NATIONAL CENTRE FOR NUCLEAR RESEARCH ŚWIERK

Doctoral Thesis

Probabilistic Safety Assessment for High Temperature Gas-cooled Reactors

Mina Torabi

This dissertation is submitted in partial fulfilment of the requirements

for the degree of

Doctor of Physical Sciences

at the

National Centre for Nuclear Research

Supervisor: Prof. dr. hab. Mariusz P. Dąbrowski

Auxiliary supervisor: Dr. Karol Kowal

June 2023

Acknowledgements

Although, a Ph.D thesis is an individual activity, I could not have achieved it without the help, inspiration, contribution and encouragements of many people who have crossed my path.

First of all, I would like to appreciate my supervisor, Professor Mariusz Dąbrowski, for his guidance and support in my Ph.D. dissertation, without which the completion of this work would not have been possible. I would also like to acknowledge my auxiliary supervisor, Dr. Karol Kowal, for his invaluable assistance throughout the course of my Ph.D. journey. His guidance have been instrumental in shaping the direction of my research and greatly contributing to the completion of my Ph.D. dissertation. I would also like to extend my thanks to Dr. Sławomir Potempski for his review of our papers and guidance. His insights and feedback have been invaluable in refining our work and enhancing its quality.

I wish to express my sincerest gratitude to Professor Niemela, and Dr. Voigt, for their invaluable support which have aided me to improve my Ph.D path and for being great friends.

I am grateful to my friends, especially: Tomasz, Ewelina, Mateusz, Michał(s), Zuzanna, Hisham, Marek, Nairi, and Eryk, for making my five years unforgettable. Special thanks to my Iranian friends in Warsaw for their friendship and solidarity, which eased my adaptation.

Most importantly, my deepest gratitude goes to my beloved husband, Mohsen, for his unwavering love, support, and mentorship during my Ph.D. journey. I am also grateful to my parents, Enshaallah and Zahra, sisters Leila and Mahsa, brothers Ali and Arash, and my nephew Arsam, for their continuous support and encouragement. I am blessed to have such a loving and supportive family who has been by my side, cheering me on every step of the way.

I dedicate this thesis from the bottom of my heart to all brave Iranian women and men who have inspired me with their courage and perseverance. Their resilience and determination have been an inspiration to me, and I am honored to dedicate this work to them . . .

Abstract

This thesis presents an extension of the Probabilistic Safety Assessment (PSA) oriented toward applicability in High Temperature Gas-cooled Reactors (HTGRs). The PSA methodology is a widely used approach for evaluating the safety and reliability of Nuclear Power Plants (NPPs). It plays a pivotal role in the licensing process by providing a quantitative evaluation of potential accident sequences and the associated risks which can be used to identify and prioritize potential scenarios, and to improve the reactor design. The objective of this research is to improve the standard PSA analysis by incorporating life-cycle simulations of systems reliability and availability, as an alternative to the conventional static Event Tree (ET) and Fault Tree (FT) calculations. The study focuses on addressing the limitations of the PSA methodology in the context of HTGR applications and adapting it to the unique operational conditions and safety features of HTGRs. To achieve these goals, the traditional PSA model is developed, encompassing ET and FT analyses for a representative initiating event in HTGRs, specifically focusing on the Loss of Forced Cooling accident(LOFC). Furthermore, the novel approach is proposed to replace the standard FTs with comprehensive life-cycle simulations, enabling a more accurate assessment of system reliability and availability within the PSA models. The proposed methodology is applied to the High-Temperature engineering Test Reactor (HTTR) as a reference HTGR, with a specific emphasis on the Depressurized Loss of Forced Coolant Accident (DLOFC) variant. By analyzing the frequency of LOFC and its associated risks, the proposed approach demonstrates its effectiveness in providing a comprehensive evaluation of potential accidents in HTGRs. Moreover, the improved PSA methodology proves to be adaptable and effective in assessing the risks associated with a range of potential accidents in HTGRs. The findings of this work indicated that the improved PSA methodology is a

comprehensive and valuable tool for the design and safety evaluations of HTGRs. The new method reflects the unique characteristics and operational conditions of HTGRs, thus providing a more realistic assessment of potential risks and crucial insights for reliable and safe operation.

Streszczenie

Niniejsza rozprawa dotyczy rozszerzenia metod Probabilistycznych Analiz Bezpieczeństwa (PSA) na zastosowania w wysokotemperaturowych reaktorach jądrowych chłodzonych gazem (HTGR). Metodyka PSA to powszechnie stosowane podejście do oceny bezpieczeństwa i niezawodności elektrowni jądrowych. Odgrywa ona kluczową rolę w procesie licencjonowania, zapewniając ilościową ocenę potencjalnych sekwencji awarii i związanych z nimi ryzyk, które można wykorzystać do identyfikacji i uporządkowania potencjalnych scenariuszy awarii oraz do udoskonalenia projektu reaktora. Celem niniejszej pracy było ulepszenie standardowego podejścia do analiz PSA poprzez zastosowanie symulacji niezawodności i dostępności w ciągu całego cyklu życia reaktora, jako alternatywy dla klasycznych obliczeń, bazujących na statycznych modelach drzew zdarzeń i uszkodzeń. Praca koncentruje się na uwzględnieniu ograniczeń metodologii PSA w kontekście jej zastosowania do reaktorów wysokotemperaturowych oraz dostosowania jej do unikalnych warunków eksploatacji i cech bezpieczeństwa HTGR. W tym celu, opracowane zostały standardowe modele PSA, obejmujące drzewa zdarzeń i drzewa uszkodzeń dla reprezentatywnego zdarzenia inicjującego w HTGR, tj. utraty wymuszonego przepływu chłodziwa (LOFC). Następnie, zaproponowane zostało nowe podejście, w którym drzewa uszkodzeń zastąpiono przez kompleksowe symulacje cyklu życia reaktora, umożliwiające m.in. dokładniejszą ocenę niezawodności i dostępności systemów w ramach modeli PSA. Zaproponowana metoda została zastosowana dla reaktora HTTR (High-Temperature engineering Test Reactor), jako referencyjnego HTGR, ze szczególnym uwzględnieniem wariantu utraty wymuszonego przepływu chłodziwa ze stratą ciśnienia (DLOFC). Analiza częstości LOFC i związanego z tym ryzyka pokazuje, że ta metoda zapewnia bardziej kompleksową ocenę potencjalnej awarii w HTGR. Ponadto, ulepszona metodyka PSA okazuje się elastycznym i

skutecznym podejściem w ocenie ryzyka związanego z szeregiem potencjalnych awarii HTGR. Wyniki tej pracy wskazują, że ulepszona metodologia PSA jest użytecznym narzędziem do projektowania i oceny bezpieczeństwa HTGR. Nowa metoda odzwierciedla unikalne cechy i warunki pracy HTGR, zapewniając w ten sposób bardziej realistyczną ocenę potencjalnych zagrożeń i kluczowe wnioski dla niezawodnej i bezpiecznej eksploatacji.

Table of contents

List of figures

List of tables

List of Abbreviations

AC	Accident Condition	**FMEA**	Failure Mode and Effect Analysis
ACS	Auxiliary Cooling System	**FOR**	Forced Outages Rate
AOO	Anticipated Operational Occurrence	**FP**	Fission Product
APS	Emergency Air Purification System	**FT**	Fault Tree
ASN	Nuclear Safety Authority	**FTA**	Fault Tree Analysis
CDF	Core Damage Frequency	**FTO**	Failure to Operate
CET	Containment Event Tree	**FTS**	Failure to Supply
CHD	Coaxial Hot-gas Duct	**GTG**	Gas Turbine Generator
CIV	Containment Isolation Valves	**HGB**	Hexagonal Graphite Blocks
CNF	Cumulative Number of Failures	**HPS**	Helium Purification System
CSP	Cooling System Pipes	**HTGR**	High Temperature Gas Cooled Reactor
CWP	Cooling Water Panel	**HTTR**	High Temperature Engineering Test Reactor
DBA	Design Basis Accident	**HV**	High Voltage
DEC	Design Extension Conditions	**HX**	Heat Exchanger
DiD	Defence in Depth	**IIP**	Insufficient Input Power
DLOFC	Depressurized Loss Of Forced Cooling	**JAEA**	Japan Atomic Energy Agency
EAP	Emergency Air Purification System	**LB**	Lower Boundary
EF	Electrical Facility	**LERF**	Large Early Release Frequency
ETA	Event Tree Analysis	**LOFC**	Loss Of Forced Coolant
FCM	Fuel Compact Matrix	**LOOP**	Loss Of Offsite Power

LOR	Loss Of Redundancy
LV	Low Voltage
LWR	Light Water Reactor
MCUP	Minimal Cut-Sets Upper Bound
MTTR	Mean Time To Repair
NC	Normally Closed
NO	Normally Open
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
PCS	Primary Cooling System
PGC	Primary Gas Circulator
PLOFC	Pressurized Loss Of Forced Cooling
PPWC	Primary Pressurized Water Cooler Cooling
PSA	Probability Safety Assessment
PSU	Power Supply Unit
PWC	Pressurized Water Cooler
PWCS	Pressurized Water Cooling System
RBD	Reliability Block Diagram
RCV	Reactor Containment Vessel
RES	Reactor Electric System
RPN	Risk Priority Number
RPV	Reactor Pressure Vessel
RSS	Reactor Scram System
RVS	Reactor Ventilation System
SA	Spurious Action
SC	Short Circuit
SO	Spurious Operation
SPWC	Secondary Pressurized Water Cooler
TRISO	Tri-Structural Isotropic
UB	Upper Bound
UPS	Uninterruptible AC Power System
VCS	Vessel Cooling System

Chapter 1

Introduction

1.1 Background and context

The study and application of nuclear energy as a source of power has been a topic of significant research and advancement in the field of nuclear physics and technology for several decades, leading to the development of safer and more efficient reactor designs and contributing to the global quest for sustainable and clean energy solutions. Among the different types of nuclear reactors, High Temperature Gas-cooled Reactors (HTGRs) have created significant attention for their potential to revolutionize the nuclear energy industry. These reactors, considered to be a type of Generation IV concept, are designed for deployment in a cogeneration mode which is firstly a high temperature heat production apart from electricity generation and hydrogen production [6]. They provide several advantages over traditional Light Water Reactors (LWRs) such as increased efficiency, improved safety features, and the ability to utilize two fuel options either prismatic or pebble bed fuel elements. This makes the development and implementation of HTGR technology a crucial area of focus within the nuclear energy industry. These reactors are characterized by their use of graphite as a moderator and helium gas as a coolant, which allows for the achievement of high outlet temperatures in the range of 750-950°C. The safety systems of HTGRs are primarily designed to rely on passive features, resulting in an inherently safe operating behaviour. The passive safety features of HTGRs can be listed as follows:

- Tri-Structural Isotropic fuel particles (TRISO) : The use of TRISO fuel particles (small ceramic particles containing uranium dioxide fuel in the form of a coating) provides inherent safety by preventing the release of Fission Products (FPs) even at high temperatures.

- High-temperature capability: The use of graphite as a moderator and helium gas as a coolant allows HTGRs to operate at high temperatures, which increases the thermal efficiency of the reactor and reduces the risk of coolant boiling and subsequent damage to the reactor.
- Passive cooling: In case of a loss of coolant accident, the design of HTGRs is such that the residual heat is removed by natural convection and radiation, without relying on active cooling systems. This results in a safe shutdown of the reactor without the need for operator intervention.
- Double containment: HTGRs are designed with a double containment system, which provides an additional layer of protection against the release of radioactive materials in the unlikely event of a primary containment failure.
- Negative temperature coefficient of reactivity: The fuel in HTGRs is designed to have a negative temperature coefficient of reactivity, which means that as the temperature increases, the reactivity of the fuel decreases, resulting in a self-regulating effect that reduces the likelihood of a uncontrolled chain reaction.
- Inherent shutdown: HTGRs have an inherent shutdown capability, where a loss of cooling or other abnormal events will cause the reactor to shut down automatically, without relying on operator intervention.

However, despite the inherent safety features and potential benefits of HTGRs, a thorough and accurate assessment of their safety and profitability is crucial for their successful deployment, particularly in accordance with legal requirements and regulations. One key aspect of this assessment is the use of Probabilistic Safety Analysis (PSA) methodologies. These methodologies have been traditionally developed for LWRs, which may not accurately reflect the unique characteristics of HTGRs. Therefore, there is a need for the improvement and implementation of PSA methodology that are tailored specifically to the design and safety features of HTGRs. The use of data-driven approaches and advanced techniques can provide a more comprehensive understanding of the safety and reliability of HTGRs.

The main goal of this research is to overcome the limitations of traditional PSA methodologies by creating a new approach for the unique features and operational conditions of safety-related systems of HTGRs. This new approach incorporates the use of life-cycle reliability and availability simulations, to provide a more comprehensive and accurate assessment of the safety and reliability of HTGRs by taking

into account the particularities and safety characteristics of HTGRs. Overall, this research will provide crucial insights for the design and development of safer and more efficient HTGRs.

In this research, the experimental High Temperature Engineer Test Reactor (HTTR) [59] developed by the Japan Atomic Energy Agency (JAEA) is selected as a case study for the application of PSA in HTGRs. The HTTR, which is the first of its kind in Japan, was designed and established by JAEA to serve as a research facility for the advancement of HTGR technology. The HTTR has been operated and tested extensively by JAEA, providing valuable experimental data and insights for the evaluation of the safety features, performance, and hydrogen production capabilities of the future commercial HTGRs. Additionally, the experimental data and insights provided by the HTTR will be used to analyze and improve PSA methodologies specifically for HTGRs and provide valuable insights for the design and development of safer and more efficient HTGRs. The outcome of this study will be instrumental in promoting the safe and sustainable operation of future HTGRs, and will serve as a valuable resource for licensing and regulatory considerations.

1.2 Research objectives and hypothesis

The primary objective of this research is to improve the PSA standard approach for the HTGRs through incorporation of the referential initiating event of Depressurized Loss of Forced Coolant (DLOFC) accident, taking into account the characteristics of safety-related systems of HTGRs. The resulting approach, once developed, can also be applied to other accident scenarios. The goal is to consider the differences in the mitigation safety systems functions between LWRs and HTGRs under accident conditions, in order to improve PSA methodologies for HTGRs by incorporating these characteristics and safety features into the Fault Tree Analysis (FTA) as well as Event Tree Analysis (ETA).

The **main hypothesis of this research is that the application of life-cycle reliability and availability simulations instead of standard Fault Tree (FT) method improve the standard PSA methodology by taking into account realistic operational conditions of HTGR safety systems**. In order to verify this hypothesis, the research aims to implement a traditional PSA model including an ET and the conventional FTs for a referential initiating event (i.e. DLOFC). **Subsequently, the method for substituting the FTs with life-cycle simulations of the systems reliability and availability will be initiated within the PSA model. Finally, a comparative analysis will be conducted on the results obtained from the standard and innovative approaches.**

This research is driven by the need to address the limitations in the standard PSA methodology for LWRs and enhance its capability to accurately evaluate the safety and reliability of HTGRs. This is due to the fact that **the conventional PSA approach may not fully take into account the specific characteristics and operating conditions of safety systems of HTGRs, leading to potential inaccuracies in its safety assessments.** The proposed study aims to address this challenge by developing a comprehensive and customized PSA methodology that considers the unique features of HTGRs. This methodology can be used to more effectively analyze and predict the behaviour of these reactors during different accident scenarios, thereby improving the safety and reliability of these reactors.

Chapter 2

Exploring PSA approaches in nuclear power plants

2.1 FMEA as a complementary tool in PSA methodology

The FMEA [13, 62] is a widely used method and is often employed in field of PSA. This structured and systematic approach evaluates different system components, considering the possibility of component failure due to various inevitable factors such as poor design, manufacturing defects, ageing, and environmental factors [67].

The FMEA provides numerous benefits through its systematic approach. The early identification of potential problems during the design phase of a complex system enables prompt resolution, reducing the possibility of incurring expensive and time-consuming repairs or upgrades. Furthermore, the FMEA approach can be applied to existing systems, providing a comprehensive evaluation of the potential impact of proposed modifications and thus, optimizing system reliability and minimizing the risk of failure. Tang et al. [70] demonstrated the effectiveness of the FMEA method through its utilization in identifying crucial maintenance items. A comprehensive review of the FMEA application issues, opportunities for improvement, and integration of FMEA with other methods was presented by Spreafico, et al. [66].

Application of FMEA in the NPP industry dates back to the 1960s when the method was first introduced in the aerospace sector [45]. The early application of FMEA in aerospace aimed to ensure the reliability and safety of these systems, where even minor failures could have severe consequences.

This success quickly caught the attention of the NPP industry, which similarly required reliable risk management practices to maintain the safety and reliability of their complex systems. By the 1970s, FMEA was widely adopted and applied within the NPP industry as concerns over safety and reliability grew amid rapid expansion of this sector. The method was seen as a way to reduce the risk of failures, accidents, and malfunctions and to enhance overall safety and reliability of NPP facilities [45]. Over the years, FMEA has continued to evolve and improve to meet the changing needs of NPPs and other industries. Despite these modifications, the core principles of FMEA remain unchanged and the method remains widely used as a robust and effective tool for risk management and improvement.

Today, as mentioned above, FMEA is a critical background element of PSA in the NPP industry, playing an essential role in ensuring the design and operation of NPP systems maximizes their reliability and minimizes risk of failure. The results of the FMEA analysis can also inform the ongoing maintenance and improvement of these systems, as well as support decision-making and risk management in the case of potential accidents or incidents. Researchers and practitioners have made significant contributions to improve the FMEA method, making it more comprehensive, efficient, and effective. For instance, new risk assessment techniques have been developed to more effectively prioritize potential failure modes, and software tools have been created to automate the FMEA process [91, 47, 65]. The continued evolution and refinement of the FMEA method demonstrate its importance and relevance in maintaining safety and reliability in NPPs and other industries [87, 39, 91, 47, 65].

The use of FMEA in PSA of HTGR facilities has received considerable attention in recent years. This is due to the effectiveness of the FMEA methodology in identifying and addressing potential failures that may impact the availability and reliability of the plant components and systems. For instance, in the paper by Cadwallader et al. [15], FMEA was applied to an HTGR facility to identify and correct failures in a cost-effective manner, thereby increasing the overall availability and reliability of the plant. Our study [72] demonstrates the effectiveness of FMEA in risk assessment of the electrical system in an HTGR-based plant. Additionally, Guimaraes et al. [26] proposed a novel approach to safety analysis in HTGRs, which involved combining FMEA with hazard and operability study. The increasing use of FMEA in HTGR PSA highlights the importance of this method for providing valuable insights into the safety and reliability of these systems. The continued advancement and refinement of the FMEA method, highlights its significance and relevance in the NPP industry and beyond.

The FMEA process involves several well-defined steps, including the definition of the system and its components, identification of potential failure modes, evaluation of their effects, determination

of likelihood of occurrence, and calculation of the Risk Priority Number (RPN) [87]. The RPN is a key output of the FMEA analysis, serving as a numerical representation of the risk associated with each failure mode. It is determined through the multiplication of the ***Severity*** (***S***), ***Occurrence*** (***O***), and ***Detection*** (***D***) parameters of a particular failure mode. These parameters serve to characterize and evaluate the inherent and probable characteristics of each failure mode on a scale of 1 to 10. The resulting RPN, derived by multiplying these parameters, ranges from 1 to 1000 and offers a comprehensive evaluation of the risk. The use of RPN as a qualitative method provides a convenient means of synthesizing the results of the FMEA analysis, facilitating decision-making processes in risk management. The FMEA process can be repeated periodically to ensure its results remain relevant and to consider any newly identified failure modes.

In this study, the FMEA method will be applied to the electrical system and VCS of the HTTR, both of which are critical systems for ensuring the safe operation of the reactor under both normal and abnormal conditions. Despite being a widely recognized tool in the field of PSA, the application of the FMEA method to the HTTR EF and VCS has not been explored yet in the literature. However, such analyses for power systems have been considered several times in the literature. To date, limited studies have addressed the application of FMEA for cooling systems [27, 30]. The innovative FMEA-based Gradual Screening Approach is also proposed in this research aims to identify the failure modes that have the greatest impact on the reliability of the EF of the HTTR. The results of the FMEA analysis will contribute valuable insights to the operational reliability analysis of the system.

In the context of PSA, the FMEA methodology plays a critical role in ensuring that complex systems are designed and operated with maximum reliability, thereby minimizing the risk of costly downtime and recovery procedures. FMEA results can be used to develop event trees and fault trees, which help identify potential accident scenarios, calculate their likelihoods, and estimate their consequences. The FMEA process involves evaluating potential failure modes of components and assessing their impact on the overall system. The insights gained from this process inform decision-making, such as necessary changes to design or operation and prioritizing investments in safety-critical components. Overall, FMEA is a key step in developing a comprehensive risk management plan for complex systems, and is a valuable tool in the context of PSA.

2.2 Standard PSA approach in NPPs

PSA [32] has emerged as one of the indispensable systematic and comprehensive tools for evaluating probabilistic safety aspects throughout the life-cycle of complex engineering and technological systems, particularly in the nuclear power industry [37], where safety is of utmost importance [73]. PSA has a long-standing tradition of being applied in the nuclear power industry, starting with its widespread adoption in the 1970s and 1980s [37]. This methodology was first officially established in the WASH-1400 report [19] as a result of safety studies of LWRs. The objective of this study was to compare the acceptability of NPP risks with other risks faced by the public including both involuntary risks (e.g. natural disasters, environmental pollution) and voluntary risks (e.g. smoking, participating in extreme sports), in order to provide a more comprehensive understanding of how the public perceives the risks associated with NPPs.). Since then, PSA has become an essential tool in ensuring safety and risk management in NPPs, providing a reasonably complete identification of any accident progression scenarios and evaluating the effectiveness of mitigating systems and components.

In recent years, numerous PSAs have been conducted for a significant number of NPPs. As an example of the PSA implementation, it is extensively used by the US Nuclear Regulatory Commission (USNRC) to review and evaluate the safety of existing and proposed NPPs [19]. The NRC has utilized PSA in the licensing and regulation of NPPs in the country, as a means to ensure that safety risks are thoroughly evaluated and mitigated. In France, the French Nuclear Safety Authority (ASN) has utilized the capabilities of PSA to carry out a comprehensive evaluation of the safety of its NPPs [24]. This involves the integration of PSA into both the licensing process and ongoing monitoring and analysis of the plants' safety performance. PSA is deemed a crucial tool in ensuring safety and risk management, as it provides a thorough identification of potential accident progression scenarios and an evaluation of the effectiveness of safety-critical systems and components in mitigating these risks.

One of the key approaches in standard PSA is FTA [74], which is used to identify potential failure scenarios and evaluate the probability of their occurrence. For example, in the context of a NPP, FTA may be used to analyse the potential failure of a coolant pump, and evaluate the likelihood of such a failure occurring [52]. Another important approach in PSA is ETA [54], which is used to identify potential sequences of events and evaluate the probability of their occurrence. For example, in a NPP, ETA may be used to analyse the potential sequence of events that could lead to a loss of coolant accident, and evaluate the likelihood of such an event occurring [56, 14]. Additionally, FMEA [67] is also used

to identify and classify potential failure modes and associated consequences. For example, in a NPP, FMEA may be used to analyse the potential failure modes of a reactor coolant system, and evaluate the consequences of each failure mode in order to prioritize related failure modes [72]. All FTA, ETA and FMEA are essential tools in PSA for identifying and evaluating potential risks in NPPs. Together, they provide a comprehensive approach for identifying and mitigating safety risks in the design and operation of NPPs.

The implementation of PSA in the design and operation of NPPs can provide a range of benefits, including [85, 49, 42]:

- Incorporating detailed risk insights into the design and operation process, resulting in a more reliable and safer design,
- Supporting decision-making in the risk-informed aspects of the design and licensing process, leading to a more efficient and effective regulatory process,
- Classifying structures, systems, and components based on safety, which can help prevent and mitigate accidents and reduce the likelihood of severe incidents,
- Improving the reliability and availability of safety systems by identifying and eliminating critical failure modes through the use of FMEA and reliability analysis techniques,
- Enhancing overall safety and risk management of the power plant to ensure sustainable operation and increase public confidence.

However, it is essential to continually improve and adapt PSA methodologies to the unique characteristics and conditions of various reactor types, such as HTGRs, to ensure their safe and efficient operation.

It is widely acknowledged that the traditional/standard PSA framework, which is commonly used for LWRs, includes three distinct levels [1–3]. *The first phase models the plant's response to an initiating event that could damage the reactor core. This analysis aims to estimate the frequency of core melt (which does not happen in HTGR). The second phase evaluates the magnitude and probability of releases of radioactive materials that could occur as a result of the core damage during an accident. Finally, the third phase examines the consequences of these releases on public health and the environment.* The results of each level of PSA analysis are used as inputs for the next level, with the output of

each level also being used to meet regulatory requirements, justify design modifications, and inform decision-making strategies.

However, there exist several limitations in traditional PSA approach when applied to LWR, such as assumptions and simplifications made in the analysis which may not accurately represent the complexity of the system and its behaviour during an accident, or the traditional PSA approach may not be able to fully capture the effects of ageing and degradation on the safety performance of a power plant. Furthermore, it is important to note that the *limitations of traditional PSA should be considered when applying it to other types of reactors such as HTGRs.*

2.3 Current PSA strategies for HTGRs

The growth and development of HTGRs have resulted in a renewed interest in performing PSAs for their design and licensing procedures. Although traditional PSA techniques, which are commonly used for LWRs, can be applied to HTGRs, modifications are necessary due to the unique safety characteristics of HTGRs. One such characteristic is the presence of inherent safety features, such as the ability to prevent core meltdown during severe accidents, which sets HTGRs apart from LWRs and highlights the need for specialized PSA techniques [33]. As a result, it has been observed that traditional PSA risk metrics, such as Core Damage Frequency (CDF) and Large Early Release Frequency (LERF) [53], may not be fully capturing the safety features of these reactors, which calls into question the appropriateness of these metrics for HTGRs. The paper [41] highlights the need for innovate PSA approaches to PSA that accounts for such novel technology. Thus, it is crucial to determine the appropriate success criteria for PSA in HTGRs that are tailored to the specific requirements of the application.

To address the limitations of the traditional PSA methodologies for LWRs, innovative modifications have been proposed in the literature, aimed at re-defining the success criteria in terms of core damage prevention and large early release prevention. These alternative approaches shift the focus from traditional criteria such as fuel and reactor pressure vessel temperature to model the release of radioactive material from each barrier in the analysis . The most widely preferred approach is the three-level integrated framework, as presented by Liu, et al. [46]. This framework is a novel integral PSA approach that considers the latest knowledge and research on the safety characteristics of advanced NPPs and uses the HTGR as a case study. Another approach is the integrated format, which combines levels 1 and 2 of

PSA and defines the release categories as the end states of the ET. The integrated framework has been widely endorsed for PSA assessments in HTGRs [4, 71, 21].

In the development of a new PSA framework for HTGRs, it is crucial to consider not only the conventional format requirements, but also the unique characteristics of HTGR safety-related systems during normal and accident conditions that differentiate them from LWRs. This distinction is a crucial aspect of the research, deserving particular attention to ensure a precise and accurate evaluation of the safety performance of HTGRs. An exhaustive examination of these distinguishing attributes, including consideration of the safety components and system's distinct mission time, operation continuity, repairability, and the potential consequences of operational interruptions, is imperative for a comprehensive and accurate evaluation of the safety performance of HTGRs. To account for the differences, a more rigorous and precise analysis must be performed to guarantee the reliability and efficacy of the mitigation measures in the new PSA framework. Such a comprehensive PSA study for HTGR has not been undertaken elsewhere. This updated methodology takes into account the continuous operation of HTGR safety-related systems and provides some more accurate assessment of their safety performance, thus contributing to the overall enhancement of the PSA framework for HTGRs.

The conventional FTA approach applied in PSA studies for LWRs [22] is often limited in its accuracy due to oversimplified assumptions of the safety systems. This approach, assumes the safety systems in LWRs operate in a standby mode and only activate upon demand [14]. In contrast, the most of the safety-related systems in HTGRs operate continuously throughout both normal and accidental conditions [59]. As a result, the traditional FTA approach considers only the mission (activation) time of the system when needed in LWRs, while in the case of HTGRs, the entire life-cycle parameters should be considered in the FTA. One crucial life-cycle parameter that is often neglected in traditional FTA, but can have a significant impact on the PSA results, is equipment ageing. The effect of ageing on the equipment has been demonstrated to play a significant role in the PSA results [75, 18]. In order to address this issue, various methods for considering equipment ageing in PSA have been proposed [17, 76]. Another difference in the traditional FTA approach for LWRs and HTGRs is the consideration of the repair process. In HTGRs, the repair of safety-related systems is considered as a consequence of a failure leading to a reactor scram. The scram of reactors in HTGRs results in a heightened Forced Outage Rate (FOR), which then decreases the overall availability of the power plant. The duration of the repair is, therefore, a crucial factor in determining the operational capability of these facilities. Conversely, the safety systems in LWRs are configured to be in a standby state and only become operational upon

request, and their repair is not taken into consideration in conventional FTA. The repair time, as a result, becomes a critical factor in maintaining the availability of these nuclear power plants. Additionally, the implementation of the Minimal Cut-Sets Upper Bound (MCUP) approximation in conventional FT software during the calculation of PSA may not lead to precise and dependable results.

In light of these limitations, there has been a growing interest in the use of simulation-based techniques to enhance the accuracy of PSA results [81]. This study proposes the integration of life-cycle reliability and availability simulations [40] as a means of improving the conventional FTA approach in PSA studies for HTGRs. This approach replaces the traditional FTA approach with a simulation-based model that takes into account the effects of time, including the impact of ageing, maintenance, and repair activities on system performance and operation. By providing a more realistic representation of the behavior and performance of safety-related systems in HTGRs, the integration of life-cycle simulations into the PSA framework can improve the accuracy of risk assessments and inform decision-making in the management of safety and risk in HTGRs. Currently, no integrated method exists that considers the unique features of the HTGR safety systems. Thus, the proposed integration of life-cycle simulations into the PSA framework has the potential to significantly improve the reliability and efficacy of risk assessments in HTGRs.

The general first step in performing PSA is *to identify and classify all potential initiating events* in the power plant. These events are categorized into four groups: normal operation, Anticipated Operational Occurrences (AOO), Design Basis Accidents (DBA), and Design Extension Conditions (DEC) [34]. The safety databases of HTGRs are not fully provided yet, due to the lack of experience in operation and construction of HTGRs. However, following the purpose of providing safety properties of commercial HTGRs, various comprehensive safety demonstration tests have been launched in HTTR [60] which is the only operational experimental HTGR. However, due to the unavailability of data on HTR-10, a Chinese HTGR of pebble bed type, it remains uncertain whether there are any other operational experimental HTGRs besides HTTR. The experiments include the coolant flow reduction tests to simulate the Loss of Forced Cooling (LOFC) accident. As a results of such experiments it is shown that among all initiating events within the HTGRs, the DLOFC as a DBA, is determined as one of the most severe accidents in HTGRs for the safety barriers to withstand. The potential consequences of DLOFC include low heat removal as a consequence of no flow condition as well as graphite oxidation as a result of potential air ingress. Depending on the initial conditions and underlying assumptions in DLOFC, the FP emission through the coolant release is another important consequence to be taken seriously.

The general purpose of the presented study is to propose an improved and efficient PSA approach associated with the DLOFC accident in HTTR which would be applicable for all initiating events in all HTGR designs. Initially, a traditional PSA approach will be employed, by modelling the accident progression using standard ET and FTs. Although a standard ET for the DLOFC in the HTTR has been created elsewhere [51], the role of the emergency air purification system, a crucial safety-related system in preventing the release of FPs, has not been considered. Then, the simulation results will be employed in standard ET and the results of the proposed PSA will be compared with the standard PSA to evaluate the efficacy of this new approach in providing a more accurate and realistic assessment of the risk associated with HTGRs.

Chapter 3

An innovative PSA approach for HTGRs

3.1 Extending FMEA methodology for HTGR

The FMEA is one of the widely-used analytical methodologies in the field of PSA. It serves as a powerful complementary tool for PSA to identify potential failure modes and evaluate their impact on the system or a component. The FMEA methodology adopts a systematic approach aimed at preventing failures and improving the design and operation of the system. It is a valuable technique for minimizing the risk of potential failures and enhancing the overall safety of the system.

The criticality of system failures is determined by asking three key questions [45, 66, 67]:

- What can go wrong?
- How likely is it to happen?
- How severe are the consequences?

These questions guide the classification of potential failure modes of the system or components. As discussed in Section 2 (page 9), the *RPN* is a key output of the FMEA analysis, representing the risk associated with each failure mode and determined through the multiplication of the S, O, and D parameters. The outcomes are typically documented in FMEA tables, which cover the three major parameters. These parameters are rated on a discrete scale, usually between 1 and 10, and are used to prioritize the risks associated with each potential failure mode.

In this study, the FMEA methodology was applied to identify and evaluate the failure modes of two critical safety systems in HTTR: the EF and VCS. The FMEA was also used to simulate the

reliability of both systems. In general, The FMEA methodology presents a systematic approach for identifying and evaluating potential failure modes and assessing associated risks. This analysis provides a comprehensive understanding of the safety risks associated with the system or component under consideration. The results of this analysis can be used to optimize system design and operation, mitigate risks, and ultimately enhance system safety and reliability.

FMEA severity rating

Severity refers to the seriousness of the potential consequences resulting from a single failure, and is categorized based on the degradation state of functionality of items. This can apply to either a single system or the entire facility and may encompass various aspects such as regulatory compliance, safety, environmental protection, and profitability. Each severity level can be distinguished by identification of more detailed criteria of possible consequences. The criteria are structured with respect to the purpose(s) of the study.

FMEA occurrence rating

Occurrence is a quantitative estimation of the frequency of a failure mode, representing the expected number of times a particular type of event will occur due to a given factor over the anticipated lifetime of the analyzed system. The occurrence can be estimated by the failure rate parameter (λ), which is typically expressed in failures per unit time (e.g., 1/h or 1/year), or by the Cumulative Number of Failures (CNF) per 100 or 1000 components during expected lifespan of the system being analyzed.

While the order of magnitude of the failure rate parameter is a simple quantitative criterion for determining occurrence, more accurate categorization may be required for very high or very low values to ensure that failure modes with the same occurrence rank can be compared in terms of their influence on system reliability. For example, failure rates between 1 and 9 per 100 years can be treated as comparable, but not those between 1 and 9 per year. Moreover, analyzing real-world data can provide information about the range of failure rates for different component types, and the rating scale of occurrence can be adjusted accordingly, such as using the main percentiles of the actual data distribution to define frequency ranges.

FMEA detection rating

Detection plays a crucial role in FMEA, as it determines the system's ability to identify faulty components through existing detection means before they cause significant performance degradation. Early detection can minimize the impact of a failure, as preventative actions can be taken to prevent further failure of the item or the system. Therefore, it is essential to consider the detection capability of the system as part of the FMEA process. The prioritization of two failure modes of the same severity and occurrence rating can vary greatly based on their detectability. The development of a suitable rating scale for detection depends on the analysis objectives and system design maturity, and may incorporate mixed qualitative and quantitative criteria tailored to specific needs and capabilities.

In order to evaluate the detectability of failure modes, some criteria must be established that address key questions related to the failure modes. These may include, but are not limited to, the following:

- Can the failure be identified before it causes significant deterioration of the system?
- Can the failure be recognized during tests or maintenance activities? If so, are the scope and frequency of such activities adequate for early symptom identification, and are the inspection procedures effective for detecting early symptoms? Does the organizational culture promote early notification of failure symptoms, and are there training programs in place to enhance personnel skills in early symptom detection?
- Can the failure mode be detected by measuring any physical quantity? If so, can direct measurement provide the desired information about a particular component, and how many sensors are applied to control a particular component (directly/indirectly)? Are the sensors capable of detecting a specific root cause of failure or only the symptoms? Is engineering process control integrated with long-term statistical process control?
- Is there any other detection mechanism? If so, what is its effectiveness, and what factors influence its effectiveness?

However, in Detection rating where the ability to detect failure is unknown or cannot be estimated, the FMEA methodology suggests that the detection rank be set to 10.

3.1.1 FMEA of HTTR electrical system

HTTR electrical system structure

Fig. 3.1 [59] shows a schematic diagram of the Electrical Facility (EF) in the HTTR. This facility comprises various components and systems, including a commercial Offsite Power Line, a High Voltage (HV) AC Power System, four Low Voltage (LV) AC Power Centers (A, B, C, and D), an Uninterruptible AC Power System (100 V), a DC Power System (100 V), and a Computer Power Providing System (100 V).

Offsite power line

The HTTR's High Voltage AC Power System is powered by a commercial Offsite Power Line, which is connected to the electricity transmission grid for power distribution. The HTTR's electrical structure, as shown in [59], includes only one Offsite Power Line.

High voltage AC power system (6600 V)

The High Voltage AC power system in the HTTR comprises a 6600 V Bus and the Main HV Breaker, where the former is responsible for the distribution of power to four Low Voltage (LV) Power Centres and the Primary Gas Circulators (PGCs) of the Pressurized Water Cooler (PWC).

Low voltage AC power system (440 V)

The LV AC power system of HTTR receives power from the HV line, which is connected through independent transformers A, B, C, and D. Each LV power bus has a unique load that cannot be supplied through another power bus. In the event of a loss of offsite power, two independent Gas Turbine Generators (GTGs) A and B provide energy to the Power Centres A and B, respectively, where the safety-class loads are connected. One of the GTGs ensures a safe reactor shutdown. However, there is no switch between power centres to enable power transfer from one generator to another. LV Buses C and D, which deliver power to non-safety-class loads, are supplied only from the offsite power.

DC power system (100 V)

The DC Power System of the HTTR comprises two battery systems with equivalent capacities, capable of supplying power for up to 10 hours. The batteries are charged during periods of offsite power availability,

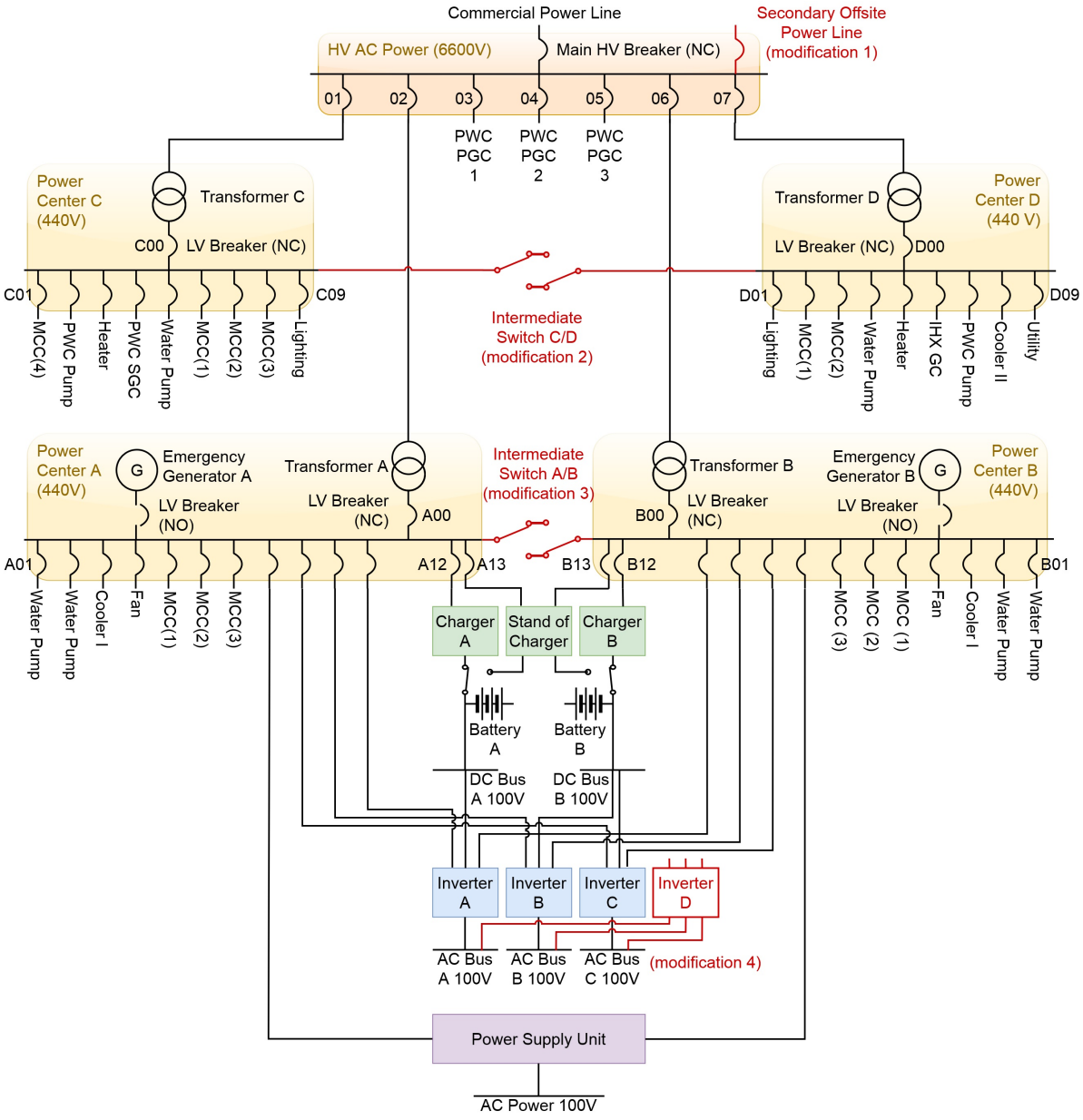

Fig. 3.1 Standard configuration of the HTTR EF (NC – Normally Closed, NO – Normally Open) with three modifications (marked by red line) considered in terms of system reliability improvement, taken from [42].

and the power is then delivered to the DC Bus A and B. In the event of offsite power loss, the safety loads are powered by the batteries. Two independent Chargers A and B supply power to the respective batteries, while the Standby Charger serves as a backup power source and is connected to both Power Centers A and B.

Uninterruptible AC power system (100 V)

The Uninterruptible AC Power System (UPS) of HTTR is comprised of three inverter units, each supplied by Power Centers A and B. In the event of loss of both power lines, the UPS delivers power to the safety instrumentation channels located in 100 V DC Bus A and B and C through the inverters, using energy from the batteries.

Computer power providing system (100 V)

The HTTR plant includes a computer power providing system that supplies power to the non-safety equipment, including computers, control panels, and other instrumentation. The system comprises a 100 V AC Bus and a Power Supply Unit (PSU), which redundantly takes electrical power from both Power Centers A and B. This ensures a reliable and uninterrupted power supply to the non-safety equipment during normal operation.

FMEA Severity rating of electrical system

In the case of HTTR's EF, FMEA was conducted to determine the reliability of normal operations and identify the frequency of failures that may result in unplanned reactor shutdowns. Severity ratings were assigned based on the importance of electrical loads that could be lost due to associated failure modes, as shown in Tab. 3.1.

The ranking scale ranged from 1 to 10, with 1-3 assigned to loads with redundant power sources and non-safety-class equipment connected to Power Centers C or D, and 4-7 assigned to 100 V AC/DC loads and single safety-class loads powered by Power Centers A or B. The higher rankings of 8-9 were given to scenarios where there is a loss of all safety-class items A or/and B due to insufficient input power, which would require starting the Gas Turbine Generator (GTG). The highest ranking of 10 was assigned to situations where loss of all safety-class items A or B is coupled with the inability to restore power via GTG, such as in the event of a common power distribution bus failure. However, if there is a second

Table 3.1 rating scale for severity (S), taken from [42].

S	Description	Reactor shutdown	Emergency generator
1	Loss of redundancy in power distribution	Not needed	Not needed
2	Loss of single load on the HV Bus or LV Bus C or D	Needed	Not needed
3	Loss of all loads on the LV Bus C or D	Needed	Not needed
4	Insufficient power on Computer System	Needed	Not needed
5	Insufficient power on the DC Bus A or B	Needed	Not needed
6	Insufficient power on Uninterruptible AC Buses	Needed	Not needed
7	Loss of single load on the LV Bus A or B	Needed	Not needed
8	Insufficient input power to the LV Bus A or B	Needed	Needed/Can be used
9	Insufficient input power to the LV Bus A and B	Needed	Needed/Can be used
10	Loss of all loads on the LV Bus A or B	Needed	Cannot be used

power distribution bus available and sufficient input power (from offsite or the second GTG), a safe reactor shutdown is still possible. It is important to note that this study only considers normal operation conditions and does not account for multiple failures, which can pose challenges to the safety of the reactor shutdown. Therefore, any potential failure mode with an S value greater than 1 is assumed to result in an immediate reactor scram, assuming successful operation of the VCS and Auxiliary Cooling System (ACS).

FMEA occurrence rating of electrical system

In this study, the database of the U.S. Nuclear Regulatory Commission (NRC) was examined to determine suitable ranges of failure frequency to be used in FMEA [20, 55]. The results of the data analysis conducted on the main data source used in this study, Technical Report NUREG/CR-6928 [20], are presented in Fig. 3.2. The data analysis of Technical Report NUREG/CR-6928 revealed failure rates ranging from $2.5E-11/h$ (λ_{min}) to $9.5E-03/h$ (λ_{max}) for different component types and failure modes. The median value was approximately $2.2E-07/h$ ($\lambda_{50\%}$), and the distribution was highly positively skewed (skew = 5.3). Half of the data records were within the box, with about 70% located between $1E-08/h$ and $1E-05/h$ (yellow field), about 15% higher than $1E-05/h$ (red field), and about 15% lower than $1E-08/h$ (green field). Based on this information, the following rating scale for occurrence was developed:

- Moderate: failure rates of the same order of magnitude as $\lambda_{50\%}$;

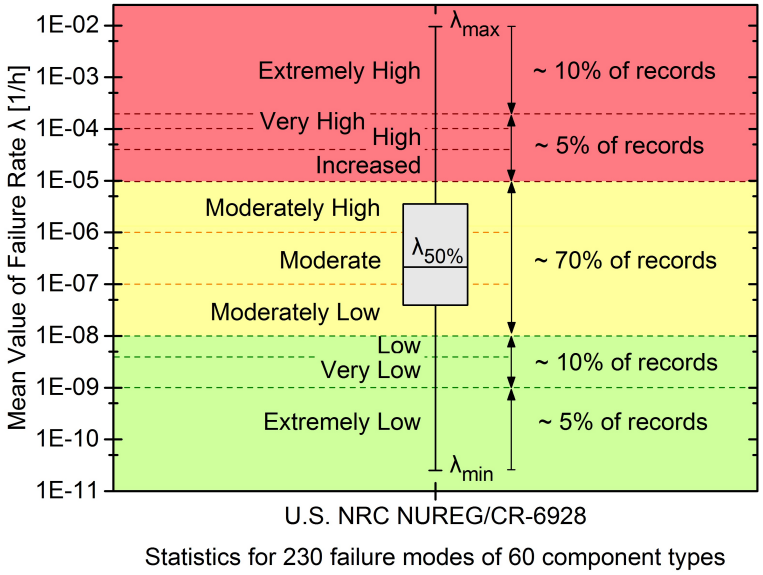

Fig. 3.2 Distribution of the failure rate values for a variety of component types and failure modes as collected in the U.S. NRC NUREG/CR-6928, taken from [42].

- Moderately Low and Moderately High: failure rates one order of magnitude lower or higher than $\lambda_{50\%}$, respectively;
- Extremely High: failure rates above $2E-04$ (the top 10% of records);
- Extremely Low: failure rates at or below $1E-09$ (the bottom 5% of records);
- Other ranges were defined based on the λ values closest to the 10th, 86th, and 88th percentiles of the NRC data distribution (Tab. 3.2).

FMEA detection rating of electrical system

Given the lack of relevant information regarding detection mechanisms in HTTR EF, this study assigns the maximum rating ($D = 10$) to all failure modes.

3.1.2 Gradual screening approach

In this study, in order to prioritize the failure modes, the RPN was calculated based on severity, occurrence, and detection rankings. Using this RPN as a basis, a novel Gradual Screening Approach

Table 3.2 FMEA rating scale for Occurrence (p – the nearest percentile of the U.S. NRC data distribution corresponding to the boundary value of failure rate, taken from [42].

O	Description	Range of λ [1/h]	Nearest p
1	Ext. Low	$\lambda \leq$ 1E-09	$p \leq$ 5th
2	Very Low	1E-09 $< \lambda \leq$ 1E-09	5th – 10th
3	Low	4E-09 $< \lambda \leq$ 1E-08	10th – 15th
4	Mod. Low	1E-08 $< \lambda \leq$ 1E-07	15th – 36th
5	Moderate	1E-07 $< \lambda \leq$ 1E-06	36th – 68th
6	Mod. High	1E-06 $< \lambda \leq$ 1E-05	68th – 84th
7	Increased	1E-05 $< \lambda \leq$ 4E-05	84th – 86th
8	High	4E-05 $< \lambda \leq$ 1E-04	86th – 88th
9	Very High	1E-04 $< \lambda \leq$ 2E-04	88th – 90th
10	Ext. High	2E-04 $< \lambda$	90th $< p$

was proposed. The approach first prioritizes all identified failure modes based on their RPNs, and then presents the resulting data in a two-dimensional risk matrix showing the frequency and severity of each failure mode. Based on this approach the failure modes fall into two categories: those that can be excluded from the reliability analysis, and those that require further investigation due to uncertainty and ageing effects. This approach is presented in Tab. 3.3 and complements the FMEA analysis presented in Tabs. 3.4–3.8.

The gradual screening procedure developed in this study is founded based on a matrix with the user-defined risk areas, as follows:

- The light green area in the bottom left corner of Tab. 3.3 indicates failure modes with low occurrence and severity rankings, which can be deemed less critical and excluded from further analysis;
- The dark green area represents potential failure modes with moderately low rankings, for which their reliability can be evaluated using constant failure rates over time (λ_{mean});
- The yellow area on the matrix represents failure modes with a significant impact on system reliability, requiring a more precise reliability assessment using uncertainty distributions of failure rates (λ). This is necessary to account for the likelihood that the true λ values may exceed the initial frequency ranges defined in Tab. 3.2. Various analytical and simulation methods can be employed to evaluate parameter uncertainties in the reliability models [86];

- The adjacent orange field includes failure modes with a dominant effect on system reliability, necessitating reliable assessment of the dynamic behavior of failure rates. This requires analyzing uncertainty and ageing phenomena. The aim is to ensure that the frequency of system failures λ_{EF} during the facility's lifetime does not exceed an unacceptable level of risk. Modelling ageing phenomena is challenging because it involves introducing time-dependence into component failure rates while most databases only provide average values. However, Bayesian inference from different data sources can be used to address this issue by utilizing knowledge about source-to-source variability in the number of failures that occurred in the past and the exposure time when these events were observed [38]. An alternative approach to address time-dependence in failure rates is to use an appropriate Weibull model to define the bathtub curve, which distinguishes the early operation time (with decreasing λ), stable conditions (with constant λ), and the wear-out phase (with increasing λ) [50];
- The top-right section of the matrix denotes the highest risk failure modes that significantly reduce system reliability, requiring design modifications to achieve an acceptable reliability level.

When utilizing this method, it is crucial to remember that severity and occurrence ratings are case-sensitive and may vary depending the analysis objective. severity ratings can differ in safety studies versus reliability analysis, yet they range from 1 to 10. Different combinations of severity and occurrence can yield the same RPN, and analysts may assign varying weights to each factor based on their priorities. For instance the presented risk matrix considers failure modes with an occurrence rating of 10 to have the most likely and significant impact on system reliability and efficiency, whereas those with an occurrence rating of 1, irrespective of their severity, are represented by a light green color to indicate the least likely scenario of impacting system reliability. The five areas on the matrix should reflect actual system conditions and reliability priorities, and need not be symmetric.

3.1.3 FMEA of HTTR VCS system

HTTR VCS structure

The VCS comprises upper, lower, and side cooling panels, as well as heat removal adjustment panels surrounding the Reactor Pressure Vessel (RPV). The entire system is enclosed within concrete biological shielding [58, 59]. VCS is made up of two active cooling water circulation sections, A and B, each

Table 3.3 Risk matrix of the HTTR EF (the cells include the number of identified failures), taken from [42].

	S									
O	1	2	3	4	5	6	7	8	9	10
10										
9										
8										
7										
6	3		2	2		6		2	2	
5		3	8	2	8	6		4	4	4
4	15	18	2				14	2		
3			20					2	8	26
2										
1										

Σ	
15	Can be excluded from further reliability studies
54	Reliability models based on averaged λ values
82	Consideration of λ uncertainty distribution
12	Consideration of ageing effects, i.e. $\lambda = \lambda(t)$
12	Cannot be accepted (design changes required)

Table 3.4 FMEA for high-voltage equipment of the HTTR EF. LOIP stands for Loss of Input Power, FTS stands for Failure to Supply, SC stands for Short Circuit, SA stands for Spurious Action, IIP stands for Insufficient Input Power, FTO stands for Failure to Operate, taken from [42].

No.	Component	Function Lost	Most severe effect	Causes	*S*	*O*	*D*	*RPN*
1	Commercial Offsite Power Line 01/02	FTS power to the HV Bus	LOIP to LV Bus A and B	Grid	6	9	10	540
				Weather	5	9	10	450
				Switchyard	6	9	10	540
2	Main HV Breaker	FTS power to HV Bus	LOIP to LV Bus A and B	SA	5	9	10	450
				FTO	3	9	10	270
3	HV Bus (6600 V)	FTS power to HV loads	LOIP to LV Bus A and B	FTO	5	9	10	450
				SC	5	9	10	450
4	HV Breakers 01/07	FTS power to Power Center C/D	Loss of all loads on LV Bus C/D	SA	5	3	10	150
			LOIP to LV Bus A and B	SC	3	9	10	270
5	HV Breaks 02/06	FTS power to Power Center A/B	LOIP to LV Bus A or B	SA	5	8	10	400
			LOIP to LV Bus A and B	SC	3	9	10	270
6	HV Breakers 03/04/05	FTS power to PWC PGC 1/2/3	Loss of single HV load: PGC 1/2/3	SA	5	2	10	100
			LOIP to LV Bus A and B	SC	3	9	10	270

Table 3.5 FMEA for the Low Voltage Power Centers C and D (non-safety-class loads). FTO stands for Failure to Operate, SC stands for Short Circuit, SA stands for Spurious Action, taken from [42]..

No.	Component	Function Lost	Most severe effect	Causes	*S*	*O*	*D*	*RPN*
1	Transformers C/D	FTS LV Bus C/D	Loss of all loads on LV Bus C/D	FTO	3	6	10	180
				SC	5	3	10	150
2	Main LV Breakers C00/D00	FTS LV Bus C/D	Loss of all loads on LV Bus C/D	FTO	4	3	10	120
				SC	3	3	10	90
3	LV Bus C/D (440 V)	FTS LV loads	Loss of all loads on LV Bus C/D	FTO	5	3	10	150
				SC	5	3	10	150
4	LV Breakers C01-C09 D01-D09	FTS LV loads	Loss of single load on LV Bus C/D	SA	4	2	10	80
			Loss of all loads on LV Bus C/D	SC	3	3	10	90

Table 3.6 FMEA for the DC Power System (100 V). LOR stands for Loss of Redundant, FTO stands for Failure To Operate, FTS stands for Failure To Supply, SC stands for Short Circuit, taken from [42].

No.	Component	Function Lost	Most severe effect	Causes	*S*	*O*	*D*	*RPN*
1	Charger A/B	FTS charging power to Battery A or B	LOR in battery charging	FTO	6	1	10	60
				SC	5	1	10	50
2	Stand of Charger	FTS charging power to Battery A and B	LOR in battery charging	FTO	6	1	10	60
				SC	5	1	10	50
3	Battery A/B	FTS safety equipment	Insufficient power on DC Bus A/B	FTO	5	5	10	250
				SC	5	5	10	250
4	DC Bus A (100 V)	FTS Inverter A	Insufficient power on DC Bus A	FTO	5	5	10	250
				SC	5	5	10	250
5	DC Bus B (100 V)	FTS Inverter B and C	Insufficient power on DC Bus B	FTO	5	5	10	250
				SC	5	5	10	250

Table 3.7 FMEA for the Low Voltage Power Centers A and B (safety-class loads). LOR stands for Loss of Redundant, FTS stands for Failure to Supply , FTO stands for Failure To Operate, SC stands for Short Circuit, SA stands for Spurious Action, IIP stands or Insufficient Input Power, taken from [42].

No.	Component	Function Lost	Most severe effect	Causes	*S*	*O*	*D*	*RPN*
1	Transformers A/B	FTS pow. to LV Bus A/B	IIP to LV Bus A/B	FTO	6	8	10	480
				SC	5	8	10	400
2	Main LV Breakers A00/B00	FTS pow. to LV Bus A/B	IIP to LV Bus A/B	SA	4	8	10	320
				SC	3	8	10	240
3	LV Bus A/B (440 V)	FTS pow. to LV loads	Loss of all loads on LV Bus A/B	FTO	5	10	10	500
				SC	5	10	10	500
4	LV Breakers A01-07, B01-07	FTS pow. to LV loads	Loss of single loads on LV Bus A/B	SA	4	7	10	280
			Loss of all loads on LV Bus A/B	SC	3	10	10	300
5	LV Breakers A08/B08	FTS Comp. Pow. Providing Sys.	LOR pow. supplying line for Comp.	SA	4	1	10	40
			Loss of all loads on LV Bus A/B	SC	3	10	10	300
6	LV Breakers A09-11 B09-11	FTS pow. to Inverters A/B/C	LOR pow. supplying line for Inverters	SA	4	1	10	40
			Loss of all loads on LV Bus A/B	SC	3	10	10	300
7	LV Breakers A12/B12	FTS pow. to Battery Charger A/B	LOR pow. supplying line for Batteries	SA	4	1	10	40
			Loss of all loads on LV Bus A/B	SC	3	10	10	300
8	LV Breakers A13/B13	FTS pow. to Stand of Charges	LOR pow. supplying line for Chargers	SA	4	1	10	40
			Loss of all loads on LV Bus A/B	SC	3	10	10	300

Table 3.8 FMEA for Uninterruptible and Computer AC Power System (100 V). FTS stands for Failure to Supply , FTO stands for Failure To Operate, SC stands for Short Circuit, IIP stands for Insufficient Input Power, taken from [42].

No.	Component	Function Lost	Most severe effect	Causes	*S*	*O*	*D*	*RPN*
1	Uninterruptible AC Bus	FTS pow. to Safety Inst. Channels	IIP to Safety Inst. Channels	FTO	5	6	10	300
				SC	5	6	10	300
2	Inverters A/B/C	FTS uninter. AC Bus A/B/C	IIP to AC Bus A/B/C (100 V)	FTO	6	6	10	360
				SC	6	6	10	360
3	Comp. Pow. Sup. Unit	FTS Comp. Sys. AC Bus (100 V)	IIP to Comp. AC Bus (100 V)	FTO	6	4	10	240
				SC	6	4	10	240
4	Comp. AC Bus (100 V)	FTS non-safety equipment	IIP to non-safety equipment	FTO	5	4	10	200
				SC	5	4	10	200

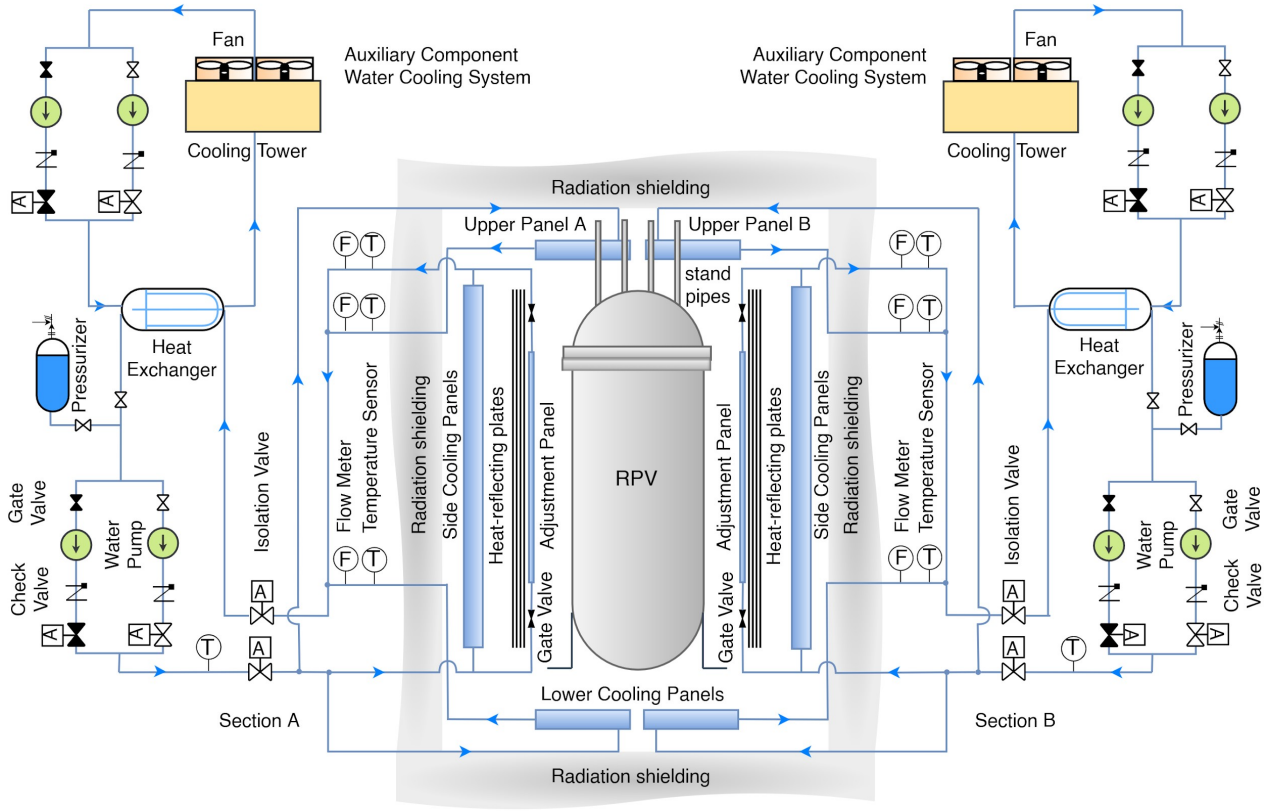

Fig. 3.3 Schematic diagram of the HTTR Vessel Cooling System cf. [44, 43, 57]

equipped with two pumps, with one pump on standby mode. The HTTR VCS structure is presented in Fig. 3.3.

Under normal operation, the VCS operates at a steady flow rate of 100% to eliminate 2-3% of the reactor's thermal output, while the main cooling system takes care of the remaining output. The cooling panels, enclosed by concrete biological shielding, absorb heat from the shielding and transfer the water back to the heat exchanger. The heat exchanger in secondary side obtains water from the cooling tower via backup pumps. To achieve specific temperature objectives, such as maintaining the concrete temperature below 65°C, the outlet gas temperature above 950°C, and the fuel temperature below the maximum limit of 1600°C, the VCS must sustain a heat removal rate below 0.6 MW during normal operation [44]. The valves in the adjustment panels regulate heat removal to accomplish these targets. The design and operation of the VCS are described in detail in [44].

During LOFC accident, when the main and auxiliary cooling systems are unavailable, the VCS must be capable of removing residual heat with just one section. To ensure this capability, a minimum cooling

capacity of each VCS section has been established to be above 0.3 MW. However, it was discovered through thermal radiation tests conducted by Kunitomi et al. [44] that operating both sections of the VCS would result in excessive heat removal, which could make it difficult to maintain the desired outlet coolant temperature during normal operation. To resolve this issue, heat-reflecting plates were installed between the RPV and side cooling panels. These plates are designed to reduce the amount of heat removed from the RPV. However, in the event of an accident where only one section of the VCS is active, the adjustment cooling tubes on the innermost plates can be used to increase heat removal. Experimental verification has been carried out on the reflector plates, adjustment panels, and the thermal emissivity of the RPV material [44].

The HTTR VCS has been meticulously designed to accommodate the anticipated heat distribution on the concrete biological shielding, while simultaneously ensuring that the reactor could generate its rated thermal power during normal operation and be safely shut down during an emergency. A visual depiction of the cooling water panel configuration has been presented in Fig. 3.4.

The VCS's upper part is composed of a steel casing under the upper radiation shielding, housing 48 tubes with penetrations for the RPV stand-pipes. Six inlet headers supply cooling water from the inlet ring to the cooling water tubes, which then pass through the space between the stand-pipes, ensuring uniform cooling of the upper radiation shielding. After cooling, the water exits via the six outlet headers. The flow diagram for a single upper panel can be seen in Fig. 3.4 (a).

The side cooling panel of the VCS is located on the vertical surface of the concrete biological shielding surrounding the RPV. It consists of 18 water cooling tubes, which are arranged in parallel and connected by steel plates. The flow diagram for the side panel is illustrated in Fig. 3.4 (b). The tubes of both the upper and side cooling panels are configured in a way that ensures a uniform distribution of heat. In order to cool the side panel, the cooling water is supplied from the lower ring and then directed to the heat exchanger through the upper ring. Each unit of the side panel has four thermal reflector plates, which help to reduce the amount of heat that is absorbed from the RPV during normal operation when both sections of the VCS are active. Additionally, there are eight heat adjustment tubes located on the surface of the innermost plate. These tubes can be used to increase heat removal in the event of one section being active during an accident, and when the VCS heat removal rate drops below 0.3 MW.

The VCS's lower part is divided into two sections: the lower-side panel and the lower-bottom panel. The lower-side panel is made up of 12 units that are installed on the vertical wall of the RPV's lower cavity. Each unit consists of 16 water tubes and two thermal reflectors, similar to the side cooling panels

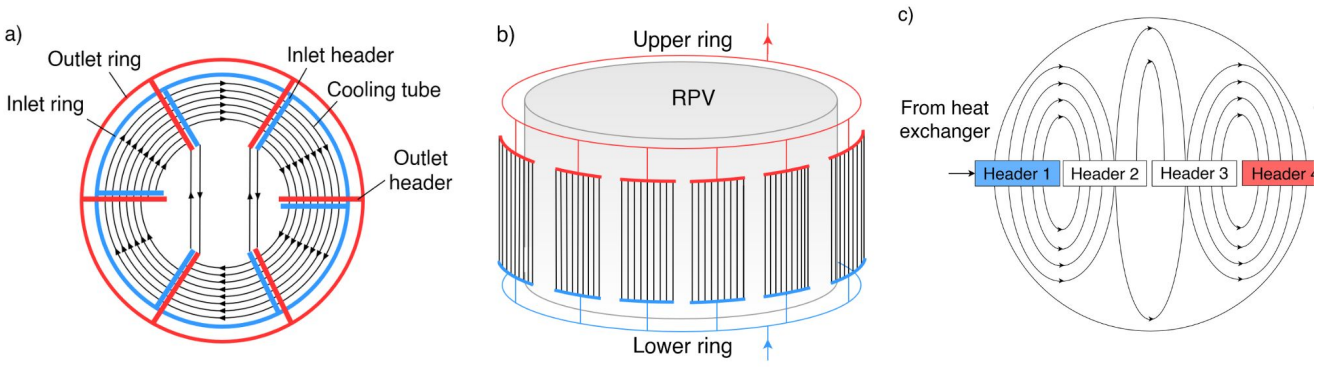

Fig. 3.4 Flow diagram of VCS panels for a single section: (a) upper panel,(b) side panel, and (c) lower-bottom panel [57].

shown in Fig. 3.4 (c). On the other hand, the lower-bottom panel is positioned at the bottom of the cavity and receives cooling water from the lower-side structure before directing it to the heat exchanger

In order to ensure the structural integrity of the fuel, RPV, and biological shielding, it is crucial to keep the heat removal value of the VCS in check. This is done by monitoring the flow rate and temperature of the cooling water entering and exiting each cooling panel. The temperature of the fuel, RPV surface, and biological shielding must be kept within safe limits to maintain structural integrity, with maximum values of 1495°C, 360°C, and 58°C respectively, and must not exceed 1600°C, 550°C, and 65°C. During normal operation, the inlet and outlet temperature of the VCS panels is maintained between 32-35°C and 36-41°C, respectively, which is crucial for maintaining the desired temperature range [57].

An analysis of the decay heat removal during Pressurized and Depressurized Loss of Forced Cooling accidents (PLOFC and DLOFC) is performed by Kunitomi et al. [43]. The study concluded that a single section of the VCS, which uses radiation and natural convection to indirectly cool the reactor core, is sufficient to prevent overheating of the fuel and RPV, with fuel temperatures reaching a maximum of 1330°C and RPV temperatures reaching a maximum of 1380°C. The results also indicated that the reactor core would remain safe during loss of forced cooling, even in the absence of VCS operation, due to the high heat capacity of the core and effective heat transfer to the RPV and radiation shielding.

If the VCS system fails during a PLOFC/DLOFC accident, the RPV temperature may approach the structural integrity limit of 550°C, with peak temperatures of 537°C/547°C occurring within 20/30 hours. However, running a single VCS section can significantly reduce the maximum temperature, keeping it below the design limit for up to 72 hours. During this time, residual heat is transferred to the biological shield, resulting in a maximum temperature of around 100°C when a single VCS section is operational and over 350°C when it fails. Although not essential for reactor safety, the VCS system is critical in maintaining the RPV and biological shield temperatures within the design limits during DLOFC. Failure to do so may compromise their integrity and accelerate long-term deterioration. Therefore, the VCS system is vital for protecting the plant's investment and ensuring long-term operation.

The safety of HTTR has been evaluated through thermal-hydraulics safety studies, but these have not been fully validated by experiments. While tests were conducted by the JAEA in 2007, they were discontinued after the Fukushima Daiichi accident in 2011. Only two LOFC tests were conducted before the accident, both at 30% reactor power, with one test involving both VCS sections and the other with only one [68, 23]. The fuel, RPV, and concrete shielding temperatures did not increase

significantly in either test due to the large heat capacity of the graphite core. Ongoing LOFC tests are being conducted with both VCS sections deactivated at 30% reactor power and full-power experiments are under consideration.

FMEA of VCS

As previously discussed, before conducting a FMEA and FTA, it is essential to identify and explore existing industrial equipment failure databases. This step is crucial in determining reliability models for the associated system. The reliability models of VCS are developed using a failure rate distribution and repair time range. Data were collected from publicly available databases that are systematically updated, cover a wide range of component types and failure modes, and reflect the characteristics of nuclear facilities, including the specificity of HTGRs, are used for the development and application of the reliability models. Some of the relevant sources include [48, 5, 28, 29, 16].

The FMEA of VCS was performed with a focus on two of the three measures: severity and occurrence, due to the lack of sufficient information on the control and instrumentation of the HTTR. The severity scale criteria used was ranged as follows:

1. No discernible effect which indicates that the VCS system would continue to function normally despite the failure of certain components, such as the monitoring system or temperature/pressure sensor.

2. Loss of redundancy on a single VCS section which could result in short-term effects until standby components are activated, such as water pumps and associated valves in a parallel structure.

3. Loss of a single VCS section with a failure outside the RCV in which the repairs could potentially be carried out without delaying the reactor cooldown, such as heat exchangers, cooling fans, pressurizers, or piping.

4. Loss of a single VCS section with a failure outside the RCV, an additional delay time of 72 hours is necessary to allow for the reactor to cool down before repair work can commence, namely Cooling Water Panels (CWP)s tubes or water supply pipes.

5. Loss of both VCS sections due to a common cause failure whic could have a severe impact on the reactor operation, and immediate action must be taken to address the issue, such as loss of cooling towers, electrical power, or leakages caused by the degradation of the CWPs welds.

3.2 Results and discussion

In this section, the analysis of two critical safety-related systems of HTTR - EF and VCS - was performed using the FMEA method to investigate potential component failure modes.

The new FMEA-based gradual screening approach has been proposed and applied for EF. This approach includes a three-step process: (1) An initial calculation based on average failure rates, (2) Implementation of uncertainties of the failure rates, and (3) consideration of ageing phenomena effects. By prioritizing higher risk failure modes, the gradual screening approach enables more accurate modeling of critical events, which in turn allows for better-informed decision-making regarding risk mitigation. Additionally, this approach reduces the time and cost of reliability studies by focusing on failure modes that have the most significant impact on overall system reliability. Moreover, this approach also simplifies the analysis by screening out the failure modes with lower frequency and severity, thereby providing a more rational and manageable basis for further analysis. The subsequent section will present the associated reliability analysis that integrates the insights derived from our proposed approach.

In order to determine the criticality of individual failure modes for the VCS components, the FMEA method was utilized and the associated failure modes were ranked based on their impact on system availability under both normal and accident conditions. This analysis is crucial as it provides insight into the time required to restore the system to full functionality, which is essential for maintaining system availability. Building on the insights gained from the FMEA ranking, reliability and availability analysis of the VCS system is conducted. The results of this analysis will be presented in a subsequent section, providing a comprehensive understanding of the system's overall performance and identifying areas for improvement.

3.3 Application of standard PSA model in HTGR

The comprehensive approach to ensuring the safety of nuclear facilities encompasses the integration of both deterministic and probabilistic analyses. The combination of these two elements serves as a crucial foundation for ensuring the overall safety of nuclear facilities. Such comprehensive safety analysis plays a crucial role in mitigating potential risks, optimizing decision-making processes, and improving overall safety performance. The deterministic aspect provides a solid foundation for safety, while the probabilistic element, commonly referred to as PSA, enhances the level of confidence in safety by

quantifying the likelihood and consequences of potential safety events. The standard/traditional PSA approach, widely adopted in the field of nuclear safety and risk management, serves as a systematic tool for assessing the probabilistic safety performance of NPPs. This methodology has become a well-established method for the systematic evaluation of the reactor's safety components and systems. The insights gained from PSA provide valuable information to support early risk identification and mitigation and informed decision-making, leading to enhance safety outcomes.

The traditional PRA performs three levels of analysis. The objectives of these levels are as follows:

- Level 1: To estimate the frequency of events that lead to core damage. This level of PSA usually involves the use of FTA and ETA to identify and evaluate the likelihood of initiating events and their potential consequences.
- Level 2: To evaluate the frequency of containment integrity response and determine release frequencies using the results of the level 1 analysis. This level involves the use of models such as the Containment Event Tree (CET) [8] to evaluate the likelihood of containment failure and the potential consequences of such a failure.
- Level 3: to evaluate the potential radiological impacts on the public and environment using established models for source term and consequence analysis [36]. This analysis uses the information from Level 2 to determine the release frequencies and potential source terms.

In general, the outcome of each level serves as the input for the next level. In order to perform such a comprehensive PSA analysis, the two specific techniques such as ETA and FTA are used in this research. FTA, is a top-down approach that involves constructing a logical diagram to represent the relationships between events and conditions that could lead to an accident. Another applied tool which is ETA, is a bottom-up approach that involves modeling the progression of an accident scenario and the subsequent events that occur as a result of the accident. These tools enable a quantitative evaluation of the safety performance of the reactor and provide a comprehensive assessment of the probabilities and consequences of different accident scenarios. The details of ETA and FTA will be thoroughly discussed in subsequent sections of this chapter.

The HTGRs, as kind of Generation IV reactors, present a unique set of structural characteristics that set them apart from LWRs, including inherent safety features and specific safety-related systems that distinguish them from LWRs. As such, *the standard PSA approaches used for LWRs need to be*

adapted to incorporate these unique features. The alternative methods that better account for the specific safety-related systems of HTGRs will be investigated in further sections. In this section, a standard PSA was conducted on the referential HTGR, the HTTR, for a referential accident scenario, which is DLOFC. The analysis will be conducted using the SAPHIRE software which is designed specifically for PSA analysis. The results obtained from the study will then be compared with the novel approach and the differences will be thoroughly analysed and discussed in the final conclusions of the study.

Moreover, by utilizing the standard PSA methodology, this research aims to demonstrate the significance and relevance of considering the unique features of the HTGR design in the evaluation of its safety performance. This approach not only enhances the level of confidence in the safety of the HTGR, but also optimizes the decision-making processes aimed at ensuring its safe and sustainable operation.

3.3.1 Accident scenario analysis

Physical barriers during accidents

The Defense-in-Depth (DiD) concept [35] is a critical component in ensuring safety and minimizing the consequences of accidents in nuclear facilities. The DiD approach outlines the fundamental principles of safety by implementing multiple layers of defense [25], from the design of the facility to operational procedures. The concept is based on the premise that a comprehensive approach to accident prevention and mitigation can be achieved through the application of multiple layers of protection. The DiD approach aims to protect workers, the public, and the environment from radiation exposure, and it is typically implemented through a deterministic approach.

Conducting a PSA requires a thorough understanding of the methods employed by the reactor to ensure safety during potential accident scenarios. The DiD concept is a crucial aspect of these methods and provides a framework for understanding the safety measures in order to mitigate the impacts of accidents. Understanding the DiD principles and their application in the design and operation of nuclear facilities is essential for accurate evaluation the likelihood of accidents and determining the necessary measures to minimize their consequences.

In order to achieve the safety objectives through DiD, several physical barriers are implemented in NPP designs which include different equipment and safety systems. In LWRs, the barriers are defined as follows [25]:

- Fuel matrix,

- Cladding of the fuel,
- Reactor coolant boundary,
- Containment structure.

These barriers serve to protect the public and the environment from radionuclide releases, by preventing the spread of radioactive material beyond the facility's boundaries in the event of an accident scenario.

In HTGRs, the barriers against radionuclides confinement that provide DiD are defined based on their design and safety objectives. The general barriers of HTGRs are defined as follow [33]:

- Kernel element of the fuel particle,
- Coatings of fuel particle,
- Graphite structure of the core,
- Primary pressure boundary of the coolant,
- Reactor building.

The HTTR comprises a sufficient and variety levels of barriers, each equipped with a set of safety systems, aimed at not only mitigating the impact of any potential accidents, but also at containing radioactive substances within the reactor containment and preventing their release into the environment. This comprehensive approach to accident management is reflected in Tab. 3.9, providing a detailed understanding of the HTTR's implementation of the DiD principle and its assurance to maintaining the safety of NPPs.

DLOFC accident scenario

In this study, DLOFC scenario was considered, in which the simultaneous rupture of both the concentric inner and outer primary hot gas ducts in the HTTR was assumed to occur. The severe consequences of such an event would result in an immediate escape of the primary coolant, helium, into the Reactor Containment Vessel (RCV), potentially leading to the spread of FPs and radioactive graphite dust may release in the service area and environment. The findings of this study demonstrate that the RCV is

Table 3.9 Physical Barriers of HTTR against FPs release under an abnormal event

No	Physical barrier	Safety function(s)	Associated system(s)
1	Fuel compact	Maintaining radioactive material	FCM
			HGB
2	He pressure boundary	Controlling the chemical impurities of the He	HPS
3	RPV	Heat removal	VCS
			HX
			PPWC
			SPWC
			AHX
			CHD
			CSP
4	RCV	FPs retaining	RCV
		Minimizing the air ingress during DLOFC	
		Residual heat removal	
5	Reactor Building	Maintaining negative pressure of service area	RVS (normal operation)
		Preventing FP Release	APS (AC)

the most effective physical barrier in preventing the release of fission products outside the plant during primary pipe rupture accidents.

The safety processes in response to a DLOFC scenario are initiated by the automatic detection of a differential pressure between the Primary Cooling System (PCS) and Pressurized Water Cooling System (PWCS). The detection of a differential pressure initiates the reactor scram, which is performed either by a control rod or a reserved shutdown system. To prevent the spread of radionuclides into the atmosphere, signals are activated to isolate the RCV. It involves closure of the isolation valves, stopping the air conditioner and ventilator, and activating the emergency air purification system. The residual heat of the core is then removed through conduction and radiation to the RPV surface, cavity wall, and ultimate heat sink. The ACS is not operated under this accident due to the likelihood of air ingress into the core through the forced convection [59]. The graphical representation of this sequence of events is depicted in Fig. 3.5.

3.3.2 Event tree analysis

The ETA is a widely adopted tool in the field of PSA for evaluating the risk and likelihood of potential accidents. The ET provides a graphical representation of the sequential progression of the events that lead

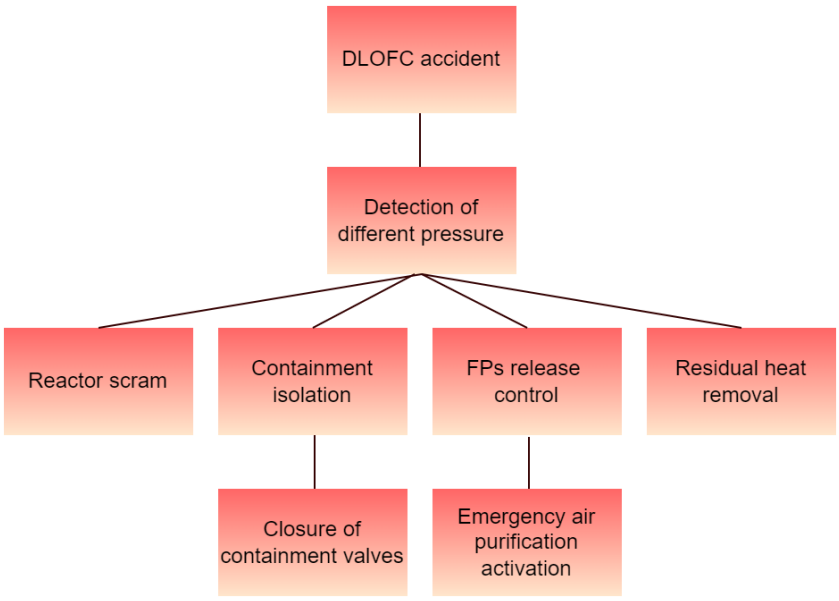

Fig. 3.5 Conceptual block diagram of the safety functions under DLOFC accident in HTTR.

to the specific accident scenarios and calculates the probability of each event in the sequence. The ETA methodology is characterized by its systematic and quantitative approach to provide a comprehensive evaluation of the interdependent relationships between various systems and components, and the modes of potential failures that lead to specific outcomes. This enables a thorough understanding of the system's overall safety performance.

The first step in ETA involves the identification of the initiating event, that has the potential to trigger an accident. These events can be caused by internal or external phenomena such as loss of coolant, earthquakes, loss of offsite power, fires, floods, etc. Once the initiating event has been identified, the subsequent step determines the operational safety systems or actions involved in responding to it. These systems are usually arranged in a sequential manner. The ET branches at nodes where the probability of success or failure must be specified are calculated using FTA or obtained directly from failure rate data.

The right side of the ET represents the damage state that results from a specific path through the tree, and this damage state is determined through the understanding of the processes, operating experience, accident history, and safety analyses. The results of the combinations of failure or success of the safety-related systems or actions appear in the end states of the plant at the right branches of the ET. These end-states are determined using thermal-hydraulic analyses to define temperature profiles and assess potential consequences. These end-states may serve as initiators for FPs releases both within the

plant and outside of it. For LWRs, the ultimate objective is to prevent the occurrence of core damage during the accident, which is considered the most severe failure scenario. Thus, the assessment of the potential outcomes is typically defined as either the occurrence or non-occurrence of the core damage.

In HTGRs, the occurrence of core melting as the most severe consequence under accident scenarios is greatly unlikely due to its inherent safety features. As a result, the end-state of the ET should be defined based on the established safety criteria for HTGRs. As mentioned in the previous chapter, there exist several literatures proposing the release categories of FPs as consequences of accident sequences, the determination of this information is limited due to a lack of comprehensive experimental data.

In this study, the ET of the DLOFC accident scenario of HTTR is presented in Fig. 3.6. This ET was developed using the SAPHIRE software and aimed to model the potential consequences of the DLOFC scenario. The end state of each sequence is expected to result in a specified category release of FPs. To address this, the safety systems aimed at preventing the discharge of radioactive substances were included as top events in the ET. For this analysis, a mission time of 21 days (500 hours) is assumed based on thermal-hydraulics results presented in Ref. [43], which indicate that the RPV temperature is reduced to approximately 200°C within 500 hours after a DLOFC.

As depicted in Fig 3.6, following the initiation of DLOFC, the power supply system is the primary system to activate the safety systems following the DLOFC scenario. The reactor scram system, containment isolation system, filtered release control system, and vessel cooling system are the consecutive safety systems to be operated. It is important to note that, except for the reactor scram system, all of these safety systems are dependent on the electrical system. As a result, in the event of a station blackout, which is a failure of the offsite and emergency electric system, all of the active safety systems will fail, and the flat line will go to the end state. This is reflected in the ET as a flat branch connecting to the end state.

While proper functioning of all safety systems ensures that the core does not overheat and that the FPs do not spread beyond the reactor building, an analysis of temperature transients during a depressurized accident, considering the failure of the VCS in the HTTR, revealed that the maximum temperature of the fuel was 1495°C [43]. It is then within the admissible design limit of 1600°C as specified in reference [31]. Although the validity of these findings cannot be verified through experimental results, they suggest that the risk of core damage is minimal under these circumstances. However, further research and experimentation are necessary to fully confirm this conclusion. Thus, the FPs will be the only concern to be prevented under this accident.

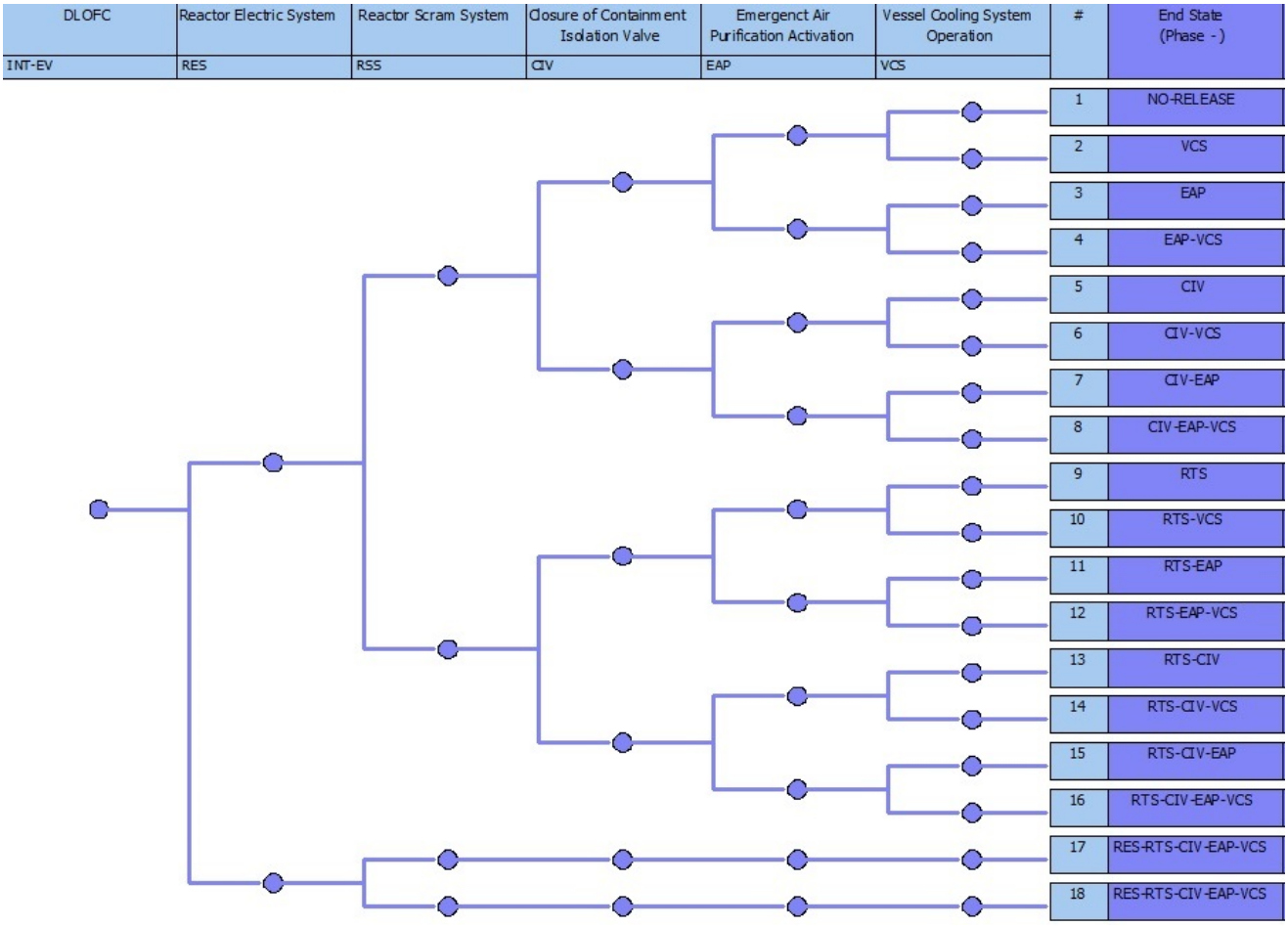

Fig. 3.6 Event tree for the initiating event DLOFC

Here, the end state is represented by the abbreviation of the respective failed safety systems, in the corresponding sequence. The potential for the improvement of the end state specification in this scenario can be addressed through implementing various safety measures, as indicated by the associated FPs release category, in the future.

In order to estimate the failure probability of each sequence for a specific initiating event (such as DLOFC) the following formula is utilized:

$$P(\text{sequence i}) = P(\text{initiating event}) \prod_{j=1}^{n} P(\text{top event j}), \tag{3.1}$$

where the notation $\prod_{j=1}^{n}$ represents the product of all probabilities from $j = 1$ to $j = n$.

3.3.3 Fault tree analysis

FTA is a logical method that can be used to model complex systems and identify the causes of failures or malfunctions. In FTA, the system under analysis is represented as a logical structure composed of basic events and intermediate events. Basic events represent the failure modes of the individual components, while intermediate events represent the logical relationships between the basic events that contribute to the occurrence of the top event or undesired system state. The logical relationships are defined using gates such as AND, OR, and k-out-of-n gates.

Qualitative FTA involve identifying the minimal cutsets (the smallest set of basic events that must occur for the top event to occur). On the other hand, quantitative analyses involve assigning probabilities to the basic events in the FT, and computing the probability of the top event using probabilistic methods, such as Monte Carlo simulation or numerical integration. The calculation of these probabilities can be challenging, especially when the underlying function is not coherent or monotonic, as it may require advanced statistical techniques, such as Bayesian inference or machine learning algorithms.

FTA is a common method that is often used in combination with ETA to assess the likelihood and consequences of hazardous events. ETA is a graphical approach that models the potential consequences of a hazardous event and the contributing factors based on the sequence of events leading up to it. In contrast, FTA focuses on identifying the root causes of the hazardous event, specifically the initiating events and factors that contribute to them. These causes are then integrated into the ETA model to further understand the likelihood and severity of the hazardous event. The FTA-ETA combination is widely

used in a variety of industries, such as nuclear power, oil and gas, aviation, and chemical processing, to improve safety and reduce the risks associated with hazardous events.

In this study, the FT of the associated safety systems during DLOFC in HTTR was created in order to use the failure rate results in the ET to ultimately show the results of the standard ET model. As noted before, the mitigation systems required for DLOFC accident are as follows: Reactor Electric System (RES), Reactor Scram System (RSS), Containment Isolation Valves (CIV), Emergency Air Purification System (EAP), and Vessel Cooling System (VCS). The following sections will provide a brief overview of these systems.

Reactor electrical system

The HTTR uses a commercial offsite power line for normal operations but also uses dedicated emergency power lines to keep all safety equipment connected. The emergency power lines are backed by two independent diesel generators, which activate automatically to supply power when needed. Further details on this system will be provided in subsequent chapters.

Reactor scram system

This system was designed to safely shut down the reactor during accidents. Two independent means are in place for reactor scram, consisting of control rods and the reserved shutdown system. The Control Rod Drive Mechanism, connected to an AC motor, controls the movement of control rods. In the event of control rod failure, the reserved shutdown system is capable of initiating scram by dropping B4C/C pellets into the fuels. During a scram event, nine pairs of control rods in the reflector region are immediately inserted. To prevent overheating of control rod sleeves, the remaining seven pairs are inserted once the core temperature drops below 750°C. During the DLOFC event, all control rods are inserted simultaneously.

Containment isolation valves

There are three types of isolation valves located at three different locations in HTTR. The first isolation valves are situated inside the containment vessel on the piping of the helium purification system. The second isolation valves are located outside the containment vessel on the same piping, and the third isolation valves are situated outside the containment vessel on the piping of the helium purification

system connected to the auxiliary cooling system. These isolation valves act as a crucial barrier in limiting the escape of FPs outside the containment.

Emergency air purification system

The emergency air purification system is designed to protect the environment in the event of an accident by automatically filtering out radioactive substances released from the stack. It also ensures that the pressure in the service area remains lower than the pressure of the outside in order to prevent the spread of radioactive materials outside the containment. The system includes multiple filtering units, each of which is equipped with an electric heater, fine dust filters, and an active charcoal filter to effectively remove harmful materials from the air. The system includes two independent units, if one system fails, the other system will automatically activate, ensuring an uninterrupted operation of the system.

Vessel cooling system

The VCS in HTTR is the ultimate heat sink and residual heat removal system which operates under both normal and accident conditions. It keeps the fuel and RPV temperatures below safety limits and maintains the integrity of the biological shielding concrete. The system has numerous safety countermeasures, including a backup dual system supported by the emergency electrical system. More details on this system has already been provided in section 3.1.3.

FTA of HTTR under DLOFC

The standard FT of each of those mitigating systems was created using SAPHIRE software. The standard FTA is an effective tool for identifying potential failure modes and their corresponding consequences. However this tool implies a particular mission time of the system activated on demand, which may not accurately reflect the operating conditions of continuously-operated safety systems. To address this, it is important to consider the exact mission time of each system in order to accurately assess the likelihood of system failure. Therefore, for the systems that are activated on demand, the mission time of the system's activation can be incorporated into the FT analysis. However, for the safety systems of HTTR such as EPS and VCS that are operated continuously under both normal and accident conditions, the operation time under normal operation is not taken into account in the traditional FTA. This omission can result in non-exact results and may not provide an accurate assessment of the system's overall

reliability. Furthermore, traditional FTA methods do not typically account for the ageing phenomena that can significantly affect the probability of system failure rate calculation. However, this factor can be particularly important for continuously-operated systems where the ageing of components can lead to failure over time. Therefore, it is essential to incorporate ageing mechanisms in the FTA to obtain a more accurate estimate of the system's failure probability.

Moreover, standard FTA assumes that safety systems are in standby mode during normal operation, meaning that their failure does not lead to any reactor scram. This means that the impact of repairs on the overall failure probability of the system is not taken into consideration. In other words, once a component or system fails in standard FTA, it is assumed to be completely failed and cannot be restored to its original state. However, in the case of continuously-operated safety-related systems in HTGR, under normal operation, the failure of a single component can potentially lead to the reactor scram, and repair time needs to be considered. This consideration is highlighted by the fact that the failure of continuously operated safety systems in HTGR influences the Forced Outage Rate. As such, the importance of repair and maintenance considerations of these systems cannot be overstated.

In addition to the previously discussed limitations, the standard FTA technique employs the Minimal Cut-Sets Upper Bound (MCUB) approximation as a simplification technique. The MCUB method aims to determine the minimum number of failures required for a top-level event to occur. However, it does not consider the interdependencies between these events. Consequently, some of the combinations identified by the MCUB method may be unlikely to occur in practice, leading to an overestimation of the system's failure probability. While the MCUB approximation can be useful for identifying critical components in a system and prioritizing them for maintenance or replacement, its limitations and overly conservative nature have also been identified as potential areas for improvement which will be presented later.

To estimate the failure probability of mitigating systems, publicly available data sources such as [20, 55, 5, 28, 29, 48] were used as basic events in the FTA. Reliability data was used to calculate equipment failure probabilities, but limitations such as incomplete or heterogeneous data and lack of information on specific equipment can impact the accuracy of the analysis. These limitations will be discussed further.

The overall probability of system failure in FTA is calculated using the following formula:

$$P(\text{top event}) = 1 - \prod_{i=1}^{n}(1 - P_i), \tag{3.2}$$

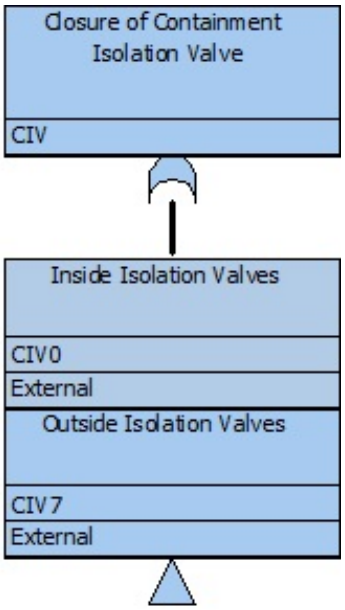

Fig. 3.7 FT diagram of Containment Isolation Valves of HTTR

where $P(\text{top event})$ is the probability of the top event occurring, and $\prod_{i=1}^{n}(1-P_i)$ is the product of the probabilities of all the minimal cut sets that lead to the top event, where P_i is the probability of the i-th basic event.

The FTA for CIV of HTTR is shown in Figs 3.7 and 3.8, providing a visual representation of the analysis and logical relationships between events. These figures serve as an example of the performed FTA and aim to identify potential failure modes associated with the CIVs of HTTR.

3.4 Results and discussion

This study employed the ETA and FTA methods to carry out a standard PSA for the DLOFC scenario, resulting from the simultaneous rupture of both the inner and outer primary hot gas ducts in the HTTR. The DLOFC initiates several safety processes, including operation of RES, RSS, CIV, EAP, and the VCS. The study utilized the ET methodology to model the potential consequences of the accident scenario and associated mitigating systems. To identify failure modes and corresponding failure frequencies of safety-related systems, the FTA technique were employed. The failure rate results obtained from the FTA were then incorporated into the ET model to assess the likelihood of the consequences and provide the standard ET model results. The DLOFC accident frequency was assumed to be 1.31E-04/year. This

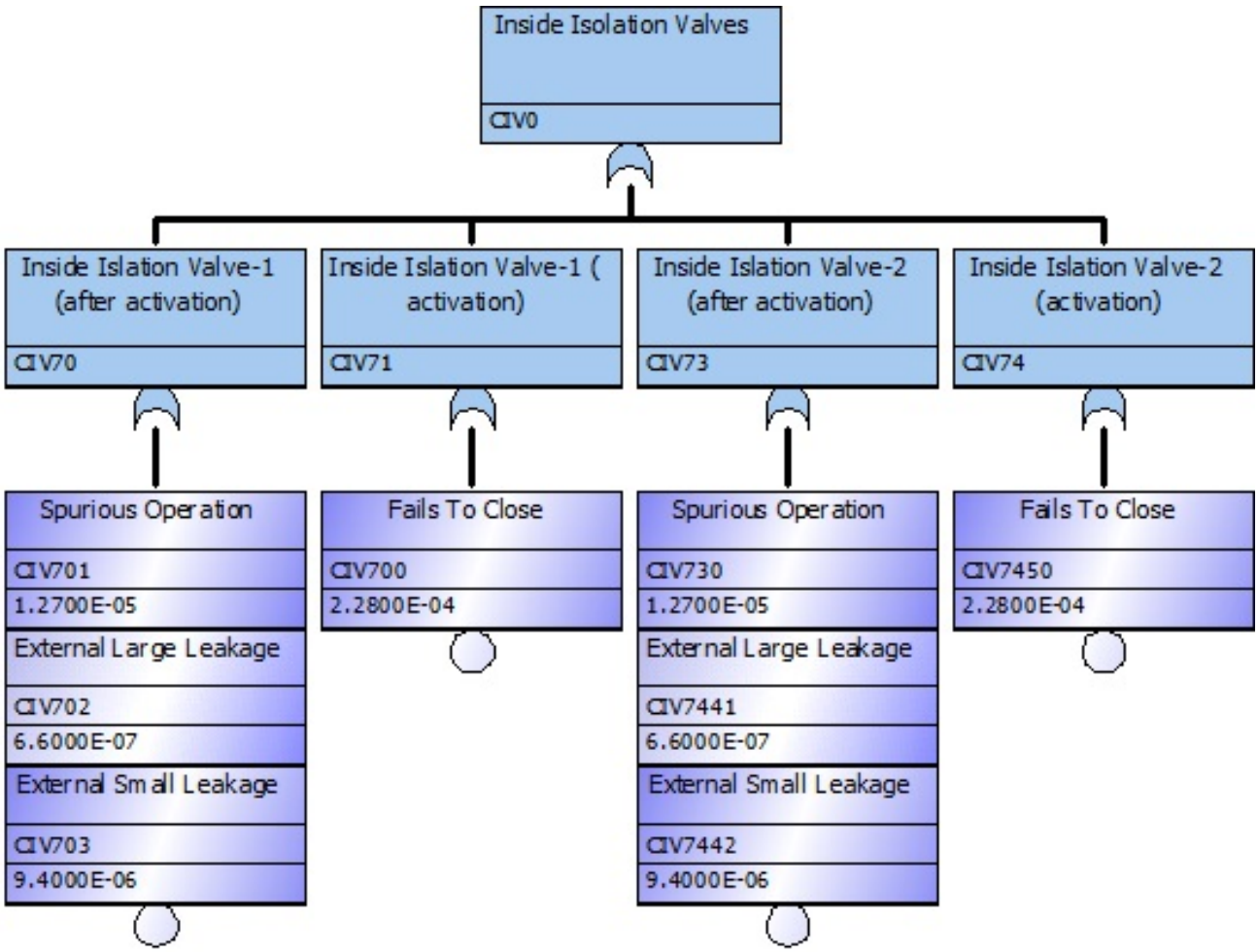

Fig. 3.8 Expanded FT diagram of Inside Containment Isolation Valves of HTTR

estimate was based on the available data for Medium Loss-of-Coolant Accident at Pressurized Water Reactors, as no relevant data could be found for the concentric inner and outer pipe break scenario in HTGRs [48]. The results are shown in Table 3.10, which will be further compared with the results of proposed approaches.

Table 3.10 Frequency of end states

End State	Frequency (/*y*)
1	1.31E-04
2	1.81E-08
3	1.15E-09
4	1.58E-13
5	2.18E-07
6	3.00E-11
7	1.91E-12
8	2.61E-16
9	2.79E-10
10	3.84E-14
11	2.44E-15
12	1.75E-19
13	4.64E-13
14	6.40E-17
15	1.82E-18
16	1.00E-20
17	1.14E-06
18	2.43E-12

3.5 Development of new PSA approach for HTGR

The traditional PSA method, which relies on fault and event tree analysis, has been widely used to assess the likelihood and consequences of accidents in NPPs. However, this method has some limitations when it comes to HTGRs compared to LWRs. As previously discussed, some of the differences that motivate the application of a new method in HTGRs are:

- The repairs of safety-related systems are not considered in the traditional FTA method.

- Most of the safety-related systems in HTGRs are operated continuously, while in LWRs they are on standby and activated on demand.
- The MCUB approximation is implemented in FTA, which may not always provide accurate results.
- The traditional FTA method used in LWRs assumes a specific mission time for safety systems that are activated on demand. However, the continuous operation of safety systems in HTGRs and thus ageing phenomena play a more significant role. This important factor cannot be fully considered in the standard PSA approach. As a result, a new PSA approach is required to accurately assess the risks and hazards associated with HTGRs.

To address these limitations, this research introduces a novel life-cycle simulation-based approach. By utilizing techniques such as reliability and availability simulations, this approach offers an improved assessment of risks and hazards in HTGRs. The ReliaSoft software is utilized to initiate this new approach, and this section of the thesis will provide a comprehensive overview of the specific techniques and tools employed in this novel approach.

3.5.1 Simulation-based analysis of repairable systems

In this section, the utilization of simulation techniques will be explored to address the limitation of the standard PSA approach by considering the repair of safety-related systems. The repair and and maintenance of HTGR safety-related systems over time are essential to ensure their continuous performance. By utilizing simulation techniques, various metrics and calculations can be applied to evaluate system downtime, availability, reliability, and the expected number of failures. These metrics can then be integrated into the proposed PSA approach, thus enabling the evaluation of repairable systems and overcoming the limitations of the standard FTA method.

These models are typically based on the principles of probability theory and statistical analysis, which allow for the incorporation of uncertainties and variability into the simulation. Such models can be even used to evaluate the performance of the system under different conditions, such as changes in maintenance policies, environmental factors, or other variables. Simulation-based analysis is particularly useful for repairable systems because it can help to predict the impact of repair and maintenance actions on the overall system performance, as well as it can identify areas where improvements could be made to

reduce maintenance costs or extend the life of the system. In the context of HTGRs, some safety-related systems must be continuously operated, and any failure can potentially lead to the reactor shutdown which highlights the importance of the life-cycle simulation-based techniques in such system analysis.

The following section provides the subject of simulation-based analysis techniques used in the study of repairable systems. Through this exploration, the different metrics and calculations utilized to analyze a system's downtime, availability, and reliability will be introduced. The ultimate goal of this discussion is to introduce the comprehensive process of modeling and simulating repairable systems in the proposed PSA approach that can overcome the limits of conventional FTA.

3.5.2 Reliability block diagram configuration for simulation-basedanalysis

Reliability Block Diagrams (RBDs) are widely used graphical tool in simulation-based analysis to model the arrangement of components in complex systems, enabling the assessment of system reliability as well as identification of critical components. The configuration of components or subsystems influences the analysis methods used to compute the reliability of a system. The traditional configurations include units arranged in series, parallel, or combined series/parallel configurations.

In addition to these traditional configurations, other variations such as k-out-of-n parallel configurations, load sharing containers, standby containers, inherited subdiagrams, and multi-block configurations can also be used in RBDs to model more complex systems. Each of these configurations requires a distinct analysis method to accurately assess the reliability of a system.

In the present study, the BlockSim software tool was utilized to model the RBD of the safety-related systems of HTTR. The forthcoming sections will provide a comprehensive description of the various configurations implemented for modeling the safety systems of HTTR, along with the corresponding analysis methods employed to assess their reliability.

Series systems in RBDs

The concept of a series configuration involves arranging system components in a linear sequence, as illustrated in Fig 3.9 which shows an example of 5 outside CIV components of HTTR. The fundamental principle behind this design is that the failure of any of these components will cause the entire system to fail. This is because the output of the failed component is no longer available as an input for the subsequent components.

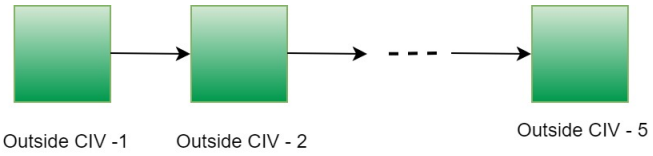

Fig. 3.9 Series configuration of CIV components in the HTTR

The reliability of a series system is directly dependent on the reliability of its individual components. When system components are assumed to be independent, as is the case in our current research, the reliability of the entire system can be calculated by multiplying the reliabilities of its individual components, as shown in Eq. (3.3). This is expressed mathematically as the product of the probability that each component will operate without failure.

$$R_S = \prod_{i=1}^{n} R_i, \tag{3.3}$$

where R_S is the reliability of the system and R_i is the reliability of the i^{th} component.

It is important to note that the reliability of a series system is always less than the reliability of the least reliable component. This is because a failure in any component will cause the entire system to fail.

The present study adopts a series configuration approach to model the safety systems of the HTTR, considering the associated system's design arrangements and operational requirements. This modeling strategy allows for a comprehensive analysis of the reliability and safety of the HTTR's components under various operating conditions.

Parallel systems in RBDs

A simple parallel system is a type of system design where multiple identical components, referred to as redundant units, are arranged in parallel to improve system reliability. In this design, the system will continue to operate if at least one of the units is functioning correctly. This approach is widely used in mission-critical systems. This redundancy in the design enhances the reliability of the system, and minimizing the likelihood of a complete system failure. For instance the HTTR's VCS is designed with redundancy to improve its reliability. Specifically, the system consists of two identical lines, each equipped with pumps and valves arranged in a parallel configuration. One of the two lines is actively used, while the other line serves as a standby unit in case of any failure or maintenance requirements.

Further examples of parallel systems will be presented in the next sections, where additional elements of RBDs are introduced.

The reliability of a simple parallel system can be calculated using the probability of each component operating without failure, given that the events are statistically independent. This is expressed mathematically as:

$$R_S = 1 - \prod_{i=1}^{n}(1 - R_i), \tag{3.4}$$

where R_S is the reliability of the system and R_i is the reliability of the i^{th} component.

It is important to note that the reliability of a simple parallel system is always greater than the reliability of the most reliable component. This is because the system will continue to function as long as at least one component is operational.

In this study, the simple parallel system design is adopted to model the redundancies present in the safety systems of the HTTR. This approach enables us to comprehensively analyze the system's reliability and safety under various operational conditions.

Series and parallel combinations

In practice, more complex systems like the safety system designs of HTTR may involve both series and parallel configurations. In such cases, the reliability of the system can be analyzed by first determining the reliability of individual series and parallel sections and then combining them in a suitable manner.

k-out-of-n parallel configuration

The k-out-of-n configuration is a type of parallel redundancy where at least k out of n parallel components must function for the system to succeed. This configuration is commonly found in safety critical systems, where multiple units are required for safe operation. As the number of required units approaches the total number of units, the behaviour of the system becomes more similar to that of a series system. To effectively model the redundancy in the safety systems components of HTTR, a k-out-of-n model configuration was utilized.

When considering a k-out-of-n configuration, the reliability of the system depends on the reliability of each component and the relationship between them.

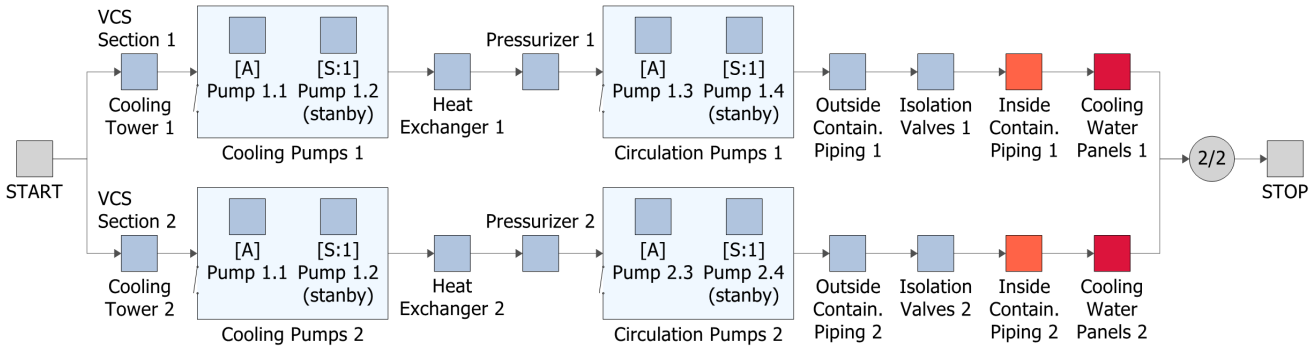

Fig. 3.10 k-out-of-n redundancy configuration of HTTR VCS components.

When the components in a k-out-of-n configuration are independent and identical, the reliability of the system can be evaluated using the binomial distribution. The reliability of such a system is given by the formula:

$$R_s(k,n,R) = \sum_{r=k}^{n} \binom{n}{r} R^r (1-R)^{n-r}, \tag{3.5}$$

where n is the total number of units in parallel, k is the minimum number of units required for system success, and R is the reliability of each unit. This formula assumes that the units fail independently of each other and have the same reliability value.

For example, in the case of the VCS components of HTTR under normal conditions, a k-out-of-n configuration was employed, as shown in Fig. 3.10. The 2/2 node indicate that both cooling paths are necessary for the system to function properly during normal operation.

However, when the components in a k-out-of-n configuration are independent but not necessary identical, their reliability can be calculated using a different formula:

$$R_s(k,n,R_1,R_2,\ldots,R_n) = \sum_{r=k}^{n} \binom{n}{r} \prod_{i=1}^{r} R_i \prod_{j=r+1}^{n} (1-R_j), \tag{3.6}$$

where n is the total number of units in parallel, k is the minimum number of units required for system success, R_i is the reliability of the i-th unit, and the product term $\prod_{i=1}^{r} R_i \prod_{j=r+1}^{n} (1-R_j)$ represents the probability that exactly r out of the n components function successfully.

This formula assumes that the units fail independently of each other, but they can have different reliability values.

This case touches the incorporated spare inverter D and battery chargers unites within the improved design of the electrical system of HTTR. Unlike another similar units, they have unique reliability values due to its varying manufacture and/or design, which will be further detailed later.

Standby redundancy

Standby redundancy configurations are an essential element of many systems designed to provide backup options for active components in the event of a failure. The container block comprises multiple other blocks, enabling the more streamlined representation and analysis of standby configurations. The container block serves two critical functions. Firstly, it clearly defines the relationships between active and standby units, and secondly, it acts as a switch mechanism that manages the process of switching between them. In reliability analysis, standby redundancy configurations can be evaluated by defining a standby container with a probability of successfully activating standby units as needed. This enables the analysis of the effectiveness of standby redundancy and its impact on the overall system reliability.

Figure 3.11 shows an example of standby redundancy configuration in the EF of HTTR. The diagram shows two components arranged in a standby configuration, with one active component (labeled with [A]) and the other on standby. It should be noted that the container block must have at least one component operational at all times to prevent system failure.

Inherited subdiagrams

In BlockSim, subdiagram blocks is used to simplify the overall diagram by incorporating smaller subdiagrams as components. A subdiagram block inherits some or all of its properties from another block diagram. This means that an analyst can maintain separate diagrams for different portions of a system and incorporate those diagrams as components of another diagram. With this technique, it is possible to generate and analyze extremely complex diagrams representing the behaviour of many subsystems in a manageable way. In this configuration, the overall reliability of the larger diagram that incorporates the subdiagram block is calculated based on the reliability of the subdiagram block. Fig. 3.12 illustrates a simple example of such configuration in CIV of HTTR, where the top diagram shows the Subdiagram Block of inside valves, representing the series configuration of the subsystem reflected in the bottom diagrams.

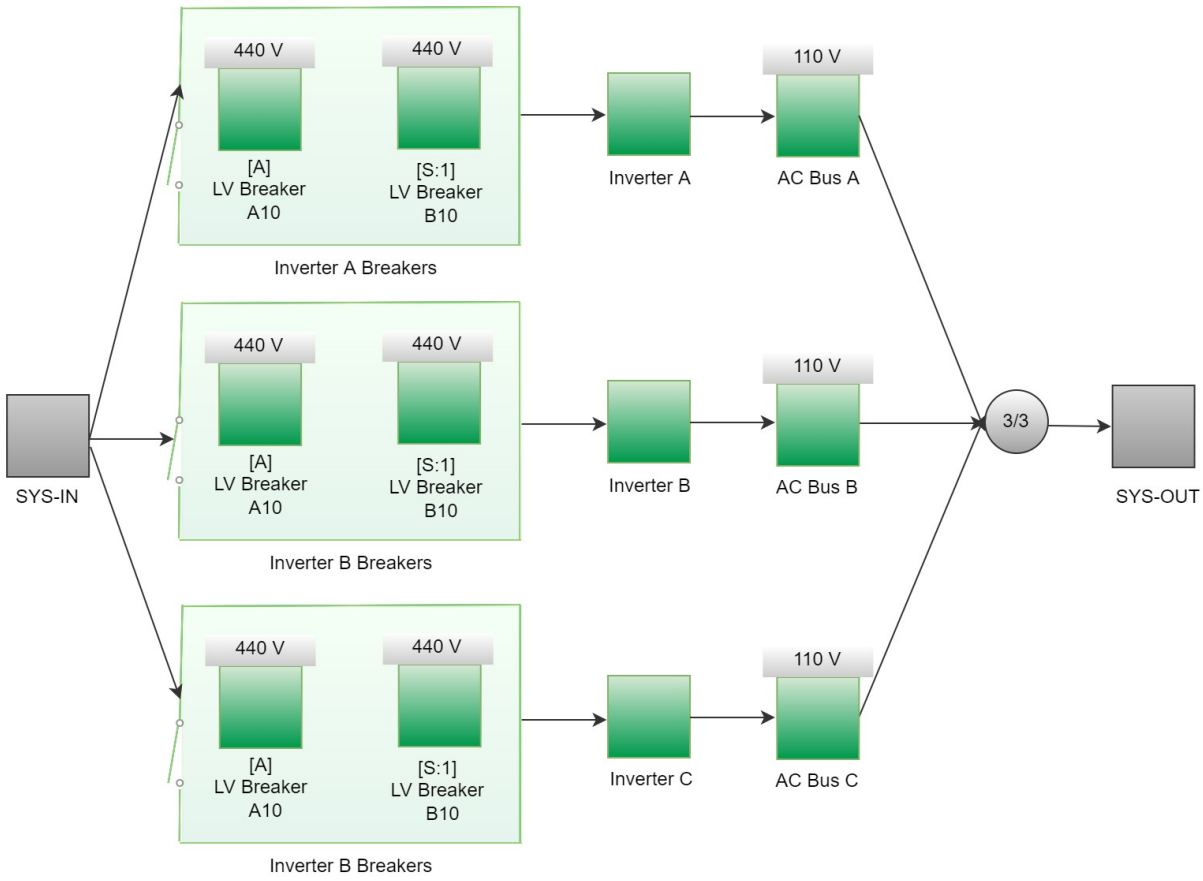

Fig. 3.11 Standby redundancy configuration of HTTR Electrical system components

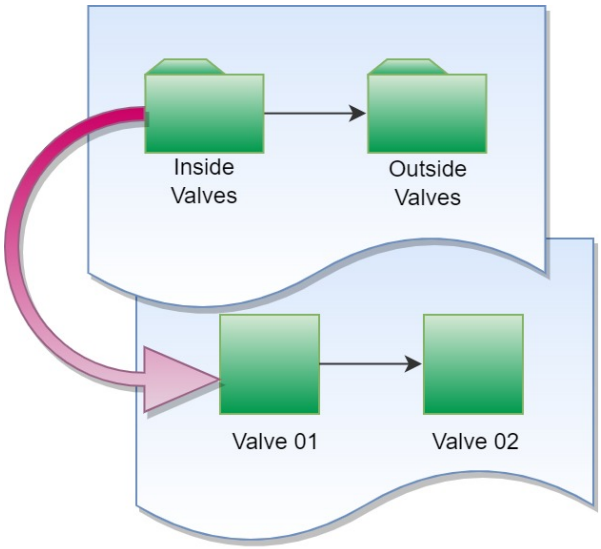

Fig. 3.12 Inherited Subdiagram Blocks of Inside and Outside Valves Configuration in the HTTR CIV System

3.5.3 Simulation-based maintenance and repair strategies

The utilization of maintenance and repair within simulation-based approaches is a major concern in current research. Simulation-based maintenance and repair strategies provide the potential to accurately model the lifecycle of a system, enabling a deeper understanding of system performance and optimization of maintenance schedules. This study focuses on repairs, which are implemented in BlockSim through the use of maintenance tasks. In simulation-based approach, there are several types of maintenance tasks available to users, each with its unique features and benefits. These maintenance tasks can be broadly classified into four categories: corrective maintenance, preventive maintenance, on-condition maintenance, and inspection. The latter three options are often referred to as scheduled maintenance tasks because they are carried out based on a predetermined schedule or set of conditions.

The maintenance tasks implemented in this study were predicated upon the notion that corrective maintenance would be performed for the safety systems of HTTR, and that maintenance activities would be promptly initiated upon the occurrence of component failure. The repair time for each component associated with the safety systems, which is defined as the duration required for corrective maintenance, was derived from multiple references [29, 16, 28, 16]. These references were selected based on their rigorous methodologies and comprehensive data sets. In the present study, the mean value of repair time was utilized to estimate the repair time for each component. The use of mean values is a common

practice in maintenance modeling, as it provides a representative estimate of the average repair duration. However, it is important to note that repair times may exhibit considerable variability, and therefore, employing more advanced statistical techniques may yield more accurate estimates. Nevertheless, the utilization of mean values is a practical and effective method for estimating repair times in the absence of more detailed data.

The scheduled maintenance is performed only for the electrical system and the VCS, which operate continuously under normal and accident conditions. Preventive maintenance, a type of scheduled maintenance, which were used here, is typically performed at regular intervals regardless of the component's condition to prevent potential failures. For this study, a specific maintenance schedule of approximately 60 days every two years of HTTR operation, as outlined in Ref [64], was utilized for the purpose of for the preventive maintenance as well as refueling procedure. These maintenance tasks are critical in predicting and estimating the precise downtime of HTTR and ensuring its safety and reliability.

3.5.4 Deterministic system downtime without component ageing

Series system

In the preceding section, the utilization of the RBD technique in a simulation-based approach for analyzing the safety systems of HTTR was explained. Furthermore, the repair tasks that were implemented in this study were introduced. In this section, the analysis of repairable systems is presented using RBDs, along with the application of RBDs in simulating system behavior. In order to better illustrate these concepts, a simple deterministic example featuring two components A and B in a series configuration will be presented. Components A and B are subject to failure every 100 hours and 120 hours, respectively, and each takes 10 hours to repair. The total downtime for this scenario is 40 hours resulting from four downing events, which leads to an overall system availability of 0.86667. The availability of the system at a given time referred to as point availability, equals 1 if the system is up at that time and 0 if it is down.

The availability of a system is a key performance indicator that measures the proportion of time that the system is operational and able to perform its required functions. This is an important metric in system reliability analysis and maintenance planning. The availability equation used to calculate the overall system availability is expressed as:

$$A = MTTF/(MTTF + MTTR). \tag{3.7}$$

Here, A represents the mean availability of the system, $MTTF$ represents the average time between system failures, and $MTTR$ represents the average time required to repair the system after a failure has occurred. It is important to note that in this research, the assumption was made that a repaired component is in the same condition as a new one. While this assumption generally holds true for systems that use new components as replacements, it may not always be the case for imperfect repairs or the utilization of the used components.

Here, in a simple deterministic system consisting of two components in series, the MTTF can be calculated as:

$$MTTF = \frac{1}{\frac{1}{100} + \frac{1}{120}} = 60, \tag{3.8}$$

and the MTTR is 10 for each component. Substituting these values into the availability equation gives:

$$A = \frac{60}{60+10+60+10+60+10+60} = 0.86667. \tag{3.9}$$

This implies that the system, on average, will be available 86.667% of the time. The system behaviour during an operation from 0 to 300 hours is shown in Fig. 3.13.

In system reliability analysis, it is often assumed that components don't age while the system is down, which is usually true. This is because when a component is not operational, it is not exposed to the stresses and strains that cause ageing and wear. However, in some cases, a component may age even when the system is down, resulting in a different operating profile. This is known as "operating through failure". Operating through failure can occur due to factors such as corrosion, self-discharge, or the presence of residual stresses.

Operating through failure can significantly affect the failure rate of a component. If a component has an increasing failure rate and continues to operate through system failure, it will have a higher failure rate when the system resumes operation. In such cases, the component may experience a sudden failure due to its increased failure rate. This is because the component may have been subjected to higher-than-normal stresses during the downtime, resulting in accelerated ageing and wear.

Therefore, while the assumption that components don't age while the system is down is usually true, it is essential to consider cases of operating through failure where components may age and wear even

[1] Source: https://reliawiki.com/index.php/Repairable_Systems_Analysis_Through_Simulation

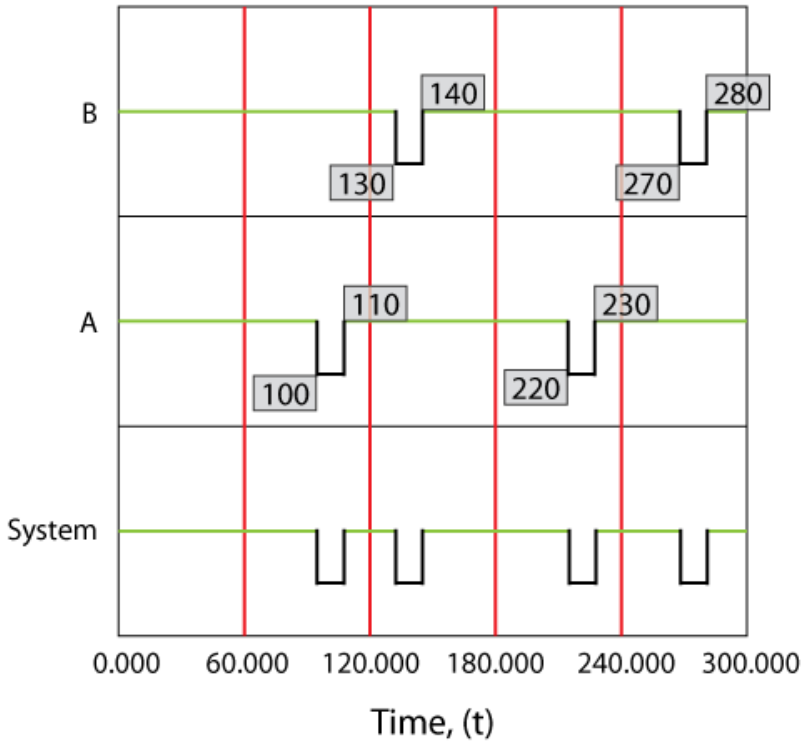

Fig. 3.13 Deterministic availability analysis of repairable two-Series component without operating through Failure[1]

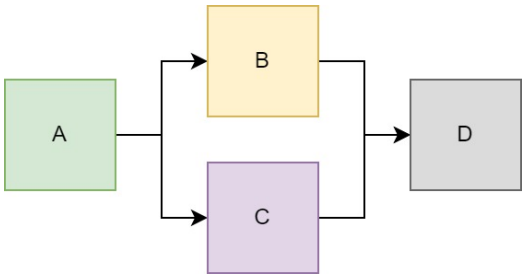

Fig. 3.14 Parallel and series components RBD configuration

when the system is not operational. Understanding and accounting for such scenarios can significantly impact the reliability and safety analysis results of a system.

Parallel system

Here, a system configured in parallel, consisting of four components A, B, C, and D, is considered. Each with respective failure times of 100, 120, 140, and 160 time units, and each requiring 10 time units to repair. In this deterministic model, the system fails twice during the operating period of 300 time units. The system operation behaviour during an operation from 0 to 300 hours is shown in Fig3.15.

Note that for illustrative purposes, deterministic events are being used, which can result in sequences of events that are unlikely to occur probabilistically. For instance, in the case that both fail at exactly 100, the assumption is made that one event occurs infinitesimally before the other. This is highly improbable in the real world, where such events would need to occur simultaneously. In such rare events, BlockSim selects the unit with the lowest ID value as the first failure, as indicated by the unique numerical ID assigned to each component.

3.5.5 Probabilistic system downtime

When dealing with systems that are subject to random failures and repairs, these events occur stochastically and follow an underlying probability distribution as depicted in Figs 3.16 and 3.17. Such analysis was considered through this research in order to enhance the realism of the analysis.

[2]Source: https://reliawiki.com/index.php/Repairable_Systems_Analysis_Through_Simulation
[3]Source: https://reliawiki.com/index.php/Repairable_Systems_Analysis_Through_Simulation
[4]Source: https://reliawiki.com/index.php/Repairable_Systems_Analysis_Through_Simulation

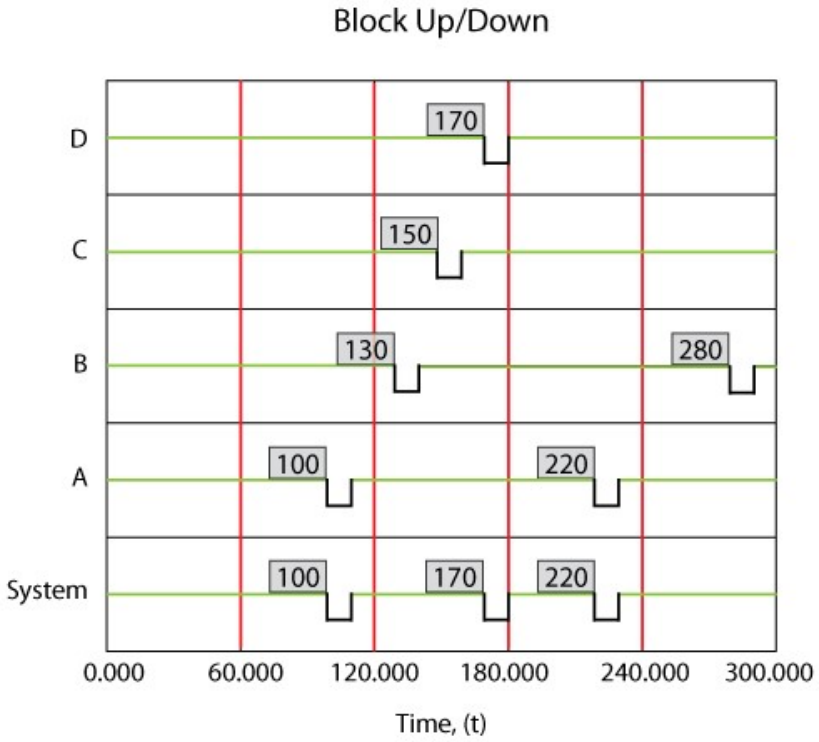

Fig. 3.15 Deterministic availability analysis of a repairable system having parallel components of B and C without operating through failure[2]

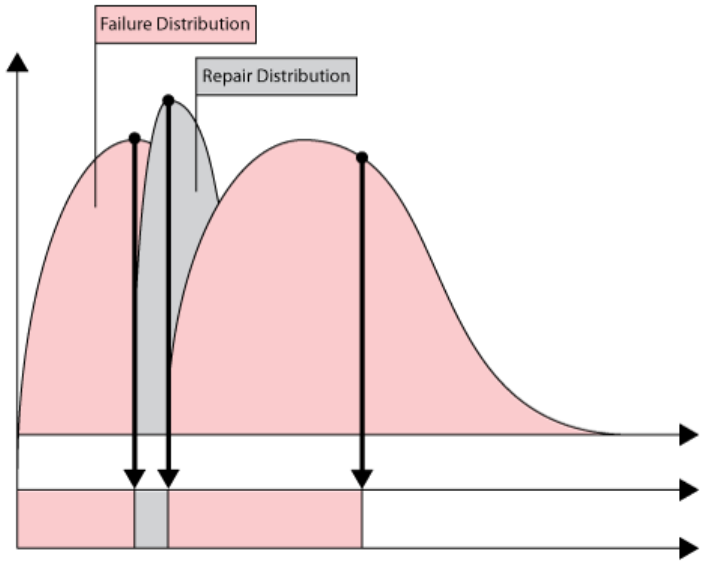

Fig. 3.16 Failure and Repair distributions for a repairable system in a probabilistic view[3]

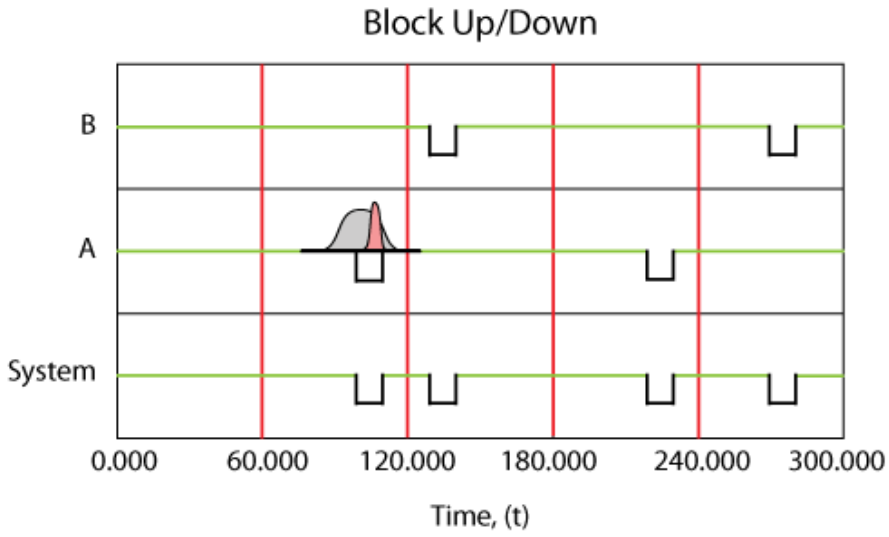

Fig. 3.17 Probabilistic availability analysis of a repairable system without operating through failure[4]

To model and analyze the behaviour of components and systems, discrete event simulation is often used. The simulation involves generating random times from distribution functions. These distributions are used to simulate the variability and uncertainty inherent in the system being analyzed. As previously discussed, the Weibull distribution is a commonly used model to simulate the time to failure and time to repair of system components in probabilistic analysis. Further details regarding the characteristics of this distribution will be presented.

To generate a random time from the Weibull distribution using a uniform random number $UR[0,1]$, the following equation is used:

$$TR = \eta \cdot (-\ln[UR[0,1]])^{1/\beta}, \tag{3.10}$$

where TR is a random variable that represents a generated time from the Weibull distribution, and β represents the shape parameter of the Weibull distribution.

3.5.6 Reliability analysis of HTTR electrical system

The simulation-based reliability of the HTTR EF performed in detail in this section is built upon the findings of the FMEA-based gradual screening approach, discussed in previous section. The analysis assumes continuous operation over a one-year period. Subsequently, the JAEA standard design and the

proposed improved design were compared in terms of reliability, taking into account potential failure modes and system ageing. The proposed improvements included the addition of components such as a secondary Commercial Offsite Power Line, Intermediate Switches between Power Centers, and a spare Inverter D. The analysis aimed to provide insights into the most reliable configuration for the electrical system, considering its potential failure modes and the impact of system ageing.

The FMEA outcomes of the HTTR's standard design reveal the critical importance of the Commercial Offsite Power Line, as it would lead to the most severe Anticipated Operational Occurrence (AOO), i.e., loss of offsite power, which is crucial for the heat removal from the reactor core [59]. In the event of LOOP, emergency generators are activated to supply safety loads while ensuring a safe reactor shutdown [69]. However, the failure of these generators, coupled with the loss of offsite power, could trigger a station blackout event, resulting in the potential loss of most instrumentation and control systems unless battery backups are used [79]. Given these risks, the severity and frequency of the LOOP failure mode were considered very high and moderately high, respectively. The RPN indicates that the Commercial Offsite Power Line had the highest value among all failure modes in the standard design, and there is no additional line available in the standard design.

There are various techniques available for assessing the reliability of a grid power system, including those discussed in [78] and [10]. The likelihood of a LOOP event occurring depends on several factors, such as the geographical location of the system, the system's design, and the reliability of the grid, as well as the prevailing weather conditions [84, 83]. Consequently, it is crucial to use site-specific reliability data when analyzing the HTTR's electrical system, rather than relying on generic data. This ensures a more accurate evaluation of the system's reliability and can help identify areas that require additional attention or improvements.

Average failure rate

The reliability of the components involved in the second reliability analysis strategy category was modeled using the exponential reliability model, which assumes a constant failure rate over the time. The model is represented by the following equation:

$$R^{\text{Exp}}_{\text{mean}(i)} = e^{-\lambda_{\text{mean}(i)}t}, \tag{3.11}$$

Where, $\lambda_{\text{mean}(i)}$ represents the mean failure rate of component i, and t represents the continuous operation time of the system, which was assumed to be 8760 hours, equivalent to one year (365 days) of continuous operation.

To ensure an accurate reliability analysis, data from reliable sources were used. The failure rates of various components were obtained from NRC reports [20, 55]. In addition, frequency data related to the LOOP, such as switchyard, weather, and grid-related factors, were obtained from reputable sources such as GRS (Gesellschaft für Anlagen- und Reaktorsicherheit gGmbH), IRSN (Institut de Radioprotection et de Sûreté Nucléaire), and NRC [77, 80].

The reliability of the n redundant non-identical components, such as inverter units and battery chargers, was modeled using the previously discussed Eq. (3.6). This equation allows for calculating the probability of having at least k out of the n units in operation.

The Tab. 3.11 shows the results of the reliability analysis of the standard and improved designs associated with the first year operation. The results show that the the first year reliability of the system have a significant increase (from below 0.5 up to 0.7). Moreover, the reliability of the Uninterruptible AC Power System (which was demonstrated to be as the most weak item within the standard design) increased from 0.76 up to 0.94 by the means of adding spare part (Inverter D). Furthermore, the reliability of offsite power increases from below 0.96 up to above 0.99 due to to an additional Commercial offsite power Line, under the assumption that weather related events are addressed as a common hazards for both lines. The reliability of the LV loads located in Buses A, B, C, and D, are also increased from 0.94 up to above 0.97 because of adding Intermediate Switches between Power Centers C/D and A/B.

Nevertheless, there exist various differences in reordered reliability data of the Inverters within the U.S. NRC and U.S. Army databases [20, 28] which might slightly justify the low reliability of the Inverters in the standard design. Further analysis was performed adding a spare Inverter D with different manufacturer and/or design. This matter results in achieving different reliability specifications compared with the regular items. Accordingly, for the Inverters A, B, and C the failure frequency was driven from the NRC database, while the failure rate of the spare Inverter was taken from the U.S. Army database. It is worth mentioning that the high reliability value of the Inverter D is justified with the fact that this unit operates during the regular Inverters repairs or maintenance which is relatively sort operated time.

Table 3.11 First-year reliability of the HTTR EF in the standard and improved design – $\lambda_{\text{mean}(i)}$, taken from [42].

No	System/Section	Standard Design	Improved Design
1	HTTR EF (the whole system)	0.4742	0.7011
2	Commercial Offsite Power	0.9556	0.9909
3	High Voltage AC Power System (6600 V)	0.9491	0.9491
4	Low Voltage AC Power Center A (440 V)	0.9380	0.9738
5	Low Voltage AC Power Center B (440 V)	0.9380	0.9738
6	Low Voltage AC Power Center C (440 V)	0.9373	0.9731
7	Low Voltage AC Power Center D (440 V)	0.9373	0.9731
8	DC Power System (100 V)	0.9678	0.9678
9	Uninterruptible AC Power System (100 V)	0.7644	0.9381
10	Computer Power Providing System (100 V)	0.9144	0.9144

Failure rate uncertainties

The reliability analysis was extended based on the FMEA tables, by performing an uncertainty analysis. The reliability data for most of the components was obtained from U.S. NRC NUREG/CR-6928 [20], which provided mean values and Probability Density Functions (PDF)s for the failure frequency of the components. The Gamma distribution was used to model the PDF of the failure rates of the components, and is represented by the following equation:

$$f^{\text{Gamma}}(\lambda_i) = \frac{1}{\Gamma(k_i)\theta^{k_i}} \lambda_i^{k_i-1} e^{-\frac{\lambda_i}{\theta_i}}, \tag{3.12}$$

where θ_i is the scale parameter and k_i is the shape parameter of the failure rate PDF of the i-th component.

Within other data sources, the minimum and maximum values of the λ_i were assumed to correspond to the 5th and 95th percentiles of the Gamma PDF. This allowed for the calculation of the main percentiles of the failure rate, including the 5th, 25th, 50th, 75th, and 95th percentiles.

To estimate the bounds of the system reliability, the associated failure rates were used in the following equation:

$$R_{n(i)}^{\text{Exp}} = e^{-\lambda_{n(i)} t}, \tag{3.13}$$

where $\lambda_{n(i)}$ is the n-th percentile of the Gamma PDF, which describes the variability of the failure rate of component i. Here, n takes the values of 5, 25, 50, 75, and 95.

The system failure rates were then evaluated using the obtained reliability bounds $R_{n(\mathrm{EF})}$ for each percentile as follows:

$$\lambda_{n(\mathrm{EF})} = -\frac{\ln(R_{n(\mathrm{EF})})}{t}. \tag{3.14}$$

It should be noted that the obtained failure rate bounds $\lambda_{n(\mathrm{EF})}$ serve as a model by which all component failure rates (λ_i) are associated with the n-th percentile of their respective PDFs. The results presented are based on point (non-continuous) values, and as such, do not represent the n-th percentiles of the PDF of the system failure frequency.

The result of the failure frequency (λ_{EF}) of both standard and improved electrical system designs is illustrated in Fig. 3.18. The ends of the whiskers in the plots represent the $\lambda_{5(\mathrm{EF})}$ and $\lambda_{95(\mathrm{EF})}$. The borders of the boxes indicate $\lambda_{25(\mathrm{EF})}$ and $\lambda_{75(\mathrm{EF})}$, while incorporated lines inside the boxes denote $\lambda_{50(\mathrm{EF})}$. As it be seen from the plots, the $\lambda_{50(\mathrm{EF})}$ of the improved design which is 3.0E-05, is more than two times lower than the value of the standard configuration which is 6.6E-05. This also can be observed from the results that apply the screening approach which reduces the lower bounds significantly. However, this approach does not influence the results of the upper bounds. This can be taken as an advantage of this approach by which the higher significant failures having higher RPN can be modeled more precisely.

Ageing phenomena

Drawing on the results of the FMEA-based gradual screening approach, the components deemed to have the greatest potential for ageing phenomena were selected for further analysis. These components include:

- Busbar Joints,
- Electrical Cables,
- Transformers,
- Circuit Breakers,
- Disconnectors.

Busbars are prone to physical defects resulting from the ageing process, particularly at the joint parts. These defects can cause creeping over the conductor materials and chemical reactions on the

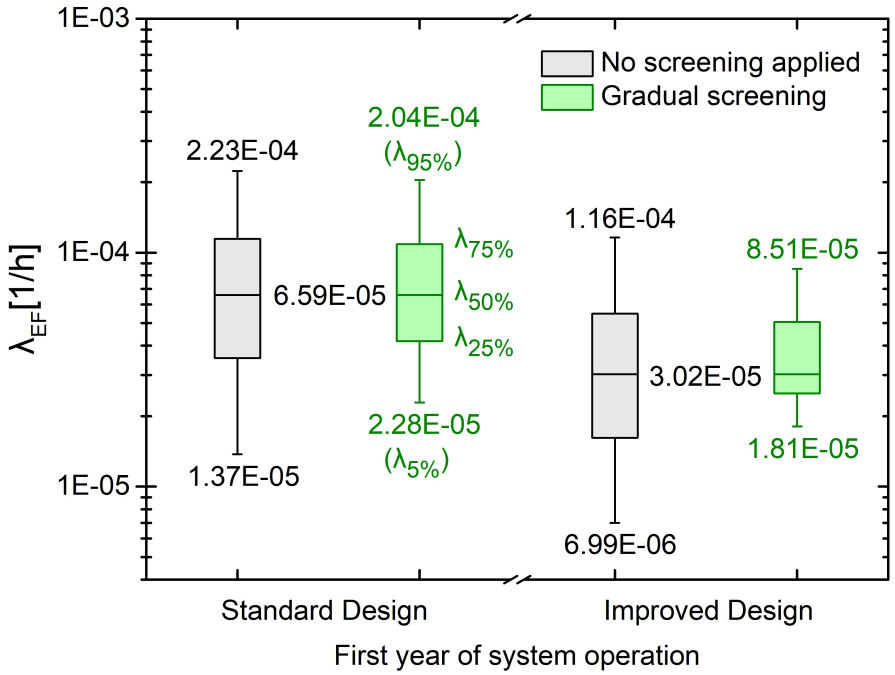

Fig. 3.18 Failure rate of the HTTR EF (λ_{EF}) for the first year of the system operation, taken from [42].

constriction zones. Although both of these processes occur simultaneously, chemical reactions are more insidious. Therefore, the lifetime of Busbar Joints is not only affected by current loads but also depends on other factors such as conductor materials, ambient temperature, and assembly quality. Studies have shown that the calculation and modeling of the lifetime of Busbar Joints should take these factors into account [12, 11].

Ageing-related failures of Electrical Cables can be attributed to mechanical and thermal stresses caused by various weather conditions and external hazards. For high voltage lines, corrosion of conductors is the most undesirable consequence of the ageing effect, leading to increased failure rates [88, 90]. In contrast, low and medium voltage lines are particularly susceptible to defects caused by water penetration into micro-cracks of insulating materials. This can generate a water tree in the insulator, which can turn into an electric tree following an electrical current flow. This phenomenon can rapidly weaken the strength of the dielectric and lead to significant failures.

Transformers are critical components in EFs, and they are vulnerable to the effects of ageing. There is a significant body of literature on the ageing of transformers [88–90, 7, 9]. Ageing-related defects in transformers include corrosion, oil degradation, and insulation deterioration. The failure frequency

of transformers is affected by various factors, including moisture, acidity, oxidation, and thermal and electrical stresses, with the latter being among the most significant causes. Ageing-related failures of transformers typically occur early in their lifetime [89]. Statistical analysis by the German Electricity Association–VDEW (Verband der Elektrizitätswirtschaft) shows that only 20% of transformer failures are due to random events, while the remaining 80% are caused by mechanical and electrical stresses associated with ageing [7]. It has been found that the lifetime of transformers is highly dependent on the hot-spot temperature, according to various transformer lifetime models [7, 9].

The reliability of Circuit Breakers is found to be high in the initial 15 years of operation. However, the ageing phenomenon reduces their reliability between the 15th and 20th year of operation. Beyond the 20th year, the failure frequency of Circuit Breakers increases sharply. Circuit Breakers can fail due to various reasons such as frequent mechanical switching, inappropriate operating conditions, environmental temperature, and moisture [89, 7].

The Disconnectors exhibit a similar ageing-related behavior as the Circuit Breakers, with the main difference being a shorter period of high reliability, typically lasting up to 12-13 years. After this period, the failure rate slightly increases, and between the 15th and 20th year of operation, the frequency of failures sharply rises, occurring earlier than in Circuit Breakers. The main factors contributing to the wear-out mechanism are material fatigue and stresses. The stresses are often related to mechanical failures that increase as the number of load cycles exceeds the material-specific threshold value [90].

The failure rate of a component often increases towards the end of its life cycle. This time-dependent behaviour of the failure rate can be characterized by the lifetime distribution of the component, which is typically determined using statistical data from ageing tests, operational experience, and probabilistic models that consider the associated stress over time [89]. By analyzing the lifetime distribution, one can estimate the remaining useful life of the component and develop maintenance strategies that maximize its operational lifespan which can be performed using a statistical tool.

The *Weibull distribution* is one of the powerful statistical tools that has been widely adopted in various engineering disciplines, including materials science, renewable energy analysis, and reliability engineering. For instance, In materials science, the *Weibull distribution* is commonly used to analyze fatigue data and estimate the probability of failure of a material or device under repeated loading or stress [61]. In the renewable energy sector, the *Weibull distribution* is frequently used to model the distribution of wind speeds at a particular location and estimate the power output of wind turbines [82, 63]. In the field of electrical engineering, the *Weibull distribution* is frequently employed to investigate the

time-dependent failure rate of the electrical components (component's lifetime) [88, 89, 9]. In general, the flexibility and efficiency of *Weibull distribution* make it a popular choice for analyzing endurance life and reliability data, especially in the context of assessing the time-dependent failure rates of various components.

The PDF function of the *Weibull distribution* is given by:

$$f_i^{\text{Weib}}(t) = \frac{\beta_i}{\eta_i}\left(\frac{t}{\eta_i}\right)^{\beta_i - 1} e^{-\left(\frac{t}{\eta_i}\right)^{\beta_i}}, \tag{3.15}$$

where t denotes the operating time, and β_i and η_i are the *shape* and *scale* parameters of the component i, respectively. To estimate the Weibull parameters for a component, the cumulative failure probability over time is analyzed by fitting the Weibull Cumulative Distribution Function (3.16) to at least two points of the component's failure probability curve. This fitting allows for the estimation of both β_i and η_i, which are essential parameters in determining the component's failure rate over time.

$$F_i^{\text{Weib}}(t) = 1 - e^{-\left(\frac{t}{\eta_i}\right)^{\beta_i}}. \tag{3.16}$$

Once β_i and η_i are obtained, the time-dependent failure rate of the component i can be calculated using the following equation:

$$\lambda_i(t) = \lambda_{\text{mean}(i)} + \lambda_i^{\text{Weib}}(t). \tag{3.17}$$

This equation defines that the failure rate $\lambda_i(t)$ of a component i can be expressed as a combination of two factors. The first factor, denoted by $\lambda_{\text{mean}(i)}$, accounts for the random failures that are modeled by the Exponential distribution. The second factor, denoted by $\lambda_i^{\text{Weib}}(t)$, captures the *age-related* failures that are modeled by the Weibull distribution. Specifically, the function $\lambda_i^{\text{Weib}}(t)$ represents the time-dependent failure rate of the component i at time t, based on its Weibull shape and scale parameters β_i and η_i.

The Weibull Failure Rate Function in Eq. (3.17) characterizes the time-dependent failure rate of a component i due to age-related failures and is expressed as:

$$\lambda_i^{\text{Weib}}(t) = \frac{\beta_i}{\eta_i}\left(\frac{t}{\eta_i}\right)^{\beta_i - 1}. \tag{3.18}$$

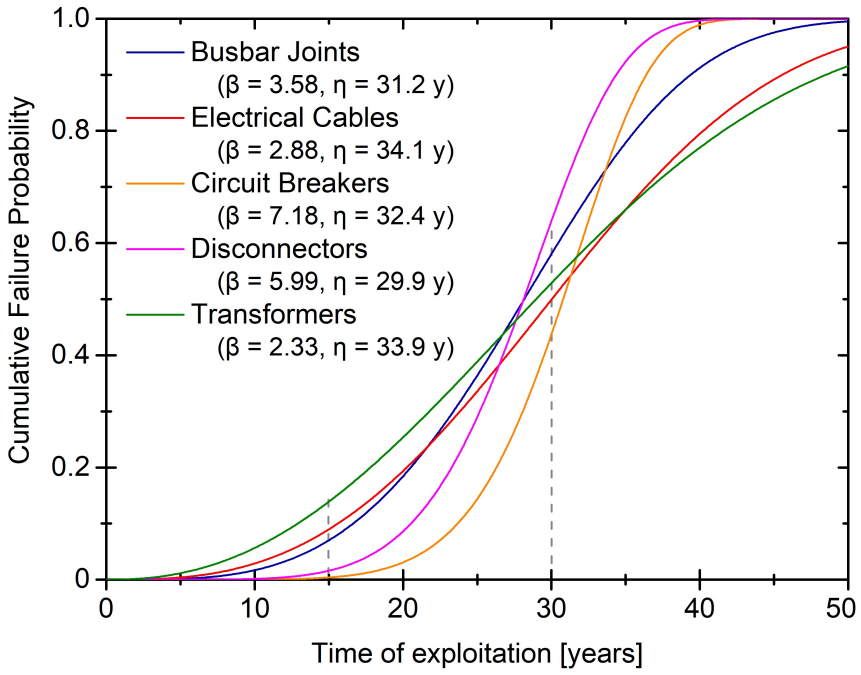

Fig. 3.19 Cumulative failure probability of the selected electrical components, taken from [42].

To model the lifetime of each electrical component, this study utilized the *Weibull distribution* (Eq.(3.15)), which is a widely-used statistical model for reliability analysis. The *shape* and *scale* parameters for each component were obtained from Eq.(3.16), which estimates the parameters based on the component's associated probability of failure after specific operating times (e.g., 15 and 30 years) as reported in the literature [88, 90, 89, 7]. These parameters are crucial for predicting the failure rate of the component over its lifetime, and for making informed decisions regarding maintenance and replacement strategies.

The results of this assessment is given in Fig. 3.19. Thus, the time-dependent failure rates were estimated using the obtained β and η parameters based on Eq. (3.17) and (3.18) as shown in Fig. 3.20.

In this section, it is assumed that the PDF of the failure rate (λ_i) of each component can be modeled using the Gamma distribution (Eq.((3.12) by the failure rate behavior within Fig. 3.20 assuming a constant variance over the model. Accordingly, the last year failure rates PDFs were modelled using this assumption (Fig. 3.21). Afterwards, the main percentiles of the PDFs including 5th, 25th, 50th, 75th, and 95th were estimated. Then, the result were applied in reliability models. Then, the n-th-order bounds of the failure rate (λ_{EF}) of the system were obtained. Finally, the results were compared with the first year of the operation (Fig. 3.22).

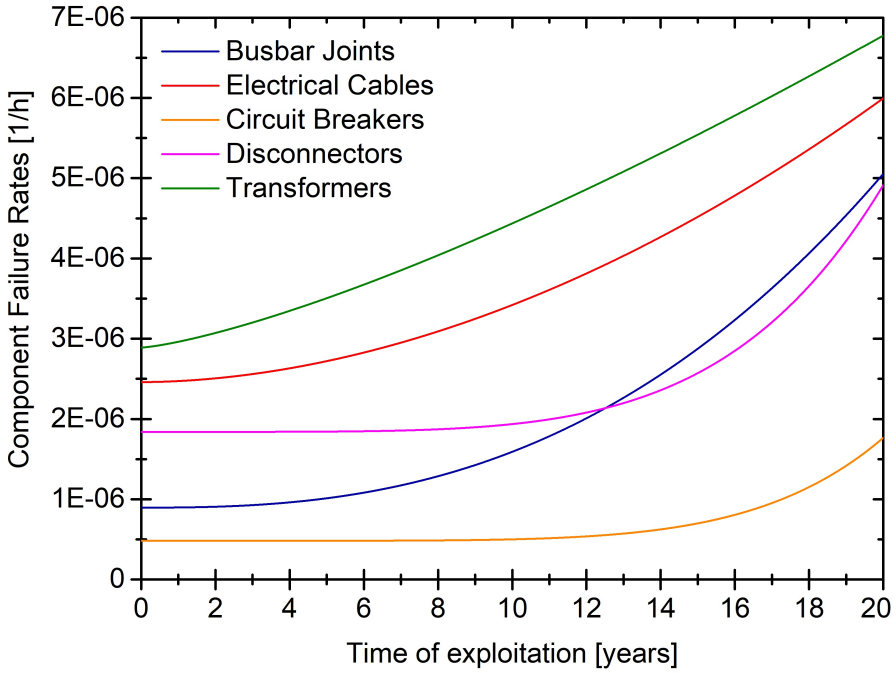

Fig. 3.20 Time-dependent failure rates of the selected electrical components, taken from [42].

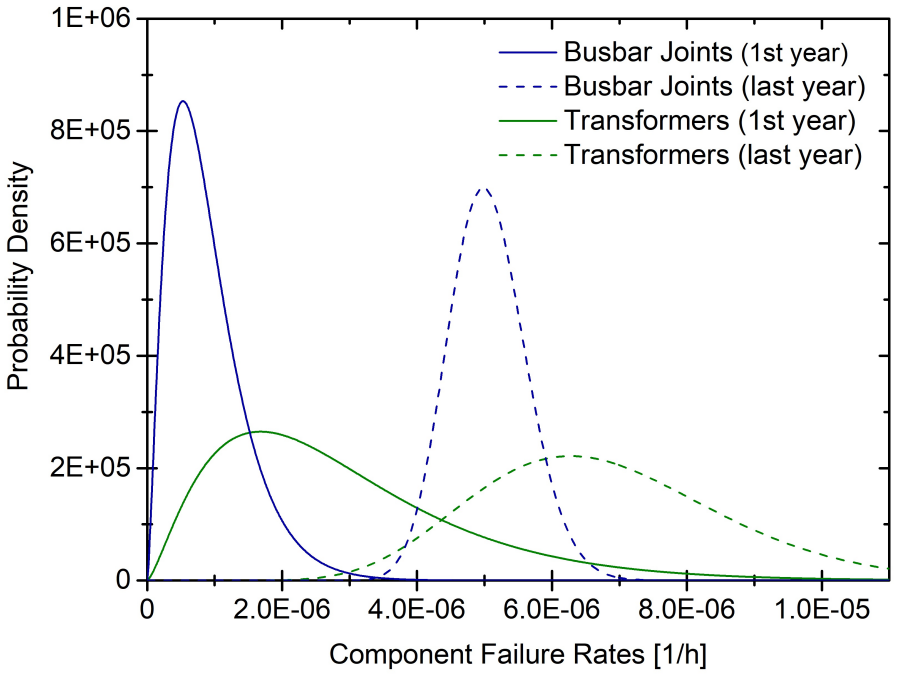

Fig. 3.21 Probability density of the component failure rates for the first and last year of operation, taken from [42].

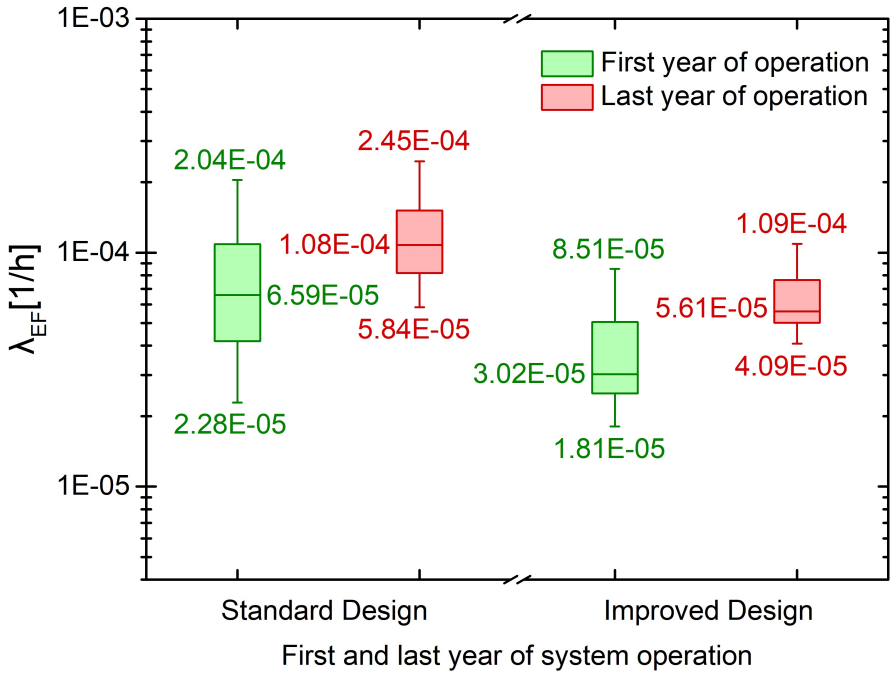

Fig. 3.22 Failure rate of the HTTR EF (λ_{EF}) for the first and last year of operation, taken from [42].

The ageing phenomenon is the procedure which leads to the failure rate increment over the lifetime of the components. According to (Fig. 3.22) the median failure rate of the standard design will be increased about 64% more compare to the first year of operation. This factor reaches to about 86% for the improved design which states that the ageing-related effects have a more dominant negative effects in the systems with higher redundancy. Despite such details, the median failure frequency of the standard design is 90% higher than the improved design. However, the failure rate upper bounds $\lambda_{95(\mathrm{EF})}$ show almost no change in the first and last year of operation for both designs. It shows about 20% increment for the standard design, and an increase of about 28% for the improved design. Whereas, more than two times increment is observed for the lower bounds $\lambda_{5(\mathrm{EF})}$ after 20 years, for both designs. The most prominent outcome from the results is that the failure frequency of the improved design after 20 years of operation will still be lower than the first year operation for the standard one.

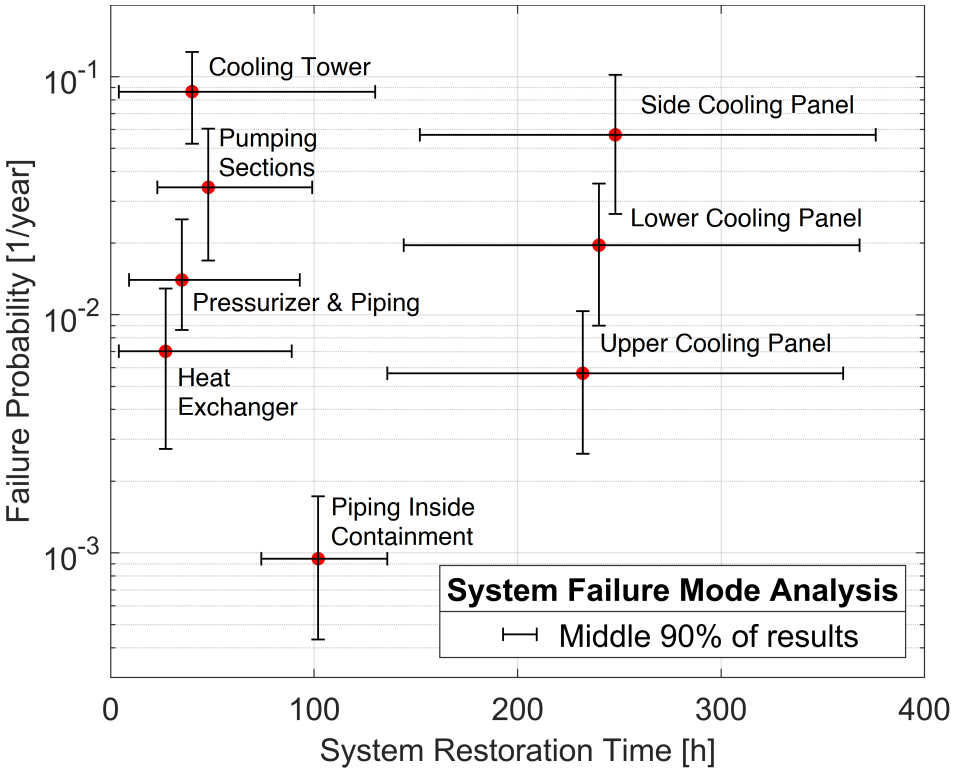

Fig. 3.23 One-year probability of failure and restoration time for a VCS section (including the associated valves)

3.5.7 Simulation-based analysis of HTTR VCS

This section presents the results of the FTA, reliability and availability analysis of HTTR VCS, based on the insights gained from the earlier FMEA analysis (presented in section 3.1.3).

The Fig. 3.23 presents the outcomes of the component FTA, which illustrates a comparison between failure probabilities and restoration durations for the key components of a single VCS section.

According to the results of the FTA, the cooling tower, which includes two fans, associated pipes, and valves, has the highest probability of failure in one year of VCS system operation, at approximately 1E-01. The dominant event contributing to this probability is the failure of a cooling fan during continuous operation. The side cooling panel failure is the second most likely event due to its complex structure and a total length of tubes exceeding 1500 m. The lower and upper cooling panels have lower failure probabilities due to simpler construction and resulting tube lengths of about 500 and 150 m, respectively. Repair time and reactor cooldown delay uncertainties affect VCS restoration time after a cooling panel failure. The heat exchanger and pressurizer components have medium values of failure probability

(around 1E-02/year). The heat exchanger's fault tree only includes tube leakage and plugging, while the pressurizer's fault tree combines the failures of the pressurizer itself and the related piping system with valves located outside the RCV. The piping located inside the containment vessel and the pump sections have the lowest failure probabilities (about 1E-03/year). The pump sections have redundancy, which enables the repair of a failed component after activation of the standby line without affecting the VCS system's functionality.

3.5.8 Reliability and availability analysis of VCS

This section aims to conduct a simulation-based analysis to determine the life-cycle reliability and inherent availability of the VCS system in both normal and emergency conditions, and assess its impact on the overall performance of the HTTR-based cogeneration plant. The study also covers the evaluation of the contribution of VCS failures to the Forced Outage Rate (FOR_{VCS}) of the cogeneration plant. The results of this study will provide valuable insights into improving the VCS system's reliability and availability, particularly in its role as an operating safety system under DLOFC. These improvements will not only enhance the safety of the nuclear cogeneration plant but also increase its profitability and efficiency.

The VCS component reliability model for the associated failure mode was defined using a one-parameter exponential function, assuming a constant failure rate over time (Eq. (3.11)).

To address the potential non-constant failure rate of the system, a two-parameter Weibull function was used to model the system reliability (Eq. (3.15)).

The inherent availability of the VCS system during normal operation $A_{\mathrm{Inher.}}$ was calculated using the following equation:

$$A_{\mathrm{Inher.}} = \frac{SH_{\mathrm{VCS}(2/2)}}{SH_{\mathrm{VCS}(2/2)} + CM_{\mathrm{VCS}(2/2)}}, \tag{3.19}$$

where the term $SH_{VCS(2/2)}$ represents the total amount of time that the VCS system operates successfully at 100% flow rate. The term $CM_{VCS(2/2)}$ represents the total amount of downtime required for corrective maintenance over the system's entire life cycle to restore full operability after failures.

The availability of the system during emergency conditions $A_{\mathrm{Emerg.}}$ was estimated using the following formula:

$$A_{\text{Emerg.}} = \frac{SH_{\text{VCS(1/2)}}}{SH_{\text{VCS(1/2)}} + CM_{\text{VCS(1/2)}}}, \tag{3.20}$$

where $SH_{VCS(1/2)}$ represent the total service hours of the VCS system during emergency conditions. $CM_{VCS(1/2)}$ represent the total corrective maintenance hours required to restore the system's minimal operability after failures.

The lifetime availability of the HTTR-based cogeneration plant was calculated using the following equation:

$$A_{\text{Cogen.}} = \frac{SH_{\text{Cogen.}}}{SH_{\text{Cogen.}} + PM + FOH_{S_1,\ldots,S_n}}. \tag{3.21}$$

Here, $SH_{\text{Cogen.}}$ represents the sum of service hours of the cogeneration plant over its life cycle. PM is the sum of hours of refueling and preventive maintenance actions. $FOH_{\text{S}_1,\ldots,\text{S}_n}$ represents the sum of forced outage hours of the plant resulting from failures of each system within the plant. In the following equation, the term FOH_{VCS} will be used instead of $FOH_{\text{S}_1,\ldots,\text{S}_n}$, since the analysis focused only on the failures of the VCS system. Thus, the remaining systems were considered 100% reliable. Therefore, the rate of forced outages caused by VCS system failures was quantified using the following equation:

$$FOR_{VCS} = \frac{FOH_{VCS}}{SH_{Cogen.} + FOH_{VCS}} \times 100. \tag{3.22}$$

Here, the hours spent on preventive maintenance and refueling were not considered in order to isolate the impact of the VCS system on the availability of the cogeneration plant based on HTTR.

Simulation model assumptions

The simulation models used in this study were developed based on several assumptions:

- Adjustment panels are not required for normal operation when both VCS sections are used.
- If the heat removal falls below 0.3 MW and only one VCS section is operational, all 48 tubes of the adjustment panels must run coolant to increase heat removal.
- The VCS system failures occurring outside the RCV can be fixed prior to the reactor cooldown.
- Preventive maintenance and refueling outages are planned for about 60 days per two years of operation.

- The lifespan of the HTTR-based facility was estimated to be approximately 20 years.
- It was assumed that the VCS mission time following an LOFC accident would be 21 days.
- The duration of forced outages of the cogeneration plant due to outside containment failures of VCS was simulated as a random variable with a normal distribution. The lower bound ($\tau_{down(5\%)}$) was set at 168 hours (one week) and the upper bound ($\tau_{down(95\%)}$) at 336 hours (two weeks).
- The duration of HTTR outages caused by inside containment failures of VCS followed a Normal distribution, with a lower bound of 2 weeks and an upper bound of 3 weeks.

The simulation model for the VCS system includes different requirements for its operation. One such model is the parallel-unit operation mode, where both VCS sections are necessary for normal operation. The reliability model was developed using RBDs, as shown in Fig. 3.10. The paths are joint by a criteria node of 2/2, indicating that both sections are required for normal operation. If one path fails, the entire system is down. In the case of emergency conditions, the criteria node was set for 1/2. During normal operation, all cooling panels are continuously active except for the adjustment tubes. If there is a significant deterioration in at least one cooling panel or loss of a single VCS section, the reactor would automatically shut down. In emergency situations, full operability of at least one VCS section, including the adjustment tubes, is required. In order to determine the failure frequency of the components with multiple failure modes the FT structures were developed.

Simulating reliability and availability of VCS

The Figs. 3.24 and 3.25 exhibit the outcomes of the simulations pertaining to the system reliability and inherent availability during normal operation. The Fig. 3.26 depicts the results for emergency conditions.

In order to establish a foundation for quantifying the level of uncertainty, a standardized approach was employed in the simulations. Specifically, the simulations were conducted using three distinct parameters: optimistic failure rates ($\lambda_{5\%}$) , which represent the upper limit of results (UB); pessimistic failure rates ($\lambda_{95\%}$), which represent the lower limit of results (LB); and mean values (λ_{mean}), which represent the base case results. Furthermore, component repair times and forced outage times were stochastically sampled within each simulation run, adhering to their respective probability distribution functions.

The life-cycle reliability analysis of the VCS under normal operation displays an exponential trend Fig. 3.24. The Weibull reliability functions fitted to the simulation points yield β parameters ranging

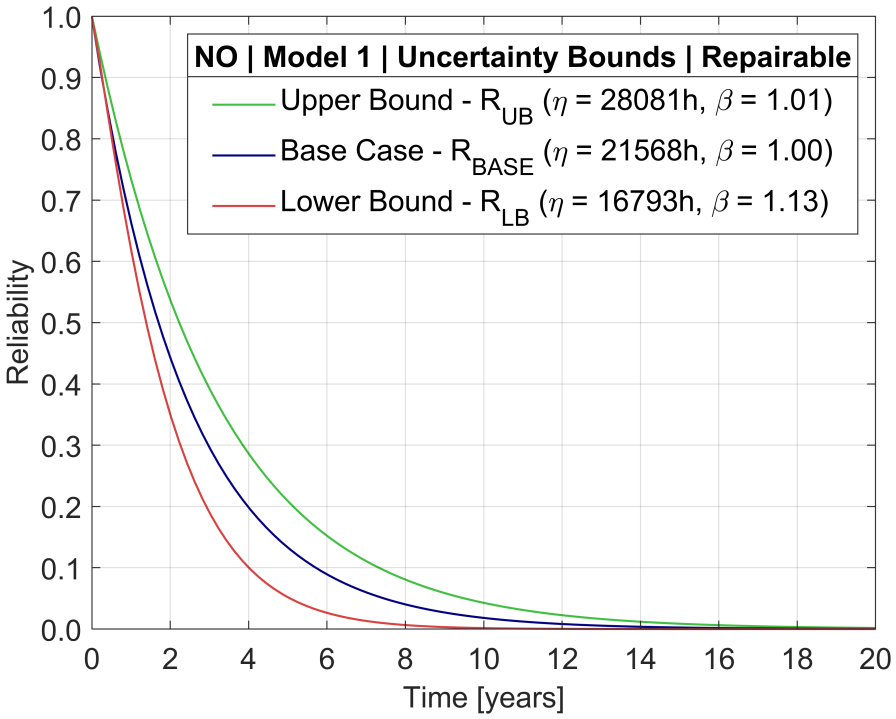

Fig. 3.24 Life-Cycle Reliability of VCS System in Normal Operation

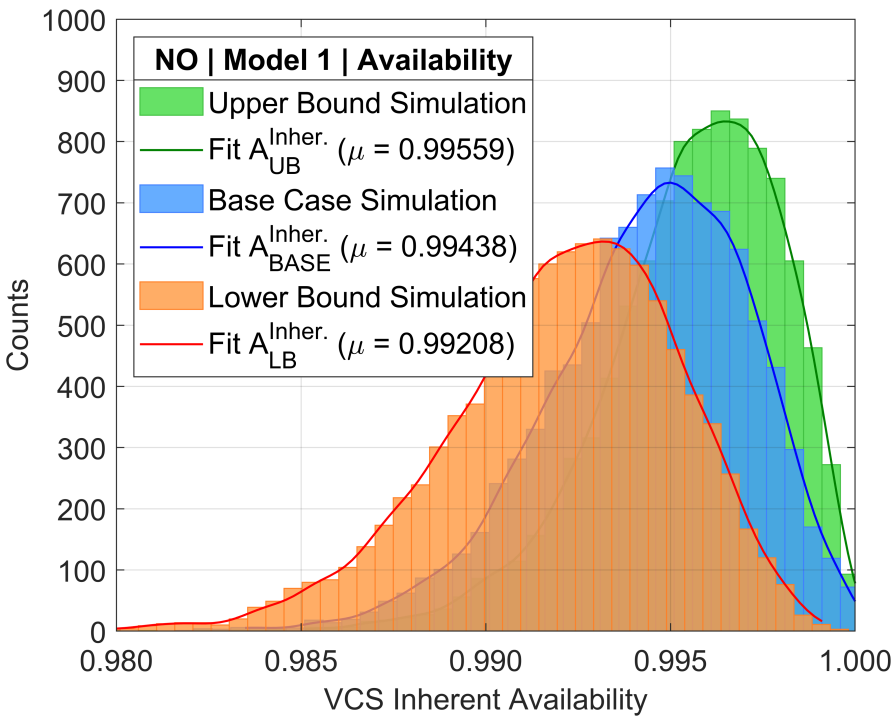

Fig. 3.25 Inherent Availability of VCS system in Normal Operation

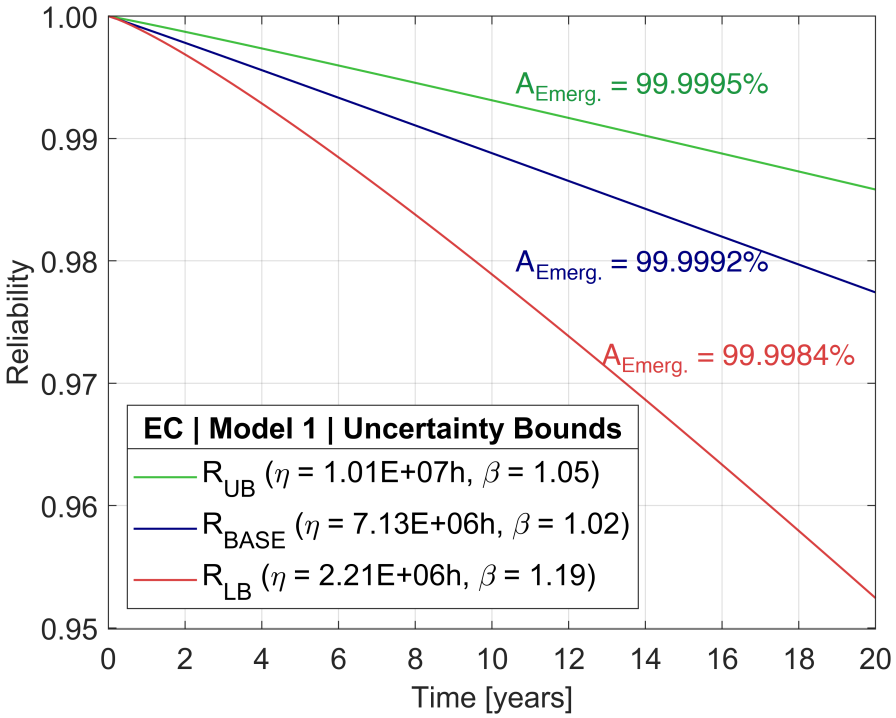

Fig. 3.26 Life-Cycle Reliability of VCS System in emergency condition

from 1.00 (base case) to 1.13 (LB). The constant failure rate of the system during normal operation, $\lambda_{\mathrm{VCS}(2/2)}$, can be calculated as the inverse of η parameter, with values of 3.56E-05/h (UB), 4.64E-05/h (base case), and 5.95E-05/h (LB). The inherent VCS availability ($A_{\mathrm{Inher.}}$) is also obtained from the resulting reliability graphs (Fig. 3.25), with mean values of 99.56% (UB), 99.46% (base case), and 99.21% (LB). These findings suggest potential for enhancing the system's operability.

During emergency conditions where only one section is required, exponential characteristics were observed as a result of reliability evaluation (Fig. 3.26), with β values ranging from 1.02 (base case) to 1.19 (LB). Calculations yielded a system failure rate, $\lambda_{\mathrm{VCS}(1/2)}$, of 9.90E-08/h (UB), 1.40E-07/h (base case), and 4.53E-07/h (LB). The mean system availability for emergency conditions ($A_{\mathrm{Emerg.}}$) was found to be as high as 99.9995% (UB), 99.9992% (base case), and 99.9984% (LB), demonstrating the exceptional performance of the VCS in removing residual heat from the reactor core and RPV following the LOFC accident.

3.5.9 A Novel approach to probability estimation in ETA

In this section, an improved probability estimation within the ETA framework is proposed, aiming to enhance the estimation of accuracy of accident scenario likelihood in HTGRs.

The standard ETA relies on the results of the traditional analytical FT method which utilizes exact algebraic equations and focuses solely on the failure characteristics of individual components. However, when dealing with long-term operating systems, it becomes imperative to account for the dynamic nature of life-cycle factors, including maintenance strategies, aging effects, repair and restoration actions, and other pivotal factors that significantly shape system performance over time. Taking into account this comprehensive set of life-cycle characteristics allows for a more precise assessment of the system's probability estimation, which cannot be effectively addressed through the analytical FT method.

In contrast to the traditional approach, the simulation-based method utilizes the discrete event simulation which provides more realistic representation of system behaviour. This approach considers non-uniform component ages and discontinuous system operation time, enabling a holistic evaluation of system performance. Furthermore, it allows for a wide range of analysis metrics beyond probability estimation, such as system availability, throughput, spare parts utilization, and life cycle costs. Moreover, the simulation-based method is capable of handling highly complex scenarios involving multiple probabilistic events, taking into account resource utilization, efficiency, and costs. It facilitates the optimization of procedures and resource allocation, analysis of relationships between systems and components, maximization of the throughput, and minimization of the work downtimes.

By incorporating this method into the ETA framework and conducting a detailed case study analysis, the limitations associated with the traditional Fault Tree (FT) approach are successfully overcome. As a result, an improved estimations of failure and success probabilities for HTGR safety systems is achieved.

The following formula is commonly used in analytical FT analysis to estimate the failure probability of a set of n safety systems involved in a specific event sequence during DLOFC accident. This formula is also applicable in simulation-based approaches to estimate the failure probability, assuming that only the failure rate characteristics of the systems are considered and restoration actions are not taken into account. The formula is as follows:

$$\lambda_{Seq.}^{DLOFC} = \lambda^{DLOFC} \prod_{i=1}^{n} (1 - R_{Sys\_NonRepair,i}(T_{DLOFC})), \tag{3.23}$$

where $\lambda_{Seq.}^{DLOFC}$ represents the frequency of the particular event sequence when n safety systems fail under a DLOFC accident. λ^{DLOFC} denotes the frequency of DLOFC accident, $R_{Sys\_NonRepair,i}(T_{DLOFC})$ represents the probability of failure of i-th safety systems in the associated event sequence, assuming that they cannot be repaired or restored within the considered mission time T_{DLOFC}. For this analysis, as previously stated, a mission time of 21 days (500 hours) is assumed.

In the next formula simulation-based improvement is extended using conditional probability:

$$\lambda_{Seq.}^{DLOFC} = \lambda^{DLOFC} \prod_{i=1}^{n} (1 - R_{Sys\_NonRepair,i}(T_{DLOFC}|T)). \tag{3.24}$$

where $R_{Sys\_NonRepair}(T_{DLOFC}|T)$ represents the conditional reliability. Conditional reliability is defined as the probability that a component or system will continue to operate without failure for a specific mission time, denoted as T_{DLOFC}, given that it has already been in operation and survived up to a certain time T. For this work, T represents a period of 2 years, during which the period between preventive maintenance of HTTR was fixed at 60 days. However, it is important to note that the current formulation does not account for the impact of corrective and preventive maintenance actions.

In the last step, further improvement is implemented by considering the possibility of repairing and performing preventive maintenance on the associated safety systems after any failure. This is reflected in the equation by including the system availability factor as follows:

$$\lambda_{Seq.}^{DLOFC} = \lambda^{DLOFC} \prod_{i=1}^{n} (1 - (A_{\mathrm{Emrg.},i} \cdot R_{Sys\_Repair,i}(T_{DLOFC}|T))), \tag{3.25}$$

where $A_{\mathrm{Emrg.},i}$ represents the inherent availability of the i-th safety-related system in associated sequence, which is defined similarly to the inherent availability for the VCS system (as described in Eq. 3.20). It estimates the probability of the system being available when needed during a DLOFC event.

3.6 Results and discussion

In order to accurately investigate the probabilities of event sequences in HTGRs within the framework of FT and ET appraches in PSA, it is essential to consider the unique characteristics of their safety-related systems, which differ from those in LWRs in which the traditional PSA in implemented. Traditional PSA methods, relying on conventional FT analysis, are limited in capturing the behavior of these systems during accidents. Therefore, there is a need to improve the PSA methodology when applied to HTGRs.

One key difference of HTGR safety-related systems is their continuous operation under both normal and accident conditions, highlighting their dynamic nature. Conventional FT analysis, which relies on algebraic analysis, cannot fully capture such characteristics. In order to address this limitation, a more comprehensive strategy analysis is necessary to accurately evaluate the failure probabilities associated with their safety-related systems.

In this study, a simulation-based method, that utilizes discrete event simulation, was utilized as an alternative to the conventional FT approach that relies on algebraic analysis. The simulation method allows for the incorporation of maintenance activities, including preventive and corrective measures, throughout the operational lifetime of the associated safety systems. As a result, enhanced robustness and accuracy are achieved in estimating accident probabilities within the PSA framework. This approach successfully overcomes the limitations of traditional methods, which often oversimplify system dynamics and neglect the significance of maintenance. By adopting a life-cycle simulation-based approach, a pathway towards more reliable estimations of failure and success probabilities for safety-related systems in HTGRs throughout their operational lifetime is established.

Tab. 3.12 presents an overview of the mean frequencies results obtained for the standard (traditional) and simulation-based approaches. The simulation-based method results show a significant reduction in the majority of sequences, ranging from one to over three orders of magnitude, compared to the standard approach.

In order to determine the range of frequency boundaries in two approaches, an uncertainty analysis was conducted, as illustrated in Figs 3.27, 3.28 and 3.29. The whiskers on the plots represent the 5th and 95th percentiles of the frequency points for each specific sequence. The borders of the boxes represent the 25th and 75th percentiles, while the line inside the boxes corresponds to the 50th value.

However, it is worth noting that for certain sequences (such as 1, 3, 9, and 11), failures occur solely in safety-related systems that are in standby mode and only operate during the accident time, such as EAP, and/or RSS. Consequently, given the unchanged results between the standard and simulation-based approaches, the corresponding data was excluded in uncertainty analysis. For sequence number 16, the differences could not be clearly demonstrated due to the very low values involved (changing from 1.00E-20 to 5.59E-17 in the standard approach and remaining at 1.00E-20 in the simulation-based method).

To facilitate a better visualization of the data ranges, the plots were arranged in such a way that sequences with similar orders of magnitude were presented together in the same plot framework.

Table 3.12 Comparison of end state frequencies in the event tree of DLOFC accident in HTTR: Standard vs. Simulation-based approaches using mean frequencies

Sequence No.	Standard*	Improved*
1	1.31E-04	1.31E-04
2	1.81E-08	7.11E-10
3	1.15E-09	1.15E-09
4	1.58E-13	4.57E-15
5	2.18E-07	3.16E-09
6	3.00E-11	1.71E-14
7	1.91E-12	2.76E-14
8	2.61E-16	1.16E-19
9	2.79E-10	2.79E-10
10	3.84E-14	1.51E-15
11	2.44E-15	2.44E-15
12	1.75E-19	1.00E-20
13	4.64E-13	6.72E-15
14	6.40E-17	1.45E-20
15	1.82E-18	1.45E-20
16	1.00E-20	1.00E-20
17	1.14E-06	2.07E-07
18	2.43E-12	4.40E-13

* The values are expressed as frequency per year.

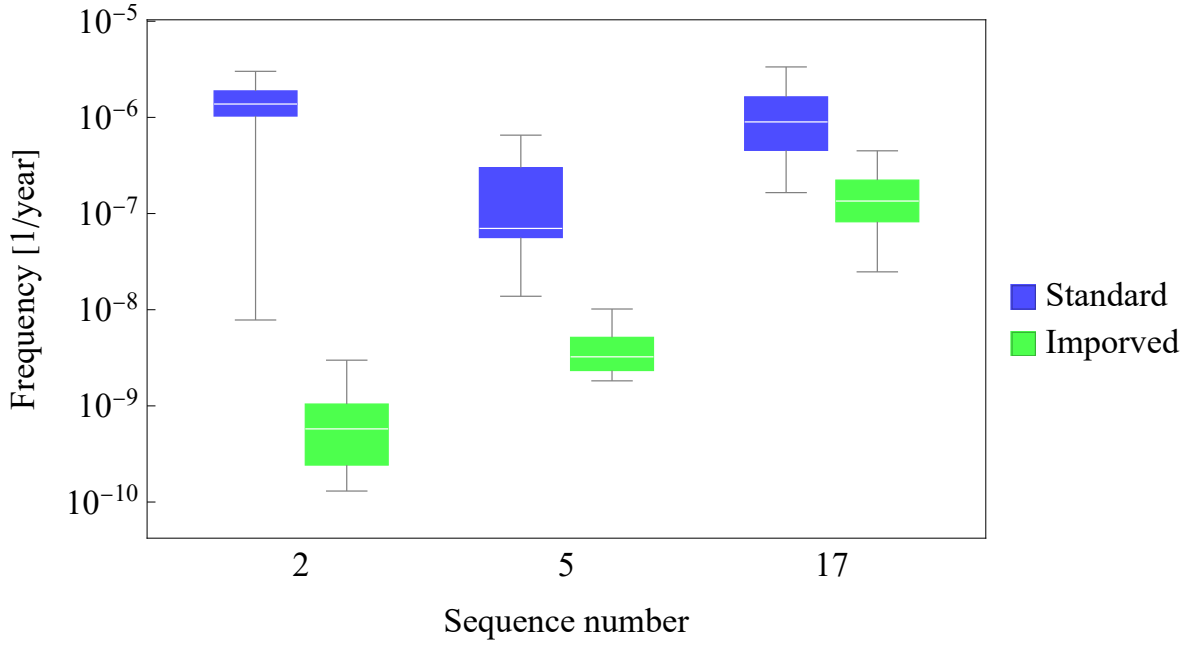

Fig. 3.27 Frequency of DLOFC event tree sequences in HTTR (Standard vs. Improved approaches)

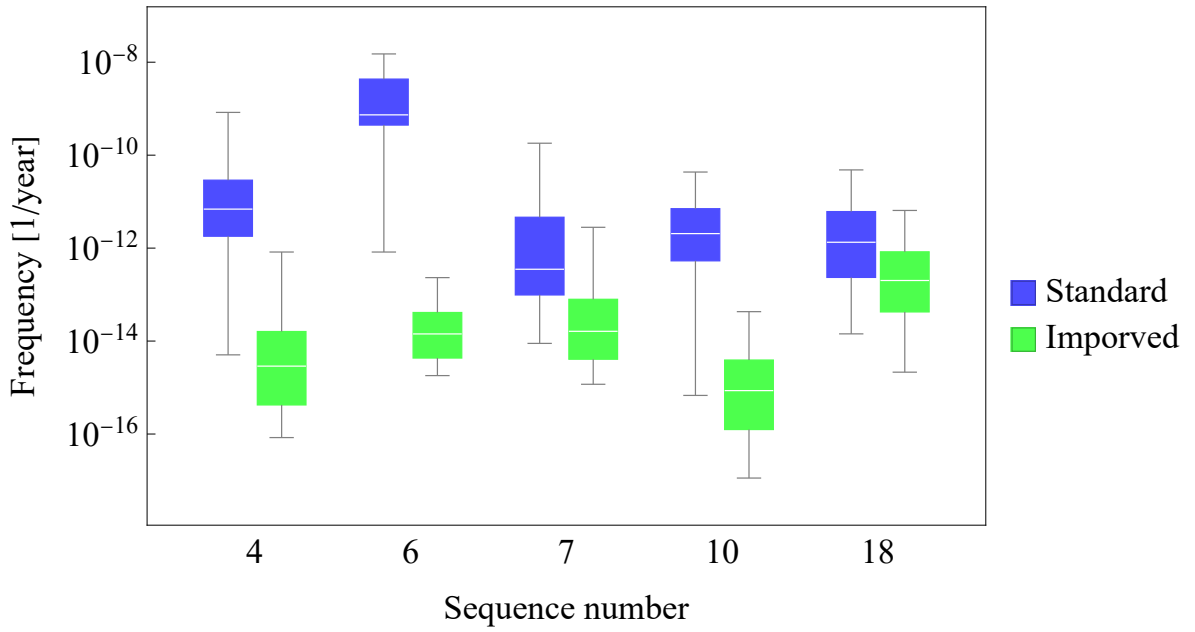

Fig. 3.28 Frequency of DLOFC event tree sequences in HTTR (Standard vs. Improved approaches)

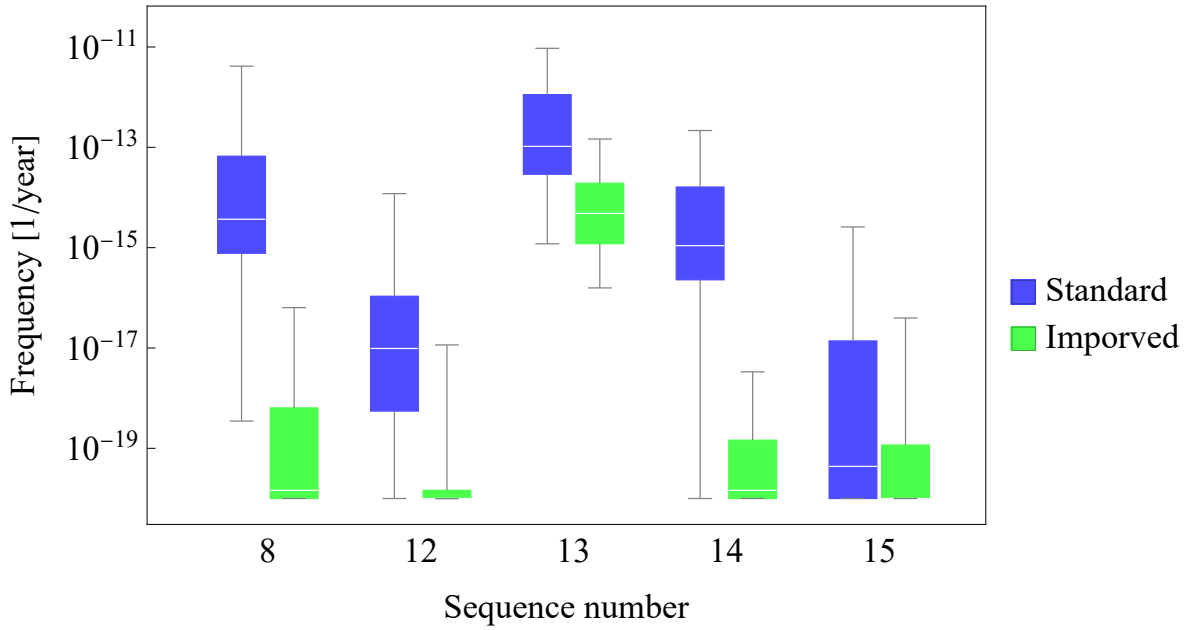

Fig. 3.29 Frequency of DLOFC event tree sequences in HTTR (Standard vs. Improved approaches)

It is noteworthy that the median values in the improved approach are significantly lower, ranging from one to over than five orders of magnitude, compared to the standard approach. The lower boundary (5th percentile) also exhibits a reduction of one to two orders of magnitude. Similarly, the 25th, 75th, and 95th percentiles show reductions ranging from one to five orders of magnitude.

In conclusion, the results reveal that the standard approach tends to overestimate event frequencies and risks, whereas the simulation-based approach provides more accurate and realistic results. By considering operational conditions, and maintenance actions, the simulation-based approach provide a robust PSA of HTGRs. These findings contribute valuable insights into the reliability and safety of HTGRs under different operating conditions.

Chapter 4

Summary and overall conclusions

The inherent safety features of HTGRs hold great promise for achieving safe and sustainable nuclear energy generation in the near future. However, when it comes to the PSA assessment of such reactors, the applicability of conventional PSA methods developed for LWRs raises concerns regarding their ability to accurately capture the specific characteristics and operational conditions of HTGRs. Therefore, the primary objective of this thesis was to improve the traditional PSA methodologies and address their limitations when applied to HTGRs, in order to provide a more comprehensive and accurate assessment of their safety.

In order to achieve a more precise and realistic quantification of event sequence frequencies, a novel approach based on life-cycle simulations of system reliability and availability was proposed. The standard PSA model was initially implemented to analyze the DLOFC event in the HTTR using ET technique and FT analysis, where statistical calculations is employed. Subsequently, the standard FT analyses were replaced with a simulation-based method to provide a more accurate representation of event sequences probability.

The research findings emphasize that the standard PSA approach, which lacks the ability to incorporate the realistic operational conditions of HTGR safety-related systems, often leads to pessimistic results for HTGRs. To address this limitation, an improved PSA methodology was developed in this study to effectively capture the real and long-term operational characteristics of HTGR safety systems during accident conditions, resulting in significantly improved accuracy and reliability of the results.

In conclusion, this research underscores the significance of advancing and implementing tailored PSA methodologies for HTGRs. The findings strongly advocate for a departure from conventional

approaches and the adoption of comprehensive simulation-based techniques that accurately capture the realistic operational conditions of HTGRs. By continuously enhancing and refining these PSA methodologies, the nuclear industry can effectively ensure the safe and sustainable operation of HTGRs. This research provide valuable insights for informed risk decision-making, facilitating effective risk assessment and mitigation strategies. Furthermore, the findings inform decision-making processes, shape regulatory requirements, and ultimately enhancing the overall safety of HTGRs.

4.1 Directions for future research

The research conducted in this thesis has laid the foundation for further advancements and exploration in the field of PSA for HTGRs. Several promising directions for future research are identified:

1. **Incorporation of ageing phenomena:** The proposed methodology can be extended to consider the effects of ageing phenomena on the failure rates of components and systems in HTGRs. This would more enhance the accuracy of reliability assessments by accounting for the potential increase in failure rates over time.

2. **Extension to other initiating events:** While this research focused on the DLOFC variant as the reference initiating event, future research should expand the methodology to include other potential internal and external accident scenarios in HTGRs. This would broaden the scope of the analysis and provide a more comprehensive assessment of the safety and reliability aspects under different operational conditions.

3. **Verification with real reliability data:** In order to enhance the credibility and applicability of the proposed methodology, future research should focus on validating and refining the approach using real reliability data obtained from operational HTGRs. Comparing the results with actual plant performance will further strengthen the methodology and increase confidence in its outcomes.

4. **Integration of human factors analysis:** Human factors have a significant influence on the safe operation of nuclear power plants. To optimize the design and operation of HTGRs, future research should explore the integration of human factors analysis into the PSA methodology. This consideration will provide valuable insights into the impact of human-system interactions and help identify strategies for enhancing safety and performance.

By pursuing these research directions, further advancements can be made in the field of PSA for HTGRs, leading to improved safety assessments and reliable operation of HTGRs in the future.

References

[1] (1992). *Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1)*. Number 50-P-4 in Safety Series. Vienna.

[2] (1995). *Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 2): Accident Progression, Containment Analysis and Estimation of Accident Source Terms: A Safety Practice*. Number 50-P-8 in Safety Series. INTERNATIONAL ATOMIC ENERGY AGENCY, Vienna.

[3] (1996). *Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 3): Off-Site Consequences and Estimation of Risks to the Public: A Safety Practice*. Number 50-P-12 in Safety Series. Vienna.

[4] (2012). Development of probabilistic safety assessment with respect to the first demonstration nuclear power plant of high temperature gas cooled reactor in china. *Nuclear Engineering and Design*, 251:385–390. 5th International Topical Meeting on High Temperature Reactor Technology (HTR 2010).

[5] (2020). *Reliability Data for Research Reactor Probabilistic Safety Assessment*. Number 1922 in TECDOC Series. INTERNATIONAL ATOMIC ENERGY AGENCY, Vienna.

[6] (2022). *High-temperature Gas-cooled Reactors and Industrial Heat Applicationse*. Nuclear Energy Agency.

[7] Abd El Aziz, M. M., Ibrahim, D. K., Kamel, H. A., et al. (2010). Estimation of the lifetime of electrical components in distribution networks. *The Online Journal on Electronics and Electrical Engineering (OJEEE)*, 2(3):269–273.

[8] Ang, M. and Buttery, N. (1997). An approach to the application of subjective probabilities in level 2 PSAs. *Reliability Engineering & System Safety*, 58(2):145–156.

[9] Awadallah, S. K., Milanović, J. V., and Jarman, P. N. (2014). The influence of modeling transformer age related failures on system reliability. *IEEE Transactions on Power Systems*, 30(2):970–979.

[10] Benabid, R., Merrouche, D., Bourenane, A., and Alzbutas, R. (2018). Reliability assessment of redundant electrical power supply systems using fault tree analysis, reliability block diagram, and Monte Carlo simulation methods. In *2018 International Conference on Electrical Sciences and Technologies in Maghreb (CISTEM)*, pages 1–7. IEEE.

[11] Bergmann, R., Löbl, H., Bohme, H., and Großmann, S. (1997a). Calculation of the lifetime of electrical busbar joints. *European transactions on electrical power*, 7(6):403–408.

[12] Bergmann, R., Löbl, H., Böhme, H., and Großmann, S. (1997b). Model to describe the chemical ageing behaviour of electrical busbar joints. *European transactions on electrical power*, 7(5):345–350.

[13] Bertsche, B. (2008). *Reliability in automotive and mechanical engineering: determination of component and system reliability*. Springer Science & Business Media.

[14] Borysiewicz, M., Bronowska, K., Kopka, P., Kowal, K., Kwiatkowski, T., Prusiński, A. M., Prusiński, P. A., and Siess, G. (2013). The PSA analysis of pwr emergency coolant injection availability following SBLOCA. *Nukleonika*, 58.

[15] Cadwallader, G., Hannaman, G., Jacobsen, F., and Stokely, R. (1976). HTGR plant availability and reliability evaluations. volume ii. appendices. Technical report, General Atomic Co., San Diego, CA (USA).

[16] Cadwallader, L. C. (2012). Review of maintenance and repair times for components in technological facilities. Technical report, Idaho National Lab.(INL), Idaho Falls, ID (United States).

[17] Čepin, M. and Volkanovski, A. (2009). Consideration of ageing within probabilistic safety assessment models and results. *Kerntechnik*, 74(3):140–149.

[18] Commission, N. R. et al. (1991). Nuclear plant aging research (NPAR) program plan. Technical report, Nuclear Regulatory Commission.

[19] Commission, U. N. R. (1975). *Reactor safety study: An assessment of accident risks in US commercial nuclear power plants*, volume 2. National Technical Information Service.

[20] Eide, S., Wierman, T., Gentillon, C., Rasmuson, D., and Atwood, C. (2007). Industry-average performance for components and initiating events at US commercial nuclear power plants.

[21] Everline, C., Bellis, E., and Vasquez, J. (1986). Probabilistic risk assessment of the modular HTGR plant. revision 1. Technical report, GA Technologies, Inc., San Diego, CA (United States).

[22] Faghihi, F., Ramezani, E., Yousefpour, F., and Mirvakili, S. (2008). Level-1 probability safety assessment of the iranian heavy water reactor using SAPHIRE software. *Reliability Engineering & System Safety*, 93(10):1377–1409.

[23] Fujiwara, Y., Nemoto, T., Tochio, D., Shinohara, M., Ono, M., and Takada, S. (2017). Loss of core cooling test with one cooling line inactive in vessel cooling system of high-temperature engineering test reactor. *Journal of Nuclear Engineering and Radiation Science*, 3(4).

[24] Georgescu, G., Corenwinder, F., and Evrard, J. M. (2008). EPR risk-informed activities at IRSN. In *Proceedings of PSA '08, International Topical Meeting on Probabilistic Safety Assessment, Knoxville, Tennessee*.

[25] Group, I. N. S. A. (1996). *Defence in Depth in Nuclear Safety: INSAG-10: a Report*. International Atomic Energy Agency.

[26] GUIMARÃES, A. C., LAPA, C. M. F., CARLOS, A., MÓL, A., and MOREIRA, M. D. L. (2009). Fuzzy methodology supporting probabilistic safety assessment. *Advances in Computer Science and Engineering*.

[27] Guimarães, A. C. F. and Lapa, C. M. F. (2004). Fuzzy FMEA applied to PWR chemical and volume control system. *Progress in Nuclear Energy*, 44(3):191–213.

[28] Hale, P. and Arno, R. G. (2000). Survey of reliability and availability information for power distribution, power generation, and HVAC components for commercial, industrial, and utility installations. In *2000 IEEE Industrial and Commercial Power Systems Technical Conference. Conference Record (Cat. No. 00CH37053)*, pages 31–54. IEEE.

[29] Hannaman, G. (1978). Gcr reliability data bank status report. Technical report, General Atomics, San Diego, CA (United States).

[30] Hashim, M., Yoshikawa, H., Matsuoka, T., and Yang, M. (2014). Quantitative dynamic reliability evaluation of ap1000 passive safety systems by using FMEA and GO-FLOW methodology. *Journal of nuclear science and technology*, 51(4):526–542.

[31] Hayashi, K., Sawa, K., Shiozawa, S., and Fukuda, K. (1989). Assessment of fuel integrity of the high temperature engineering test reactor (HTTR) and its permissible design limit. Technical report, Japan Atomic Energy Research Inst.

[32] Henley, E. J. and Kumamoto, H. (1996). Probabilistic risk assessment and management for engineers and scientists. *IEEE Press (2nd Edition)*.

[33] Hicks, T. (2011). Modular HTGR safety basis and approach. Technical report, Idaho National Lab.(INL), Idaho Falls, ID (United States).

[34] IAEA. (2017). *Safety of nuclear power plants: design*. International Atomic Energy Agency.

[35] INSAG, I. (1999). 12 "basic safety principles for nuclear power plants 75-INSAG-3 rev. 1.". *IAEA International Nuclear Safety Advisory Group*.

[36] Ishikawa, J., Muramatsu, K., and Sakamoto, T. (2002). Systematic source term analyses for level 3 PSA of a BWR with mark-ii type containment with THALES-2 code. In *International Conference on Nuclear Engineering*, volume 35960, pages 87–94.

[37] Keller, W. and Modarres, M. (2005). A historical overview of probabilistic risk assessment development and its use in the nuclear power industry: a tribute to the late professor norman carl rasmussen. *Reliability Engineering & System Safety*, 89(3):271–285.

[38] Kelly, D. L. and Smith, C. L. (2009). Bayesian inference in probabilistic risk assessment—the current state of the art. *Reliability Engineering & System Safety*, 94(2):628–643.

[39] Kim, K. O. and Zuo, M. J. (2018). General model for the risk priority number in failure mode and effects analysis. *Reliability Engineering & System Safety*, 169:321–329.

[40] Kowal, K. (2022). Lifetime reliability and availability simulation for the electrical system of HTTR coupled to the electricity-hydrogen cogeneration plant. *Reliability Engineering & System Safety*, 223:108468.

[41] Kowal, K., Potempski, S., Siess, G., and Stano, P. M. (2018). Application of probabilistic safety assessment for nuclear-chemical installations with high temperature reactors: Challenges and insights. In *HTR 2018 International Conference on High Reactor Technology Proceedings*, page 141.

[42] Kowal, K. and Torabi, M. (2021). Failure mode and reliability study for electrical facility of the high temperature engineering test reactor. *Reliability Engineering & System Safety*, 210:107529.

[43] Kunitomi, K., Nakagawa, S., and Shinozaki, M. (1996a). Passive heat removal by vessel cooling system of HTTR during no forced cooling accidents. *Nuclear engineering and design*, 166(2):179–190.

[44] Kunitomi, K., Shinozaki, M., Kodama, H., Yamamoto, M., and Hontani, K. (1996b). Design and fabrication of the reactor vessel cooling system (VCS) in HTTR. Technical report.

[45] Liu, H.-C., Liu, L., and Liu, N. (2013). Risk evaluation approaches in failure mode and effects analysis: A literature review. *Expert systems with applications*, 40(2):828–838.

[46] Liu, T., Tong, J., and Zhao, J. (2008). Probabilistic risk assessment framework development for nuclear power plant. In *2008 IEEE International Conference on Industrial Engineering and Engineering Management*, pages 1330–1334. IEEE.

[47] Lo, H.-W., Liou, J. J., Yang, J.-J., Huang, C.-N., and Lu, Y.-H. (2021). An extended fmea model for exploring the potential failure modes: A case study of a steam turbine for a nuclear power plant. *Complexity*, 2021:1–13.

[48] Ma, Z., Kvarfordt, K. J., and Wierman, T. E. (2022). Industry-average performance for components and initiating events at US commercial nuclear power plants: 2020 update. Technical report, Idaho National Lab.(INL), Idaho Falls, ID (United States).

[49] Martorell, P., Martón, I., Sánchez, A. I., Martorell, S., Sanchez-Saez, F., and Saiz, M. (2018). Evaluation of risk impact of completion time changes combining PSA and DSA model insight and human reliability analysis. *Reliability Engineering & System Safety*, 178:97–107.

[50] Murthy, D. P., Bulmer, M., and Eccleston, J. A. (2004). Weibull model selection for reliability modelling. *Reliability Engineering & System Safety*, 86(3):257–267.

[51] Nelson, P. F., Flores, A., and Francois, J. L. (2007). A design-phase PSA of a nuclear-powered hydrogen plant. *Nuclear engineering and design*, 237(3):219–229.

[52] Piterka, L., Jirickova, J., and Loveckỳ, M. (2014). Fault tree analysis of emergency core cooling system and containment spray system of WWER440/V213. In *Proceedings of the 2014 15th International Scientific Conference on Electric Power Engineering (EPE)*, pages 715–719. IEEE.

[53] Prasad, M., Vinod, G., Gaikwad, A. J., and Ramarao, A. (2017). Site core damage frequency for multi-unit nuclear power plants site. *Progress in Nuclear Energy*, 96:56–61.

[54] Rasmuson, D. M. (1992). A comparison of the small and large event tree approaches used in PRAs. *Reliability Engineering & System Safety*, 37(1):79–90.

[55] Rasmussen NC, e. a. (1975). An assessment of accident risks in US commercial nuclear power plants.

[56] Redondo-Valero, E., Queral, C., Fernandez-Cosials, K., and Sanchez-Espinoza, V. H. (2022). Analysis of MBLOCA and LBLOCA success criteria in VVER-1000/V320 reactors. new proposals for PSA level 1. *Nuclear Engineering and Technology*.

[57] Saikusa, A., Nakagawa, S., Fujimoto, N., Tachibana, Y., and Iyoku, T. (2003). Data on test results of vessel cooling system of high temperature engineering test reactor.

[58] Saito, S., Tanaka, T., and Sudo, Y. (1991). Present status of the high temperature engineering test reactor (HTTR). *Nuclear engineering and design*, 132(1):85–93.

[59] Saito, S., Tanaka, T., and Sudo, Y. (1994). Design of high temperature engineering test reactor (HTTR). Technical report, Japan Atomic Energy Research Inst.

[60] Sakaba, N., Nakagawa, S., Takamatsu, K., Takada, E., Saito, K., Furusawa, T., Tochio, D., Tachibana, Y., and Iyoku, T. (2004). Safety demonstration test (SR-2/S2C-2/SF-1) plan using the HTTR. contract research. Technical report, Japan Atomic Energy Research Inst.

[61] Sakin, R. and Ay, I. (2008). Statistical analysis of bending fatigue life data using weibull distribution in glass-fiber reinforced polyester composites. *Materials & Design*, 29(6):1170–1181.

[62] Sankar, N. R. and Prabhu, B. S. (2001). Modified approach for prioritization of failures in a system failure mode and effects analysis. *International Journal of Quality & Reliability Management*.

[63] Shi, H., Dong, Z., Xiao, N., and Huang, Q. (2021). Wind speed distributions used in wind energy assessment: a review. *Frontiers in Energy Research*, page 790.

[64] Shimazaki, Y., Homma, F., Sawahata, H., Furusawa, T., and Kondo, M. (2014). Development of the maintenance technologies for the future high-temperature gas cooled reactor (HTGR) using operating experiences acquired in high-temperature engineering test reactor (HTTR). *Journal of Nuclear Science and Technology*, 51(11-12):1413–1426.

[65] Snooke, N. and Price, C. (2012). Automated FMEA based diagnostic symptom generation. *Advanced Engineering Informatics*, 26(4):870–888.

[66] Spreafico, C., Russo, D., and Rizzi, C. (2017). A state-of-the-art review of FMEA/FMECA including patents. *Computer Science Review*, 25:19–28.

[67] Stamatis, D. H. (2003). *Failure mode and effect analysis: FMEA from theory to execution*. Quality Press.

[68] Takamatsu, K., Tochio, D., Nakagawa, S., Takada, S., Yan, X. L., Sawa, K., Sakaba, N., and Kunitomi, K. (2014). Experiments and validation analyses of HTTR on loss of forced cooling under 30% reactor power. *Journal of Nuclear Science and Technology*, 51(11-12):1427–1443.

[69] Takeda, T., Nakagawa, S., Honma, F., Takada, E., and Fujimoto, N. (2002). Safety shutdown of the high temperature engineering test reactor during loss of off-site electric power simulation test. *Journal of nuclear science and technology*, 39(9):986–995.

[70] Tang, Y., Liu, Q., Jing, J., Yang, Y., and Zou, Z. (2017). A framework for identification of maintenance significant items in reliability centered maintenance. *Energy*, 118:1295–1303.

[71] Tong, J., Zhao, J., Liu, T., and Xue, D. (2012). Development of probabilistic safety assessment with respect to the first demonstration nuclear power plant of high temperature gas cooled reactor in china. *Nuclear engineering and design*, 251:385–390.

[72] Torabi, M. and Kowal, K. (2022). Failure modes analysis of the electrical power supply for the GEMINI+ high temper-ature gas-cooled reactor. *Proceedings of the 32nd European Safety and Reliability Conference (ESREL 2022)*.

[73] Torabi, M., Lashkari, A., Masoudi, S. F., and Bagheri, S. (2018). Neutronic analysis of control rod effect on safety parameters in tehran research reactor. *Nuclear Engineering and Technology*, 50(7):1017–1023.

[74] Vesely, B. (2002). Fault tree analysis (FTA): Concepts and applications. *NASA HQ*.

[75] Vesely, W. (1992). *Approaches for age-dependent probabilistic safety assessments with emphasis on prioritization and sensitivity studies*. Citeseer.

[76] Volkanovski, A. (2012). Method for assessment of ageing based on PSA results. *Nuclear Engineering and Design*, 246:141–146.

[77] Volkanovski, A., Ballesteros Avila, A., and Peinador Veira, M. (2016). Statistical analysis of loss of offsite power events. *Science and Technology of Nuclear Installations*, 2016.

[78] Volkanovski, A., Čepin, M., and Mavko, B. (2009). Application of the fault tree analysis for assessment of power system reliability. *Reliability Engineering & System Safety*, 94(6):1116–1127.

[79] Volkanovski, A. and M, P. (2015). Station blackout and nuclear safety. *Safety and Reliability of Complex Engineered Systems*, pages 659–664.

[80] Volkanovski, A. and Peinador Veira, M. (2018). Analysis of loss of essential power system reported in nuclear power plants. *Science and Technology of Nuclear Installations*, 2018.

[81] Vrbanic, I., Simic, Z., and Basic, I. (2004). Use of PSA tools and techniques in life cycle management of maintenance and operation of complex system. In *Annual Symposium Reliability and Maintainability, 2004-RAMS*, pages 492–499. IEEE.

[82] Wang, Z. and Liu, W. (2021). Wind energy potential assessment based on wind speed, its direction and power data. *Scientific reports*, 11(1):16879.

[83] Ward, D. M. (2013). The effect of weather on grid systems and the reliability of electricity supply. *Climatic Change*, 121(1):103–113.

[84] Wellssow, W., Schick, E., Zdrallek, M., Schuëller, G., and Kafka, P. (1999). Modeling the impact of weather on the reliability of electric power systems. *Safety and Reliability, ESREL*, 99.

[85] Yang, H., Lim, J. W., Kim, H. S., Chang, D. J., and Sung, K. Y. (2008). Regulatory PSA model development for risk evaluation of kori nuclear unit 1 continued operation. In *Transactions of the Korean Nuclear Society Spring Meeting*.

[86] Yin, L., Smith, M. A., and Trivedi, K. S. (2001). Uncertainty analysis in reliability modeling. In *Annual Reliability and Maintainability Symposium. 2001 Proceedings. International Symposium on Product Quality and Integrity (Cat. No. 01CH37179)*, pages 229–234. IEEE.

[87] Zammori, F. and Gabbrielli, R. (2012). ANP/RPN: A multi criteria evaluation of the risk priority number. *Quality and Reliability Engineering International*, 28(1):85–104.

[88] Zhang, X. and Gockenbach, E. (2006). Assessment of the actual condition of the electrical components in medium-voltage networks. *IEEE Transactions on reliability*, 55(2):361–368.

[89] Zhang, X., Gockenbach, E., Wasserberg, V., and Borsi, H. (2006). Estimation of the lifetime of the electrical components in distribution networks. *IEEE Transactions on Power Delivery*, 22(1):515–522.

[90] Zhang, X., Zhang, J., and Gockenbach, E. (2009). Reliability centered asset management for medium-voltage deteriorating electrical equipment based on germany failure statistics. *IEEE Transactions on Power Systems*, 24(2):721–728.

[91] Zhao, J., Liu, T., Zhao, Y., Liu, D., Yang, X., Lin, Y., Lin, Z., and Lei, Y. (2016). Reliability evaluation of NPP's power supply system based on improved GO-FLOW method. *Science and Technology of Nuclear Installations*, 2016.