakage/rupture	4.99E-03	/reactor -year	5	[CCPS, 1989]	3.2.1.4	
%OGPMJCFLIN522	Piping section (jumper)	Leakage/rupture	6.13E-06	/reactor -year	5	[Cadwallader , 1998]	Table A-2, Row 1	
%OGPMSCFLIN522	Piping section (metal)	Leakage/rupture	3.13E-06	/reactor -year	5	[CCPS, 1989]	3.2.1.1	
%OGTRPPGPT522	Particle trap	Plugging	2.63E-02	/reactor -year	10	[Blanchard and Roy, 1998]	FLT-PG-C	
%OGXVMPG522A	Manual valve	Plugging	4.38E-03	/reactor -year	10	[Blanchard and Roy, 1998]	XVM-PG-G	
%OGXVMPGV620	Manual valve	Plugging	4.38E-03	/reactor -year	10	[Blanchard and Roy, 1998]	XVM-PG-G	
%OGBEDPGCB1A	Charcoal bed	Plugging	2.63E-02	/reactor -year	10	[Cadwallader , 1998]	Table 1, Row 1	
%OGXVMPGV624	Manual valve	Plugging	4.38E-03	/reactor -year	10	[Blanchard and Roy, 1998]	XVM-PG-G	

Event Name	Component Type	Failure Mode	Failure Rate	Units	Error Factor	Source	Source Identifier	Notes
OGXVMPGV621	Manual valve	Plugging	5.00E-07	/hour	10	[Blanchard and Roy, 1998]	XVM-PG-G	Assumed to be checked every 24 hours for plugging
OGBEDPGCB1B	Charcoal bed	Plugging	3.00E-06	/hour	10	[Cadwallader, 1998]	Table 1, Row 1	Assumed to be checked every 24 hours for plugging
OGXVMPGV625	Manual valve	Plugging	5.00E-07	/hour	10	[Blanchard and Roy, 1998]	XVM-PG-G	Assumed to be checked every 24 hours for plugging
OGXVMPGV620	Manual valve	Plugging	5.00E-07	/hour	10	[Blanchard and Roy, 1998]	XVM-PG-G	Assumed to be checked every 24 hours for plugging
OGBEDPGCB1A	Charcoal bed	Plugging	3.00E-06	/hour	10	[Cadwallader, 1998]	Table 1, Row 1	Assumed to be checked every 24 hours for plugging

Event Name	Component Type	Failure Mode	Failure Rate	Units	Error Factor	Source	Source Identifier	Notes
OGXVMPGV624	Manual valve	Plugging	5.00E-07	/hour	10	[Blanchard and Roy, 1998]	XVM-PG-G	Assumed to be checked every 24 hours for plugging
%OGXVMPGV621	Manual valve	Plugging	4.38E-03	/reactor -year	10	[Blanchard and Roy, 1998]	XVM-PG-G	
%OGBEDPGCB1B	Charcoal bed	Plugging	2.63E-02	/reactor -year	10	[Cadwallader , 1998]	Table 1, Row 1	
%OGXVMPGV625	Manual valve	Plugging	4.38E-03	/reactor -year	10	[Blanchard and Roy, 1998]	XVM-PG-G	
%OGXVMPG522B	Manual valve	Plugging	4.38E-03	/reactor -year	10	[Blanchard and Roy, 1998]	XVM-PG-G	
%OGCKVPG557A	Check valve	Plugging	4.38E-03	/reactor -year	10	[Blanchard and Roy, 1998]	CKV-PG-G	
%OGXVMPG557B	Manual valve	Plugging	4.38E-03	/reactor -year	10	[Blanchard and Roy, 1998]	XVM-PG-G	

E.2. Fault Tree and Basic Event Data for Pivotal Event #1 – Fuel Salt Drain

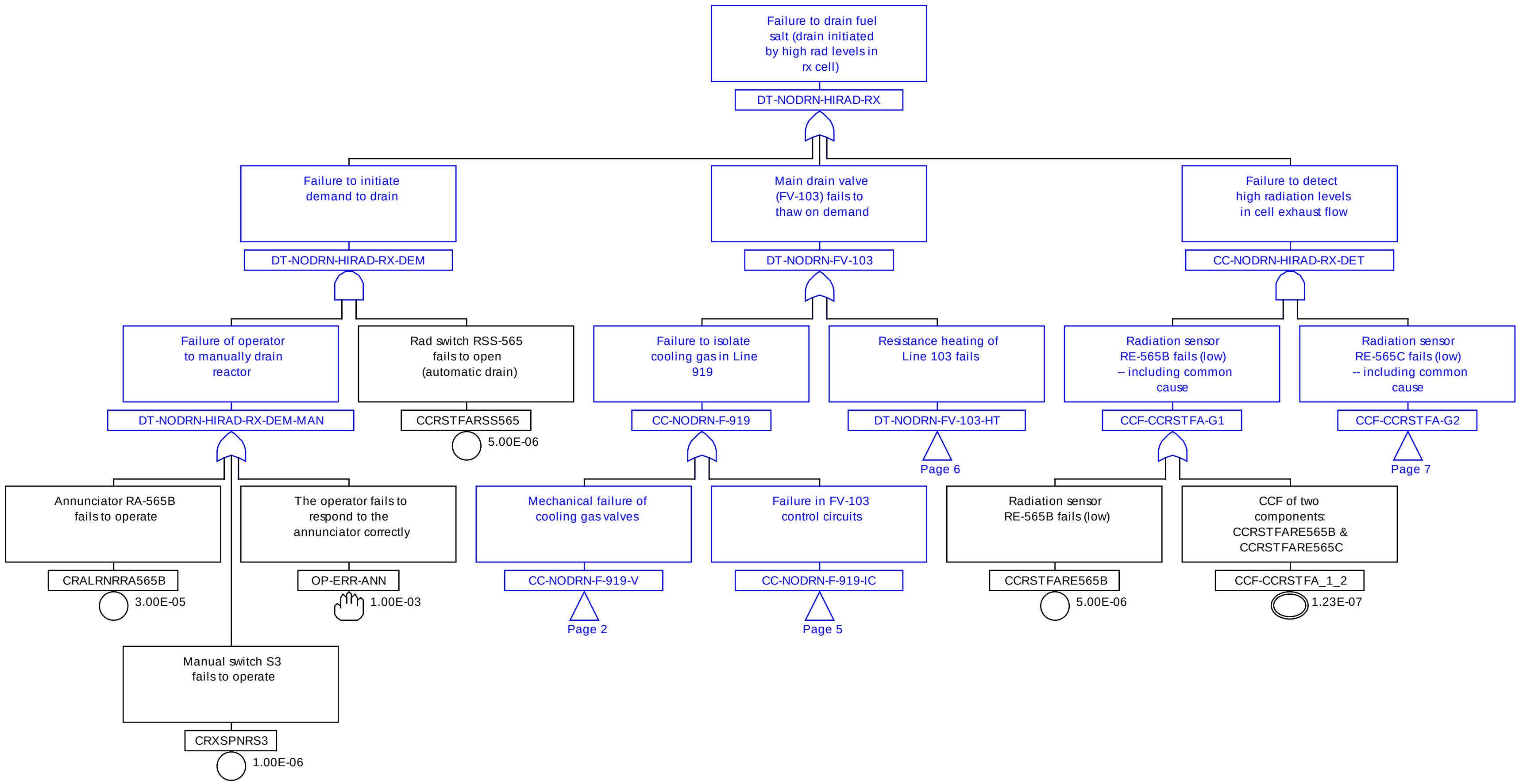


Figure 64: Fault tree for fuel salt drain (Page 1 of 7)

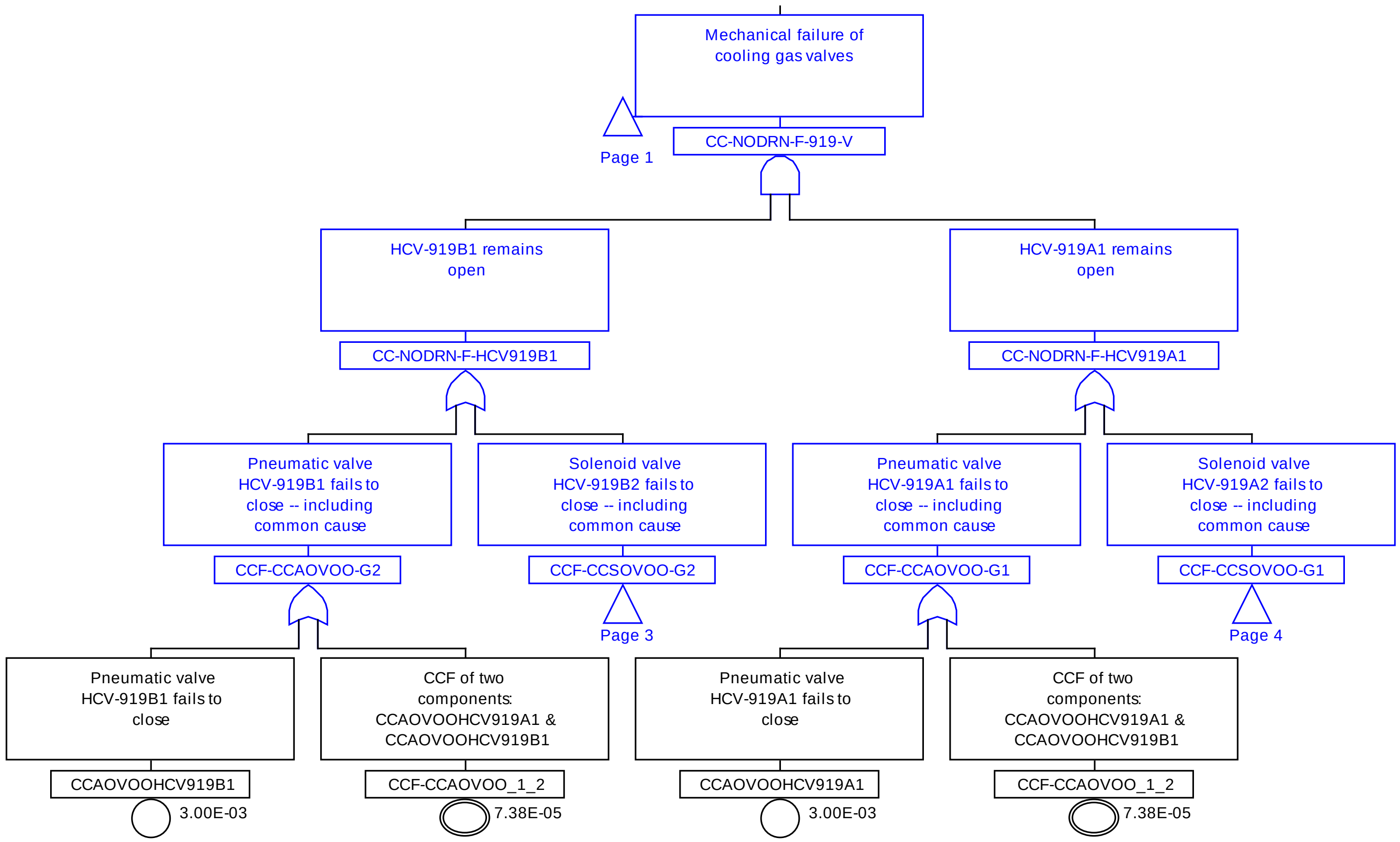


Figure 65: Fault tree for fuel salt drain (Page 2 of 7)

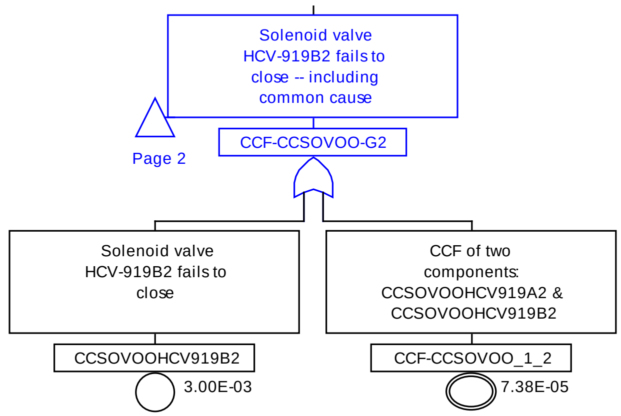


Figure 66: Fault tree for fuel salt drain (Page 3 of 7)

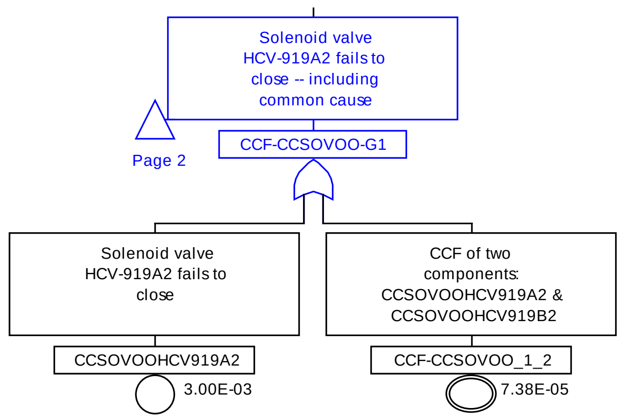


Figure 67: Fault tree for fuel salt drain (Page 4 of 7)

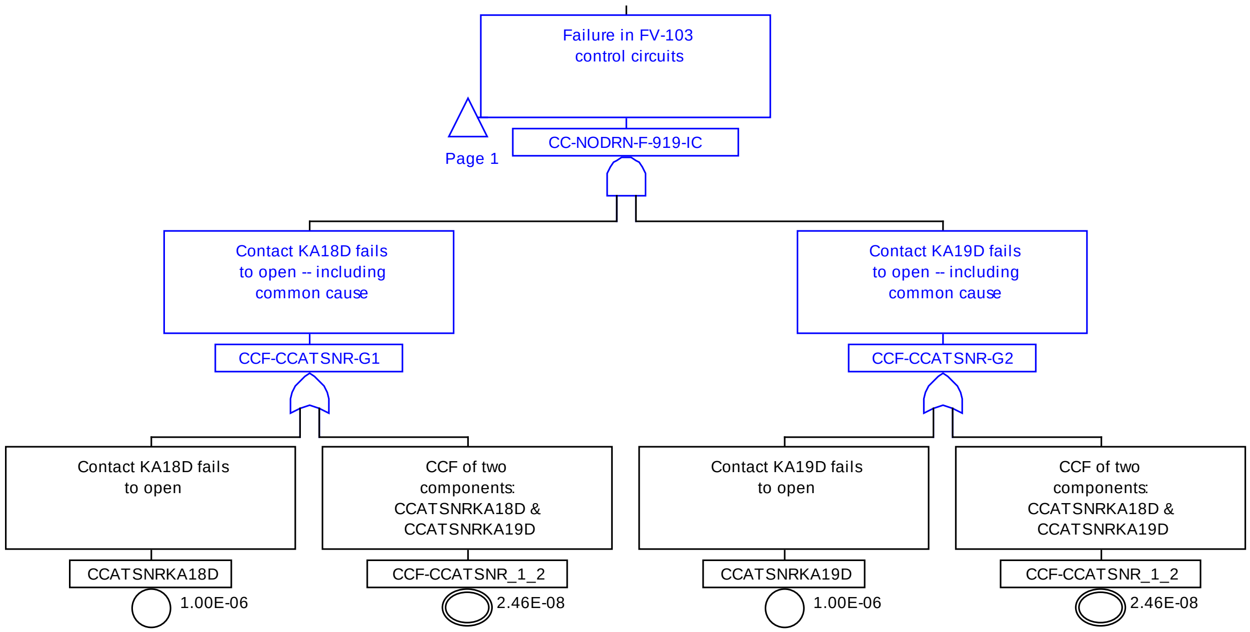


Figure 68: Fault tree for fuel salt drain (Page 5 of 7)

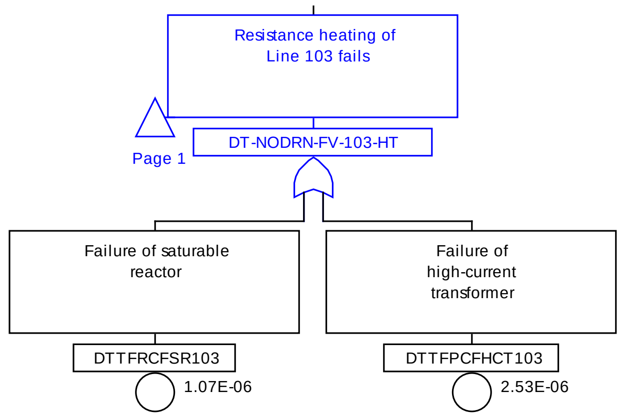


Figure 69: Fault tree for fuel salt drain (Page 6 of 7)

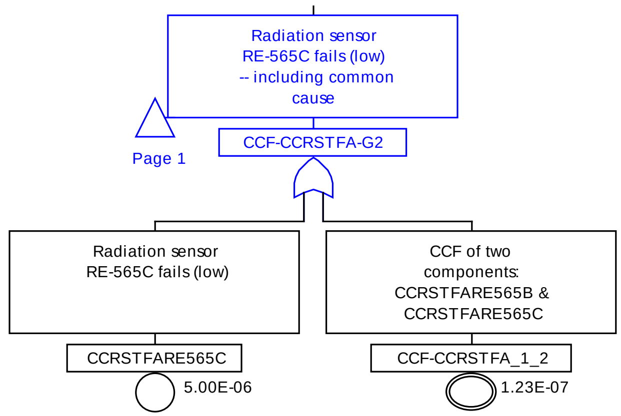


Figure 70: Fault tree for fuel salt drain (Page 7 of 7)

Table 22: Basic event data for fault tree of fuel salt drain

Event Name	Component Type	Failure Mode	Failure Rate	Units	Error Factor	Source	Source Identifier	Notes
CRALRNRRA565B	Annunciator	Fails to alarm	3.00E-05	/hour	10	[Blanchard and Roy, 1998]	ALR-NR-I	
CRXSPNRS3	Manual switch	Fails to open/close	1.00E-06	/hour	10	[Blanchard and Roy, 1998]	XSP-NR-E	
OP-ERR-ANN	Operator Error	Failure to correctly respond to annunciator	1.00E-03	/demand	3	[Swain and Guttmann, 1983]	Table 11-13	
CCRSTFARSS565	Radiation switch	Failure to open	5.00E-06	/hour	5	[Blanchard and Roy, 1998]	RST-FA-I	
CCAOVOOHCV919B1	Pneumatic Valve	Fails to Close	3.00E-03	/demand	10	[Blanchard and Roy, 1998]	AOV-OO-G	CCF group: CCF-CCAOVOO
CCSOVOOHCV919B2	Solenoid Valve	Fails to Close	3.00E-03	/demand	10	[Blanchard and Roy, 1998]	SOV-OO-G	CCF group: CCF-CCSOVOO
CCAOVOOHCV919A1	Pneumatic Valve	Fails to Close	3.00E-03	/demand	10	[Blanchard and Roy, 1998]	AOV-OO-G	CCF group: CCF-CCAOVOO
CCSOVOOHCV919A2	Solenoid Valve	Fails to Close	3.00E-03	/demand	10	[Blanchard and Roy, 1998]	SOV-OO-G	CCF group: CCF-CCSOVOO

Event Name	Component Type	Failure Mode	Failure Rate	Units	Error Factor	Source	Source Identifier	Notes
CCATSNRKA18D	Contact/ switch	Fails to open	1.00E-06	/hour	10	[Blanchard and Roy, 1998]	ATS-NR-E	CCF group: CCF-CCATSNR
CCATSNRKA19D	Contact/ switch	Fails to open	1.00E-06	/hour	10	[Blanchard and Roy, 1998]	ATS-NR-E	CCF group: CCF-CCATSNR
DTTFRCFSR103	Saturable Reactor	No Output	1.07E-06	/hour	5	[CCPS, 1989]	1.2.8.3	Assumed to be similar to Rectifier Transformer
DTTFPCFHCT103	High-current Transformer	No Output	2.53E-06	/hour	5	[CCPS, 1989]	1.2.8.1	Assumed to be similar to Power Transformer
CCRSTFARE565B	Radiation sensor	Failure	5.00E-06	/hour	5	[Blanchard and Roy, 1998]	RST-FA-I	CCF group: CCF-CCRSTFA
CCRSTFARE565C	Radiation sensor	Failure	5.00E-06	/hour	5	[Blanchard and Roy, 1998]	RST-FA-I	CCF group: CCF-CCRSTFA

E.3. Fault Tree and Basic Event Data for Pivotal Event #2 – Isolation of Cell Evacuation Flow

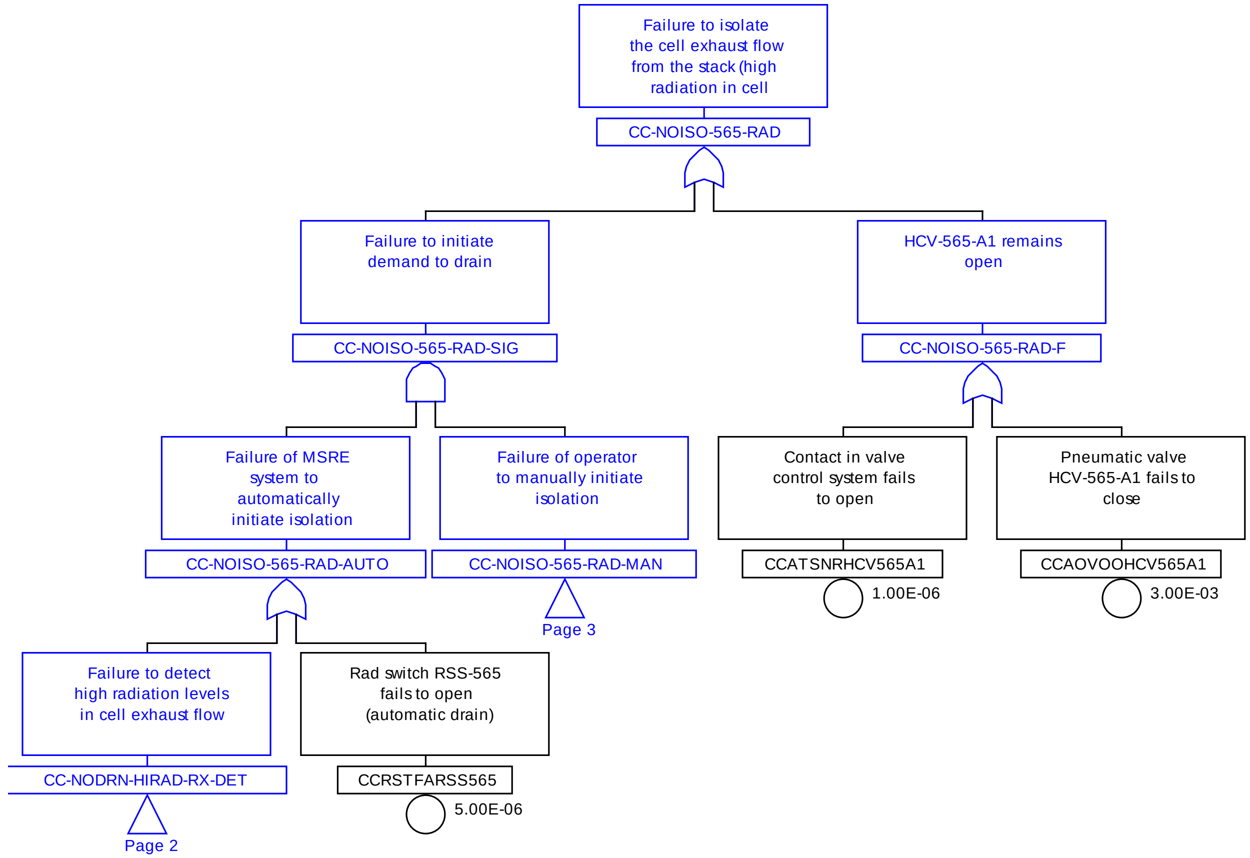


Figure 71: Fault tree for failure to isolate cell exhaust flow (Page 1 of 7)

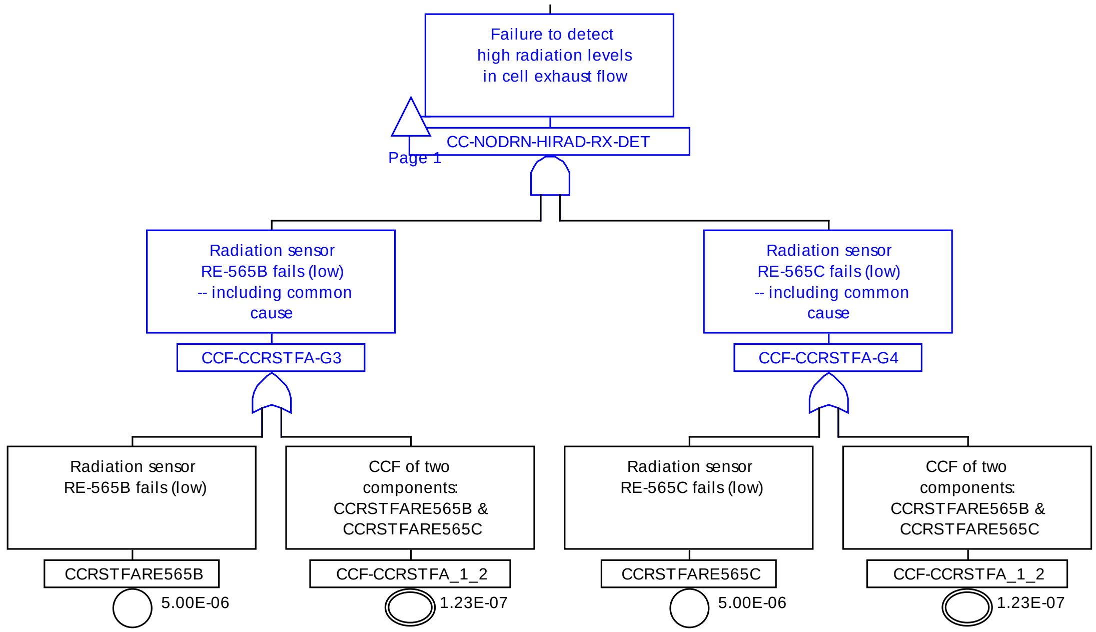


Figure 72: Fault tree for failure to isolate cell exhaust flow (Page 2 of 7)

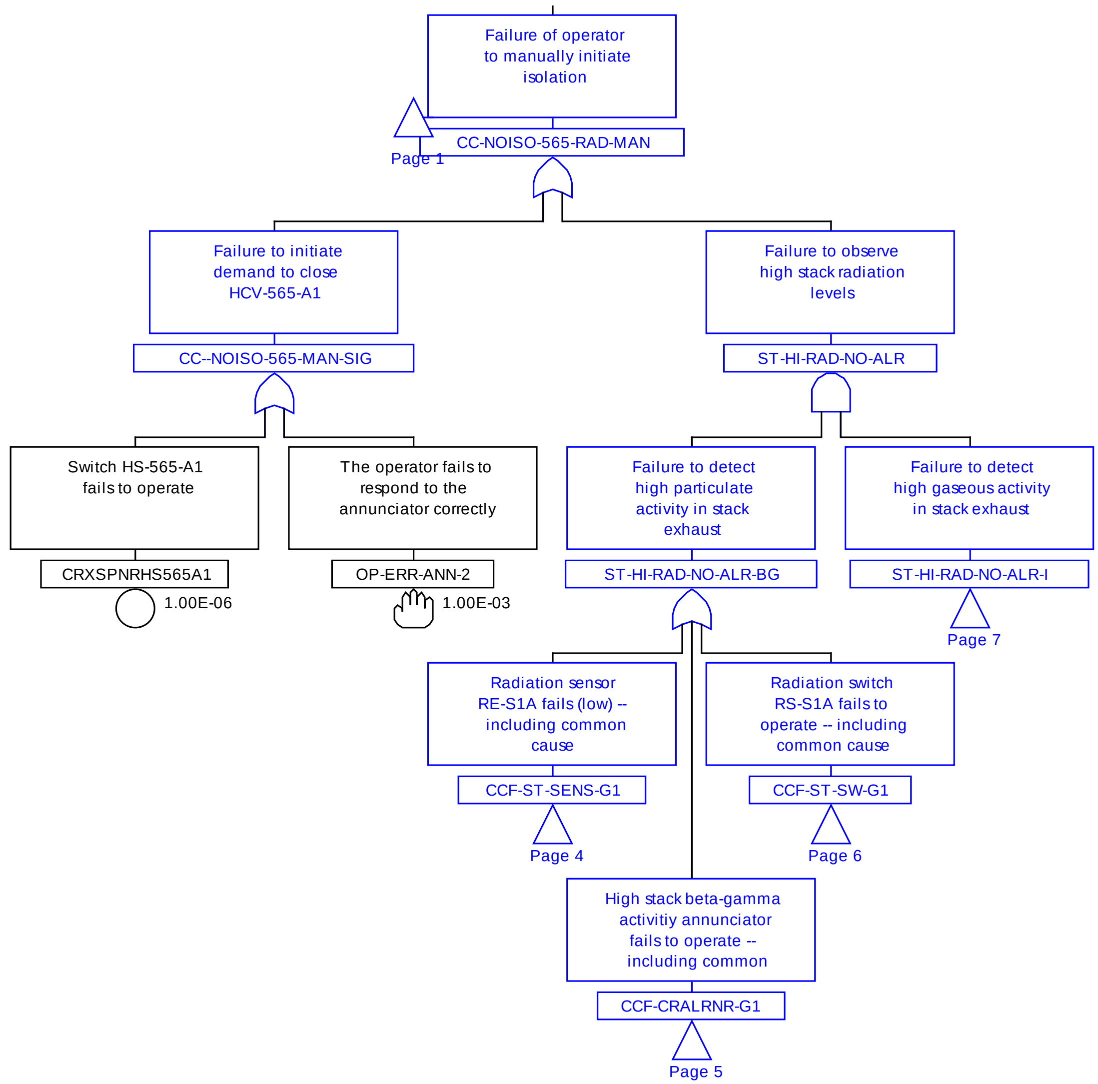


Figure 73: Fault tree for failure to isolate cell exhaust flow (Page 3 of 7)

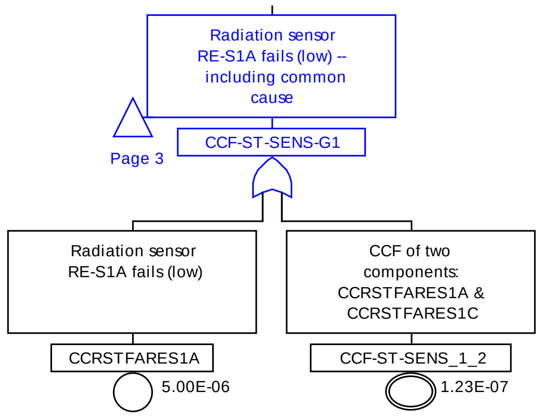


Figure 74: Fault tree for failure to isolate cell exhaust flow (Page 4 of 7)

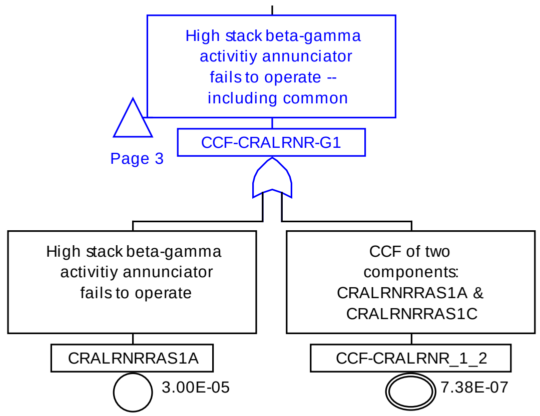


Figure 75: Fault tree for failure to isolate cell exhaust flow (Page 5 of 7)

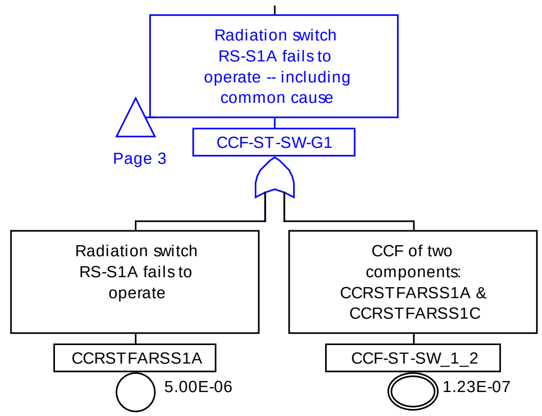


Figure 76: Fault tree for failure to isolate cell exhaust flow (Page 6 of 7)

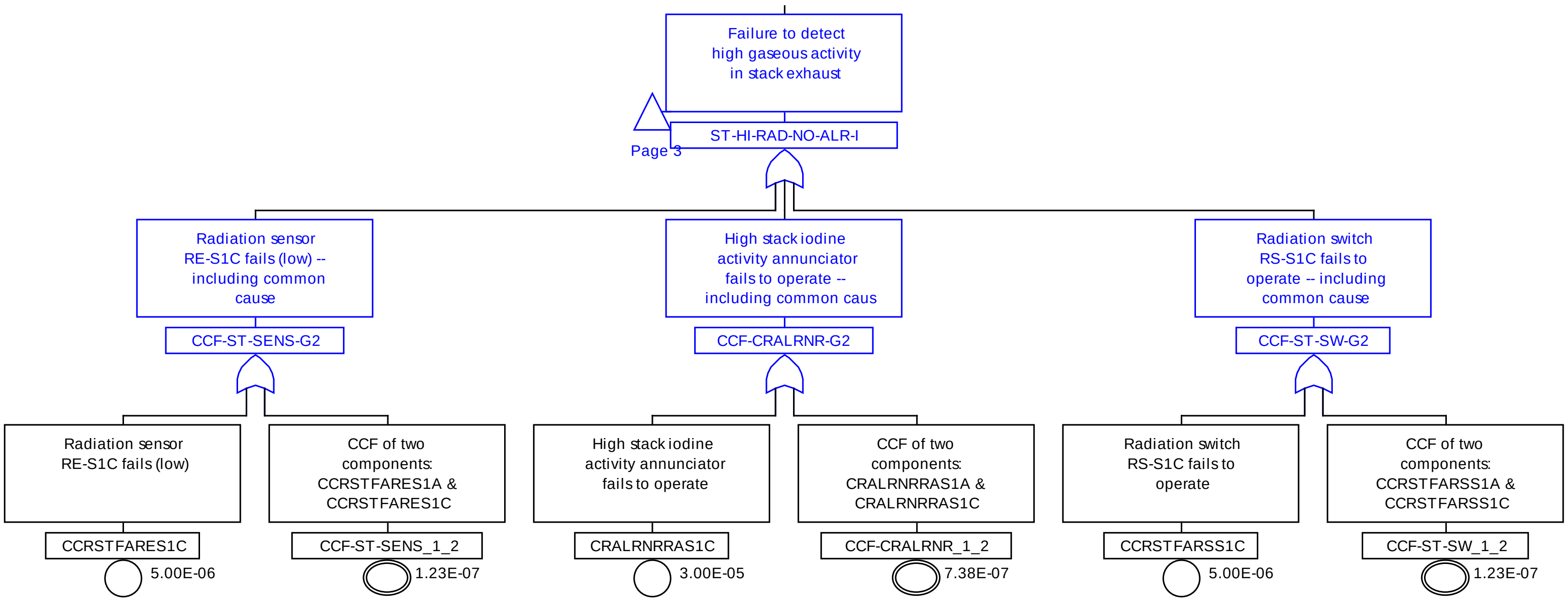


Figure 77: Fault tree for failure to isolate cell exhaust flow (Page 7 of 7)

Table 23: Basic event data for fault tree of failure to isolate cell exhaust flow

Event Name	Component Type	Failure Mode	Failure Rate	Units	Error Factor	Source	Source Identifier	Notes
CCRSTFARE565B	Radiation sensor	Failure	5.00E-06	/hour	5	[Blanchard and Roy, 1998]	RST-FA-I	CCF group: CCF-CCRSTFA
CCRSTFARE565C	Radiation sensor	Failure	5.00E-06	/hour	5	[Blanchard and Roy, 1998]	RST-FA-I	CCF group: CCF-CCRSTFA
CCRSTFARSS565	Radiation switch	Fails to open/close	5.00E-06	/hour	5	[Blanchard and Roy, 1998]	RST-FA-I	
CRXSPNRHS565A1	Manual switch	Fails to operate	1.00E-06	/hour	10	[Blanchard and Roy, 1998]	XSP-NR-E	
OP-ERR-ANN-2	Operator action	Failure to respond to annunciator	1.00E-03	/demand	3	[Swain and Guttmann, 1983]	Table 11-13	
CCRSTFARES1A	Radiation sensor	Fails (low)	5.00E-06	/hour	5	[Blanchard and Roy, 1998]	RST-FA-I	CCF group: CCF-ST-SENS
CRALRNRRAS1A	Annunciator	Fails to alarm	3.00E-05	/hour	10	[Blanchard and Roy, 1998]	ALR-NR-I	CCF group: CCF-CRALRNR
CCRSTFARSS1A	Radiation sensor	Fails (low)	5.00E-06	/hour	5	[Blanchard and Roy, 1998]	RST-FA-I	CCF group: CCF-ST-SW
CCRSTFARES1C	Radiation sensor	Fails (low)	5.00E-06	/hour	5	[Blanchard and Roy, 1998]	RST-FA-I	CCF group: CCF-ST-SENS

CRALRNRRAS1C	Annunciator	Fails to alarm	3.00E-05	/hour	10	[Blanchard and Roy, 1998]	ALR-NR-I	CCF group: CCF-CRALRNR
CCRSTFARSS1C	Radiation sensor	Fails (low)	5.00E-06	/hour	5	[Blanchard and Roy, 1998]	RST-FA-I	CCF group: CCF-ST-SW
CCATSNRHCV565A1	Contact/switch	Fails to open	1.00E-06	/hour	10	[Blanchard and Roy, 1998]	ATS-NR-E	
CCAOVOOHCV565A1	Pneumatic valve	Fails to close	3.00E-03	/demand	10	[Blanchard and Roy, 1998]	AOV-OO-G	

References for Appendix E

Blanchard, A., and Roy, B.N. [1998] Savannah River Site Generic Database Development. Westinghouse Safety Management Solution, WSRC-TR-93-262, Rev. 1.

Cadwallader, L.C. [1998] Selected Component Failure Rate Values from Fusion Safety Assessment Tasks. Idaho National Engineering and Environmental Laboratory (INEEL), Idaho Falls, ID, INEEL/EXT-98-00892.

Center for Chemical Process Safety (CCPS) [1989] Guidelines for Process Equipment Reliability Data with Data Tables. American Institute of Chemical Engineers (AIChE), New York, NY.

Swain, A., and Guttmann, H. [1983] Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. US NRC, Washington, DC, NUREG/CR-1278.

APPENDIX F, CALCULATIONS TO ESTIMATE RADIOACTIVITY OF GASEOUS FLOW INTO MSRE OGS

Table 24 displays the calculations for the radioactivity being swept by the helium cover gas from the gas space of the fuel salt pump bowl into the OGS each second. For these calculations, the radioelements were grouped based on their expected state of matter (solid, liquid, or gas) at 150°F, which was the maximum ambient temperature of the reactor cell during normal operations [Guymon, 1973; Robertson, 1965]. The ability to leak to the reactor cell, as well as the mitigating effects of the filters in the MSRE CCS and ventilation system, would be different for gases and particulates.

The estimates for radioactivity given by Houtzeel and Dyer [1972] are given in disintegrations/min/inch of pipe. The pipe is 1 inch inner diameter; thus, the volume of a 1 inch section is π * (0.5 in)^2 * 1 in = 0.785 in^3 = 0.0129 L. Given a flowrate of 4 L/min through the pipe, 4 / 0.013 = 308 sections/min = 5 section volumes per second. Finally, to get curies of isotope per second flowing through the pipe the following conversion was used:

(X dis/min/inch) / (2.22e12 dis/min/Ci) * (5 section volumes per second) = Y curies flowing into line per second

Table 24: Estimated radioactivity of OGS flow in Line 522

Isotope	Gas or Particulate	dis/min/in	Source	Ci per inch of pipe	Ci/sec	Bq/sec
H-3	Gas	N/A	[Briggs, 1971] page 5 (60 curies/day)	N/A	6.94E-04	2.57E+07
Kr-87	Gas	1.3E+14	[Houtzeel and Dyer, 1972] Table 7.4	58.56	292.8	1.08E+13
Kr-88	Gas	1.2E+14	[Houtzeel and Dyer, 1972] Table 7.4	54.05	270.3	1.00E+13
Rb-88	Particulate* (Note 1)	1.8E+13	[Houtzeel and Dyer, 1972] Table 7.4	8.11	40.5	1.50E+12
Kr-89	Gas	2.2E+14	[Houtzeel and Dyer, 1972] Table 7.4	99.10	495.5	1.83E+13

Isotope	Gas or Particulate	dis/min/in	Source	Ci per inch of pipe	Ci/sec	Bq/sec
Ru-89	Particulate	8.2E+13	[Houtzeel and Dyer, 1972] Table 7.4	36.94	184.7	6.83E+12
Kr-90	Gas	7.3E+13	[Houtzeel and Dyer, 1972] Table 7.4	32.88	164.4	6.08E+12
Nb-95	Particulate	9E+12	[Houtzeel and Dyer, 1972] Table 7.4	4.05	20.3	7.50E+11
Xe-135	Gas	1.3E+13	[Houtzeel and Dyer, 1972] Table 7.4	5.86	29.3	1.08E+12
Xe-135m	Gas	5E+13	[Houtzeel and Dyer, 1972] Table 7.4	22.52	112.6	4.17E+12
Xe-138	Gas	1E+14	[Houtzeel and Dyer, 1972] Table 7.4	45.05	225.2	8.33E+12
Cs-139	Particulate* (Note 1)	1E+13	[Houtzeel and Dyer, 1972] Table 7.4	4.50	22.5	8.33E+11
Xe-139	Gas	1E+13	[Houtzeel and Dyer, 1972] Table 7.4	4.50	22.5	8.33E+11
Xe-140	Gas	1E+12	[Houtzeel and Dyer, 1972] Table 7.4	0.45	2.3	8.33E+10
Sr-91	Particulate	2E+12	[Houtzeel and Dyer, 1972] pg 74	0.90	4.5	1.67E+11
Nb-97	Particulate	1E+14	[Houtzeel and Dyer, 1972] pg 74	45.05	225.2	8.33E+12
Mo-99	Particulate	3.3E+13	[Houtzeel and Dyer, 1972] pg 74	14.86	74.3	2.75E+12
Ru-105	Particulate	3.4E+12	[Houtzeel and Dyer, 1972] pg 74	1.53	7.7	2.83E+11
Rh-105	Particulate	8E+12	[Houtzeel and	3.60	18.0	6.67E+11

Isotope	Gas or Particulate	dis/min/in	Source	Ci per inch of pipe	Ci/sec	Bq/sec
			Dyer, 1972] pg 74			
Te-129m	Particulate	2E+12	[Houtzeel and Dyer, 1972] fig 7.9	0.90	4.5	1.67E+11
Te-131m	Particulate	7.5E+11	[Houtzeel and Dyer, 1972] pg 79	0.34	1.7	6.25E+10
I-131	Particulate* (Note 2)	5E+12	[Houtzeel and Dyer, 1972] pg 79	2.25	11.3	4.17E+11
I-132	Particulate* (Note 2)	1.2E+13	[Houtzeel and Dyer, 1972] pg 81	5.41	27.0	1.00E+12
TOTAL		**1.00E+15**		**451.4**	**2257**	**8.35E+13**
SUM	**Gases Only**	**7.17E+14**		**323.0**	**1615**	**5.98E+13**

*Note 1: Elements that were liquids at 150°F were assumed to behave as particulates

*Note 2: Although elemental iodine is gaseous at 150°F, the iodine in the OGS was assumed to be in a compound that would behave as a particulate.

References for Appendix F

Briggs, R.B. [1971] Additional Calculations of the Distribution of Tritium in the MSRE. Oak Ridge National Laboratory, ORNL CF-71-7-8.

Guymon, R.H. [1973] MSRE Systems and Components Performance. Oak Ridge National Laboratory, ORNL-TM-3039.

Houtzeel, A., and Dyer, F. [1972] A Study of Fission Products in the Molten-Salt Reactor Experiment by Gamma Spectroscopy. Oak Ridge National Laboratory, ORNL-TM-3151.

Robertson, R.C. [1965] MSRE Design and Operations Report - Part I: Description of Reactor Design. Oak Ridge National Laboratory, ORNL-TM-728.