Application of a Method to Estimate Risk in Advanced Nuclear Reactors: A Case Study on the Molten Salt Reactor Experiment

Brandon Chisholm*[a], Steve Krahn[a], Amir Afzali[b], and Eric Harvey[c]
[a] Vanderbilt University, Nashville, TN, USA
[b] Southern Company Services, Birmingham, AL, USA
[c] Electric Power Research Institute (EPRI), Palo Alto, CA, USA

Abstract: Advanced nuclear reactor designs are receiving interest from electric utilities and regulators due to the possible enhanced safety, economic, and fuel cycle benefits they can offer. However, because these designs incorporate novel design features, structures, systems, and components (SSCs), the consideration of some hazards and failure mechanisms that are not present in commercial Light Water Reactor (LWR) designs is required in order to adequately analyze the risk significance of design choices in these reactors.

This paper describes initial work conducted to demonstrate the incorporation of industry standard analysis methodologies into the design and risk assessment processes in a manner that will help generate safety feedback for the design process, while simultaneously contributing to the development of a Probabilistic Risk Assessment (PRA). These flexible and comprehensive hazard analyses help show where stakeholders should focus to ensure that risks are properly addressed by reactor designs that may not have significant industry operating experience yet. The suggested approach involves performing one or more process hazards analysis of reactor subsystems to produce results that are directly useful to designers and then can be utilized to conduct Event Tree Analysis (ETA) and Fault Tree Analysis (FTA). The quantitative results of such ETA and FTA can then highlight risk significant components and event sequences to each source term relevant to a given reactor design.

Keywords: Risk Assessment, Advanced Reactor, Hazard Analysis

1. INTRODUCTION

In contrast to the PRA approach developed for Light Water Reactors (LWRs), there have been few applications of a method to develop a balanced and supportive safety case for advanced reactor designs having limited to no commercial operating experience. Furthermore, the integration of appropriate risk assessment methods into the design process can provide valuable safety insights and give feedback to designers early in the process when changes are less costly to make. Guidelines for building a PRA in support of risk-informed, performance-based applications for an advanced non-LWR plant are being developed by the industry-led Licensing Technical Requirements Modernization Project (LMP) [1]. However, because risk assessment of advanced reactor designs will require the consideration of hazards that are not present in LWRs, a comprehensive and flexible method to identify all significant hazards is needed to inform the collection of input data needed for the performance of the early stage PRA development. Qualitative and semi-quantitative Process Hazard Analysis (PHA) methodologies are considered to be well-suited for such applications, and generate outputs that can readily support the construction of fault trees and event trees to be used in the quantitative PRA activities. Use of PHA methods in this context is also consistent with approaches endorsed domestically by the US Department of Energy [2] and the draft ASME/ANS PRA Standard for Advanced Non-LWR Nuclear Power Plants [3]. Furthermore, this approach is consistent with international methodologies, such as the Generation IV International Forum's Integrated Safety Assessment Methodology (ISAM) [4].

The six Generation IV advanced reactor systems, as defined by the Generation IV International Forum, include the gas-cooled fast reactor (GFR), lead-cooled fast reactor (LFR), molten salt reactor (MSR), sodium-cooled fast reactor (SFR), supercritical-water-cooled reactor (SCWR), and very-high

**Email address: brandon.m.chisholm@vanderbilt.edu*

temperature reactor (VHTR) [5]. In this work, the system chosen as the reactor type to provide an example of how standard hazard assessment techniques can be used as inputs to PRA is the fluid-fueled MSR. Although the intention is that the developed safety assessment process could be applied to any technology, MSRs present an opportunity to analyze a particularly unique hazard profile. Some of the purported benefits of MSRs that are consistent with expressed regulatory expectations (e.g. Ref. [4]) include passive safety, relying on fundamental properties, and simplified safety systems. However, these reactor designs often incorporate a number of novel design elements and, therefore, require the consideration of hazards and failure mechanisms that are not present in commercial LWR designs. Additionally, during normal operations, the radioactive isotopes in the fuel (and the fission products generated in the fuel) are dissolved and circulating within the fuel salt system. Generally speaking, these systems represent a significantly larger volume than the structures confining these isotopes in other reactor designs (such as fuel pellets, particles, or rods). Finally, due to the chemistry of the fuel salt, the radioactive isotopes within the reactor can coexist in many different physical states and chemical compounds under normal operating conditions within the system.

The work described in this report builds upon recent applications of PHA to MSRs [6,7,8], and shows how PHA studies can be applied to subsystems that are both unique to a class of reactors and integral to reliable and safe reactor operation. In addition, this paper explores how to select a specific PHA methodology based on the intended use of the hazard assessment results, and discusses considerations for how to conduct the PHA to maximize the usefulness of the study. A Hazards and Operability (HAZOP) study was conducted on the Component Cooling System (CCS) and Off-Gas System (OGS) of an MSR design, and it is demonstrated how these results can be used to build event trees to investigate the risk significance of various event sequences. In addition, a Failure Modes and Effects Analysis (FMEA) was conducted on the systems that contribute to the proper functioning of the MSR freeze valve component. This paper also discusses how to use FMEA results to construct fault trees to analyze the effect of individual components on system reliability.

1.1. The Molten Salt Reactor Experiment (MSRE)

The specific MSR design analyzed in this work is the Molten Salt Reactor Experiment (MSRE), an 8 MWth test reactor designed, constructed, and operated at Oak Ridge National Laboratory (ORNL) in the 1960s. This particular reactor design was selected because it represents a detailed non-proprietary MSR design, with extensive design information and five years of documented operational experience. The MSRE contains representative examples of many common functions, subsystems, and components seen in modern fluid-fueled MSR designs. The following paragraphs briefly describe significant aspects of the MSRE design; however, much more detailed discussion is available in the MSRE Design and Operations report [9], and the MSRE Systems and Components Performance report [10].

The MSRE was a single-region, circulating liquid salt-fueled and cooled, thermal-spectrum reactor. The fuel was UF_4 dissolved in a carrier salt of $LiF\text{-}BeF_2\text{-}ZrF_4$, and the operating temperature of the fuel salt loop averaged around 650°C (1200°F). In the fuel salt loop, the fuel salt was recirculated by a vertical short-shaft pump through a shell-and-tube heat exchanger and the reactor vessel. Heat from fission was generated in the fuel salt as it passed through the graphite channels of the reactor vessel, and then transferred in the heat exchanger to a liquid $LiF\text{-}BeF_2$ coolant salt. The coolant salt was circulated by a similar centrifugal pump through the heat exchanger and through a radiator. Air was blown by axial flow blowers past the radiator tubes to remove the heat, and this air was then exhausted to the atmosphere via a stack.

Drain tanks were provided for storing the fuel and coolant salts when the reactor was not operating. The salts were drained to the drain tanks by gravity, and transferred back to the circulating systems by pressurizing the drain tanks with helium. 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, they were swept out by a low flow purge of helium into the Off-Gas System (OGS). The plant was also provided with a simple processing facility for the offline treatment of fuel salt batches with hydrogen fluoride (for removing oxide contamination) and fluorine (for removing the uranium).

Major auxiliary systems for the MSRE included: (1) a cover-gas system with treating stations for removing oxygen and moisture from the helium cover gas; (2) two closed-loop oil systems for lubricating the bearings of the fuel and coolant pumps; (3) a closed loop Component Cooling System (CCS) for cooling in-cell components using 95% N_2 and less than 5% O_2; (4) several cooling water systems; (5) a ventilation system for contamination control; and (6) an instrument air system.

1.2. Process Hazards Analysis (PHA) Overview

In the chemical industry, a PHA (also known as a hazard evaluation) 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." [11] In NUREG-1513, the NRC calls this type of study an Integrated Safety Analysis (ISA) and describes how PHA techniques should be applied to nuclear fuel cycle facilities in order to address the special hazards present at the facilities as well as their potential for causing criticality incidents and radiological releases, in addition to certain chemical releases [12]. The NRC has also recognized that ISAs have succeeded 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 [13]. As previously mentioned, PHAs have been identified by regulators as a suitable method to analyze these same concepts in advanced nuclear reactor designs [3,4].

The NRC recognizes that the American Institute of Chemical Engineers (AIChE) Guidelines for Hazard Evaluation Procedures [11] is perhaps the most clear and comprehensive reference to provide information on common PHA methodologies, in addition to being well-suited to practitioners of hazard analysis [12]. The Guidelines describe 12 different PHA methodologies that provide a spectrum of processes available to perform industry-standard PHA efforts. Choosing among these options is based on the design information available for the evaluation, as well as the intended use of the results. For example, in a previous study [6], the "What If" analysis was chosen due to the relative immaturity of the reactor design being analyzed at the time of the study. However, in the present work, the two methodologies selected are the Hazards and Operability (HAZOP) study and the Failure Modes and Effects Analysis (FMEA). These three methodologies (What-If/Checklist, HAZOP, 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 [11].

The HAZOP approach was selected for a comprehensive PHA of the entire MSRE system, since the hazard evaluation efforts are intended to eventually support the development of a preliminary PRA model, and because detailed design information is available. HAZOP is the most comprehensive of the primarily non-quantitative PHA methods and is recognized in industry standards as a method that provides sufficiently detailed results to directly support PRA efforts [4,14]. This methodology has been successfully used on projects early in design phases to inform the design process on an iterative basis [11]. The HAZOP approach is based on the principle that 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". [13]

As a supplement to the HAZOP study, an FMEA was performed on the components that directly contribute to the operation of the main MSRE freeze valve (between the reactor vessel and the fuel salt drain tanks). The FMEA was selected for the analysis of the freeze valve because the components being studied were exclusively mechanical or electrical in nature [12]. Additionally, as discussed in Section 4 of this paper, the consideration of specific effects associated with individual component failure modes allows the results of the FMEA to be more readily adaptable into basic events for Fault Tree Analysis (FTA).

2. SYSTEM CHARACTERIZATION

According to the CCPS Guidelines [11], one of the first stages of any PHA study is to establish the appropriate level of resolution for the study and define the boundaries for the system, subsystem, or process being analyzed (also known as “nodes” in HAZOP studies). Another important part of preparation for a PHA study is to identify the important system parameters that should to be used to consider potentially risk significant deviations from normal operation. The definition of these kinds of attributes for a PHA requires a thorough understanding of the system design and intended operation. For the MSRE, detailed design information was obtained from ORNL technical reports that describe MSRE reactor design [9], instrumentation and controls [15,16], and performances of systems and components [10]. This section of the paper will discuss significant concepts to consider while preparing a system to be studied in a PHA and how these concepts were applied to the MSRE.

2.1. Source Term Characterization

From a practical standpoint, PRA models are typically developed for a specific combination of radionuclide source, plant operating state, and hazard group [3]. Thus, in order to produce PHA results that will provide useful input to a PRA model, it is valuable to start with the characterization of the source terms that will have event sequences with associated potential consequences. Starting with the identification and characterization of radionuclide sources is also consistent with the PRA development process suggested for advanced reactors by the LMP [17].

Important aspects to consider when identifying radionuclide sources include the magnitude and form of the radioactivity, relative locations, and barriers to the release of the radioactive material. The form (e.g. physical state or chemical compound) and amount of radioactivity will affect the severity of the consequences associated with the release of a given source term, and sources with different forms can require different analyses to model the behavior of the material. Similarly, the location of the material (in relation to the entire system and/or the public) can determine what barriers or functions are used to prevent a release of the material, and event sequences that require the failure or success of the same barriers or functions can often be grouped together in an initial PRA model developed during an early design phase.

Major radionuclide sources identified for the MSRE during normal operation include the fuel salt circulating within the fuel salt system and the volatile fission products (as well as their radioactive daughters) in the Off-Gas System. The molten fluoride-based fuel salt has fission products and transuranics dissolved within it as it circulates around the fuel salt loop. ORIGEN calculations performed after the final MSRE shutdown estimated a total of 28.5 million curies contained within the fuel salt by the time the final shutdown and drain was conducted [18]. However, in the fuel salt pump bowl, a portion of the salt is sprayed out of holes in a distributor, which allows the noble gas fission products (mostly xenon and krypton) to vent from the salt [9]. A helium sweep gas is introduced to the pump bowl to carry an estimated 280 curies each second out of the fuel salt loop and into the off-gas system, which is designed to allow for the decay of all radioactive isotopes to insignificant amounts with the exception of ^{85}Kr, ^{131m}Xe, and ^{133}Xe. After being held up for this decay, the effluent of the off-gas disposal system is exhausted to the atmosphere after passing through filters to retain solids and is massively diluted [9]. Other radionuclide sources inherent to the MSRE design include the radioactive material present in the fuel processing and handling equipment during fuel processing operations (the MSRE did not perform online fuel processing), tritium that diffused to the reactor cell atmosphere, and any radioactivity contained in the liquid waste system [9]. Consideration of these sources would likely be necessary for a complete analysis of the MSRE, especially in analysis for maintenance evolutions and decommissioning; however, due to lack of information on the form and amount of radioactive material or the absence of any possible event sequences that could feasibly occur during normal operation, these minor sources were not considered further in this work.

The MSRE was designed and operated such that any component containing multi-curie levels of radioactive material had at least two barriers between the radioactivity and the environment [9]. For the fuel salt, the first barrier to release is the physical integrity of the fuel salt loop and the drain tanks. During normal operation, the fuel salt is circulated through the reactor vessel, the fuel salt pump, and the shell side of the heat exchanger. The fuel salt is prevented from draining to the drain tanks by a frozen "plug" of salt inside a freeze valve in the drain line at the bottom of the core. The second barrier to release of the fuel salt is a seal welded containment vessel in which all of the components containing fuel salt are housed. The first barrier to release of the fuel salt does contain penetrations, and some of these penetrations connect the fuel salt system to the system(s) for the handling and disposal of the second major source of radionuclides, the fuel salt off-gas. Components constituting the first barrier for the off-gas source also include the particle filter trap, the off-gas holdup pipe, the main charcoal bed, and the auxiliary charcoal bed.

The second barrier for the off-gas source term is composed of multiple smaller structures in different locations around the MSRE building. The off-gas line from the reactor pump bowl starts in the reactor cell, which also contains the off-gas holdup pipe. However, after the holdup pipe, the off-gas line continues through the reactor cell wall penetration and through the coolant salt areas encased in a larger pipe (surrounded by lead shielding). The line then passes through valves in a pressure tight instrument box located in the lower portion of the vent house. From this box, the line continues in an underground shielded duct to an underground valve box and then to the charcoal bed cell, which has cooling water flowing through the cell. As discussed previously, after exiting the charcoal beds the gas flow is primarily helium carrier gas. This mostly clean gas flows to an underground valve box, then to a filter pit before mixing with air and being drawn through the "absolute filters" of the ventilation system to be discharged from a stack.

2.2. Selection of Nodes for Process Hazard Analyses

In order to conduct a PHA study, it is necessary to subdivide the entire reactor 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 [19]. If the section being analyzed is too small, there is the possibility of initiating events and/or effects being overlooked because they occur outside of the section boundary. If too large a section is taken, then the function of the design intention can become imprecise or very complicated such that it is difficult to determine all significant effects that occur due to a failure or deviation from normal operation. Although there is no simple, universal method to divide the design into sections, there are some considerations that can help ensure the results of the PHA study readily facilitate the development of a PRA model.

The first recommendation while dividing the system into nodes is to ensure that each node can be determined to have one major function and that multiple nodes do not perform the same function (with the exception being redundant subsystems). It will be demonstrated in Section 3 that the failure of a node can often be represented in event tree analysis as a gate on an event tree, so it is desirable to be able to analyze the causes and effects of each failed function within the study of a node. If the results of the PHA study are intended to inform quantitative risk assessment, it may also be beneficial to structure the nodes such that each node has similar operating conditions (such as temperature, pressure, and/or working fluid). This grouping facilitates the gathering of component reliability, as failure rate data is often grouped using these attributes (for example, see [20]). Finally, when preparing these nodes, it is valuable to thoroughly document all interfaces between nodes, as these interfaces may be capable of propagating a potential accident from one node to another.

Based on a review of MSRE design information [9,10,15,16], more than 20 unique nodes were defined based on primary function and nominal operating conditions. Some of the nodes identified do not differ substantially from systems with significant industrial experience (e.g. tower cooling water system, instrument air system) and other nodes had previously been analyzed in great detail by the MSRE design team (hazards in the fuel salt loop are discussed in [21]). Additionally, because MSRE was a test reactor, some of the nodes are not common to modern MSR designs (e.g. the sampler-enricher). Thus, the first MSRE nodes analyzed in a HAZOP study were the off-gas system (OGS) and the component cooling system (CCS). The major components in these systems are shown in Figure 2.

These gas systems perform functions that will likely need to be addressed in common MSR designs, are integral to safe operation of the MSRE, and have not been subject of detailed prior hazard evaluations or risk assessments.

The components that constitute the MSRE freeze valve subsystem analyzed in the FMEA are displayed schematically in Figure 3. This subsystem includes some components that are also in the CCS node analyzed in the HAZOP study, as well as some pneumatic and electric control components that were not previously studied. The subsystem divided into two separate sections for the FMEA based on primary function. The first section was composed of the CCS components, since this section has a single working fluid (i.e. reactor cell atmosphere gas) and the primary function of this section in the context of freeze valve performance is to supply cooling gas to the freeze valve (regardless of freeze valve condition). The second section was composed of the instrumentation and control associated with the two pneumatic valves that manage the condition of the freeze valve by determining 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 20 psig.

2.3. Identification of Important System Parameters

One final helpful task that can be performed during the preparation for a PHA study is to identify the system parameters to be considered during the study. For a HAZOP study, these parameters are combined with guidewords to generate the deviations used to analyze the system [8,19]. In an FMEA, although the parameters are not used explicitly, consideration of the list of important parameters during the study can help encourage 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 from system to system, care should be taken to ensure that the design intention of each node and the overall system is carefully considered. It is possible that some parameters that apply to one section may not apply to every node, and new parameters of interest may be identified during the PHA study [19]. In order to start the process of developing a list of parameters, generic lists of process variables are available [19].

The relevant top-level phenomena to be 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 list are common process parameters that are typically measured in real time and given 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 [12]. 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 MSR for reasons including the fact that the chemical composition of the 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 assessment of other advanced reactor technologies [17].

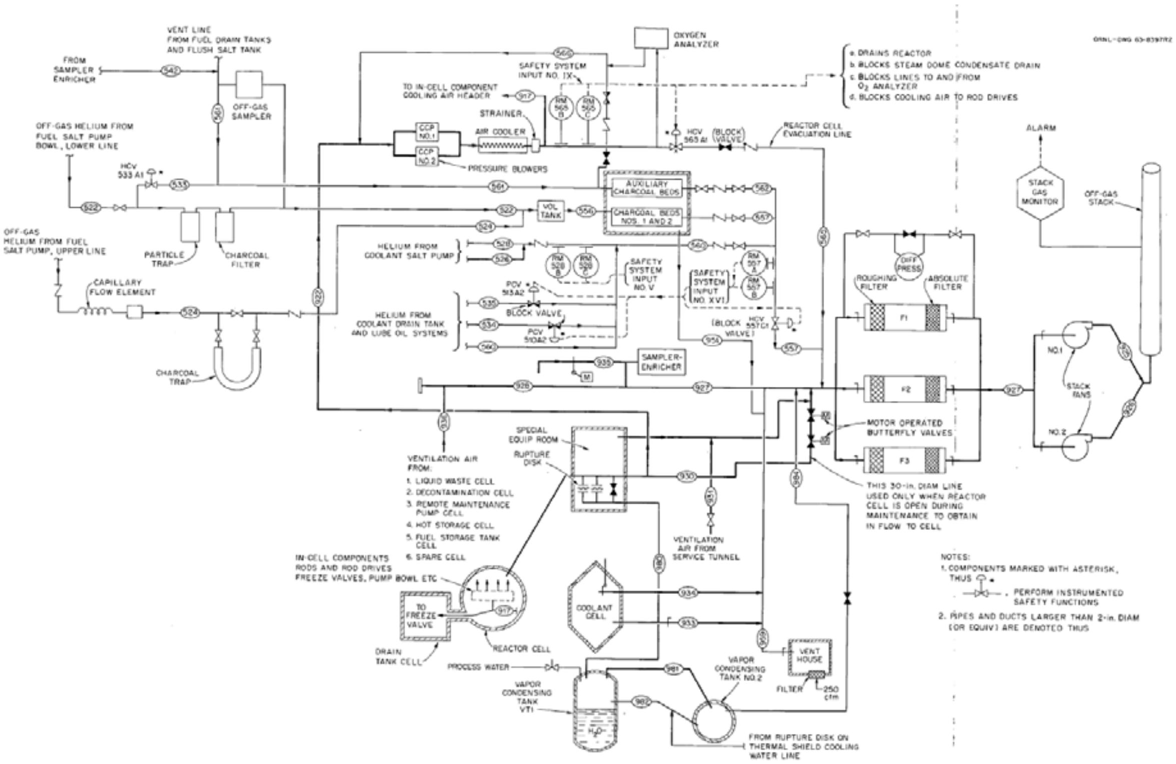

Figure 2: MSRE OGS and CCS [15]

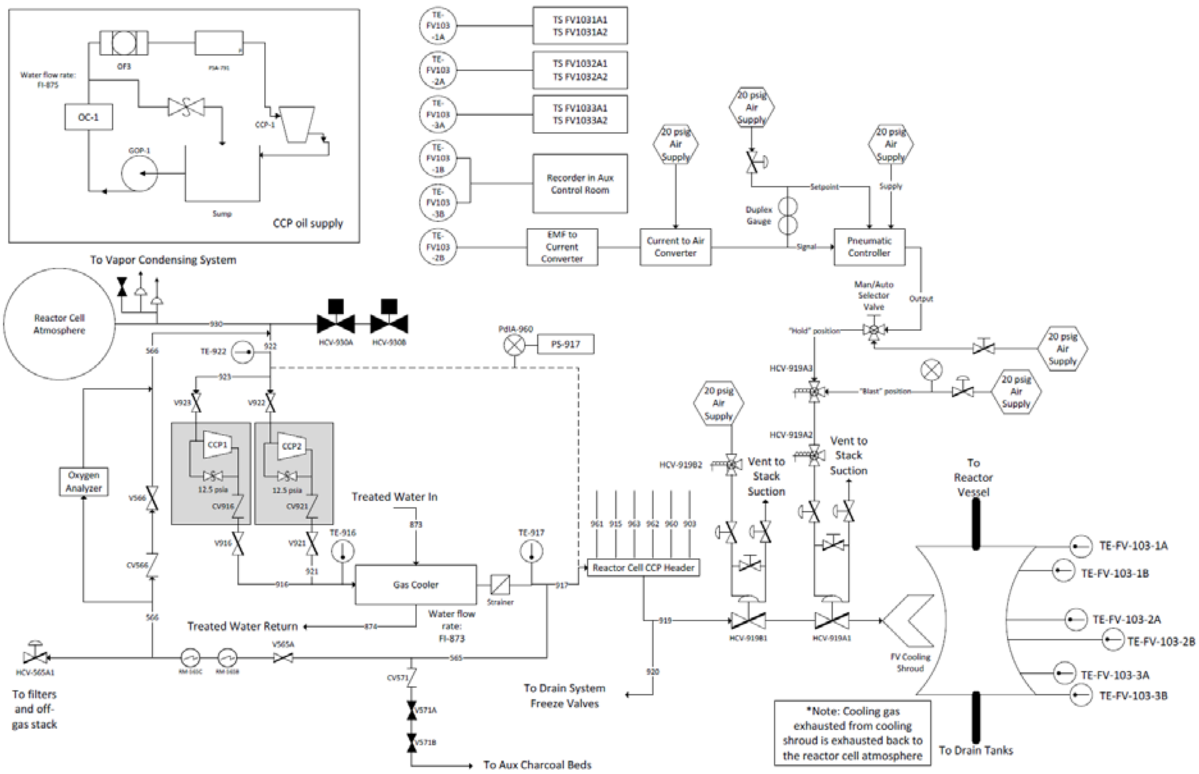

Figure 3: MSRE freeze valve schematic

3. HAZARDS AND OPERABILITY (HAZOP) STUDY

As an illustrative example of how to perform a HAZOP study on nodes in an advanced reactor design, two important MSRE subsystems, the off-gas system (OGS) and component cooling system (CCS), were evaluated as designed and operated by ORNL. The HAZOP study process and results are described in greater detail in prior work [7,8]. Rather than focus on the general mechanics of the HAZOP methodology or the insights gained from the HAZOP study of the MSRE OGS and CCS, this section will discuss how to use the results to construct event trees and measures during the study to maximize the use of the results for this purpose.

3.1. The HAZOP Study Process

Conducting the HAZOP study involves a structured assessment with a team of subject matter experts familiar with the design and operation of the system. The fundamental concept of a HAZOP study is to identify potential situations outside of the intended operation range of the node, or deviations, by coupling a guideword and a parameter. “Guidewords” are action words or phrases such as “no,” or “reduced,” that describe how the important system parameters could change in relation to their values during normal operation. Each cause of a given deviation is documented, and the consequences and safety systems mitigating these consequences are documented for each cause. An additional column of the results table records potential “actions” (e.g. clarifications on the current design or operating procedures) identified during the HAZOP analysis that may require resolution outside of the study. Once all information for a specific deviation has been recorded, the team proceeds to generate the next deviation. After all applicable guidewords for a given parameter have been considered, the HAZOP team considers the next parameter of interest, and repeats the analysis process. The examination of a system or subsystem is completed when no further important parameters remain. The format of the results generated during a HAZOP study generally follows a common tabular structure, such as that suggested in References 11 and 19 (and evident in Table 1, below).

3.2. HAZOP Study of the MSRE OGS and CCS

The HAZOP study of the MSRE OGS and CCS was conducted with the aid of a commercially available hazard assessment software program to facilitate the systematic review of each deviation, the potential consequences and mitigation, prevention, and control systems. A total of 35 potential deviations were identified and evaluated for the OGS, in addition to the 38 deviations pertaining to the CCS. The HAZOP study revealed the possibility of a cooling water leak to generate hydrogen fluoride gas in the charcoal beds of the OGS, which is a scenario not previously identified that could produce a corrosive and toxic hazard. The study also identified that the cooling capacity of the CCS gas cooler affects the ability to control salt flow since this system is used to remove heat from the freeze valve. An excerpt of the results table is displayed below in Table 1; however, a more complete discussion of the HAZOP study and the results is available in Ref. [8].

3.3. Transitioning from HAZOP Results to Event Tree Analysis (ETA)

The event tree in Figure 4 provides an example how the PHA results in Table 1 can be used to facilitate the development of a PRA model for the off-gas source term in the MSRE OGS. This event tree is qualitative and simpler than the ETA that would be required for a full PRA; however, the intention in this paper is to focus on describing the process of transitioning from HAZOP results to ETA. The cause of the first deviation in Table 1 (high fuel salt pump bowl cover gas pressure) is an initiating event that, if unmitigated, could reduce the residence time of the off-gas in the OGS before it is exhausted to the atmosphere and increase the radiological release rate; thus, this cause represents the first gate of the event tree. Looking at the safety systems listed for both deviations in Table 1, it can be seen that the OGS has automatic system responses intended to mitigate these consequences, as well as a variety of indications to the operator that such a scenario is occurring. Because these success or failure of these functions affects the final consequence of the event sequence, they become the second, and third gates of the ETA.

The redundant radiation monitors in the off-gas line are designed to detect high levels of radiation and automatically isolate the off-gas line from the stack. If these components operate successfully, the scenario is terminated and there is no increase in release rate. However, if the automatic systems fail, the MSRE is designed such that the operator would receive visual and audial indications of off-normal conditions (e.g. high pump bowl pressure and high stack radiation levels). If the operator responded swiftly and correctly to these indications and drained the fuel salt from the fuel salt loop, there would likely be no significant increase in the release rate of the radioactive off-gas. However, if isolation was not achieved by either the safety system or the reactor, the consequence is not mitigated and the potential exists for a higher rate of radioactive off-gas to be exhausted by the MSRE stack.

Table 1: Example MSRE OGS HAZOP study results

Deviation	Cause	Consequences	Safety Systems
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	• PT-522 pressure indication in fuel salt pump bowl • PT-592 pressure indication in fuel salt pump bowl • RM-557A radiation indication downstream of charcoal beds (trips HCV-557-C1) • RM-557B radiation indication downstream of charcoal beds (trips HCV-557-C1) • Temperature indications throughout system (VH-2, particle trap, charcoal beds)
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)	• RM565B and RM565C that trigger closing of HCV-565A • Ventilation filters for particulates • Stack monitors RIA-S1 and RIA-S2

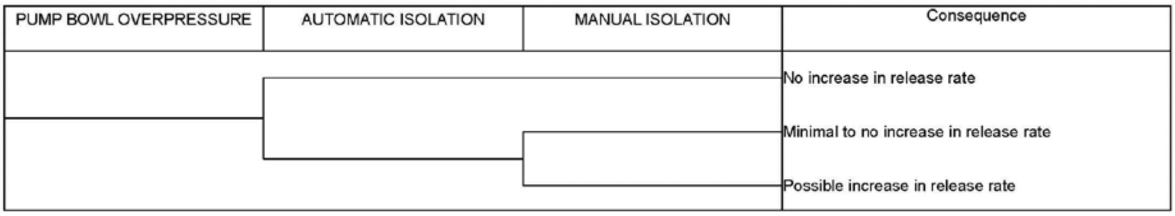

Figure 4: Example qualitative MSRE OGS event tree

During the HAZOP study of the MSRE OGS and CCS, it was found that comprehensively documenting all unmitigated effects of a scenario within the node was beneficial to the process of constructing event trees. Similarly, listing the consequences of the deviation at each nodal interface ensured that the event sequence could be sufficiently analysed using HAZOP results from multiple nodes. Because the intention will be to eventually construct quantitative fault trees to estimate the probability of each event tree gate and event sequence, it was also helpful to differentiate between automatic system responses and actions required by operators in response to system indications. This differentiation will aid in the handling of human error within the MSRE PRA model.

4. FAILURE MODES AND EFFECTS ANALYSIS (FMEA)

The impetus behind an FMEA of the components contributing the proper functioning of the MSRE freeze valve was two-fold; first, the freeze valve “component” is important to the operability of the MSRE and an estimated failure rate of the component is necessary for a quantitative estimate of risk in the MSRE. Because no estimate of freeze valve reliability can be found in existing literature, an FMEA will be used to help structure fault trees and provide an estimate of freeze valve failure rates.

Second, the FMEA results, combined with a sensitivity study using quantitative FTA, can allow insight towards the individual components that are the most critical for ensuring proper freeze valve performance and how freeze valve reliability can be maximized.

4.1 The FMEA Process

An FMEA is performed in a deliberate, systematic manner to reduce the possibility of omissions and to enhance the completeness of the study [11]. The study is performed by examining each individual component at a time, and then listing all credible failure modes associated with the equipment type and operating conditions. For the FMEA of the MSRE freeze valve, industry-standard component reliability databases were consulted [20] to ensure that no failure modes were overlooked. 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. The key to performing a consistent FMEA is ensuring that the effects of all equipment failures are analyzed on a common basis [11]. In the FMEA of the freeze valve, the effects were evaluated on a worst case basis by assuming that existing safeguards did not work. An additional column recording any notes or unresolved actions or question about the design can also be included in the results table for later resolution. The FMEA analysis proceeds systematically until all failure modes for each component in the system have been considered and the results have been recorded.

Table 2: Example MSRE freeze valve FMEA results

Identification/ Description	Failure Mode	Effects	Safety Systems
TE-FV103-1A (temperature sensor and transmitter)	Fails to bottom of range	Close TS-FV103-1A1 Open TS-FV-103-1A2	Redundant channels TE-1B and TE-3B are displayed on recorder in auxiliary control room
TS-FV-103-1A2 (temperature switch, normally closed)	Spurious opening	De-energize solenoid to close HCV-919B2	Annunciator on high freeze plug temperature (TE-2A and TS-2A2)

More than 170 failure modes were analyzed during the FMEA of the MSRE freeze valve system, and an excerpt of the results is displayed in Table 2. The same software used for the HAZOP study was able to be used for the FMEA.

4.2 Transitioning from FMEA to Fault Tree Analysis (FTA)

The qualitative fault tree in Figure 5 demonstrates an example of how the FMEA results shown in Table 2 contribute to building a model of a subset of the freeze valve system. Similar to the event tree in Figure 4, this fault tree is of relatively simple construction to allow emphasis on the transition between PHA results and FTA. By looking at Figure 3, it is evident that pneumatic valve HCV-919B1 opens to allow cooling gas to flow to the freeze valve body, such that if this valve is closed, it is not possible to cool the freeze valve and keep the salt in the plug frozen. The position of this pneumatic valve is controlled by solenoid valve HCV-919B2, which much be energized to allow HCV-919B1 to open. Using the failure of HCV-919B2 to remain open as the top gate of the fault tree in Figure 5, the FMEA results showed that this failure could be produced by a mechanical failure of HCV-919B2 or by the de-energization of the solenoid. From the FMEA results in Table 2, it can be seen that the solenoid is energized if two temperature switches (TS-FV103-1A2 and TS-FV103-3A2) are closed, and these temperature switches are closed if the temperature indication from the associated thermocouple (TE-FV103-1A and TE-FV103-3A, respectively) is above a given setpoint. Thus, HCV-919B2 could be closed by the opening of either temperature switch, which could occur due to the failure of the temperature switch itself or due to the failure of the associated temperature sensing channel.

Compared to the HAZOP results, the FMEA results were much more detailed and single rows of the results table did not generally describe event sequences in a comprehensive manner. For the CCS components that had previously been analyzed using the HAZOP methodology, the FMEA did not contribute much new analysis of physical failures that was not covered during the HAZOP study 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 did allow for the analysis of human errors that had not previously been discussed, such as the mispositioning of a manual valve. By contrast, the FMEA was very helpful to analyze the effects of the control components, such as the switches, sensing elements, and transmitters in Table 2. Because the performance of control system can be affected in different ways depending on the failure mode (e.g. a temperature switch spuriously opens/closes or fails to open/close), the FMEA proved to be a useful tool to build FTA models that include these components.

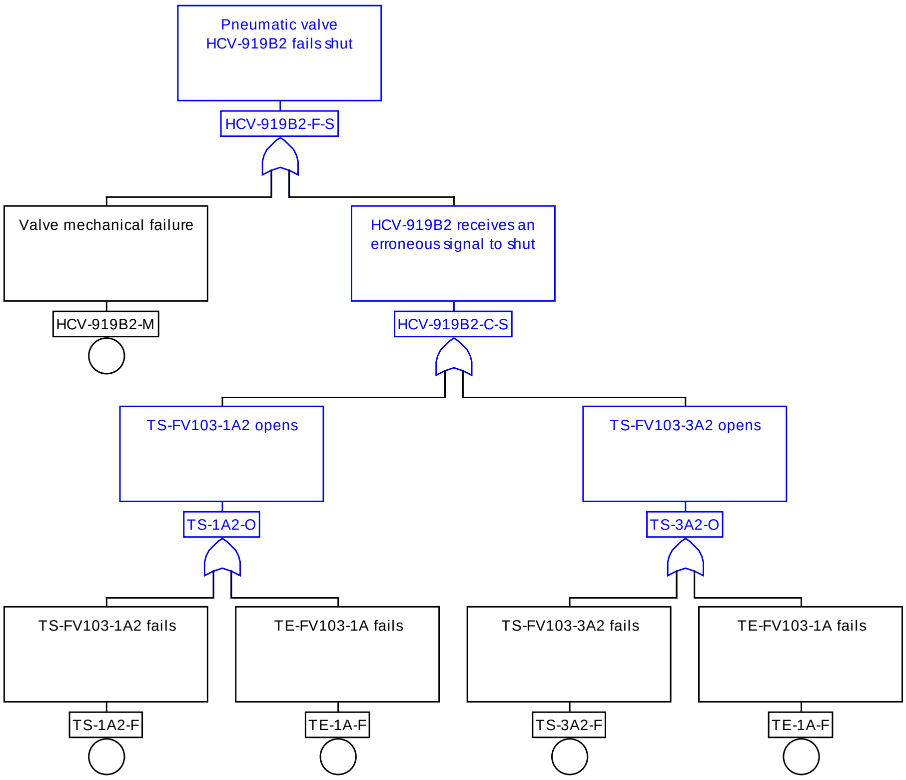

Figure 5: Example qualitative fault tree for MSRE freeze valve

5. CONCLUSION

The work in this paper provides a preliminary demonstration of how industry standard process hazard analysis methodologies can be used to flexibly and comprehensively identify hazards in advanced reactor designs. Not only can these methodologies be tailored such that they are technology neutral, they can also be conducted in a way that facilitates the construction of a PRA model for the system being analyzed. As a demonstration, a HAZOP study and a FMEA were performed on portions of the MSRE. The HAZOP study is capable of informing the construction of event trees and fault trees for most mechanical systems; however, more complex electrical and/or control systems can benefit from the higher detail of an FMEA. Future work will involve completing HAZOP studies for each of the nodes defined for the MSRE design (identified in Section 2.3, above) in order to facilitate the construction of a PRA model that is capable of estimating the likelihood and frequency of hazardous event sequences for each of the major source terms in the design. In order to quantify the PRA model, it will be necessary to complete the initial construction of a database of MSR-specific component failure rates [8].

Acknowledgements

The authors would like to acknowledge EPRI and Southern Company Services for sponsorship of this research. The authors would also like to acknowledge the assistance of Oak Ridge National Laboratory in providing access to the technical information documenting the MSRE design during this project. This material is based upon work supported under a Department of Energy, Office of Nuclear Energy, Integrated University Program Graduate Fellowship.

References

[1] Nuclear Energy Institute (NEI), "Licensing Technical Requirement Modernization Project," ML17013A140, Washington, DC, January 2017.

[2] US Nuclear Regulatory Commission (NRC), Policy Statement on the Regulation of Advanced Reactors. NRC-2008-237, 2008.

[3] GEN IV Risk and Safety Working Group (RSWG), An Integrated Safety Assessment Methodology (ISAM) for Generation IV Nuclear Systems. Version 1.1, June 2011.

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

[5] OECD Nuclear Energy Agency, "Technology Roadmap Update for Generation IV Nuclear Energy Systems." Generation IV International Forum, Jan 2014.

[6] Electric Power Research Institute (EPRI), Program on Technology Innovation: Technology Assessment of a Molten Salt Reactor Design: The Liquid-Fluoride Thorium Reactor (LFTR). 2015: 3002005460. Palo Alto, CA. p. 208 pages.

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

[8] Chisholm, B, Krahn, S. Croff, A., Marotta, P., Sowder, A., and Smith, N. "Preliminary Hazard Assessment and Component Reliability Database for the Molten Salt Reactor Experiment". ICAPP 2018 Proceedings, Charlotte, North Carolina, April 8-11, 2018. pp 513-522.

[9] Robertson, R. "MSRE Design and Operation Report Part I: Description of Reactor Design," ORNL-TM-728, January 1965.

[10] Guymon, R., "MSRE Systems and Components Performance". ORNL-TM-3039, 1973.

[11] Center for Chemical Process Safety (CCPS), Guidelines for Hazard Evaluation Procedures. Third Edition, American Institute of Chemical Engineers (AIChE). Vol. ISBN: 978-0-471-97815-2. 2008, New York: John Wiley & Sons.

[12] US Nuclear Regulatory Commission. "Integrated Safety Analysis - Guidance document. NUREG-1513." (2001).

[13] US Nuclear Regulatory Commission (NRC), A Comparison of Integrated Safety Analysis and Probabilistic Risk Assessment, Office of Nuclear Material Safety and Safeguards, December 2010.

[14] US Department of Energy (DOE), Development of Probabilistic Risk Assessments for Nuclear Safety Applications, DOE-STD-1628-2013, November 2013.

[15] Tallackson, J. "MSRE Design and Operations Report Part IIA: Nuclear and Process Instrumentation," ORNL-TM-729, February 1968.

[16] Moore, R. "MSRE Design and Operations Report Part IIB: Nuclear and Process Instrumentation," ORNL-TM-729, September 1972.

[17] Southern Company, "Modernization of Technical Requirements for Licensing of Advanced Non-Light Water Reactors Probabilistic Risk Assessment Approach," Draft Report for Collaborative Review ML17158B543, June 2017.

[18] Bell, M. "Calculated Radioactivity of MSRE Fuel Salt," ORNL-TM-2979, May 1970.

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

[20] Blanchard, A., Savannah River Site generic data base development. Savannah River Site (US), WSRC-TR93-262, Rev 1, May 1998.

[21] Beall, S., Breazeale, W., and Kinyon B. "Molten-Salt Reactor Experiment Preliminary Hazards Report," ORNL-CF-61-2-46, February 1961.