ABSTRACT

HAMZA, MOSTAFA. OpenPHI – A Human Reliability Analysis Methodology to Risk-Inform the Importance of Operator Actions for Advanced Reactors during Early Design Stages (Under the direction of Dr. Mihai A. Diaconeasa).

Human interventions are an integral part of any system, whether through design, operation, maintenance, or upgrading. Moreover, although the reliance on human intervention in safety-related actions in advanced reactors (e.g., Generation IV) is expected to be reduced or completely replaced by automated actions, nuclear power plants require human actions throughout their lifecycle from design, construction, operation, and decommissioning. Hence, the impacts of all operator actions are required to be captured and incorporated in the probabilistic risk assessment (PRA) of the modeled plant. Furthermore, a risk-informed and performance-based design and licensing approach expects that a PRA model, including human reliability analysis (HRA), is developed starting from the early design stages and used to inform all design iterations. However, due to the lack of details during the early design stages, HRA is often postponed until the design is mature enough.

Conducting HRA in the final design stages, though adequate in capturing pre-, at-, and post-initiators, comes short of informing the design itself in the iterative design lifecycle. Moreover, due to most HRA methodologies being developed utilizing mostly the operating experience of existing light water reactors, limited guidance is available to the applicability of different HRA methodologies during the early stages of the design. Limited guidance is available, as well, on how to utilize the results of HRA in informing the design of later iterations.

Hence, this study presents an investigation of the applicability of different HRA methodologies during the early stages of the design. The structure of a representative set of nine HRA methodologies is assessed against the available operating and emergency procedures within

different design stages. Furthermore, these different HRA methodologies are assessed based on the availability of guidance on how to use their results to risk-inform the design in an iterative design process.

Moreover, this study presents a framework to include HRA during the design's early stages, pre-conceptual and conceptual. The proposed framework provides a process for the screening of operator actions that do not contribute to the risk and the identification of all key operator actions that are critical to the safety of the design. The results of the framework are then used to risk-inform the design of those safety-related operator actions to update the design further. Then, using information from the updated design, this framework can be reapplied to investigate the impact of the design update on human reliability and human factors engineering program.

The PRA model of the X-energy's pre-conceptual Xe-100 high-temperature gas-cooled pebble-bed reactor (HTGR-PB) design is used to demonstrate the approach. In the pre-conceptual Xe-100 PRA model, also called Phase 0 PRA model, operator actions were considered an integral part of analyzing the plant response to the identified initiating events. In this study, all possible operator actions in the Xe-100 PRA model are identified, analyzed, and removed to emulate a design relying only on the available automated control systems. The preliminary outcome of the assessment showcases the inherent safety of the Xe-100 design even under the conservative assumption of crediting no operator actions. The results also list necessary event sequences in which operator actions are critical to the risk profile of the Xe-100 design.

OpenPHI – A Human Reliability Analysis Methodology to Risk-Inform the Importance of Operator Actions for Advanced Reactors during Early Design Stages

by
Mostafa Hamza

A thesis submitted to the Graduate Faculty of
North Carolina State University
in partial fulfillment of the
requirements for the degree of
Master of Science

Nuclear Engineering

Raleigh, North Carolina
2022

APPROVED BY:

_____	_____
Dr. Mihai A. Diaconeasa Committee Chair	Dr. Nam Dinh
_____	
Dr. Xu Wu	

DEDICATION

To my colleague, friend, love, and wife, Nermeen. You are my everything; thank you for just being you.

To my mom, Walaa, my dad, Mohamed, and my brother, Mahmoud. Thank you for supporting my dreams with your prayers and efforts.

To all my aunts. May Allah bless you with prolonged, joyful, and healthy lives.

To my little nephew, may your future be full of joy and achievements.

"إِنۡ أُرِيدُ إِلَّا ٱلۡإِصۡلَٰحَ مَا ٱسۡتَطَعۡتُۚ وَمَا تَوۡفِيقِيٓ إِلَّا بِٱللَّهِۚ عَلَيۡهِ تَوَكَّلۡتُ وَإِلَيۡهِ أُنِيبُ"

هود ٨٨

“I only intend reform as much as I am able. And my success is not but through Allāh. Upon Him I have relied, and to Him I return”

Hūd 88

BIOGRAPHY

Mostafa Hamza was born in Alexandria, Egypt's second biggest city, on March 19, 1993. He received his bachelor's degree in nuclear engineering from the Nuclear and Radiation Engineering Department at Alexandria University in 2016. Following his graduation, Mostafa continued serving the academic/higher education program in Egypt as a teaching assistant and lab instructor at Alexandria University and Zewail City of Sciences and Technology. His passion is in risk-informed reactor design; his short-term goal is to continue his post-graduate research, and his long-term dream is to keep pushing the field of probabilistic risk assessment further.

ACKNOWLEDGMENTS

I am so grateful to Dr. Mihai A. Diaconeasa for guiding my research and graduate journey as an advisor and friend. Also, I appreciate the valuable comments from my colleagues in the Probabilistic Risk Assessment Group at NCSU. Further, I thank the probabilistic risk assessment team at X-energy for their insights, expertise, and guidance.

I would like to thank Dr. Nam Dinh and Dr. Xu Wu, my committee members, for their insights and guidance in developing and finalizing this work.

Moreover, I am so grateful to Dr. Abdel Fattah Solyman and Dr. Yousry Azmy for their continuous and unconditional support and guidance throughout the hardest of times.

Finally, I would like to thank everyone who taught me even a single word. Without you all, I would not have been here. Thank you.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ANS	American Nuclear Society
AOO	Anticipated Operational Occurrence
ARDP	Advanced Reactor Demonstration Program
ASEP	Accident Sequence Evaluation Program
ASME	American Society of Mechanical Engineers
ATHEANA	A Technique for Human Error Analysis
BDBE	Beyond Design Basis Event
CBHRA	Computation-Based Human Reliability Analysis
CDF	Core Damage Frequency
CFM	Crew Failure Modes
CFR	Code of Federal Regulation
CPC	Common Performance Condition
CRD	Crew Response Diagram
CREAM	Cognitive Reliability and Error Analysis Method
CRT	Crew Response Tree
DBE	Design Basis Event
DT	Decision Tree
EC	Error of Commission
EFC	Error Forcing Context
EO	Errors of Omission
EPRI	Electric Power Research Institute
ES	Event Sequence

ET	Event Tree
F-C	Frequency-Consequence
FSAR	Final Safety Analysis Report
GOMS	Goals, Operators, Methods, and Selection
HEP	Human Error Probability
HFE	Human Failure Event
HRA	Human Reliability Analysis
HTGR-PB	High-Temperature Gas-Cooled Pebble-Bed Reactor
HUNTER	Human Unimodal for Nuclear Technology to Enhance Reliability
HVAC	Heating, Ventilation, and Air Conditioning System
IAEA	International Atomic Energy Agency
IDAC	Information-Decision-Action Crew
IDHEAS	Integrated Human Event Analysis System
IE	Initiating Event
INL	Idaho National Laboratory
LB-LOCA	Large-Break Loss of Coolant Accident
LBE	Licensing Basis Event
LERF	Large Early Release Frequency
LMP	Licensing Modernization Project
LOCA	Loss of Coolant Accident
LWR	Light-Water Reactor
MS	Mental State
MSIV	Main Steam Isolation Valve

NPP	Nuclear Power Plant
OCS	Operational Control System
OpenPHI	Open Preliminary Human Importance
PIF	Performance Influencing Factor
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment
PSRV	Pressure Safety Relief Valve
RB	Reactor Building
RCCS	Reactor Cavity Cooling System
RSF	Required Safety Function
SB-LOCA	Small-Break Loss of Coolant Accident
SMR	Small Modular Reactor
SPAR-H	Standardized Plant Analysis Risk Human Reliability Assessment
SU/SD	Startup/Shutdown System
THERP	Technique for Human Error-Rate Prediction
TRISO	Tri-Structural Isotropic
U.S. DOE	The United States Department of Energy
U.S. NRC	The United States Nuclear Regulatory Committee
VHTR	Very High Temperature Reactor

CHAPTER 1. INTRODUCTION

1.1. Background and Motivation

The human element has a critical impact in any complex engineering system throughout its life cycle. Whether during design, construction, operation, maintenance, or disassembly, human personnel are an integral part of the life cycle of most systems. Not even autonomous systems are completely immune from human impacts, since they rely on human inputs during software development, maintenance, and troubleshooting.

The impact of the human element increases in systems that may cause financial, mission, or safety losses. Hence, ensuring human reliability in those systems to prevent such losses is required; of that need emerged multiple fields including human reliability analysis (HRA). The nuclear industry realized the importance of the human factor early in its history. This is clear in the early publications of the industry itself and the regulatory bodies which assessed the impact of human reliability on the safety of nuclear power plants (NPP) [1]-[4].

In 1975, the first reactor safety study (WASH-1400) was issued in which the field currently known as probabilistic risk assessment (PRA) was pioneered. In WASH-1400, the concepts of PRA were utilized to realistically analyze the public risk associated with an accident in a commercial NPP [5]. Even within WASH-1400, the importance of human actions was not overlooked. The method developed by Swain in the 1960s [4] came in use in analyzing the human reliability within WASH-1400. A complete HRA was conducted in WASH-1400 which later became the technique for human error rate prediction (THERP) methodology [27].

However, despite having a myriad of HRA methods, an inherent aspect of most of these methods is that they were developed to model an existing NPP. Resources are available to use within the HRA that are not necessarily available during initial stages of the design. Operating procedures,

emergency operating procedures, and severe accident management guidelines are available for light-water reactors (LWR) with a long operational history that build the experience needed to build HRA models. However, for non-LWRs, especially those under design, such information may not be available to be utilized in building their associated HRA.

Moreover, both the Licensing Modernization Project and the PRA Standard for Advanced Non-Light-Water Reactor Nuclear Power Plants present a methodology to implement and utilize PRA during the development and licensing of advanced non-LWRs [7][8]. In both methodologies, the impact of human actions is expected to be assessed in each iteration of the plant design and used to inform the later iterations of the design.

1.2. Probabilistic Risk Assessment

The field of PRA came into light following WASH-1400 which assessed the risks associated with accidents in commercial NPPs. Despite having earlier studies, including WASH-740 and WASH-1250 [9][10], WASH-1400 was the first approach to comprehensively and realistically, rather than conservatively, estimate the risk associated with different accidents. To the surprise of the nuclear engineering community at the time, WASH-1400 concluded that small-break loss of coolant accidents (SB-LOCA) pose higher risk than this of large break loss of coolant accidents (LB-LOCA) [5].

To understand the conclusions of WASH-1400, the definition of risk needs to be presented following Kaplan and Garrick's most widely accepted definition of risk [11]. Risk is defined as a "complete" set of three parameters, along with any associated uncertainty, that is represented formally in Equation (1).

$$\boldsymbol{R} = \{< \boldsymbol{s_i}, \boldsymbol{p_i}, \boldsymbol{x_i} >\}, \qquad \boldsymbol{i} = \boldsymbol{1}, \boldsymbol{2}, \dots, \boldsymbol{N} \tag{1}$$

The three parameters form the answer to the three fundamental questions of risk analysis, which forms the goal of PRA as defined by the United States Nuclear Regulatory Commission (U.S. NRC):

- What can go wrong? The answers give the first parameter of scenario description (i.e., s_i).
- How likely can it happen? The answers give the second parameter of scenario probability estimation (i.e., p_i).
- And what are the consequences? The answers give the third parameter of scenario consequence evaluation (i.e., x_i).

In light of this definition, the conclusion remarks of WASH-1400 can be understood. Since the risk of any scenario is a combination of its likelihood and consequences, the risk associated with core melts resulting from the more probable SB-LOCAs is higher than the risk associated with the less probable LB-LOCAs. The results of WASH-1400 was supported during the Three Mile Island accident in which an SB-LOCA resulted in the melting of about two thirds of the core leading to the eventual decommissioning of the unit.

In LWRs, the U.S. NRC [12] and the International Atomic Energy Agency (IAEA) [13] divides PRA, or probabilistic safety assessment (PSA) for IAEA, models for NPPs into three levels. In the level 1 PRA, the model focuses only on sequences that could lead to damage to the reactor core estimating the core damage frequency (CDF). Whereas level 2 PRA/PSA models start from core damage and estimate the frequency of having release of radioactive material into the environment (i.e., large early release frequency) (LERF). Finally, level 3 PRA/PSA models start from release accidents and estimate the public doses and other environmental damage.

On the other hand, the proposed approach for non-LWR PRA in the Licensing Modernization Project (LMP) [7], which was endorsed by the U.S. NRC in the regulatory guide 1.233 [14], is to

assess the aggregate plant-level risk. This is done by identifying and assessing the licensing basis events (LBE) and investigating the entire scenario starting from initiating events (IE) and ending with end states that include public doses and other environmental damage. The consequence of the end state is then assessed resulting in a frequency-consequence pair associated with each LBEs. In other words, the PRA model of a non-LWR is the combination of level 1, level 2, and level 3 PRA of LWRs.

1.3. Human Reliability Analysis

Despite being highly automated systems, the importance of assessing human reliability in estimating the risk of NPPs was clear from the start of the nuclear industry. In fact, the main concepts that was utilized by WASH-1400 to assess human reliability were developed by Swain over a decade before WASH-1400 [2]-[4]. In WASH-1400, an entire special section was given to the approach used in assessing human reliability which was adequately titled “human reliability analysis”. Human intervention during automatic system malfunction along with human-system interactions during routine operation, testing, and maintenance were considered in the analysis conducted in WASH-1400.

Throughout the history of the nuclear industry, the impact of human intervention is clear. All three major nuclear accidents were either initiated, exacerbated, or alleviated due to human interventions. During the Three Mile Island accident, human actions played a critical role in the accident progression. Due to misdiagnosing the loss of coolant accident (LOCA), the operators throttled off the emergency core cooling system pumps to avoid the pressurizer going solid. Their decision resulted in uncovering the core due to a lack of coolant inventory [15]. Moreover, the Chernobyl accident was initiated due to the initiation of a test by the operator disregarding all operating procedures and safe practices [16]. Finally, during the Fukushima Daiichi accident, the

valiant efforts of the operators, despite very limiting conditions, managed to reduce the consequences of this accident [17].

Hence, HRA is the part of the PRA model that assess human reliability and its impact on the risk of NPPs. The main goal of HRA is to identify human failure events (HFE), which represent system failure or unavailability due to human action or inaction, and quantify human error probabilities (HEP), which represent the likelihood of human failure. HFEs include failing to initiate the correct action within specified timeframe or initiating incorrect actions. It should be noted that HFEs are categorized into three categories [8]:

- Pre-initiator (category A) HFEs: failures due to actions performed during maintenance or calibration prior the initiation of an event.
- At-initiator (category B) HFEs: failures due to actions that cause or contribute to the occurrence of an event with abnormal plant conditions.
- Post-initiator (category C) HFEs: failures due actions performed during the response to an event with abnormal plant conditions.

In general, the U.S. NRC, along with the nuclear industry, issued multiple guidance reports for good practices while implementing HRA, and PRA, in LWRs and non-LWRs [18][19]. The U.S. NRC also funded a project in which 10 HRA methodologies were compared against good practices issued in NUREG-1792 and the underlying model, strengths, and limitations associated with each methodology are identified [20]. Moreover, the LMP requires that the impact of human actions be captured as part of the programmatic defense-in-depth and as part of the uncertainty evaluation [7].

1.4. Nuclear Power Plant Design Stages

Similar to other large complex systems, NPPs go through multiple iterations of the design before commencing operation. Moreover, due to the strict regulations that NPPs follows, system designs may go through even more iterations within the same overall design iteration. From PRA perspective, the scope and fidelity of the PRA model will differ based on the design stage and the associated information available. It is expected that the PRA model scope would be very limited during the early design changes and progressively increase in scope, fidelity, and completeness as the design matures.

Within the scope of this study, the different stages of NPPs are assumed to be categorized as follows:

- Design stages: only paper designs are available with no associated constructions, which is further subdivided into:
    - Pre-conceptual design: only high-level low-fidelity information is available on the overall design of the NPP for a generic site, along with functional system requirements. The design is not mature enough to have detailed operational or emergency procedures.
    - Conceptual design: only high-level low-fidelity information is available on the overall design of the NPP for a bounding site, along with a mix of high-level system designs and safety functional system requirements. The design is not mature enough to have detailed operational or emergency procedures, however high-level operator actions that support safety functions are identified.
    - Preliminary design: a mix of low- and high-fidelity information is available on the overall design of the NPP for a bounding site with a prospective specific site, along

with high-fidelity system designs. The design is mature enough to have limited, high-level operational and emergency procedures.

  - Final design: site-specific high-fidelity information is available on the overall design of the NPP, along with high-fidelity system designs. The design is mature enough to have detailed operational and emergency procedures.

- Construction stage: construction activities associated with a specific site being following the final design.
- Commissioning stage: construction activities are complete and required safety tests and other pre-operational, including fuel loading, activities being.
- Operational stage: operation and electricity/heat production activities begin, along with any necessary intermittent maintenance activities.
- Decommissioning stage: electricity/heat production activities stop, fuel is removed, and decontamination and disassembly activities begin.

It should be noted that, within the scope of this study, the early stages of design are both pre-conceptual and conceptual design stages, in which no or extremely limited information is available regarding the expected human operator actions. Moreover, the design goes through multiple changes, updated, and iterations through all design stages until reaching the final design.

According to the ANS/ASME PRA standard for advanced non-light-water reactor nuclear power plants, simply mentioned in this study as the non-LWR standard, there are two capability categories for PRA depending on design maturity. Capability Category I limits the scope and the fidelity of the PRA to identify important IEs, event sequences, and HFEs using generic plant models. Whereas Capability Category II expands the scope and fidelity to cover all risk-significant contributors using plant-, site-, or design-specific models. Figure 1 depicts the different stages of

an NPP project, including the Capability Category associated with each step [73]. It should be noted that, depending on design maturity, other systems can fall within different Capability Categories in the same design stage.

Figure 1. Project Stages and The Associated Capability Category.

During the early years of NPPs development, conservative deterministic safety analysis and safety margins dictated the design of different systems in each of these iterations. However, starting with WASH-1400, the U.S. NRC started implementing reliability and quantitative risk assessment techniques to "perform realistic assessment as opposed to the conservatively-oriented safety" [5]. However, most of the PRA studies conducted ever since were implemented for NPPs at the operational stage [5][10][21]. Therefore, very limited guidance is available on the use of PRA, not to mention HRA, in informing the design. In fact, the first regulatory mention of the idea of "risk-informing" came in the U.S. NRC memorandum in November of 1993 concurring "the need to systematically expand the use of PRA within the agency," which started the PRA implementation plan, improved into risk-informed regulation implementation plan, and finally retitled into the risk-informed performance-based plan since 2007 [22]-[24].

1.5. Research Objectives

As can be seen, the applicability of different HRA methodologies were not needed to be investigated. Due to PRA being retroactively applied to NPPs during the operational stages, the inputs of PRA were limited to update specific systems in those NPPs as what happened following

the three major nuclear accidents [15]-[17]. The lack of information served as a deterrent in utilizing PRA, and HRA specifically, during the early stages of design. However, with the current push towards risk-informing the design and towards having PRA supporting the licensing of NPPs, it became more and more important to apply PRA during all stages of the design. One area of concern with the new push on risk assessments is that there is no guidance available on whether different HRA methodologies are applicable during different stages of the design.

Hence, the work presented in this study assesses the applicability of different HRA methodology during the early stages of design. Multiple HRA methodologies are chosen based on their wide use in the industry or academia which can be deemed as a representative set of most approaches. Moreover, a framework is presented that applies and utilizes HRA to inform the design during all stages of design, which fulfils the regulatory expectations from HRA allows for the inputs of HRA to inform later design stages. Finally, a conservative HRA methodology is presented to fill the gap identified in this study and to be implemented during the early stages of design which have limited information regarding the operational and emergency procedures. Using the presented methodology allows the identification of important operator actions which is used as inputs for later design stages. It should be noted that, despite using the non-LWR standard in developing this study, the presented methodology can be implemented to any NPP regardless of the specific technology.

1.6. Overview of Thesis

Following the introductory chapter, in which a general overview of the motivation, contribution, and background of this work, CHAPTER 2 studies the applicability of different HRA methodologies. Also, in CHAPTER 2 an overview of the methodology history, basic structure, and general high-level advantages and limitations is presented. In this chapter, a representative set

of the most widely used HRA methodologies are analyzed to cover different generations of HRA methodologies.

CHAPTER 3 presents the framework developed to implement HRA during different stages of design. The chapter starts by presenting the regulatory expectations from the HRA element in the PRA model. It is followed by the open preliminary human importance (OpenPHI) framework that presents both the iterative HRA approach to informing the design and the conservative HRA methodology to be implemented during the early stages of design, i.e., the pre-conceptual and conceptual design stages. The chapter then presents a high-level comparison between different HRA methodologies with respect to their applicability during the early stages of design.

Moreover, CHAPTER 4 presents a case study of the framework presented in this thesis. The chapter starts by presenting a brief background information of the Xe-100 whose pre-conceptual design is used in demonstrating the OpenPHI framework. Following that, a specific example is given on applying OpenPHI in one of the event sequences identified for the Xe-100. The chapter concludes by presenting the aggregate results obtained from applying the OpenPHI methodology to the proprietary pre-conceptual design of the Xe-100. Finally, CHAPTER 5 presents the expected limitations of the OpenPHI along with some concluding remarks and suggestions for improvement and future work.

CHAPTER 2. HUMAN RELIABILITY ANALYSIS METHODOLOGIES

Development of HRA methodologies began in the 1960s and continued ever since, with a myriad of methodologies developed through the past couple of decades. However, investigating all HRA methodologies is a daunting task that is outside the scope of this study, especially considering that some of these methodologies are proprietary while others have quite limited guidance. Hence, nine HRA methodologies were chosen for the analysis conducted in this study. These methodologies are considered a representative set of most approaches in HRA as will be clear by the end of this chapter. Moreover, the set spans the, so-called, three generations of HRA methodologies [25]: first generation HRAs (e.g., THERP), second generation HRAs (e.g., CREAM, ATHEANA), and third generation HRAs (e.g., IDAC, Phoenix).

In this chapter, a brief history of each of the methodologies under study is presented, along with an overall description of its basic structure. The general high-level advantages and limitations of each method are also presented whenever enough literature is available. Finally, the applicability of each methodology is investigated and the verdict of its applicability during the early stages of design, which is the scope of this study, is given.

2.1. THERP

Initially developed in Sandia National Laboratories, the technique for human error rate prediction (THERP) is one of the earliest methods developed for HRA. The basic assumption of THERP is that, depending on the type, human errors occur at constant rate. Hence, by decomposing a task into its low-level elementary subtasks, HEPs can be quantified using the estimated nominal probability of failure in each subtask [26]. Associated with these nominal probabilities are multiple performance shaping factors (PSFs), stress etc., that impact human performance and HEPs.

Despite having many variations in its implementation, THERP's basic structure, shown in Figure 2 [27], consists of:

- A familiarization step consisting of either plant visits or reviewing the system analysis.
- A qualitative assessment step in which the task is analyzed and decomposed and the HRA event tree is developed for the task.
- A quantitative step in which nominal HEPs are assigned to a task, estimating the impact of PSFs, assessing the tasks dependencies, quantifying the success and failure probabilities, and assessing the impact of recovery actions.
- An implementation step in which any required sensitivity analysis is conducted and the results of the HRA is presented to the system analysts.

THERP is a comprehensive methodology developed in over a decade by Swain & Guttmann [27], and is one of few methods that emphasizes error recovery. Recovery actions are considered in a proceduralized task where an operator might notice an error in one of the procedures in a later step. Error recovery will result, if neglected, in an overestimation of human errors in any proceduralized task. Dependency is another area that is quantitatively considered by THERP, among few other HRA methods, in its methodology. In THERP, five dependence levels are considered between actions ranging from zero to complete dependence. By considering the dependencies, THERP manages to capture any interdependency between different actions within a task.

THERP is one of the most comprehensive HRA methods developed, with advantages including being well-used in practice, and a pioneer in considering both error recovery and dependencies. However, THERP suffers from the lack of cognitive modeling capability forcing it to be "regarded as a practical method of predicting human reliability rather than as a hypothetical model" [27],

requiring considerable resources in some models, and lack of guidance regarding the implementation of PSFs [29].

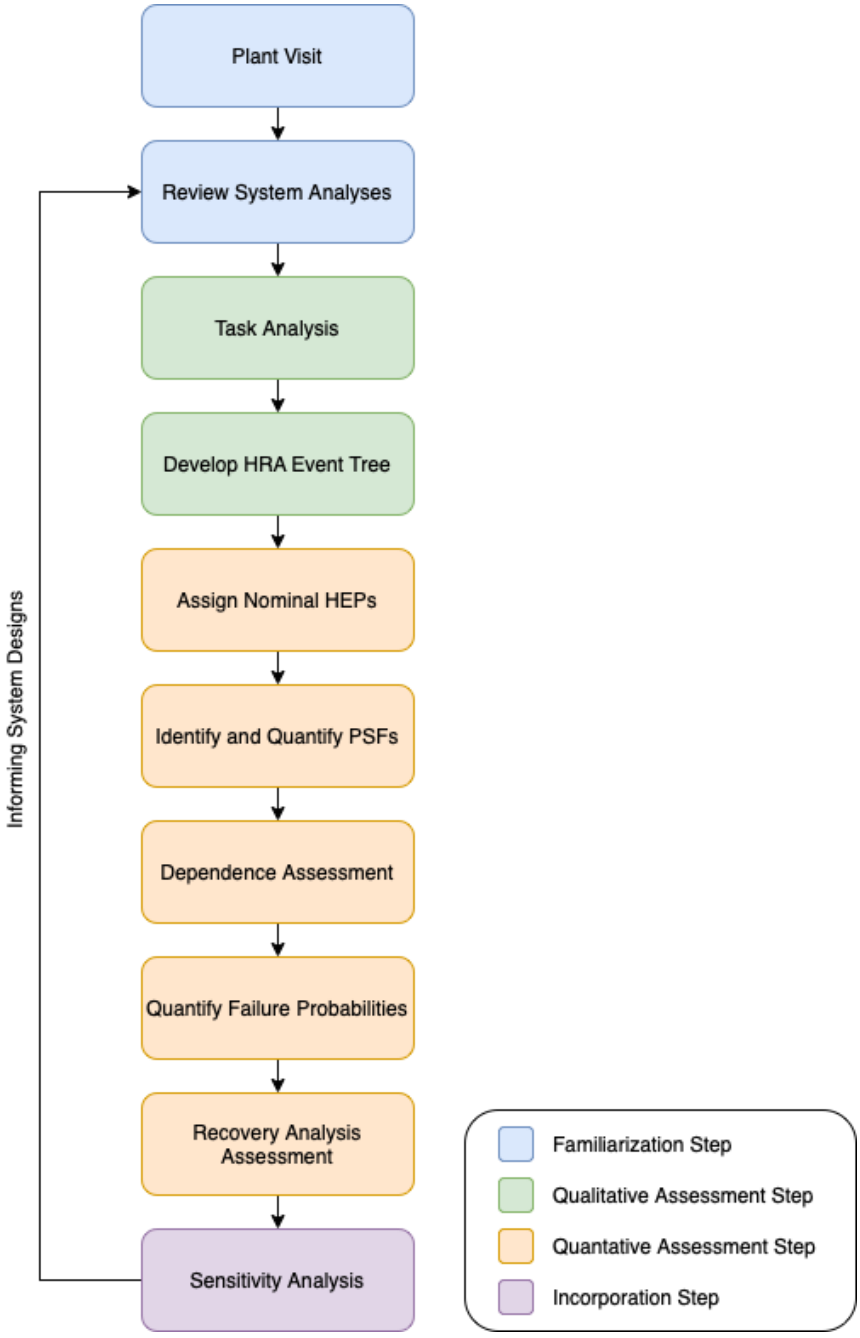

Figure 2. The Basic Structure of THERP.

However, THERP utilizes the method for man-machine task analysis [28] to decompose the task to its related human operations. Although it can be used during high-level analysis, some of the

human tasks may only be known as functional events without concrete knowledge of associated sub actions. This is evident in the use of HRA event trees in THERP, which are a form of event trees that tracks correct and incorrect performance within a specific task and relies heavily on the task decomposition conducted in the task analysis step.

Finally, THERP emphasizes the importance of conducting different sensitivity analyses to assess the impact of different assumptions or the impact of different human actions. THERP also provides an approach to screen different human tasks that have low impact on the system failure. However, THERP does not present a concrete guidance on how to assess the impact of these tasks, nor does it present a guidance on which tasks can be screened out. Hence, although the screening approach in THERP can still be used during the early stages of the design, guidance is still needed on implementation.

2.2. ATHEANA

Initially developed in Brookhaven National Laboratory, a technique for human error analysis (ATHEANA) is based on a multidisciplinary framework that accounts for human-centered factors along with situational conditions to identify error forcing contexts (EFCs). ATHEANA was developed to address errors of commission, realistically model the human-system interactions, and implement recent developments in other fields [30]. Hence, the ATHEANA methodology consists of the following steps [31]:

- An identification step in which possible HFEs are identified along with their associated unsafe actions that could result in HFEs from the PRA scenario.
- An analysis step in which EFCs associated with each unsafe action are identified and the probability of each EFC is quantified.

- A quantification step in which the probability of all possible EFCs is used to quantify the associated HEP.

One of the motivations behind ATHEANA's development is the explicit treatment of errors of commission along with the contextual analysis, which are two of the main advantages of ATHEANA. However, ATHEANA suffers from the limited theoretical basis of its quantification approach, along with requiring considerable resources to build the required knowledge/expertise [32]. Hence, even though ATHEANA presents an improvement to THERP on some fronts, like the treatment of errors of commission, it is a less applicable method than THERP during the early stages of the design.

2.3. SPAR-H

Standardized plant analysis risk human reliability assessment (SPAR-H), developed by Idaho National Laboratory (INL), subdivides human tasks into action and diagnosis tasks, while also accounting for contextual and environmental factors. Within SPAR-H, action tasks are defined as carrying out one or more activities where diagnosis tasks are defined as understanding existing conditions, planning, and prioritizing activities. Action tasks are assigned a nominal generic HEP of 1.0E-03 where diagnosis tasks are assigned a nominal generic HEP of 1.0E-02.

To account for environmental factors, SPAR-H utilizes nine PSFs which were derived from psychological research on human error. The PSFs include available time, stress, complexity, experience, procedures, ergonomics, fitness for duty, and work processes. Out of the nine PSFs, only available time, stress, and complexity are assessed in a basic SPAR-H model. The remaining five are considered plant specific and usually conducted when a plant-specific model is developed. Dependencies are modeled, to some level, in SPAR-H by a dependency model that mimics THERP's that ranges from zero to complete dependence [31].

The SPAR-H method consists of the following steps [34]:

- A categorization step in which the HFE is categorized into diagnosis, action, or both, and assigned a nominal HEP.
- A PSF identification step in which all PSFs that impact, either negatively or positively, the HFE is identified.
- A modification step in which the initial nominal HEP is modified to account for the impact of the relevant PSFs.
- A dependence evaluation step in which the dependence between different HFEs is assessed and the HEP is modified accordingly.
- A screening step in which a cutoff value is used to prevent the consideration of incredible HFEs which have infinite number of potential failure mechanisms, like an operator having a heart attack.

The advantages of SPAR-H include the ease of use and trace, covering many situations through its nine PSFs, and accounting for the dependencies in both subtasks and event sequences [35]. In addition, SPAR-H can be utilized by both HRA experts and operators with no background in HRA alike since the documentation provides sufficient guidance for analysis [26]. Unfortunately, SPAR-H suffers from the limited PSFs that might be inadequate for detailed analysis, and not being clear for the selection of their database values [35].

Although SPAR-H does not provide any guidance on the level of task decomposition needed, it is clear that "the analyst needs considerable knowledge of the tasks and contexts to be rated" [31]. This is evident by the reliance of SPAR-H on other techniques, like ATHEANA (section 2.2), to acquire the needed knowledge to implement SPAR-H. Moreover, although SPAR-H consider the

treatment of incredible HFEs, this is done on an HFE level; no guidance is given on assessing the impact of a certain HFE on the overall plant response.

2.4. CREAM

Cognitive reliability and error analysis method (CREAM) is a bidirectional analysis that can be utilized both in retrospective analysis as well as predictive analysis. Developed in 1993, CREAM differentiates between competence, a person's skill and knowledge, and control, a continuum from no control to complete control based on context. The contextual factors that decide the level of control (i.e., control mode) is defined as common performance conditions (CPCs) which include adequacy of organization, working conditions, adequacy of man-machine interface, availability of procedures, number of simultaneous goals, available time, time of day, adequacy of training, and crew collaboration quality [36].

CREAM also differentiates between genotypes (causes) and phenotypes (manifestations). Genotypes are divided into having direct/indirect link to behavior (first category), man-machine interface related (second category), and environmental/organizational related (third category). Whereas phenotypes, which are the consequences of human behavior, are divided into actions at the wrong time, actions of the wrong type, action at the wrong object, and finally actions in the wrong place [36].

The CREAM consists of the following steps [37]:

- A task analysis step in which the task is analyzed and decomposed, and the associated CPCs are extracted.
- A CPCs assessment step in which the impact level of relevant CPCs is assessed and quantified.

- A categorization step in which the control mode is determined based on the task analysis and the associated CPCs.

CREAM's advantages include providing a cognitive and contextual control model [37], and the flexibility of implementations like the study conducted in [39]. Despite multiple studies utilizing it [40]-[43], CREAM suffers from very limited development, and lack of validation and clear guidance [40]. Moreover, the developer of CREAM no longer considers the methodology itself to be relevant. According to [44], due to focusing on how actions fail rather than performance, focusing on the human component only, and lacking clear support to the concept of error, "Although CREAM still appears to be used and referenced, it is only fair to point out that the method from [Erik Hollnagel's] point of view is obsolete." Furthermore, the level of detail required from the task analysis to determine the control mode renders CREAM at the same level of applicability, during early stages of the design, as the previous methodologies. However, the lack of guidance, support, and development reduces its applicability even further during all other stages.

2.5. Phoenix

The model based HRA methodology, named Phoenix, was developed by Ekanem et. al. to overcome the limitations of other model-based methods. The limitations include the lack of theoretical and experimental basis for the method's assumptions, the lack of causal model, the simplistic approach of performance influencing factors (PIFs) which are similar in definition to PSFs, and/or the subjectivity of the expert elicitation process required for estimating HEPs. Utilizing a 5-step qualitative framework, Phoenix identifies possible HFEs and characterizes the scenarios that might lead to these HFEs.

The qualitative analysis of Phoenix consists of analyzing the PRA scenarios along with their associated ETs to extract possible HFEs, developing the crew response trees (CRTs) based on task

analyses associated with each possible HFEs, identifying possible crew failure modes (CFMs) for CRTs, and building the failure logic model (i.e., fault tree) of each HFEs, identifying CFM/PFS interdependencies, and developing HFE scenarios. These broad steps include several sub-steps that when applied properly, according to the method's developers, provide extensive HFE scenario analysis [45].

To quantify HEPs at each HFE, an analyst starts by identifying possible (relevant) CFMs that could result in this specific HFE followed by identifying possible (relevant) PFSs that impact the CFMs under investigation. The following step in the quantitative analysis is to determine the temporal order of those relevant CFMs and estimate the conditional probability associated with each CFM utilizing a Bayesian belief network connecting all PIFs. Finally, the analyst can estimate HEPs associated with each HFE by implementing the conditional probabilities quantified in the previous step along with the cut sets associated with each HFEs. Figure 3 gives a high-level overview of the Phoenix qualitative and quantitative methodology. Diaconeasa [46] improved and demonstrated the methodology on a wide range of operator actions during emergency operations and maintenance operations for design basis and beyond design basis accidents due to internal and seismic events.

As depicted in Figure 3, the Phoenix methodology, even with simplification, requires high degree of system, scenario, and procedures familiarity. The level of detail needed is evident by the task decomposition step within the step of developing CRTs, in which "procedures are used to provide explicit step-by-step guidance required by the crew in completing the safety function." [45] Furthermore, going deeper into PFSs identification requires more detailed procedures and further complicates the analysis. More complications arise further going into the quantitative analysis in which estimating conditional probabilities presents a challenge even to familiar procedures. All

these issues accompanied with the limited benefit obtained from having such a high-fidelity methodology result in the limited applicability of the Phoenix methodology during the early stages of the design.

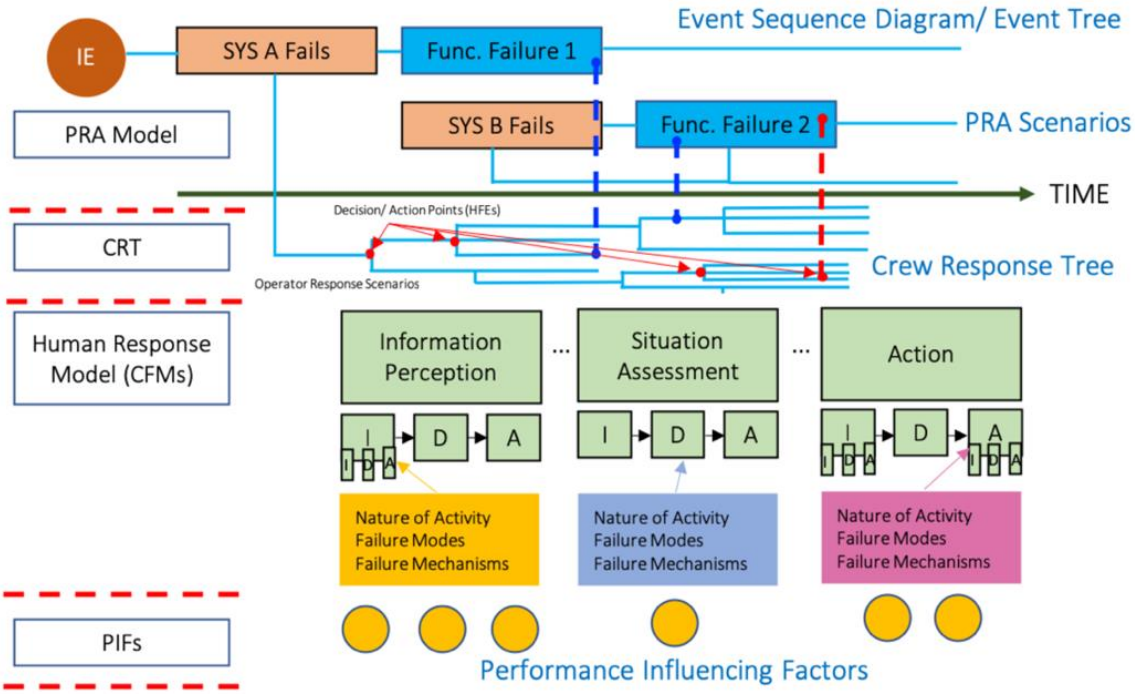

Figure 3. The Phoenix Qualitative Analysis Framework Layers and A Typical PRA Event Sequence Mode. Reprinted with permission from [46].

2.6. IDHEAS

The integrated human event analysis system (IDHEAS), developed by Electric Power Research Institute (EPRI) and the U.S. NRC, focuses on reducing the variability within HRA hence increasing the consistency of the HEP estimates resulting from it [47]. Within IDHEAS, a similar process to that of Phoenix is implemented in which HFEs are identified from the PRA scenario, crew response diagram (CRD) is developed through which CFMs are identified, and decision trees (DT) are built to quantify the associated HEPs.

The IDHEAS method consists of the following steps [47]:

- A scenario analysis step in which the PRA scenario is analyzed to identify possible HFEs.
- A task analysis step in which a CRD is developed for each HFEs and the associated CFMs are identified.
- A CFM analysis step in which all associated PIFs that could impact the CFM are identified and an associated DT is built.
- A quantification step in which the paths within DT that would result in CFM are identified and the associated HEP is quantified.

The advantages of IDHEAS include having a structured qualitative analysis framework, the implementation of a causal cognitive model, and having a clear, formal, and traceable approach. On the other hand, IDHEAS suffers from subjectivity of PIF levels evaluation, limited guidance on task analysis and building CRDs, and the limitation associated with the binary approach of the DTs that limits the consideration of PIFs to only success or failure [48]. Similar to Phoenix, IDHEAS is a resource intensive method that suffers from the same limitations in its applicability during early stages of the design.

2.7. IDAC

The information-decision-action crew (IDAC) HRA method simulates the operator decision making process during accident scenarios. IDAC is based on results from the fields of cognitive psychology, behavioral science, neuroscience, human factors, field observations, and various other HRA methods. Through a few fundamental behavioral rules that govern the dynamic response of the operator, IDAC can simulate complex operator performance. The simulation is possible due to the high level of regulation to the actions of the operator within the nuclear industry.

Utilizing four modeling blocks, IDAC consists of an information processing block (I), problem-solving and decision-making block (D), and action execution block (A), and the mental state block

(MS) [49]. The interaction between the MS block and the I, D, and A blocks is a dynamic two-way interaction in which the mental state influence the operator activities and the activities influence the mental state. IDAC covers situation assessment, diagnosis, and recovery actions in its simulation of operator performance. Due to the complexity of internal rules, quantity of input/output information, and its probabilistic response generation, IDAC method can only be implemented through simulation [50].

By realistically simulating the operator mental state and activities using a set of causal models, IDAC presents the finest resolution in HRA analysis among all other methods. However, being a model based HRA method, IDAC suffers from the same disadvantages of Phoenix. Furthermore, being a high-fidelity HRA method in which the operator mental state and activities are continuously simulated, IDAC requires more resources than any other HRA method discussed in this study making it unapplicable during the early stages of design.

2.8. ASEP

Accident sequence evaluation program (ASEP) method was developed as a simplified and less resource-intensive version of THERP. ASEP includes a detailed screening for pre- and post-accident tasks with separate HEPs for each. Whereas, with THERP, HEPs are calculated by the analyst, ASEP utilizes a predefined HEPs for pre- and post-accident tasks. The simplification increases the speed and the simplicity of the analysis at the expense of accuracy [26]. ASEP categorizes errors according to tabular definitions which ensures the consistency between different analysts as long as they agree on the same category. In addition, the use of tables for calculations eliminates any ambiguity in calculation of HEPs.

ASEP's advantages include the speed and ease of use, the ability to be computerized [29], accounting explicitly for all except for open-ended PSFs [26]. However, ASEP suffers from having

more conservative error estimation and less accurate results than THERP. It should be noted, however, that both ASEP and THERP can be combined, where ASEP is used for screening and THERP is used for risk significant errors [29].

Although ASEP utilizes a conservative screening approach that requires limited resources, no clear guidance on the screening criteria is given [51]. Hence, even though ASEP is the most applicable method, out of all investigated methodologies in this study, during the early stages of design, this applicability is still hindered by the lack of clear guidance on how to utilize the results of the analysis to inform the design.

2.9. HUNTER

The human unimodal for nuclear technology to enhance reliability (HUNTER) includes a simplified cognitive model based on cognitive psychology and human performance modeling. HUNTER, like IDAC, falls into the simulation-based category of HRA methods. This category, which is also known as computation-based HRA (CBHRA), relies on simulating an interface between a virtual operator with a realistic thermal-hydraulic system code.

Utilizing the goals, operators, methods, and selection rules method (GOMS), operator action types are categorized into actions, checking, retrieval, instruction communication, selection, and decisions. Using these types, all procedure steps can be decomposed to their elemental types. While quantifying HEPs, HUNTER utilizes legacy methods, mainly THERP, as a starting point for quantifying GMOS which are then used in quantifying HEPs [52].

Aside from high-level information in [52]-[54], no complete guidance is available for HUNTER. However, being a simulation based HRA method, HUNTER suffers from the same limitations as IDAC. Moreover, being in development, HUNTER lacks the necessary guidance, until the time of

this study, to being implemented during any stage of the design which renders it less applicable than IDAC.

2.10. Summary

As previously described, nine HRA methodologies are investigated concerning their applicability during the early design stages. Only ASEP is applicable during the conceptual design stage because it requires limited knowledge of the operating and emergency procedures. Such information is developed with low fidelity during the conceptual design stage. However, all investigated methodologies, including ASEP, lack the guidance and criteria to identify critical operator actions, especially for non-LWRs. Moreover, all analyzed methodologies are not applicable during the pre-conceptual design stage, in which no information about operating or emergency procedures is available. Hence, the methodology presented in CHAPTER 3 addresses this gap and introduce a framework to use HRA results to inform the design during all stages of design, especially the pre-conceptual and conceptual.

CHAPTER 3. OPENPHI

As can be seen in CHAPTER 2, despite the myriad of HRA methodologies available to use, all but one method cannot be applied during early stages of design. Of all HRA methodologies discussed, only ASEP requires limited resources that allows for its application during the early stages of design. However, even ASEP has limited guidance on how to apply it and utilize its results to inform the design. Hence, a need arises of an HRA method that can be applied during the early stages of design, along with a guidance on how to identify important operator actions that can be then used to modify/update the design. It should be noted that, as described in section 1.4, the design is expected to go through multiple iterations through the pre-conceptual, conceptual, and preliminary design stages increasing in fidelity until reaching the final design.

In CHAPTER 3, a framework is presented that combines a high-level conservative HRA methodology with a detailed steps on how to identify important operator actions and utilize the results in updating the design in compliance with all regulatory expectations. In section 3.1, the regulatory expectation from the HRA conducted within the PRA model are presented. In section 3.2, the framework of open preliminary human importance analysis (OpenPHI) is presented, which is followed by a high-level overview of the applicability of all HRA methodologies presented during the early stages of design in section 3.3.

3.1. Regulatory Expectations

As previously described, WASH-1400 was the first study to apply the PRA concepts to NPPs, where NUREG-1150 augmented that by analyzing 5 existing NPPs. After TMI-2, the importance of PRA became evident to the community with multiple analyses, public and proprietary, ensuing. Moreover, the U.S. NRC issued a memorandum in November of 1993 concurring “the need to systematically expand the use of PRA within the agency”, which started the PRA implementation

plan, improved into risk-informed regulation implementation plan, and finally retitled into the risk-informed performance-based plan since 2007 [55]-[57].

In June of 2020, the U.S. NRC issued the initial revision of the regulatory guide 1.233 [58], which endorsed the approach presented by the LMP [59][60]. This report presented a "guidance on using a technology-inclusive, risk-informed, and performance-based methodology to inform the licensing basis and content of applications for non-light-water reactors (non-LWRs) […]. This [regulatory guide] may be used by non-LWR applicants applying for permits, licenses, certifications, and approvals under Title 10 of the Code of Federal Regulations (10 CFR) Part 50, […] and 10 CFR Part 52 […]" [58][61][62]. These documents require that the impact of human actions be captured as part of the programmatic defense-in-depth. The LMP also involves the inclusion of human actions as part of the uncertainty evaluation.

In addition, part of the final safety analysis report (FSAR) of any licensing application, as required by 10 CFR Part 52 [5,6] and 10 CFR Part 53, is a complete assessment of the risk associated with the design including HRA. Another expected part of the licensing application is the human factors engineering program that ensures high personnel performance and feeds into the development of HRA through a bidirectional iterative process [7,8]. Furthermore, the non-LWR standard lists technical requirements for the 18 elements needed to develop a full-scope PRA [9]. The standard defines two PRA Capability Categories, CC-I and CC-II, based on plant-, site-, or design-specific models to represent the risk profile of the plant in a realistic way. By following CC-I requirements, most risk significant events can be identified, whereas following CC-II requirements will result in a more detailed, specific, and realistic risk profile assessment. Human actions are integral to all 18 PRA elements, with the element (f) being responsible for HRA and should be captured in both capability categories.

3.2. OpenPHI [73]

Current HRA methodologies require well-established design information, emergency operating procedures, and severe accident management guidelines of the current generation LWRs. However, for advanced reactors, either LWRs (e.g., NuScale, BWRX-300, SMR-160) or non-LWRs (e.g., Aurora, Hermes, Natrium, Xe-100, eVinci), the details of the procedures differ greatly depending on the design stage. Due to limited operating experience, the plant control philosophy and the written procedures are limited in the early design stages of advanced reactors.

Furthermore, due to the simplicity of the design, reliance on passive systems, and limited required operator actions, it is expected that advanced NPPs will have a reduced number of licensed control room staff compared to LWRs. The effort to obtain approval for reduced control room staffing, under Conditions of Licenses 10 CFR 50.54, is currently underway, with NuScale Power, LLC the first to submit a topical report to justify their control room staffing plan for their NuScale plant. NuScale argues that only three operators can operate up to 12 modules from a single control room [63]. For these reasons, performing HRA for advanced NPP is usually deferred to later in the design lifecycle, preventing HRA from informing the design and procedures at early design stages. In this section, we present an iterative framework to implement HRA during all stages of design, ranging from pre-conceptual to final design. This approach utilizes available design information and available plant control philosophy to assess the impact of operator actions on the risk profile of the design. Using this approach, all critical operator actions can be identified early in the design. These human actions can then be accounted for in later stages of the design. Figure 4 illustrates the steps of the proposed framework. It also indicates that this is an iterative process throughout all stages of the design.

Step 1: Evaluate Plant Design

In this step, the design stage of the plant is evaluated. As mentioned previously in Figure 1, the design stage is considered per system. Some systems can have a more mature design in comparison with other systems. The plant design maturity is assessed, based on design maturity of the systems delivering safety functions, plant control philosophy, and emergency operating procedures to decide whether enough information is available to support a full high-fidelity HRA.

Step 2: Design Maturity Assessment

At this decision point, using the results of the previous step, the design maturity of the current design stage is assessed. If the design stage is mature enough to support a full HRA using legacy methods, then a full high-fidelity HRA is conducted and used to inform the design in the following stages. This is conducted by comparing the available information from the current design stage against the HRA method's requirements, for example THERP's task analysis step "involves determining the detailed performance required of people and equipment, and the effects on them of environmental conditions, malfunctions, and other unexpected events. Within each task, behavioral steps are analyzed for the perceptions, decisions, memory storage, and motor outputs required, as well as for expected errors" [27]. On the other hand, if one or more of the elements required to perform a full HRA lack the required maturity to support a full HRA, the proposed framework is utilized.

Step 3: Identify and Categorize Human Failure Events

In the early design stages, utilizing systems analysis and event sequence analysis, all necessary human actions are identified for all postulated IEs. These actions are required to support the required safety functions (RSFs) of each system and can be categorized into two categories:

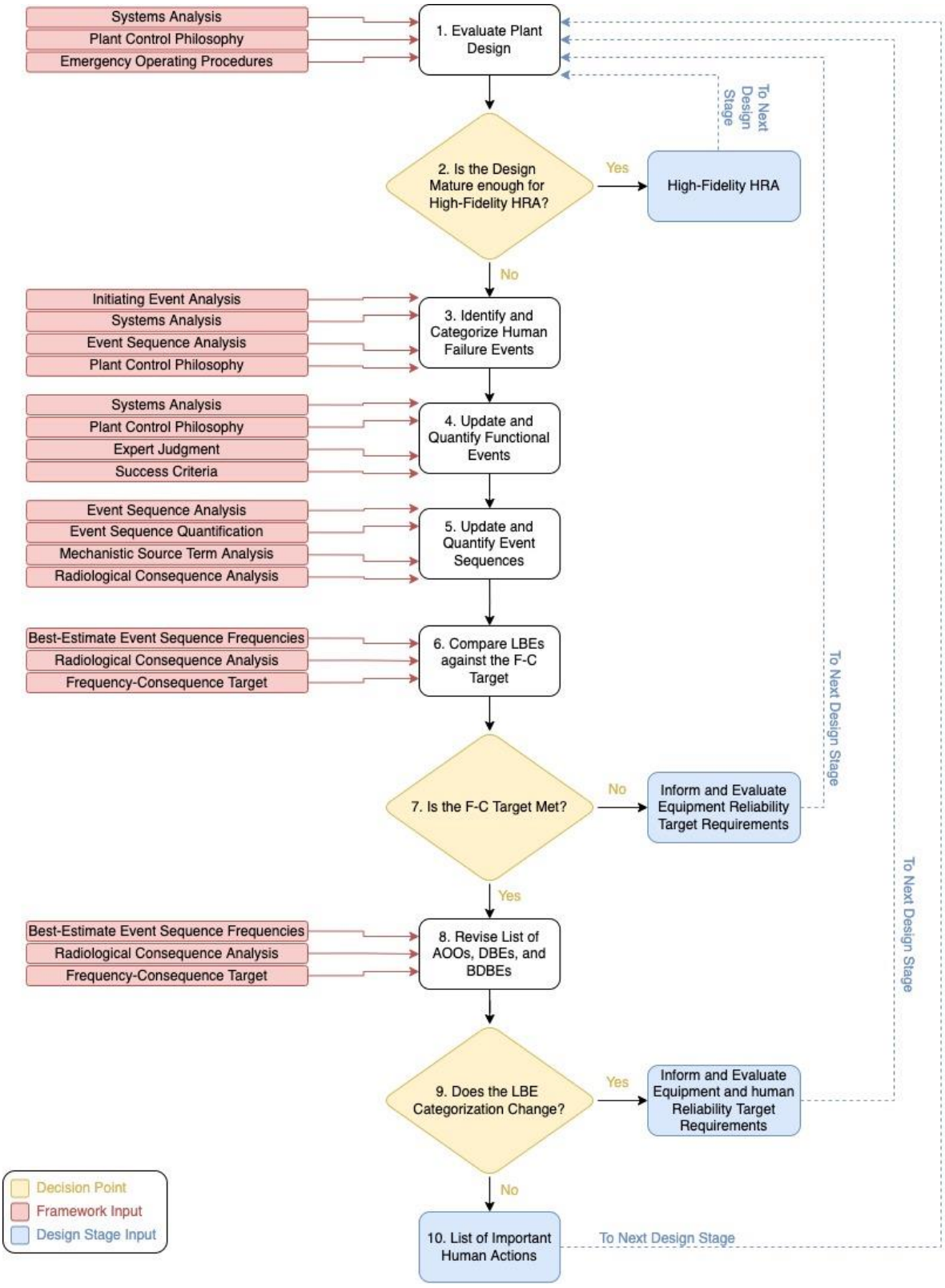

Figure 4. Framework for Assessing Operator Actions' Impact on the Licensing Basis Events.

- Primary actions: represent actions in completely manual systems that rely entirely on human intervention, e.g., opening/closing a manual valve.
- Secondary actions: represent actions that support an already automated system; these actions are only used in case of a failure of the automatic actuation of the system, e.g., manually tripping the reactor.

Step 4: Update and Quantify Functional Events

The next step is to assume no operator or operator failure to perform the required actions. Using this assumption, the probability of failing to achieve the RSF of a particular system can be calculated. This step can be performed, depending on the action categorization, using one of the following approaches:

- For primary actions:
    - Approach I: systems relying on primary actions are assumed to fail; the RSFs associated with these systems are supposed to not be achieved.
- For secondary actions:
    - Approach II: highly automated systems that depend minimally on human intervention are assumed to be fully automated; the RSFs associated with these systems are considered to rely on the reliability of the automatic actuation.
    - Approach III: partially automated systems, where human intervention constitutes part of their reliability, are assumed to be a combination of fully manual and fully automated subsystems; the RSFs associated with these systems are considered to entirely depend on the reliability of the fully automated actuation.

Step 4 utilizes available system analysis, success criteria, plant control philosophy, and procedures. Depending on the design stage, more realistic assumptions can be incorporated into approaches I,

II, and III to represent the systems better. Furthermore, this step can be combined with conservative assumptions, regarding the RSF reliance on manual interventions, to prove that safety goals are met without reliance on human intervention. Figure 5 illustrates how to implement the three approaches to calculate the probability of failure, P(F), to achieve the RSF.

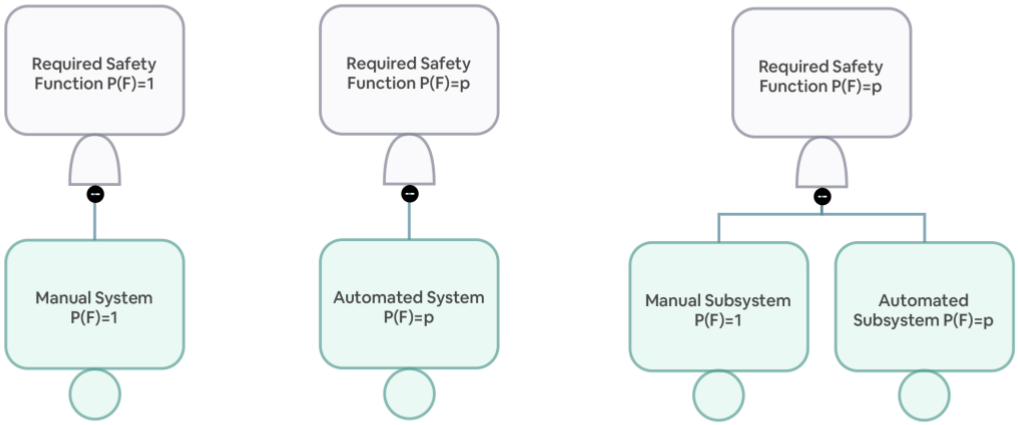

Figure 5. Required Safety Function Failure Probabilities (a) Approach I, (b) Approach II, and (c) Approach III.

Step 5: Update and Quantify Event Sequences

The following step is to implement the new failure probabilities of the RSFs in the event sequence analysis and the event sequence quantification using event trees (ETs). Moreover, the impact of HFEs on the consequences is also assessed in which human actions may result in exacerbating the event progression, like TMI, leading to a change in the end state of a branch.

The results of this step are a new list of LBEs frequencies, and consequences if applicable, for the design without crediting any human action. Depending on the assumed system response, the LBE:

- Remains unchanged for sequences with responses from fully or highly automated systems.

- Gets removed, zero frequency, for sequences with a successful response from fully manual systems.
- Increases in frequency for sequences with responses from partially automated systems.

Step 6: Compare LBEs against the Frequency-Consequence Target

In Step 6, the updated frequencies of the LBEs are compared with their original frequencies, which include human actions, and compared with the frequency-consequence (F-C) target and cumulative risk target of the LMP process. According to [7], "the F-C Target is selected such that the risk, defined as the product of the frequency and consequence, does not increase as the frequency decreases". Figure 6 shows the different regions of LBE frequencies along with the consequence target associated with each LBE.

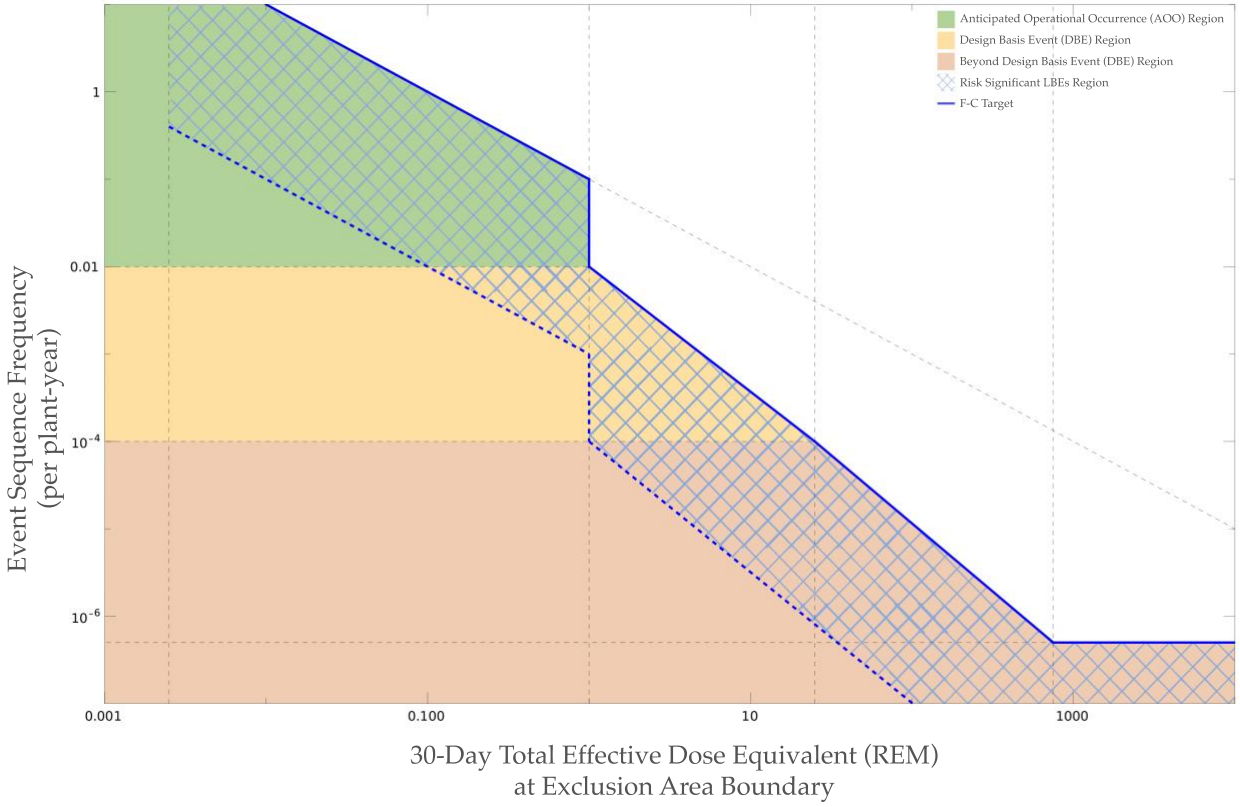

Figure 6. Frequency-Consequence Target.

Step 6 utilizes the event sequence analysis, best-estimate event sequence frequencies, and radiological consequence analysis. Depending on the maturity of the design, radiological consequence analysis can either be deterministically calculated or assumed based on the expert judgment of the end state of a specific sequence. The result of this step is a list of all impacts of operator actions on the risk profile of the design. Depending on the changes in the frequency, a certain LBE:

- Remains unchanged.
- Gets removed, i.e., no longer applicable.
- Increases in mean frequency or uncertainty bounds within the same initial region.
- Increases in mean frequency or uncertainty bounds out of the initial region within the F-C target.
- Increases in mean frequency or uncertainty bounds into the risk significant region.
- Increases in mean frequency or uncertainty bounds out of the F-C target.

Step 7: F-C Target Compliance Assessment

At this decision point, the LBEs are compared with the F-C target. If the LBE fails to meet the F-C target, then this information is used to inform and evaluate the system reliability target requirements. LBEs should not rely on human intervention to meet the F-C target; hence, an update to the system design might be required in the subsequent design stage. On the other hand, if all LBEs meet the F-C target, then the changes in their categorizations are assessed next.

Step 8: Revised List of AOOs, DBEs, and BDBEs

In step 8, the LBE frequencies are compared with their original mean frequencies, uncertainty bounds, and the LBE categorizations' boundaries. LBEs are categorized [7], based on their frequencies, into:

- Anticipated Operational Occurrences (AOOs) with mean frequencies larger than 1.0E-02 per plant year.
- Design Basis Events (DBEs) with mean frequencies larger than 1.0E-04 per plant year.
- Beyond Design Basis Events (BDBEs) with mean frequencies larger than 5.0E-07 per plant year.

The change in LBE frequencies might push the LBE frequencies outside the boundaries of their initial region and LBE categorization. Moreover, the change might push the uncertainty bounds outside the boundaries of the LBE categorization, in which case the LBE is to be evaluated according to the rules of both LBE categories [7].

Step 9: LBE Categorization Changes Assessment

At the final decision point, if an LBE's frequency has a change that changes the LBE categorization, then this information is used to inform and evaluate the system and/or human reliability target requirements. This change in categorization might challenge the licensing criteria or investment requirements; hence, changes to system designs or procedures and guidelines might be required in the subsequent design stage. However, if all LBEs remain within their original categorization, then documentation of all the results is conducted in the next step.

Step 10: List of Important Human Actions

Finally, all the results of the first iteration of the framework are recorded and documented. The results of one iteration of the framework are important human actions that either keep an LBE within the F-C target, keep an LBE within a specific region, or achieve investment goals. These results are then fed into updating the system design or procedures in follow-up design stages.

The framework highlights vital actions that are important to the safety or investment goals of the design. The following section applies the framework to an advanced reactor design while highlighting how the results can be used in improving the design.

3.3. Applicability of HRA Methods

By taking the OpenPHI methodology into consideration, and following the study conducted in CHAPTER 2, the applicability of each HRA methodology analyzed in this study can be mapped out based on the design stage. The different stages of the design of NPPs assumed in this study are presented in section 1.4, moreover, Figure 7 gives more focus on the status of the operating and emergency procedures during each of these design stage. Furthermore, Table 1 gives an overview of the applicability map of all the HRA methodologies throughout all four defined design stages.

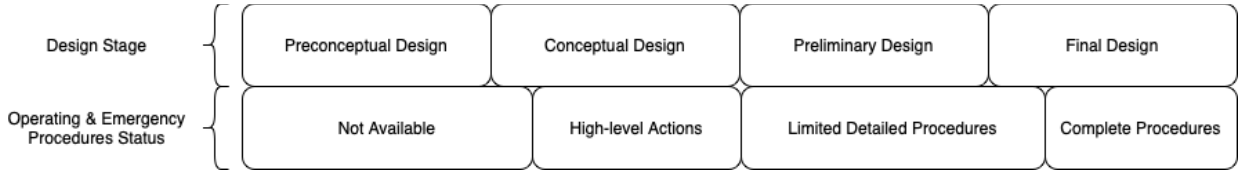

Figure 7. The Status of Procedures during Different Design Stages.

It should be noted that OpenPHI resembles the screening approach used in ASEP, however, as discussed previously in section 2.8, ASEP lacks guidance on how to use the results of HRA to risk-inform the design. Moreover, all current HRA methodologies suffer from the lack of non-LWRs experience which hinders a streamline approach to implement them in non-LWRs. This is exemplified by the guidance given in THERP, which has the most complete guidance of all HRA methodologies, for the screening process in which the impact on CDF is the deciding risk metric [27]. As can be seen, this is quite limiting with respect to reactor technology, for example, the core damage of molten salt reactors is not as well defined as for LWRs.

Finally, it should be noted that, despite being developed to be implemented during the pre-conceptual and conceptual design stages, OpenPHI can be applied through all design stages. Similar to ASEP, OpenPHI can be used as a screening methodology to remove inconsequential operator actions before implementing another high-fidelity resource intensive HRA methodology. Hence, OpenPHI can be coupled with other HRA methodologies during the preliminary and final design stages either to screen out inconsequential operator actions or as a sensitivity analysis tool.

Table 1. Applicability Map of HRA Methodologies in Different Design Stages.

	Pre-conceptual Design	**Conceptual Design**	**Preliminary Design**	**Final Design**
THERP	Not Applicable	Not Applicable	Limited[1]	Applicable
ATHEANA	Not Applicable	Not Applicable	Not Applicable	Applicable
SPAR-H	Not Applicable	Not Applicable	Not Applicable	Applicable
CREAM	Not Applicable	Not Applicable	Not Applicable	Limited[2]
Phoenix	Not Applicable	Not Applicable	Limited[3]	Applicable
IDHEAS	Not Applicable	Not Applicable	Not Applicable	Limited[2]
IDAC	Not Applicable	Not Applicable	Not Applicable	Applicable
ASEP	Not Applicable	Limited[1]	Applicable	Applicable
OpenPHI	Applicable	Applicable	Applicable	Applicable

[1] Due to lack of guidance for non-LWRs
[2] Due to limited guidance and development
[3] Due to intensive resources required

CHAPTER 4. OPENPHI CASE STUDY: XE-100 [73]

As presented in section 3.2, the OpenPHI methodology presents an approach of implementing HRA during early, preconceptual and conceptual, stages of the design. By implementing HRA early in the design process, important operator actions that support safety functions are identified. The design can be updated and risk-informed, either to reduce the safety function reliance on operator actions or increase human reliability through training, clear procedures, and better man-machine interface.

In CHAPTER 4, a case study is presented to demonstrate how to apply the OpenPHI methodology. The preconceptual design of an advanced non-LWR is used to demonstrate the OpenPHI process amid the most limited stages, resource-wise, of the design. Due to the nature of the design used, a commercial NPP, the complete preconceptual design of the Xe-100 is proprietary. However, by restricting the analysis to a publicly available event sequence and the results to high-level aggregate results, the demonstration of both the methodology and the results can be published and became public as part of the publication resulting from this study [73].

4.1. Xe-100

In October of 2020, the United States Department of Energy (U.S. DOE) awarded X-energy $80 million in initial funding under the new advanced reactor demonstration program (ARDP). In the following year, the United States congress appropriated about $1.1 billion, under the Infrastructure Investments and Jobs Act, to the development of X-energy's advanced small modular reactor (SMR) [26][65].

X-energy (Rockville, Maryland) is a U.S. based company developing small and micro reactors along with the tri-structural isotropic (TRISO) fuel to power them. X-energy's SMR design, the Xe-100, is a high-temperature gas-cooled pebble-bed (HTGR-PB) reactor. The Xe-100 design

follows the very high temperature reactor (VHTR) design chosen by the generation IV international forum as one of the candidates of Gen-IV reactors [66][67].

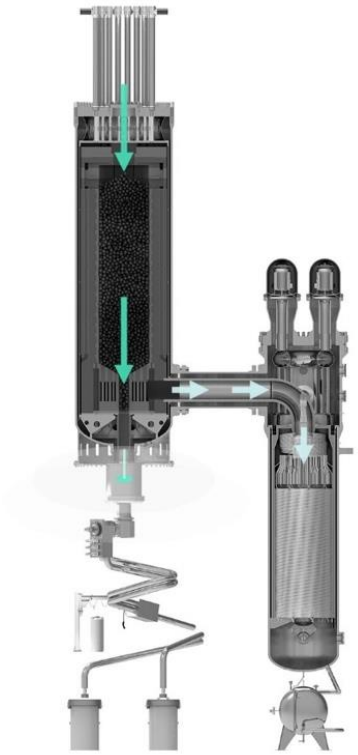

Figure 8. Primary Cycle of the Xe-100.

As mentioned previously, the Xe-100 is an HTGR-PB SMR with an expected electric output of 80 MWe. It utilizes a helium coolant that circulates and cool about 220,000 of TRISO fuel particles. The maximum helium temperature is expected to be around 750 ℃, hence the high-temperature moniker, with an expected operational life of 60 years. A diagram illustrating the design of the primary cycle of the Xe-100 is shown in Figure 8 [68].

4.2. Small Depressurization Event Sequence Analysis

In 2018, Brandon et al. conducted a demonstration of the LMP methodology that utilized the pre-conceptual design of the Xe-100 [69]. The demonstration utilized the existing PRA and design expertise of both HTGRs [70]-[72] and LWRs. This expertise was used to analyze the pre-

conceptual design of the Xe-100 and develop a preliminary PRA model of the design. An initial set of internal IEs was identified using the master logic diagram methodology; the plant response to these IEs is then analyzed using event sequence (ES) diagrams and ET. Finally, a list of LBEs along with their expected dose consequences is compiled, which was used to ""improve the regulatory certainty of X-energy's Xe-100 design and its associated safety design approach" [69]. Even though the pre-conceptual design, and the preliminary PRA study, is proprietary, the pilot study included the FT associated with a small helium depressurization IE. This FT, Shown in Figure 9, is used to demonstrate the PHI methodology shown in CHAPTER 3 and published in [73]. The PHI methodology is applied throughout the entire so-called Phase 0 PRA model of the Xe-100; the results of which are given in section 4.3 and are used to inform and update the later stages of the design.

First, all operator actions assumed and credited in the ET in Figure 9 are identified. Table 2 lists the identified actions that are assumed and/or incorporated in analyzing the ET. The identified actions are either used as a top event in the ET, included as a subsystem, or not modeled explicitly in the initial analysis. The table shows if and how it was included in the ET and the action categorization assumed (primary vs. secondary actions).

Then, the approach for assessing the impact of each action was decided based on the action categorization and available system information. Table 2 lists the method assumed to account for all operator actions and the updated split fractions and failure probability for each associated top event. It should be noted that:

- The failure of manual systems/subsystems in approach III was assumed to be 1.0E-02.
- All actions associated with valve operation were assumed to be mainly automated since valves will probably have little human intervention.

- Circulator trips were assumed to be principally automated since circulator controls are highly reliable.
- HVAC filtration was assumed, conservatively, to be mainly manual since it might require manual system alignment.

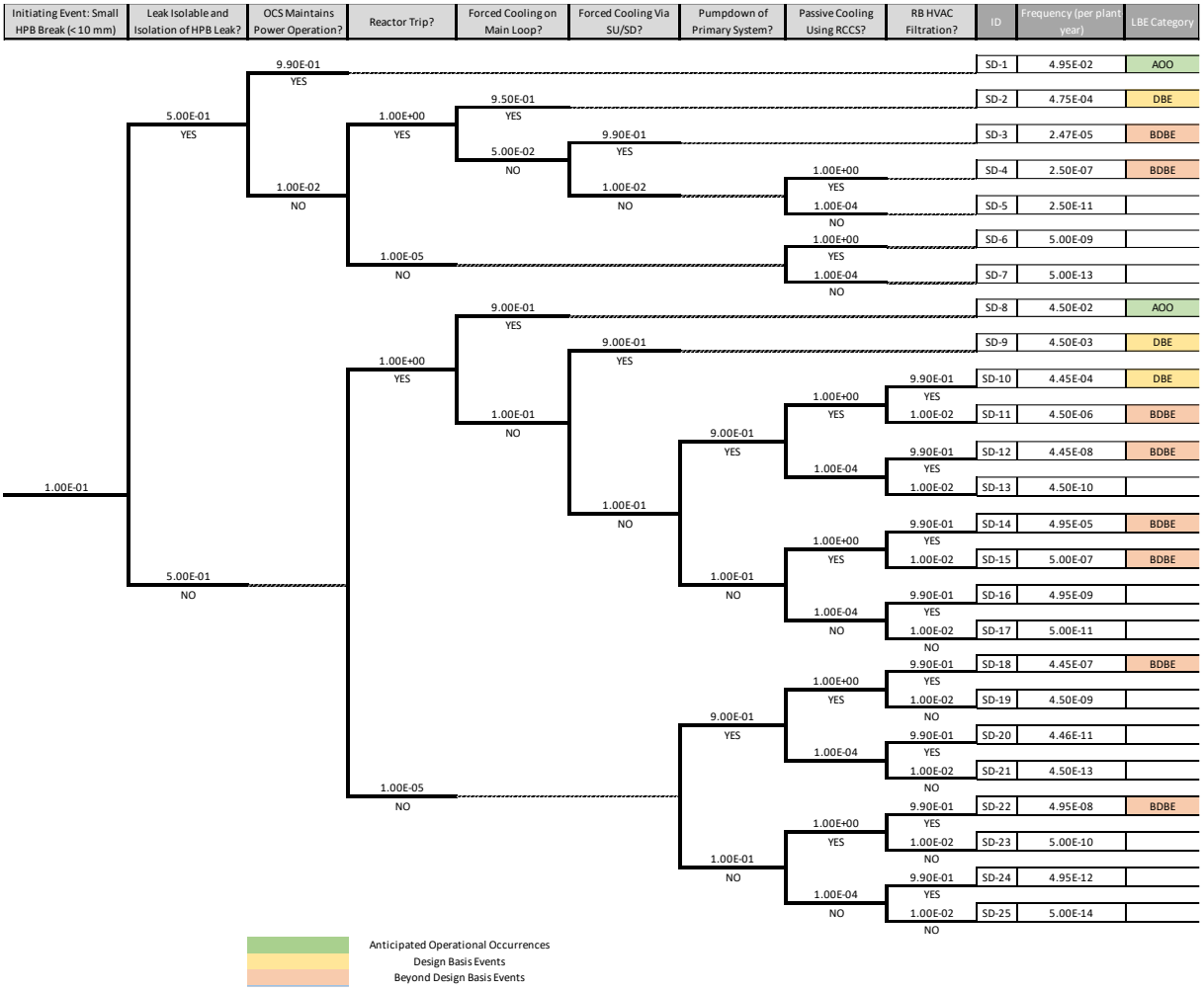

Figure 9. Small Helium Depressurization Event Tree with Associated LBEs.

Finally, the updated split fractions were used to quantify the frequency of all LBEs. The updated frequencies were then compared against the original frequencies. And then, combined with radiological consequences, the updated LBEs were compared with the F-C target. It should be

noted that conservative dose release values were assigned to each end state consequence. The analysis results, which are shown in section 4.3, highlight the impact of operator actions on the risk profile of the Xe-100 pre-conceptual design.

Table 2. Operator Action in Small Helium Pressure Boundary Break Initiating Event.

Operator Action	Designation	Inclusion in Phase 0	Category
Isolation of Leak	OA1	Included as a top event	Primary
OCS[4] maintains power operation	OA2	Included as a top event	Primary
Manual Reactor Trip	OA3	Included as a subsystem	Secondary
Pump down of Primary system	OA4	Included as a top event	Primary
Manually closing MSIV[5] to establish FC[6] using the main loop	OA5	Not modeled explicitly	Secondary
Manually closing main loop isolation valve to establish FC using SU/SD[7]	OA6	Not modeled explicitly	Secondary
Manually opening SU/SD isolation valve to establish FC using SU/SD	OA7	Not modeled explicitly	Secondary
Manually tripping the circulator in case of SU/SD failure with automatic trip failure	OA8	Not modeled explicitly	Secondary
RB HVAC[8] manual filtration actuation	OA9	Not modeled explicitly	secondary

[4] OCS: Operational Control System
[5] MSIV: Main Steam Isolation Valve
[6] FC: Forced Cooling
[7] SU/SD: Startup/Shut Down System
[8] RB HVAC: Reactor Building Heating, Ventilation, and Air Conditioning System

Table 3. Operator Actions Quantification.

Operator Action Designation	Approach	Original Split Fraction	Updated Split Fraction
OA1	I	5.0E-01	1.0E+00
OA2	I	1.0E-02	1.0E+00
OA3	III	1.0E-05	1.0E-03
OA4	I	1.0E-01	1.0E+00
OA5	II	N/A[9]	N/A
OA6	II	N/A	N/A
OA7	II	N/A	N/A
OA8	II	N/A	N/A
OA9	III	1.0E-02	1.0E+00

4.3. Results

After implementing the previous steps, the updated frequencies of the end states were compared with their original frequencies. Figure 10 shows the updated ET of the small HPB break IE where 19 sequences in the ET depended entirely on operator actions in at least one of their top events. Hence, the frequencies of the end states associated with these 19 sequences became zero indicating that these sequences are no longer valid. Most of the remaining end state frequencies increased; however, some sequences had significant changes in the LBE categorization.

[9] N/A: Not Applicable

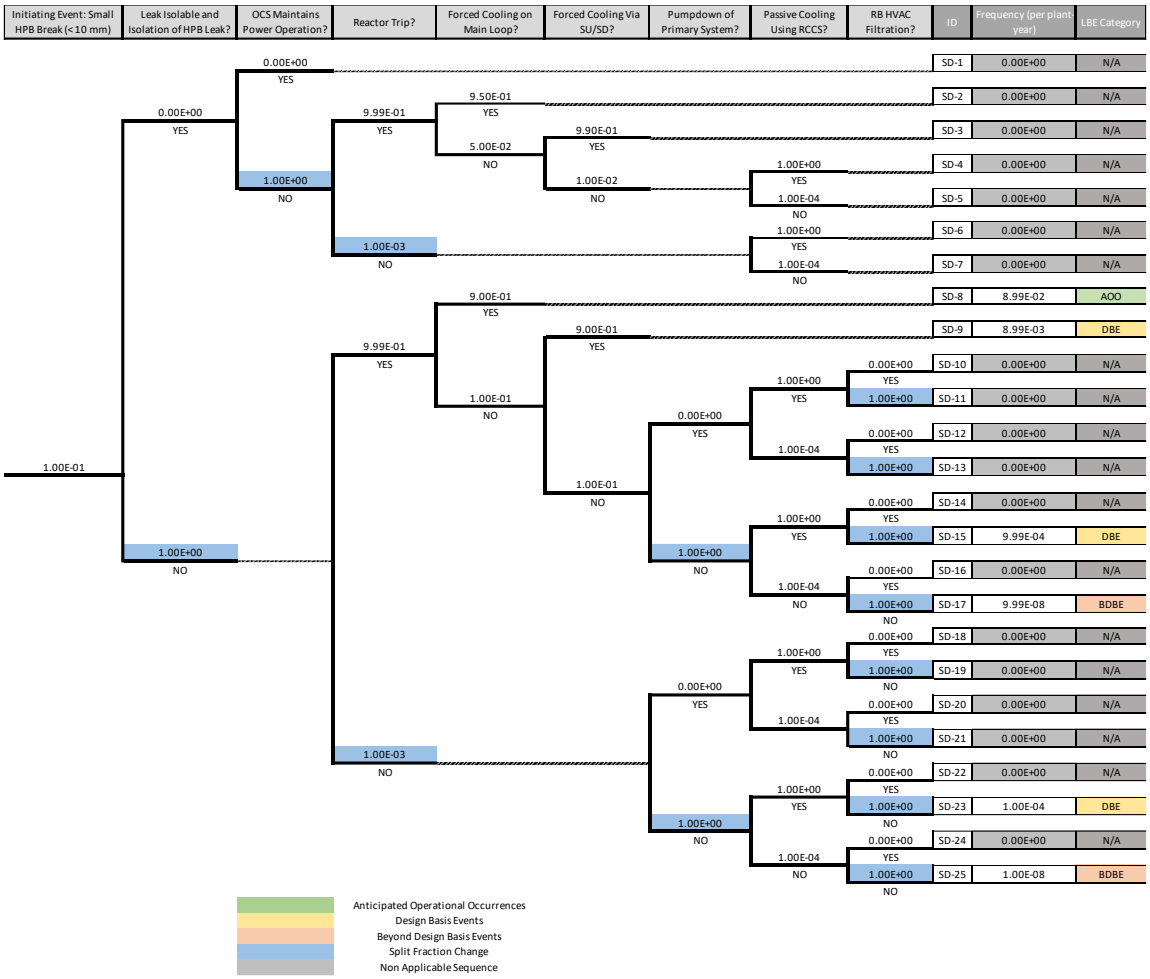

Figure 10 Updated Small Helium Depressurization Event Tree with Associated LBEs.

Further, of all 177 LBEs resulted from all IEs investigated in the Phase 0 PRA [74], a total of 57 sequences were removed from the analysis. The removal was due to the sequences becoming unrealistic while not crediting any operator actions. Moreover, a total of 23 sequences had a significant increase in frequencies that the LBE categorization changed. Out of those 23 sequences, three LBEs increased in frequency to the AOOs region. Of the three LBEs, two were originally in the DBEs region, and one was initially in the BDBEs region. The frequency of seven LBEs increased to the DBEs region out of the BDBEs region. Finally, a total of 13 LBEs increased in frequency from the scarce BDBEs region, that is with a frequency less than 5.0E-07, to the BDBEs region.

Table 4 lists the LBEs that increased in frequency to the AOOs region, where in the case of LBEs in the BDBEs region, it was associated with a release of 2.0E-02 rem. For reference, according to the NRC [75], all-natural and man-made radiation sources result in a background annual average dose per person of about 6.2E-01 rem. This release is higher by an order of magnitude than the worst anticipated releases of the Xe-100 [69][74].

Table 5 lists the sequence description of these LBEs. In addition, Figure 11 to Figure 13 illustrates these significant changes in LBEs with both LMP regions and F-C target superimposed on them. It should be noted that, though most of all these LBEs are not associated with any releases, it was assumed that the consequence of these end states is equal to the highest consequence assigned to any of them in the Phase 0 PRA [69][74]. So, in the case of LBEs in the AOOs and DBEs region, it was assumed that these end states have a release of 1.0E-05 rem.

Table 4. LBEs with Updated Frequencies in the AOOs Region.

LBE Designation	Phase 0 Frequency	Phase 0 LBE Category	Updated Frequency	Updated LBE Category
TT-6	1.0E-06	BDBE[10]	1.0E-02	AOO[11]
LOFW-2	5.0E-04	DBE[12]	5.0E-02	AOO
LOOP-2	4.1E-03	DBE	8.1E-02	AOO

In the case of LBEs in the BDBEs region, it was associated with a release of 2.0E-02 rem. For reference, according to the NRC [75], all-natural and man-made radiation sources result in a

[10] AOO > 1.0E-02 per plant year
[11] 1.0E-02 per plant year > DBE > 1.0E-04 per plant year
[12] 1.0E-04 per plant year > BDBE > 5.0E-07 per plant year

background annual average dose per person of about 6.2E-01 rem. This release is higher by an order of magnitude than the worst anticipated releases of the Xe-100 [69][74].

Table 5. Sequence Description of LBEs with Updated Frequencies in the AOOs Region.

LBE Designation	Plant Response
TT-6	Turbine trip IE, Reactor Trip Failure, Conduction Cooldown via RCCS[13]
LOFW-2	Loss of feedwater IE., SSS Failure, Conduction Cooldown via RCCS
LOOP-2	Loss of offsite power IE., T.G. Failure, Power restored < 3hrs, Forced cooling via SSS

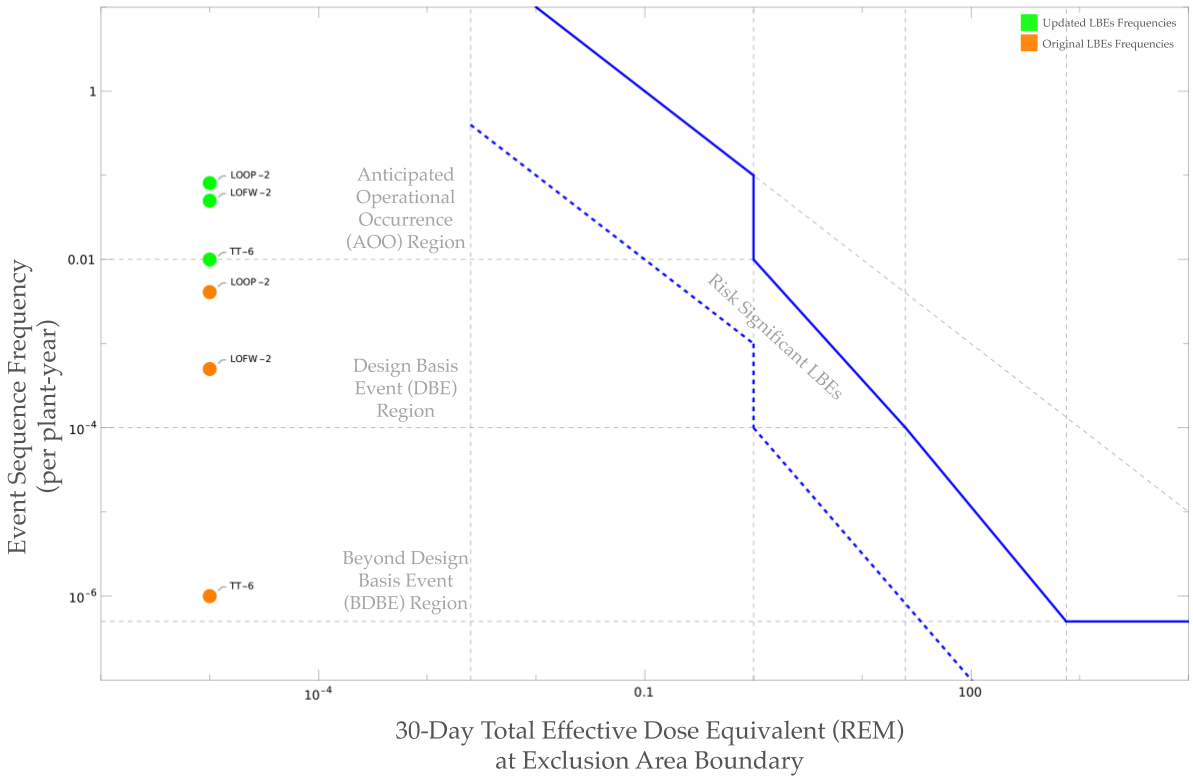

Figure 11. LBEs with Updated Frequencies in AOOs Region.

[13] RCCS: Reactor Cavity Cooling System

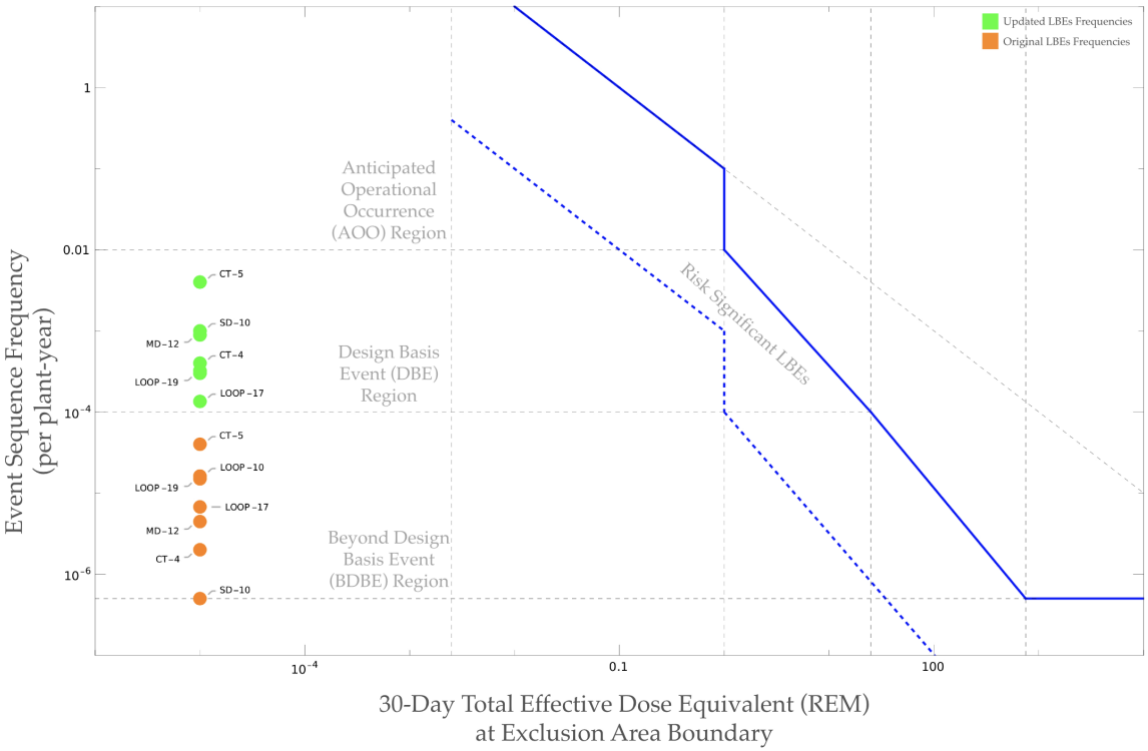

Figure 12. LBEs with Updated Frequencies in DBEs Region.

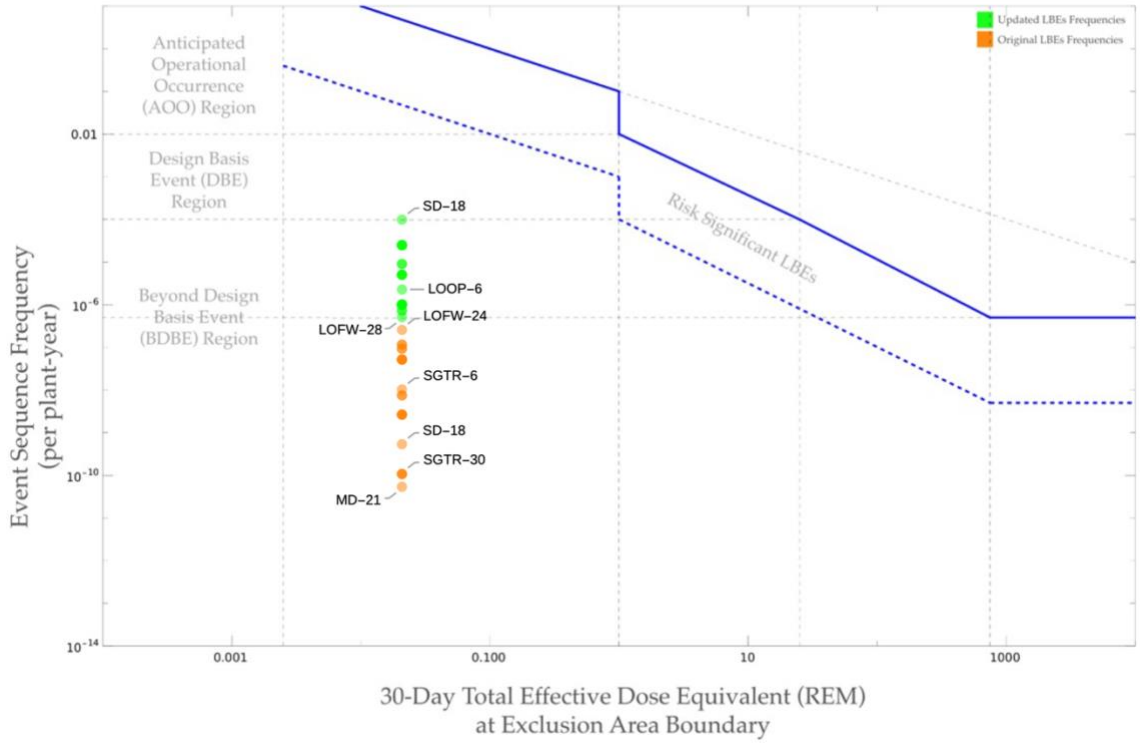

Figure 13. LBEs with Updated Frequencies in BDBEs Region.

From the previous results, we can conclude that the safety impact of operator actions in the Xe-100 is negligible. Out of the 177 LBEs identified in Phase 0, only 23 LBEs increased their frequencies enough to warrant further investigation. Of those 23 LBE, only nine end states have possible release paths with the remaining LBEs with an end state of an intact reactor pressure vessel.

Despite the conservative assumption of the total effective dose equivalent associated with the end states, no LBE exceeded the F-C target, as shown in Figure 11 to Figure 13. This indicates that the Xe-100 design still meets the LMP F-C target even while crediting no operator actions. The results confirm the inherent safety of the design and the minimal dependence on human intervention.

However, the results also highlight a few critical sequences in which operator actions are essential to keeping the LBE at a lower category. The LBEs, though they might have no releases associated with them, might challenge the LMP process. As an example, TT-6, which relies on passive cooling, requiring operator action to keep it out of the AOOs region, is one of these critical sequences.

4.4. OpenPHI Limitations

In this section, some of the limitations of the OpenPHI are presented and addressed. Although the case study presented utilized only point estimates in the assessment of the frequency and the consequences, this is not an inherent limitation in OpenPHI but rather an attribute of the low fidelity of the PRA model conducted during this stage of the design. As the fidelity of the PRA model improves, the 5^{th} and 95^{th} percentile associated with each LBE's frequency and consequence is quantified and OpenPHI presents the approach to treat each following the LMP requirements [7].

The most significant limitation to the framework is that it requires an early-stage PRA model. The steps utilize most PRA elements ranging from initiating events analysis to risk integration. Whereas this might have been a limitation in legacy approaches, both the LMP process and the non-LWR standard [7][8] require the integration of PRA in the early stages of design. The required PRA model provides the necessary elements required for the proposed framework through all stages of design.

Further, step IV utilizes the radiological consequences to calculate the consequences of each end state. The input is conceivably hard to acquire in the early stages of design since it requires a deterministic safety assessment, a somewhat mature design. However, this limitation is overcome by utilizing expert judgment, empirical correlations, or scaled legacy data whenever suitable until more representative consequences values are available.

Finally, due to lack of information, some assumptions are perhaps too conservative with the operator actions impact highly uncertain. The conservative assumptions however limiting also represent a bounding case that informs the system design of the worst possible scenarios to help develop the plant control philosophy and the human factors engineering program. In later design stages, since more realistic assumptions are incorporated and the uncertainties are evaluated, this limitation is expected to be mitigated.

CHAPTER 5. CONCLUSIONS AND FUTURE WORK

5.1. Conclusions

The study investigates the applicability of different HRA methodology during the early stages of NPP design. Out of a myriad of HRA methodologies, a set of nine HRA methodologies are chosen and deemed representative of most approaches used in HRA. However, due to the fact that PRA in general and HRA specifically has been historically retroactively applied to operating NPPs, most HRA methodologies are very limited during the early stages of design. Moreover, since most of the operating experience used to develop these methodologies are of LWRs, limited guidance is given on how to inform the design of non-LWRs using the results of HRA.

Hence, in the second part of the study, we present an iterative framework, OpenPHI, to apply HRA in different stages of design. The framework utilizes the PRA elements developed in all design phases to identify operator actions, assess their impact, and highlight critical actions included in the design. By following OpenPHI, the inputs of HRA can be used to inform the design even during the preconceptual design stage in which scarce resources are available to apply any other HRA methodology. Moreover, OpenPHI present a complete framework on how to identify important operator actions and use this to inform later design stages.

Furthermore, the study presents a demonstration of the OpenPHI framework through X-energy's Xe-100 preconceptual design. By applying the framework steps, the safety posture of the Xe-100 design is evaluated even under the conservative assumption of crediting no operator actions. Moreover, the analysis highlights key sequences which further illicit investigations and should be incorporated in updating the system design and/or procedures. The results of this analysis will be used in later stages of the design to further enhance the safety case of the Xe-100 allowing for more risk-informed design. Finally, the framework's assumptions and limitations, which are

mainly due to lack of design information, are presented and addressed to show their limited impact on the validity of the framework.

5.2. Future work

The OpenPHI framework will be refined in future work by applying it to other NPP designs and other early, conceptual or preliminary, design phases of design process in which more limitations might arise to be addressed accordingly. Another benefit of applying OpenPHI in other design stages is to demonstrate the approach of how to treat uncertainty bounds, not just point estimates. Moreover, within the scope of this study, only errors of omission (EOs), in which an operator fails to perform the required action within the specified time, were considered. However, errors of commission (ECs), in which an operator performs an incorrect action, may result in new event sequences. Hence, by explicitly modeling ECs, future implementations of OpenPHI can identify additional limitations that need to be addressed. These implementations allow for more refining of the OpenPHI guidance with respect to ECs.

Finally, as it stands, this work showcases the OpenPHI framework as a means of supporting and risk-informing the design of advanced NPPs, augmenting current HRA methodologies, and addressing some of their limitations especially during the early stages of designs.

REFERENCES

[1] Garrick, B J, Gekler, W C, Goldfisher, L, Shimizu, B, and Wilson, J H. EFFECT OF HUMAN ERROR AND STATIC COMPONENT FAILURE ON ENGINEERED SAFETY SYSTEM RELIABILITY. United States: N. p., 1967. Web.

[2] Swain, A. D. HUMAN FACTORS IN DESIGN OF RELIABLE SYSTEMS. United States: N. p., 1964. Web. doi:10.2172/4070176.

[3] Swain, A D. A METHOD FOR PERFORMING A HUMAN-FACTORS RELIABILITY ANALYSIS. United States: N. p., 1963. Web.

[4] Swain, A D. HUMAN RELIABILITY ASSESSMENT IN NUCLEAR REACTOR PLANTS. United States: N. p., 1969. Web.

[5] Reactor safety study. An assessment of accident risks in U. S. commercial nuclear power plants. Executive summary: main report. [PWR and BWR]. United States: N. p., 1975. Web. doi:10.2172/7134131.

[6] Lee, J. C., & McCormick, N. J. (2012). Risk and Safety Analysis of Nuclear Systems. John Wiley & Sons.

[7] W. L. Moe, "NEI 18-04 Risk-Informed Performance-Based Technology Inclusive Guidance for Advanced Reactor Licensing Basis Development," Idaho National Lab. (INL), Idaho Falls, ID (United States), INL/EXT-19-55375-Rev000, Apr. 2019. doi: 10.2172/1557649

[8] "Probabilistic Risk Assessment Standard for Advanced Non-LWR Nuclear Power Plants," ASME/ANS RA-S-1.4-2021, 2021

[9] Beck, C. K., Cowan, F. P., & et. al. (1957). Theoretical Possibilities and Consequences of Major Accidents in Large Nuclear Power Plants (WASH-740, 4344308; p. WASH-740, 4344308). Brookhaven National Laboratory. https://doi.org/10.2172/4344308

[10] "The Safety of Nuclear Power Reactors (Light Water Cooled) and Related Facilities", U.S. Atomic Energy Commission Report WASH-1250, July 1973

[11] Kaplan, S., & Garrick, B. J. (1981). On The Quantitative Definition of Risk. Risk Analysis, 1(1), 11–27. https://doi.org/10.1111/j.1539-6924.1981.tb01350.x

[12] Probabilistic Risk Assessment (PRA). NRC Web. Retrieved August 23, 2022, from https://www.nrc.gov/about-nrc/regulatory/risk-informed/pra.html

[13] International Nuclear Safety Advisory Group. (1992). Probabilistic Safety Assessment. INTERNATIONAL ATOMIC ENERGY AGENCY. https://www.iaea.org/publications/3789/probabilistic-safety-assessment

[14] Reckley, W. (2020). 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 (Guidance ML20091L698; p. 31). U.S. Nuclear Regulatory Commission. https://www.nrc.gov/docs/ML2009/ML20091L698.pdf

[15] Three Mile Island: a report to the commissioners and to the public. Volume I. United States: N. p., 1979. Web. doi:10.2172/5395798.

[16] Implications of the accident at Chernobyl for safety regulation of commercial nuclear power plants in the United States: Volume 1, Main report: Final report. United States: N. p., 1989. Web. doi:10.2172/6300378.

[17] Internationale Atomenergie-Organisation (2015). The Fukushima Daiichi accident. International Atomic Energy Agency.

[18] NUREG-1792 “Good Practices for Implementing Human Reliability Analysis” (Final). (2005). 110.
[19] U.S. Nuclear Regulatory Commission. Office of Nuclear Regulatory Research. (2007). Regulatory Guide 1.200 an approach for determining the technical adequacy of probabilistic risk assessment results for risk-informed activities. [Washington, D.C.]: U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research
[20] NUREG-1842 “Evaluation of Human Reliability Analysis Methods Against Good Practices, Final Report.” (2006). 288.
[21] Benjamin, A S, Boyd, G J, Lewis, S R, Amos, C N, Cunningham, M A, and Murphy, J A. NUREG-1150 risk assessment methodology and results. United States: N. p., 1987. Web.
[22] PRA Implementation Plan (1994 to 1999). NRC Web. Retrieved July 29, 2022, from https://www.nrc.gov/about-nrc/regulatory/risk-informed/history/1994-1999.html
[23] Travers, W. D. (2000). Risk-Informed Regulation Implementation Plan. 6.
[24] Reyes, L. A. (2007). Implementation And Update of The Risk-Informed and Performance-Based Plan. 26.
[25] Zheng, X., Bolton, M. L., Daly, C., & Biltekoff, E. (2020). The development of a next-generation human reliability analysis: Systems analysis for formal pharmaceutical human reliability (SAFPH). Reliability Engineering & System Safety, 202, 106927. https://doi.org/10.1016/j.ress.2020.106927
[26] R. Boring and D. Gertman, “Atomistic and holistic approaches to human reliability analysis in the US nuclear power industry:” Safety and Reliability, vol. 25, pp. 21–37, Jun. 2005, doi: 10.1080/09617353.2005.11690802.
[27] A. D. Swain and H. E. Guttmann, “Handbook of human-reliability analysis with emphasis on nuclear power plant applications. Final report,” NUREG/CR-1278, SAND-80-0200, 5752058, Aug. 1983. doi: 10.2172/5752058.
[28] Miller, R. B. (1953). “A Method for Man-Machine Task Analysis.” Defense Technical Information Center. https://doi.org/10.21236/AD0015921
[29] B. Kirwan, A Guide to Practical Human Reliability Assessment. CRC Press, 1994. Ch.5, pp. 39-317.
[30] Cooper, S. E.; Ramey-Smith, A. M.; Wreathall, J. & Parry, G. W. A technique for human error analysis (ATHEANA), report, May 1996; Washington D.C. https://www.nrc.gov/docs/ML1200/ML120090039.pdf
[31] Taylor, J., O`Hara, J., & Luckas, W. (1997). ATHEANA: “a technique for human error analysis” entering the implementation phase (NUREG/CP-0157-Vol.3; CONF-9610202-Vol.3). US Nuclear Regulatory Commission (NRC), Washington, DC (United States). Office of Nuclear Regulatory Research; Brookhaven National Lab. (BNL), Upton, NY (United States). https://www.osti.gov/biblio/467925D.
[32] Bell, J., & Holroyd, J. (2018). Review of human reliability assessment methods (No. RR679). https://pdf4pro.com/amp/view/review-of-human-reliability-assessment-methods-rr679-530d5b.html
[33] Gertman et al., “The SPAR-H human reliability analysis method, NUREG/CR-6883,” Idaho National Laboratory, pre-pared for U. S. Nuclear Regulatory Commission Office of Nuclear Regulatory Research Washington, DC 205555-0001.

[34] W. J. Galyean, A. M. Whaley, D. L. Kelly, & R. L. Boring. (2011). SPAR-H Step-by-Step Guidance (INL/EXT-10-18533, 1027888; p. INL/EXT-10-18533, 1027888). https://doi.org/10.2172/1027888

[35] J. Forester et al., "Evaluation of Analysis Methods Against Good Practices. Final Report. NUREG-1842," U.S. Nuclear Regulatory Commission Office of Nuclear Regulatory Research Washington, DC 20555-0001.

[36] Hollnagel, E. (1998). Cognitive reliability and error analysis method: CREAM (1st ed.). Oxford; New York: Elsevier, 1998. https://catalog.lib.ncsu.edu/catalog/NCSU4527636

[37] Petrillo, A., De Felice, F., Romano, U., & Carlomusto, A. (2013). Modelling application for cognitive reliability and error analysis method. International Journal of Engineering and Technology, 5, 4450–4464.

[38] V. D. Pasquale, R. Iannone, S. Miranda, and S. Riemma, An Overview of Human Reliability Analysis Techniques in Manufacturing Operations. IntechOpen, 2013. doi: 10.5772/55065.

[39] M. Marseguerra, E. Zio, and M. Librizzi, "Human Reliability Analysis by Fuzzy 'CREAM,'" Risk Analysis, vol. 27, no. 1, pp. 137–154, 2007, doi: 10.1111/j.1539-6924.2006.00865. x.

[40] S. Collier, "A Simulator Study of CREAM to Predict Cognitive Errors. In Proceedings of the International Workshop. Building the new HRA. Errors of commission form research to application," 2003, Nuclear Energy Agency. Pages 56-75.

[41] L. Zhao and S. Liu, "Retrospective Analysis of Amusement Rides Accidents Based on Cognitive Reliability and Error Analysis Method," 2020 IEEE 7th International Conference on Industrial Engineering and Applications (ICIEA), 2020, pp. 1088-1092, doi: 10.1109/ICIEA49774.2020.9101961.

[42] Liao, P.-C., Luo, X., Wang, T., & Su, Y. (2016). The Mechanism of how Design Failures cause Unsafe Behavior: The Cognitive Reliability and Error Analysis Method (CREAM). Procedia Engineering, 145, 715–722. https://doi.org/10.1016/j.proeng.2016.04.088

[43] Chen, X., Liu, X., & Qin, Y. (2021). An extended CREAM model based on analytic network process under the type-2 fuzzy environment for human reliability analysis in the high-speed train operation. Quality and Reliability Engineering International, 37(1), 284–308. https://doi.org/10.1002/qre.2736

[44] CREAM. Retrieved August 16, 2022, from https://erikhollnagel.com/ideas/cream.html

[45] N. J. Ekanem, A. Mosleh, and S.-H. Shen, "Phoenix – A model-based Human Reliability Analysis methodology: Qualitative Analysis Procedure," Reliability Engineering & System Safety, vol. 145, pp. 301–315, Jan. 2016, doi: 10.1016/j.ress.2015.07.009.

[46] Diaconeasa, M. A. (2019). Human reliability analysis for nuclear power plants using the extended PHOENIX methodology and software platform (GIRS-2019-01/L; Prepared for Japan Nuclear Regulation Authority). The B. John Garrick Institute for the Risk Sciences, University of California Los Angeles.

[47] NUREG-2199, Vol. 1, "An Integrated Human Event Analysis System (IDHEAS) for Nuclear Power Plant Internal Events At-Power Application—Volume 1.". 317.

[48] Liao, H. (2015). Insights from Pilot Testing of the IDHEAS HRA Method. Procedia Manufacturing, 3, 1350–1357. https://doi.org/10.1016/j.promfg.2015.07.291

[49] Chang, Y. H. J., & Mosleh, A. (2007). Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents: Part 1: Overview of

the IDAC Model. Reliability Engineering & System Safety, 92(8), 997–1013. https://doi.org/10.1016/j.ress.2006.05.014

[50] M. A. Diaconeasa and A. Mosleh, "Performing an Accident Sequence Precursor Analysis with the ADS-IDAC," Los Angeles, p. 7, 2018.

[51] Swain, A. D. (1987). Accident Sequence Evaluation Program: Human reliability analysis procedure (NUREG/CR-4772; SAND-86-1996). Sandia National Labs., Albuquerque, NM (USA); Nuclear Regulatory Commission, Washington, DC (USA). Office of Nuclear Regulatory Research. https://doi.org/10.2172/6370593

[52] R. Boring et al., "Human Unimodel for Nuclear Technology to Enhance Reliability (HUNTER): A Framework for Computational-Based Human Reliability Analysis," Oct. 2016.

[53] Boring, R., & Skogstad, M. (2016, September 26). GOMS-HRA: A method for treating subtasks in dynamic human reliability analysis.

[54] Boring, R., Mandelli, D., Joe, J., Smith, C., & Groth, K. (2015). A Research Roadmap for Computation-Based Human Reliability Analysis (INL/EXT-15-36051). Idaho National Lab. (INL), Idaho Falls, ID (United States). https://doi.org/10.2172/1230074

[55] PRA Implementation Plan (1994 to 1999). NRC Web. Retrieved July 29, 2022, from https://www.nrc.gov/about-nrc/regulatory/risk-informed/history/1994-1999.html

[56] Travers, W.D. (2000). Risk-Informed Regulation Implementation Plan. 6.

[57] Reyes, L.A. (2007). Implementation and Update of The Risk-Informed and Performance-Based Plan. 26.

[58] Reckley, W. (2020). 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 (Guidance ML20091L698; p. 31). U.S. Nuclear Regulatory Commission. https://www.nrc.gov/docs/ML2009/ML20091L698.pdf

[59] Moe, W.L. (2019). NEI 18-04 Risk-Informed Performance-Based Technology Inclusive Guidance for Advanced Reactor Licensing Basis Development (INL/EXT-19-55375-Rev000). Idaho National Lab. (INL), Idaho Falls, ID (United States). https://doi.org/10.2172/1557649.

[60] Moe, W., & Afzali, A. (2020). Modernization of Technical Requirements for Licensing of Advanced Non-Light Water Reactors: Probabilistic Risk Assessment Approach (INL/EXT--20-60395, SC--29980-101-Rev.01, 1700670; p. INL/EXT--20-60395, SC--29980-101-Rev.01, 1700670). https://doi.org/10.2172/1700670.

[61] U.S. Code of Federal Regulations (CFR) "Domestic Licensing of Production and Utilization Facilities," Part 50, Chapter 1, Title 10, "Energy."

[62] CFR, "Licenses, Certifications, and Approvals for Nuclear Power Plants," Part 52, Chapter 1, Title 10, "Energy."

[63] NuScale Power, LLC Submittal of 'NuScale Control Room Staffing Plan,' TR-0420-69456, Revision 0.

[64] U.S. Department of Energy announces $160 million in first awards under Advanced Reactor Demonstration Program. Energy.gov. (n.d.). Retrieved July 11, 2022, from https://www.energy.gov/ne/articles/us-department-energy-announces-160-million-first-awards-under-advanced-reactor

[65] Landed, W. (2021, November 15). Congress appropriates ~$1.1B dollars to X-energy's ARDP project with historic legislation recognizing clean energy supply as vital to US

infrastructure and economic health. - X-energy. X. Retrieved July 11, 2022, from https://x-energy.com/media/news-releases/congress-appropriates-1-billion-dollars-to-x-energys-ardp-project

[66] Energy: HTGR: Advanced Nuclear Reactors (SMR) & Triso Fuel. X. Retrieved July 11, 2022, from https://x-energy.com/

[67] A Technology Roadmap for Generation IV Nuclear Energy Systems Executive Summary. United States. https://doi.org/10.2172/859105

[68] Reactor: Xe-100 - X-energy: HTGR: Nuclear reactors (SMR) & Triso Fuel. X. Retrieved July 11, 2022, from https://x-energy.com/reactors/xe-100

[69] Brandon, W., Fleming, K., Silady, F., Huning, A., & Redd, J. (n.d.). High Temperature, Gas-Cooled Pebble Bed Reactor—Licensing Modernization Project Demonstration. Retrieved August 15, 2020, from https://www.nrc.gov/docs/ML1822/ML18228A779.pdf

[70] PBMR (Pty) Ltd., "US Design Certification, Licensing Basis Event Selection for the Pebble Bed Modular Reactor," ADAMS Accession Number ML061930123, June 2006.

[71] GA Technologies, "Probabilistic Risk Assessment for the Standard Modular High Temperature Gas-Cooled Reactor," DOE-HTGR-86-011, Rev. 3, January 1987, ADAMS Accession Number ML111310342 (Volume 1).

[72] Idaho National Laboratory, "Next Generation Nuclear Plant Probabilistic Risk Assessment White Paper," INL/EXT-11-21270, September 2011. ADAMS Accession Number ML11265A082.

[73] Hamza, M., & Diaconeasa, M. A. (2022). A framework to implement human reliability analysis during early design stages of advanced reactors. Progress in Nuclear Energy, 146, 104171. https://doi.org/10.1016/j.pnucene.2022.104171

[74] X-energy, LLC., "Phase 0 Probabilistic Assessment Report," XE-P1-GL-G0-A26-100410, Rev. 1, December 2016. (X-energy Proprietary)

[75] US NRC, "Doses in Our Daily Lives" X. [Online]. Available: https://www.nrc.gov/about-nrc/radiation/around-us/doses-daily-lives.html. [Accessed: 19-Sep-2021]

APPENDICES

Appendix A.

Table 6 lists the licensing basis events identified in the Phase 0 PRA model of the Xe-100; along with these events are the frequency and dose associated with each of them. The doses are all calculated at the exclusion area boundary based on scaled estimates of the Modular High-Temperature Gas-cooled Reactor (MHTGR) and the Pebble-Bed Modular Reactor's (PBMR) dose consequences [69].

Table 6. Licensing Basis Events of the Phase 0 PRA of the Xe-100.

LBE Designation	**LBE Description**	**Event Sequence Frequency (per plant-year)**	**Dose (rem)**
TT-1	Turbine trip, plant runback to reduced power level	1E+01	<1E-05
RT-01	Reactor trip, forced cooling via main-loop system	6E+00	<1E-05
CT-01	Circulator trip, forced cooling via main-loop system	4E+00	<1E-05
CT-02	Circulator trip, forced cooling via SU/SD system	4E-01	<1E-05
RT-02	Reactor trip, forced cooling via SU/SD system	3E-01	<1E-05
LO-01	Loss of offsite power, plant maintains house load	1E-01	<1E-05
TT-02	Turbine trip, forced cooling via main-loop system	9E-02	<1E-05
FW-01	Feedwater pump trip, forced cooling via SU/SD system	5E-02	<1E-05

Table 6. (continued).

SD-01	Small helium leak, isolated, plant maintains operation	5E-02	1E-05
SD-08	Small helium leak, no isolation, forced cooling via main-loop	5E-02	1E-05
CT-03	Circulator trip, forced cooling failure, passive cooling via RCCS	2E-02	<1E-05
SG-01	Steam generator tube rupture, isolation, forced cooling via SU/SD system	9E-03	1E-05
CR-01	Rod withdrawal, forced cooling via main-loop	9E-03	<1E-05
LO-02	Loss of offsite power < 3 hr., forced cooling via SU/SD	5E-03	<1E-05
TT-03	Turbine trip, forced cooling via SU/SD system	5E-03	<1E-05
SD-09	Small helium leak, no isolation, forced cooling via SU/SD system	5E-03	1E-04
RT-03	Reactor trip, passive cooling via SU/SD	3E-03	<1E-05
FW-02	Feedwater pump trip, passive cooling via RCCS	5E-04	<1E-05
CR-02	Rod withdrawal, forced cooling via SU/SD	5E-04	<1E-05
MD-01	Medium helium break, isolation, forced cooling via SU/SD	5E-04	3E-05

Table 6. (continued).

SD-02	Small helium leak, isolation, forced cooling via main-loop	5E-04	1E-05
SD-10	Small helium leak, passive cooling via RCCS, pump down successful	5E-04	2E-04
MD-02	Medium helium break, no isolation, forced cooling via SU/SD	5E-04	3E-05
LO-09	Loss of offsite power < 24 hr., forced cooling via SU/SD	4E-04	<1E-05
LF-01	Loss of offsite power, passive cooling via RCCS	4E-04	<1E-05
LO-05	Loss of offsite power < 3 hr., passive cooling via RCCS	4E-04	<1E-05
LO-03	Loss of offsite power < 3 hr., passive cooling via RCCS	3E-04	<1E-05
LO-16	Loss of offsite power < 24 hr., passive cooling via RCCS	2E-04	<1E-05
SG-02	Steam generator tube rupture, isolation and dump, forced cooling via SU/SD	9E-05	1E-05
SG-04	Steam generator tube rupture, isolation, dump stuck open, forced cooling via SU/SD	9E-05	1E-05

Table 6. (continued).

SG-18	Steam generator tube rupture, no isolation, forced cooling via SU/SD	9E-05	2E-04
SG-09	Steam generator tube rupture, isolation, dump fails to open, forced cool ing via SU/SD	9E-05	1E-04
SD-14	Small helium leak, no isolation, passive cooling v ia RCCS	5E-05	4E-04
TT-04	Turbine trip, passive cooling via RCCS	5E-05	<1E-05
MD-14	Medium helium break, passive cooling via RCCS	5E-05	2E-04
FW-04	Feedwater pump trip, circulator trip fails, passive cooling via RCCS	4E-05	<1E-05
CT-05	Circulator trip, passive cooling via RCCS	4E-05	<1E-05
LO-12	Loss of offsite power < 24 hr., passive cooling via RCCS	3E-05	<1E-05
SD-03	Small helium leak, isolation, forced cooling via S U/SD	3E-05	1E-05
LO-10	Loss of offsite power < 24 hr., passive cooling via RCCS	2E-05	<1E-05
LO-19	Loss of offsite power > 24 hr., passive cooling via RCCS	2E-05	<1E-05

Table 6. (continued).

FW-06	Feedwater pump trip, circulator trip fails, passive cooling via RCCS	1E-05	<1E-05
SG-20	Steam generator tube rupture, no isolation, open PSRV, passive cooling via RCCS	1E-05	2E-02
SG-12	Steam generator tube rupture, isolation, stuck open PSRV, forced cooli ng via SU/SD	1E-05	5E-03
LO-17	Loss of offsite power > 24 hr., passive cooling via RCCS	9E-06	<1E-05
FW-12	Feedwater pump trip, circulator trip fails, open PSRV, passiv e cooling via RCCS	7E-06	<1E-05
LD-01	Large helium break, passive cooling via RCCS, re actor building success	7E-06	8E-05
MD-02	Medium break, isolation, forced cooling via SU/S D	6E-06	3E-05
SD-11	Medium helium leak, no isolation, passive coolin g via RCCS, pumpdown	6E-06	2E-04

Table 6. (continued).

MD-12	Medium helium break, no isolation, passive cooling via RCCS	6E-06	3E-04
CR-03	Rod withdrawal, passive cooling via RCCS	5E-06	<1E-05
MD-26	Medium helium break, no isolation, forced cooling via SU/SD	5E-06	2E-04
MD-03	Medium helium break, isolation, passive cooling via RCCS	5E-06	3E-05
CT-04	Circulator trip, passive cooling via reactor building	2E-06	<1E-05
LD-02	Large helium break, passive cooling via RCCS, reactor building failure	2E-06	8E-05
LD-09	Large helium break, passive cooling via RCCS, reactor building failure	1E-06	8E-05
SG-05	Steam generator tube rupture, isolation, dump stuck open, passive cooling via RCCS	1E-06	2E-05
TT-06	Turbine trip, passive cooling via RCCS	1E-06	<1E-05
SG-10	Steam generator tube rupture, isolation, open PSRV, forced cooling via SU/SD	1E-06	2E-05

Table 6. (continued).

SG-25	Steam generator tube rupture, no isolation, no feedwater pump trip, forced cooling success	8E-07	8E-04
SD-15	Small helium leak, no isolation, passive cooling via RCCS	6E-07	4E-04
MD-15	Medium helium break, no isolation, passive cooling via RCCS	6E-07	2E-04

Appendix B.

The following depicts the human reliability analysis (HRA) event trees as used by the Technique for Human Error Rate Prediction (THERP) methodology. HRA event trees are graphical task analysis approaches to track the correct and incorrect human actions and quantify HEPs. Figure 14 depicts the HRA event tree of a series and parallel systems as illustrated in [27]. The system depicted in Figure 14 consists of two actions, where the series system requires both human actions to be successful for the system to be successful, and the parallel system requires only one of the two actions to be successful.

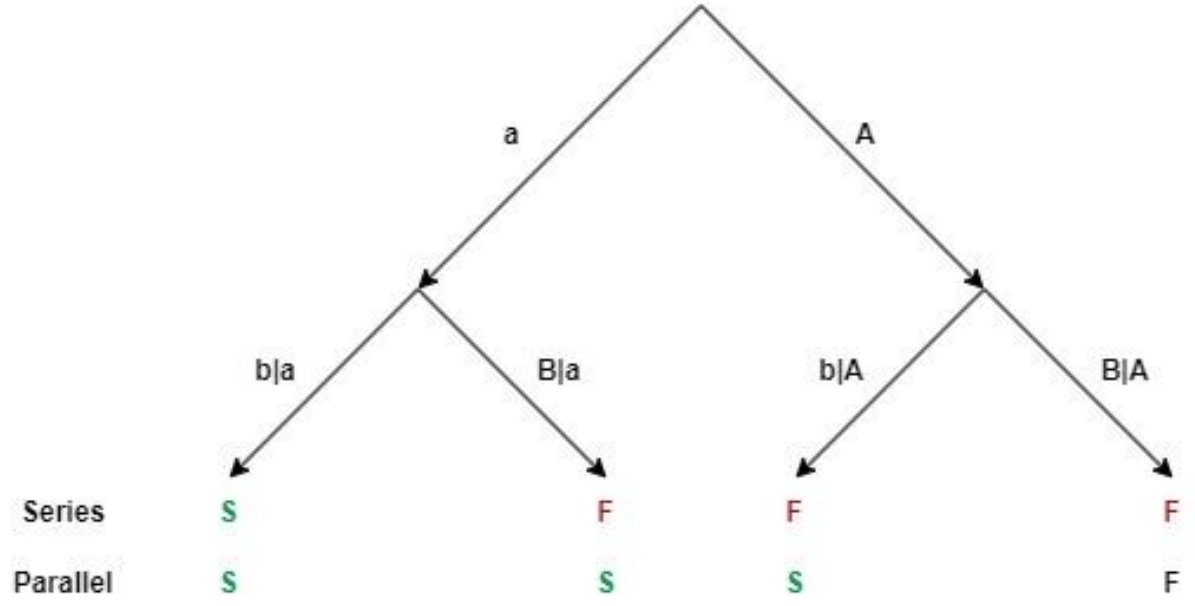

Figure 14. HRA Event Tree for Series or Parallel System.

It should be noted that:

- Task “A” represents the first human action
- Task “B” represents the second human action
- “a” represents the probability of a successful performance of action “A”

- “A” represent the probability of a failure in performing action “A”
- “b|a” and “b|A” represent the probability of a successful performance of action “B” given a successful performance and unsuccessful performance of action “A,” respectively.
- “B|a” and “B|A” represent the probability of an unsuccessful performance of action “B” given a successful performance and unsuccessful performance of action “A,” respectively.
- “S” and “F” represent the success and failure of the entire system, respectively.