30599200R0041
Revision 1
Deliverable PD 07

NUCLEAR TECHNOLOGIES AND MATERIALS ADVANCED REACTOR CONCEPTS-20

FAST MODULAR REACTOR SAFETY APPROACH AND PROBABILISTIC RISK INSIGHTS

Sponsored by the U.S. Department of Energy
Under Contract # DE-NE0009052

Contractor: **General Atomics**
Address: **PO Box 85608**
San Diego, CA 92186-5608

DESTRUCTION NOTICE: For Unclassified, limited distribution documents, destroy by any method that will prevent disclosure of contents or reconstruction of the document.

REVISION HISTORY

Revision	Date	Description of Change
1	2024/08/21	Initial Release; ECN-116839.

POINT OF CONTACT

Title	Contact Information
Lead Author	Name: John Bolin Phone: 858-762-7576 E-mail: John.Bolin@ga.com
Contributing Author	Name: Steven Krahn Phone: 615-322-7311 E-mail: Steve.Krahn@vanderbilt.edu
Responsible Manager	Name: John Bolin Phone: 858-762-7576 E-mail: John.Bolin@ga.com
Chief Engineer	Name: Hangbok Choi Phone: 858-762-7554 E-mail: Hangbok.Choi@ga.com

TABLE OF CONTENTS

R&D Released 2024/08/21 12:31:39

R&D Released 2024/08/21 12:31:39

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

Acronym	Definition
AC	Alternating Current
ALARA	As Low As Reasonably Achievable
ANS	American Nuclear Society
AOO	Anticipated Operational Occurrence
ARC-20	Advanced Reactor Concepts-20
ARDP	Advanced Reactor Demonstration Program
ASME	American Society of Mechanical Engineers
ATWS	Anticipated Transient Without Scram
AVR	Arbeitsgemeinschaft Versuchsreaktor
CDRL	Contract Data Requirements List
CMMT	Commitment
CRA	Control Rod Assembly
DBA	Design Basis Accident
DC	Design Certification
DHR	Decay Heat Removal
DID	Defense-In-Depth
D-LOFC	Depressurized Loss of Forced Cooling
Doc.	Document
DOE	Department of Energy
EAB	Exclusion Area Boundary
EAR	Export Administration Regulations
ECN	Engineering Change Notice
EPA	Environmental Protection Agency
EPRI	Electric Power Research Institute
EPZ	Emergency Planning Zone
F-C	Frequency-Consequence
FMEA	Failure Modes and Effects Analysis
FMR	Fast Modular Reactor
FSF	Fundamental Safety Function
GA	General Atomics
GA-EMS	General Atomics Electromagnetic Systems
GCR	Gas-Cooled Reactor
GFR	Gas-cooled Fast Reactor
GT-MHR	Gas Turbine-Modular Helium Reactor
HAZOPs	Hazard and Operability Studies
HPS	Helium Purification System
HTGR	High-Temperature Gas-Cooled Reactor

R&D Released 2024/08/21 12:31:39
R&D Released 2024/08/21 12:31:39

Acronym	Definition
I&C	Instrumentation and Control
IAEA	International Atomic Energy Agency
ITAR	International Traffic in Arms Regulations
LBE	Licensing Basis Event
LB-LOCA	Large Break LOCA
LOCA	Loss of Coolant Accident
LOFA	Loss of Flow Accident
LOFW	Loss of Feedwater
LOOP	Loss of Offsite Power
LPZ	Low Population Zone
LUHS	Loss of Ultimate Heat Sink
LWR	Light Water Reactor
MBSE	Model Based Systems Engineering
MHTGR	Modular High-Temperature Gas-Cooled Reactor
MLD	Master Logic Diagram
MWe	Megawatt electric
N/A	Not Applicable
NEI	Nuclear Energy Institute
No.	Number
non-LWR	non-Light Water Reactor
NRC	Nuclear Regulatory Commission
PAG	Protective Action Guide
PCS	Power Conversion System
PCU	Power Conversion Unit
PEO (T)	Program Executive Officer (Tactical)
PHA	Process Hazard Analysis
PIE	Preliminary Initiating Event
P-LOFC	Pressurized Loss of Forced Cooling
PRA	Probabilistic Risk Assessment
QHO	Quantitative Health Objective
Rev	Revision
RHR	Residual Heat Removal
RI-PB	Risk-Informed, Performance-Based
RPS	Reactor Protection System
RSPS	Response
RVCS	Reactor Vessel Cooling System
SB-LOCA	Small Break LOCA
SBO	Station Blackout
SDA	Standard Design Approval

Acronym	Definition
SiD	Safety in Design
SSC	Structure, System, and Component
TCG	Turbine-Compressor-Generator
THTR	Thorium High Temperature Reactor
TLRC	Top-Level Regulatory Criteria
UK	United Kingdom
VHTR	Very High Temperature Reactor

1 INTRODUCTION

General Atomics (GA) Electromagnetic Systems (GA-EMS) is developing a helium-cooled Fast Modular Reactor (FMR) [Reference 1]. The project has been selected by the U.S. Department of Energy (DOE) for Advanced Reactor Concepts-20 (ARC-20) under Advanced Reactor Demonstration Program (ARDP). The long-term goal is to design, license, and commercialize the FMR plant by the mid-2030s. To achieve the goal of licensing the FMR, GA-EMS has been engaged with the Nuclear Regulatory Commission (NRC) from the initial stage of the project.

A fundamental aspect of the licensing process is the development of a comprehensive licensing basis. This entails creating a collection of documents and technical criteria that will serve as the foundation upon which the NRC will grant a license for a Standard Design Approval (SDA) or a Design Certification (DC) that will lead to the construction and operation of the nuclear facility. The NRC requires reactor designs to be evaluated based on several different kinds of events that are considered part of the licensing basis. Licensing basis events (LBEs) are certain event sequences that are chosen to be considered in the design of a nuclear power plant. These LBEs rely on plant structures, systems, and components (SSCs) to perform various safety functions. These SSCs are classified based on their safety and risk significance. As an effort to support the FMR pre-application regulatory engagement plan, GA-EMS has developed a safety approach for the FMR that uses inherent and passive safety along with probabilistic risk insights to satisfy safety and environmental protection requirements.

The licensing basis for the FMR design follows guidance developed by the Nuclear Energy Institute (NEI) and provided in NEI 18-04 [Reference 2]. This guidance provides an integrated and highly interdependent methodology for identifying and evaluating licensing basis events, classifying, and establishing performance criteria for SSCs, and evaluating defense-in-depth (DID) for advanced reactor designs.

The following are included in this report:

- Safety objectives
- Inherent and passive safety features
- Radionuclide release barriers
- Functional safety approach
- Risk-informed safety approach
- Probabilistic risk insights
- Summary and conclusions

R&D Released 2024/08/21 12:31:39

2 DESIGN FEATURES OF GA-EMS FMR

The FMR is a gas-cooled fast reactor (GFR), operating at system temperature range of 506 °C to 824 °C. It is a grid-capable power source with a gross electric output of ~44 MW. The reactor core uses helium coolant and uranium dioxide (UO_2) fuel pellets encapsulated in a silicon carbide (SiC) composite cladding, arranged in a triangular pitch, and forming a hexagonal fuel assembly.

The reactor core is an annular shape surrounded by solid reflector blocks of zirconium silicide (Zr_3Si_2) and graphite that preserve neutrons and enhance heat transfer. Zr3Si2 is a heavy reflector specifically developed for the GFR. This material is favorable in fast reactors to avoid power peaking around the core periphery from neutron thermalization.

Helium is chemically inert and will not aggravate an accident by contributing to any chemical or nuclear reaction. The use of helium as the coolant in combination with conventional fuel and effective neutron reflector offered enhanced neutronic and thermal efficiencies and several advanced safety characteristics such as efficient fuel utilization, high temperature operation, and inherently safe design that minimize the likelihood of accidents. For example, the helium coolant is intrinsically safe for it does not react with other materials or burn in air. The major systems and components are underground as illustrated in Figure 1.

The Power Conversion System (PCS) is a crucial component of the FMR power plant that converts the thermal energy generated by the reactor into electricity. The concept of the FMR PCS is similar to that for the gas turbine-modular helium reactor (GT-MHR). GA-EMS will develop the PCS of the FMR based on the previous experiences with the conceptual design of power conversion unit (PCU), leveraging the latest advancements in power conversion technology to optimize the efficiency and reliability of the PCS (i.e., PCU + generator system). The turbine-compressor-generator (TCG) are mounted on an inline vertical configuration. The generator is in a separate, connected vessel at the top of the PCU.

The Maintenance Cooling System (MCS) is primarily used to cool the reactor core during maintenance outages particularly when the PCS is unavailable for maintenance. During accidents in which the PCS is disabled, the MCS can also remove residual heat after reactor shutdown.

R&D Released 2024/08/21 12:31:39
R&D Released 2024/08/21 12:31:39
R&D Released 2024/08/21 12:31:39

1. Reactor vessel
2. Reactor vessel cooling panel
3. Power conversion unit
4. Generator
5. Circulator
6. Maintenance cooling system
7. Steel containment
8. Concrete
9. Maintenance caps
10. Main control room
11. Water tank
12. Spent fuel storage
13. Fueling machine
14. Reactor building
15. Ground level

Figure 1. FMR Nuclear Island Components

One of the advanced design features of the FMR is its ability to passively remove decay heat from the core and vessel, regardless of whether helium is present. This is achieved through the implementation of a gravity-driven reactor vessel cooling system (RVCS). RVCS is always in operation [Reference 3] and continues passively removing the heat from the reactor vessel by natural circulation of water circulating in the RVCS loop. Unlike traditional gas-cooled reactors, which are typically packed with solid graphite, the FMR does not rely on conduction-cooldown. Instead, the passive safety of the core is primarily enhanced by the radiation heat transfer mechanism. For a rodded core like the FMR, the radiation heat transfer is the dominant heat transfer mechanism from the fuel rods to the surrounding solid structures, rather than conduction or convection.

Other design features, such as the large thermal margin, low power density, and annular core configuration, further enhance the passive safety of the core. Heat from the reactor vessel is transferred to the cooling panel of the RVCS through radiation. This system ensures that any decay heat generated by the core can be safely and efficiently removed, without the need for active cooling systems or other complex mechanisms. As a result, the FMR is able to offer exceptional levels of safety and reliability, making it an attractive option and a significant advancement in nuclear power generation technology.

3 SAFETY OBJECTIVES

The primary safety objective of the FMR is to limit the dose from accidental releases so that regulatory requirements for protection of the health and safety of the public are met at an exclusion area boundary (EAB) that is no more than a few hundred meters – 300 - 500 m – from the reactor. To eliminate the need for public evacuation or sheltering beyond the site boundary, the FMR design goal is to meet the Environmental Protection Agency (EPA) plume exposure Protective Action Guide (PAG) at the EAB [Reference 4].

LBE selection, safety classification of SSCs, and DID adequacy are parts of a systematic and reproducible process for establishing the licensing basis defined in NEI 18-04 [Reference 2]. The frequency-consequence evaluation criteria, hereafter referred to as the frequency-consequence (F-C) Target, is shown in Figure 2 and is key to informing LBE selection, SSC classification, and DID adequacy. Top-level regulatory criteria (TLRC) are defined that establish the limits on consequences shown in the F-C Target. The TLRC are based on the following objectives:

1) Provide direct public health and safety acceptability limits in terms of individual consequences
2) Be technology-inclusive and independent of site
3) Provide well-defined, quantifiable risk criteria

The following primary sources have been identified as containing criteria that establish limits on the risk or consequences of potential radiological releases from nuclear power plants in the U.S.

- Reactor Safety Goal Policy Statement (51 FR 28044) [Reference 5] - On August 4, 1986, the NRC adopted a safety goal policy for the operation of nuclear power reactors. The objective of this policy is to establish goals that broadly define an acceptable level of radiological risk. Two qualitative safety goals supported by two quantitative health objectives (QHOs) were established. These two supporting objectives are based on the principle that nuclear risks should not be a significant addition to other societal risks.

This policy limits public safety risk resulting from nuclear power plant operation. Limits are stated in the form of the maximum allowable risk of immediate death and the risk of delayed mortality from exposure to radiological releases of all types from nuclear power plants.

- 10 CFR Part 20, Standards for Protection against Radiation (Subpart C, Occupational Dose Limits) - The regulations promulgated under 10 CFR Part 20 establish standards for protection against ionizing radiation resulting from activities conducted under licenses issued by the NRC. Event sequences expected to occur within the plant lifetime, considering multiple reactor modules, are classified as Anticipated Operational Occurrences (AOOs). AOOs are evaluated against the dose limits of 10 CFR Part 20.

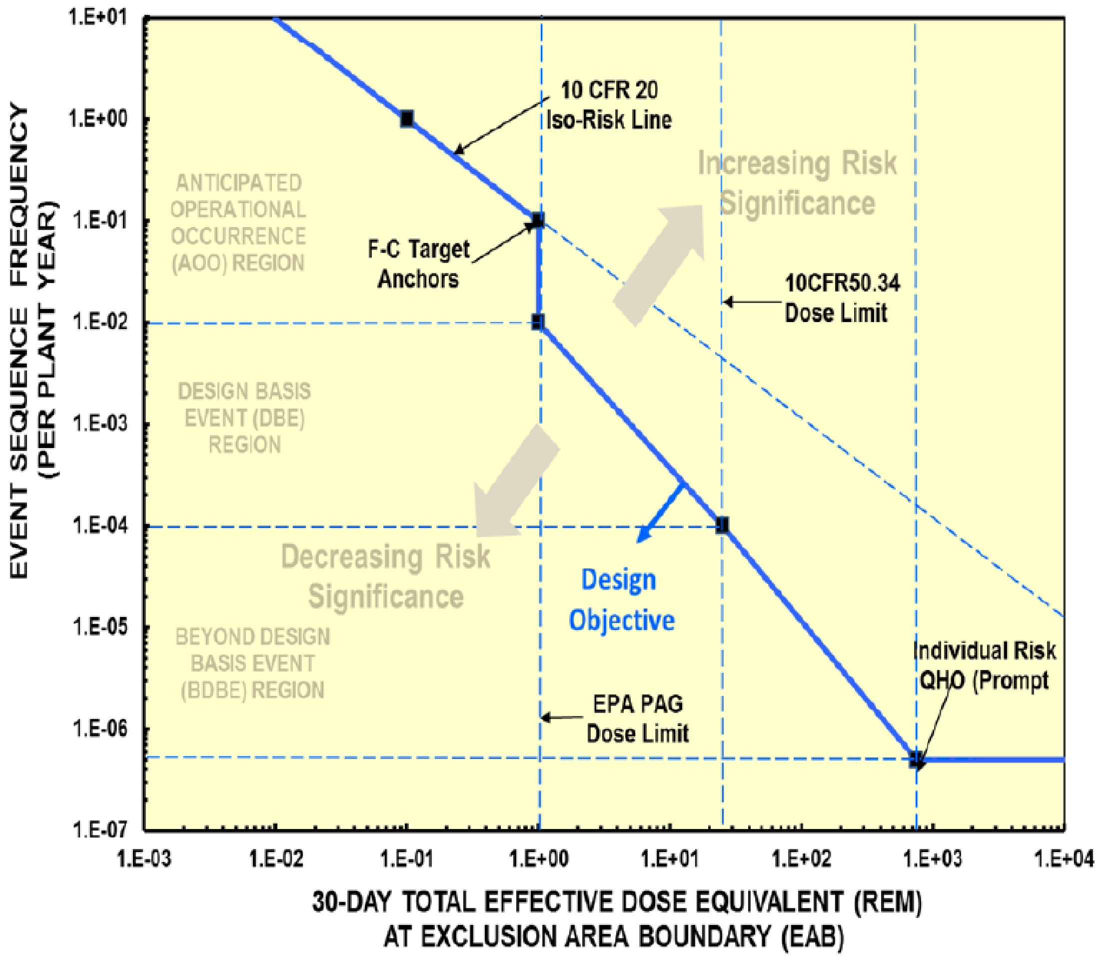


Figure 2. Frequency-Consequence Target

- 10 CFR Part 20, Standards for Protection against Radiation (Subpart D, Radiation Dose Limits for Individual Members of the Public) - These criteria (§20.1301) limit the dose consequences of releases associated with relatively high frequency events that occur as part of normal plant operations.
- 10 CFR Part 50 Appendix I, Numerical Guides for Design Objectives and Limiting Conditions for Operation to Meet the Criterion “As Low As Reasonably Achievable” (ALARA) for Radioactive Material in Light-Water-Cooled Nuclear Power Reactor Effluents - This appendix provides explicit limits on doses from planned discharges that meet the NRC’s definition of ALARA.
- 10 CFR Part 52 Subpart C, Combined Licenses - Under the provisions of 10 CFR §52.79, an application for a combined license must include the principal design criteria for a proposed facility. The principal design criteria establish the necessary design, fabrication, construction, testing, and performance requirements for SSCs important to safety. This provides reasonable assurance that the facility can be operated without undue risk to the health and safety of the public.

R&D Released 2024/08/21 12:31:39

R&D Released 2024/08/21 12:31:39

- 40 CFR Part 190, Environmental Radiation Protection Standards for Nuclear Power Operations - These standards provide the generally applicable exposure limits for members of the general public from all operations except transportation and disposal or storage of spent fuel associated with the generation of electrical power by nuclear power plants.
- 10 CFR Part 100, Reactor Site Criteria (Subpart B, Evaluation Factors for Stationary Power Reactor Site Applications on or After January 10, 1997) - §100.20 defines the EAB and Low Population Zone (LPZ) of a nuclear reactor site and requires that the combination of the site and reactor located on that site be capable of meeting the dose and dose rate limits set forth in 10 CFR §50.34(a).
- 10 CFR §50.34(a)(1)(ii)(D), Contents of Applications, Technical Information - This section of the regulation specifies dose limits for evaluating the acceptance of the engineered safety features that are intended to mitigate the radiological consequences of accidents. These dose limits are consistent with those utilized in 10 CFR Part 100 for determining the extent of the EAB and Emergency Planning Zone (EPZ).

4 INHERENT AND PASSIVE SAFETY FEATURES

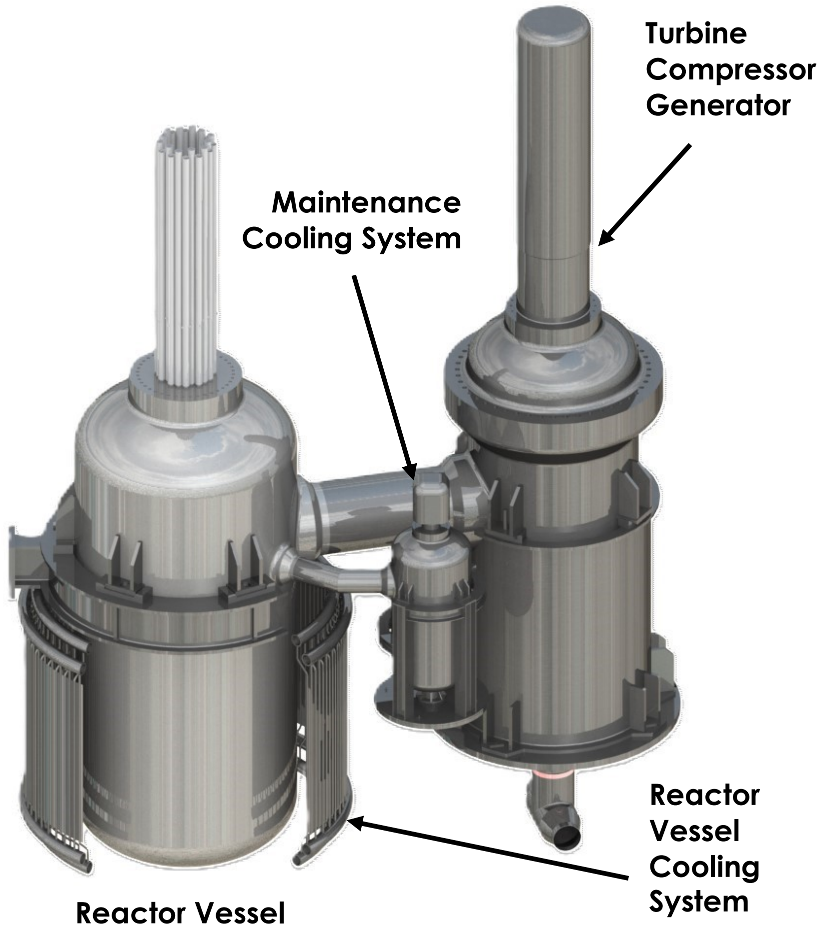
To achieve the safety objectives, the FMR relies on inherent and passive safety features. These safety features balance both accident prevention and accident mitigation.

The helium coolant of the FMR is an inert, single-phase, non-reactive and non-activating gas. It has negligible reactivity effects during a loss of coolant accident (LOCA) and has a high thermal conductivity. Helium is also non-corrosive, non-toxic and optically transparent. Prior to refueling, the helium coolant is purified and stored for reuse after the refueling outage is completed.

The reactor system has a compact annular core surrounded by an advanced fast neutron reflector composed of zirconium silicide (Zr_3Si_2). A graphite reflector surrounds the Zr_3Si_2 reflector. The low core power density and use of UO_2 fuel and SiC composite (SiGA®) cladding provides both heat capacity and thermal safety margin for the fuel system.

The negative reactivity temperature coefficient of the fuel is another inherent safety feature of the FMR. The gravity-driven and diverse reactivity control systems provide further confidence in the ability to shut down the reactor. A three-batch refueling scheme is used to enhance higher fuel utilization and reduce excess reactivity control. The average linear power of the FMR fuel rod is ~2.3 kW/m, which is much lower than that of a typical light water reactor (~19 kW/m) [Reference 6].

During plant transients, heat can be removed from the reactor core in four modes as depicted in Figure 3. For normal shutdowns, the motor-generator is used in conjunction with the grid to cool the reactor as reactor power is reduced by control rod insertion. If offsite grid power is lost, then the reactor, turbomachine, and generator are quickly reduced to maintain internal house loads within the FMR plant. If the plant failure removes the ability of the generator to make or use electricity, then backup generators can supply electricity to the MCS to remove residual heat after reactor shutdown.



Normal cooldown	• Controlled shutdown • Transition from generator to motor to maintain cooling with grid power
Loss of offsite power	• Reactor/turbine power reduced to house loads until grid restored
Loss of offsite power and turbine trip	• Reactor trip • Power from backup generators • Core cooling by MCS
Station blackout	• Reactor trip • Radiative and convective heat transfer to RVCS
Normal cooldown	• Controlled shutdown • Transition from generator to motor to maintain cooling with grid power

Figure 3. Modes of Heat Removal

The ultimate safety-related means to remove residual heat is the RVCS. The annular core arrangement is an inherent design feature that promotes radiative heat transfer from the reactor core, conduction heat transfer through the reflectors to the reactor vessel, and radiation heat transfer from the reactor vessel to the RVCS panels. Passive heat removal in the RVCS is by buoyancy-driven flow of water. The system has two completely redundant trains that are supplied by two actively cooled water tanks. Active cooling of the water tank is not required to passively remove heat during design basis accidents (DBAs). During a station blackout (SBO), a single RVCS train relying on water boil-off from the tank can remove residual heat from the reactor vessel and keep peak fuel temperature below accident design limits.

No AC powered safety-related systems and no operator actions are required to respond to any of the accident scenarios that have been postulated for the FMR.

5 RADIONUCLIDE RELEASE BARRIERS

The four barriers to radionuclide release that form a DID containment system for FMR are as follows:

1) High-density uranium dioxide fuel pellet
2) SIGA® cladding
3) Reactor helium pressure boundary
4) Leak-tight steel containment

The effectiveness of these barriers in containing radionuclides depends upon a number of factors including the chemistry and half-lives of the various radionuclides, service conditions, and irradiation effects. The effectiveness of these release barriers is also event specific.

5.1 High-Density Uranium Dioxide Fuel Pellet

The FMR uses the same high-density uranium dioxide fuel pellets that are used in light water reactors (LWRs) but with a higher enrichment. The maximum ^{235}U enrichment used in the FMR is 19.75 wt.%. The uranium dioxide is in a sintered pellet form with a density of 10.42 gm/cm^3, which is 95% of theoretical density.

The lower power density in FMR fuel pellets compared to LWR fuel offsets the higher coolant and cladding temperature of the FMR. Based on the baseline design of the FMR, the fuel will experience irradiation conditions more similar to typical LWR fuel. The maximum fuel temperature is approximately 1200 C. The fuel temperature of the FMR is lower than the typical maximum fuel temperature of LWR UO_2 fuel. High temperature activated fuel performance phenomena usually observed in fast reactor oxide fuel, such as central void and columnar grains formation, are not expected in the FMR fuel [Reference 7].

R&D Released 2024/08/21 12:31:39

The fuel pellet in FMR, as in LWRs, is effective in retaining non-volatile fission products like cesium and strontium particularly since the FMR peak fuel temperature is lower the typical LWR fuel. Volatile fission gas release peaks after 30 years of exposure due to high temperature and burnup. During the last 15 years of fuel lifetime, power density and fuel temperatures are lower such that fission gas release fraction decreases slightly. Depending on the fission gas release model, end-of-life fission gas release ranges between 14% to 30% [Reference 7].

5.2 SIGA® Cladding

The SiC composite SiGA® cladding enables high-temperature operation to supply 800°C helium to the turbomachine for high thermal efficiency. The SiC of the SiGA® cladding has high fast neutron irradiation tolerance which enables high-burnup operation and results in a long fuel lifetime. The SiC composite maintains its mechanical strength up to 1800ºC which is set as the design limit for FMR analysis. The multi-layer SiC composite cladding can withstand high hoop stress. During refueling when the FMR is depressurized, the hoop stress for the composite SiC layer enters the tensile domain. The maximum tensile hoop stress remains lower than 40 MPa, which is far below the proportional limit strength of 150 MPa [Reference 7]. Because the SiC composite is ceramic, the hoop strain design limit is 0.62% beyond which the impermeability of the SiC composite would be compromised. Throughout the fuel lifetime, no pellet-cladding contact was predicted. Therefore, the cladding is free from “hard” contact with the ceramic fuel. The major source of cladding hoop stress is from the pressure difference between the plenum and coolant. SiC is also used for the fuel assembly structure so that structural integrity and coolability of the reactor core are maintained during a LOCA and SBO event.

5.3 Reactor Helium Pressure Boundary

Any fission products or activation products released to the primary coolant are contained within the reactor helium pressure boundary. Reactor helium quality is controlled by the Helium Purification System (HPS) which periodically removes a portion of the primary coolant for purification. Although the primary purpose of the HPS is to control chemical impurities in the helium, the HPS efficiently removes both gaseous and metallic fission products from the helium.

For the condensable fission products, the dominant removal mechanism is deposition (“plateout”) on the various helium-wetted surfaces in the primary circuit (i.e., the plateout rate far exceeds the purification rate). The plateout rate is determined by the mass transfer rates from the coolant to the fixed surfaces, by the sorptivities of the various materials of construction for the condensable fission products, and by the temperature of the surfaces. The recuperator, precooler and intercooler provide effective plateout surfaces due to their large surface area and low temperature.

R&D Released 2024/08/21 12:31:39
R&D Released 2024/08/21 12:31:39

Condensable fission products may also be transported throughout the primary circuit sorbed onto particulates ("dust") which may be present. The distribution of these contaminated particulates is noticeably different from the distribution of radionuclides transported as atomic species. Contaminated particulates settle in areas with low convective forces where gravitational settling can trap them.

The circulating, dust, and plateout activities in the primary circuit are potential sources of release to the environment in the event of pressure boundary leaks or as a result of venting of helium in response to over-pressurization of the primary circuit. The fraction of the circulating activity lost during such events is essentially the same as the fraction of the helium that is released. The radionuclide release can be mitigated by pump down through the HPS if the leak rate is sufficiently slow.

A small fraction of the plateout near the leak location may also be re-entrained, or "lifted off" and a small fraction of the contaminated dust may by resuspended if the rate of depressurization is sufficiently rapid. The amount of fission product liftoff is expected to be influenced by the amount of dust in the primary circuit as well as the presence of friable surface films on primary circuit components which could possible spall off during a rapid depressurization.

Another mechanism that can potentially remove and subsequently release primary circuit plateout activity is "washoff". The cause of radionuclide release is water that has entered the primary circuit. In principle, both water vapor and liquid water could partially remove plateout activity. The primary sources of water ingress are the precooler, intercooler, and MCS heat exchanger. Even if a fraction of the plateout activity were removed from fixed surfaces, there would only be an environmental release in the case of venting of helium/water from the primary circuit. Due to the low temperature and pressure of the potential water sources, the pressure relief valve does not lift. Moreover, the radiologically important nuclides, such as iodine and cesium, are expected to remain preferentially in the liquid water that remains inside the primary circuit.

5.4 Leak-Tight Steel Containment

The containment is the final barrier to the transport and release of radionuclides to the environment. Typically, a vented low-pressure reactor building is the baseline design for both prismatic and pebble bed modular high-temperature gas-cooled reactors (MHTGRs). In order to expedite licensing, public acceptance, and siting flexibility, a leak-tight steel containment was designed for the FMR.

During a leak or break in the reactor helium pressure boundary, containment isolation will occur on detection of either high containment pressure, high containment radiation, or low primary coolant pressure. After successful containment isolation, natural radionuclide removal mechanisms occur in the containment including condensation, settling, and plateout. No active means of radionuclide removal are necessary to meet the FMR safety objectives.

The transport behavior of radionuclides during depressurized loss of forced cooling (D-LOFC) accidents is much simpler than the LOCAs in LWRs. Relatively few radionuclides (primarily radioisotopes of Kr, Xe, I, Te, Ag, Cs, and Sr) are released from the core. No heavy metals or core structural materials are released, and the radionuclide mass concentrations are so low that aerosol agglomeration is minimal. Dust present in the primary circuit during normal operation and liftoff of plateout may add to the activity released from the primary circuit, but the chemical and physical nature of this material is quite different from an LWR corium aerosol.

6 FUNCTIONAL AND RISK-INFORMED SAFETY APPROACH

The safety case of the FMR system is being developed by using the Safety-in-Design (SiD) methodology [Reference 8], which supports a flexible, fit-for-purpose incorporation of safety analysis into the design process that is commensurate with the technological maturity of the design. The SiD methodology was developed to support integration of early-stage safety assessment of advanced reactor concepts using industry-standard tools and practices.

SiD is intended to support the incremental development of the safety case for advanced reactor designs, which feature combinations of fuels, coolants, moderators, and heat transfer system designs that deviate from LWRs, by:

1) Providing earlier identification of safety-related research and development needs in time to facilitate efficient design iteration and improvement.
2) Incremental development of quantitative safety analyses in support of an eventual probabilistic risk assessment (PRA).
3) Promoting effective early-stage regulatory engagement.

The framework of the SiD methodology, shown below in Figure 4, illustrates how SiD can be used over the duration of the reactor design process, assuming that the design would ultimately require the development a PRA. Figure 4 demonstrates how the individual steps of the SiD process can be used as “building blocks” for an eventual PRA – even during design efforts that are not yet at the level of fidelity required to support quantitative risk assessment.

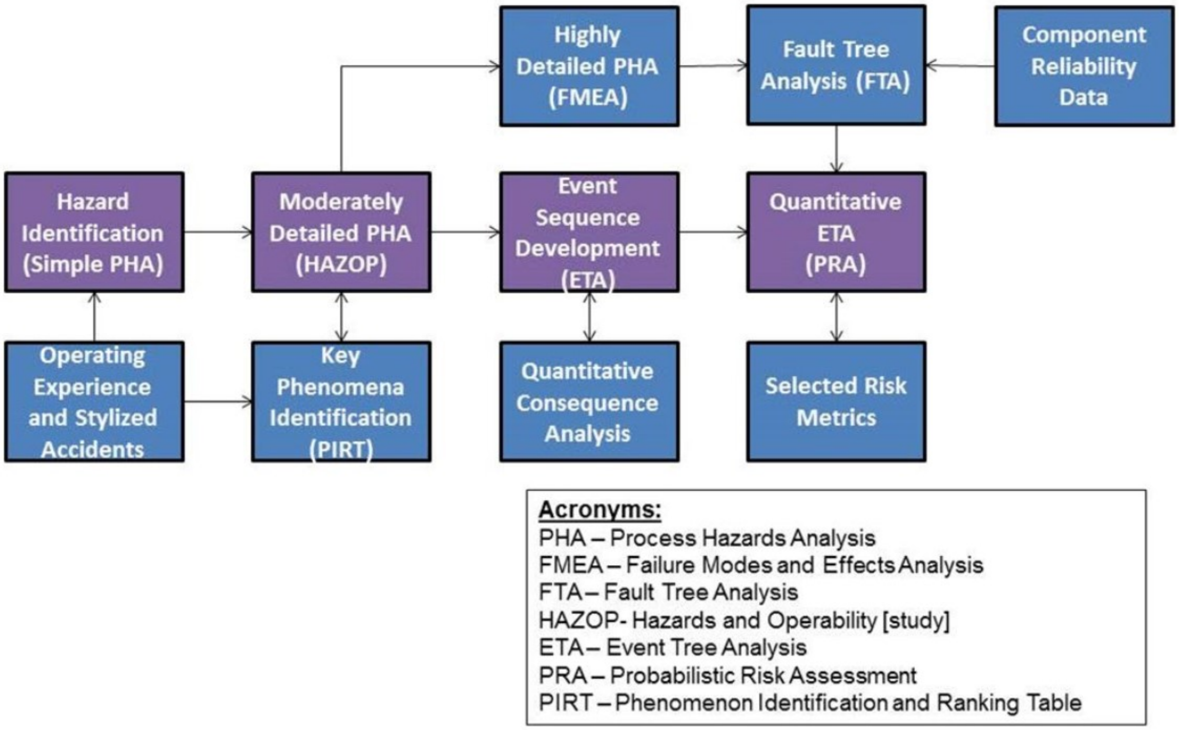


Figure 4. Overview of Processes Associated with SiD Methodology [Reference 8]

The principles of SiD methodology are consistent with guidance published in relevant regulatory documents such as NEI 18-04 [Reference 2] and its subsequent endorsement from the NRC in Reg. Guide 1.233 [Reference 9]. For example, when determining the initial events to be considered as LBEs, NEI 18-04 states that the initial event selection "*can be supported by analysis techniques such as failure modes and effects analyses (FMEAs), hazard and operability studies (HAZOPs), and master logic diagrams (MLDs)*".

Furthermore, NEI 18-04 goes on to state that "*Prior to the first introduction of the PRA, it is necessary to develop a technically sound understanding of the potential failure modes of the reactor concept, how the plant would respond to such failure modes, and how protective strategies can be incorporated into formulating the safety design approach. The incorporation of safety analysis methods appropriate to early stages of design, such as FMEA and process hazard analysis (PHA), provide early-stage evaluations that are systematic, reproducible, and as complete as the current stage of design permits*".

R&D Released 2024/08/21 12:31:39
R&D Released 2024/08/21 12:31:39

While certain safety analysis methods have been explicitly recognized in NEI 18-04 as being valuable to include during the design process, there is no formal guidance on *how* the methods should be applied. Further complicating the matter is the fact that no GFR has been constructed or operated, thus requiring an adaptable approach that can provide safety-related insights while not being reliant on detailed design information. To that end, a three-phased approach – guided by the SiD method – was developed to support the preliminary safety case evaluation of the FMR concept. The phases of the functional safety approach are summarized below:

1) **Phase I:** Performance of a literature review of preliminary initiating events (PIEs) found within high temperature gas reactor (HTGR), very high temperature reactor (VHTR), and GFR references, including a screening for relevancy to the FMR,
2) **Phase II:** Performance of an FMEA that supports evaluation of the present iteration of the FMR design, and
3) **Phase III:** Development of an MLD for a later-stage iteration of the FMR design, documented using model-based systems engineering (MBSE) and SysML.

Each of these respective phases in the preliminary safety case are discussed in more detail in the following sections. The MLD is foundational to event sequence development. Reliability data, fault tree analysis, and event tree quantification are the final steps in developing a PRA to risk-inform LBE selection, SSC safety classification, and DID adequacy as described in NEI 18-04 [Reference 2].

6.1 Comprehensive Identification of Initiating Events

Given the novelty of the FMR design concept, and the lack of operating experience with other similar technologies, the first phase of the SiD approach for the FMR has included an exhaustive identification of preliminary initiating events (PIEs)[1] to a provide a comprehensive understanding of the range of PIEs relevant to the FMR design. Recent NRC guidance

[1] An initiating event is an event originating from an internal or external hazard that both challenges normal plant operation and requires successful mitigation [Reference 10]. The label of 'preliminary' was applied in the current context to reflect the initial nature of the initiating event characterization for the FMR concept.

R&D Released 2024/08/21 12:31:39

R&D Released 2024/08/21 12:31:39

[References 11 and 12] has re-emphasized the importance of performing such a systematic search, stating that "*identification of initiating events is the starting point for the safety assessment of nuclear power plants*" and that a determination of a comprehensive set of PIEs is "*crucial in determining what events could propagate to undesirable consequences… and overall plant risk*". To that end, a literature review was performed to characterize PIEs previously analyzed for other GFR designs, HTGRs, VHTRs and the fleet of gas-cooled reactors (GCRs) operated in the United Kingdom (UK).

The initial literature review revealed that several of the PIEs identified from the non-GFR technologies evaluated were found to be relevant to the FMR, and that several insights could be gleaned from these PIEs that are potentially valuable to the emerging safety case development of the FMR. The most frequently assessed PIEs were LOCAs and loss of flow accidents (LOFAs), which are analogous to D-LOFC and P-LOFC events, respectively. Repeated mention of these accident-types emphasizes the importance of maintaining constant system pressurization due to potential depressurized events leading to more severe downstream effects in several designs. Conversely, less emphasis to-date was observed on the assessment of initiating events and failures within auxiliary systems (e.g., HPSs) and novel safety systems (e.g., passive decay heat removal systems) required for GFR operation. Assessing such systems may well play an important role in the development of the GFR safety case and, therefore, warrant additional consideration in future safety analyses.

6.2 Failure Modes and Effects Analysis

To further expand upon the PIEs, and to identify additional PIEs not included in the initial literature review, several systematic safety analysis technique(s) were considered to develop a more detailed understanding of the events specific to the FMR design and its subsystems. The evaluated techniques included HAZOP, FMEA, and MLD. The selection of the appropriate PHA technique is dependent upon the design stage of the evaluated system and the availability of design-related information – which is used to support the analysis. Using the insights derived from the Phase I PIE literature review, it was determined that performance of a FMEA was appropriate for the second phase of the safety assessment approach.

FMEAs are performed by examining each individual component or subsystem, one at a time, and then listing all credible failure modes associated with the equipment type and operating conditions [Reference 13]. Once the failure modes for a specific component are identified, the effects of the failure on the system are recorded. Additionally, safety systems that mitigate the likelihood or consequence of the effects on the systems can be designated to each identified failure mode to provide an initial understanding of the system's ability to address the postulated failure modes.

FMEAs often include evaluation of equipment failures, but they can also access systems in terms of their ability to perform various system functions. Regardless of the approach taken for

R&D Released 2024/08/21 12:31:39

the FMEA, the analysis proceeds systematically until all the credible failure modes for each component or function of the system has been considered and the results have been recorded [Reference 14]. In the context of the SiD methodology, FMEAs can be used to supplement the identification of PIEs in the form of specific failure modes in the design that can lead to an undesired consequence.

6.3 Master Logic Diagram

A frequently utilized technique that can be used to facilitate the identification and organization of PIEs is the MLD approach [Reference 15]. MLD can be used to determine elementary failures (or combinations of elementary failures) that could challenge the success of system barriers, and it is visually similar to a fault tree. However, MLDs are typically comprised of qualitative information and are therefore less rigorously structured compared to a full-scale fault tree. In particular, MLDs are organized hierarchically, with the overall event of interest specified at the highest level and more simple contributing events comprising the lower levels. Consequently, MLDs are a type of deductive analyses that can be combined with inductive analyses (such as FMEA) to ensure completeness of PIE identification.

7 PROBABILISTIC RISK INSIGHTS

7.1 Identification of PIEs Relevant to the FMR

A comprehensive and systematic identification of initiating events from documented operating experience and stylized accidents from similar concepts was determined to be the appropriate early-stage SiD approach to identify potentially relevant PIEs for the FMR design concept. The method used to perform the review of potentially relevant GFR PIEs was broken into three distinct elements:

1) Collecting/organizing initiating events from relevant literature.
2) Screening initiating events firstly for general relevancy to GFRs and subsequently to the FMR concept specifically.
3) Analysis of the remaining relevant PIEs in relation to the FMR design.

The first step in the review was to identify relevant literature containing initiating events that could be applicable to the FMR design, which was done using keyword searches in relevant databases – primarily Google Scholar due to its expansive literature coverage (e.g., conference papers, government reports, etc. in addition to peer-reviewed journal articles). Within the literature, these events are generally referred to as "initiating events." However, as initiating events from the literature were extracted and recorded, using Microsoft Excel spreadsheets, the term "PIE" was adopted to describe each event, since, as described below, their relevance to GFRs and the FMR is preliminary – requiring further evaluation at the time of the literature review and likely continued evaluation as the concept and FMR design mature. PIEs from similar, albeit more mature, gas-cooled reactor concepts, including HTGRs, VHTRs, and UK GCRs were also included in the literature review.

R&D Released 2024/08/21 12:31:39

R&D Released 2024/08/21 12:31:39

R&D Released 2024/08/21 12:31:39

It should be noted, however, that these concepts operate at different temperature ranges, with different neutron spectra, and, in the case of the UK GCRs, a different coolant (CO_2) than GFRs; the foregoing suggests that design differences between these concepts should be considered when assessing PIEs for use within GFR and FMR safety analyses. The PIEs were organized in a manner that retained the author and title of the originating document, the reactor concept, and specific design. Any relevant additional information associated with the PIE that was provided within the originating document, such as event frequency, event categorization, event/accident severity, operating parameters, etc., was also captured. The analysis of the PIEs identified in the open literature also included several sub-analyses:

1) Determination of whether the phenomena involved within each PIE were relevant to GFRs
2) Determination of whether the subsystems/components specified within each PIE were relevant to GFRs and the FMR specifically
3) Removal of repeated PIEs

In total, 124 references were evaluated, with 106 references yielding initiating event information for further consideration. The references reviewed included several test reactors and conceptual designs – many of which had previously identified and analyzed event/accident scenarios to support safety case development for the respective design. Other references included safety analyses conducted for power-producing plants, including Fort. St. Vrain and CO_2-cooled reactors operated in the UK. It should be noted that several references were identified and reviewed for additional gas-cooled reactor concepts, including the Peach Bottom Unit I HTGR, and the German Arbeitsgemeinschaft Versuchsreaktor (AVR) and Thorium High Temperature Reactor (THTR) designs. However, these sources, amongst others reviewed, contained limited documentation related to safety/accident analysis available in the public domain. Consequently, these designs were not able to be reviewed in detail and may represent additional sources of initiating event data that were not reflected in the literature review.

Once the PIEs were isolated and recorded from the data sources, they were categorized based on their functional descriptions. Unless otherwise specified, the category description for each of the PIEs were based on the descriptions found within NUREG-2122 [Reference 10]. Although the scope of the glossary is tailored toward terms used in LWR PRAs, many of the terms can also be applied to the current literature review, since they feature similar high-level plant characteristics. Descriptions of each of the PIE categories for the FMR concept are provided below in Table 1.

Table 1. PIE Category Descriptions for the FMR Concept

PIE Category	Description
Large-Break Loss of Coolant Accident (LB-LOCA)	Large-diameter (e.g., > 10 in.) breaks/leaks/ruptures within reactor coolant systems that have the potential to impact reactor heat removal and containment of radionuclides

R&D Released 2024/08/21 12:31:39

PIE Category	Description
Small-Break Loss of Coolant Accident (SB-LOCA)	Small-diameter (e.g., < 10 in.) breaks/leaks/ruptures within reactor coolant systems that have the potential to impact reactor heat removal and containment of radionuclides
Loss of Coolant Accident – Break Size not Specified (LOCA)	Breaks/leaks/ruptures (size not specified) within reactor coolant systems that have the potential to impact reactor heat removal and containment of radionuclides
Aggravating Event	Although not specifically PIEs, these can represent important phenomena or success/failure pathways in accident progression that may require modeling within a future safety assessment
Reactivity Transient/Control Rod Assembly (CRA) Withdrawal	Removal or lack of insertion of control rods into the core, which have the potential to challenge the fundamental safety function of reactivity control
Flow-Related Transient	Coolant flow within the reactor increases or decreases by some means, but coolant mass is not "lost" as in a LOCA
Loss of Ultimate Heat Sink (LUHS)	Loss of the heat removal capacity by the heat sink
Loss of Offsite Power (LOOP)	Loss of non-emergency Alternating Current (AC) power assumed to result in the loss of all power of the plant, except diesel generators
Station Blackout (SBO)	Loss of all offsite and onsite AC power concurrent with a turbine trip
Anticipated Transient Without Scram (ATWS)	Those events that require a plant trip and challenge safety systems but are followed by failure of control rod insertion to terminate the fission process
Loss of Feedwater (LOFW)	Those events that result in the partial or complete loss of feedwater flow through the secondary circuit
Turbine/Reactor Trip	Inadvertent shutdown or rundown of the turbine generator or the reactor that has the potential to challenge reactor heat removal capacity
External Event	Those events that originate outside the plant that directly or indirectly cause initiating events that can challenge fundamental plant safety functions
Human Error	Those events that involve any human action, including inaction, which exceeds some limit of acceptability, excluding malevolent behavior
Treatment System Event	Those events that result in failures within the helium treatment/purification and/or radioactive waste management systems
Uncategorized Transient	Those PIEs that were not able to be appropriately categorized under any of the other categories (typically due to a lack of specificity in the event analyzed within the literature)

R&D Released 2024/08/21 12:31:39

R&D Released 2024/08/21 12:31:39

Across the 106 PIE-containing data sources evaluated for various gas-cooled reactor concepts, a total of 932 PIEs were identified. Many of the PIEs recorded across the various references analyzed the same type of event; because of this, duplicate events were screened to yield 549 PIEs describing unique events. For example, a commonly analyzed initiating event in the literature was the D-LOFC event. Some of the recorded events of this type solely analyzed the effects of the D-LOFC, whereas others analyzed the effects of the D-LOFC in conjunction with failures of other systems, such as a residual heat removal system. Such PIEs were retained as "unique" for the purposes of this work due to their unique combinations of events and/or analysis parameters. Distributions of unique PIEs within each of the categories for the concepts reviewed are summarized in Figure 5, Figure 6, Figure 7, and Figure 8.

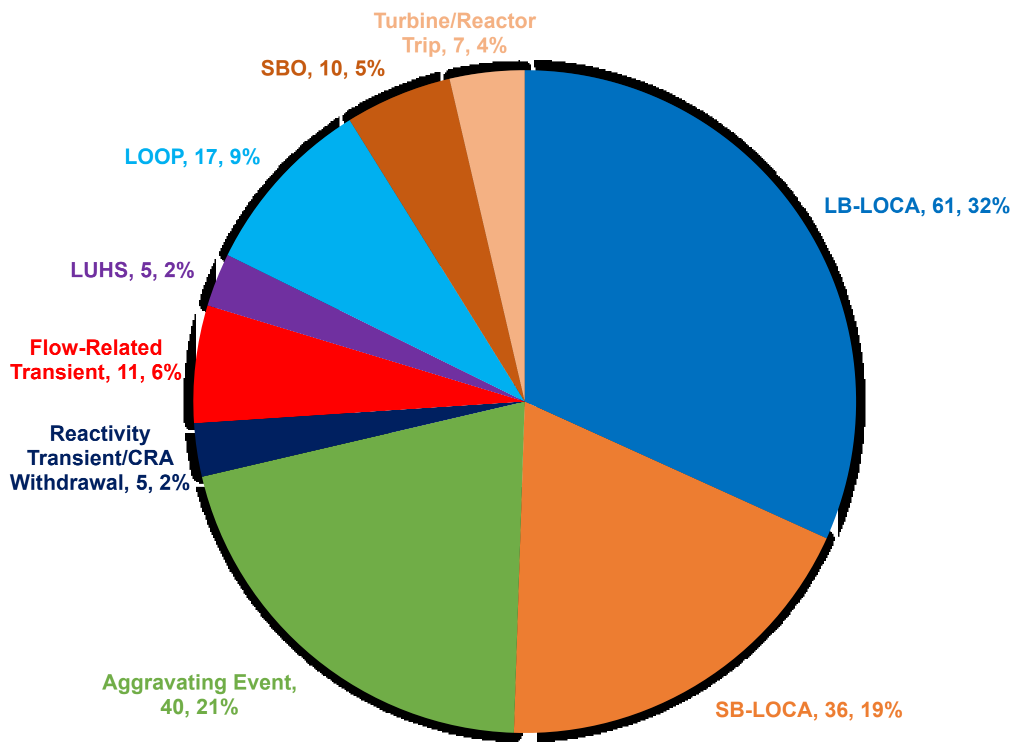


Figure 5. GFR PIE Distribution Results

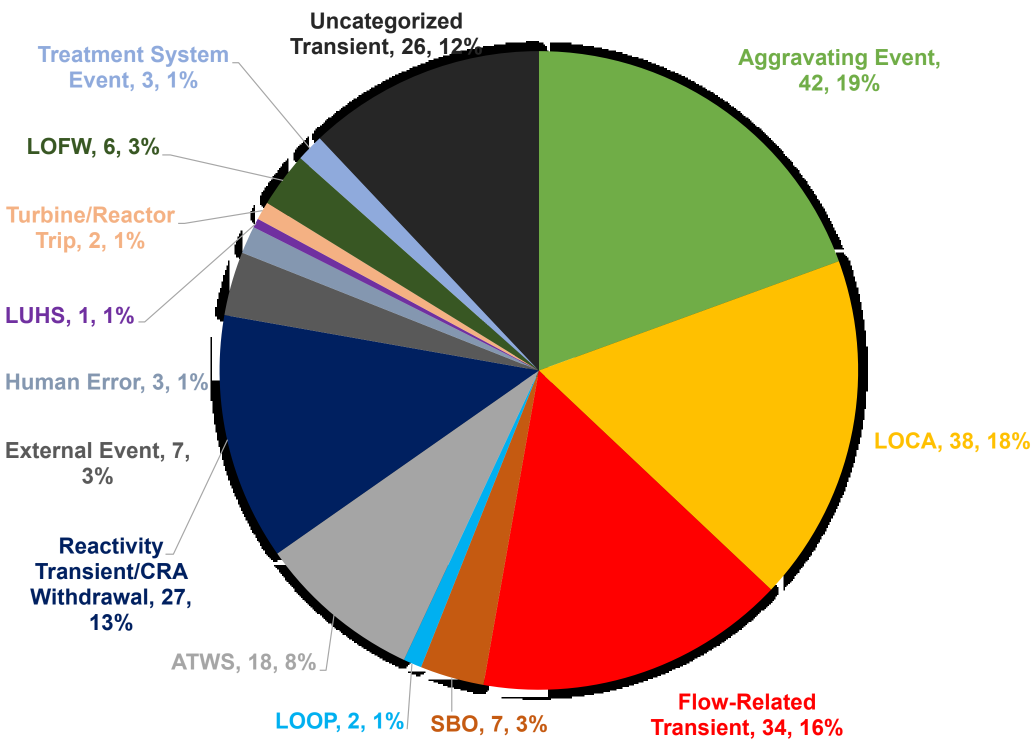


Figure 6. HTGR PIE Distribution Results

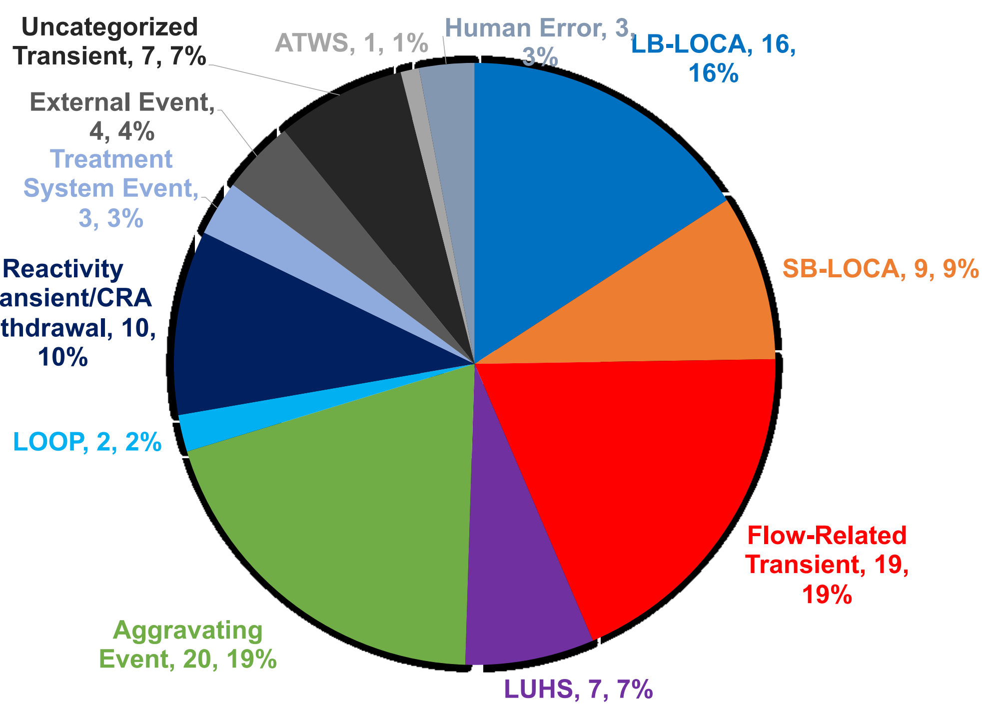


Figure 7. VHTR PIE Distribution Results

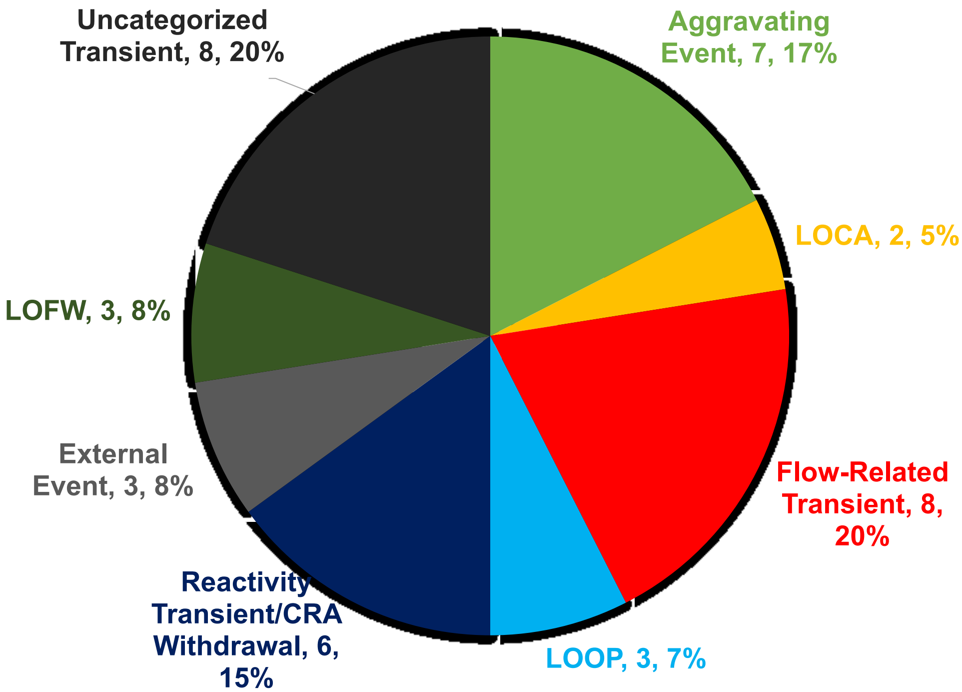


Figure 8. UK GCR PIE Distribution Results

The literature review of initiating events associated with the four gas-cooled reactor concepts produced a dataset of safety-related insights potentially applicable to the FMR. A significant number of the PIEs exhibited similarity to those analyzed as part of a LWR's safety case, particularly for PIEs within those categories that do not represent failures of design-specific features (LOOP, SBO, External Events, LUHS, Reactivity Transients/CRA Withdrawals). However, many PIEs specific to gas-cooled reactors have also been identified. For each of the technologies evaluated, the most pervasive PIE categories included LOCAs and flow-related transients; aggravating events, although not explicitly PIEs, also constituted a large portion of the results from the literature review. These three categories accounted for 78% of GFR PIEs, 53% of HTGR PIEs, 63% of VHTR PIEs, and 42% of UK GCR PIEs.

In the context of gas-cooled reactors, LOCAs correspond to breaks in the reactor coolant system which cause the gas coolant (i.e., helium or CO_2) to flow from the primary system to the surrounding environment (e.g., the reactor building). This outward flow of coolant causes a pressure drop in the primary system, and, if the pressure loss persists, equilibrium between the primary system and the adjacent surrounding pressure will be reached. These events, although functionally similar to the LOCA concept developed for LWRs, are commonly described in the gas-cooled reactor literature as D-LOFCs. Many of the LOCA PIEs identified within the literature analyze coolant loss in conjunction with failures in startup or operation of decay heat removal (DHR) systems and/or breaks in the guard containment. However, design differences between the FMR and the GFRs identified in the literature review impact the direct relevancy of these

R&D Released 2024/08/21 12:31:39

particular events since the FMR utilizes a passive, gravity-driven DHR system as opposed to the active helium-driven DHR systems featured in the ALLEGRO and GFR2400 designs.

Another event that was often analyzed was the pressurized loss of forced cooling (P-LOFC), which was categorized as a flow-related transient in the literature review. P-LOFCs assume a primary coolant flow coast-down; however, unlike in D-LOFCs, the primary system boundary remains intact, and coolant does not leak out. These PIEs were also commonly analyzed in conjunction with failures of DHR systems, and included core/flow channel blockages, pump/blower failures, and spurious valve closures.

The third category that constituted a major share of the recorded PIEs for each of the evaluated technologies was aggravating events. These events follow the occurrence of a PIE, and they have the potential to cause more severe downstream effects than the PIE taken in isolation. In particular, aggravating events in which water or air ingress occurs following a D-LOFC have been extensively analyzed in the literature since oxidation resulting from air ingress can lead to core structural damage, and water ingress can lead to several consequential outcomes such as a positive reactivity insertion and chemical degradation of graphitic components.

7.2 Event Frequency Data

A number of references reviewed in the PIE literature review provided frequency values or ranges for the analyzed PIE. Additionally, several references included qualitative categorizations of PIEs based on expert judgement (e.g., a PIE was determined to be an anticipated operational occurrence or design-basis accident) but did not attempt to quantify the event frequency. To support the derivation of downstream probabilistic risk insights, potentially relevant to the FMR, the quantitative event sequence frequency data for the GFR references reviewed were summarized[2] and are included below in Tables 2-8.

[2] Event frequency data were recorded for the HTGR, VHTR, and UK GCR references, as well. However, the GFR references were prioritized for the current report.

R&D Released 2024/08/21 12:31:39

R&D Released 2024/08/21 12:31:39

Table 2. GFR SB-LOCA Event Frequency Data

GFR SB-LOCAs	Location						
Size		Not Given	SB-LOCA + Close/Guard Containment rupture	Cold leg of PCU	Heat Exchangers	Reactor Coolant System	Secondary Circuit
	Not Given	1E-4/yr<f<1E-2/yr	$P_{conventional}$=1E-07 $P_{conditional}$=1E-06		1E-4/yr<f<2.50E-1/yr	f=5E-04/yr	f=3.18E-01/yr
	Up to 2”	f<1E-2/yr					
	Up to 3”	1E-4/yr<f<1E-2/yr					
	5 cm^2			$P_{conditional}$=0.305			
	“very SB-LOCA”					f=5E-02/yr	

Legend
GFR 2400
ALLEGRO
Both GFR 2400 and ALLEGRO
600 MWt GCFR

Table 3. GFR LB-LOCA Event Frequency Data

GFR LB-LOCAs	Location								
Size		Not Given	LB-LOCA + DHR loop(s) failure	LB-LOCA + Close/Guard Containment rupture	Heat Exchangers	Internal Break	Secondary Circuit	Helium supply system	Power Conversion System
	Not Given	1E-07/yr<f<1E-04/yr	f<1E-07/yr	$P_{conventional}$=1E-06 $P_{conditional}$=1E-07	3.00E-03/yr, 1.2E-2/yr	1E-7/yr<f<1E-4/yr			5E-06/yr
	10”		f<1E-04/yr		1E-04/yr<f<1E-02/yr		1E-7/yr<f<1E-4/yr	f<1E-04/yr	
	55”								
	500 cm^2								$P_{conditional}$=0.305

Legend
GFR 2400
ALLEGRO
Both GFR 2400 and ALLEGRO
600 MWt GCFR

R&D Released 2024/08/21 12:31:39
R&D Released 2024/08/21 12:31:39

Table 4. GFR Reactivity Transient/CRA Withdrawal Event Frequency Data

GFR Reactivity Transient/CRA Withdrawal Events	Event		
Reference Design		Control rod assembly/ absorber withdrawal/ ejection	Control assembly withdrawal + failure of stroke limiting device
	GFR 2400	2E-02/yr	1.24E-04/yr (CDF=4.54E-11/yr)
	GFR 2400	2E-02/yr	1.24E-04/yr (CDF=4.54E-11/yr)

Table 5. GFR Flow-related Transient Event Frequency Data

GFR Flow-Related Transients (primary LOFA)	Event		
Reference Design		Frequency	Additional Information
	GFR 2400	4.66E-01/yr	CDF=3.82E-08/yr
	ALLEGRO	1E-02/yr<f<1E-04/yr	LOFA categorized as a “class 3” initiator which could result in a max cladding temperature of 735 ˚C
	GFR 2400	4.66E-01/yr	Mean frequency presented for partial and total LOFA, with resulting CDF of 3.82E-08/yr

R&D Released 2024/08/21 12:31:39
R&D Released 2024/08/21 12:31:39

Table 6. GFR LUHS Event Frequency Data

GFR LUHS	Event		
Reference Design		LUHS	Loss of Feed Water (LOFW)
	GFR 2400	2.57E+00/yr	
	ALLEGRO	1E-02/yr<f<1E-04/yr	
	GFR 2400	2.57E+00/yr	2.57/yr (mean)

R&D Released 2024/08/21 12:31:39

R&D Released 2024/08/21 12:31:39

Table 7. GFR LOOP Event Frequency Data

GFR LOOPs	Event							
		Long Duration (>24 hr) LOOP	"Long Duration" (>2 hr) LOOP	(LOOP) Duration Unspecified	Short Duration (<24 hr) LOOP	Safeguard switchboard loss	Loss of one electrical switchboard train	LOOP + failure of 2 DHR loops + failure of closing of a main loop
Reference Design	GFR 2400	1E-05/yr		1E-02/yr	1E-02/yr	1E-02/yr		
	GFR 2400	1E-05/yr		1E-02/yr (mean)	1E-02/yr	1E-02/yr	1E-02/yr (mean)	
	GFR 2400	1E-05/yr			1E-02/yr			
	ALLEGRO			1E-04/yr<f<1E-02/yr				
	GFR 2400							f<1E-4/yr
	GFR 2400		1E-04/yr<f<1E-02/yr					

Table 8. GFR Turbine/Reactor Trip Event Frequency Data

GFR Turbine/Reactor Trips	Event						
Reference Design		Generator or Main Turbine Trip or Fault	Inadvertent Reactor Trip	Inadvertent turbomachinery rundown	Spurious reactor trip	Generator trip or fault (secondary or tertiary)	Turbomachinery trip or fault
	GFR 2400	1/yr		0.229/yr	1E-01/yr		
	GFR 2400	1/yr	1.1/yr	0.229/yr	1E-01/yr	1.00/yr (mean)	2.29E-01/yr (mean)
	GFR 2400		1E-01/yr				

7.3 Relating FMR Requirements to FSFs

As a part of the PIE identification process, FMR functional requirements were related to each PIE to help provide an initial understanding of the adequacy of the barriers in place to prevent/mitigate the propagation of the initiator specific to the FMR design. To tie the FMR requirements to their relevant barriers and PIEs, the NRC's "Fundamental Safety Function" (FSF) framework was used. The FSF framework was first introduced for use within the advanced reactor regulatory space in SECY 18-0096 [Reference 16], and adopts similar terminology and definitions promulgated by the International Atomic Energy Agency (IAEA) in SSR-2/1 (Rev. 1) [Reference 17]. Three FSFs are commonly recognized, and, at a high level, these FSFs can be interpreted as the barriers progressively put in place to facilitate safety:

1) Control reactivity
2) Remove heat
3) Confine radioactive material [3]

The FMR's requirements are intended to support the eventual safe and efficient operation of the reactor design—and thus can be traced back to these three FSF(s). The relevant FSF (or FSFs) were assigned to each FMR requirement associated with the identified PIEs as an early form of a barrier analysis commensurate with the maturity of the FMR design.

In assigning FSFs to each requirement, a scheme was also developed to identify the type of safety-related action that was being undertaken; FMR requirements were classified within the four following actions:

   a) Monitor the parameter (e.g., reactivity, coolant temperature, radiation levels)

[3] Sometimes, a fourth fundamental safety function is added to these discussions. NRC Reg. Guide 1.244 [Reference 18] lists FSF4 as "maintenance of adequate shielding against radiation." NRC comments on the Southern Company SC-16166-100, Technology Inclusive Content of Application Project for Non-Light Water Reactors, also mention controlling chemical reactions as a potential fourth fundamental safety function.

b) Detect/alarm when the reactor/parameter is out of the bounds of the safe operational envelope
c) Take the necessary control actions to either maintain or bring the reactor/parameter back into safe operational bounds
d) Other (this action class was primarily reserved for requirements that specify normal process conditions [e.g., process fluid, flow rate, etc.] that are not specified in the requirement to be safety-related limits)

The results of the barrier analysis were organized by event category type, and the number of mentions of FMR requirements performing each FSF/action combination were tallied in each PIE category to gain an understanding of how the FMR requirements satisfy the FSFs in response to each PIE category.

7.3.1 Aggravating Events

One of the most useful insights to come from the barrier analysis was the identification of where opportunities exist for expansion/clarification of the FMR requirements. In the case of aggravating events, the largest opportunity for clarification of FMR requirements and functions is in the case of monitoring parameters that ensure all three FSFs are performed. Specific insights for enhancing FMR monitoring capabilities identified for aggravating events include:

- Although detection of off-normal coolant parameters is identified within the FMR requirements, the need to monitor such parameters is not emphasized, as suggested by the lack of monitoring actions identified in the relevant FMR requirements.
  - For aggravating events specifically, opportunity exists to prioritize locations/ subsystems for coolant purity monitoring (in addition to the helium supply system) to understand baseline impurity concentrations and help detect air ingress and subsequent oxidation of the SiC cladding.
- For containment system requirements that indicate the need to isolate lines/close valves in certain process conditions, the FMR requirements do not presently specify the need to monitor the positions of these valves, which is likely necessary for valves designated as safety significant or safety-related.

Table 9. Number of Mentions of Specific FSF/Action Classes within FMR Requirements Relevant to Aggravating Events

Aggravating Events												
	Fundamental Safety Function											
	1 (control reactivity)				2 (remove heat)				3 (confine radioactive material)			
Action	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs
a (monitor)	0	0	6	0	0	2	1	0	0	0	0	0
b (detect/ alarm)	10	2	2	0	9	36	10	1	7	21	3	1

R&D Released 2024/08/21 12:31:39

Aggravating Events												
	Fundamental Safety Function											
	1 (control reactivity)				2 (remove heat)				3 (confine radioactive material)			
Action	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs
c (control actions)	17	2	4	2	24	9	7	3	20	28	6	1
d (other)	5	4	2	0	21	3	12	0	3	0	4	0

7.3.2 Flow-Related Transient Events

The results of the barrier analysis for the flow-related transient events found within the literature are summarized in Table 10. Unsurprisingly, most of the FMR requirements relevant to flow-related transients were classified as FSF2. Further, FMR requirements appear to indicate good coverage of monitor, detection, and control actions for this category of PIEs.

Table 10. Number of Mentions of Specific FSF/Action Classes within FMR Requirements Relevant to Flow-Related Transient Events

Flow-Related Transient Events												
	Fundamental Safety Function											
	1 (control reactivity)				2 (remove heat)				3 (confine radioactive material)			
Action	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs
a (monitor)	2	11	2	5	4	42	4	15	2	11	2	5
b (detect/ alarm)	1	0	2	0	2	41	3	10	0	10	1	0
c (control actions)	2	0	4	0	7	14	7	4	1	10	3	0
d (other)	0	0	0	0	31	4	35	0	0	0	0	0

7.3.3 LOCA, LB-LOCA, and SB-LOCA Events

Because of differences in the information available for the four concepts reviewed, three categories of LOCA events were identified in the literature—generic LOCAs (no break size indicated), LB-LOCAs, and SB-LOCAs. Due to the similarities in the FMR requirements relevant to the PIEs within each LOCA category, they are considered together here. Table 11, 12, and 13 present the results of the barrier analysis for the LOCA, LB-LOCA, and SB-LOCA categories, respectively. The FMR requirements found to be most relevant to LOCAs were those with concerned with FSF2 and FSF3, with good coverage of action b (detect/alarm, in this case, detecting leak/break locations) and action c (control actions, in this case isolating leaking lines, containing radionuclides, and using the residual heat removal system to remove heat from the reactor core). However, once again, limited consideration of monitoring parameters that indicate leakage (i.e., action a) is given in the relevant FMR requirements.

Monitoring is a precursor to detection/alarm functions and requires thoughtful consideration of the direct and surrogate parameters that, in this case, could be used to help identify when a leak/break occurs and where it is located. Further, monitoring provides baseline measurements that may be useful to help identify deviations from normal process conditions. For LOCAs, consideration should be given to the means for performing and verifying leak detection; some resultant design questions include:

- Will the FMR feature leak detection system(s)? What type(s) of leak detection are being employed?
- Can other parameters already being monitored (e.g., flow rate, pressure, radiation measurements) be used to confirm/verify the location of a leak/break?

Table 11. Number of Mentions of Specific FSF/Action Classes within FMR Requirements Relevant to LOCA Events

LOCA Events												
	Fundamental Safety Function											
	1 (control reactivity)				2 (remove heat)				3 (confine radioactive material)			
Action	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs
a (monitor)	--	0	--	0	--	1	--	0	--	0	--	0
b (detect/alarm)	--	0	--	0	--	35	--	2	--	32	--	2
c (control actions)	--	0	--	0	--	14	--	0	--	33	--	2
d (other)	--	0	--	0	--	2	--	0	--	2	--	0

Table 12. Number of Mentions of Specific FSF/Action Classes within FMR Requirements Relevant to LB-LOCA Events

LB-LOCA Events												
	Fundamental Safety Function											
	1 (control reactivity)				2 (remove heat)				3 (confine radioactive material)			
Action	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs
a (monitor)	0	--	0	--	2	--	0	--	0	--	0	--
b (detect/ alarm)	3	--	1	--	71	--	23	--	56	--	17	--
c (control actions)	6	--	2	--	34	--	4	--	64	--	18	--
d (other)	2	--	0	--	39	--	4	--	1	--	0	--

Table 13. Number of Mentions of Specific FSF/Action Classes within FMR Requirements Relevant to SB-LOCA Events

SB-LOCA Events												
	Fundamental Safety Function											
	1 (control reactivity)				2 (remove heat)				3 (confine radioactive material)			
Action	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs
a (monitor)	0	--	0	--	0	--	0	--	0	--	0	--
b (detect/ alarm)	3	--	0	--	37	--	16	--	37	--	6	--
c (control actions)	5	--	0	--	18	--	5	--	42	--	8	--
d (other)	1	--	0	--	13	--	1	--	1	--	0	--

7.3.4 LOOP Events

The results of the barrier analysis for the LOOP events identified within the literature are found in below in Table 14. During a LOOP event, emphasis is placed FSF1 (shutting down the reactor to control reactivity) and FSF2 (maintaining adequate heat removal). Similar to many of the other PIE categories, few references to monitoring functions were found in the relevant FMR

R&D Released 2024/08/21 12:31:39
R&D Released 2024/08/21 12:31:39

requirements for LOOPs. One FMR requirement was found related to facilitating FSF2a for a LOOP. Opportunity exists to further clarify the specific AOOs and accident conditions, such as LOOPs, that the reactor protection system (RPS) should be expected to recognize, differentiate, and respond to.

Table 14. Number of Mentions of Specific FSF/Action Classes within FMR Requirements Relevant to LOOP Events

LOOP Events												
	Fundamental Safety Function											
	1 (control reactivity)				2 (remove heat)				3 (confine radioactive material)			
Action	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs
a (monitor)	0	0	0	0	1	0	0	0	0	0	0	0
b (detect/ alarm)	15	0	2	0	16	0	1	0	0	0	0	0
c (control actions)	15	0	2	0	37	2	3	3	0	0	0	0
d (other)	0	0	0	0	1	0	4	0	0	0	0	0

7.3.5 LUHS Events

The literature for three reactor concepts (GFRs, HTGRs, and VHTRs) included PIEs that considered LUHS events. The LUHS barrier analysis results are summarized in Table 15. During LUHS events, the emphasis is on maintaining adequate heat removal from the reactor (FSF2). The relevant FMR requirements are primarily classified as FSF2d; many specify coolant temperatures, coolant system layout, and technologies. Opportunity exists to further evaluate the conditions that could lead to an LUHS within the FMR, and to write requirements that ensure the FMR meets the FSFs upon the occurrence of this event.

Further, one reactor concept (VHTRs) considered protected and unprotected LUHS events; these PIEs suggest that additional consideration should be given to the interface between the RPS and ultimate heat sink—for example which signals from the ultimate heat sink should be sent to the RPS to initiate reactor shutdown upon the occurrence of an LUHS.

Table 15. Number of Mentions of Specific FSF/Action Classes within FMR Requirements Relevant to LUHS Events

LUHS Events												
	Fundamental Safety Function											
	1 (control reactivity)				2 (remove heat)				3 (confine radioactive material)			
Action	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs
a (monitor)	0	0	0	--	0	0	0	--	0	0	0	--
b (detect/ alarm)	0	0	2	--	2	0	0	--	0	0	0	--
c (control actions)	0	0	4	--	4	3	3	--	0	0	2	--
d (other)	0	0	0	--	15	1	21	--	0	0	0	--

7.3.6 Reactivity Transient/CRA Withdrawal Events

Reactivity transient/CRA withdrawal events are a frequently examined category of PIE for each of the reactor concepts reviewed, as suggested by the results of the barrier analysis in Table 16 below. The RPS and reactor instrumentation subsystem are the primary FMR subsystems credited upon occurrence of reactivity transients/CRA withdrawals. Analysis of this category of PIE is primarily concerned with proving out the ability of the FMR to continue to meet FSF1. However, one of the FMR requirements relevant to reactivity transient/CRA withdrawal events, describes the monitoring functions that should be performed by the reactor instrumentation system, which, in addition to monitoring reactivity, control rod positioning, and neutron flux also monitors temperature, pressure and flow to facilitate FSF2a and 3a.

Table 16. Number of Mentions of Specific FSF/Action Classes within FMR Requirements Relevant to Reactivity Transient/CRA Withdrawal Events

Reactivity Transient/CRA Withdrawal Events												
	Fundamental Safety Function											
	1 (control reactivity)				2 (remove heat)				3 (confine radioactive material)			
Action	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs
a (monitor)	5	24	0	6	5	24	0	6	5	24	0	6

Reactivity Transient/CRA Withdrawal Events												
	Fundamental Safety Function											
	1 (control reactivity)				2 (remove heat)				3 (confine radioactive material)			
Action	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs
b (detect/ alarm)	5	0	10	0	0	0	0	0	0	0	0	0
c (control actions)	21	23	40	6	1	4	1	0	10	1	20	0
d (other)	0	0	0	0	0	0	3	0	0	0	0	0

7.3.7 SBO Events

SBO events were found in the literature for two concepts—GFRs and HTGRs, as shown in Table 17 below. The primary FMR requirements relevant to the SBO PIEs satisfied FSF2c and FSF2d. No references to monitoring or detect/alarm functions specific to SBOs were found in the FMR requirements, likely attributed to the design requirement that specifies the FMR's response to an SBO be passive. However, the other FSFs may not be met in a passive means during an SBO.

Table 17. Number of Mentions of Specific FSF/Action Classes within FMR Requirements Relevant to SBO Events

SBO Events												
	Fundamental Safety Function											
	1 (control reactivity)				2 (remove heat)				3 (confine radioactive material)			
Action	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs
a (monitor)	0	0	--[a]	--	0	0	--	--	0	0	--	--
b (detect/ alarm)	0	1	--[a]	--	2	0	--	--	0	0	--	--
c (control actions)	0	1	--[a]	--	29	7	--	--	0	0	--	--
d (other)	0	1	--[a]	--	0	0	--	--	0	0	--	--

7.3.8 Turbine/Reactor Trip Events

Turbine/reactor trip events were found in the literature for GFRs and HTGRs as shown in Table 18. Turbine trip events are primarily concerned with maintaining the performance of FSF2 and FSF3. Similar to LOOP events described above, FMR requirements were developed for monitoring turbine trips in support of FSF2. Reactor trips are primarily concerned with maintaining performance of FSF1 and are frequently attributed to various FMR requirements which address FSF1b and 1c and FSF1c and 3c, similar to reactivity transients/CRA withdrawal events. However, in examining the results of the barrier analysis for reactivity transient/CRA withdrawal events in conjunction with reactor trips, the FMR requirements do not appear to specify any monitoring or alarm/detections functions that could help differentiate between inadvertent/spurious reactor trips and reactivity transients caused by other means.

Table 18. Number of Mentions of Specific FSF/Action Classes within FMR Requirements Relevant to Turbine/Reactor Trip Events

Turbine/Reactor Trip Events												
	Fundamental Safety Function											
	1 (control reactivity)				2 (remove heat)				3 (confine radioactive material)			
Action	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs
a (monitor)	0	0	--	--	4	1	--	--	0	0	--	--
b (detect/ alarm)	2	0	--	--	4	1	--	--	5	0	--	--
c (control actions)	4	1	--	--	1	0	--	--	8	0	--	--
d (other)	0	0	--	--	0	0	--	--	0	0	--	--

7.3.9 ATWS Events

ATWS events were identified in the VHTR and HTGR literature and are defined broadly such that the barrier analysis indicated that FMR requirements attributed all three FSFs were relevant to these PIEs. Many of the same requirements relevant to reactivity transients/CRA withdrawals are referenced for ATWS events. The FMR's instrumentation and control (I&C) system is also frequently credited for ATWS events through requirements in support of FSF1c and 3c and in support of FSF1c.

R&D Released 2024/08/21 12:31:39
R&D Released 2024/08/21 12:31:39
R&D Released 2024/08/21 12:31:39

Table 19. Number of Mentions of Specific FSF/Action Classes within FMR Requirements Relevant to ATWS Events

ATWS Events												
	Fundamental Safety Function											
	1 (control reactivity)				2 (remove heat)				3 (confine radioactive material)			
Action	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs
a (monitor)	--	1	1	--	--	12	1	--	--	12	1	--
b (detect/alarm)	--	0	1	--	--	1	0	--	--	0	0	--
c (control actions)	--	14	4	--	--	6	1	--	--	1	2	--
d (other)	--	0	0	--	--	0	0	--	--	0	0	--

7.3.10 External Events

Some external events were identified in the literature for HTGRs, VHTRs, and UK GCRs, although by no means were the external events in the literature comprehensive. The most frequently identified external events in the literature were earthquakes, although generic external hazards, high winds, and missiles were also mentioned. Depending on the context of an individual PIE, an external event may have the potential to challenge any or all of the three FSFs. Table 20 below summarizes the number of references to each FSF/action within the FMR requirements deemed relevant to each external event PIE. When the maturity of the design permits, it is recommended that functional requirements for monitoring and alarm/detection of external events be expanded.

Table 20. Number of Mentions of Specific FSF/Action Classes within FMR Requirements Relevant to External Events

External Events												
	Fundamental Safety Function											
	1 (control reactivity)				2 (remove heat)				3 (confine radioactive material)			
Action	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs
a (monitor)	--	0	0	0	--	0	0	0	--	0	0	0

External Events												
	Fundamental Safety Function											
	1 (control reactivity)				2 (remove heat)				3 (confine radioactive material)			
Action	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs
b (detect/ alarm)	--	0	0	0	--	1	1	0	--	1	2	0
c (control actions)	--	5	2	3	--	8	5	3	--	6	4	3
d (other)	--	0	0	0	--	0	0	0	--	0	0	13

7.3.11 Human Error Events

Human error PIEs were identified in the HTGR and VHTR literature and primarily include instances of inadvertent control rod withdrawal, reactor shutdown, safety valve opening/closing. The results of the barrier analysis for these human error events were attributed to FSF1d, FSF2d, and FSF3d. It is recommended that refinement and expansion of the human factors engineering requirements occurs when the design is at an appropriate level of maturity.

Table 21. Number of Mentions of Specific FSF/Action Classes within FMR Requirements Relevant to Human Error Events

Human Error Events												
	Fundamental Safety Function											
	1 (control reactivity)				2 (remove heat)				3 (confine radioactive material)			
Action	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs
a (monitor)	--	0	0	--	--	0	0	--	--	0	0	--
b (detect/ alarm)	--	0	1	--	--	0	0	--	--	0	0	--
c (control actions)	--	0	4	--	--	0	0	--	--	0	3	--
d (other)	--	4	1	--	--	3	0	--	--	3	1	--

R&D Released 2024/08/21 12:31:39
R&D Released 2024/08/21 12:31:39

7.3.12 LOFW Events

Table 22 summarizes the results of the barrier analysis performed on the LOFW events. Within the HTGR and UK GCR literature, a total of nine LOFW events were identified; however, due to the specificity of the PIEs, only one relevant FMR requirement was identified for one of the PIEs. This requirement is concerned with internal diagnostic monitoring for temperature and flow of cooling loops to detect abnormal operation to support accomplishment of FSF2a and FSF2b; however, it does not address mitigative measures if abnormal conditions are detected. Thus, opportunity exists to develop additional FMR requirements that address the control actions that should be taken upon the I&C system's detection of abnormal conditions in the FMR's cooling loops.

Table 22. Number of Mentions of Specific FSF/Action Classes within FMR Requirements Relevant to LOFW Events

LOFW Events												
	Fundamental Safety Function											
	1 (control reactivity)				2 (remove heat)				3 (confine radioactive material)			
Action	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs
a (monitor)	--	0	--	0	--	0	--	1	--	0	--	0
b (detect/ alarm)	--	0	--	0	--	0	--	1	--	0	--	0
c (control actions)	--	0	--	0	--	0	--	0	--	0	--	0
d (other)	--	0	--	0	--	0	--	0	--	0	--	0

7.3.13 Treatment System Events

Treatment system events were identified within the literature for HTGRs and VHTRs, and the results of the barrier analysis for these PIEs are shown in Table 23 below. Helium treatment systems for GFRs are generally at a low level of technology maturity, and this is reflected in the literature. Only six PIEs among all the references reviewed were identified as pertaining to the He treatment system, although the system is tasked with maintaining the purity of the coolant inventory in support FSFs 1 and 2. Additionally, because the treatment system contains radioactive primary coolant, it is also subject to containment requirements in order to meet the objectives of FSF3.

Because the treatment system of the FMR (the Helium Service System) is tasked with decontamination of the primary coolant inventory, the referenced FMR requirements pertained

R&D Released 2024/08/21 12:31:39

R&D Released 2024/08/21 12:31:39

to monitoring, detecting the location of, and treating the primary coolant inventory for contaminants. Given the importance of the Helium Service System to safety and operability, it is recommended that the coverage of the Helium Service System Requirements is expanded to ensure that it meets the three FSFs.

Table 23. Number of Mentions of Specific FSF/Action Classes within FMR Requirements Relevant to Treatment System Events

Treatment System Events												
	Fundamental Safety Function											
	1 (control reactivity)				2 (remove heat)				3 (confine radioactive material)			
Action	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs
a (monitor)	--	0	0	--	--	0	0	--	--	1	0	--
b (detect/ alarm)	--	0	0	--	--	4	4	--	--	2	2	--
c (control actions)	--	0	0	--	--	0	0	--	--	1	1	--
d (other)	--	1	2	--	--	2	2	--	--	0	0	--

7.3.14 Uncategorized Transient Events

Uncategorized transient events—a category for PIEs that were not able to be appropriately categorized under any other category—were identified within the literature for three reactor concepts (HTGRs, VHTRs, and UK GCRs). The results of the barrier analysis for the uncategorized transients are shown in Table 24. Given the lack of specificity in the definition of this category, it is not surprising to see diversity among the FSFs and actions referenced in the relevant FMR requirements.

R&D Released 2024/08/21 12:31:39
R&D Released 2024/08/21 12:31:39

Table 24. Number of Mentions of Specific FSF/Action Classes within FMR Requirements Relevant to Uncategorized Transient Events

Uncategorized Transient Events												
	Fundamental Safety Function											
	1 (control reactivity)				2 (remove heat)				3 (confine radioactive material)			
Action	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs	GFRs	HTGRs	VHTRS	UK GCRs
a (monitor)	--	3	1	1	--	5	2	2	--	4	1	1
b (detect/ alarm)	--	3	1	1	--	3	2	2	--	2	0	1
c (control actions)	--	3	1	3	--	8	3	4	--	3	0	2
d (other)	--	0	3	2	--	3	8	1	--	3	0	1

7.4 Safety Analysis of Passive Safety Systems

As described earlier in Section 8.1, the PIE literature review revealed that failures associated with the startup or operation of the DHR system were often analyzed for previously developed conceptual GFR designs. However, the DHR systems included in the GFR designs that were reviewed are active helium-driven systems, whereas the FMR DHR system utilizes a passive, gravity-driven system that is capable of removing reactor decay heat without the need for any active components or human actuation. Because of the emphasis of the ability of the DHR system to perform its intended function during accident scenarios, it was determined that further analysis of this particular system was warranted. Specifically, the role of the FMR's passive DHR system, the RVCS, was determined to play a potentially significant role in the development of the overall FMR safety case. To that end, a comprehensive review of passive system safety assessment approaches applied for other similar systems was performed in order to ascertain the most appropriate technique(s) that should be used to evaluate the RVCS.

Defining Passivity. A generally accepted definition of "passive" within the nuclear industry is the combination of two elements as follows [Reference 19]:

Passive Component: A component which does not need any external input to operate, and

Passive System: Either a system which is composed entirely of passive components and structures or a system which uses active components in a very limited way to initiate subsequent passive operation.

R&D Released 2024/08/21 12:31:39

R&D Released 2024/08/21 12:31:39

Four categories of passivity have been identified for use in qualitative evaluation and classification of passive systems, from most passive to least passive, as follows:

- **Category A**
  - Characteristics
    - No signal inputs of intelligence[4]
    - No external power sources or forces
    - No moving mechanical parts
    - No moving working fluid[5].
  - Example safety features
    - Physical barriers against the release of fission products, such as nuclear fuel cladding and pressure boundary systems
    - Hardened building structures for the protection of a plant against seismic and or other external events
    - Core cooling systems relying only on heat, radiation, and/or conduction from nuclear fuel to outer structural parts, with the reactor in hot shutdown
    - Static components of safety-related passive systems (e.g., tubes, pressurizers, accumulators, surge tanks), as well as structural parts (e.g., supports, shields).
- **Category B**
  - Characteristics
    - No signal inputs of intelligence
    - No external power sources or forces
    - No moving mechanical parts, but

[4] Intelligence is described as a signal or parametric change to initiate action.
[5] The no-motion requirement does not extend to unavoidable changes in geometry such as thermal expansion.

        - Moving working fluids are allowed. The fluid movement is only due to thermal-hydraulic conditions occurring when the safety function is activated. No distinction is made among fluids of different nature (e.g., borated water and air) although the nature of the moving fluid may be significant for the availability of the function performed within this category.
    - Example safety features
        - Reactor shutdown/emergency cooling systems based on injection of borated water produced by the disturbance of a hydrostatic equilibrium between the pressure boundary and an external water pool
        - Reactor emergency cooling systems based on the natural circulation of air or water in heat exchangers immersed in water pools (inside containment) to which the decay heat is directly transferred
        - Containment cooling systems based on natural circulation of air flowing around the containment walls, with intake and exhaust through a stack or in tubes covering the inner walls of silos of underground reactors
        - Fluidic gates between process systems, such as “surge lines” of LWRs.
- **Category C**
    - Characteristics
        - No signal inputs of intelligence
        - No external power sources or forces
        - Moving mechanical parts and moving working fluids are allowed. The fluid motion is characterized as in category B. Mechanical movements are due to imbalances within the system (e.g., static pressure in check and relief valves, hydrostatic pressure in accumulators) and forces directly exerted by the process.
    - Example safety features
        - Emergency injection systems consisting of accumulators or storage tanks and discharge lines equipped with check valves
        - Overpressure protection and/or emergency cooling devices of pressure boundary systems based on fluid release through relief valves
        - Filtered venting systems of containments activated by rupture disks; and – mechanical actuators, such as check valves and spring-loaded relief valves, as well as some trip mechanisms (e.g., temperature, pressure and level actuators).

- **Category D**
  - Characteristics: This category addresses the intermediary zone between active and passive, where the execution of the safety function is made through passive methods as described in the previous categories, except that internal intelligence is not available to initiate the process.
    - An external signal is permitted to trigger the passive process but the operation of the process is passive (active initiation/passive execution). To recognize this departure, this category is referred to as "passive execution/active initiation."
    - No external power or forces. Energy for initiation must only be obtained from stored sources such as batteries or compressed or elevated fluids, excluding continuously generated power such as normal AC power from continuously rotating or reciprocating machinery
    - Active initiation components are limited to controls, instrumentation and valves, but valves used to initiate safety system operation must be single-action relying on stored energy
    - Manual initiation is excluded.
  - Example safety systems
    - Emergency core cooling/injection systems, based on gravity driven or compressed nitrogen driven fluid circulation, initiated by fail-safe logic actuating battery-powered electric or electro-pneumatic valves
    - Emergency core cooling systems, based on gravity-driven flow of water, activated by valves which break open on demand (if a suitable qualification process of the actuators can be identified)
    - Emergency reactor shutdown systems based on gravity driven, or static pressure driven control rods, activated by fail-safe trip logic [Reference 19].

The foregoing categories highlight an oftentimes overlooked consideration with respect to passive systems: they are typically claimed to be fully passive but seldom attempt to categorize the degree of passivity. Guidelines providing more detailed insights on evaluating decay heat removal systems are not available in the public literature. Such guidance is necessary since all decay heat removal systems include moving mechanical parts (e.g., valves, perhaps pumps) which means they would be in Category C or D depending on the initiation approach. The advantage of including mechanical parts is that ease and efficiency of normal reactor operation is improved; however, the disadvantage is that the mechanical parts must operate properly when needed and the reliability of such operation must be considered in the safety analysis.

One DHR design by Framatome [Reference 20] proposes to achieve greater passivity by having the decay heat removal system operate continuously using mechanical parts, accepting the degradation of reactor thermal efficiency from doing so, but designing the embedded natural circulation loop to have no mechanical parts so that the reactor core would be adequately cooled during a DBA. The design is conceptually very similar to the RVCS of the FMR. By having the safety function during normal operation be performed by only moving working fluids (water), and assuming that the Framatome design is the same as the FMR RVCS, the decay heat removal system would be classified as Category B. Although many gas-cooled reactor designs rely heavily on Category A passive means for transferring heat out of the core itself, designing a Category A passive system in an operable reactor would seem unlikely because of the need to transfer heat from the reactor cavity to an external heat sink without a working fluid, i.e., by conduction or radiation.

With respect to passive system safety assessments, three general approaches to modeling failure rates have been identified and they are summarized below [Reference 21].

Independent failure modes approach. The independent failure modes approach entails:(i) identifying the failure modes leading to the unfulfillment of the passive system function, and (ii) evaluating the system failure probability as the probability of failure modes occurrence. Typically, failure modes are identified from the application of a FMEA procedure. However, because physical phenomena are central to passive systems, failure is characterized by the definition of the probability distributions and failure ranges of the critical physical parameters. For example, in passive decay heat removal system, these may include non-condensable gas build-up, the undetected leakage, the heat exchange process reduction due to surface oxidation, piping layout, thermal insulation degradation, etc. To evaluate the probability of failure, the probabilities of the different failure mode events, assuming mutually non-exclusive independent events, are used. This means that a single failure mode event is sufficient to lose the system function which means the resulting value of system failure probability would be an upper bound of the failure rate. Consequently, this estimate may be overly conservative and a potential disadvantage of this approach.

Hardware failure modes approach. In the hardware failure modes approach, the failure rates of the passive system are obtained by accounting for the probabilities of hardware failures that degrade the physical mechanisms which the passive system relies upon for its function. For example, natural circulation failure due to high concentration of non-condensable gas is modelled in terms of the probability of occurrence of vent lines failure to purge the gases. Another example is natural circulation failure because of insufficient heat transfer to an external source, which is assessed through two possible hardware failure modes: (1) insufficient water in the pool and make-up valve malfunctioning or (2) degraded heat transfer conditions due to excessive fouling of the heat exchanger pipes. Thus, the probabilities of degraded physical mechanisms are expressed in terms of unreliability of the components whose failures degrade the function of the passive system. Potential weaknesses of this approach are: (a) potential lack of completeness of the identification of possible failure modes and corresponding hardware failures, (b) failures due to unfavorable initial or boundary conditions being neglected, and (c) fault tree models typically adopted to represent the hardware failure modes may inadequately address complex thermohydraulic phenomena and behavior.

Functional failure approach. The functional failure approach is, eponymously, based on the concept of the functional failure. In the context of passive systems, this is defined as the probability of failing to achieve a safety function, i.e., the probability that a given safety variable (i.e., the load imposed on the system) will exceed a safety threshold (i.e., the capacity of the system to handle the load). To model uncertainties, probability distributions in passive systems are assigned, frequently by engineering judgment, to both the capacity (for example, the maximum allowable cladding temperature) and the load (i.e., the cladding temperature under various scenarios). At this juncture, heavy reliance on expert judgement is unavoidable because of the paucity of data concerning the performance of passive systems.

After assembling and reviewing the literature on analysis of passive decay heat removal system safety analysis approaches, a number of challenges were frequently mentioned regarding their analyses and calculation of their failure rates and uncertainties therein.

Defining failure. The general definition of failure in an active safety system is straightforward: a mechanical or electrical component either fails to perform its function at some point during the required mission time (a time-base failure of a continuously operated system) or fails to perform its function on demand (a demand-based failure—for example failure to open of a valve). The key assumption usually made is that the component's behavior can be represented as binary: it works or it does not work. Although even this Boolean behavior of active components can be argued against (e.g., partially open or closed valves), this assumption is frequently used in active systems and is justified by the large driving forces involved. However, the driving forces in passive systems are relatively small because they depend on driving heads via natural forces such as buoyancy, heat conduction and radiation, and gravity. As a consequence, the magnitude of the natural driving forces depends on the environment around the passive system. Stated another way, the passive system may partially work, but it may not work well enough to meet safety expectations.

Functional failures are important in passive systems. Two additional consequences of the low magnitude of the driving forces associated with passive systems are that (1) phenomena that are unimportant in active safety systems can be very important by comparison and (2) counter-intuitive results can occur. Examples are as follows:

- The importance of insulation thermal conductivity and heat transfer coefficient in containment on fluid flow in natural circulation loops.
- The effect of the temperature profile surrounding the various parts of the passive system.
- The heat capacity of reactor structures is important in gas-cooled reactors because of the small heat capacity of helium.

The potential for partial failure of passive system performance and the low magnitude of driving forces in such systems has led to the need to model such failures. Of the three general modeling approaches described in earlier, only the functional failure approach directly addresses partial failures and is the most commonly used approach in the literature examined. As described above, “functional failure” can be described in terms of a “load” exerted during the performance of the system on its components and the “capacity” of these components to withstand that load. The difference between load imposed on the system and the capacity of the system to handle the load is often labeled “safety margin”, and it can be smaller in passive systems because of the larger uncertainties in the environment around the system [Reference 21]. As an example of a functional failure, consider the following [Reference 22]:

> *“To clarify the distinction between a functional failure and a traditional hardware failure, let us define the two concepts considering the example of a pump whose mission is to provide a specified flow rate. The pump is supposed to work in a given environment, defined by the temperature and pressure of the fluid. Hardware failure of a component or system is said to occur when one or more subcomponents physically breaks, disabling the component. In the example of the pump, a mechanical failure of the rotor shaft would be classified as hardware failure. This type of failure is included explicitly in the PRA. If there are no uncertainties regarding the model describing the system and the numerical values of its important parameters, then only hardware failures have to be considered. The only epistemic uncertainties in such a case are those associated with the numerical values of failure rates. However, because of the existence of these uncertainties, it is possible that even if no hardware failure occurs, the system may not be able to accomplish its mission. In this case, a functional failure is said to have occurred. In the example of the pump, a failure to accomplish the mission due to uncertainties in the temperature and pressure of the fluid would be classified as a functional failure.”*

7.5 FMEA and MLD Development

Given the results of the evaluation of the review of passive system safety assessments, it was determined that a FMEA was the appropriate technique to apply to the FMR. FMEA was selected as the appropriate PHA technique to apply for the following reasons:

- FMEA is used across the nuclear industry and is well-understood by safety analysts, regulators, and engineers alike.
- The use of FMEA in early-stage, advanced Non-LWR safety analysis is anticipated by the ASME/ANS standard on PRA, incorporated into the industry-recommended approach to risk-informed, performance-based (RI-PB) analysis to support licensing Non-LWRs [Reference 2], and is referred to in the NRC endorsement of the RI-PB approach to licensing advanced Non-LWRs [Reference 9].

R&D Released 2024/08/21 12:31:39

R&D Released 2024/08/21 12:31:39

R&D Released 2024/08/21 12:31:39

- FMEA can support semi-quantitative or quantitative identification of component failure rates, which facilitates later-stage safety analyses, such as fault tree analysis, required as part of a plant's PRA.
- The results of the FMEA can also be used to complement the results from MLD that will be performed on a later-stage iteration of the FMR concept.

However, it was not feasible to perform a comprehensive FMEA for the entire FMR; therefore, a single subsystem was chosen as the subject of the FMEA. Due to its potential impact on the overall safety case of the FMR, and because of its repeated mention throughout the PIE literature review, the RVCS was selected as the subject of the FMEA. The goal of the FMEA is to identify potential failure mechanisms that contribute to the overall risk profile of the RVCS. Because of its passive operation, there is increased emphasis on the functional performance of the system in the event of accident scenarios. Compared to active systems, whose failure mechanisms are typically characterized on a binary basis (i.e., a mechanical or electrical component is either able or unable to perform its intended function on a time or demand basis), passive systems are much more sensitive to the physical characteristics of the system and the operational environment. In particular, they are much more sensitive to changes in operating parameters, boundary conditions, and the surrounding environment. The results of the FMEA will be complemented by the development of the MLD, which will support evaluation of top-level events and their contributing initiators. Both the FMEA and MLD are currently under development and results will become available at the conclusion of the project.

8 SUMMARY AND CONCLUSIONS

GA-EMS has developed a safety approach for the FMR that uses inherent and passive safety along with probabilistic risk insights to satisfy safety and environmental protection requirements. The key safety-related passive system for the FMR is the RVCS. The RVCS removes residual heat during severe accidents including SBO to ensure that the barriers to radionuclide release can achieve their safety functions. The four barriers to radionuclide release that form a DID containment system for FMR are as follows:

1) High-density uranium dioxide fuel pellet
2) SIGA® cladding
3) Reactor helium pressure boundary
4) Leak-tight steel containment

The licensing basis and safety approach for the FMR design follows guidance developed by the NEI in NEI 18-04 [Reference 2] and endorsed by the NRC in Reg. Guide 1.233 [Reference 9]. This guidance provides an integrated and highly interdependent methodology for identifying and evaluating licensing basis events, classifying, and establishing performance criteria for SSCs, and evaluating DID for advanced reactor designs.

The functional safety approach for the FMR uses the SiD methodology published by EPRI [Reference 8]. The SiD methodology is consistent with NEI 18-04 and the FSF Framework referred to by the NRC [Reference 16]. Three FSFs are commonly recognized, and can be interpreted as the barriers progressively put in place to facilitate safety:

1) Control reactivity
2) Remove heat
3) Confine radioactive material

Using historical GCR risk assessments, PIEs were identified, categorized, binned by frequency and evaluated for applicability to the FMR. The FMR's requirements are intended to support the eventual safe and efficient operation of the reactor design—and thus can be traced back to these three FSF(s). The relevant FSF (or FSFs) were assigned to each FMR requirement associated with the identified PIEs as an early form of a barrier analysis commensurate with the maturity of the FMR design.

As the design matures, the FMEA of the passive RVCS will be key to the safety case for the FMR. The results of the FMEA will be complemented by the development of the MLD, which will support evaluation of top-level events and their contributing initiators. Both the FMEA and MLD are currently under development and results will become available at the conclusion of the conceptual design project.

9 REFERENCES

1) H. Choi, *et al.*, "The Fast Modular Reactor (FMR) - Development Plan of a New 50 MWe Gas-cooled Fast Reactor", *Tran. Am. Nucl. Soc.* **124**, 454–456, 2021.
2) NEI 18-04, Revision 1, "Risk-Informed Performance-Based Technology Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development," Nuclear Energy Institute, August 2019.
3) H. Choi, *et al.*, "Fast Modular Reactor Conceptual Design Status," International Congress on Advances in Nuclear Power Plant (ICAPP), Gyeongju, Korea, April 23-27, 2023.
4) EPA-400/R-17/001, "PAG Manual: Protective Action Guides and Planning Guidance for Radiological Incidents," EPA 2017.
5) 51 FR 28044, "Safety Goals for the Operations of Nuclear Power Plants; Policy Statement," NRC 1986.
6) J. W. Winters, "AP-1000 Design Control Document," APP-GW-GL-700, Westinghouse Electric Company 2004.
7) Yinbin Miao, *et al.*, "Steady-state fuel performance analyses for the preliminary fuel concept of General Atomics Fast Modular Reactor," *Journal of Nuclear Materials* **591**, 2024.

R&D Released 2024/08/21 12:31:39

8) EPRI, “Program on Technology Innovation: Early Integration of Safety Assessment into Advanced Reactor Design” - Project Capstone Report. Report 3002015752, Electric Power Research Institute (EPRI): Palo Alto, CA, 2019.

9) Regulatory Guide 1.233, “Guidance for a Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light-Water Reactors,” NRC 2020.

10) NUREG-2122, “Glossary of Risk-Related Terms in Support of Risk-Informed Decisionmaking,” NRC 2013.

11) NRC, Pre-Decisional Draft Regulatory Guide DG-1413: Technology-Inclusive Identification of Licensing Events for Commercial Nuclear Plants, 2022.

12) Regulatory Guide 1.253, “Guidance for a Technology-Inclusive Content of Application Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light-Water Reactors,” NRC 2024.

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

14) International Electrotechnical Commission, “International Standard: Failure modes and effects analysis (FMEA and FMECA),” IEC 60812, 2018.

15) NUREG/CR-2300, “PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants,” NRC 1983.

16) SECY-18-0096, “Functional Containment Performance Criteria for Non-Light-Water Reactors”, NRC 2018.

17) IAEA SSR2/1, “Safety of Nuclear Power Reactors: Design”, Specific Safety Requirements SSR2/1 (Rev. 1), Vienna, Austria (2016)

18) Regulatory Guide 1.244, “Control of Heavy Loads at Nuclear Facilities,” NRC 2021.

19) IAEA-TECDOC-626, "Safety related terms for advanced nuclear plants", IAEA, September 1991.

20) M. Miller, “Reactor Cavity Cooling System”, presentation at the public meeting on *Regulatory Process Improvements for Advanced Reactor Designs*, Nuclear Energy Institute, Washington, DC, July 26, 2018.

21) F. Di Maio et al., “Reliability Assessment of Passive Safety Systems for Nuclear Energy Applications: State-of-the-Art and Open Issues”, *Energies* **14** 4688 https://doi.org/10.3390/en14154688

22) L. P. Pagani, G. E. Apostolakis, and P.I. Hejzlar, "The Impact of Uncertainties on the Performance of Passive Systems", *Nuclear Technology* **149**, 129-140, February 2005.

23) ASME/ANS RA-S-1.4-2021, “Probabilistic Risk Assessment Standard for Advanced Non-Light Water Reactor Nuclear Power Plants,” American Society of Mechanical Engineers (ASME) / American Nuclear Society (ANS) 2021.
24) NUREG-1407, “Procedural and Submittal Guidance for the Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities,” NRC 1991.
25) IAEA SSG-3, “Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants,” IAEA 2010.
26) EPRI 3002005287, “Identification of External Hazards for Analysis in Probabilistic Risk Assessment: Update of Report 1022997,” EPRI 2015.

GENERAL ATOMICS
ELECTROMAGNETICS
P.O. BOX 85608 SAN DIEGO, CA 92186-5608 (858) 455-3000