

***Modular High Temperature Gas-
cooled Reactor Safety Design
Methodology and Implementation
Examples***

FOREWORD

A0076-Paper-Reitsma_Topsafe2017_Rev1

The IAEA has launched the CRP on Modular High Temperature Gas-cooled Reactor Safety Design in 2014 to investigate the development of new safety design criteria [5,17]. The participating member states are China, Germany, Indonesia, Kazakhstan, Korea (Republic of), Japan, Ukraine, UK and the USA. This project is coordinated by the Nuclear Energy Department of the IAEA (not the department responsible for safety requirements) and the final reports from this project will reflect the wishes and proposals of the participating member states on this matter. It will not have the status of an official IAEA safety requirement document since this requires a comprehensive process of drafting and review that typically takes several years to acquire [2]. The project thus largely reflects the perspectives of the designers and safety analysts. The outcome of this project could be a valuable start towards the goal to develop official HTGR safety design requirements.

CONTENTS

1.	INTRODUCTION / SCOPE.....	1
1.1.	BACKGROUND	1
1.2.	HISTORICAL PERSPECTIVES ON HTGR LICENSING EXPERIENCE.....	2
1.3.	THE IAEA COORDINATED RESEARCH PROJECT ON MODULAR HTGR SAFETY DESIGN.....	3
1.4.	1ST GOAL IS TO DESIGN A SAFE NUCLEAR PLANT	4
1.5.	DEVELOPING MODERN REQUIREMENTS (STRENGTHENING)...	4
1.5.1.	Relevance of past licensing experience in the modern licensing environment (post 9/11 and Fukushima) – Overview here (with detail in appendix such as 15hrs vs 72 hours; aircraft impact).....	5
2.	DEFINITION OF MODULAR HTGRS.	6
2.1.	THE INHERENT OR INTRINSIC CHARACTERISTICS OF THE FUEL, MODERATOR MATERIALS AND COOLANT.	8
2.2.	SAFETY DESIGN FEATURES.	14
2.2.1.	Coated Particle Fuel.....	14
2.2.2.	Helium as Primary Coolant.....	15
2.2.3.	Reactivity and Reactor Shutdown.....	15
2.2.4.	Core Thermodynamic Characteristics	15
2.2.5.	Residual Heat Removal	16
2.3.	STRONG MOTIVATION ON THE DIFFERENCES OF MHTGRS (CLIFF EDGE, NO COMMON MODE; LOOK AT MATERIAL IN PAPERS RELATED TO HTGRS; HTR2016 PAPER).....	16
2.3.1.	Control of Reactivity	20
2.3.2.	Heat Removal (and Reactor Coolant Systems).....	21
2.3.3.	Confinement of Radioactive Material.....	22
2.3.4.	Multiple Plants or Units (and Co-Location)	23
2.3.5.	Fuel Requirements	25
2.3.6.	Testing, Monitoring and Instrumentation	26
2.3.7.	Other	26
2.4.	EXEMPLARY DESIGNS THAT ALL APPLIED THE MODULAR HTGR SAFETY APPROACH, TWO PEBBLE BED AND TWO PRISMATIC DESIGNS	27
2.4.1.	HTR-MODULE (Germany)	27
2.4.2.	MHTGR (US)	32
2.4.3.	HTR-PM (China)	37
2.4.4.	GTHTR300 (Japan)	41
3.	RELEVANT PAST AND CURRENT WORK RELATED TO HTGR SAFETY.	46
3.1.	ADVANCED REACTORS / NON-WATER COOLED	46
3.2.	IAEA DOCUMENTS.....	46
3.2.1.	IAEA Safety Reports Series N° 54 – Accident Analysis for Nuclear Power Plants with Modular High Temperature Gas Cooled Reactors (2008)	46
3.2.2.	IAEA TECDOC 1570 - Proposal for a Technology-Neutral Safety Approach for New Reactor Designs (2007)	47

3.2.3.	IAEA-TECDOC-1487 - Advanced nuclear plant design options to cope with external events (2006)	48
3.2.4.	IAEA-TECDOC-1366 - Considerations in the development of safety requirements for innovative reactors: Application to modular high temperature gas cooled reactors (2003).....	49
3.2.5.	IAEA - Nuclear Energy Series - No. NP-T-2.2 - Design Features to Achieve Defence in Depth in Small and Medium Sized Reactors (2009).....	50
3.2.6.	INSAG-12 - Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev.1 (1999).....	51
3.3.	COUNTRY EFFORTS ON REQUIREMENT DEVELOPMENT (KAERI, RSA, CHINA, EUROPE, INDONESIA, JAPAN, USA)	52
3.3.2.	Current Licensing experience on the HTR-PM	60
3.3.3.	Licensing experience for HTGRs in the past.....	61
3.3.4.	Reactors that operated and went through some licensing process in the past (short with references, if detail in appendix reference this) Historic built, HTR-Module HTTR, HTR-10, PBMR, ...	61
3.4.	OECD/NEA GSAR (NEW NAME), GIF?	62
4.	SAFETY DESIGN CRITERIA APPROACHES	62
4.1.	APPROACH 1 (BOTTOM UP APPROACH)/ APPROACH 1 TO DEVELOPMENT OF MODULAR HTGR SAFETY DESIGN CRITERIA	64
4.1.1.	Top Level Safety Requirements	65
4.1.2.	Licensing Basis Event Selection.....	67
4.1.3.	Safety Functions	81
4.1.4.	Safety Design Criteria for the MHTGR.....	90
4.2.	APPROACH 2 (TOP DOWN APPROACH)	99
4.2.1.	Development Process.....	100
4.2.2.	Safety Function Analysis	101
4.2.3.	Functional Requirements Analysis (Objectives Provisions Tree Analysis)	104
4.2.4.	Requirements for coupling heat application facility.....	106
5.	SUMMARY OF SAFETY DESIGN CRITERIA COMPARISON FROM THE TWO APPROACHES	108
5.1.	SUMMARY AND PATH FORWARD	108
6.	DEFENCE IN DEPTH IN TERMS OF THE RADIONUCLIDE RETENTION ALLOCATION TO THE BARRIERS.....	110
6.1.	RADIONUCLIDE RELEASE BARRIERS.....	110
6.1.1.	Fuel Particle Kernel	110
6.1.2.	Fuel Particle Coatings.....	111
6.1.3.	Core Graphite and Carbonaceous Materials	111
6.1.4.	Reactor Building	113
6.2.	FRAMEWORK FOR ESTABLISHING ADEQUACY OF DEFENSE-IN-DEPTH (DID)	115
6.2.1.	Defense-in-Depth Philosophy.....	115
6.3.	FRAMEWORK FOR ESTABLISHING DID ADEQUACY	116

6.4.	INTEGRATED APPROACH FOR INCORPORATION AND EVALUATION OF DID	117
6.5.	COMPENSATORY ACTION SELECTION AND SUFFICIENCY ...	117
6.5.1.	Choosing DID Compensatory Actions	117
6.5.2.	Plant or Programmatic Changes	117
6.5.3.	DID Attributes to Achieve Plant Capability DID Adequacy.....	118
6.6.	HTR-MODULE BARRIER CONCEPT	122
6.6.1.	First Barrier	122
6.6.2.	Second Barrier	124
6.6.3.	Third Barrier	129
7.	FUKUSHIMA LESSONS LEARNED.....	132
8.	KEY R&D CONSIDERATIONS (IDENTIFICATION OF ANY RESEARCH AND DEVELOPMENT GAPS).....	137
8.1.	IDENTIFICATION OF SIGNIFICANT RESEARCH & DEVELOPMENT GAPS AND ANALYSIS METHOD VERIFICATION AND VALIDATION NEEDS.....	137
8.1.1.	United States of America.....	137
8.1.2.	Japan	138
8.2.	TEST FACILITIES NEEDED FOR THE HTR-PM.....	139
8.3.	EUROPEAN FRAMEWORK HTR PROGRAMS.....	141
8.4.	GENERATION IV INTERNATIONAL FORUM VHTR PROJECT FUTURE DEPLOYMENT.....	143
9.	SUMMARY AND CONCLUSIONS	145
9.1.	SUMMARY.....	145
9.2.	CONCLUSIONS	145
10.	APPENDICES	146
APPENDIX I.	OBJECTIVE PROVISIONS TREE ANALYSIS FROM APPROACH 2	147
APPENDIX II.	TECHNICAL REPORT: HTR-MODULE: CLASSIFICATION AND QUALITY REQUIREMENTS FOR SYSTEMS AND COMPONENTS.	156
APPENDIX III.	APPROACH 2 SPECIFIC SAFETY REQUIREMENTS FOR DESIGN OF MHTGRS	161
REFERENCES.....		162
ANNEX I.	INPUTS FROM OTHER COUNTRIES ON APPROACH 1 ELEMENTS.....	165
ANNEX II.	HTR-PM CONTAINMENT CONSIDERATIONS	177
ANNEX III.	SPENT NUCLEAR FUEL MANAGEMENT	178
ANNEX IV.	UK HAZARDS APPROACH: EXAMPLE USED ON SIZEWELL B AND THE PROPOSED APPROACH TO COMBINED HAZARDS ASSESSMENT	179

ANNEX V.	MHTGR FUNCTIONAL CONTAINMENT	182
ANNEX VI.	CONTAINMENT CONCEPT USED FOR HTR-MODULE ...	185
ANNEX VII. MODULE	LICENSING PROCEDURE CONCEPT FOR THE HTR- 187	
ANNEX VIII.	HTR-MODULE LICENSING BASIS EVENTS	196

1. INTRODUCTION / SCOPE

1.1. BACKGROUND

A0076-Paper-Reitsma_Topsafe2017_Rev1

After nearly 60 years the nuclear power industry is today dominated by water cooled reactors (WCRs), with over 90 % of electricity generation share. It therefore also makes sense that the nuclear licensing authorities are focused on WCRs and why it is the area of most interest and expertise. It follows logically that the IAEA safety requirements, that follow the best practices established in the Member States, and is agreed by Member States on the basis of consensus, are also largely developed with WCR nuclear power plants (NPP). The IAEA nuclear power plant design safety requirements [1],[2] acknowledge this as stated in the scope of the latest revision: *“It is expected that this publication will be used primarily for land based stationary nuclear power plants with water cooled reactors designed for electricity generation or for other heat production applications (such as district heating or desalination). This publication may also be applied, with judgement, to other reactor types, to determine the requirements that have to be considered in developing the design.”* are also largely developed for these nuclear power plants (NPP).

High Temperature Gas Cooled Reactors (HTGRs) is one of the advanced nuclear power systems considered for the future and also one of the systems included in the Generation IV Forum [3]. As so many other advanced reactors technologies considered for deployment, the basic concept is not new and prototype HTGR power plants have been licensed, built and operated in the past. The last two prototype nuclear power plants, Fort St. Vrain (in the USA) and the THTR-300 (in Germany), were however both shutdown in the 1980's. So the question should be asked why the topic of a safety and licensing approach need to be raised when this type of plant has been licensed and operated before. The answer is two-fold: In the last 30 years the safety and licensing requirements have been strengthened substantially but in the process it also became more light water reactors (LWR) technology specific with the consequence that it is more difficult to interpret and apply to HTGRs. The second is the change in the safety philosophy used in all modern HTGR designs, where many of the safety systems required in LWRs is made obsolete. The earlier prototype HTGR plants did not strictly adhere to this new philosophy that was really conceived only after their demise.

In the last few years more calls have been made that a new approach should be developed and followed to allow licensing of advanced reactors, especially in the USA. Efforts to develop HTGR specific safety requirements have also started. In South Africa the National Nuclear Regulator (NNR) established several pebble bed specific requirement documents and the US-NRC, in cooperation with the US-DOE, have developed and proposed general design requirements for non water cooled reactor technologies, including specific recommendations for HTGRs.

Some efforts have been made over the years to develop a germane safety and licensing approach for HTGRs. Historically most of these efforts used the well-known LWR safety requirements as the starting point and then introduced interpretations or exceptions for HTGRs. This approach is hugely based on engineering judgement and expert opinion. This approach was followed in the case of past operating HTGRs and also more recently in the licensing of the HTR-PM. A more

fundamental approach, that requires a detailed plant design and thus a substantial effort, has also been proposed. In this approach safety functions are assigned to systems, structures and components for the specific design and then high level safety requirements are derived.

1.2. HISTORICAL PERSPECTIVES ON HTGR LICENSING EXPERIENCE

A0076-Paper-Reitsma_Topsafe2017_Rev1

Several prototype and demonstration HTGRs were built and operated as shown in Figure 1. It started with the Dragon project, an OECD project hosted by UK, followed shortly after with the AVR and Peach Bottom reactors. These early prototypes were followed by two larger demonstration plants, the Fort St Vrain in the USA and the THTR in Germany. More licensing information are available for these later demonstration plants [4],[5]. The lessons learned during licensing clearly pointed towards the need for HTGR specific requirements and specifically that the coated particle fuel and its ability to contain fission products to high temperatures (and for an extended period of time) should be acknowledged. These reactors already demonstrated some of the safety principles and the large safety margins inherent in gas-cooled reactor technology.

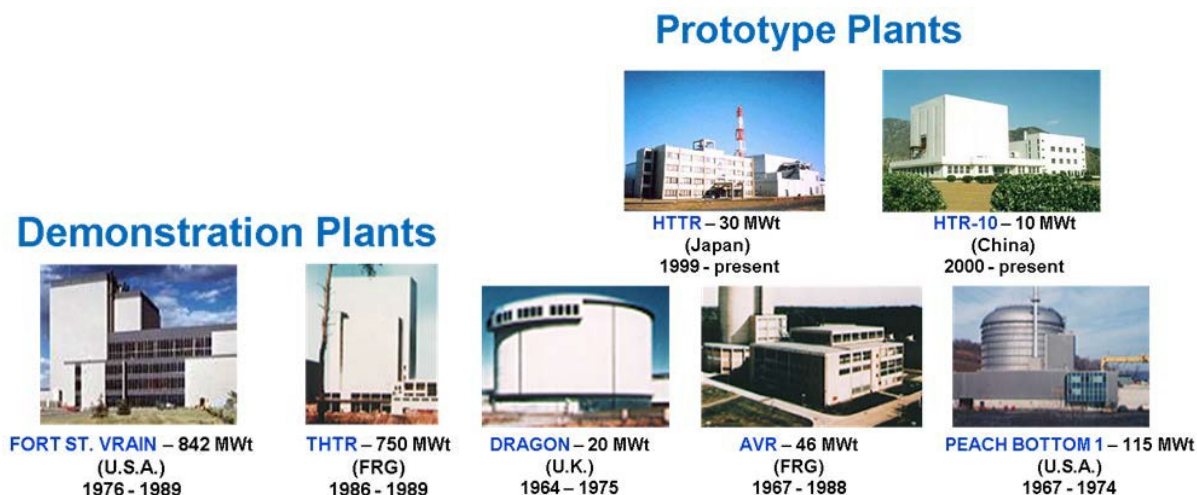


FIG. 1. The built and operated HTGR prototype and demonstration plants (past and present).

For several decades (1960's to 1980's) the nuclear power industry has suffered from uncertainty in the licensing environment and many projects were delayed due to changing requirements and licensing procedures. With the safety first culture in the nuclear industry any delays to improve safety is of course appropriate but some changes in the safety requirements were not necessarily applicable to the non-water-cooled technologies and could indeed be counterproductive. A selection of examples from the licensing of the Fort St. Vrain plant (and large HTGR) in the USA and the THTR-300 plant in Germany is given. These examples should not leave the impression that HTGR licensing in a WCR world was the main reasons for delays and eventual early shutdown of these reactors (many other factors and design issues probably played a major role). The

examples rather show the importance that HTGR specific safety requirements need to be in place to ensure success in the future. It also shows the need to have an informed regulator.

Today two smaller test reactors are still available, the HTTR in Japan and the HTR-10 in China. The licensing and operations of these reactors, especially with all the safety demonstrations already performed and planned, are making a significant contribution to the licensing efforts of future NPPs. The licensing and experience gained with the HTR-10 test reactor were excellent preparation for both the designers and regulators to prepare for the licensing of the commercial demonstration plant. The Preliminary Safety Analysis Report (PSAR) for the HTR-PM has been reviewed and accepted and construction has started in December 2012. The FSAR is being finalised and commercial operation is planned in 2018.

Other noteworthy licensing experience are available from the efforts to license the HTR Module (late 1980's) in Germany [5], the South African Pebble Bed Modular Reactor (PBMR) project from 1999 to 2010 [6][7], and licensing preparation activities with the NRC, USA that started as part of the PBMR and Next Generation Nuclear Plant (NGNP) project [8]. In the USA these efforts have now led to the release of draft advanced non-light water reactor design criteria [9] including specific criteria for HTGRs. The proposed general design criteria (GDCs) already reflect due consideration of the HTGR specific safety characteristics. These include concepts such as functional containment, a move away from the LWR emphasis on loss of cooling accidents (LOCAs), specifically mention of air and water ingress, and a distinction made between fuel design limits (LWRs) and core radionuclide release limits that takes the behaviour of coated particle fuel into account.

1.3. THE IAEA COORDINATED RESEARCH PROJECT ON MODULAR HTGR SAFETY DESIGN

The IAEA Coordinated Research Project On Modular HTGR Safety Design: Status And Outlook, Reitsma 2016

The IAEA Coordinated Research Project (CRP) on Modular High Temperature Gas-cooled Reactor (HTGR) Safety Design started in December 2014. The project investigates and makes proposals on safety design criteria by not only considering the existing water cooled reactors safety requirements for nuclear power plant design but also making use of past and current experience of HTGR licensing in the IAEA member states. Two approaches are being followed to establish the criteria. The first is to develop and apply a safety design process to specific reactor designs. The second is to use the existing IAEA specific safety requirements for designs based on water cooled reactor technology and then through expert judgement and review propose changes that is needed to make it applicable to HTGRs.

1.4. 1ST GOAL IS TO DESIGN A SAFE NUCLEAR PLANT

The IAEA Coordinated Research Project On Modular HTGR Safety Design: Status And Outlook, Reitsma 2016

Improvements in the development of nuclear power plant safety requirements for design, and the further strengthening of safety based on the lessons learned over the last 30 years, have led to improved nuclear power plant designs. All modern NPPs designs explicitly include specific design features, strategies and actions to mitigate severe accidents. These accidents were previously considered to be beyond the design basis and therefore no specific provisions were made and no systems designed to prevent or mitigate its consequences. In many cases the regulatory authorities did however ask for a selection of these severe accident cases to be analyzed. For some time these requirements have also been reflected in the IAEA Specific Safety Requirements No. SSR-2/1 Safety of Nuclear Power Plants: Design [2].

Since the inception of the philosophy of the modular HTGRs in the 1980's the salient safety features have been promoted. The claim is that the intrinsic safety characteristics and modular design minimize and, in many cases, eliminate concerns over off-site and on-site power and that typically there is no need for active safety systems or operator actions to avoid large radionuclide releases. Often the specific design solutions to fulfil the fundamental safety functions are quite different than for the current fleet of WCRs.

From a designers perspective this necessitates the development of new HTGR specific reactor design criteria. Examples of member state work to develop these requirements are available in literature in [10],[11]. In addition the need for a well-defined licensing framework in advance of licensing engagement is clear. The future licensing and deployment of HTGRs in IAEA member states will therefore benefit from the availability of technology specific safety design requirements.

INL/EXT-16-38812 (A08)(US)

The primary qualitative safety objective for the modular HTGR is not to disturb the normal day-to-day activities of the public. The corresponding quantitative objective of the modular HTGR design is to limit the dose from accidental radionuclide 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, (e.g., 400 m), from the reactor. In addition, to eliminate the need for public evacuation or sheltering beyond the site boundary, the modular HTGR design goal is to meet the Environmental Protection Agency (EPA) plume exposure Protective Action Guides (PAGs) (EPA 1992) at the EAB.

1.5. DEVELOPING MODERN REQUIREMENTS (STRENGTHENING)

The IAEA has also published and performed activities in the past to develop technology neutral but also HTGR specific guidance. A selection of this is referenced in [12],[13],[14],[15].

1.5.1. Relevance of past licensing experience in the modern licensing environment (post 9/11 and Fukushima) – Overview here (with detail in appendix such as 15hrs vs 72 hours; aircraft impact)

2. DEFINITION OF MODULAR HTGRS.

INL/EXT-16-38812 (A08)(US)

Modular HTGR History

In the 1980s, HTGR designers at the German company INTERATOM, under license to Handelsregister Abteilung B (HRB), the designer of the Arbeitsgemeinschaft Versuchsreaktor (AVR) and thorium high-temperature reactor (THTR), developed a new pebble bed design that modified the reactor system in such a way that the residual heat could be removed passively. The resulting pebble bed design was called the High Temperature Reactor (HTR) MODUL (Reutler and Lohnert 1984). For typical prior reactor designs, the reactor core height and diameter were almost equal for neutron economy reasons. However, in the HTR MODUL, the core height was three times larger than the diameter. The advantage of the slender core geometry is that if the normal flow of helium is unavailable, the residual heat can be removed radially and fully passively by natural convection, conduction, and radiation to and from an uninsulated steel reactor vessel. The disadvantages are increased neutron leakage and a higher core flow resistance.

The U.S. modular HTGR concept began in 1984 when Congress challenged the HTGR industry to investigate the potential for using HTGR technology to develop a “simpler, safer” nuclear power plant design. The goal was to develop a passively safe HTGR plant that was also economically competitive. To retain radionuclides within the coated-particle fuel during passive residual heat removal, the core’s physical size had to be limited; the maximum reactor power capacity was found to be 200 to 250 MW(t) for a cylindrical core geometry. However, this rating was projected to be not economically competitive for electric power generation. This judgment led to the development of an annular core concept with prismatic fuel elements to enable larger cores with increased power capacity. The DOE and a team led by General Atomics (GA), which included Combustion Engineering and Bechtel developed a 350 MW(t) Modular High Temperature Gas-Cooled Reactor (MHTGR) using the annular prismatic block core arrangement. Licensing activities included preapplication interaction with the NRC and the submittal of numerous documents including a Preliminary Safety Information Document (DOE 1992). The results of the NRC review were documented in a Preliminary Safety Evaluation Report (NRC 1989 and NRC 1995).

In fiscal year (FY) 2006, the U.S. DOE initiated the NGNP project at Idaho National Laboratory (INL) as directed by the 2005 Energy Policy Act (EPA 2005). The objective of the NGNP project was to demonstrate the HTGR technology to produce electricity and high-temperature heat. In FY-07, preconceptual designs of a pebble bed annular plant were developed by Pebble Bed Modular Reactor Pty Ltd. from South Africa with Westinghouse Electric Company, LLC, and prismatic annular core designs were developed by AREVA NP, Inc., and GA. These plants were designed for production of electricity and hydrogen with reactor ratings that varied from 500 to 600 MW(t) and reactor outlet temperatures of 900 to 950°C. Subsequent to the preconceptual design work, significant interaction with potential industrial end users of the modular HTGR technology along with the completion of trade studies concluded that the HTGR should be viewed as a source of high-temperature process heat that can be used to meet the energy needs of industry in several forms such as electricity, steam, high-temperature gas, hydrogen, and oxygen. This work resulted in a decision to reduce the reactor core outlet temperature and refine the configurations and

operating conditions of the pebble bed and prismatic-reactor-based plants to ensure they meet the energy needs of industry.

A03_BriVaTech-HTR-027

The major safety goal for modular HTGRs is that significant fuel failure should neither result from postulated accidents (DBAs) and as far as possible nor from other events (e.g. BDBAs).

This safety goal drives the design features that define modular HTGRs.

Design Features for Modular HTGRS

- High quality ceramic coated particle fuel
- Single phase helium coolant
- Strongly negative fuel temperature feedback reactivity
- Post shutdown decay heat removal solely through physical processes (thermal conduction, radiation, convection), because of the selection of a low mean power density in the core
- Ceramic core (low power density, large heat capacity, high thermal conductivity)
- Large margins between fuel operating temperature and temperatures that could damage the fuel

B03_JAEA report_MHTGR definition_R0

The definition of Modular HTGRs is determined as follows.

- Modular HTGRs are consists of the following fundamental elements:
 - Coated fuel particles which consist of multiple coating layers surrounding the fuel kernel,
 - Graphite for moderator and core internals,
 - Helium gas for coolant.
- Safety of Modular HTGRs is assured by following inherent and passive safety design features:
 - Large negative temperature reactivity feedback characteristic,
 - Slow and relatively small temperature transients of the core under the transient of the reactor power or a loss-of-forced cooling event,
 - Passive residual heat removal from the outside of reactor pressure vessel,
 - Radioactive confinement by robust coated fuel particles even during accidents.

The IAEA Coordinated Research Project On Modular HTGR Safety Design: Status And Outlook, Reitsma 2016

Furthermore modular high temperature gas cooled reactors refer to the HTGR designs that are based on design principles that ensure no core meltdown or significant radionuclide release are possible even in the event of depressurization of the helium coolant and loss of all active forced convection systems. The residual heat removal is ensured solely through physical processes (thermal conduction, radiation, convection). In order to achieve this, the reactor designs typically have the following properties:

- Low power density
- Long slender core and/or annular design
- A Reactor Cavity Cooling System external from the reactor to remove the decay heat
- Uninsulated reactor pressure vessel

2.1. THE INHERENT OR INTRINSIC CHARACTERISTICS OF THE FUEL, MODERATOR MATERIALS AND COOLANT.

The IAEA Coordinated Research Project On Modular HTGR Safety Design: Status And Outlook, Reitsma 2016

HTGRs have many favorable inherent safety characteristics based on a few properties:

- High quality ceramic coated particle fuel
- Single phase helium as coolant
- Strong negative reactivity coefficients
- Slow transients due to large mass of graphite in the core

A04_BriVaTech-HTR-025

The engineered configuration and nuclear design of Modular MHTGs should be such that even in the event of assumed failures of all active shutdown and residual heat removal systems, the peak fuel temperature stabilizes at time dependent accident temperatures (e.g. 1600°C). Typical limits are somewhat arbitrary, and in fact depend on the type of fuel irradiation history, manufacturing processes and many other factors. It should be noticed also that predictions of peak fuel temperatures versus time analyses often neglect to mention that only a relatively small portion of the core fuel is at or near the peak.

Sufficient margin should exist between the peak fuel temperature and the temperature at which additional fuel failures are conservatively assumed to occur, and that the core temperature coefficient has enough negative reactivity to shut down the reactor and stop further temperature increase. This safety margin is possible, if a nominal temperature differential of approximately 700K exists between the maximum allowable fuel temperature and the maximum operating temperature of the fuel elements in the reactor cores. This should be also true even in the presence of accident induced excess reactivity, e.g. water ingress.

Furthermore, residual core heat can be dissipated from the reactor to the surrounding components, structures and surfaces solely through natural physical processes. These include thermal conduction, radiation, and convection. The design choices of low mean power density in the reactor core, the geometric design of the core and the surrounding core internals, and the use of suitable materials, make this inherent (i.e. natural) core decay heat removal characteristic possible.

Modular HTGRs normally include active operational systems for residual heat removal. These active systems are normally used to limit loadings on the passive heat removal components and structures. In addition, system, structure, and component (SSC) design margins are selected such

that active systems may fail to operate for several hours, the allowable design limits of for the SSCs are not exceeded and the passive engineered safety features will respond in ample time.

For Modular HTGRS the selection of the primary system, core design and material should reduce the safety requirements on the water/steam cycle and the startup and shutdown systems, so that these systems can be designed and operated as purely conventional plant systems.

A04_JAEA report_Safety features_R0

This report provides the safety features of Modular HTGRs.

As the name implies, LWRs use light water for both the coolant and the neutron moderator. In contrast, Modular HTGRs use helium for the coolant and high-purity graphitic and other carbonaceous materials for the moderator. If an accident causes loss of the helium coolant, the graphitic/carbonaceous materials remain and provide a large capacity to absorb the residual nuclear decay heat. That, combined with the relatively low power density of Modular HTGRs relative to LWRs, results in a much slower heat up of the nuclear fuel during a loss-of-coolant accident.

A key design feature of Modular HTGRs that allows for high-temperature operation is the use of ceramic, coated fuel particles (CFPs). A typical CFP design consists of a microsphere (“kernel”) of nuclear fuel (usually in the form of an oxide, carbide, or oxycarbide) that is coated with multiple layers of pyrolytic carbon and silicon carbide. A coating structure in current use is referred to as a TRISO coating. The TRISO coating is an engineered structure and consists of a low-density carbon buffer layer that surrounds the kernel, followed by a high-density inner pyrolytic carbon (IPyC) layer, a silicon carbide (SiC) layer, and a high-density outer pyrolytic carbon (OPyC) layer. The size of a CFP is determined by the diameter selected for the kernel and the thicknesses selected for the coating layers, with an overall diameter typically on the order of one millimeter or less. Nuclear, mechanical, thermal, and safety performance considerations are factored into the design of the CFP. CFPs with TRISO coatings have been independently developed in several countries and have been successfully utilized in several research and demonstration HTGRs.

For a typical Modular HTGR core design, the CFPs are consolidated into high-purity graphitic fuel elements that are cooled by flowing helium at high pressure. Fuel element designs include spherical pebbles and prismatic blocks with a fuel-free zone or web that precludes direct contact of the helium coolant with the CFPs. The TRISO coating is designed to act as a micro-containment structure for very high retention of radionuclides during both normal operation and severe accidents.

A typical Modular HTGR core will contain billions of CFPs. The Modular HTGR safety design approach places primary emphasis on the CFP itself (especially the coating structure) for containment of radionuclides, even during severe accidents. Much less emphasis is placed on other barriers, including the fuel element, the primary coolant pressure boundary, and containment structure (called confinement or reactor building). In contrast, LWR fuel is designed for high retention of radionuclides during normal operation, but the LWR design basis allows for very high levels of fuel failure (fuel melting) and radionuclide release from the fuel during severe accidents.

During unmitigated severe accidents, the LWR containment structure is the primary barrier to radionuclide release and is designed as a high-pressure containment structure for that purpose.

For Modular HTGR, the radionuclide source term during unmitigated severe accidents can be split into a prompt component and a delayed component. As an example, a large break in the primary coolant pressure boundary is postulated, resulting in a rapid depressurization and loss of coolant. The prompt source term would consist of the small amount of radioactivity in the primary circulating coolant and some fraction of the primary circuit plateout activity that may be re-entrained into the coolant as the result of high surface shear forces during the depressurization. This prompt source term is released into the containment structure over a period of seconds to minutes, but represents a small fraction of the total source term over the course of an unmitigated accident. The delayed source term derives from the slow heatup of the core and typically occurs over a period of several days. The delayed component of radionuclide release results primarily from the very small fraction of exposed fuel kernel material, which includes residual fuel contamination leftover from manufacturing and any defective CFPs that escape quality-control screening and fail during operations or during the slow heatup transient.

The characteristics and timing of the radionuclide source term during an accident can affect the design approach for the containment structure. Modular HTGR containment structures are typically designed to vent at relatively low differential pressure. This design approach has been shown to reduce the overall radiological consequences of the accident by preventing a high differential pressure driving force that could release radioactivity that has built up over a long period of time in the containment structure atmosphere as a result of the slow heatup. Imposing a high-pressure containment structure for the Modular HTGR containment structure is an example of an LWR safety design requirement that could be counterproductive for the Modular HTGR.

The allowable fractions for contamination and defective CFPs are major design criteria derived from assessments of operational states and accidents. These assessments include evaluations of the radiological consequences with respect to the regulatory criteria. The actual fractions for contamination and defective CFPs are measured on a batch-to-batch basis as part of the fuel manufacturing quality control program. A fundamental requirement for fuel quality is the actual contamination/defect fractions must be less than the allowable contamination/defect fractions, with some margin to account for uncertainties. The allowable fractions will depend on both the performance (failure rates) of CFPs during operations and accidents and on the level of credit taken for retention provided by barriers outside the fuel, including the fuel element, the primary circuit pressure boundary, and the containment structure. A design goal for the Modular HTGR is to minimize the level of credit required for barriers outside the fuel in order to meet design and regulatory requirements. If credit for these barriers is required, the level of retention must be quantified through analysis and/or testing.

The Modular HTGR safety design philosophy is based on using only inherent safety design features and passive Structures, Systems, and Components (SSCs) to perform the required safety functions. Examples of inherent and passive safety design features for major safety functions for Modular HTGRs are summarized in Table 1. Examples of inherent safety design features include the core design with negative temperature coefficients of reactivity under all conditions, low power density, large core heat capacity, high thermal conductivity, and the core heat removal capability

by radiation and convection from outside reactor pressure vessel, the selection of materials with high-temperature capability for CFP and reactor internal components, and the selection of chemically and neutronically inert, single-phase helium for the primary coolant. The selection of low oxidation rate high-quality graphite and the protective film formation on SiC of CFP are example of inherent design features for control chemical attack. The CFPs are examples of passive structures. Example of passive systems are a gravity-driven reactor shutdown system and a natural convection Vessel Cooling System (VCS) that operates continuously and removes decay heat during accidents to keep fuel, reactor vessel, and containment structure temperatures well below failure/damage thresholds. Studies have shown the Modular HTGR can be designed with appropriate inherent safety design features and passive SSCs to prevent significant levels of fuel failure during severe accidents when both active and passive cooling systems are compromised, e.g., the decay heat can be dissipated at sufficiently high rates even if the VCS is nonfunctional as the result of damage and/or flow blockage.

TABLE 1. SAFETY FEATURES OF MODULAR HTGRS

Safety Function categories	Reactivity control function	Core heat removal function	Chemical attack control function	Radioactive material containment function
Inherent safety design features	• Large negative temperature reactivity feedback	• Low power density • Large core heat capacity • High thermal conductivity • Radiation and convection from outside reactor pressure vessel	• Low oxidation rate of high-quality graphite • Protective film formation on SiC of coated fuel particle	• High thermal resistance and high confinement performance of coated fuel particle • High thermal resistance of core internal • Chemically and neutronically inert helium coolant
Passive safety design features (Passive SSCs)	• Gravity-driven reactor shutdown system	• Natural convection vessel cooling system	• Reactor coolant pressure boundary • Confinement (reactor building)	• Ceramic coated fuel particle • Graphite fuel element • Reactor coolant pressure boundary • Confinement (reactor building)

SSCs: Structures, Systems, and Components

INL/EXT-16-38812 (A08)(US)

To achieve the safety objectives for the modular HTGR, the design relies on inherent and passive safety features. Modular HTGRs use the inherent high temperature characteristics of tristructural isotropic (TRISO)-coated fuel particles, graphite moderator, and helium coolant, along with passive heat removal capability of a low-power-density core with a relatively large height-to-diameter ratio within an uninsulated steel reactor vessel to assure sufficient core residual heat removal under loss-of-forced cooling and/or loss-of-coolant-pressure conditions.

The primary radionuclide retention barrier is the set of ceramic coating layers surrounding the fissionable fuel kernel to form a fuel particle. As shown in Figure 2, these coating layers include

the inner pyrocarbon (IPyC), silicon carbide (SiC), and outer pyrocarbon (OPyC), which together with the buffer layer constitute the TRISO coating. The coating system constitutes a miniature pressure vessel that has been engineered to provide containment of the radionuclides and gases generated by fission of the nuclear material in the kernel. Thousands of these TRISO-coated particles are bonded in a carbonaceous material into either a cylindrical fuel compact for the prismatic HTGR or a spherical fuel element for the pebble bed HTGR. These fuel particles can withstand extremely high temperature without losing their ability to retain radionuclides under all accident conditions. Fuel temperatures can remain at temperatures up to 1800°C for several hundred hours without loss of particle coating integrity (INL 2010a). This high temperature radionuclide retention capability is the key element in the design and licensing of modular HTGRs.

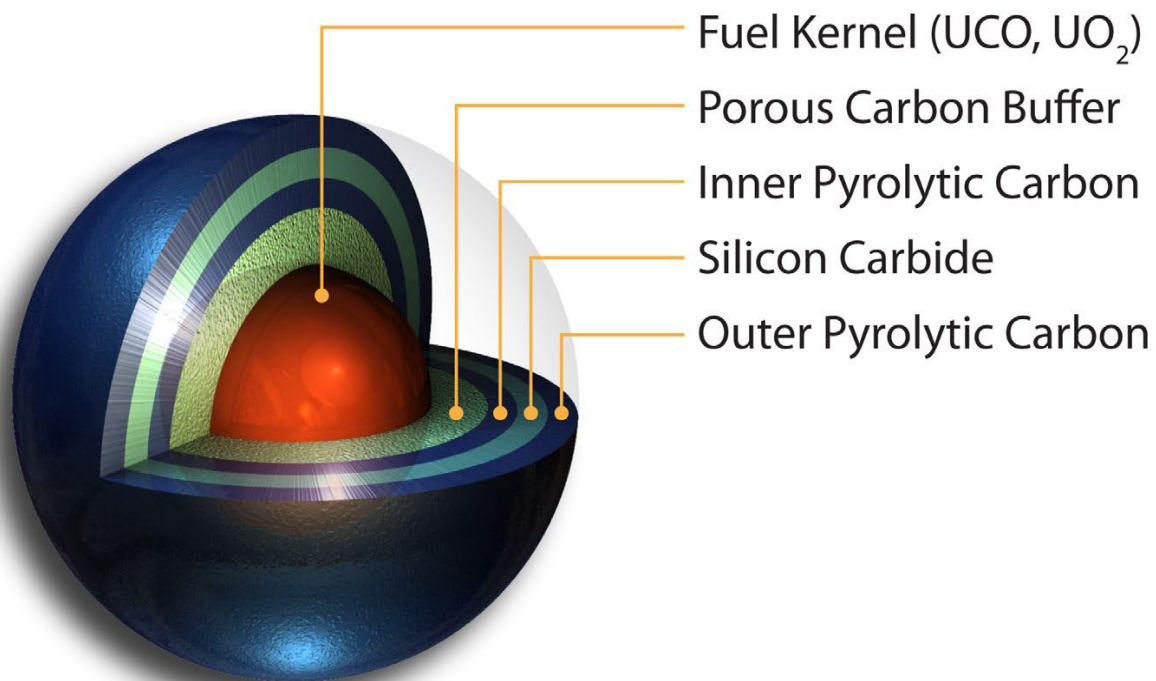


FIG. 2. TRISO-coated fuel particle cross section.

Graphite can withstand even higher temperatures than the fuel without structural damage, which complements the fuel's high-temperature capability. Massive graphite structures in the core provide an extremely large heat capacity. The high heat capacity and low power density of the core result in very slow and predictable temperature transients. In addition, the strength of graphite increases with temperature over the full range of temperatures applicable to the modular HTGR. The long mean free path of neutrons in graphite provides a neutronic stable core. The graphite also holds up the transport of certain radionuclides, further reducing potential release from the core.

Helium is chemically inert and neutronic transparent, meaning it will not aggravate an accident by participating in any chemical or nuclear reaction. Helium will not change phase in the reactor; therefore, it is impossible to have problems of two-phase flow within the reactor, which would

affect reactivity and temperature control. The use of helium minimizes the problems of primary system corrosion and greatly reduces the resultant buildup of radioactive byproducts associated with water-cooled reactors.

The large negative temperature coefficient of modular HTGRs, along with their large thermal margins, provide for an inherent shutdown capability to deal with failures to scram the reactor as demonstrated in AVR and HTR-10 testing. Gravity-driven and diverse reactivity control systems provide further confidence of the ability to shut down the reactor. The low power density, large heat capacity, and large thermal margins also allow the reactor to reach as high as 200% power during reactivity insertion accidents without significant changes in fuel temperature.

The concrete walls surrounding the reactor vessel are covered by panels that remove the heat radiating from the reactor vessel. These panels are a key part of the Reactor Cavity Cooling System (RCCS) used in modular HTGR designs. The RCCS can be air-cooled or water-cooled. Both designs have a passive cooling capability that does not rely on electric power.

No alternating current (AC) powered safety systems and no operator actions are required to respond to any of the accident scenarios that have been postulated for the modular HTGRs throughout their licensing history. In addition to requiring no operator actions, the design is insensitive to operator errors.

2.2. SAFETY DESIGN FEATURES.

The IAEA Coordinated Research Project On Modular HTGR Safety Design: Status And Outlook, Reitsma 2016

These safety features and design principles are well known in the HTGR community but a detailed understanding is essential to comprehend and carefully evaluate the proposed amendments to the existing WCR design requirements. Some design and safety aspects are therefore highlighted below.

2.2.1. Coated Particle Fuel

The TRISO (triple isotropic) coated particle (CP) fuel is capable to contain almost all fission products for the expected operating and postulated accident temperatures in a modular HTGR. The core design and operating parameters ensure large margins between these temperatures and temperatures that could damage fuel. No large early release of fission products due to coated particle failure is therefore possible (no credible conditions).

The failure mechanisms of CP fuel are decoupled and totally independent. One coated particle failure cannot lead to the failure of a neighboring CP, as it is driven by the maximum fuel temperature. A CP failure also has no effect on the cool-ability of the fuel as a failure will not change the heat removal path. The amount of fission products that can potentially be release when a failure occurs is of course very small, and many CP will need to fail to be of any consequence. In this respect it is very different from WCR fuel where one pin failure can inhibit the cooling of neighbors and cause significant additional failures or a partial core melt.

2.2.2. Helium as Primary Coolant

Helium under high pressure (typically 4 – 9 MPa) is used as the primary system coolant or heat transfer medium. Since it is an inert noble gas it does not undergo any phase change and has a very low chemical reactivity. It is also invisible to neutrons, with basically no core reactivity effect. Another favorable characteristic is the high heat transfer coefficient with no heat transfer limits.

Unlike in the case of loss of coolant in WCRs, helium, when leaked out of the primary pressure boundary, does not condense. In a sealed containment this will lead to a sustained elevated pressure that cannot be reduced by cooldown. The sustained high pressure can serve as a driving force for the larger delayed release as fuel temperatures increases.

This requires a different approach to the containment function and specifically the reactor building requirements.

2.2.3. Reactivity and Reactor Shutdown

The modular HTGR designs have a negative temperature coefficient of reactivity over the complete operating and accident temperature range. The individual effects of these coefficients are as follows:

- The Doppler or fuel temperature coefficient acts promptly. This effect stabilizes the nuclear chain reaction.
- The moderator coefficient effects is very slightly delayed as the heat is transferred from the very small kernels to the surrounding graphite material.
- The reflector temperature coefficient, that may be positive, has a delayed effect since its temperature changes are not strongly coupled to power changes in the fuel. Temperature changes induced by changes in the coolant temperature will be slow due to the large thermal capacity and mass of graphite.

In general either by on-line refueling (as for pebble bed designs) or by the use of burnable poisons (some prismatic designs) the modular HTGR has a relatively low excess reactivity that also reduce the safety demands on the reactivity control and shutdown systems.

2.2.4. Core Thermodynamic Characteristics

Even though the typical modular HTGR is quite low in power (typically 100-600MWth) the reactor vessels are quite large due to the low power density, large graphite moderated cores and the thick graphite reflectors used. The large mass of graphite, with its high heat capacity, causes very slow core temperature changes and thus very slow transient response. Combined with the large temperature coefficient of reactivity this makes for benign behavior and enough time for the operators to respond. For example in the case of loss of forced circulation accident scenarios the fuel temperature will only reach its peak after days, and then slowly reduce.

2.2.5. Residual Heat Removal

Modular HTGRs typically rely on passive residual heat removal if none of the active systems are available. This will be the case independent if the helium coolant is still present in the primary system or has been lost. From a safety case perspective the post shutdown decay heat removal is solely through physical processes (thermal conduction, radiation, convection). The decay heat is dissipated from the core through the reactor structures to the uninsulated reactor vessel and then primarily by radiation to the reactor cavity cooling system (RCCS) on the outside. This is a natural process that does not require any coolant or engineered system to function. (This does not mean that an active system may not be included in the designs but these are not needed in the safety argument).

This approach can be followed based on the selection of a low mean power density, long slender cores and the materials selected. The maximum fuel temperatures will increase slowly over days but is limited to values where a large margin is still maintained to fuel-damage temperatures where any large amount of fission products may be released.

Typically the maximum accident temperatures are kept well below temperatures at which point fission product retention of some coated particles may be challenged or coating may fail, even though it will only lead to a small amount of fission products to be released into the graphite matrix. The failed coated particles can only be described as a statistical process and typically in fuel tests these failures only occur if these high temperatures are maintained for a long time (several 100 hours). More importantly only a very small fraction of the fuel (typically < 5%) will be at these high temperatures, while the rest of the fuel is substantially cooler.

The RCCS may be active or passive; water or air cooled; and is typically a safety system credited in analysis. It could be possible for some designs to show that the natural dissipation of the heat through the core cavity concrete structures (to the surroundings) may be adequate and that the RCCS is not needed for safety. It has been shown that the maximum fuel temperature, and thus the potential release of fission products from the fuel, is only weakly dependent on a functioning RCCS. Some designers classify the RCCS as investment protection since it is important to keep the reactor vessel material temperature within limits (and not shorten its life), and also protects the concrete (behind the RCCS) from elevated temperatures. It may also be a cost effective choice to avoid exotic material choices for the reactor vessel or the need for special high temperature concrete.

2.3. STRONG MOTIVATION ON THE DIFFERENCES OF MHTGRS (CLIFF EDGE, NO COMMON MODE; LOOK AT MATERIAL IN PAPERS RELATED TO HTGRS; HTR2016 PAPER)

A0076-Paper-Reitsma_Topsafe2017_Rev1

THE MODULAR SAFETY APPROACH

This principle of a modular design in HTGRs was first introduced by the designers of the HTR-Module in the 1980's [5]. This design approach has been universally adapted in some form by the

high temperature reactor community. The design must ensure that no early or large fission products release is possible under any credible event, including the total loss of the coolant. This drives the design features that lead to the following principles:

- use of high quality ceramic coated particle fuel that contains the vast majority of fission products to a very high temperature and for a long time (several hours) at these temperatures
- a long slender core with adequate heat loss through the reactor outer structures so that decay heat is removed by all-natural means relying only on radiation, conduction and convection and with no need for the coolant to be present
- a low power density so that the fuel temperature rise is limited in an event where all active cooling and coolant are lost, so that the maximum fuel temperature will, with some margin, remain below a value where most fission products are contained in the coated particles
- use of an inert coolant such as helium with no phase changes, no heat transfer limits and with insignificant neutronic interactions
- strong negative temperature reactivity feedback coefficients
- relative large core with ceramic core internals that have a large heat capacity that lead to slow response times and thus long and gradual temperature transients

One very important characteristic of the coated particle (CP) fuel and fission product retention in HTGRs is worth highlighting: “The failure mechanisms of CP fuel are decoupled and totally independent. One coated particle failure cannot lead to the failure of a neighboring CP, as it is driven by the maximum fuel temperature. A CP failure also has no effect on the cool-ability of the fuel as a failure will not change the heat removal path. The amount of fission products that can potentially be release when a failure occurs is of course very small, and many CP will need to fail to be of any consequence. In this respect it is very different from WCR fuel where one pin failure can inhibit the cooling of neighbors and cause significant additional failures or a partial core melt.” [6].

In contrast the argument is quite different for WCRs as highlighted by Carlson et.al in reference [7]: “The safety terrains of today’s operating light water reactors (LWRs) are generally well understood. They are terrains that can be reasonably described as featuring a number of cascading “cliff edge” effects (e.g., core uncover leading to massive core

damage, vessel failure, and containment breach). Such cascading effects have long been predicted to appear over a range of postulated severe events and most notably did appear in the historic events of the Fukushima Daiichi accident of March 2011.”

When applying the design principles for modular HTGRs it results in NPP designs where no active cooling or safety systems are required to perform decay heat removal. The helium coolant also does not need to be present. This then further excludes the need for cooling and coolant injection systems, the need for secured emergency power (in the case of station black-out), or the need for

severe accident mitigation systems (like a core catcher) introduced in other designs in case the engineered decay heat removal safety systems fails. For modular HTGRs the residual heat removal is ensured solely through physical processes (thermal conduction, radiation, convection) and concepts such as core melt or severe core damage is not appropriate.

The modular HTGR design approach also incorporates many of the lessons learned from the earlier (typically higher power) designs. For example the large core diameter of the THTR-300 core required in-core control and shutdown rods, a design that led to damaged fuel spheres. A smaller diameter core allows control and shutdown of the reactor with neutron absorbers located only in the outer reflectors. The larger power reactors also required active cooling to remove decay heat and maintain acceptable vessel temperatures (pre-stressed concrete in many designs). The move has therefore been towards smaller reactor units (100-600 MWth) that can be deployed as a multi-module power plant if higher output is required.

The HTGR designs also face other design and safety challenges. The two postulated accidents that may lead to a significant increase in the fission product release from the core are water ingress and massive air ingress with the consequential graphite oxidation that may expose the coated particle fuel. As in the case of other technologies design choices are made to prevent or limit the consequences of these effects. The amount of water that may leak into the core from the steam generator can be limited but water vapour will lead to additional release of fission products from fuel, especially from any damaged coated particles. The “diving bell” concept was used in the HTR-Module [5] design to limit any large penetrations at the top of the reactor and thus to prevent any chimney effects in case of a primary helium pressure boundary failure and air ingress.

From the few examples discussed in this section it should be clear that the physical phenomena and safety approach for modular HTGRs are substantially different from that of the current fleet of WCRs. This should be enough to warrant discussions and ultimately acceptance that HTGR specific safety requirements and licensing approach are needed. Many more examples can be given but all of these have been highlighted before. Perhaps the most controversial discussion and difference in opinion are normally around the need for containment (not the containment function that is clearly required but rather the containment structure). Some more words on this later.

The IAEA Coordinated Research Project On Modular HTGR Safety Design: Status And Outlook, Reitsma 2016

Many reactor designs today incorporate passive safety systems but others also make the distinction of inherent features or natural physical behavior. The debate if modular HTGR should explicitly add such requirements. For example, requirements may be written as: “The reactor core of the nuclear installation shall be designed with inherent safety design features.” This could be expanded further to include all the inherent characteristics of modular HTGRs described above. Others participants feel that in a WCR dominated world the minimum changes should be made to SSR-2/1 (perhaps with some interpretations suggested) and that no specific additional requirements related to inherent safety design features should be added.

If the additional modular HTGR specific requirements are added the following areas will probably be addressed:

- Maintaining the heat removal path (from the fuel to the coolers)
- Functional containment (nested and independent)
- More requirements on fuel and coated particles
- Chemical attack (air / steam)
- Multiple units and co-location industrial plants

The established approach (as reflected in the latest safety requirements) is to include specific design features, strategies and actions to mitigate severe accidents. This has been included in the modular HTGR safety design philosophy from the start (the 1980's). The safety approach is however quite different as explained before [46]: “No fuel failure for loss of coolant flow and coolant accidents, or for all foreseeable reactivity events, even with no corrective actions”.

The latest definition of plant states (see Figure 3) introduced “design extension conditions” with a sub-category of “with core melting”. It is still unclear to the modular HTGR community how this should be interpreted or if it should be redefined in the proposed safety requirements. Similarly many other concepts and text in the safety requirements are difficult to interpret or rewrite especially since they have entrenched connotations (and design solutions) for WCRs.

With the inherent fuel and reactor core characteristics that exclude core melting the focus of these mitigation strategies is naturally quite different than for WCRs where designs may for example include a “core catcher”. For modular HTGRs one example of an accident, with very low probability, that may be included under design extension conditions, may be systems or mitigation strategies to limit massive air ingress. Despite a very low probability to occur, if not prevented by design, the accident may lead to significant fission product releases above the regulatory limits.

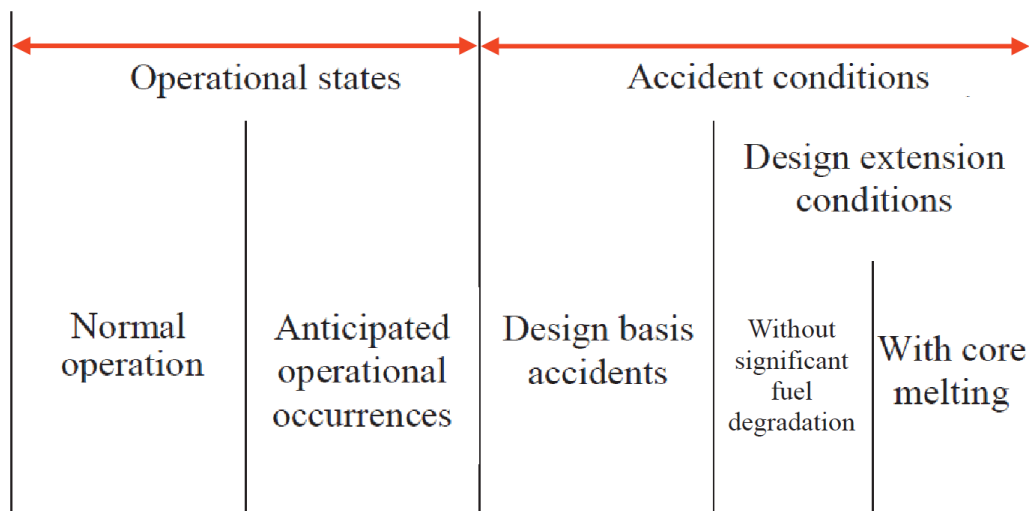


FIG. 3. Definition of plant states (considered in design) [2] including design extension conditions with core melting.

The older approach still followed in NS-R-1 [25] was more general and applicable to modular HTGRs. “Certain very low probability plant states that are beyond design basis accident conditions and which may arise owing to multiple failures of safety systems leading to significant core degradation may jeopardize the integrity of many or all of the barriers to the release of radioactive material. These event sequences are called severe accidents.”

The affected requirements and paragraphs are: ¶4.13A, §13 (¶5.1d), §20 (especially ¶5.30), and ¶6.44B.

The design extension conditions as defined as a high level requirement may be applicable with interpretation to modular HTGRs but it is felt that it has very strong underlying meaning for safety experts and the industry that automatically hint at specific design solutions in WCRs (prevent core melt, to maintain the integrity of the leak-tight containment, inclusion of a core catcher, etc.). It is therefore felt that this requirement is not applicable to modular HTGR, and needs to be redefined.

2.3.1. Control of Reactivity

§6.6. *The maximum degree of positive reactivity and its rate of increase by insertion in operational states and accident conditions not involving degradation of the reactor core shall be limited or compensated for, to prevent any resultant failure of the pressure boundary of the reactor coolant systems, to maintain the capability for cooling and to prevent any significant damage to the reactor core.*

The overall negative temperature coefficient of reactivity was explained in Section III.C. In addition, if an indirect cycle is employed and water or steam ingress a possibility, the heavy metal loading of the fuel may need to be limited to reduce the reactivity effect and power increase (in an under moderated system). The mass of water can also be limited by design features such as isolation and steam dumping. Excess reactivity and load follow requirements can also affect the maximum reactivity that can be inserted by the accidental removal of control rods.

The §46 for reactor shutdown has undergone subtle changes from NS-R-1 to SSR-2/1 although the main requirement is more or less the same: *Means shall be provided to ensure that there is a capability to shut down the reactor of the nuclear power plant in operational states and in accident conditions, and that the shutdown condition can be maintained even for the most reactive conditions of the reactor core.*

In NS-R-1 ¶6.15 read: “At least one of the two systems shall be, on its own, capable of quickly rendering the nuclear reactor subcritical by an adequate margin from operational states and in design basis accidents, on the assumption of a single failure. Exceptionally, a transient recriticality may be permitted provided that the specified fuel and component limits are not exceeded.”

The latest SSR-2/1 ¶6.7 reads: *The effectiveness, speed of action and shutdown margin of the means of shutdown of the reactor shall be such that the specified design limits for fuel are not exceeded., and*

¶6.7 *At least one of the two different shutdown systems shall be capable, on its own, of maintaining the reactor subcritical by an adequate margin and with high reliability, even for the most reactive conditions of the reactor core.*

In general modular HTGRs have two independent (normal and reserve) shutdown systems. Some designers propose that the large negative Doppler coefficient combined with the helium circulator trip should be credited as a shutdown mechanism. It is relatively fast and will keep the reactor subcritical for a considerable time period as the core heat up and then (due to the large heat capacity) cool down slowly. This was in fact the standard procedure during AVR operations and always used when a regular shut-down of the reactor was intended.¹⁹ “The rods first remain in their normal position. They are only moved into the core after some time, - when the core has cooled down substantially.” It is also consistent with the residual heat removal approach where core heat-up takes place.

The passive shutdown was also demonstrated in the HTTR and the HTR-10 (also for the more severe case with a single control rod withdrawal at normal speed). Re-criticality at low power will eventually occur after a long time but the power level will remain small (will be equivalent to the heat removal through the RCCS at that time). At these low power conditions no limits on fuel or components will be exceeded.

It is unclear if this approach can fulfil the new requirement (when the re-criticality allowance was removed). The advantage of having adequate time to take further action is also an aspect that is not credited in the shutdown requirements. Provided that heat is not actively removed from the core (i.e. circulator trip for example) the core will remain sub-critical for several days without any operator action or shutdown system action. As in other areas the availability of substantial time (to act) should be important (and should be credited).

Finally the definitions of some concepts such as controlled state and shutdown state needs to be carefully considered (sub-criticality margin, core average temperature, and zero xenon state). This is also closely coupled to the definition of the most reactive condition and aspects such as maintenance temperatures.

2.3.2. Heat Removal (and Reactor Coolant Systems)

The design of the reactor coolant system and the heat removal during normal operation and accident conditions are closely intertwined. Whereas the presence and availability of water for cooling is critical for WCRs, it is not the case for the helium in modular HTGRs.

A part of §47: Design of reactor coolant systems - that prevent the loss of coolant (¶6.13), or to control the inventory, temperature and pressure (§49) is not relevant and needs to be removed or updated. The same apply to the emergency cooling of the reactor core (§52 ¶6.18-6.19).

Requirements on the overpressure of the coolant pressure boundary (§48) is applicable but the second part of the requirement: “*and will not lead to the significant release of radioactive material from the nuclear power plant directly to the environment*” although applicable may need some thought. Some designs may vent directly to the environment (via the stack) in the case of a large

over pressurization (opening of pressure relief and safety valves) but can show that the release to the environment will be far below limits, and this can be assured since the circulating activity (during normal operations) can be monitored. This was the case with the HTR-Module design, but others argue that this is not acceptable.

Other requirements on the limits to the release of the activity in the coolant and aspects such as the cleanup of coolant are largely applicable.

Some additional requirements not applicable to WCRs should be added:

- The primary coolant circulators shall be designed to be stopped under the specified conditions and not to be restarted to ensure the appropriate design limits are not exceeded during anticipated operational occurrences or accident conditions. (this requirement is critical also for reactivity and confinement of reactivity as it prevents unexpected cooldown and possible corrosion by air ingress)
- Whereas the function to maintain the helium coolant is not so critical, the pressure boundary design and layout must limit the possibility of air ingress and consequent corrosion.
- Also, if a design relies on a secondary coolant system with water or steam, specific requirements must also be added to prevent and limit possible water and steam ingress. In addition this limits any reactivity effects and chemical attack on fuel and graphite structures needs to be controlled.

In as far as the removal of residual heat from the reactor core concerned; §51 states: *Means shall be provided for the removal of residual heat from the reactor core in the shutdown state of the nuclear power plant such that the design limits for fuel, the reactor coolant pressure boundary and structures important to safety are not exceeded.*

Although this requirement is generic and appropriate a strengthened requirement is being considered. Passive means shall be provided to remove the core residual heat from the outside surface of the reactor vessel by radiation and natural convection and transfer it to the ultimate heat sink. This should specifically apply in accident conditions (especially loss of all coolant). This is aligned with the reliance on the RCCS external to the reactor for which some requirements may also be needed.

2.3.3. Confinement of Radioactive Material

The fundamental function to confine radioactive material shall be ensured for all plant states and includes shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.

This function and the application of defence in depth (as far as the multiple barriers to the release of radioactive material is concerned) are closely related

¶4.11. *The design:*

(a) Shall provide for multiple physical barriers to the release of radioactive material to the environment;

For the designers of modular HTGRs it is clear that the requirements in the “Containment Structure and Containment System” (§54 – 58; ¶ 6.20-6.30) needs major revision to reflect the different approach where the emphasis is placed on the coated particle fuel as the most important and ultimate barrier to fission product release. Also, since helium is not condensable the only way to reduce the pressure (and driving force to transport the larger delayed release from fuel) is to do venting in some form.

Despite the requirement text that read “*to ensure, or to contribute to, the fulfilment*”, it is clear from the rest of the detailed requirements that a leak tight containment is described. The terms confinement or functional containment is often used in the HTGR community while others define it as “vented low pressure containment with a defined leak rate”. One could use this definition and fulfill the requirements as stated. With venting and a relative high leak rate the detailed requirements on aspects such as penetrations, testing of the leak rate (now at the low design pressures), and aspects such as access and control of containment conditions must still be fulfilled. So, although this may be an option, requirements that more accurately describe the modular HTGR safety philosophy would again be more appropriate.

Some additional functions should once again be added. The confinement / containment system shall ensure, or contribute to:

- the limitation of air ingress into the reactor core at depressurization accidents
- control of carbon monoxide

The containment function of the coated article fuel and many aspects associated with it must also be addressed (the CP leak rate is not testable and inspectable in the same way as a containment building)

In the requirements the containment system are also assigned other functions (in addition to confinement) that may be fulfilled by other systems or structures. The protection against external events are the function of the reactor building while the reactor cavity concrete structure for example has the function of radiation shielding (for the reactor).

2.3.4. Multiple Plants or Units (and Co-Location)

In SSR-2/1 (Rev 1) some aspects of multiple plants or units are already addressed. The requirements have been strengthened for external hazards in §17 ¶5.15B. *For multiple unit plant sites, the design shall take due account of the potential for specific hazards to give rise to impacts on several or even all units on the site simultaneously.*

In case of modular HTGRs co-located with other facilities, such as process heat users, it is important that the responsibilities for the interfaces among reactors and process heat facilities be

clearly defined. Adequate features shall be provided to isolate the hazards - for example from a hydrogen facility.

For multi-unit modular HTGRs (as in the case of Small Modular Reactors (SMR) in general) interpretation of requirements for operators and control rooms are under discussion. Although the definition of nuclear power plant includes multi-unit plants some interpretations is needed for multiple units. One example is two or more reactors coupled to a single power turbine (such as the HTR-PM) but others may operate independently but may share some systems (the 12-unit NuScale SMR).

¶5.53. *The design for a nuclear power plant shall specify the minimum number of operating personnel required to perform all the simultaneous operations necessary to bring the plant into a safe state.*

In the NuScale design all the (independent) modules are to be managed from a single control room (the number of reactors per operator is under discussion), whereas in the HTR-PM the two reactors cannot be operated totally independently (since they are coupled via the secondary system). Up to six reactors coupled to a single power turbine are envisaged for the next commercial deployment.

The same applies to the supplementary control room (§ 66) that may be strengthened: For multi-unit plants the strategy for sharing a supplementary control room shall be established (to comply with national regulatory practices). If multiple reactor units are feeding a single power turbine the merits to have one or multiple supplementary control rooms also needs to be clarified. Similarly the strategy for sharing an emergency control center shall be established.

§33: *Safety systems, and safety features for design extension conditions, of units of a multiple unit nuclear power plant*

Each unit of a multiple unit nuclear power plant shall have its own safety systems and shall have its own safety features for design extension conditions.

5.63. *To further enhance safety, means allowing interconnections between units of a multiple unit nuclear power plant shall be considered in the design.*

In the case of more than one large WCR units in a nuclear power plant, the requirements are clear. For smaller multi-unit plants again some examples to consider. The 12 NuScale units are placed in a single reactor pool and this creates such a large reservoir of water that in case all off-site power is lost the passive boil-off can maintain decay heat removal without the need to add water. This salient safety feature may not fulfil the requirement that each unit must have its own safety system.

In a modular HTGR power station with multiple plants it may also be advantageous to share the over-pressure release paths to the stack and filter system since this increases the total expansion volume and thus decreases helium flow rates that will increase filter efficiency. The HTR-Module¹⁶ also suggested the sharing of the post-accident cleanup system (for more efficient water moisture removal). It is not clear if ¶5.63 could be interpreted to allow the above design examples.

Finally considerations for the sequential construction of multiple reactor units (or even installation in one building), needs to be addressed.

2.3.5. Fuel Requirements

The different fuel design of modular HTGRs, especially in the case of the pebble bed fuel, is one obvious area where the requirements need interpretation or redefinition. Concepts such as fuel elements and assemblies are not used or would mean something else. Requirements should be placed on the coated particle fuel and complemented by requirements on the fuel spheres / prismatic fuel assemblies.

The following was suggested:

- Fuel design limits shall include limits on the coated fuel particles defect rate and heavy metal contamination rate from manufacture, the permissible leakage of fission products from the fuel and/or fuel particle failure rate in all plant states so that the radioactive material releases are kept below acceptable limits.
- Other physical processes are at work, i.e. temperature gradients that causes kernel migration (amoeba effect) in the presence of an excess of oxygen; others are not applicable or unimportant such as and variations in performance in relation to heat transfer that could result from distortions or chemical effects or the variations in pressure and temperature resulting from variations in power demand.

Due to the reliance on the coated particle fuel as the main barrier to fission product release the required performance of the fuel is not only for all anticipated operational occurrences but also all accident conditions. Clarification is also needed to define fuel damage and fuel failure relative to core degradation and design extension conditions

§80 ¶6.64-6.68A refers to the fuel handling and storage systems for irradiated and non-irradiated fuel. In addition to the inconsistency of definitions of fuel elements and assemblies some of the specific requirements need more study and understanding in order to propose alternative text. For example the need to permit inspection sound reasonable but may be impossible for HTR pebble fuel in storage. Understanding the purpose of the inspection could lead to possible alternative means to define and fulfill this requirement. Alternatively fuel inspection might be possible but only for a selection of pebbles specifically separated for this purpose.

The prevention of the dropping of fuel in transit in ¶6.66 may be a valid requirement but pebble fuel is transported (and transferred) pneumatically and is “dropped” into the storage tanks and into the reactor – once again only within its design limits.

Other requirements such as the identification of individual fuel assemblies may not be needed as the lack of this ability does not seem to have a safety implication. This is unlike the misloading of a WCR fuel assembly and its safety implications. It is possible if needed to add identification marks (such as machined rings) to identify different types of fuel elements (variable enrichments) if required.

Most modular HTGR designers do not plan to make use of water pool systems for spent fuel storage so alternative requirements may be useful to address the mostly dry storage air cooled systems under consideration.

2.3.6. Testing, Monitoring and Instrumentation

¶6.4. *Adequate means of detecting the neutron flux distributions in the reactor core and their changes shall be provided for the purpose of ensuring that there are no regions of the core in which the design limits could be exceeded.*

In-core measurements within a pebble bed are not practically possible with traditional measurement techniques due to the high temperatures and moving irregular packed pebble bed. In cases where the operating point has large margins to the design limits, in-core detection may not be needed to fulfill the requirement and external measurement (with analysis) may be found to be sufficient

It is also important to keep in mind that the physically large HTGR core is neutronic much smaller than WCR's due to the much longer neutron mean free path length. One can show that large flux and spectrum changes do not occur locally (no neutronic hot spots) and depending on the margins show that the external detectors may predict the internal flux changes to the required accuracy.

2.3.7. Other

§35 includes power plants used for cogeneration of heat and power, heat generation or desalination. The focus is only on the transport of radionuclides to the heat application facilities and the authors probably had low temperature applications that use waste heat in mind. In the case of modular HTGRs used for high temperature process heat applications, the coupling is typically by an intermediate heat exchanger potentially connected directly with the helium pressure boundary.

The requirement needs to be strengthened: "Nuclear installations coupled with heat application facilities shall be also designed to prevent processes that transport flammable, corrosive and toxic chemicals from the heat application facilities to the nuclear plant under accident conditions in the heat application facilities". Possible explosions and shock waves from the coupled industrial plants also need consideration as part of external hazards.

Under the slightly confusing header of "Other Power Conversion Systems" where the actual power conversion system is described one would expect that alternative main power conversion system can be introduced.

For modular HTGR with a steam cycle the §77 ¶6.56–6.58 is appropriate. Since a gas-water steam generator is used, and the pressure in the power conversion system is larger than the reactor helium pressure, some additional requirements is needed such as the limitation of water ingress already mentioned.

Alternatively requirements for a Brayton cycle with a gas turbine can be used that require its own requirements: The design of turbine generators for nuclear installations shall provide appropriate protection such as overspeed protection and vibration protection to prevent the occurrence of

turbine generated missiles, and measures shall be taken to minimize the possible effects of turbine generated missiles on items important to safety.

§31 refers to ageing management: *“relevant mechanisms of ageing, neutron embrittlement and wear out and of the potential for age related degradation, to ensure the capability of items important to safety to perform their necessary safety functions throughout their design life.”*

The changes in dimensions and thermal conductivity of graphite blocks is understood to be captured by this neutron induced wear-out effects but could also be highlighted as a separate requirement. Many other properties of graphite, such as the thermal conductivity and dimensions also change with the fast fluence dose, and have safety functions in decay heat removal and reactivity control (control rods insertion into channels within the graphite fuel blocks and/or reflector)

2.4. EXEMPLARY DESIGNS THAT ALL APPLIED THE MODULAR HTGR SAFETY APPROACH, TWO PEBBLE BED AND TWO PRISMATIC DESIGNS

2.4.1. HTR-MODULE (Germany)

A05_BriVaTech-HTR-024

The reference design selected for the Pebble Bed Reactor (PBR) technology assessment is the HTR-MODULE. The HTR-MODULE is a 2x200 MWth (dual unit) modular pebble bed reactor design that was developed in Germany in the 1980s for the co-generation of electricity, process steam for the chemical industry, and/or district heat.

The HTR-MODULE is designed so that in the case of failure of all active cooling systems and a complete loss of coolant, fuel temperature limits are not exceeded, so that there is virtually no release of radioactive fission products. The design concept was reviewed and approved by German regulatory authorities, and progressed to a final design stage.

The HTR-MODULE design benefited from considerable German operating experience with pebble bed reactors, including the 15 MWel experimental pebble bed reactor, AVR, which operated from 1967 to 1988, and the 300 MWel prototype pebble bed reactor, THTR-300, which generated electricity from 1985 to 1989. The HTR-MODULE design formed the basis for subsequent modular PBR designs, including the South African PBMR and the Chinese HTR 10/HTR-PM, and therefore was selected as the reference design for this PBR technology assessment.

2.4.1.1. Summary Description of Reference Design

The HTR-MODULE design consists of two 200 MWth reactor units, each individually coupled to a turbine generator. Each reactor unit consists of a pebble bed core, a steam generator, a helium circulator, a pressure vessel unit, and associated support systems. The helium coolant is forced downward through the core and into the steam generator, where it transfers heat to water and steam

flowing in helical coil tubes. With a reactor outlet temperature of 700°C, the steam generator produces 530°C steam, which is used for electricity generation by the turbine generator or for process applications. The two reactor units are housed within a single reactor building, which provides protection against external hazards. Due to fission product retention capability of the fuel particles, a leak-tight reactor building is not required to comply with accident dose limits. To minimize impact on the environment of a postulated primary system break, the reactor building is provided with a sub-atmospheric pressure system, a pressure relief system, and a filtering system.

2.4.1.2. Reactor Core

The active core consists of a loose pebble bed of approximately 360,000 spherical fuel elements. The fuel elements are enclosed by a cylindrical ceramic core structure consisting of side, bottom, and top reflectors that reflect neutrons leaving the core back into the pebble bed. The ceramic core structure is enclosed by a metallic core barrel and the entire core is enclosed in the reactor pressure vessel as shown in Figure 4FIG. 4.

The reactor core is designed for operation between 50% and 100% power during normal power operation. Two independent shutdown systems ensure adequate shutdown margin. One shutdown system consists of six B₄C reflector rods that are inserted by gravity into the side reflector on actuation by the reactor protection system. Under normal operating conditions, the reflector rods compensate for changes in reactivity due to load changes.

The other shutdown system consists of 18 small ball shutdown units. The small ball shutdown elements containing B₄C are inserted by gravity into side reflector columns when actuated. The small ball shutdown system is provided for cold and long-term shutdown.

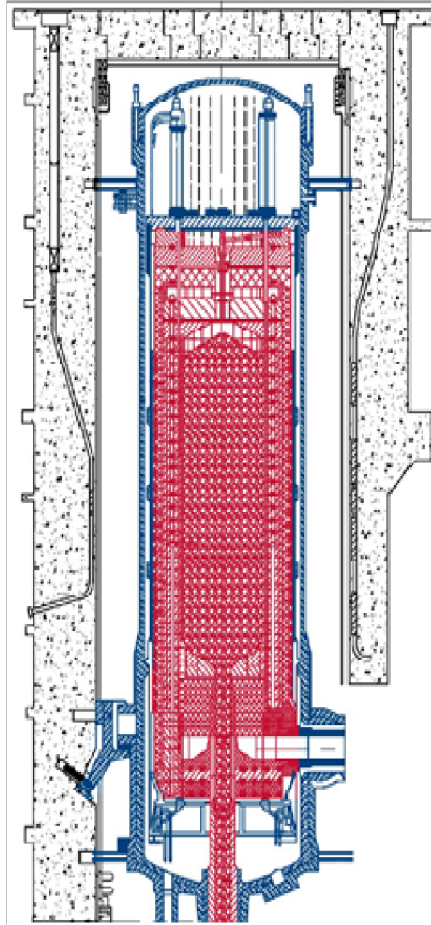


FIG. 4. HTR-MODULE PBR reactor core.

Each reactor has a separate, independent, and dedicated reactor protection system. In the event of an accident, the reactor protection system automatically shuts down the reactor and initiates protective actions.

The power density (3.0 MW/m^3) and geometry (3m diameter) of the reactor core are configured so that a maximum fuel temperature of approximately 1600°C is not exceeded under accident conditions, even without active removal of residual heat from the core.

The fuel elements are continuously recycled through the core to obtain a uniform power density distribution. On average, a fuel element will pass through the core 15 times before it reaches its target burnup of 80 GWd/MTU. The average dwell time in the reactor core for a fuel element is approximately 1000 full power days.

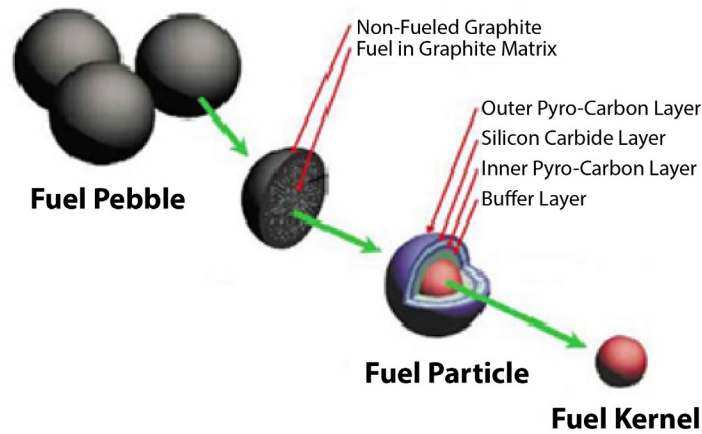


FIG. 5. HTR-MODULE PBR fuel pebble.

The fuel pebbles, shown in Figure 5, are 60mm diameter spheres with an inner fueled zone containing 7 grams of uranium at approximately 8% enrichment by weight. The fuel is in the form of spherical, 0.5mm diameter kernels surrounded by a buffer of porous carbon, two pyrolytically deposited layers of carbon, and one layer of silicon carbide (TRISO particles). The coatings provide a pressure boundary that has been demonstrated through extensive qualification testing and operating experience to confine fission products, preventing any significant releases of radioactivity when subjected to accident conditions.

For the first core, a mixture of lower enriched fuel elements and moderator and absorber elements are used to achieve the target core reactivity. The lower enriched fuel elements and moderator and absorber elements are gradually removed by the fuel handling equipment and replaced with equilibrium core fuel elements.

2.4.1.3. Primary Circuit

The primary circuit for each reactor unit, shown in Figure 6, consists of the reactor pressure vessel containing the core and core internals, the gas duct pressure vessel and hot gas duct, and the steam generator pressure vessel containing the tube bundle and the circulator. The primary circuit has an operating pressure of approximately 60 bar and a coolant mass flow of approximately 85 kg/s.

The 700°C helium leaving the reactor core is conveyed along a horizontal hot gas duct to the steam generator, where it flows through the tube bundle (shell side) from top to bottom. The steam generator consists of helical tubes connected to the feedwater and main steam systems. The cooled helium then passes through the annular gap between the steam generator shroud and the steam generator pressure vessel wall to the circulator located in the upper portion of the steam generator vessel. The cold gas leaving the circulator returns through the outer annulus of the gas duct pressure vessel to the lower region of the reactor pressure vessel. It then flows up to the core inlet plenum above the reactor core through channels in the side reflector. This flow circulation pattern and the side-by-side vessel arrangement reduce pressure vessel exposure to hot gas and allow upward evaporation in the steam generator tubes.

The reactor pressure vessel is approximately 25m in height with an inside diameter of 5.9m and a dry weight of approximately 830 tons. The steam generator pressure vessel is approximately 22m in height with an inside diameter of 3.6m and a dry weight of approximately 280 tons. The steam generator contains 220 helical tubes with a heat surface area of 2100m².

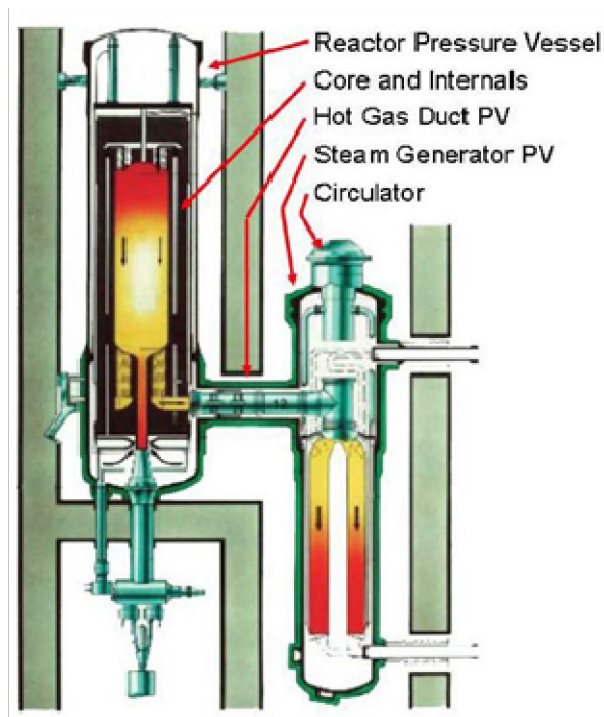


FIG. 6. HTR-MODULE PBR primary circuit.

2.4.1.4. Fuel Handling and Storage

The fuel handling system continuously supplies the core with fuel by feeding new fuel elements into the core, recirculating partially depleted fuel elements, and discharging spent fuel elements to storage/shipping casks. Damaged fuel elements and fragments are separated and discharged into failed fuel casks. Every full-load day, approximately 5000 fuel elements are circulated and approximately 360 new fuel elements are introduced into each reactor core. Fuel elements are conveyed in horizontal and vertical tubes either by gravity or pneumatically, mainly by primary helium coolant at primary system pressure and cold side temperature.

The burnup of each discharged fuel element is determined by gamma spectroscopic evaluation (662 keV gamma line of the isotope Cs-137) to decide whether it should be returned to the core or placed into storage for disposal. Spent fuel elements (360 per day per reactor) are buffered and then loaded into storage/shipping casks. Once the filled casks are conditioned, they are transported to an expandable onsite facility for temporary storage. Dedicated casks are provided for a complete core offload in case of extraordinary repairs. Casks in the storage facility are cooled by natural convection.

2.4.1.5. Cavity Cooling and Residual Heat Removal

The reactor cavity is cooled during operation and after shutdown by a cavity cooler consisting of vertical tubes arranged side-by-side to form a closed panel wall between the reactor pressure vessel and the cavity wall. The cavity cooler is supplied by an operational and a safety grade cooling system. The cavity cooler can operate passively and maintain design basis temperature limits for 15 hours post-accident before active systems or operator actions are necessary.

2.4.1.6. Energy Conversion Plant

The energy conversion plant receives steam from the steam generators for electricity generation or process applications and returns feedwater to the steam generator. The steam/power conversion system consists of two identical, suitably interconnected units. This arrangement permits uninterrupted continuation of operation during overhauls or failure of plant equipment.

For the purposes of the technology assessment, a representative configuration was assumed in which extraction steam from the high pressure turbine is used to generate high pressure and low pressure process steam in two reboilers. The actual energy conversion plant configuration would be determined based on customer requirements for a given application.

A steam generator isolation system separates the nuclear heat source from the conventional water/steam cycle. Whenever a reactor is tripped, the associated steam generator is isolated by the reactor protection system, which shuts off the main steam and feedwater lines by closing two isolation valves in series in each line. In the event of a steam generator tube break, the water or steam entering the primary circuit is limited by means of rapid secondary side emptying via the steam generator relief (dump) system. After draining the steam generator, the relief valves close to prevent primary system depressurization.

2.4.1.7. Plant Systems

Other plant systems, including helium support systems, ventilation systems, electrical and control systems, and cooling water systems, along with building structures, are more or less conventional systems.

2.4.2. MHTGR (US)

2.4.2.1. Summary Description of Reference Design

The MHTGR design is based on generic gas-cooled reactor experience and specific HTGR programs and projects, including the 52 carbon dioxide (CO₂)-cooled reactors developed in the United Kingdom and the 5 helium-cooled reactors built in Western Europe and the United States. The MHTGR is being designed to meet the rigorous requirements established by the Nuclear Regulatory Commission (NRC) and the electric utility-user industry for a second-generation power source of the late 1990s. The plant is expected to be equally attractive for deployment and operation in the United States, other major industrialized nations, and the developing nations of the world.

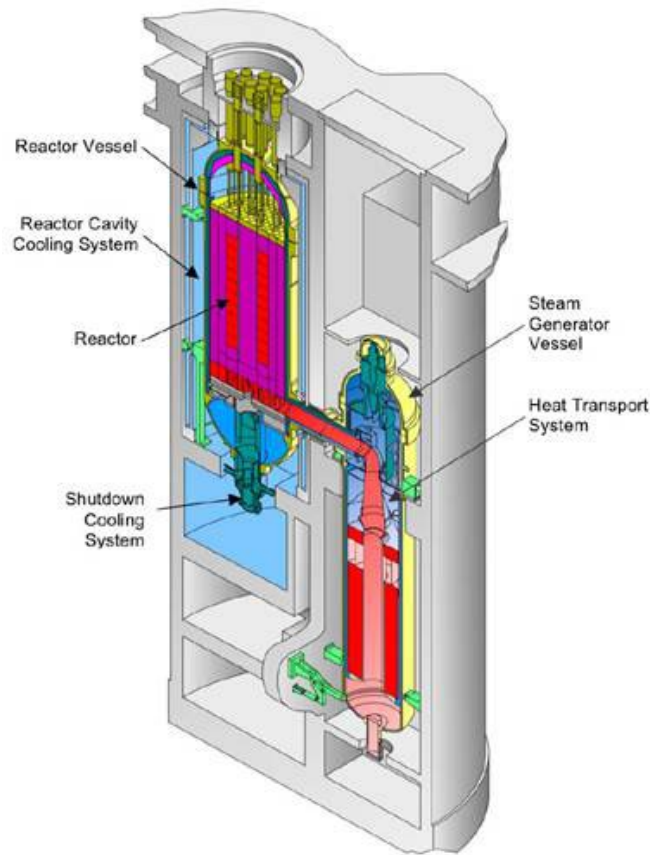


FIG. 7. Isometric drawing of 350 MW(t) MHTGR.

The overall reactor configuration is shown in Figure 7. The reactor components are contained within three steel vessels: a reactor vessel, a steam generator vessel, and a connecting cross-duct vessel. The reactor vessel is approximately the same size as that of a large boiling water reactor and contains the core, reflector, and associated supports. Top-mounted penetrations house the control-rod drive mechanisms and the hoppers containing boron carbide pellets for reserve shutdown. The penetrations are also used as access for refueling and inspection.

TABLE 2. MHTGR PLANT AND CORE PARAMETERS

Parameter	Value
Country of origin	United States of America
Reactor type	Modular prismatic high temperature gas-cooled reactor
Coolant/moderator	Helium/Graphite
Thermal capacity MW(t) (one module)	350
Thermal/electrical capacity, MW(t)/MW(e) (four modules)	1400 / 588 (gross), 538 (net)
Primary circulation	Forced circulation
Core inlet/exit temperatures (°C)	687/259
Core power density (W/cm ³)	5.9
Fuel type/assembly array	UO ₂ /Thorium oxide TRISO ceramic coated particle
Number of columns in active core	66
Number of fuel elements per column	10
Annular core diameters (m)	
- Outer	3.5
- Inner	1.6
Core height (m)	7.9

2.4.2.2. Reactor Core, Fuel Characteristics and Power Conversion Unit

The reactor core and the surrounding graphite neutron reflectors are supported on a steel core support plate at the lower end of the reactor vessel. A horizontal cross section of the reactor core and vessel internals is shown in Figure 8. The reactor core contains graphite fuel blocks that are hexagonal in cross section. The fuel is in the form of coated particles of low-enriched fissile uranium oxycarbide and fertile thorium oxide. The fuel particles are bonded together in fuel rods that are contained in sealed vertical holes in the fuel blocks. These fuel blocks are stacked in columns to form an annular-shaped core. Unfueled graphite blocks fill the center and surround the active core to form the reflector. Key reactor core design parameters are given in Table 2.

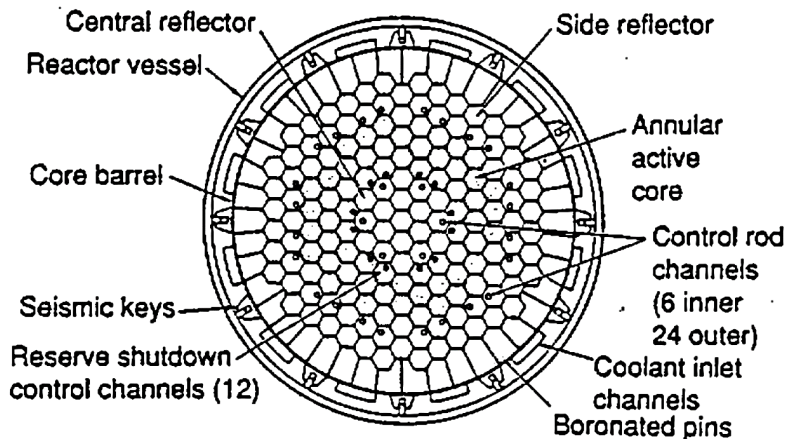


FIG. 8. Cross section of 350MW(t) MHTGR reactor core (RSC: Reserve Shutdown Control)

The heat transfer during power operation or normal decay heat removal operation is accomplished by using helium that is heated as it flows down through the core. It is collected in a plenum below the core and flows through a coaxial hot duct inside the cross vessel to a once-through helical bundle steam generator. After flowing downward over the steam generator tubes, the cool helium flows upward in an annulus between the steam generator vessel and a shroud leading to the main circulator inlet.

The main circulator is a submerged electric-motor driven, two-stage axial compressor with active magnetic bearings. The helium is discharged from the circulator and flows through the annulus of the cross vessel and hot duct and then upward to the top plenum over the core.

2.4.2.3. Reactivity Control and Chemical Attack Control

The inherent features that control reactivity include a strong negative temperature coefficient, a single phase (no void coefficient), and neutronically inert coolant. These characteristics cause the reactor to inherently shut down. For a pressurized-conduction cooldown, fuel temperatures remain low and within acceptable limits regardless of whether reactor trip occurs and even if all control rods are withdrawn (a reactivity addition of approximately 3%). The temperatures without reactor trip remain within acceptable limits for periods of time approaching several days. Accidental ingress of water is limited by the amount of steam the core can physically hold (724 kg pressurized and 63 kg depressurized) and is therefore bounded by the preceding reactivity addition. Furthermore, the plant protection system, which is separate from the operational system, includes two diverse reactivity control systems that are gravity inserted and highly reliable for protecting against even rarer events.

The inherent features for controlling chemical attack of the fuel by water include the nonreacting coolant, a water-graphite reaction that is endothermic and requires temperatures above the average normal operating conditions, and the silicon carbide coatings on the fuel. The MHTGR design features that limit water ingress and its consequences include the limited sources of water, reliable detection and isolation systems, and two forced convection core-cooling systems. The circulator

magnetic bearings eliminate the source of water that was the dominant contributor to the low-capacity factor of the Fort St. Vrain Nuclear Generating Station high temperature gas-cooled reactors.

The inherent features for controlling chemical attack of the fuel by air include the nonreacting coolant, the embedded ceramic fuel particles, the nuclear-grade vessel, and the below-grade reactor silo. The fraction of the core graphite reacted by air ingress following primary coolant leaks without forced core cooling (two LBEs and two extremely rare bounding events) is very small in all cases. The primary reason for the small amount of oxidation is the large resistance to flow that the coolant holes provide ($L/D > 700$). Once again, the impact on the core graphite is small, and the fuel remains intact.

2.4.2.4. Shutdown Cooling System, Cavity Cooling and Residual Heat Removal

For availability and maintenance requirements, a separate shutdown cooling system (SCS) is provided as a backup to the primary heat transport system. A shutdown heat exchanger and a shutdown cooling circulator are mounted on the bottom of the reactor vessel. The heat removal systems allow hands-on plant maintenance to begin within 24 h after plant shutdown.

A reactor cavity cooling system (RCCS) is located in the concrete structure external to the reactor vessel to remove plant residual heat. The RCCS consists of above-grade intake structures that naturally convect outside air down through enclosed ducts and panels that surround the below-grade core cavity before returning the warmed air through above-grade outflow structures. The core heat is transferred by conduction, convection, and radiation from the core to the RCCS. This system has no controls, valves, circulating fans, or other active components.

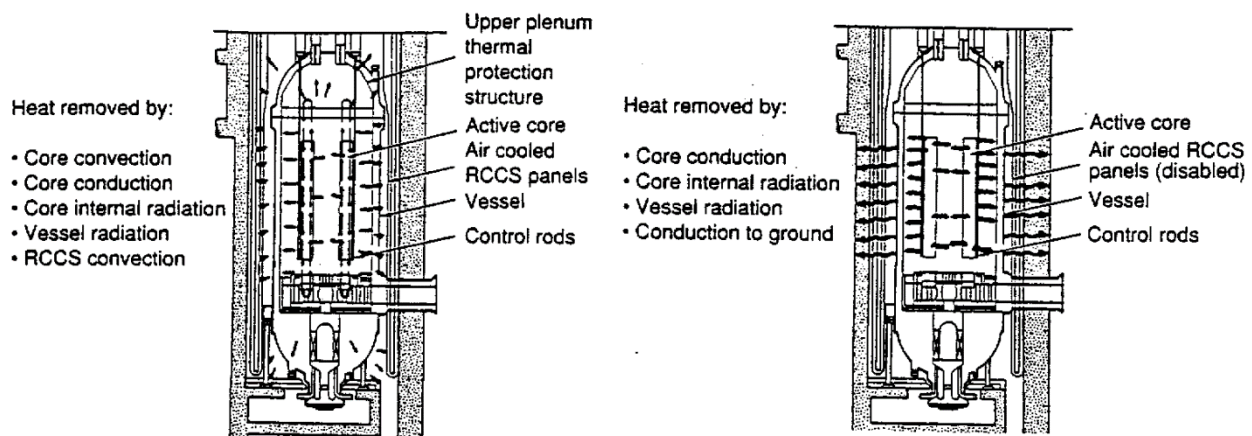


FIG. 9. MHTGR pressurized-conduction (left) and depressurized-conduction (right) cooldown heat flow paths, RCCS - Reactor Cavity Cooling System.

The inherent features for heat removal include the intrinsic core dimensions and power densities of the reactor core, internals and vessel, and passive cooling pathway from the core to the environment, as illustrated in Figure 9. Passive heat removal by conduction, radiation, and natural

convection from the core through the vessel to the RCCS limits fuel temperatures to acceptable levels.

Passive heat removal is possible because of the large thermal margins in the fuel. Fuel heatup tests have been performed in which the temperature was increased from 1100 to 2500°C in 8, 30, or 80h [47]. The fuel must exceed approximately 2000°C before thermal decomposition for the silicon carbide coating results in significant failure. The normal peak fuel temperature is much lower at 1100°C.

Finally, the ultimate and unprecedented capability of the MHTGR to withstand challenges of heat removal is demonstrated with assumption of the passive air cooled RCCS panels to be completely ineffective. In this case, the maximum core temperature is affected very little and remains within acceptable levels as the heat is transferred into the building and ground. Also note that removal of core heat in the MHTGR is largely independent of maintaining any coolant flow path geometry.

2.4.2.5. Plant Arrangement

The typical MHTGR plant includes an arrangement of four identical modular reactor units located in a single reactor building. The plant is divided into two major areas: a nuclear island (NI), containing the four reactor modules, and an energy conversion area (ECA), containing two turbine generators. Each of the reactor modules produces a thermal output of 350 MW(t). The reactor modules are paired to feed the turbine generators to produce 538 MW(e) net of electric power. The steam conditions are similar to those of a modern fossil-fired plant.

Each reactor module is housed in adjacent, but separate, reinforced concrete structures located below grade and under a common-roof structure. The below grade location provides significant design benefits by reducing the seismic amplifications typical of above grade structures.

2.4.3. HTR-PM (China)

2.4.3.1. Summary Description of Reference Design

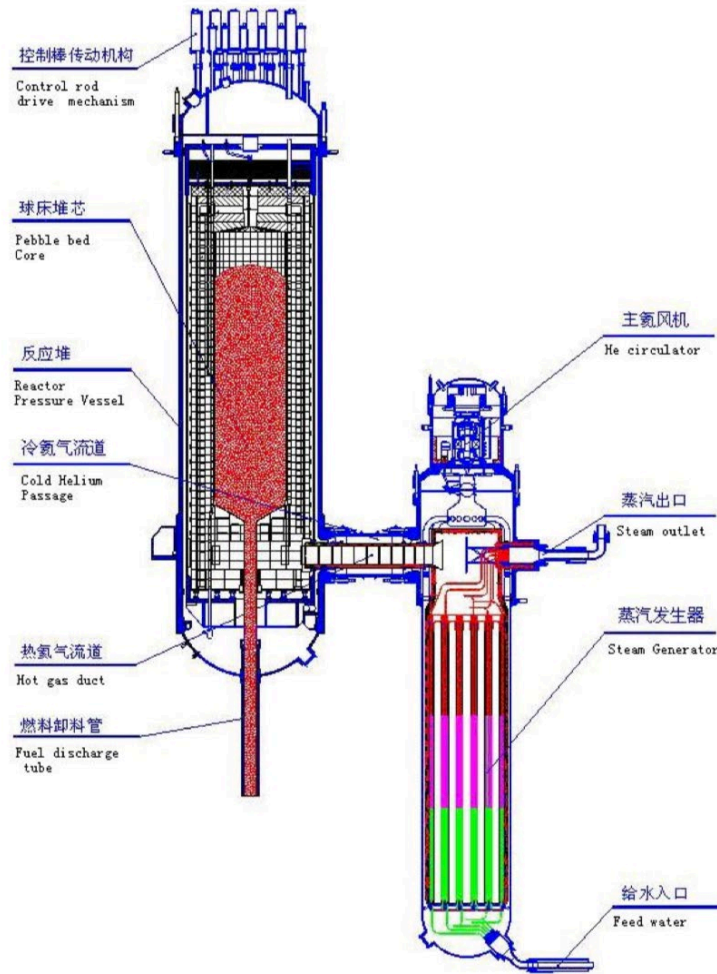


FIG. 10. HTR-PM primary loop.

TABLE 3. HTR-PM MAJOR TECHNICAL PARAMETERS

Parameter	Value
Technology developer, country of origin	INET Tsinghua University, People's Republic of China
Reactor type	Modular pebble bed high temperature gas-cooled reactor
Coolant/moderator	Helium/Graphite
Thermal/electrical capacity, MW(t)/MW(e)	2x250/210
Primary circulation	Forced circulation
System pressure (MPa)	7
Core inlet/exit temperatures (°C)	250/750
Fuel type/assembly array	Spherical elements with coated particle fuel
Number of fuel spheres	420,000 (in each reactor module)
Fuel enrichment (%)	8.5

Fuel burnup (GWd/ton)	90
Fuel cycle (months)	On-line refueling
Main reactivity control mechanism	Control rod insertion
Approach to engineered safety systems	Combined active and passive
Design life (years)	40
RPV height/diameter (m)	25/5.7(inner)
Seismic design	0.2 (g)
Distinguishing features	Inherent safety, no need for offsite emergency measures
Design status	Under construction

The HTR-PM is a commercial demonstration unit for electricity production. The twin reactor modules driving a single turbine configuration was specifically selected to demonstrate its feasibility. Technical parameters of the modular pebble bed high temperature gas-cooled reactor are listed in Table 3. Following HTR-PM demonstration plant, commercial deployment of HTR-PM based on batch construction is foreseeing, and units with more modules and bigger power size are under design. Units with multiple standardized reactor modules coupling to one single steam turbine (such as 200, 600 or 1000MW) are envisaged. A conceptual design has been finished for a 600 MW(e) multi-module HTR-PM nuclear power plant, which consists of six reactor modules coupling to one steam turbine. Each reactor module has the same design as the HTR-PM demonstration plant, with independent safety systems and shared non-safety auxiliary systems. The footprint of a multi-module HTR-PM plant is not remarkably different from that of a PWR plant generating the same power. The Figure 11 shows the 600 MW(e) HTR-PM nuclear power plant layout. Future sites have been identified for possible deployment.

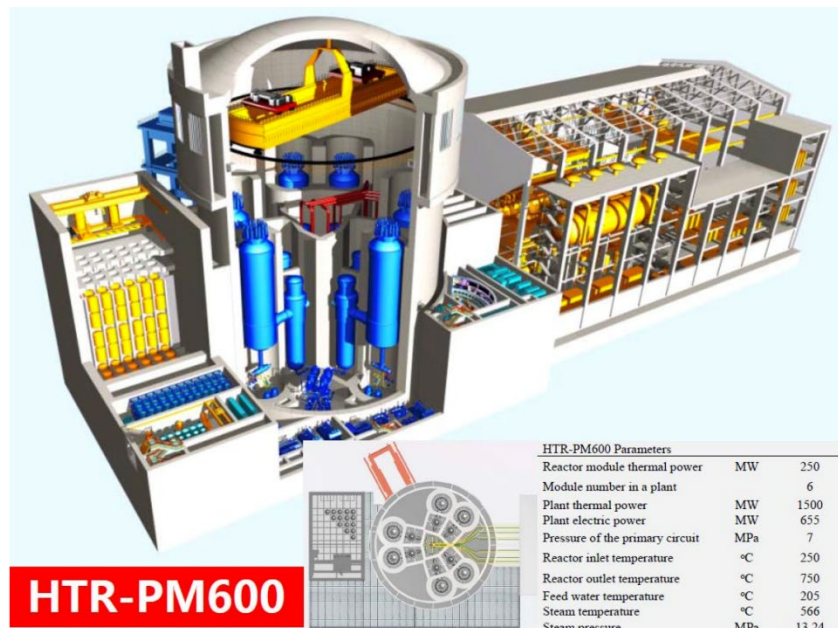


FIG. 11. HTR-PM 600 plant overview.

2.4.3.2. Reactor Core and Power Conversion Unit

The HTR-PM consists of two pebble-bed reactor modules coupled with a 210 MW(e) steam turbine. Each reactor module includes a reactor pressure vessel (RPV); graphite, carbon, and metallic reactor internals; a steam generator; and a main helium blower. The thermal power of each reactor module is 250 MW(t), the helium temperatures at the reactor core inlet/ outlet are 250/750°C, and steam at 13.25 MPa/567°C is produced at the steam generator outlet.

The primary helium coolant works at the pressure of 7.0 MPa. The rated mass flow rate is 96 kg/s. Helium coolant enters the reactor in the bottom area inside the pressure vessel with an inlet temperature of 250°C. Helium coolant flows upward in the side reflector channels to the top reflector level where it reverses the flow direction and flow into the pebble bed in a downward flow pattern. Bypass flows are introduced into the fuel discharge tubes to cool the fuel elements there and into the control rod channels for control rods cooling. Helium is heated up in the active reactor core and then is mixed to the average outlet temperature of 750°C and then flows to the steam generator.

2.4.3.3. Fuel Characteristics and Fuel Handling

Fuel elements are spherical ones. Every fuel element contains 7 g heavy metal. The enrichment of U-235 is 8.5%. Uranium kernels of about 0.5 mm diameter are coated by three layers of pyro-carbon and one layer of silicon carbon. Coated fuel particles are dispersed in matrix graphite which is 5 cm in diameter. Surrounding the fuel containing graphite matrix is a 5 mm thick graphite layer. This is illustrated above.

The operation mode of HTR-PM adopts continuous fuel loading and discharging: the fuel elements drop into the reactor core from the central fuel loading tube and are discharged through a fuel extraction pipe at the core bottom. Subsequently, the discharged fuel elements pass the burn-up measurement facility one by one. When a fuel sphere reaches the target burnup they will be discharged into the spent fuel storage tank, otherwise they are re-inserted into the reactor to pass the core once again.

2.4.3.4. Reactivity Control

Two independent shutdown systems are installed: a control rod system and a small absorber sphere (SAS) system, both placed in holes of the graphitic side reflector. Reactivity control is achieved through 24 control rod assemblies, and six SAS shutdown systems serve as a reserve shutdown system. The control rods are used as a regulating group that is used during normal plant operation to control reactivity, but also for hot shutdown. The SAS system is used for long-term shutdown. Absorber material of control rods and small absorbers is B₄C.

2.4.3.5. Cavity Cooling and Residual Heat Removal

Normally the reactor is cooled by steam generating system. Under accident conditions, the primary helium circulator shall be stopped automatically. Because of the low power density and the large heat capacity of the graphite structures, the decay heat in the fuel elements can dissipate to the outside of the reactor pressure vessel by means of heat conduction and radiation within the core internal structures, without leading to unacceptable fuel temperature limits. The decay heat shall

be removed to heat sink passively by reactor cavity cooling system (RCCS). Even if the RCCS fails, the decay heat can be removed transferring through the concrete structure of reactor cavity while the temperatures of fuel elements are under design limit.

2.4.3.6. Instrumentation, Control Systems and Plant Arrangement

The instrumentation and control system of HTR-PM is similar to those of normal PWR plant. The two reactor modules are controlled in a coordinated manner to meet various operational requirements.

The nuclear island contains reactor building, nuclear auxiliary building, spent fuel storage building and I&C building, as shown below. The steam turbo-generator, which is similar to that of a conventional fossil-fired power plant, is housed in the turbine building.

2.4.4. GTHTR300 (Japan)

2.4.4.1. Summary Description of Reference Design

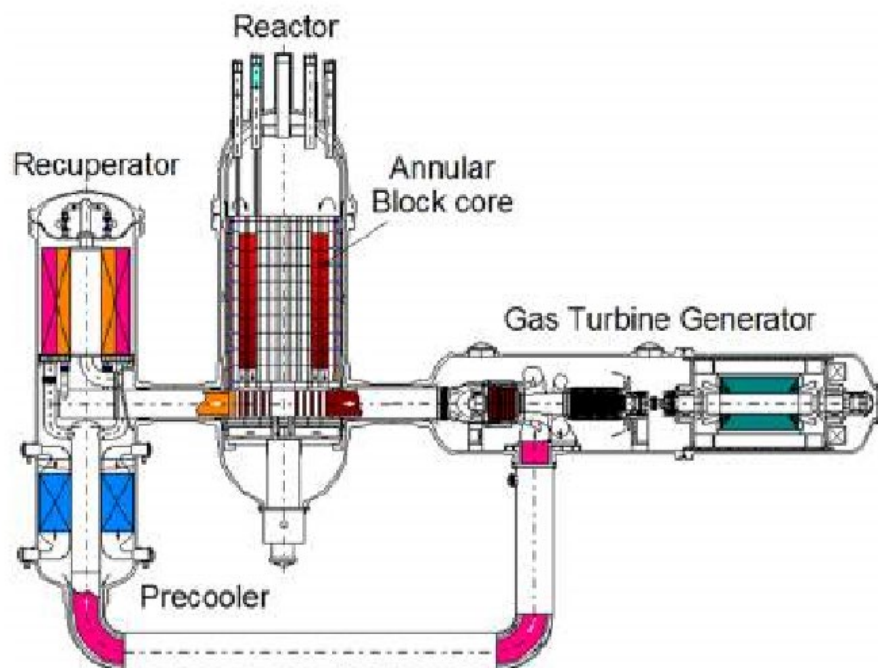


FIG. 12. GTHTR300 design.

TABLE 4. GTHTR300 MAJOR TECHNICAL PARAMETERS

Parameter	Value
Technology developer, country of origin	JAEA jointly with MHI, Toshiba/IHI, Fuji Electric, KHI, NFI, etc, Japan
Reactor type	Prismatic HTGR
Coolant/moderator	Helium
Thermal/electrical capacity, MW(t)/MW(e)	<600/100~300
Primary circulation	Forced by gas turbine
System pressure (MPa)	7
Core inlet/exit temperatures (°C)	587-633/850-950
Fuel type/assembly array	UO ₂ TRISO ceramic coated particle
Number of fuel columns	90
Fuel enrichment (%)	14
Fuel burnup (GWd/ton)	120
Fuel cycle (months)	48
Main reactivity control	Control rod insertion
Design life (years)	60
RPV height/diameter (m)	23/8
Seismic design	>0.18 g automatic shutdown
Distinguishing features	Multiple applications of power generation, H ₂ production, process heat, steelmaking, desalination, district heating
Design status	Pre-licensing basic design completed

GTHTR300 (Gas turbine High Temperature Reactor 300 MW(e)) is a multi-purpose, inherently-safe and siteflexible SMR (small modular reactor) that Japan Atomic Energy Agency (JAEA) is developing for commercialization in 2030s. As a Generation-IV technology, the GTHTR300 offers important advances comparing to current light water reactors. The reactor coolant temperature is significantly higher in the range of 850-950°C. Such high temperature capability as proven in JAEA's HTTR test reactor operation enables a wider range of applications as listed in Table 4. The design employs a direct-cycle helium gas turbine to simplify the plant by eliminating water and steam systems while delivering 45-50% power generating efficiency. The design incorporates ceramic fuel, low power density but high thermal conductivity graphite core, and inert helium coolant to secure inherent reactor safety. The inherent safety permits siting proximity to users, in particular to industries, so as to minimize cost and loss of high temperature heat transmission. Dry cooling becomes economically feasible due to high temperature (above 150°C) heat rejection from the gas turbine cycle, making inland and remote siting possible without a large source of cooling water.

The overall goal of the GTHTR300 design and development is to provide a family of system options capable of producing competitive electricity, hydrogen, desalination, other products, and yet deployable in the near term. The development of the multiple systems simultaneously does not necessarily suggest having investment and risk multiplied. Rather, the development requirement is minimized by pursuing system simplicity, economic competitiveness and originality, namely

the SECO design philosophy. More specifically, all design variants are built on the premise that they share common system technologies to the maximum extent possible, including a unified reactor and primary coolant circuit, an aerodynamically and mechanically similar line of helium gas turbines used for electricity production, and the IS process for hydrogen production. The helium gas turbine and the IS process, for which JAEA has been carrying out research and development, are particularly compatible with high temperature helium cooled reactor providing the basis for high efficiency and economical production. The design includes such distinct attributes as conventional steel reactor pressure vessel, horizontal gas turbine installation, and the threevessel system arrangement among others, reduce requirement and risk of technology development. Since the technologies are shared by several systems, the benefit of investing in any one development is increased

2.4.4.2. Reactor Core and Power Conversion Unit

The reactor system combines a high temperature gas-cooled reactor with direct-cycle gas turbine to generate power while circulating the reactor coolant. The system consists of three functionally-oriented pressure vessel units, housing the reactor core, the gas turbine, and the heat exchangers respectively. The multi-vessel system facilitates modular construction and independent maintenance access to the functional vessel units. The reactor system is placed below grade in the reactor building. The pre-application basic design of the system was completed in 2003 by JAEA and domestic industrial partners Mitsubishi Heavy Industries, Fuji Electric, Nuclear Fuel Industries and others. The reactor system design added cogeneration capabilities by adding an IHX between the reactor and gas turbine that can accept the various roles of cogeneration while sharing equipment designs with GTHTR300. While the reactor technologies required for the GTHTR300 are developed mainly with construction and operation of JAEA's 30 MW(t) and 950°C test reactor, separately is being developed and tested balance of plant key technologies needed for the commercial SMR, including test validation of the helium gas turbine equipment at one-third to full scale, production-scale fuel fabrication lines, thermochemical hydrogen production process, and the super alloy heat exchanger capable of transferring 950°C reactor heat to the hydrogen production process.

2.4.4.3. Fuel Characteristics and Fuel Handling

The fuel design is coated fuel particle of less than 1 mm in diameter. Each particle consists of a UO₂ kernel coated by four layers of low and high density pyro-carbon and silicon carbide. The all ceramic particle fuel is heat resistant up to 1600°C. Approximately ten-thousand particles are packaged into a compact of the size of a thumb. The compacts are then assembled into graphite-clad fuel rods. The fuel rods are inserted into the bore holes of a hexagonal graphite fuel block of about 1 m long and 41 cm across, where the annulus formed between the fuel rod and the bore hole provides coolant flow channels. The fuel blocks are loaded into the reactor core. The more fuel blocks are placed in the core, the higher the power output of the reactor.

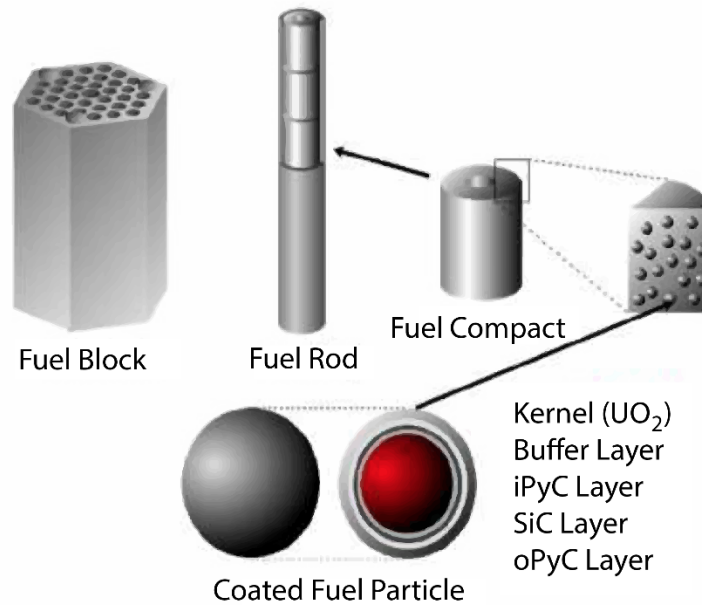


FIG. 13. Prismatic fuel designed for GTHTR300

The fuel handling system consists of fuel loading machines, door valves, a control rod exchange machine, and a transport carriage. The fuel loading machine is used to remove fuel blocks from core and load fuel blocks to core and spent fuel storage facility. The door valves are devised at the interface between fuel loading machine and spent fuel storage facility to maintain airtightness and radiation shielding performance. The control rod exchange machine is installed for removal of control rods from reactor and loading of used control rods to maintenance pit. The transport carriage is used for the transportation of the fuel loading and control rod exchange machines.

2.4.4.4. Reactivity Control

Reactivity control system consists of control rods, control rod drive mechanisms and reserve shut down systems. The system is used to adjust control rod position for reactivity control as well as shut down reactor in case of reactor scram. GTHTR300 has 30 pairs of control rod and reserve shut down systems. The control rods and reserve shut down system channels are located in the reflector blocks on the inner and outer boundaries of the fuel region.

2.4.4.5. Cavity Cooling and Residual Heat Removal

GTHTR300 design is required to remove the core decay and residual heat from the outside surface of the reactor vessel by the natural convection and radiation, and to transfer it to an ultimate heat sink in the operational states and in the accident conditions so that the design limits for fuel, the reactor coolant pressure boundary and structures important to safety are not exceeded. In accordance with the requirement, a low power density core with annular configuration of the fuel region is employed to maintain the fuel temperatures below the design limits during passive decay heat removal. A reactor cavity cooling system, an air-cooled, passive decay heat removal system is used to transfer heat received from reactor pressure vessel to atmosphere.

GTHTR300 employs a vented confinement rather than a conventional high-pressure, airtight containment used in LWRs. The confinement is designed to meet requirements designated in safety design. The confinement is designed to release helium coolant blown out from primary system in case of depressurized loss-of-forced cooling accidents. Dampers are devised and recloses when the pressure between outside and inside of confinement equalizes. The design leak rate is set to 20%/day to limit the amount of air ingress to the reactor core

2.4.4.6. Instrumentation, Control Systems and Plant Arrangement

Instrumentation and control system consists of reactor and process instrumentations, control systems, safety protection system, and engineered safety features actuating systems. Six fundamental controls: turbine bypass control, inventory control, reactor outlet temperature control, turbine inlet temperature control, process heat supply rate control and IHX differential pressure control, are combined in the basic plant control to provide controllability for a variety of transients including loss-of-load and electric load following as shown above.

The reactor building is a below-grade, steel concrete structure housing 4 units of reactor systems consists of subsystems including reactor module, gas turbine module and heat exchanger modules. The co-axial pipe connecting the modules are aligned at the same vertical level. The reactor module is fixed in horizontal direction while gas turbine and heat exchanger modules are allowed movement due to thermal expansion in the direction.

3. RELEVANT PAST AND CURRENT WORK RELATED TO HTGR SAFETY.

3.1. ADVANCED REACTORS / NON-WATER COOLED

3.2. IAEA DOCUMENTS

3.2.1. IAEA Safety Reports Series N° 54 – Accident Analysis for Nuclear Power Plants with Modular High Temperature Gas Cooled Reactors (2008)

This safety report addresses specific guidance on conducting accident analyses of nuclear power plants with modular HTGRs taking into account specific design, operational and safety features.

This report is an attempt to assist with methodology for modular HTGR accident analysis, dealing with approaches such as risk informed [16] and best estimate plus uncertainty licensing methods [17].

It contains details of initiating events and overviews of the safety aspects of events that could lead to fuel failure and potential activity release. The analysis methods for the various events differ mainly in (a) the selection of events; (b) the event consequence acceptance criteria; (c) the structures, systems and components (SSCs) that may be credited and modelled in accident mitigation analysis; and (d) the level of conservatism required in the analysis methods.

Dealing only with internal event in the reactor system or in associated connected process system, the emphasis here is on the transient behaviour of the reactor and its systems in postulated accidents, including the role of the confinement.

This report does not intend to cover the task of assigning specific events or accidents to the various levels of event classification, with their corresponding probabilities and consequences. References are made, however, to levels of severity that serve as examples in the discussion of initiating events and accident sequences.

Structure of the report shows guidance on grouping and categorization of events, such as event frequencies and challenges to fundamental safety functions, as well as discussions of acceptance criteria for accident analysis that may be applicable to modular HTGRs. Since the acceptance criteria for various categories of events differ depending on specific designs, national codes and standards, and national regulatory bodies, they are meant to serve here only as examples. One section concerns a guideline for the analysis methodology and another attempts to provide a description of some accident analyses applicable to modular HTGRs, with for each category provides descriptions of the initiating events, the consequences and safety aspects, and the modelling and data needs. Eventually, analysis code attributes required for modular HTGRs are discussed in last part of the report.

3.2.2. IAEA TECDOC 1570 - Proposal for a Technology-Neutral Safety Approach for New Reactor Designs (2007)

This TECDOC highlights the need to develop a tailored set of safety requirements derived from the general consolidated principles of nuclear safety for some innovative concepts, which better incorporates the specific characteristics of a given concept. The report identifies some of the key areas where change and development are required to the current design and licensing rules (for water power reactors), in order to design and license future innovative reactor designs. It proposes a framework (the Main Pillars of a new Safety Approach) from which to develop both technology-neutral and technology-specific requirements, but the focus is primarily on the development of technology-neutral safety requirements.

The proposed new Safety Approach is an evolution of existing design and licensing rules and safety approach with identification of areas requiring further development such as:

- Qualitative Safety Objective to be replaced by Quantitative Safety Goals
- Enhanced Defence in Depth (DiD)
- Enhanced Levels of Defence in Depth will be correlated with Quantitative Safety Goals
- Further Development of Probabilistic Safety Analyses (PSA)
- Further Development of a Sound and Well Balanced Safety Classification of Safety Systems and Components
- How to Define Research, Development and Demonstration (RD&D)
- Application of Methodologies early in the Design Process to Systematically Examine Risk and Options of Solutions such as the *Objectives Provisions Tree* Methodology
- Application of Iterative Design Processes to demonstrate that Adequate Defence in Depth is achieved (Safety driven design process).
- Comprehensive Review of Existing Safety Approach

This TECDOC aims to provide a technology-neutral safety approach that will guide the design, safety assessment and licensing of innovative reactors. It outlines a methodology to establish a new framework, generate the safety requirements, and develop a “safety-driven” plant design which complies with the new Safety Approach and the newly derived safety requirements. This TECDOC also identifies areas/issues where additional work is required for better definition of concepts and for planning, research and development. This TECDOC examines these issues in the context of defining the overall process to generate the new Safety Approach; however the development of each of these areas of work is not within the scope of this report.

One section of the report describes the model and process to develop safety requirements for new NPPs, also summarizing the IAEA hierarchy of Safety Standards and the “safety approach” (main pillars) for current water nuclear power plants (referencing a recent case study). A proposed revised “Safety Approach” for new NPPs, is discussed. The proposed new “Pillars of the Safety Approach” for new NPPs are: (1) quantitative safety goals, (2) fundamental safety functions (unchanged), and (3) defence in depth (including probabilistic considerations).

Another section discusses the applications of methodologies (combined deterministic and probabilistic) to generate safety requirements for new NPPs (technology-neutral). This section

introduces relatively modern concepts/tools such as “Objectives Provisions Trees to systematically review the implementation of the defence in depth, and a design process for innovative designs. A sample proposal of Technology-neutral Requirements based on a critical review of the Safety Requirements NS-R-1 is presented in Appendices, as well as the use of postulated initiating events (PIE), the description of redundancy, diversity and independence, and an overview of defence in depth.

Eventually, the intent of this document is that it be used as a guide to develop the new safety approach, design requirements and a safe design.

3.2.3. IAEA-TECDOC-1487 - Advanced nuclear plant design options to cope with external events (2006)

Knowing that high level of safety and improved economic competitiveness are common goals for advanced nuclear Power Plants [18],[19],[20],[21],[22], the provision of a high level of safety remains and will be the crucial issue for all evolutionary and innovative NPPs. An overall NPP safety is defined by many factors, among which an important one is plant protection from external events which is address in this TECDOC.

An external event is defined as the “event that originates outside the site and whose effects on the nuclear power plant should be considered .Such events could be of natural or human induced origin and are identified and selected for design purposes during the site evaluation process. In some cases events originating on the site but outside the safety related buildings can be treated as external events if the characteristics of the generated loads are similar to those caused by off-site events”[23].

This aspect may become even more important in the future in view of possible global deployment of nuclear power accompanied by general globalization of the world economy, which would facilitate increased export of NPPs and their deployment in a variety of siting conditions, particularly in today’s developing countries [24].

The IAEA maintains communications with the designers of many evolutionary and innovative NPPs worldwide, and through these communications it was found that a systematic consideration of the issues of plant protection from impacts of external events at an early design stage is not a common practice in Member States, especially for NPPs with innovative reactors.

In line with the above mentioned developments, the objectives of this report are the following:

1. Define, collate and present the state-of-the art in design features and approaches used to protect plants from external event impacts, making a focus on NPPs with evolutionary and, when possible, innovative designs;
2. Provide a technical and information background to assist designers of advanced NPPs in defining a consistent strategy regarding selected design and site evaluation issues in relation to extreme external events;
3. To bring to the attention of designers of advanced NPPs the recently updated IAEA safety guides and other publications on issues of plant protection from external event

impacts; to collect comments on their applicability to NPPs with evolutionary and innovative reactors; to identify safety and technological issues and proposals for their resolution.

No limitations were set on the scope of external events which include humans induced events (for example aircraft crashes, explosions or electromagnetic interference from off-site and on-site) and natural events (such as earthquakes, cyclones or volcanism). Likewise, there were no limitations on specific types of evolutionary or innovative reactors within the NPP projects to be addressed, and many designers around the world were invited to participate.

In the report, a section addresses safety requirements for siting of NPPs with advanced reactors. Referring to the best practices achieved in Member States, this section presents the criteria and methodology for hazard assessment, compatible with the design features and overall design goals of evolutionary and innovative reactors. In particular, the following issues are addressed: external event scenarios in relation to the expected challenges posed to plant safety, combination criteria for external events, interfaces with the implementation of emergency planning (triggered by external events) and the need to accommodate “unanticipated” scenarios of different nature.

Another section collates, presents and analyzes the design features and approaches used in 14 advanced NPPs, with respect to protection from both external and internal events. Ultimately, a different section is dedicated to probabilistic safety assessment (PSA) in application to external events. A summary of the experience in Member States is provided, and the applicability of IAEA safety guides is analysed. A state-of-the-art PSA methodology for external events is described, which also provides a comprehensive list of basic references.

3.2.4. IAEA-TECDOC-1366 - Considerations in the development of safety requirements for innovative reactors: Application to modular high temperature gas cooled reactors (2003)

This publication proposes a technical basis and methodology, based on principles of defence in depth, for conducting design safety assessments and in the long term generating design safety requirements for innovative reactors. The MHTGR is used as an example to illustrate this process, and the term MHTGR in this report is used to indicate a general family of modular HTGRs with common characteristics. For this purpose, the document provides an overview of the safety related features of current MHTGR technology, examines how the defence in depth principle can be implemented/adopted by the MHTGR design, and how MHTGR designs could satisfy the three fundamental safety objectives:

- general nuclear safety;
- radiation protection;
- technical safety.

To apply the defence in depth screening approach, this report considered the three fundamental safety functions (control of reactivity, core heat removal, and confinement of radioactive materials), and the challenges to the performance of these functions. Provisions identified are mainly based on design features of current PBMR and GT-MHR concepts, and are identified to

illustrate the process for assessing MHTGR concepts. This report does not consider challenges to the safety functions during various shutdown modes, or fuel storage and radioactive waste issues.

This report focuses on the MHTGR and one section of this TECDOC presents a discussion of specific safety characteristics, particularly inherent safety features that form an integral part of the safety case. This discussion serves to define the family of concepts referred to in this report as MHTGRs.

Another section introduces a method to prepare design safety requirements for the MHTGR, starting from the current requirements [25] (mostly developed for light water reactors, LWRs), adopting a top-down approach applicable to MHTGRs, and taking credit for recently-developed methodology [26] for screening defence in depth in nuclear reactors.

A “critical review” of the reference requirements is presented in another section, analysing the defence in depth implemented for advanced reactors. For each level of defence in depth and for each fundamental safety function, the section illustrates the acceptance criteria for a successful achievement of the safety functions. Finally the identification of the provisions to cope with these mechanisms create the basis for the definition of the design requirements.

Finally, a summary of the conclusions from the systematic investigation of the defence in depth of MHTGRs is drawn, hopefully contributing to the future work of preparing design requirements for this family of future reactors. In addition, the appendix contributes to this goal by providing a comparison of safety characteristics of LWRs and MHTGRs.

3.2.5. IAEA - Nuclear Energy Series - No. NP-T-2.2 - Design Features to Achieve Defence in Depth in Small and Medium Sized Reactors (2009)

This Nuclear Energy Series (NES) report provides an in-depth description of safety design features used to achieve defence in depth in 11 innovative SMR concepts selected in 2009 to represent all major reactor lines with near to medium and longer term deployment potential. These descriptions are structured to follow the definitions and recommendations of IAEA safety standard NS-R-1, Safety of the Nuclear Power Plants: Design Requirements [7] and include some references to other IAEA safety guides and documents. The concepts have been selected to include: as many concepts as possible for which noticeable progress toward advanced design stages or deployment is observed; concepts representing different reactor lines; concepts that could be deployed in the near term. Presentation of certain SMR concepts in this report was also conditioned by the agreement of their developers to cooperate.

The overall objectives of this report are:

- 1) To assist developers of innovative SMRs in defining consistent defence in depth approaches regarding the elimination of accident initiators/ prevention of accident consequences through design and the incorporation of inherent and passive safety features and passive systems in safety design concepts of such reactors;

- 2) To assist potential users of innovative SMRs in their evaluation of the overall technical potential of SMRs with inherent and passive safety design features, including their possible implications in areas other than safety.

The specific objectives of this report are: [1]
[SEP]

- To present the state of the art in design approaches used to achieve defence in depth in pressurized water reactors, pressurized light water cooled heavy water moderated reactors, high temperature gas cooled reactors, sodium cooled and lead cooled fast reactors, and non-conventional designs within the SMR range;
- To highlight benefits and negative impacts in areas other than safety arising from the implementation of inherent and passive safety design features;
- To identify issues of performance reliability assessment for passive safety systems in advanced reactors, and to highlight further research and development needs arising therefrom.

The SMR concepts included represent pressurized water reactors (5 inputs), pressurized light water cooled heavy water moderated reactors (1 input); high temperature gas cooled reactors (HTGRs, 1 input); liquid metal cooled fast reactors (1 input for sodium and 1 input for lead cooled reactors), and a single non-conventional design, which is a lead-bismuth cooled very high temperature reactor with pin-in-block HTGR type fuel.

The HTGR input is the GT-MHR (287.5 MW(e)), a collaborative US–Russian concept of an HTGR with pin-in-block type fuel, is at the basic design stage. Its progress toward deployment may be not so advanced as that of some other HTGRs, however, as passive safety design features of all HTGRs have much in common, the GT-MHR is quite representative of the passive safety design options implemented in other HTGRs.

The report includes a section providing an overview of the considerations for the incorporation of inherent and passive safety features into safety design concepts of SMRs. Another one presents the design approaches applied by the designers to achieve defence in depth in SMRs, including both passive and active safety design features and systems to highlight the role of inherent and passive features and show how they may affect the design/function of the active safety systems. Eventually, annexes provide descriptions of the design features of the considered SMRs used to achieve defence in depth. Among them, an annex is specifically dedicated to the considered HTGR, the GT-MHR.

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of the Nuclear Power Plants: Design IAEA Safety Standards Series No. NS-R-1, IAEA, Vienna (2000).

3.2.6. INSAG-12 - Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev.1 (1999)

The International Nuclear Safety Advisory Group (INSAG) provides a self-standing report on safety principles for electricity generating nuclear power plants. This report has been developed to

ensure improvement in safety of nuclear power plants over the years and to underline the need for common safety principles for all countries and all types of nuclear power plants.

INSAG has prepared this report in accordance with its terms of reference “to formulate, where possible, commonly shared safety concepts”. The understanding and application of these safety principles should improve safety and benefit everyone, especially those in countries that use or intend to use nuclear power as an energy source.

High technology does not jeopardize safety, as is often believed to be the case; it is the means by which safety is achieved. The objectives and principles set out in this report are directed towards the universal and effective achievement of this purpose in the future.

This revision of 75-INSAG-3 was prepared in order to take account of the recent development of and refinements in nuclear safety principles for nuclear power plants. When 75-INSAG-3 was issued in 1988, the total amount of experience that had been accumulated worldwide was about 4600 operating reactor-years. Today, the figure is about 8700 operating reactor-years. This greater experience in both the design and operation of nuclear plants, coupled with knowledge deriving from extensive research and development programmes, has led to significant gains in the safety and performance of most operating plants and in the safety of future plants now under construction.

Even though nuclear power technology is quite mature for some reactor systems, it is necessary to encourage the evolution and development of concepts that might be important in meeting long term global energy needs. Several future reactors (which could be built in significant numbers over the next 20 years) are being considered or are under development, and this has led to the identification of a number of additional desirable features and objectives that are set out in this revision of 75-INSAG-3. They include a simplification of design, operations and maintenance, and the increased use of information technology and digital technology. However, additional measures to prevent accidents and a further reduction in the probability and consequences of an off-site radioactive release remain the highest priorities among the future safety provisions.

INSAG hopes that this revised version of 75-INSAG-3 will be used as extensively throughout the world as the original edition and that it will continue to serve as a basic reference for the safety of nuclear power plants and for achieving a broad international consensus on basic safety principles for present reactors and future reactor concepts.

3.3. COUNTRY EFFORTS ON REQUIREMENT DEVELOPMENT (KAERI, RSA, CHINA, EUROPE, INDONESIA, JAPAN, USA)

Each CSI write ½ - 1½ page – 1Aug2018

3.3.1.1. Korea (Republic of)

The Korea Institute of Nuclear Safety (KINS) and the Korea Atomic Energy Research Institute (KAERI) has been conducting research on regulatory technologies of high temperature gas-cooled reactors (HTGR) in Korea.

In 2004-2005, KINS conducted a research on the status of regulatory technology of HTGR for hydrogen production [27],[28]. This was a basic study of HTGR regulations that analyzed the design and regulatory characteristics of HTGR, identified general safety issues, and assessed the applicability of current nuclear energy-related laws and regulations.

In 2007-2010, KINS conducted a follow-up research to develop a technology - neutral regulatory system for Generation IV nuclear reactors such as HTGR for hydrogen production and sodium - cooled fast reactors (SFR), where general design requirements for technology - neutral regulations were drafted [29].

In 2008, KINS conducted another research to establish the direction of development of Generation IV nuclear reactor licensing procedures and regulatory requirements [30]. A preliminary study was carried out to derive the direction of development of licensing procedures and regulatory requirements for multipurpose nuclear reactors used for purposes other than power generation, such as demonstration reactors of SFR and HTGR.

In 2010-2012, KINS developed key licensing technologies for HTGR [31]:

- (1) The deterministic safety requirement system similar to Approach 2 in Section 4.2 of this TECDOC was adopted as the safety requirement framework for HTGR. The draft general (Technical Standard Rules) and specific (Nuclear Safety and Security Commission Notices) safety requirements for HTGR were developed reflecting the results of a study on applicability of current LWR safety requirements to HTGR.
- (2) By analyzing the differences in major design features between HTGR and LWR, the licensing issues were identified and their workarounds were sought that should be taken into account especially in the conceptual design phase of HTGR.
- (3) Based on the findings in investigation of the core nuclear design characteristics and the major system thermal-fluidic phenomena of HTGR, the Phenomena Identification and Ranking Table (PIRT) was developed and the event classification and acceptance criteria was established. Reflecting these results, the list of demonstration tests required for the safety and performance verification was derived for a demonstration HTGR and related experimental technologies were surveyed.

In 2012-2014, KINS continued its in-depth study on the licensing technologies of HTGR.[32]:

- (1) The draft general safety requirement developed in the period 2010 - 2012 was practically refined in consultation with relevant experts from academia and design bodies.
- (2) Defense-in-depth and functional containment concepts were identified as the key issues in licensing HTGR and their solutions were explored. The implementation validity of the defense-in-depth concept was verified by the IAEA's Objective-Provision Tree (OPT) method. A review of the functional containment concept showed that confinement (not containment) could be adopted in HTGR but the barrier function against fission product leak should be sufficiently confirmed.
- (3) The safety effects of nuclear fuel, reactor core design, accident analysis methods, and passive cavity cooling system were analyzed to determine the validity of HTGR safety design. The passive safety system was found to ensure the design safety of HTGR owing

to better reliability than the active system. However, the passive system was also found to a weak driving force.

In the time frame of 2012 -2015, KAERI developed a step-wise demonstration strategy for both nuclear process heat plant and nuclear hydrogen plant using a single HTGR [33]. The first step is to demonstrate HTGR technologies at 750°C for process heat application whose technology readiness level is mature enough for a demonstration and, then, the second step is to demonstrate nuclear hydrogen technologies after system upgrade and resolution of technical challenges at 950°C. For licensing of the demonstration plant, conventional two-step licensing process, that is the construction permit and the operating license, was proposed both for 750°C and 950°C plants. In addition, standard design approvals for both plants were proposed to be pursued in compliance with Korean Nuclear Safety Act for future commercialization. In the licensing process, results of the regulatory framework studies by KINS will be reflected and, thus, the licensability of the systems is to be secured. In parallel, potential licensing issues specific to HTGR to non-electric applications were identified and reviewed. They included high temperature codes and standards, reduction of emergency planning zone (EPZ), multi-module licensing and identification of boundary between nuclear and industrial facilities, etc. In an effort to enhance the licensability of key technologies used in the design and construction of the demonstration plant, a technology verification and validation plan was developed for the design tools and methods as well as for the performance and safety tests.

3.3.1.2. South Africa

[Click here and type the body of your report]

3.3.1.3. China

In China, National Nuclear Safety Authority (NNSA) released many safety requirements and guides based on IAEA safety standards and guides. For example, in the end of 2016, NNSA released the safety design requirement based on IAEA newest version of SSR 2/1 rev.1. Also, many IAEA safety guides are converted to NNSA safety guides. Although IAEA and NNSA mentioned these safety requirements and guides are mainly based on LWR experience and focused mainly on LWR, the design of other type of NPPs can also be referenced to these requirements and guides. This is practiced in the licensing process of HTR-10 and HTR-PM in China. In general, most of the requirements in these documents are applicable to HTR design, and special requirements corresponding to HTR features either are described in “policy announcement for HTR-PM licensing”. These special requirements were released by NNSA, or are specified in design criteria for HTR-PM, which was drafted by designer and was reviewed by NNSA, before the licensing process of HTR-PM. Of course, more detailed requirement for the design, manufacturing, installation of structure, system and components are based on industrial standard such as ASME, IEEE, IEC and some Chinese standards.

Based on these experiences, another project was launched in China to develop HTR specific version of safety design requirements and guides, starting from current LWR version, and reflecting the HTR features. This project is the joint project between NNSA and designer and is

supported by National Energy Administration. For all these requirement and guides, the first draft versions are already developed and are waiting for final improvement from NNSA.

For the safety design requirement, the philosophy is comparable to the deterministic approach in this CRP (known as approach 1, see Section 4.1), and similar results are achieved. For example, the scope of Design Extension Condition, mitigation features instead of safety feature for DEC, concept of Vented Low Pressure Containment (VLPC), are closely similar. Naturally, the final text is slightly different because of different compromise and consensus in different work group. For instance, more detailed requirement for VLPC is described in Chinese version, and more feature according to HTR-PM and HTR-PM600 (new 600MWe HTR plant designed by INET) experience are described.

Besides the HTR specific version of design safety criteria, more requirement and guides which are HTR-specific are listed in Table 5, covering all aspects of HTR NPP. Therefore, it is a very large project. Through the development of guides, the applicability and effectiveness of top level requirement can be checked and supported by lower level guides. By all means, applicability and effectiveness of these requirements and guides can be checked against the design of HTR-PM and HTR-PM600, which is the biggest advantage for this project in China.

TABLE 5. LIST OF REQUIREMENTS AND GUIDES DEVELOPED FOR HTR NPP IN CHINA

No	Title	Description
1	Safety requirement for design of HTGR power plant	Based on IAEA SSR 2/1 rev.1
2	Safety requirement for operation of HTGR power plant	Top level requirement
3	Format and content of the safety analysis report for HTGR power plant	Guide, based on IAEA guide, NRC SRP, and HTR-PM experience
4	Safety design of the core for HTGR power plant	Guide
5	Design and fabrication of fuel element for HTGR power plant	Guide
6	Beyond design basis accident management programme for HTGR power plant	Guide
7	Safety evaluation and verification for HTGR power plant	Guide
8	Design of vented low pressure containment for HTGR power plant	Guide
9	Instrumentation and control system important to safety for HTGR power plant	Guide

10	Fuel handling and storage system for HTGR power plant	Guide
11	Radiation protection design for for HTGR power plant	Guide
12	Core and fuel management for HTGR power plant	Guide
13	Safety function and component classification for HTGR power plant	Guide, based on IAEA SSG 30
14	Reactor coolant system and related system for HTGR power plant	Guide
15	Operation limit and condition and operation procedure for HTGR power plant	Guide
16	Commissioning test for HTGR power plant	Guide
17	Maintenance, supervision and in-service inspection for HTGR power plant	Guide
18	Decommissioning preparedness for HTGR power plant	Guide

3.3.1.4. Europe

See elements of answer (for Germany) in:

ANNEX IX HTR-MODULE LICENSING BASIS EVENTS

ANNEX VIII LICENSING PROCEDURE CONCEPT FOR THE HTR-MODULE

ANNEX II TECHNICAL REPORT: HTR-MODULE: CLASSIFICATION AND QUALITY REQUIREMENTS FOR SYSTEMS AND COMPONENTS

3.3.1.5. Indonesia

[Click here and type the body of your report]

3.3.1.6. Japan

JAEA has been developing the HTGR technology and its heat application technologies (i.e., hydrogen production technology using the thermochemical water splitting Iodine Sulfur (IS) process and power generation by helium gas turbine), and is accumulating the valuable data on the HTGR safety features through the operation and the safety demonstration tests using the HTTR to establish the fundamental HTGR technologies for the commercial HTGR systems.

Figure 14 shows the overview of the activity to develop the safety standard for the commercial HTGR in Japan. The safety requirements for the HTTR design, safety evaluation methods, graphite structure design code and high-temperature structural design code for HTTR were developed in

1980's based on the R&D for HTTR such as fuel, graphite, heat resistant material, high-temperature component, core physics, thermal hydraulics, safety analysis, seismic evaluation methods, etc. The HTTR safety requirements were formulated by implementing the new HTGR specific requirements on LWR requirements and removing the LWR specific requirements. However, the safety features of HTGR were not fully incorporated into the safety requirements for the design of HTTR because there was no experience of the construction and operation of the HTGR type reactors in Japan at that time.

After the licensing and construction of HTTR, JAEA is accumulating the know-how and data by HTTR safety demonstration test which showed the excellent safety features of HTGR such as high quality of fuel performance, reactor shutdown by relatively large negative Doppler temperature coefficient without the control rod insertion and core heat removal from outside reactor pressure vessel during loss of forced cooling. These data can be used as technical basement of safety requirements that fully consider the safety features of HTGR. JAEA also has been developing the safety requirements and design consideration for a nuclear hydrogen production system [34].

The research committee on the safety standards for HTGRs [35] was established in 2013 under the Atomic Energy Society of Japan (AESJ) with the support of the Research Association of High Temperature Gas Cooled Reactor Plant (RAHP) which is structured by Japanese industry (utility companies and nuclear plant vendors, etc.) and academia, as a part of promotion activities on HTGR reactor plants. The objective of the research committee is to draft of the specific safety requirements (SSR) for the design of modular HTGRs analogous to the IAEA SSR for LWR design (IAEA SSR-2/1 (Rev.1)) taking into account the modular HTGR safety features so as to provide the safety requirements and guide for designers and regulators, and to show the safety advantages of modular HTGR to the future HTGR users as well as nuclear experts in other fields. The development of the safety requirements for the design of modular HTGRs, which incorporate the HTGR safety features demonstrated using HTTR, lessons learned from the Fukushima Daiichi accident and requirements for the integration of the heat application facility (i.e., hydrogen production plants) was finished in March 2015. JAEA contributed to this research committee by providing the knowledge and technical information of HTGR and leading the discussion. JAEA provided the drafted safety requirements to the IAEA CRP on the modular HTGR safety design, and it was reviewed and discussed in the CRP as Approach 2.

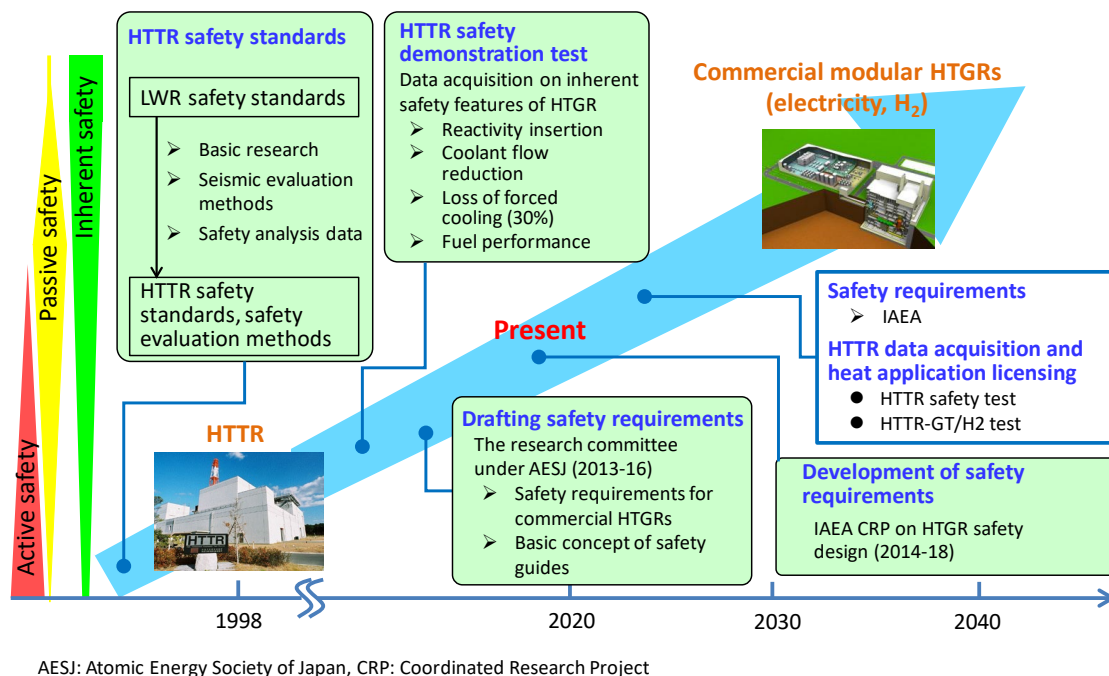


FIG. 14. The activities to develop the safety standard for the commercial modular HTGR.

3.3.1.7. United States of America

Action 2 - US developments related to CRP safety design criteria - May 30 2019 update

Recent DOE and industry interactions with the NRC continue to make progress on the regulatory framework for advanced non-LWRs in two related areas: Advanced Reactor Design Criteria and Risk-Informed Performance-Based licensing.

Advanced Reactor Design Criteria (ARDC)

On April 4, 2018 the U.S. Nuclear Regulatory Commission (NRC) issued Regulatory Guide 1.232, Guidance for Developing Principal Design Criteria for Non-Light Water Reactors. The regulatory guide's generic set of Advanced Reactor Design Criteria cover most non-light-water technologies. The regulatory guide (RG) also includes technology-specific modular High-Temperature Gas-cooled Reactor Design Criteria (mHTGR-DC).

The overall purpose of the ARDC RG is to establish clear guidance for the development of the principal design criteria (PDC) that advanced non-LWR developers will be required to include in their Nuclear Regulatory Compliance (NRC) license applications.

The expected benefits include: reduced regulatory uncertainty for advanced non-LWR developers, improved guidance for NRC staff reviewing advanced reactor license applications, and improved timeliness and efficiency of licensing activities for both applicants and NRC staff.

The proposed ARDC seek to preserve the underlying safety principle(s) originally expressed in the corresponding existing general design criteria (GDC) that were developed predominantly for LWRs. However, the ARDC also recognize that safety design solutions can differ substantially from those associated with light water reactors (LWRs), for example, advanced reactors employ simplified, passive, and inherent safety features to a greater extent: challenges to advanced reactor safety systems can greatly vary, and system components and nomenclature may be very technology-specific.

It is noted that the deterministic structure of the GDCs was modified in some cases to align with previous Next Generation Nuclear Plant (NGNP) proposals to the NRC for modular HTGRs including multi-module integrated risk, functional containment, and consideration of multiple failures (not limited to the single failure criterion). Further, the mHTGR-DC were also assessed using the required safety functions from the Design Basis Events selected with risk-informed insights gained over 25-30 years to ensure completeness. This assessment resulted in the addition of new mHTGR-DC, for example: radionuclide retention in the fuel rather than reliance on coolant retention and a leaktight containment structure the structural design bases of the reactor, the reactor vessel, and the reactor cavity cooling for passive heat removal.

The mHTGR design criteria interactions with the regulator and the issuance of this RG with MHTGR design criteria are directly relevant to the IAEA CRP Approach 2 for the development of MHTGR safety design criteria.

Industry-Led Licensing Modernization Project (LMP)

The LMP's objective is to develop technology-inclusive, risk-informed, and performance-based (RIPB) regulatory guidance for licensing non-LWRs for NRC to review and potentially endorse. The NRC has reviewed four LMP white papers: Selection of Licensing Basis Events Draft Report, Probabilistic Risk Assessment Approach Draft Report, Safety Classification and Performance Criteria for Structures, Systems, and Components, and Risk-Informed and Performance-Based Evaluation of Defence-in-Depth Adequacy. The NRC has discussed these white papers with industry and other interested stakeholders during a series of public meetings and provided feedback to the LMP project, setting the stage for industry and NRC to agree on more formal guidance for implementing the LMP's proposed approach.

In mid-2018, the Nuclear Energy Institute worked closely with the LMP Project team to develop this more formal guidance, which was then reflected in NEI 18-04, "Risk-Informed Performance-Based Technology Inclusive Guidance for Advanced Reactor Licensing Basis Development". The NRC staff then developed a companion Regulatory Guide (draft) that describes their intention to endorse the proposed approach. This information is reflected in NRC's DG-1353, "GUIDANCE FOR A TECHNOLOGY-INCLUSIVE, RISK-INFORMED, AND PERFORMANCE-BASED APPROACH TO INFORM THE CONTENT OF APPLICATIONS FOR LICENSES, CERTIFICATIONS, AND APPROVALS FOR NON-LIGHT-WATER REACTORS".

NEI 18-04 (the US industry's proposal) and DG-1353 (NRC staff's plan for endorsement) have both been reviewed by the Commission's independent Advisory Committee on Reactor Safeguards (ACRS). The ACRS concluded that "...the approach has matured to the point of being ready for

application”, and recommended that “the Commission adopt the approach proposed by the staff for a technology-inclusive, risk-informed, and performance-based methodology for informing the licensing basis and content of applications for non-light-water reactors”. The NRC’s DG-1353 document is now undergoing a final 60 day public comment period that ends in early July, 2019. After addressing any comments, it is expected that the NRC will formally endorse the approach for use by industry later in 2019.

The LMP effort, particularly as described in the safety classification white paper, is directly relevant and most closely aligned with the IAEA CRP Approach 1.

Taken together, the ARDC and LMP interactions with the US NRC have and will continue to provide guidance for a blended approach for the development of mHTGR design criteria in an analogous fashion as the IAEA CRP blend of Approaches 1 and 2 for MHTGR safety design criteria.

3.3.2. Current Licensing experience on the HTR-PM

The HTR-PM project was started in early 2001, followed by planning, feasibility study, basic design, review of PSAR, engineering design, manufacturing, construction, review of FSAR, etc. The construction started in 2012, and power operation is expected in 2020. There are many experiences in the licensing process for HTR-PM, such as:

- Early involvement of licensing authorities is very important (for example review of HTR-PM design criteria, release of policy announcement for HTR-PM licensing);
- It is more reasonable to adopt evolutionary approach instead of revolutionary approach for the design, and licensing framework (adoption of mature steam cycle, based on current available framework, adoption of new idea based on consensus and dialogue);
- The inherent safety features of modular HTGR is recognized by China National Nuclear Safety Authority (NNSA), this is the basis for the NNSA to adopt LWR based licensing framework with some flexibility;
- Most of safety requirement, or safety design criteria are the same among different type of NPPs, the current licensing framework developed from LWR experience is a very good basis for modular HTGR;
- The detailed requirements for each structure, system and component for HTR-PM are more important for design and licensing, especially by taking into account industrial experience and industrial capability;
- It is more straightforward and simpler to develop detailed specifications for each SSCs, even with the same terminology used in other type of NPPs, with clear definition and in early agreement with licensing authority. One example is to use the name of vented low pressure containment in HTR-PM;
- Detailed requirements for most important structures, systems and components are defined in HTR-PM design criteria, which is drafted by designer (and contains 40 chapters) and is reviewed by NNSA before its formal licensing process.

- The design, and the safety requirement must achieve the balance between safety requirement and feasibility/economy;
- Safety Analysis Report (SAR) structure is based on Standard Review Plan from NRC.
- Most of Standards are based on international experience (ASME, IEEE, IEC, ...)

Before the licensing phase, NNSA released “Policy announcement for HTR-PM licensing”, addressed the key issues and position from the authority viewpoint. The titles for each section in the policy announcement include:

1. Forewords
2. Safety objectives (safety goals)
3. Defense in depth
4. General design criteria
5. Containment: VLPC
6. Accident source term: mechanism based
7. Emergency plan: Technically not needed
8. Application of PSA: to support design
9. V&V for safety analysis software

The key safety features of HTR-PM are recognized in the Policy announcement:

- Inherent safety philosophy
- Long and smooth time envelop for accident
- Good performance of fuel for normal operation and accident conditions
- Limited radioactive release in case of accident
- Probabilistic safety goal: the accumulated frequency for accident scenario whose release is larger than 50mSv will be less than 10^{-6} / reactor year;
- Adoption of Vented Low Pressure Containment (VLPC) concept and terminology;
- Beyond design basis accident (BDDBA) will be evaluated as part of probabilistic safety analysis (PSA) and will be check against Probabilistic safety goal.

Based on these philosophy and preparation, the licensing process for HTR-PM is very smooth, there are no unsolved issues left; although NNSA paid much more attention to the Verification and Validation (V&V) of safety analysis software, results from the full scale test of key components and systems, and the surveillance of manufacturing and installation process.

3.3.3. Licensing experience for HTGRs in the past

(not details – just that FSV and THTR was licensed and operated but was not mHTGRs)

3.3.4. Reactors that operated and went through some licensing process in the past (short with references, if detail in appendix reference this) Historic built, HTR-Module HTTR, HTR-10, PBMR,

(not details – just that FSV and THTR was licensed and operated but was not mHTGRs)

3.4. OECD/NEA GSAR (NEW NAME), GIF?

(F. Reitsma – 1Aug2018 (MDEP-OECD – Ewa))

4. SAFETY DESIGN CRITERIA APPROACHES

Need to put here a general description of the two approaches

Two approaches are followed as demonstrated in Figure 15 and Figure 16. In the first approach the participants are developing and applying a safety design process to specific reactor designs. From this exercise the required safety functions will be assigned to systems that will then be used to derive the high level requirements (a bottom-up approach). In the second approach the current WCR requirements are used as the basis and through engineering judgement and other considerations amendments to the current requirements are proposed. The final outcome will of course be compared with the current safety requirements and also verified against the fundamental safety functions, and ultimately also the safety of the public and workers by dose limits.

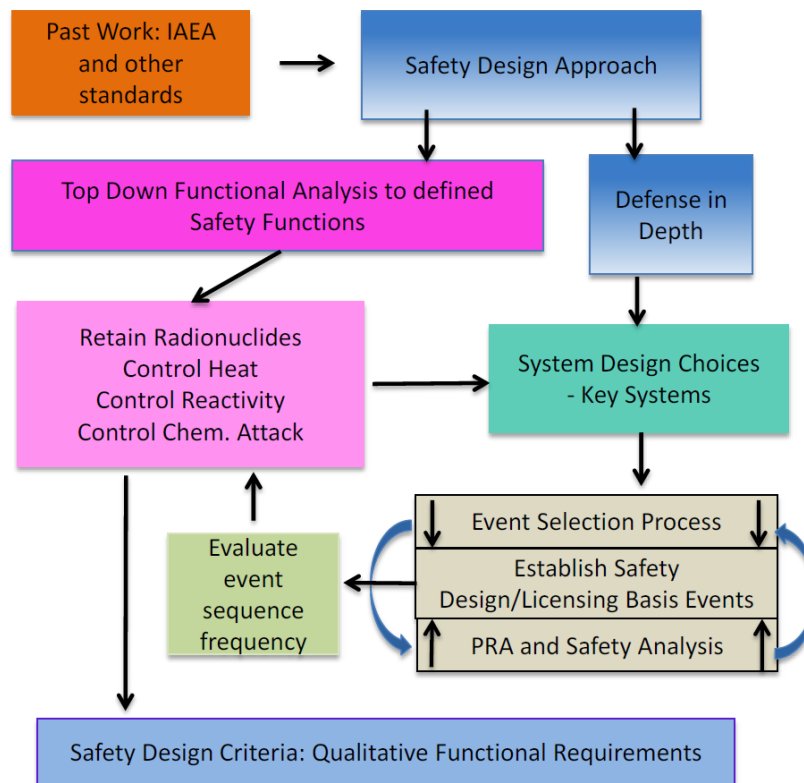


FIG. 15. Approach 1 "Bottom-Up" approach.

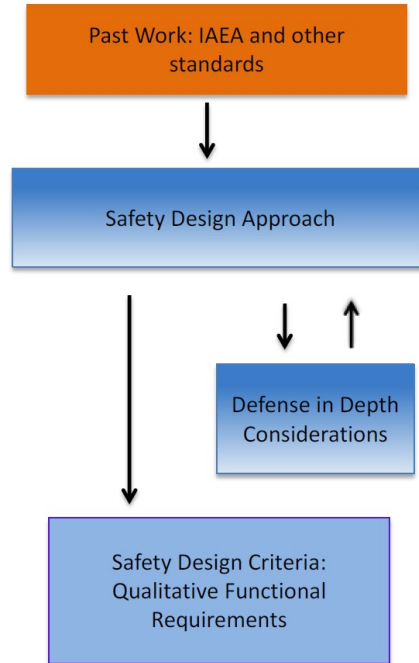


FIG. 16. Approach 2: "Top-Down" approach: from IAEA SSR-2/1 to HTGR requirements through expert judgement and review.

Examples of non-applicable requirements from the IAEA Specific Safety Requirements No. SSR-2/1 Safety of Nuclear Power Plants: Design include:

- safety concepts such as design extension conditions “with core melting” is not applicable to HTGRs and need alternative interpretations or ideally alternative definition of plant states, design basis and beyond design basis accident conditions
- specific requirements on fuel need new interpretations especially for pebble bed type fuel since concepts such as fuel pin, cladding and fuel assembly is not defined. Also pebbles fuel are much more robust and handled quite differently and is for example designed to be dropped into the core and spent fuel storage
- the focus of the requirements on the containment function and structures needs to stress the dominant role played by the coated particle fuel as the most important barrier to fission product release. HTGRs lack the “cascading cliff edge effects” [36] and the requirements of multiple barriers and the implementation of defense in depth should be considered carefully, but also clearly differently.
- since the gas coolant is not condensable a helium pressure boundary failure and release into a leak-tight containment will result in a sustained elevated pressure condition since the pressure cannot be reduced by cooldown. A pressurized containment condition will act as a driving force to transport radioactivity into the environment in case of a failure. In the case of CP fuel no large early release is expected but the delayed release, due to fuel and core heat up, can potentially be larger. It is thus generally accepted that early pressure release is preferable.

– requirements on chemical attack, especially on massive air ingress, should be added in order to strengthen the safety requirements

– since HTGRs are ideal for high temperature process heat applications and cogeneration, specific attention needs to be given to co-located facilities (such as a chemical plant) as well as multi-module considerations and aspects such as connectivity and shared systems.

The comprehensive and dual approach followed in the CRP should lead to well defined and a germane set of safety design criteria that does not only take the specific safety characteristics into account, but has also through the exercise been implemented and tested for actual example modular HTGR designs.

Need to put here a general description of the following figure (overlap circles)

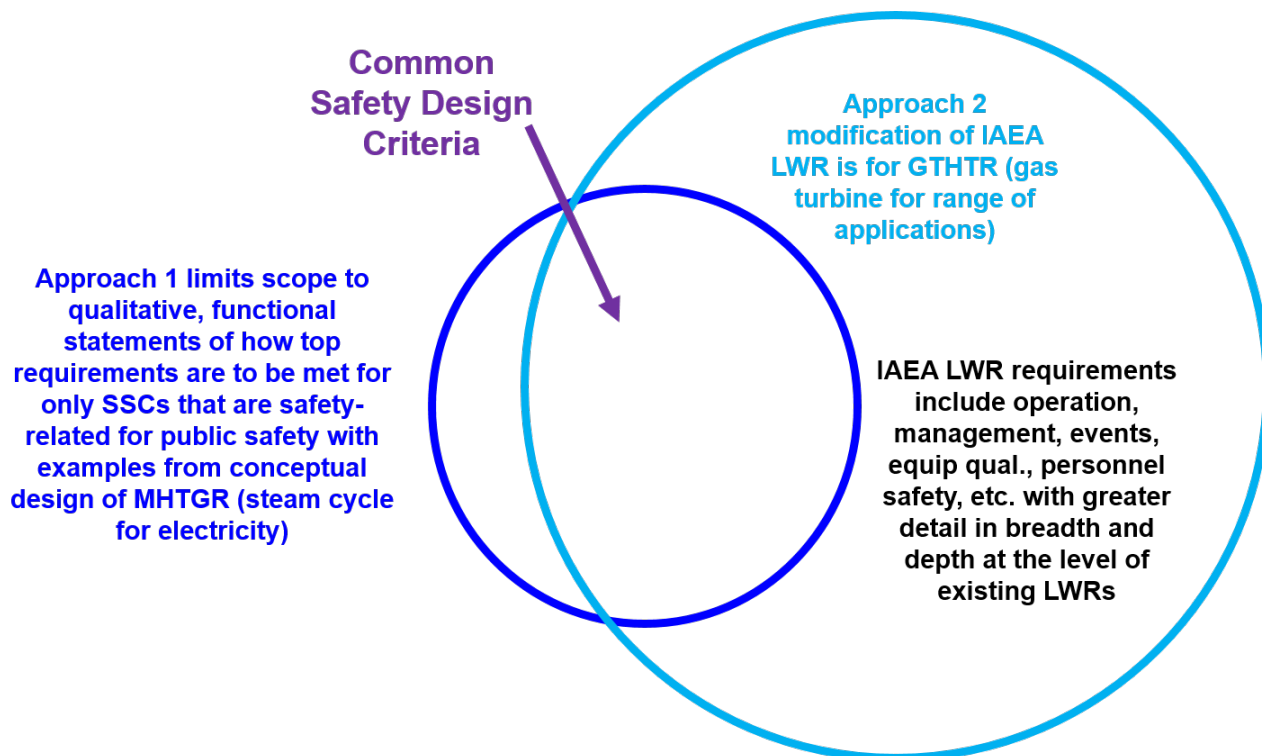


FIG. 17. Illustration of scope, breadth, depth, and terms of two approaches.

4.1. APPROACH 1 (BOTTOM UP APPROACH)/ APPROACH 1 TO DEVELOPMENT OF MODULAR HTGR SAFETY DESIGN CRITERIA

– [Draft CRP TECDOC on Blended Approach → (Action 1 (US))]

A risk-informed, performance-based approach to supporting the licensing basis that uses both probabilistic and deterministic elements has been introduced during the early stage of the U.S. modular HTGR design and licensing process. This approach differs from the current licensing framework, which was developed for reactors with a fundamentally different safety design philosophy. Risk insights developed from a probabilistic risk assessment (PRA) are viewed as essential to developing a design that is optimized in meeting safety objectives and in adapting the existing regulatory requirements to the safety design approach of the modular HTGR. Results and insights from PRA are needed to assure the safety of the design against the Nuclear Regulatory Commission (NRC) Safety Goals (NRC 1986), and to determine whether any additional requirements or guidance may be necessary that are specific to the modular HTGR. The approach has been the subject of an IAEA report (IAEA SRS No. 54).

As depicted in Table 6, the licensing elements start with first, **what** must be met with the Top Level Regulatory Criteria (TLRC), then, **when** the TLRC must be met both for probabilistic risk insights and deterministic events, and then to **how** the TLRC that ultimately lead to the SDCs.

TABLE 6. STEPS IN THE RISK-INFORMED APPROACH FOR DEVELOPMENT OF MODULAR HTGR SAFETY DESIGN CRITERIA

- | |
|--|
| <ol style="list-style-type: none"> 1. What must be met: <ul style="list-style-type: none"> – Top Level Regulatory Criteria (TLRC) 2. When TLRC must be met: <ul style="list-style-type: none"> – Risk-informed Licensing Basis Events (LBEs) – Deterministic Design Basis Accidents (DBAs) 3. How TLRC must be met: <ul style="list-style-type: none"> – Safety Functions – SSC Safety Classification – Safety Design Criteria |
|--|

– [Draft CRP TECDOC on Blended Approach → last version is from JIM (Action 1)]

4.1.1. Top Level Safety Requirements

The primary qualitative safety objective for the modular HTGR is not to disturb the normal day-to-day activities of the public. The corresponding quantitative objective of the modular HTGR design is to limit the dose from accidental radionuclide 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, (e.g., 400 m), from the reactor. In addition, to eliminate the need for public evacuation or sheltering beyond the site boundary, the modular HTGR design goal is to meet the Environmental Protection Agency (EPA) plume exposure Protective Action Guides (PAGs) (EPA 2017) at the EAB.

Existing LWR technical licensing requirements assure adequate public safety through a set of criteria from the NRC regulations and guidance. These requirements were developed for, and have been traditionally applied to, licensing of LWRs. There are significant differences in the modular HTGR technology and safety basis from those of the LWRs, that require interpretation of the NRC regulations. Additionally, these regulations were traditionally applied on a prescriptive basis during initial licensing of current LWRs. However, there has been a general trend in NRC oversight of operating LWRs toward a more risk-informed and performance-based process. The NRC assessed the advantages of applying this approach to the licensing of new and advanced nuclear technologies, and concluded that such a process appears to have merit and should be applied to the licensing of the next generation nuclear plant (NGNP) demonstration plant (NRC 2008). This was also the licensing approach recommended by the NRC and DOE in developing the licensing strategy for NGNP (DOE/NRC 2008). Accordingly, the licensing and safety basis for the modular HTGR was developed using a risk-informed, performance-based technical approach that adapts existing NRC licensing requirements in establishing HTGR design-specific licensing requirements. As part of the process of risk-informing regulatory compliance, TLRC were identified from NRC and EPA regulations and guidance that establish dose limits on consequences from LBEs to assure public safety (INL 2010c). The TLRC screening criteria:

1. Provide direct public health and safety acceptability limits in terms of individual radiological consequences
2. Are independent of modular HTGR reactor type and site
3. Provide well-defined, quantifiable risk criteria.

The primary sources in Table 6 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.

TABLE 7. TOP LEVEL REGULATORY REQUIREMENTS FROM U.S. NUCLEAR REGULATORY COMMISSION AND U.S. ENVIRONMENTAL PROTECTION AGENCY FOR PUBLIC SAFETY

10 CFR 20 Annual Off-site Dose Guidelines
• 100 mrem/yr (1 mSv) total effective dose equivalent • Measured on a cumulative basis annually at the site Exclusion Area Boundary (EAB) • For normal operation and anticipated events
10 CFR 50.34 /10 CFR 52.79 Accident Off-site Doses
• 25 rem (250 mSv) total effective dose equivalent • Evaluated at the site EAB at 2 hours and at the site Low Population Zone (LPZ) at 30 days • Design basis for off-normal events
EPA PAGs Off-site Doses
• 1 to 5 rem (10 to 50 mSv) total effective dose equivalent for sheltering or evacuation • Evaluated at the site Emergency Planning Zones • Emergency planning and protection during off-normal events

NRC Safety Goals Individual Fatality Risks

- Prompt Quantitative Health Objective (QHO) of 5×10^{-7} /yr individual risk of early fatality for offsite public to 1 mile
- Latent QHO of 2×10^{-6} /yr individual risk of late fatality for public offsite to 10 miles
- Overall assurance of negligible (0.1%) individual risks from nuclear power plants during normal operation and off-normal events.

4.1.2. Licensing Basis Event Selection

LBEs are the comprehensive set of event sequences used in development of the license application that form the basis for plant analysis and that represent the characteristic performance of the plant in all analyzed frequency and consequence ranges. LBEs include anticipated operational occurrences (AOOs), design basis events (DBEs), and beyond design basis events (BDBEs) as well as the deterministically selected design basis accidents (DBAs). Analyses of AOOs, DBEs, and BDBEs include the plant response of both safety-related and nonsafety-related SSCs. In contrast, analyses of DBAs include the plant response with only safety-related SSCs performing. The white paper on LBE selection prepared for the NGNP project describes a systematic, performance-based and risk-informed methodology for selecting and classifying LBEs for the modular HTGR, consistent with current NRC policies and guidance on the application of deterministic design criteria and the use of PRA techniques (INL 2010c). The methodology integrates the use of deterministic safety principles and risk-informed insights as critical inputs into the selection of LBEs. These events include specific scenarios for which mechanistic source terms are derived and assessed against offsite dose criteria.

Given the selection of a modular HTGR to meet the top safety requirements, as discussed in Section 4.1.1, the next major element in the approach is the selection of when these requirements must be met. The selection approach is risk-informed and results in a wide spectrum of off-normal LBEs that includes AOOs, DBEs, and BDBEs. These LBE categories are defined by the mean frequency of the event sequence on a per plant year basis.

4.1.2.1. Anticipated Operational Occurrences Region

AOOs are those conditions of plant operation expected to occur one or more times during the life of the plant. Current LWR plants were licensed to operate for an initial 40-year period; however, with the advent of license renewal, operating licenses of conventional LWRs have been increased for some plants by 20 years. Therefore, a conservative value of 1×10^{-2} per plant year is used to establish the lower bound of the AOO region.

For this region, 10 CFR Part 20 provides the applicable criteria, as it specifies the numerical guidance to assure that releases of radioactive material to unrestricted areas during normal reactor operations, including AOOs, are maintained as ALARA. This provides the upper dose consequence limit of 100 mrem TEDE at the EAB. The EAB is expected to be the same area as the controlled area boundary. The EAB is defined as that area surrounding the reactor, in which

the reactor licensee has the authority to determine all activities including exclusion or removal of personnel and property from the area.

4.1.2.2. Design Basis Event Region

The DBE region encompasses offsite radionuclide releases that are not expected to occur during the lifetime of a nuclear power plant of one or more reactors, but they may be encountered during the lifetime of a fleet of nuclear power plants of similar design.

The dose requirement from 10 CFR 50.34 for accidents that are designed for and reported in an SAR is 25 rem TEDE at 2 hours at the EAB and at 30 days at the LPZ. For Part 52 applications, the requirement is the same, but provided in 10 CFR 52.79. For site acceptability, the requirement is the same but provided in 10 CFR 100. For purposes of this report, 10 CFR 50.34 will be cited with the understanding that the same dose requirement is also provided in 10 CFR 52.79 and 10 CFR 100. Establishing 10^{-4} per plant year as the lower frequency for the design basis region is consistent with LWR regulatory guidance for the design goal frequency on a per reactor year basis of core damage events.

As noted in the draft American Nuclear Society (ANS) Standard 53.1, “Nuclear Safety Design Process for the Design of Modular Helium-Cooled Reactor Plants” [48]:

The adoption of the DBE region’s lower frequency limit of 1×10^{-4} per plant-year is appropriate because it is applied on a per-plant basis and accounts for possible multiple MHR modules. In addition, the expression of the frequency metric on a per plant-year basis enables the assessment to include event sequences involving only one or multiple reactor module source terms and thereby provides a more complete risk assessment as compared with the approach of analyzing each reactor module on an independent reactor-year basis.

For the DBE region, the 25 rem total effective does equivalent criterion in 10 CFR 50.34 provides the quantitative dose guidance for accidental releases for siting a nuclear power plant to ensure that the surrounding population is adequately protected. The combination of the selected frequency limits and dose limits for the DBE region ensures that the NRC Safety Goal QHOs for individual risk of latent cancer fatality is met by several orders of magnitude for all event sequences within the DBE region.

4.1.2.3. Beyond Design Basis Event Region

The BDBE region, comprised of very rare events that are not expected to occur during the lifetime of a large fleet of nuclear power plants, is considered to assure that the risk to the public from low frequency events is acceptable. The BDBE region considers events with a mean value below the DBE region’s lower frequency limit of 1×10^{-4} per plant-year.

The frequency cutoff implicit in the acute fatality risk goal in NUREG-0880, “Safety Goals for Nuclear Power Plant Operation,” is taken as the lower frequency boundary of the BDBE region. NUREG-0880 notes that the individual mortality risk of prompt fatality in the United States is about 5×10^{-4} per year for all accidental causes of death. The prompt mortality risk design objective limits the increase in an individual’s annual risk of accidental death to 0.1% of 5×10^{-4} ,

or an incremental increase of no more than 5×10^{-7} per year. If the frequency of a scenario or set of scenarios is at or below this value, it can be assured that the individual risk contributions from these scenarios would still be within the safety goal, independent of the magnitude of the consequences with a significant residual margin. Therefore, 5×10^{-7} per year is taken as the lower frequency for the BDBE region.

The very rare events of the BDBE region include event sequences of frequency comparable to what is commonly referred to as severe accidents for existing reactors and, in response to the Fukushima accident, the Design Extension Conditions (DEC) that consider external events and multiple failure events that the traditional deterministic licensing approach does not consider.

4.1.2.4. Depiction of Licensing Basis Events on Frequency-Consequence Chart

Frequency and consequence criteria are used to represent the TLRC summarized in Section 4.1.1 to judge the acceptability of the frequency and consequence of each AOOs, DBEs, and BDBEs. Analyses of AOOs, DBEs, and BDBEs include the plant response of both safety-related and non-safety-related SSCs. In contrast, analyses of DBAs include the plant response with only safety-related SSCs performing. Figure 18 depicts the frequency-consequence curve developed for the modular HTGR on the NGNP project based on these guidelines, which assures adequate protection of public safety (INL 2010c). Note that the event sequence mean frequency is expressed in units of per plant year rather per reactor year to encompass events involving one or more reactor modules and other nonreactor radionuclide sources such as spent fuel.

In addition to the AOOs, DBEs, and BDBEs, deterministic DBAs are included in the LBEs. These events. In contrast to the risk-informed LBEs, analyses of DBAs include the plant response with only SSCs classified as safety-related to prevent and/or mitigate the event.

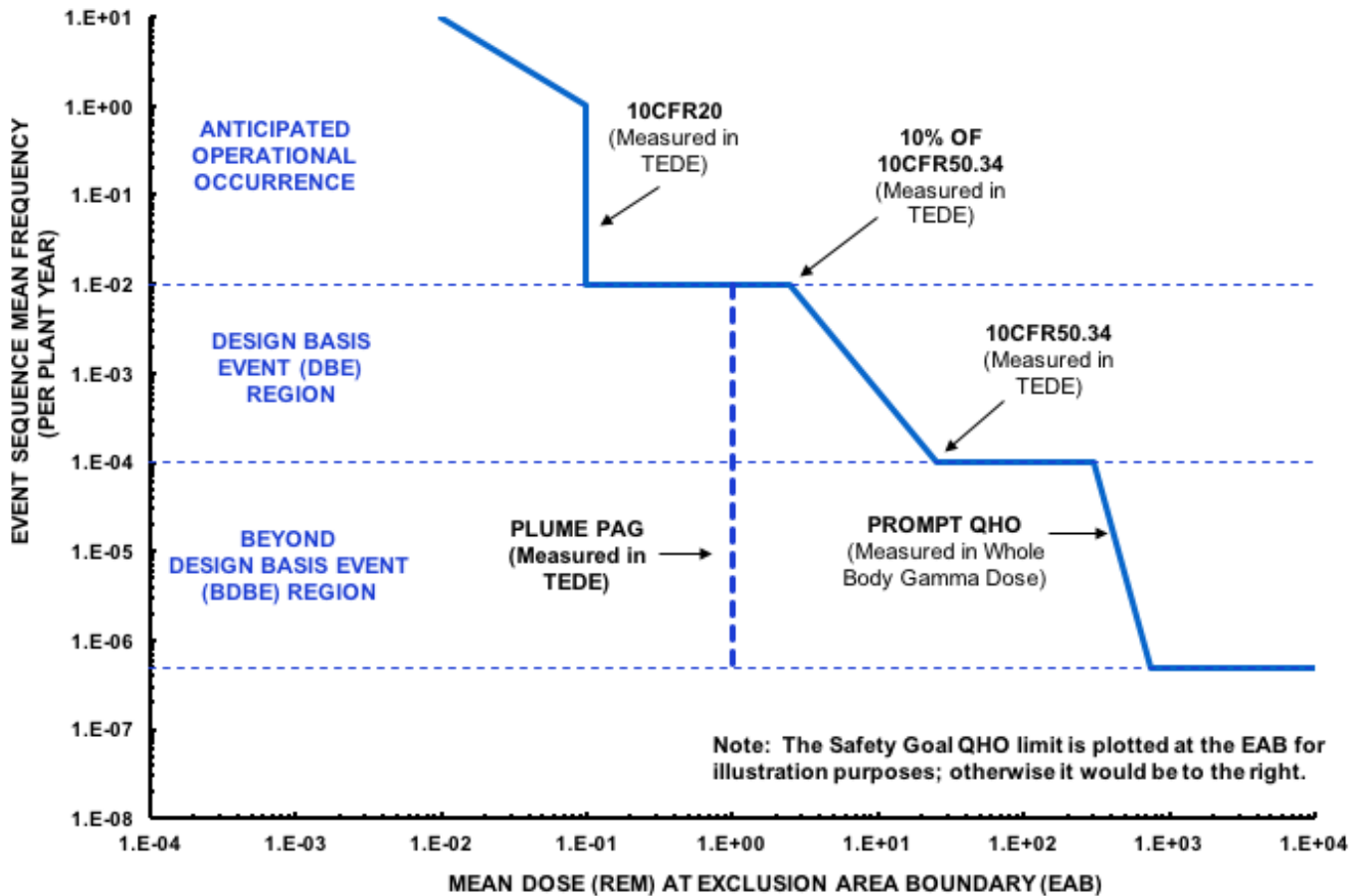


FIG. 18. Use of approach 1 for U.S. Modular HTGR frequency-consequence curve.

4.1.2.5. Selection of LBEs for U.S. modular HTGRs

The selection design process follows the following steps as depicted in the timeline flow chart in Figure 19.

1. Start with a design concept.
2. Select initial events based on history of related design/licensing efforts; used for scoping studies and early design development.
3. As the design matures, develop the PRA.
4. Risk inform the design and initial event list with insights from a scoping PRA.
5. Review of LBEs at the end of each design phase to evaluate the completeness of the event selection.
6. Each design phase seeks to satisfy the regulatory and design requirements for the entire plant of one or more reactor modules.

7. Iterative within design phases between the design process and PRA development.
8. Use engineering judgment commensurate with PRA completeness at each design phase.
9. Link PRA model to availability of design details and data.

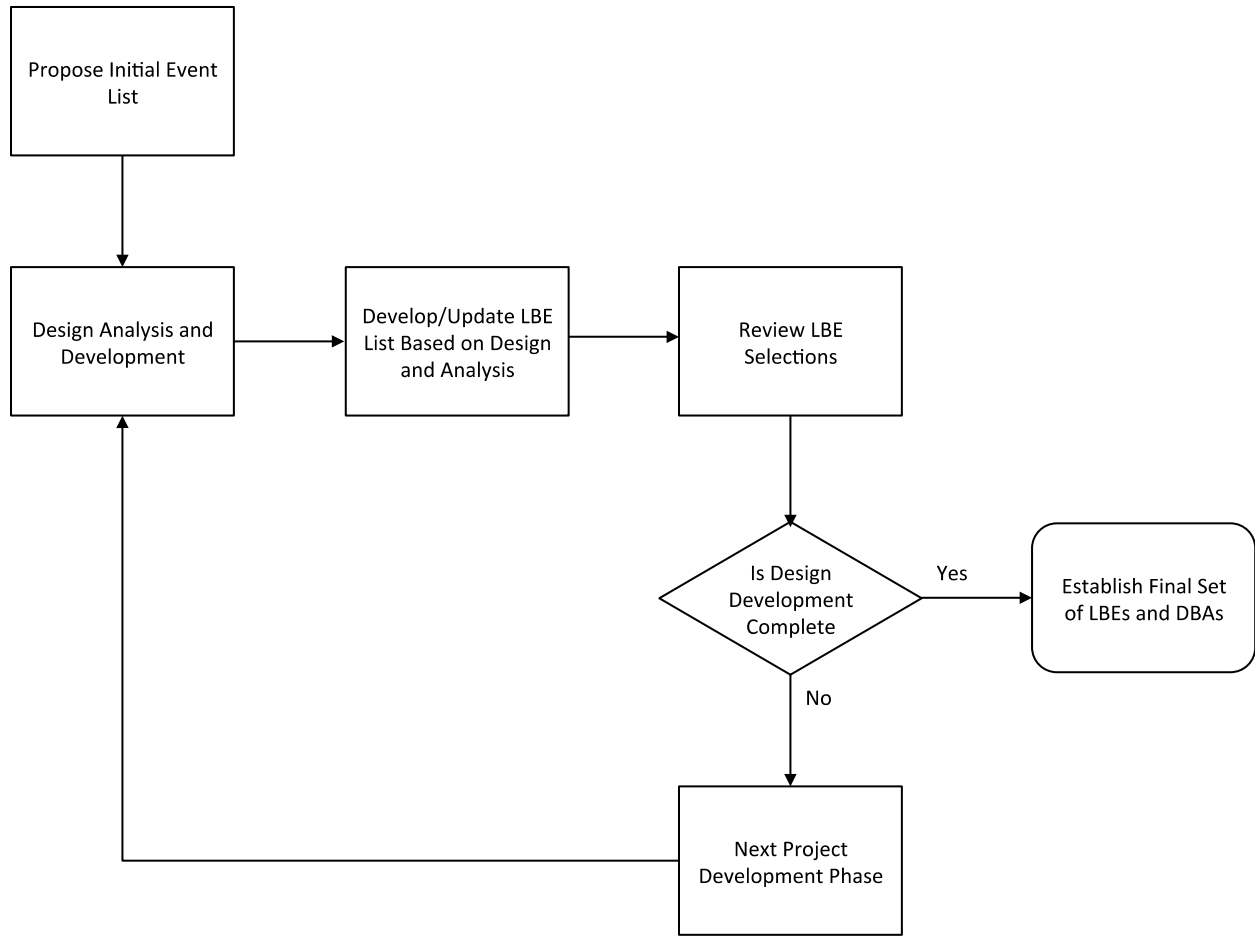


FIG. 19. Flow chart for selection of licensing basis events.

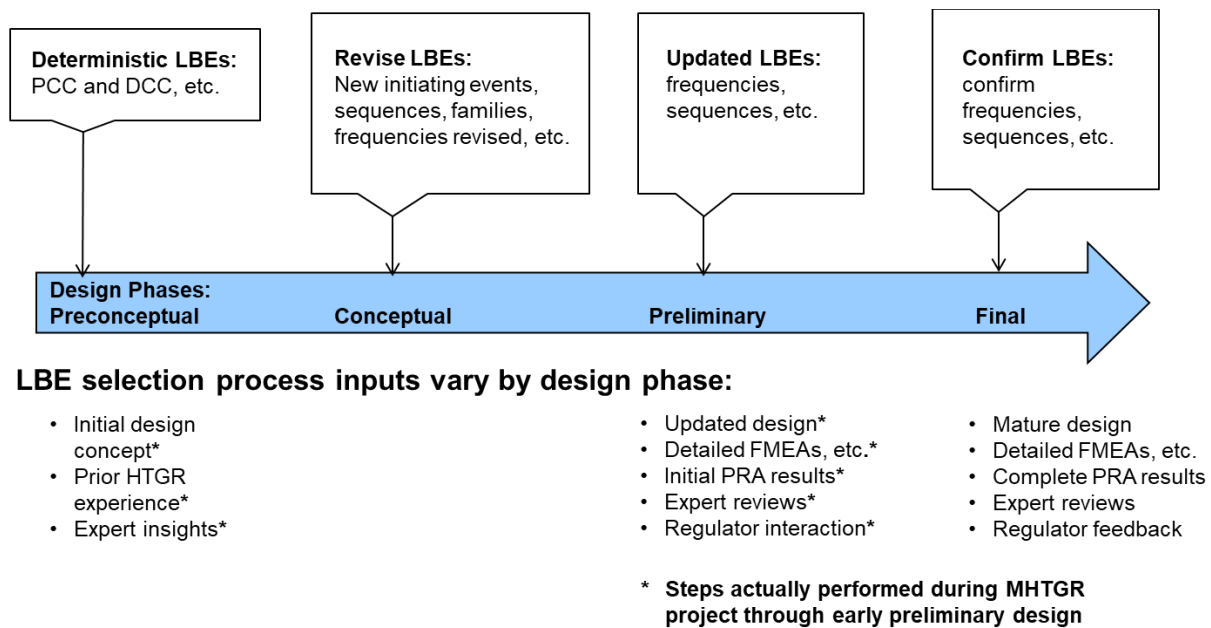


FIG. 20. Timeline of selection of modular HTGR LBEs.

Figure 21 shows a cutaway of the Nuclear Heat Supply System (NHSS) for one of the four reactor modules in the MHTGR plant that by a General Atomics led team under contract to the U.S. DOE several years in the mid-80s through the Conceptual Design Phase shown in Figure 20 and reviewed by the NRC.

The MHTGR has two diverse systems for control of core heat generation:

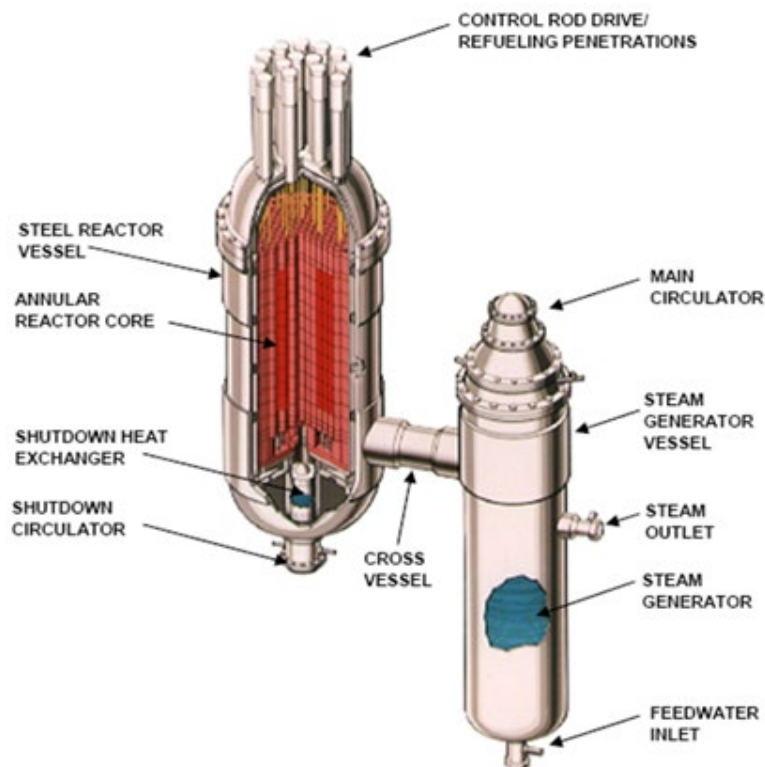
- The Reactivity Control System (RCS) with operating control rods in the reflectors and shutdown control rods in the active core and
- The Reserve Shutdown System (RSS) with boronated pellets that are also inserted from the top of the Reactor Vessel.

These two systems, coupled with the HTGR intrinsic strong negative temperature coefficient, effectively and reliably control core heat generation during normal operation, planned shutdowns, and off-normal events.

The MHTGR control of heat removal also has multiple systems for during power generation, for maintenance and shutdown cooling, and a passive system that operates during normal operation and off-normal events.

- The Main Loop Cooling is the active system that takes the core heat from the Reactor Vessel thru the inner hot duct within the Cross Vessel to the Steam Generator Vessel thru the main circulator then back to the Reactor Vessel. The steam generator transfers the heat to heat sinks in the conventional steam-cycle secondary system and heat sinks in the Energy Conversion Area.

- The Shutdown Cooling System (SCS) that circulates helium within the Reactor Vessel to a bottom-mounted water-cooled shutdown heat exchanger. The SCS water loop transfers the heat via an air-blast heat exchanger to an independent heat sink.
- The Reactor Cavity Cooling System (RCCS) passively removes the core heat from the outside surfaces of the Reactor Vessel to surrounding air-cooled panels in the below-grade concrete silo. The air panels are arranged in four redundant circuits to transport the heat by natural convection thru ducts to above grade stacks.



- **Modular Nuclear Heat Supply System (NHSS)**
 - 350MWt prismatic annular core
 - TRISO coated particle fuel
 - Helium cooled
 - Graphite moderated
 - ~700°C core outlet temp
 - 540°C/17.3 MPa steam heat
- **NHSS within Vessel System: Reactor Vessel, Steam Generator Vessel, and Cross Vessel**

FIG. 21. MHTGR(US) layout of nuclear heat supply system for a single reactor module.

Representative simplified event trees

From the PRA, a simplified event tree for the initiating event of Loss of Main Loop Cooling system is shown in Figure 22. Note that this could involve one or more of the four reactor modules, so the frequency is shown on per plant year basis. The safety challenge examined with this initiating event is assuring that radionuclides are retained in the fuel by adequate helium forced cooling of the shutdown reactor and, if forced cooling is unavailable, that adequate cooling is provided with the passive cooling system to retaining the radionuclides in the primary system.

The first response to the initiating event is whether the reactivity control systems operate as planned. The simplified tree provides the successful response in the upper branch of the RCS and/or RSS being inserted on signals from one of three independent systems, the Operational Control System, the Investment Protection System, and the Reactor Safety Protection System. The next two branch points show the response of the active SCS and the passive RCCS. In this tree, with its high reliability with both redundancy and diversity of systems, the events fall into either the AOO region with a frequency driven by the initiating event or into the BDBE region with the very unlikely failure of the RCCS. The bottom unlabeled sequence is outside the LBE regions.

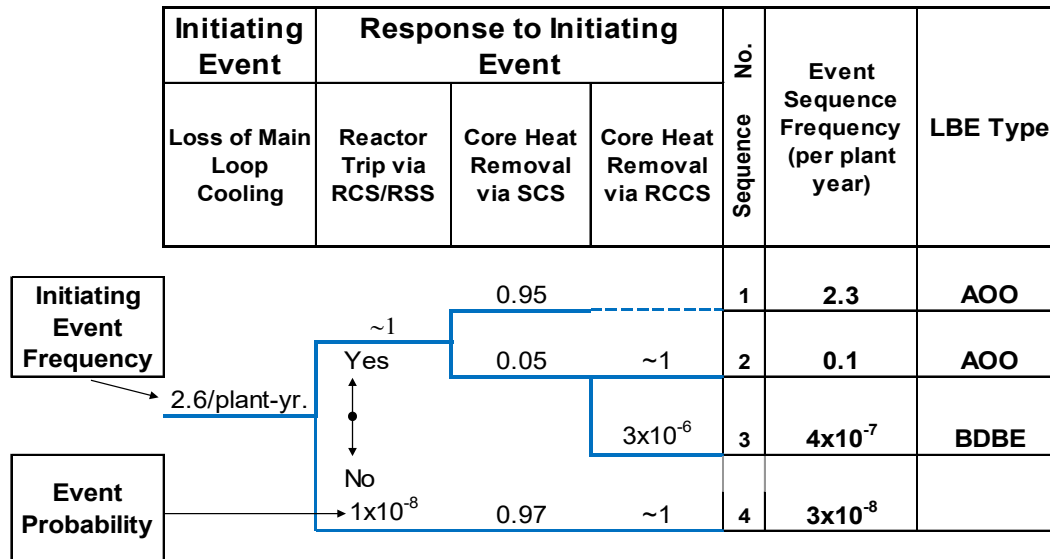


FIG. 22. Simplified event tree for MHTGR loss of main loop cooling.

The key points from the MHTGR Loss of Main Loop Cooling event tree are as follows:

- The simplified event tree is for illustrative purposes.
- The event sequence composed of initiating event in frequency units of per plant year followed by plant responses (branch point events) in dimensionless probabilities.
- The branch points are generally arranged by the timing of the plant response and consider the key safety functions and corresponding SSCs.
- The branch point probabilities may be dependent on the initiating event and prior plant responses and consider common causes.
- The frequency values shown in the simplified event tree are best estimate values: an uncertainty distribution is developed with the mean and upper and lower bounds.
- The entire plant is modelled so that in the full tree, delayed startup by the operator of an active system in the midst of a temperature transient is included.

- In this example event tree, the Helium Pressure Boundary (HPB) remains intact in all the risk-significant sequences so that there is no offsite release to the public. However, it is important for purposes of developing SDCs for the corresponding SSC requirements.

Figure 23 provides another simplified event tree initiated by a small leak in the HPB of a reactor module. The safety challenge examined with this initiating event is assuring that radionuclides released from the reactor meet the acceptable offsite limits.

For this initiating event, the main loop cooling (aka Heat Transport System (HTS)) is available as the first heat removal system. The last branch point involves the operator intentionally depressurizing the helium in the HPB thru the Helium Purification System (HPS) to storage to mitigate the release to the building and to meet the allowable offsite dose with greater margins.

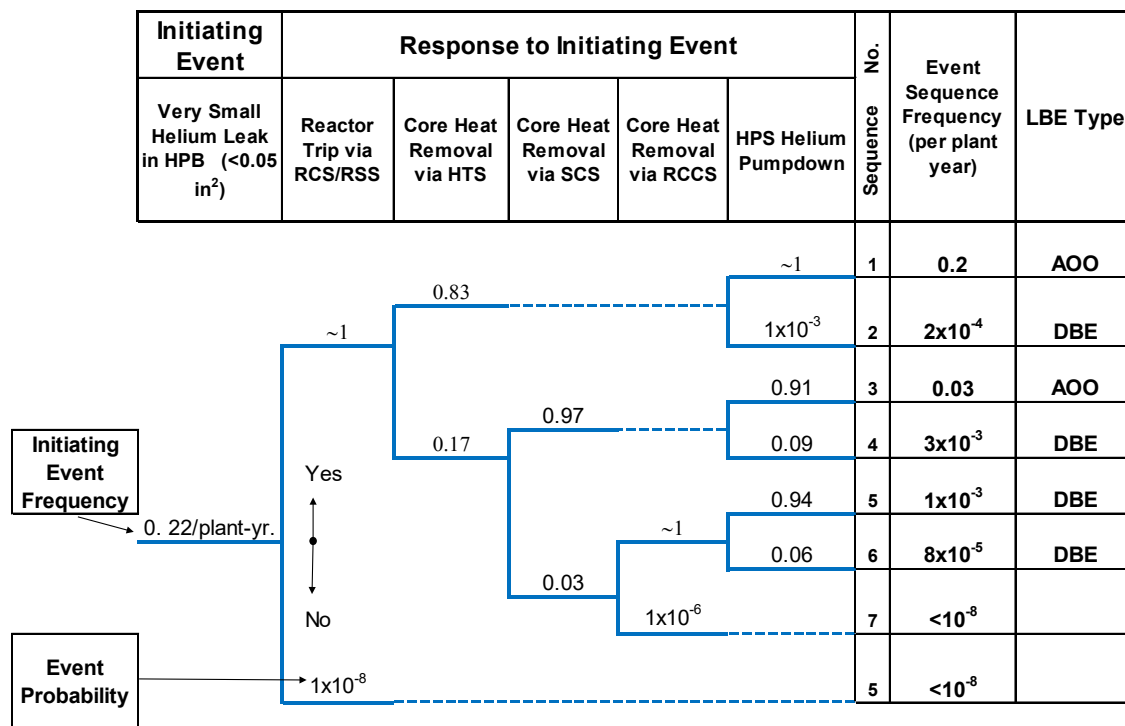


FIG. 23. Example selection of AOO and DBE from MHTGR small HPB leak event tree.

The key points from the MHTGR Small Helium Pressure Boundary (HPB) Leak event tree are as follows:

- This event tree initiating event is of lower frequency and is shown to see selection of AOOs in context with entire tree with lower event sequences
- The core heat removal with HTS branch point is a key plant response to this initiating event

- Helium depressurization is an example of an operator action to retain radionuclides within the HPB
- Event sequences with no and low doses are as important as those with high doses in terms of assuring that SSCs have the capability to mitigate and the reliability to prevent the event from having an unacceptable risk.

Table 8 provides the five AOOs selected from this risk-informed process for the MHTGR Conceptual Design Phase. The AOOs from these two, example event trees are shown in bold font.

TABLE 8. RISK-INFORMED AOOs SELECTED FOR MHTGR

AOO Designation	Anticipated Operational Occurrence
AOO-1	Main Loop Transient with Forced Cooling
AOO-2	Loss of Main Loop and Shutdown Forced Cooling
AOO-3	Control Rod Withdrawal with Control Rod Trip
AOO-4	Small Steam Generator Leak
AOO-5	Small HPB Leak

The next event tree is initiated by a loss of offsite power to the entire plant, that is, all four reactor modules, and the turbines for all reactor modules trip. The RCS control rods trip by design and drop in by gravity with this loss of power. Similarly, this tree only shows the expected case that the main loop cooling will also not be available. However, the active SCS for each reactor module with its diverse source of power is available for forced cooling in some sequences. As before, the passive RCCS is highly reliable. As shown in the last column, failure of any SCS, although rare, is predicted to be only (69% of the time) or most likely all four (27%) due to a common cause failure (e.g., incorrect maintenance).

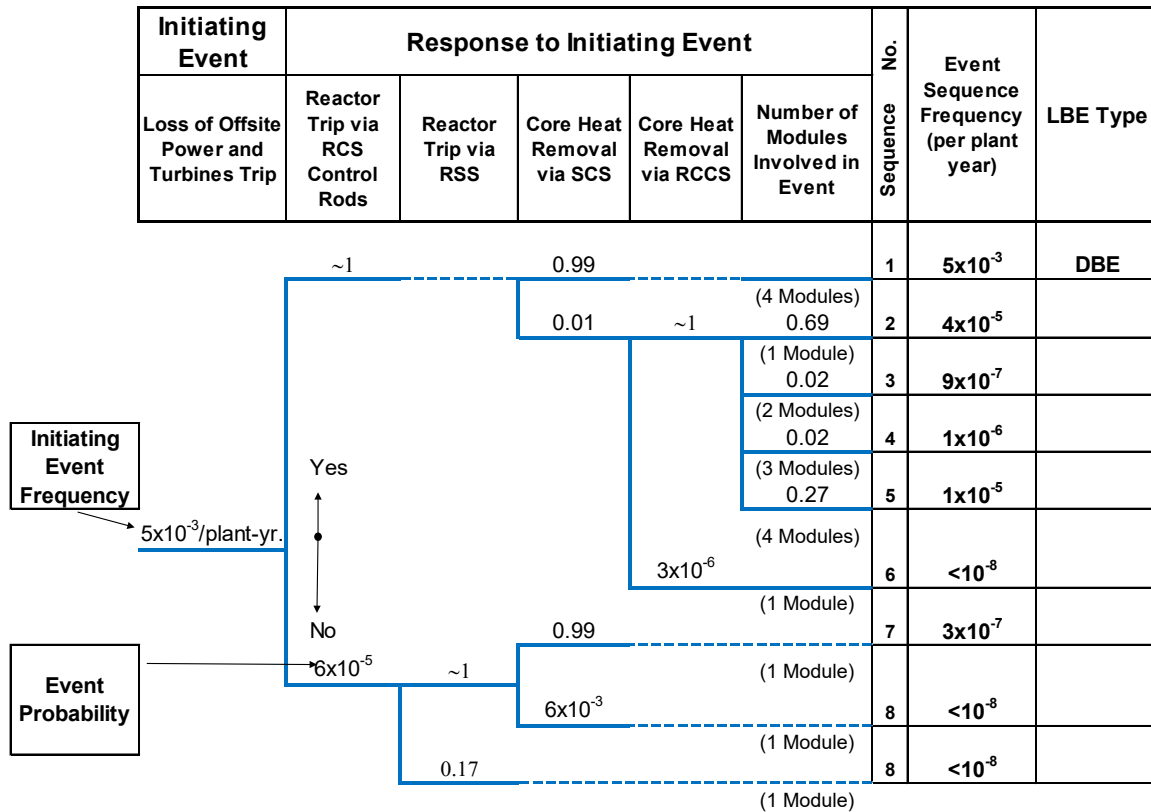


FIG. 24. Example selection of DBE from MHTGR LOSP and turbine trip event tree.

The key points from the MHTGR Loss of OffSite Power (LOSP) and Turbine Trip event tree are as follows:

- LOSP and turbine trip leads to the common cause loss of the HTS in all modules
- Each of the four reactor modules has an independent shutdown cooling system; but there is a probability that there will be failures in more than one reactor module's SCS for a combination of independent and common cause reasons
- There is one DBE identified that has successful forced cooling with the SCS in all four reactor modules. There is not an offsite radionuclide release.
- All other events are of lower frequency, for example BDBEs

The next simplified event tree is initiated by a tube rupture in the steam generator of one of the four reactor modules. Since the steam generator is at a higher pressure than the primary loop, this leads to water/steam ingress into the helium. The safety challenge with this initiating event here is to control chemical attack to meet acceptable limits after the water/steam ingress into the HPB that has the potential for increased release from the fuel, from the surfaces within the HPB, and from the HPB if the helium pressure relief valve of the Vessel System lifts meets acceptable limits.

In addition to the branch points for reactor trip and for core cooling, this tree involves the response of SSCs to detect and isolate the SG and to transfer the water/steam to a tank, as well as the response of the helium relief valve. As shown, the response of the valve may be to stay closed, to open and reclose one or more times, or to fail open.

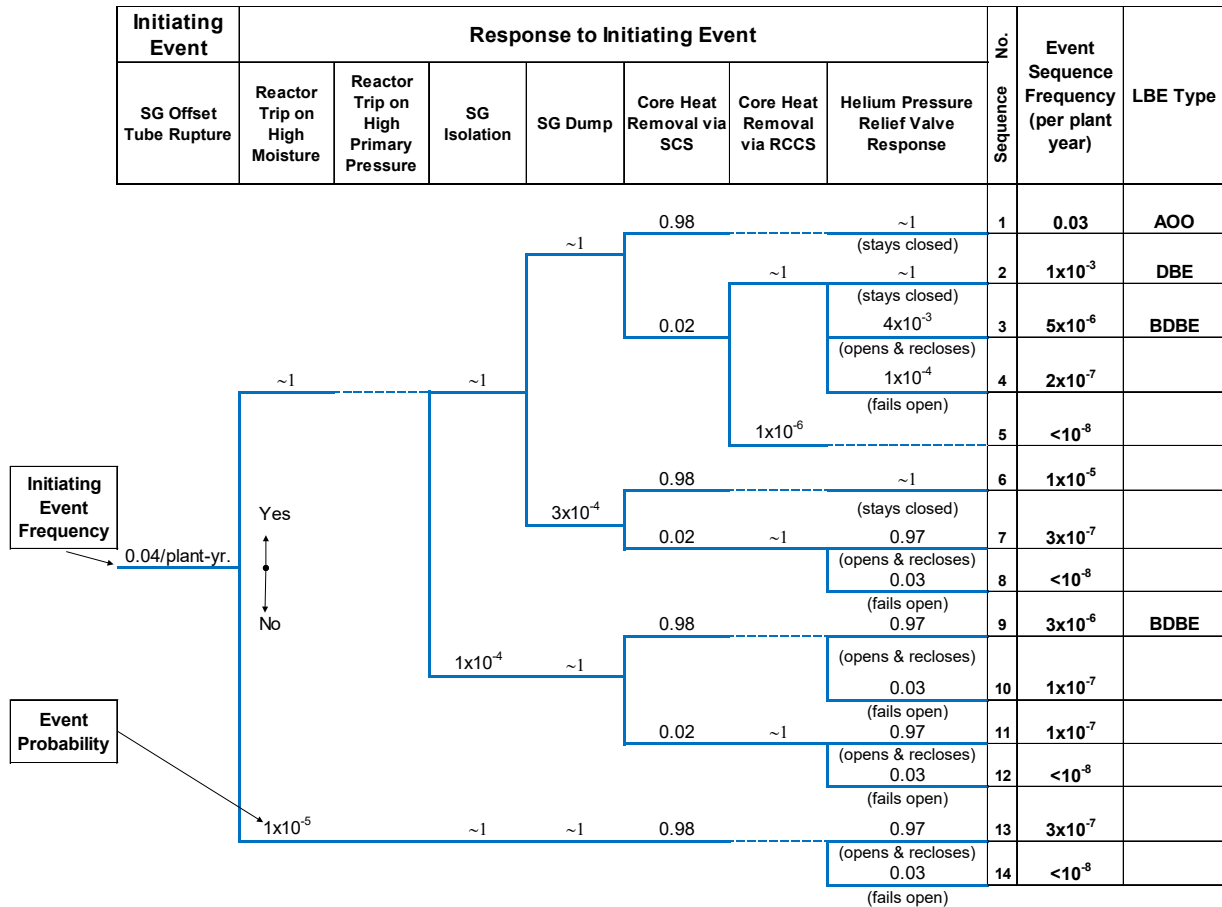


FIG. 25. Example selection of DBE from MHTGR steam generator tube rupture event tree.

The key points from the MHTGR Steam Generator Tube Rupture event tree are as follows:

- There are multiple means to detect moisture ingress
- There are multiple means to reduce the amount of water that enters the primary system and, thus, the potential for increased release from the fuel and the HPB surfaces
- Forced cooling lowers the reactor temperatures reducing the primary system pressure
- The pressure response of the primary coolant relief valve influences the radionuclide transport path and release timing

Table 9 provides the eleven DBEs selected from this risk-informed process for the MHTGR Conceptual Design Phase. The DBEs from the above simplified event trees are shown in bold font.

TABLE 9. RISK-INFORMED DBES SELECTED FOR MHTGR

DBE Designation	Design Basis Events
DBE-1	Loss of Main and Shutdown Forced Cooling
DBE-2	Main Loop Transient w/o Control Rod Trip
DBE-3	Control Rod Withdrawal w/o Main Loop Cooling
DBE-4	Control Rod Withdrawal w/o Forced Cooling
DBE-5	Earthquake
DBE-6	SG Tube Rupture w/ Isolation and Dump on Moisture Monitor Signal w/ SCS Forced Cooling
DBE-7	SG Tube Rupture w/ Isolation and Dump on Moisture Monitor Signal w/o SCS Forced Cooling
DBE-8	SG Tube Leakage w/ Isolation and Dump on High Primary Pressure Signal w/ SCS Forced Cooling
DBE-9	SG Tube Leakage w/ Isolation and Dump on Moisture Monitor Signal w/ SCS Forced Cooling and Dump Tank Valves Fail to Reclose
DBE-10	Moderate Primary Coolant Leak w/ Forced Cooling
DBE-11	Small Primary Coolant Leak w/o Forced Cooling

Figure 26 provides the MHTGR Frequency-Consequence Risk Chart as presented to the NRC in 1987 with its slightly different terminology and TLRC. Key points from this diagram are as follows:

- Each of the LBEs is shown with 95% uncertainty bands on the frequency and consequence.

- Many LBEs (AOOs, DBEs, and EPBEs) do not result in releases from the plant that result in offsite doses, but are included since without SSCs performing one or more functions leading to the acceptable consequences. These functions and the corresponding SSCs must be explicitly identified in subsequent steps of the process to specify the SDCS.
- A large DBE-10 is an example of an event that straddles the boundary between the AOO and DBE regions at 10^{-2} per plant year and was evaluated against both 10 CFR 50 and 10 CFR 100.
- In addition to EPBEs, a number of lower frequency events below the LBE de minimus cutoff of 5×10^{-7} /plant year were shown to assure that there was negligible residual risk.

The AOOs and DBEs were discussed in the MHTGR Public Safety Information Document (PSID) in Chapters 11 and 15, respectively. This document was the equivalent of a PSAR for a Conceptual Design and was reviewed by the NRC and their contractors over a three-year time period. The EPBEs (now called BDBEs) were discussed

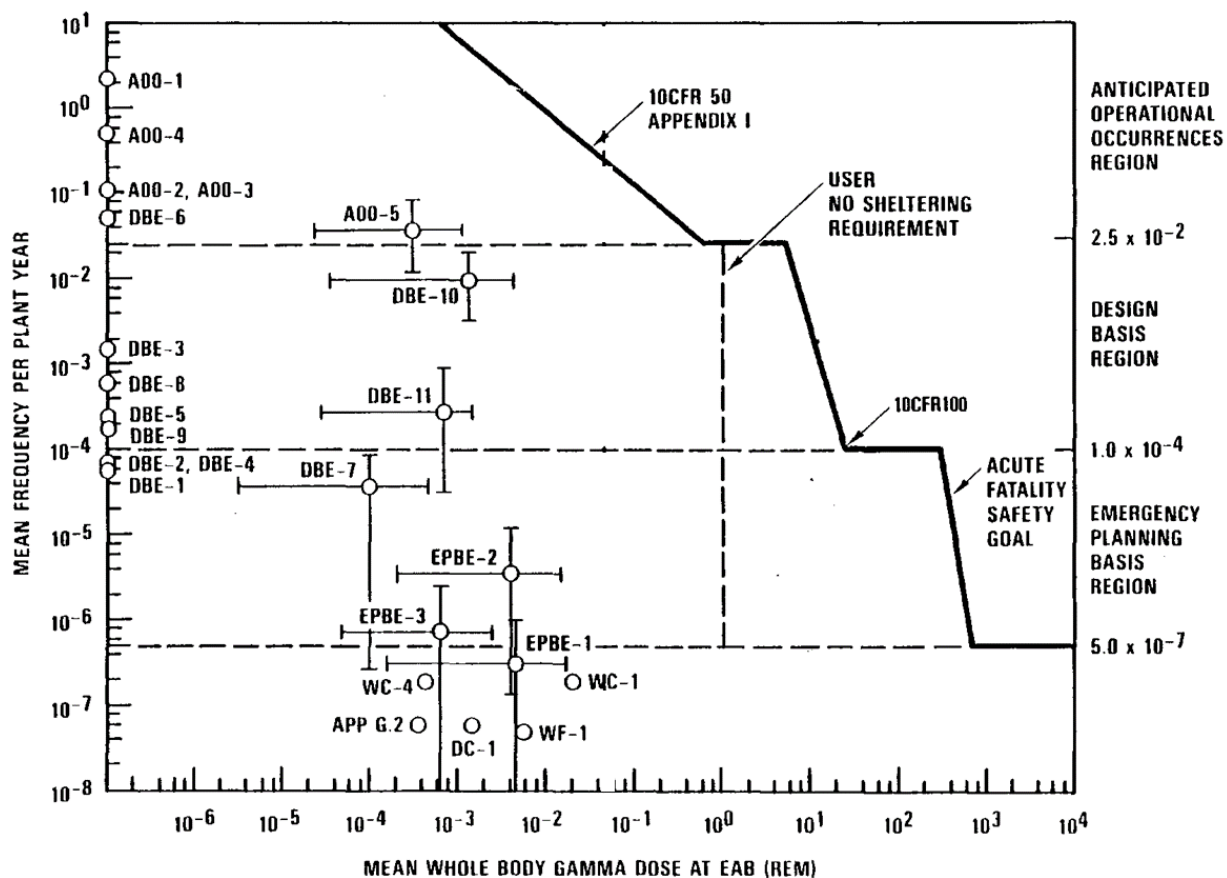


FIG. 26. MHTGR LBEs on the 1987 risk chart for each of the three regions: AOO, DBE, and BDBE (then called emergency planning basis event (EPBE) region).

4.1.3. Safety Functions

As discussed above, the safety design approach for the modular HTGR controls radionuclides primarily at their source within the coated fuel particle during normal operation and during accident conditions without requiring active design features or operator actions. The safety design approach is framed in terms of reactor-specific safety functions that are developed from the top safety objective of containing the radioactive material and then considering the specific functions that would protect the integrity of the fuel and other radionuclide retention barriers.

With the risk-informed structured, thorough approach for selection of events, each event sequence with the entire plant responding is assessed to determine which safety functions are keeping the consequences within the acceptable regions. The safety functions identified in Figure 27 assure that the design meets with margin the regulatory requirements for plant personnel and public safety during normal operation and off-normal events as well as the user requirement that off-site sheltering and evacuation of the public is not required. Consistent with the modular HTGR safety design approach, within the functional containment that includes the fuel, the HPB, and the reactor building, the primary emphasis is on retention of the radionuclides at the source within the ceramic coated fuel particles. The three key safety functions of control of chemical attack, control of core heat generation, and core heat removal are shown in Figure 27. Although not shown, sub-functions below these to maintain the core geometry and the geometry of the reactor vessel relative to the RCCS are considered.

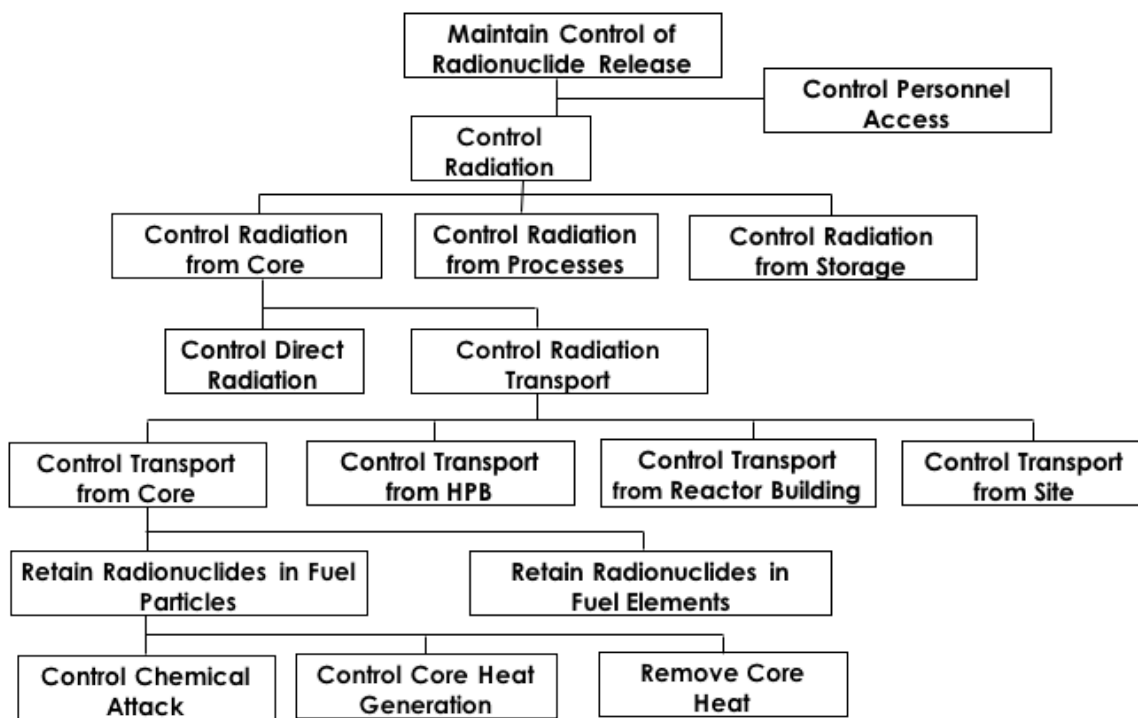


FIG. 27. Safety functions for the MHTGR to meet personnel requirements and the user design target for offsite public consequences.

4.1.3.1. Control Chemical Attack

Control of chemical attack has been a focus of the safety approach from the inception of the modular HTGR. A combination of passive design features and active features that do not rely on AC power have been utilized with the inherent characteristics of the inert high-pressure helium, nuclear-grade graphite, and coated particle fuel to assure adequate safety margins and to meet the TLRC and design objectives

Chemical attack on fuel particles and on the graphite core structure can result from air or water ingress into the helium primary system. During normal operations and during some AOOs and DBEs, contaminants are managed at the parts per million level by the helium purification system (HPS), which purifies a side stream from the primary system.

The likelihood of water entering the primary system is limited by the absence of high-pressure and high-energy sources of water in proximity to the primary system with the exception of the steam generator (SG). Under normal operating conditions, all other water coolers and heat exchangers operate at lower pressures than the pressure of the helium with which they exchange heat. Nevertheless, in the event of a tube leak in the higher pressure SG, the leak would be detected either by moisture monitors or by high primary coolant pressure. Either signal results in isolation of the SG to limit the amount of water ingress to the reactor. In addition, the moisture monitor signal or reactor operator dumps the remaining SG inventory to water tanks to limit the primary system pressure rise, graphite-steam oxidation, and the moisture cleanup time. AC power is not required for either of these functions. Core cooling can still be provided by the residual heat removal system, if available, and would limit the potential for chemical attack by lowering the graphite and fuel temperatures. If active, forced core cooling is not available, the potential of water or steam transport to the core would still be limited because the subcooled feedwater in the SG will not flash to steam unless the primary coolant helium pressure is below the water saturation pressure. If steam is generated and transported to the core, then the reaction of steam and graphite is slow and endothermic; therefore, it is not self-sustaining. Exposure to moisture does not affect fuel particles, except for the very small fraction with defective coating layers. Moisture ingress does not cause additional particle failures in and of itself. Radionuclide release from defective particles would increase because of the hydrolysis of fuel kernels as discussed above, which temporarily increases radionuclide release. However, overall radionuclide retention is adequately maintained to meet the TLRC and design objectives (DOE 1992).

The likelihood of a breach of the HPB, such that air ingress becomes a concern, is limited by the high quality associated with the pressure vessels and the limited size of penetrations. In the event of a leak or breach, primary helium coolant would leak out until the inside and outside pressures equilibrate. Most notably, the high-pressure helium would act to expel the reactor building air out the vent. Then, the ingress rate of the helium-air gas mixture would be small, as the gas mixture tries to enter the breach primarily by natural circulation and diffusion at the same time as helium coolant, which it is displacing, tries to exit through the same breach. Large ingress rates of the helium-air gas mixture would require an implausible scenario of breach of an American Society of Mechanical Engineers (ASME) Code Section III vessel to set up an effective circulation path. However, even in that circumstance, the gas mixture flow would be restricted by the flow resistance characteristics in the core (e.g., high cooling channel length-to-diameter ratio).

4.1.3.2. Control Heat Generation

Control of heat generation is accomplished by a very large core negative temperature coefficient and two independent reactivity control systems. Control rods drop by gravity into the core upon loss of electrical power. An automatic positive control action initiated in response to various accidents, including reactivity initiated accidents, can also cause the rods to drop, or the event itself may cut the power supply. It is an advantage that power is not needed to insert the control rods. In addition, modular HTGRs have a redundant and diverse system (or backup shutdown system) to drop borated graphite pellets by gravity into designated fuel element or reflector channels for reactivity control equivalent to rod insertion. Initiation of the latter system typically requires a positive control signal and an active protection system response. However, AC power is not required for these functions.

If both the control rod and backup shutdown systems fail, the temperature coefficient of reactivity will shut down the reactor from any power level following loss of forced cooling. As an example, given that no additional positive reactivity is inserted, core power will be reduced to shutdown levels by negative temperature coefficient alone, such that the RCCS alone can safely cool the core for more than 30 hours after the initial shutdown. Re-criticality due to xenon decay will increase the power and core temperatures to compensate for the loss of negative reactivity until either the control rods or backup shutdown systems have been activated. A test conducted at the Arbeitsgemeinschaft Versuchsreaktor (AVR) in Germany supports the analysis, which shows that following this initial shutdown, a gradual core temperature increase and negative reactivity addition will occur, with the core stabilizing at a near-zero power level at which the heat generation rate matches the core cooling capability of the passive heat sinks. This is an equilibrium condition that can be maintained indefinitely until corrective actions are taken to insert the control rods or drop borated control material into the core to affect a full shutdown and to allow the reactor to be taken to a cold shutdown condition.

4.1.3.3. Remove Core Heat

Modular HTGRs have multiple methods for accomplishing core heat removal. Reactor cooling can be accomplished by the main loop cooling system, an active residual heat removal system, and by passive core heat removal from the reactor vessel to the RCCS. The modular HTGR core is designed so that residual heat removal is not dependent on the helium coolant within the reactor being under pressure for either forced cooling or passive cooling scenarios. The RCCS, which is independent and diverse from the forced cooling systems, keeps structures within allowable temperature limits, including the reactor building concrete. The RCCS designs may be either passive or active under normal conditions, but always have a passive mode capable of removing residual core heat under accident conditions. Reactor heat is transferred through the reactor vessel walls to the RCCS cooling panels by conduction, natural convection, and radiation heat transfer; the vessel walls are uninsulated to facilitate this process. With RCCS cooling under core heat-up accident conditions, core temperatures will peak after about one or more days at temperatures below that at which a significant coated radionuclide release can occur. Subsequently, the core will slowly cool within several weeks to below normal operation levels.

Even if the RCCS were not available, heat from the reactor vessel walls would be transferred through the inoperable RCCS panels to the concrete walls of the reactor building and ground surrounding the reactor building. This cooling capability is also totally passive. It is not in the design basis and is not necessary to meet any safety requirements or quantitative safety goals, but exists as an ultimate passive feature. With core cooling in this mode, core temperatures peak at about the same level as with RCCS cooling, but the core cools more slowly thereafter. Also, creep deformation of the vessel at the core mid-plane and damage to the RCCS and the reactor building is likely to occur after several days (General Atomics 1988).

4.1.3.4. Safety Classification of SSCs and Deterministic DBAs

In the US, prior to the introduction of risk insights into the regulatory process, the licensing approach has traditionally postulated deterministic initiating events and then certain SSCs that are a subset of the entire plant are shown to successfully perform required safety functions to meet the offsite dose requirements. These events are termed the Design Basis Accidents (DBAs). The required safety functions are shown in shaded Figure 28. These SSCs, classified as safety-related, are the ones that are relied on to perform the required safety functions in the Safety Analysis Reports. In the MHTGR PSID, the decision was made to provide both the risk-informed DBEs with the entire plant responding regardless of safety classification and the deterministic DBAs with only safety-related SSCs.

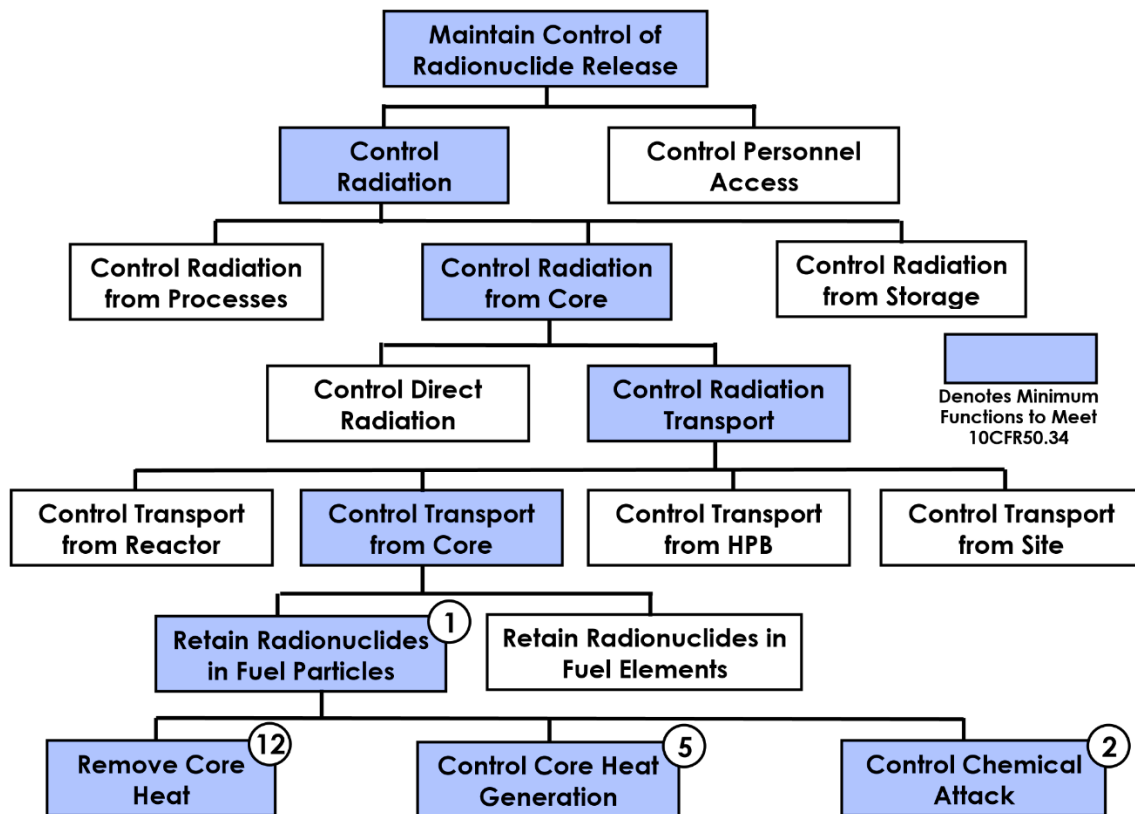
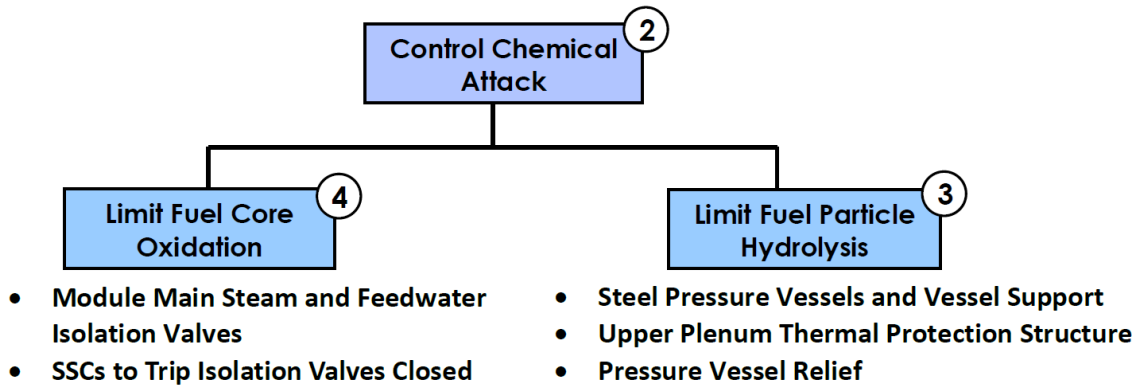
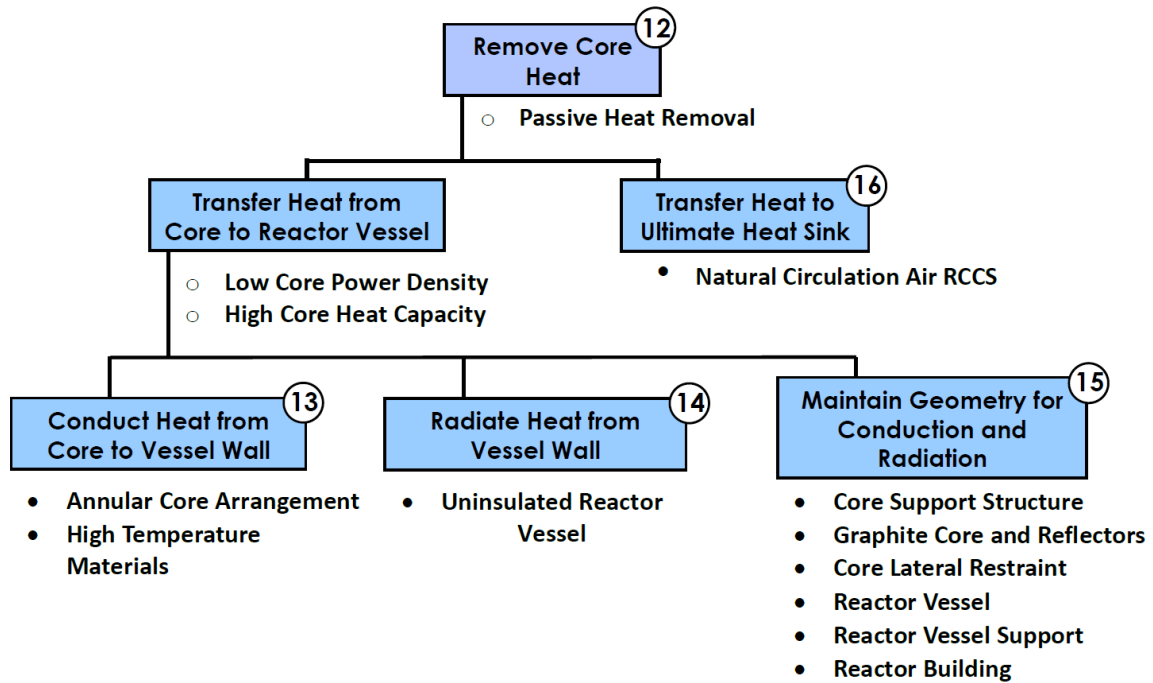
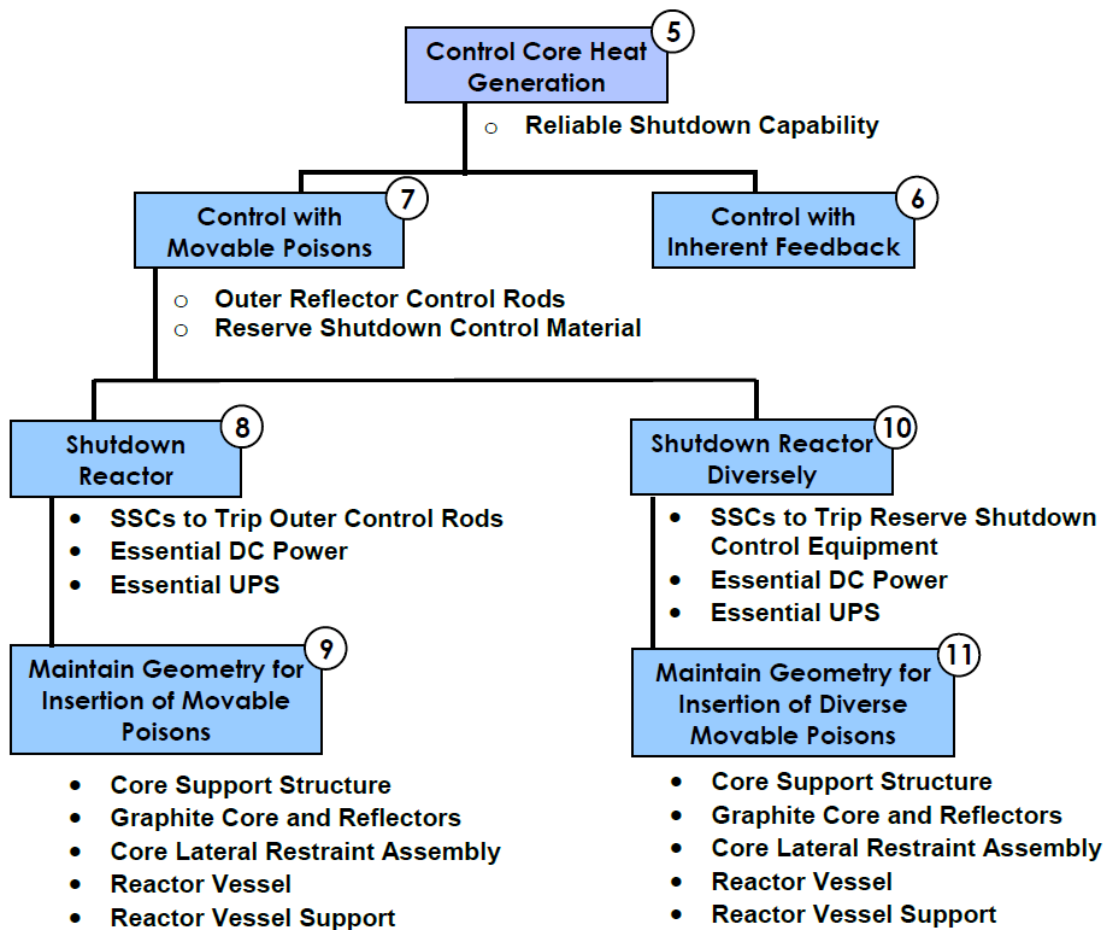


FIG. 28. Required safety functions for the MHTGR to meet regulatory offsite requirement during deterministic DBAs.





To illustrate the multi-dimensional safety classification process, one DBE is examined for one function: core heat removal. Table 10 asks the question of what SSCs are available and sufficient to perform the core heat removal function during an event sequence that is initiated by a small helium leak in the HPB from the full-power operating state of one reactor module. The Table 10 first shows the normal main heat transport system that circulates helium from the reactor to the steam generator to a secondary steam system and heat sink that are designed to remove residual heat (sensible and decay heat) with or without the primary helium pressurized. Similarly, the smaller shutdown cooling system, used for maintenance and investment protection that has an independent means to circulate primary helium and independent secondary heat removal system and heat sink, also fails. The next alternative set of SSCs relies on radiation and convection from the tall, slender core radially out to the reactor vessel and by radiation from the reactor vessel surface to a passive reactor cavity cooling system that utilizes either natural convection of air or water in enclosed panels/pipes. This passive alternative SSC set operates during normal operation and off-normal events and does not require forced or natural helium circulation. Similarly, the final set of alternative SSCs is available and sufficient as it utilizes the heat capacities within the below-grade, concrete reactor building to retain radionuclides within the fuel.

TABLE 10. ILLUSTRATION OF SSC CAPABILITIES FOR CORE HEAT REMOVAL SAFETY FUNCTION IN RESPONSE TO DBE-11

Are SSCs Available and Sufficient to Remove Core Heat in the DBE?	
Alternative Sets of SSCs	DBE 11
Initiating Event	HPB small leak
Reactor Heat Transport System (HTS) Energy Conversion Area	No
Reactor Shutdown Cooling System (SCS) Shutdown Cooling Water System	No
Reactor Reactor Vessel (RV) Reactor Cavity Cooling System (RCCS)	Yes
Reactor RV Below-grade Reactor Building (RB)	Yes

Thus, for this core heat removal function, there are two “yes” choices of SSCs as shown in the Table 11 that are available and sufficient to mitigate the consequences of the DBE-11 small helium leak. However, before choosing between these choices for this one event, the process examines the full spectrum of DBEs. These include loss of off-site power to the plant, reactivity events with and without reactor trip, earthquake, steam generator leaks/breaks into the reactor HPB, and a range of helium leaks/breaks from the HPB. As shown in Table 11, for the heat removal function, some DBEs have other SSC choices that are available and sufficient to remove the heat with the active forced cooling systems. However, only the two passive choices identified from DBE-11 are available across the spectrum of initiating events leading to the event sequences within the design basis region.

The indicated set of SSCs with the RCCS was selected by the designers as safety-related since it was the optimum selection to achieve the capability and reliability to present to the NRC in the SAR. The other set without the RCCS successfully operating, but only the below-grade reactor building and its surroundings results in large uncertainties that are dependent on their thermal properties and compositions. Further, the RCCS that is needed during normal operation to keep the reactor vessel within its code-qualified temperatures has the advantage that it is continuously operated and monitored during normal operation.

TABLE 11. ILLUSTRATION OF SSC CAPABILITIES FOR THE SAFETY FUNCTION OF CORE HEAT REMOVAL FOR THE SPECTRUM OF DBES

Are SSCs Available and Sufficient to Remove Core Heat in the DBE?										
Sets of SSCs	DBE 1	DBE 2	DBE 3	DBE 4	DBE 5	DBE 6/7	DBE 8/9	DBE 10	DBE 11	SSCs Classified as Safety Related?
Initiating Event	Loss of Offsite Power with Turbine Trip	Main Loop Transient w/o Control Rod Trip	Control Rod Withdrawal	Control Rod Withdrawal	Safe Shutdown Earthquake	SG Tube Rupture	SG Tube Leak	HPB Moderate Leak	HPB Small Leak	
Reactor HTS ECA	No	No	No	No	No	No	No	No	No	
Reactor SCS SCWS	No	Yes	Yes	No	Yes	Yes	No	Yes	No	
Reactor RV RCCS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes, optimum selection to achieve capability & reliability
Reactor RV Below-grade RB	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	

Figure 29 presents the simplified event tree for the small helium break with the sequence that relies only on safety related SSCs high-lighted in red. The key insights from this comparison are as follows:

- Control of core heat generation is performed by the safety-related SSCs of the RCS control rods and the RSS boronated pellets, both of which are inserted into the core by gravity.
- Control of core heat removal is performed by the safety related SSCs of passive core heat transfer mechanisms from the fuel elements to the side reflectors to the reactor vessel and then by radiation from the vessel surface to the RCCS, a fully passive system to the ultimate outside air.

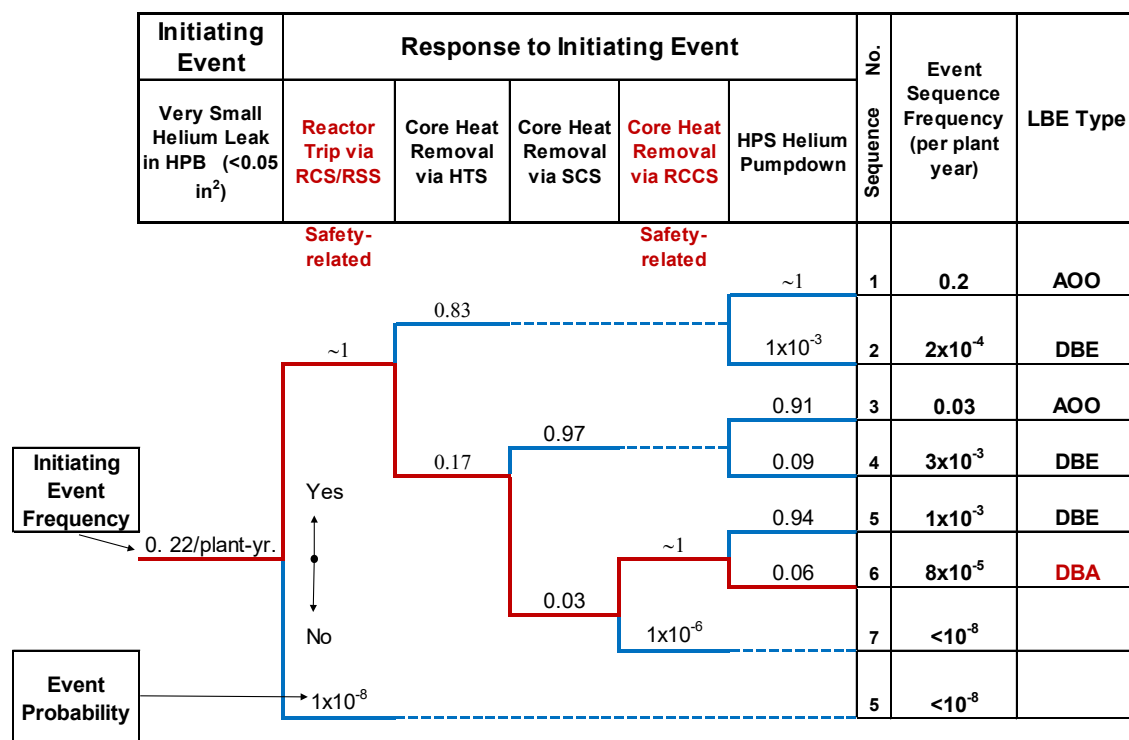


FIG. 29. DBA with only safety related SSCs responding shown on MHTGR Small HPB Leak Event Tree.

A comparison of all of the MHTGR DBEs with the corresponding DBAs is shown in Table 12. The three rows in bold font indicate no change in the event scenario between the DBE and the DBA.

TABLE 12. COMPARISON OF DBES (WITH ENTIRE PLANT) AND DBAS (WITH ONLY SAFETY-RELATED SSCS)

DBE	Design Basis Event Description	DBA	Design Basis Accident Description
DBE-1	Loss of Main and Shutdown Forced Cooling	DBA-1	Loss of Main and Shutdown Forced Cooling
DBE-2	Main Loop Transient w/o Control Rod Trip	DBA-2	Loss of Forced Cooling w/o Control Rod Trip
DBE-3	Control Rod Withdrawal w/o Main Loop Cooling	DBA-3	Control Rod Withdrawal w/ Loss of Forced Cooling
DBE-4	Control Rod Withdrawal w/o Forced Cooling	DBA-4	Control Rod Withdrawal w/o Forced Cooling
DBE-5	Earthquake	DBA-5	Earthquake with Loss of Forced Cooling
DBE-6	SG Tube Rupture w/ SG Isolation and Dump on Moisture Monitor Signal w/ Forced Cooling	DBA-6	SG Tube Rupture w/ SG Isolation on High Primary Pressure Signal w/o Forced Cooling
DBE-7	SG Tube Rupture w/ Isolation and Dump on Moisture Monitor Signal w/o Forced Cooling	DBA-7	SG Tube Rupture w/ SG Isolation on High Primary Pressure Signal w/o Forced Cooling
DBE-8	SG Tube Leakage w/ Isolation and Dump on High Primary Pressure Signal w/ Forced Cooling	DBA-8	SG Tube Leakage w/ SG Isolation on High Primary Pressure Signal w/o Forced Cooling
DBE-9	SG Tube Leakage w/ Isolation and Dump on Moisture Monitor Signal w/ Forced Cooling and Dump Tank Valves Fail to Reclose	DBA-9	SG Tube Leakage w/ SG Isolation on High Primary Pressure Signal w/o Forced Cooling w/o Forced Cooling
DBE-10	Moderate Primary Coolant Leak w/ Forced Cooling	DBA-10	Moderate Primary Coolant Leak w/o Forced Cooling
DBE-11	Small Primary Coolant Leak w/o Forced Cooling	DBA-11	Small Primary Coolant Leak w/o Forced Cooling

4.1.4. Safety Design Criteria for the MHTGR

In summary, the TLRC have been determined and a F-C chart developed for the risk-informed process for event selection has utilized a PRA to comprehensively examine the entire plant, all four modules, for the selection wide spectrum of events. With that background, the general safety functions have been identified, the required safety functions to meet the offsite accident regulatory doses have been identified, the spectrum of DBEs has

been examined one function at a time to select the safety related SSCs, and finally the deterministic DBAs that rely only on the safety related SSCs have been specified for inclusion in the SAR Chapter 15 with the DBEs.

Following the steps in Table 7, the SDCs are formulated as qualitative functional statements for the required safety functions and SSCs relied on during the DBAs.

TABLE 13. APPROACH 1 WITH MHTGR REQUIRED SAFETY FUNCTIONS AND SELECTED SSCS RELIED ON DURING DBAS

Required Safety Functions Relied on During DBAs	Selected SSCs Classified as Safety Related to Perform Function
RETAIN RADIONUCLIDES IN FUEL	
Control Chemical Attack	
Limit Fuel Particle Hydrolysis	• Module Main Steam and Feedwater Isolation Valves • RPS to Trip Isolation Valves Closed
Limit Fuel Core Oxidation	• Steel Pressure Vessels and Vessel Support • Upper Plenum Thermal Protection Structure • Vessel System Pressure Relief
Control Core Heat Generation	
Control with Inherent Feedback	• Negative Temperature Coefficient • Fuel Cycle Heavy Metal Loadings
Control with Movable Poisons	• Outer Reflector Control Rods • Reserve Shutdown Control Material
Shutdown Reactor	• RPS to Trip Outer Control Rods • Essential DC Power • Essential UPS
Maintain Geometry for Insertion of Movable Poisons	• Core Support Structure • Graphite Core and Reflectors • Core Lateral Restraint Assembly • Reactor Vessel • Reactor Vessel Support
Shutdown Reactor Diversely	• RPS to Trip Reserve Shutdown Control Equipment

	• Essential DC Power • Essential UPS
Maintain Geometry for Insertion of Diverse Movable Poisons	• Core Support Structure • Graphite Core and Reflectors • Core Lateral Restraint Assembly • Reactor Vessel • Reactor Vessel Support
Remove Core Heat	
Transfer Heat from Core to Reactor Vessel	
Conduct Heat from Core to Vessel Wall	• Annular Core Arrangement • High Temperature Materials
Radiate Heat from Vessel Wall	• Uninsulated Reactor Vessel
Maintain Geometry for Conduction and Radiation	• Core Support Structure • Graphite Core and Reflectors • Core Lateral Restraint • Reactor Vessel • Reactor Vessel Support • Reactor Building
Transfer Heat to Ultimate Heat Sink	• Natural Circulation Air RCCS

The proposed SDCs for the MHTGR are as follows:

FUNCTION: Control Radionuclides in Fuel: This function refers to the Standard MHTGR safety design approach to design, fabricate, and operate the fuel so that normal operation releases are limited to the extent that only the radionuclide inventory within the fuel itself presents a potential challenge to meeting the 10 CFR 50.34 doses. Thus, only the fuel conditions need be maintained for off-normal events to assure 10 CFR 50.34 compliance.

MHTGR SDC 1 - Control Radionuclides in Fuel

The reactor fuel shall be designed, fabricated, and operated such that radionuclides are retained within the fuel to the extent that releases to the primary coolant will not exceed acceptable values.

FUNCTION: Control Chemical Attack: This function refers to the necessity to prevent fuel degradation caused by the intrusion of compounds other than helium into the primary coolant. The principal chemical attacks to be avoided are those of air and water, which could

react with the fuel or the graphite and, as a result, degrade the fuel. Excessive air ingress is prevented by limiting the loss of primary coolant boundary integrity. Excessive water ingress is prevented by terminating the source of water following loss of primary to secondary coolant boundary integrity.

MHTGR SDC 2 - Control Chemical Attack

The vessels and other components that limit or prevent the ingress of air or water shall be designed, fabricated and operated such that the amount of air or water reacting with the core will not exceed acceptable values.

FUNCTION: Limit Fuel Hydrolysis: This function refers to limiting the amount of steam and water which can enter the reactor vessel in the event of a steam generator leak or other water source. The event must be detected and terminated to prevent the ingress of an amount of steam and water which could cause unacceptable levels of fuel hydrolysis.

MHTGR SDC 3 - Limit Fuel Hydrolysis

The steam, feedwater and other cooling systems shall be provided with a reliable means to limit to acceptable levels the amount of steam and water that can enter the reactor vessel.

FUNCTION: Limit Fuel Oxidation: This function refers to preventing and limiting the amount of air that can enter the reactor core in the event of a breach of the primary system boundary. The function is accomplished by protecting the integrity of the primary system boundary by both active and passive means.

MHTGR SDC 4 - Limit Fuel Oxidation

The primary helium pressure boundary shall be designed and fabricated to quality standards sufficient to ensure high reliability of its integrity to prevent air ingress during normal and off-normal conditions. The plant shall be designed, fabricated, operated, and maintained in a manner which ensures that the primary system boundary design limits are not exceeded.

FUNCTION: Control Heat Generation: This function refers to the necessity to control the heat generation of the reactor so that fuel temperatures are not excessive. Since Criterion 2 limits exothermic chemical reactions, the sole requirement of this function is to assure reliable reactor shutdown.

MHTGR SDC 5 - Control Heat Generation

The reactor shall be designed, fabricated, and operated such that the inherent nuclear feedback characteristics ensure that the reactor thermal power will not exceed acceptable values. Additionally, the reactivity control system(s) shall be designed, fabricated, and operated such that during insertion of reactivity, the reactor thermal power will not exceed acceptable values.

FUNCTION: Control with Inherent Feedback: This function refers to the necessity to control the heat generation of the reactor so that fuel temperatures are not excessive.

MHTGR SDC 6 - Control with Inherent Feedback

The fuel uranium enrichment and heavy metal loadings in the kernels of the fuel particles within the graphite matrix compacts within the graphite fuel elements shall

be designed, fabricated, and operated such that the inherent nuclear feedback characteristics ensure the reactor thermal power will not exceed acceptable values.

FUNCTION: Control with Movable Poisons: This function refers to the means used to reduce reactor heat generation in off-normal situations commensurate with any reduction in heat removal or increase in reactivity. Two sets of control are chosen to be redundant and diverse in order to assure high reliability. One set of control is designed solely as a backup to normal reactor shutdown. The other normally assists in reactor control during power operation and is the primary means for shutdown during off-normal situations.

MHTGR SDC 7 - Control with Movable Poisons

Two independent and diverse means of inserting negative reactivity shall be provided. Either set shall be capable of limiting the heat generation of the reactor to acceptable levels during off-normal conditions.

FUNCTION: Shutdown Reactor: This function refers to the equipment necessary to sense the need for a trip of the control rods and to command and to execute the trip. The equipment must measure and interpret plant parameters and parameter changes so that command signals can be generated and delivered to the rod drives to release the rods into the reactor. The independent electrical power required to perform the sense, command, and execute actions, or “fail safe” design features which accomplish this, separate from normal electrical power, is also referred to in this function.

MHTGR SDC 8 - Shutdown Reactor

The equipment needed to sense, command and execute a trip of the control rods, along with any necessary electrical power, shall be designed, fabricated, and operated such that reactor core shutdown is assured during off-normal conditions.

FUNCTION: Maintain Geometry for Insertion of Movable Poisons: This function refers to the necessity to maintain the relative positions of the control rods and their guide tubes and the outer reflector blocks, and to keep the control channels in the individual blocks aligned so that sufficient control rod insertion can be made when needed. To ensure insertion capability, the geometries of the control rod guide, graphite core and reflector blocks, the core support structure, the core lateral restraint assemblies, the reactor vessel, and reactor vessel support must be ensured.

MHTGR SDC 9 - Maintain Geometry for Insertion of Movable Poisons

The design, fabrication, operation, and maintenance of the control rod guide tubes, the graphite core and reflectors, the core support structure, the core lateral restraint assemblies, the reactor vessel, and reactor vessel support shall be such that their integrity is maintained during off-normal conditions so as to provide geometry which permits sufficient insertion of the control rods into the outer reflector to effect reactor shutdown.

FUNCTION: Shutdown Reactor Diversely: This function refers to the equipment necessary to sense the need for a trip of the reserve shutdown control equipment, and to command and to execute the trip. The equipment must measure and interpret plant parameters and parameter changes so that command signals can be generated and delivered to the reserve shutdown control equipment to release the control material into the reactor. The electrical

power required to perform the sense, command, and execute actions is also referred to in this function.

MHTGR SDC 10 - Shutdown Reactor Diversely

The equipment needed to sense, command, and execute a trip of the reserve shutdown control equipment, along with any necessary electrical power. shall be designed, fabricated, operated, and maintained such that reactor core shutdown is assured during off-normal conditions.

FUNCTION: Maintain Geometry for Insertion of Movable Poisons: This function refers to the necessity to maintain the relative positions of the reserve shutdown control equipment guide tubes and the reserve shutdown control material channels in the core blocks, and to keep the control channels in the individual blocks aligned so that sufficient reserve shutdown control material can be inserted when needed. To ensure insertion capability, the geometries of the graphite core and reflector blocks, the core support structure, the core lateral restraint assemblies, the reactor vessel, and reactor vessel support must be ensured.

MHTGR SDC 11 - Maintain Geometry for Insertion of Diverse Movable Poisons

The design, fabrication, and operation of the reserve shutdown control equipment guide tubes, the graphite core and reflectors, the core support structure, the core lateral restraint assemblies, the reactor vessel, and reactor vessel support shall be such that their integrity is maintained during off-normal conditions, so as to provide geometry which allows sufficient insertion of reserve shutdown control material to effect reactor shutdown.

FUNCTION: Remove Core Heat: This function refers to the necessity to remove the reactor heat during off-normal conditions so that fuel temperatures are not excessive. Since the design selections needed to meeting Criterion 2 and Criterion 5 limit chemical attack and fission heat generation, the principal requirement is to assure reliable decay heat removal.

MHTGR SDC 12 - Remove Core Heat

The intrinsic dimensions and power densities of the reactor core, internals, and vessel and the passive cooling pathways from the core to the environment shall be designed, fabricated, and operated such that the fuel temperatures will not exceed acceptable values.

FUNCTION: Conduct Heat from Core to Vessel Wall: This function refers to the necessity of providing a path for the transfer of heat away from the reactor core so that fuel temperature are not excessive during a loss of forced circulation cooling.

MHTGR SDC 13 - Conduct Heat from Core to Vessel Wall

The reactor core design and configuration shall ensure sufficient heat transfer by conduction, radiation, and convection to the reactor vessel wall to maintain fuel temperatures within acceptable limits following a loss of forced cooling. The materials which transfer the heat shall be chosen to withstand the elevated temperatures experienced during this passive mode of heat removal. This criterion shall be met with the primary coolant system both pressurized and depressurized.

FUNCTION: Radiate Heat from Vessel Wall: This function refers to the necessity to remove from the vessel wall the heat generated in the core and transferred to the vessel wall.

Heat must be removed from the vessel wall at a rate which ensures that fuel and vessel temperatures are not excessive.

MHTGR SDC 14 - Radiate Heat from Reactor Vessel Wall

The reactor vessel design shall ensure that sufficient heat is radiated to the surroundings to maintain fuel and vessel temperatures within acceptable limits. This criterion shall be met with the primary coolant system both pressurized and depressurized.

FUNCTION: Maintain Geometry for Conduction and Radiation: This function refers to the necessity to maintain the geometry of the annular core and core supports and restraints so that the path for heat transfer between the core and vessel wall are ensured, and the necessity to maintain the geometries of the vessel and the RCCS so that the heat can be transferred from the vessel wall to the ultimate heat sink. Protecting the subject geometries will ensure the fuel temperatures are not excessive.

MHTGR SDC 15 - Maintain Geometry for Conduction and Radiation

The design, fabrication, operation, and maintenance of the core support structure, graphite core and reflectors, core lateral restraint assembly, reactor vessel, reactor vessel support, and reactor building shall be such that their integrity is maintained during off-normal conditions so as to provide a geometry conducive to removal of heat from the reactor core to the ultimate heat sink to maintain fuel temperatures within acceptable limits.

FUNCTION: Transfer Heat to Ultimate Heat Sink: This function refers to the necessity to dissipate the heat transferred from the reactor vessel wall to the reactor cavity. A means must be provided to remove the heat at a rate which limits temperatures in the core and vessel to acceptable levels. To enhance the reliability of the heat removal and ultimate heat sink passive means are favored.

MHTGR SDC 16 - Transfer Heat to Ultimate Heat Sink

A highly reliable, passive means of removing the heat generated in the reactor core and radiated from the reactor vessel wall shall be provided. The system shall remove heat at a rate which limits core and vessel temperatures to acceptable levels during a loss of forced circulation.

Here is one part with table wich is not included in the Blended Approach Document

Evaluation Methods and Associated Acceptance Criterial of Licensing Basis Events

In the U.S. per NRC guidance and practice, differing analysis treatments are utilized among the categories of LBEs, in terms of the evaluation methods and the associated acceptance criteria, particularly for DBEs, BDBEs, and DBAs. In addition, the offsite dose requirement in one of the key TLRC, 10CFR50.34, is utilized for the design and performance of SSCs and for determining site suitability, but is applied using different treatment methods. In addition, the distance at which the dose consequence or risk to the public is measured varies among the TLRC. These differences are shown in Table 14.

For AEs that are in the frequency range of occurring in the plant lifetime, the first row in Table 14 indicates that the mean (expected) consequences of AEs are summed in comparison to the 10 CFR 20 offsite dose of 0.1 rem at the EAB.

For DBEs that are event sequences with the entire plant responding that are not expected to occur in the plant lifetime, but which might occur in the lifetimes of a fleet of plants, the second row in the Table 14 shows that upper bound conservative analyses are compared to the 25 rem value in 10 CFR 50.34 for both the design and performance of SSCs and for site suitability. Additionally, for emergency planning each of the DBEs is compared to the 1 rem value in the EPA PAG at the emergency planning zone (EPZ) (10 miles for existing U.S. reactors), but now on an expected value basis as represented by the mean value in the uncertainty of the consequences.

As shown in the third row, for the BDBEs that are not expected to occur in a fleet of plants, sites are evaluated for accpetability based on the mean values but with conservative weather, compared to the 25 rem at the EAB. For emergency planning, the BDBEs are evaluated on an expected basis in comparison to the 1 rem at the EPZ.

In the last row in the Table 14, for DBAs that rely only on the SSCs that are classified as safety related; therefore, the DBAs are of equal or lower frequency (relative to DBEs), conservative upper bound analysis values are compared to the 10 CFR 50.34 offsite dose of 25 rem at the EAB. They are not used for emergency planning.

Finally, as shown in the last column of the Table 14, the AEs, DBEs, and BDBEs are summed over the frequency spectrum and then compared to the NRC Safety Goal risk to an average individual member of the public as quantified in the QHOs at 1 mile for acute (early) and 10 miles for latent (delayed) chance of individual fatality.

TABLE 14. ANALYSIS TREATMENT FOR LBES AND THEIR USAGE TO MEET TLRC

Event Category/ Type	10 CFR 20: 0.1 rem	10 CFR 50.34: 25 rem		EP PAGs: 1 rem	QHOs: Individual Risks
		SSC Performance	Site Suitability		
AEs	Mean Cumulative Evaluation at EAB				Mean Cumulative Evaluation at 1 and 10 miles
DBEs		Upper Bound Evaluation at EAB	Upper Bound Evaluation at EAB	Mean Evaluation at EPZ [*]	Mean Cumulative Evaluation at 1 and 10 miles
BDBEs			Mean ^{**} Evaluation at EAB	Mean Evaluation at EPZ	Mean Cumulative Evaluation at 1 and 10 miles
DBAs		Upper Bound Evaluation at EAB	Upper Bound Evaluation at EAB		

* Design objective: EPZ = EAB

** Upper bound weather per Regulatory Guide 1.145

The differing TLRC (what must be met), LBes (when the TLRC must be met), and analysis treatments are important in selecting the radionuclide design criteria (how and how well the TLRC must be met).

BriVaTech, 2017, *Safety Principles (Germany)*, Revision 0, BriVaTech-HTR-10-2017, May 2017.
 BriVaTech, 2017, *Summary of Design Basis Events*, Revision 0, BriVaTech-HTR-011-2017, May 2017.
 DOE, 1992, *Preliminary Safety Information Document for the Standard MHTGR*, Department of Energy, HTGR-86-024, Amendment 13, September 1992.
 DOE/NRC, 2008, *Next Generation Nuclear Plant Licensing Strategy - A Report to Congress*, Department of Energy/Nuclear Regulatory Commission, August 2008.
 EPA, 2017, *PAG Manual: Protective Action Guides and Training Guidance for Radiological Incidents*, U.S. Environmental Protection Agency, EPA-400/R-17/001, January 2017.
 EPAct, Public Law 109-58, 2005, "Energy Policy Act of 2005," 109th Congress, August 8, 2005.
 General Atomics, 1988, *Probabilistic Risk Assessment for the Standard Modular High Temperature Gas-Cooled Reactor*, DOE-HTGR-86011, Rev. 5, April 1988.
 Hanson, D.L., 2004, *A Review of Radionuclide Release from HTGR Cores during Normal Operation*, Electric Power Research Institute, Report 1009382, February 2004.
 Hoinakis, 1983, "Transport of Fission Products in Matrix and Graphite," *Proceedings of a Colloquium held at the Hahn Meitner Institute in Berlin from November 8-11, 1981*, HMI B372, June 1983.
 IAEA, 1997, *Fuel Performance and Fission Product Behavior in Gas Cooled Reactors*, International Atomic Energy Agency, TECDOC-978, November 1997.
 INL, 2010a, *NGNP Fuel Qualification White Paper*, Idaho National Laboratory, INL/EXT-10-17686, July 2010.
 INL, 2010b, *Mechanistic Source Terms White Paper*, Idaho National Laboratory, INL/EXT-10-17997, Rev. 0, July 2010.
 INL, 2010c, *Licensing Basis Event Selection White Paper*, Idaho National Laboratory, INL/EXT-10-19521, September 2010.
 INL, 2010d, *Summary for the Next Generation Nuclear Plant Project in Review*, Idaho National Laboratory, INL/EXT-10-19142, Rev. 1, September 2010.
 INL, 2011, *Next Generation Nuclear Plant Probabilistic Risk Assessment White Paper*, Idaho National Laboratory, INL/EXT-11-21270, September 2011.
 INL, 2014, *Role of Nuclear Grade Graphite in Controlling Oxidation in Modular HTGRs*, W. Windes, G. Strydom, R. Smith, and J. Kane, INL/EXT-14-31720, November 2014

IAEA, 2016, *Technical Report for IAEA CRP I31026 on Modular High Temperature Gas Cooled Reactors Safety Design: First Year Activities*, Japan Atomic Energy Agency, Revision 0, July 2016

IAEA, 2016, *Technical Report for IAEA CRP I31026 on Modular High Temperature Gas Cooled Reactors Safety Design: Second Year Activities*, Japan Atomic Energy Agency, Revision 0, July 2016.

IAEA, 2015, *Specific Safety Requirements for Design of Modular High-Temperature Gas-Cooled Reactors*, IAEA CRP I31026, Japan Atomic Energy Agency, Draft Revision 1, November 2015.

Martin, R. C., 1993, *Compilation of Fuel Performance and Fission Product Transport Models and Database for MHTGR Design*, Oak Ridge National Laboratory, ORNL/NPR-91/6, October 1993.

NRC, 1983, *PRA Procedures Guide*, NUREG/CR-2300, U.S. Nuclear Regulatory Commission, January 1983.

NRC, 1986, "Safety Goals for the Operations of Nuclear Power Plants; Policy Statement," Federal Register, Vol. 51, No. 149, pp. 28044–28049, August 4, 1986 (republished with corrections, Vol. 51, No. 160, pp. 30028-30033, August 21, 1986).

NRC, 1989, *Draft Preapplication Safety Evaluation Report for the Modular High-Temperature Gas-Cooled Reactor*, NUREG-1338, U.S. Nuclear Regulatory Commission, March 1989.

NRC, 1995, *Preapplication Safety Evaluation Report for the Modular High-Temperature Gas-Cooled Reactor (MHTGR)*, NUREG-1338, U.S. Nuclear Regulatory Commission, December 1995.

NRC, 2008, *Updated Policy Statement on Regulation of Advanced Reactors*, SECY-08-130, U.S. Nuclear Regulatory Commission, September 11, 2008 and Staff Requirements Memorandum March 26, 2008.

NRC, 2013, *Summary Feedback on Four Key Licensing Issues*, Next Generation Nuclear Plant Project 0748, Draft, U.S. Nuclear Regulatory Commission, Office of New Reactors, March 8, 2013.

NRC, 2014, *Summary Feedback on Four Key Licensing Issues*, Next Generation Nuclear Plant Project 0748, U.S. Nuclear Regulatory Commission, Office of New Reactors, July 17, 2014.

NRC, 2015, *Recommendations on Issues Related Implementation of Risk Management Regulatory Framework*, SECY-15-0168, U.S. Nuclear Regulatory Commission, January 7, 2016.

NRC, 2016, *Accident Source Terms and Siting for Small Modular Reactors and Non-Light Water Reactors*, SECY-16-0012, U.S. Nuclear Regulatory Commission, February 7, 2016.

ONR, 2014, *Safety Assessment Principles for Nuclear Facilities*, Revision 0, Office for Nuclear Regulation, November 2014.

Reutler, H., and G. H. Lohnert, 1984, "Advantages of Going Modular in HTRs," Nuclear Engineering and Design Vol. 78, pp. 129–136.

4.2. APPROACH 2 (TOP DOWN APPROACH)

IAEA report_2nd Year (2) Process Safety Req_R1

Japan Atomic Energy Agency (IAEA) has been developing the HTGR technology and its heat application technologies (i.e., hydrogen production technology using the thermochemical water splitting Iodine Sulfur (IS) process and power generation by helium gas turbine), and is accumulating the valuable data on the HTGR safety features through the operation and the safety demonstration tests using the High Temperature Engineering Test Reactor (HTTR) [49] [1] Japanese first HTGR type test reactor, to establish the fundamental HTGR technologies for the commercial HTGR systems. The safety requirements for the design of HTTR were developed in 1980's based on those of Light Water Reactor (LWR) by implementing new HTGR specific requirements and eliminating the LWR specific ones. The safety requirements for the design of the commercial HTGRs are expected to be developed fully taking into account of the safety features of HTGR, and authorized by the regulatory authority prior to the construction of a lead plant of the commercial HTGRs. In this context, the research committee on the safety standards for HTGRs [35] [2] was established in 2013 under the Atomic Energy Society of Japan (AESJ) with the support of the Research Association of High Temperature Gas Cooled Reactor Plant (RAHP). The objective of the research committee is to develop the draft of the specific safety requirements (SSR) for the design of modular HTGRs analogous to the IAEA SSR for LWR design (IAEA SSR-2/1 (Rev.1)) [2] [3] taking into account the modular HTGR safety features so as to provide the safety requirements and guide for designers

and regulators, and to show the safety advantages of modular HTGR to the future HTGR users as well as nuclear experts in other fields. The safety requirements for the design of modular HTGRs, which incorporate the HTGR safety features demonstrated using HTTR, lessons learned from the Fukushima Daiichi accident and requirements for the integration of the heat application facility (i.e., hydrogen production plants) was developed in the research committee. JAEA contributed to this research committee by providing the knowledge and technical information of HTGR, and leading the discussion. This chapter provides the process to develop the safety requirements for design of modular HTGRs described as Approach 2.

4.2.1. Development Process

The developed safety requirements are expected to be applied to the land-based stationary nuclear installations with modular HTGRs designed for electricity generation and heat utilization applications (e.g., hydrogen production, process heat/steam for industrial applications, desalination, district heating, etc).

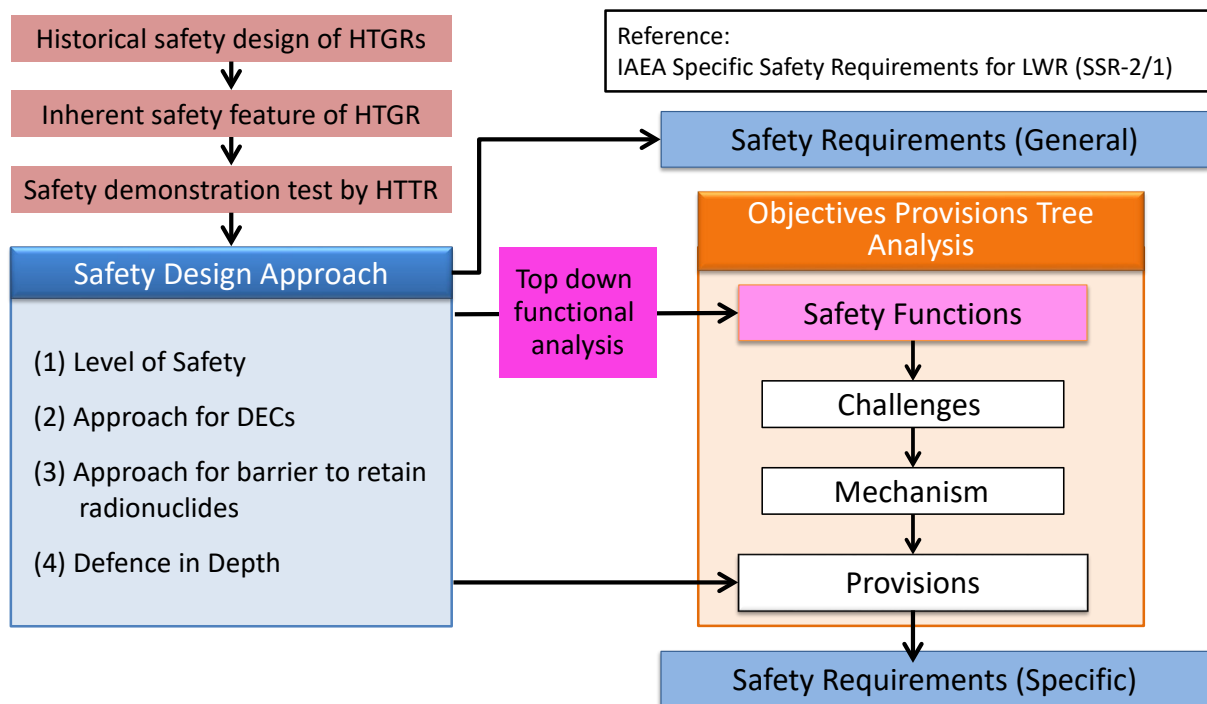


FIG. 30. Process flow scheme to develop the safety requirements from approach 2.

Figure 30 shows the process flow scheme to develop the safety requirements. The safety design approach for modular HTGRs was determined prior to the drafting of the safety requirements to establish a high level of safety design standards taking into account of the knowledge of historical design of modular HTGRs, inherent and passive safety features of modular HTGRs and the test data obtained by the safety demonstration test using HTTR.

The safety functions were analyzed by top down functional analysis based on the safety design approach. Comprehensive off-normal events are deterministically identified as challenges to the confinement function of physical barriers taking into account of the modular HTGR characteristics. The safety functions are then determined as measures to prevent the occurrence of the challenges to the confinement function of physical barriers.

The safety requirements is then developed from the safety functions by using the top down analysis methodology, objectives provisions tree method [40] [4] which is a fundamental methodology to develop the safety requirements. The IAEA specific safety requirements (SSR) for LWR design (IAEA SSR-2/1 (Rev.1)) is used as a reference for drafting the safety requirements for the design of modular HTGRs (e.g., items of requirements, general requirements, depth of documentation, etc.). The following sections provide more detail analysis procedures and its results.

4.2.2. Safety Function Analysis

Figure 31 shows a master logic diagram to determine the safety functions. The IAEA safety objective is defined as “protect people and the environment from harmful effects of ionizing radiation” in the IAEA Safety Fundamentals [2] [5]. The radiation exposure and the release of radioactive material shall be controlled in the design of the nuclear plants to meet the IAEA safety objective. Three fundamental requirements are derived as “control of the radiation exposure from reactor core and the release of radioactive material”, “control of radioactive effluents and radioactive waste” and “control of fuel handling and storage”. The latter two requirements might be independent of the reactor type. Therefore, the safety functions to ensure “control of the radiation exposure from reactor core and the release of radioactive material” were analyzed in this approach. It was categorized into “control of the radiation exposure from reactor core” and “control the release of radioactive material” as shown in the Figure 31. The shielding against radiation, the control of the release of radioactive material from intact barriers, and the control of the release of radioactive material from failed barriers were selected as the safety functions deterministically.

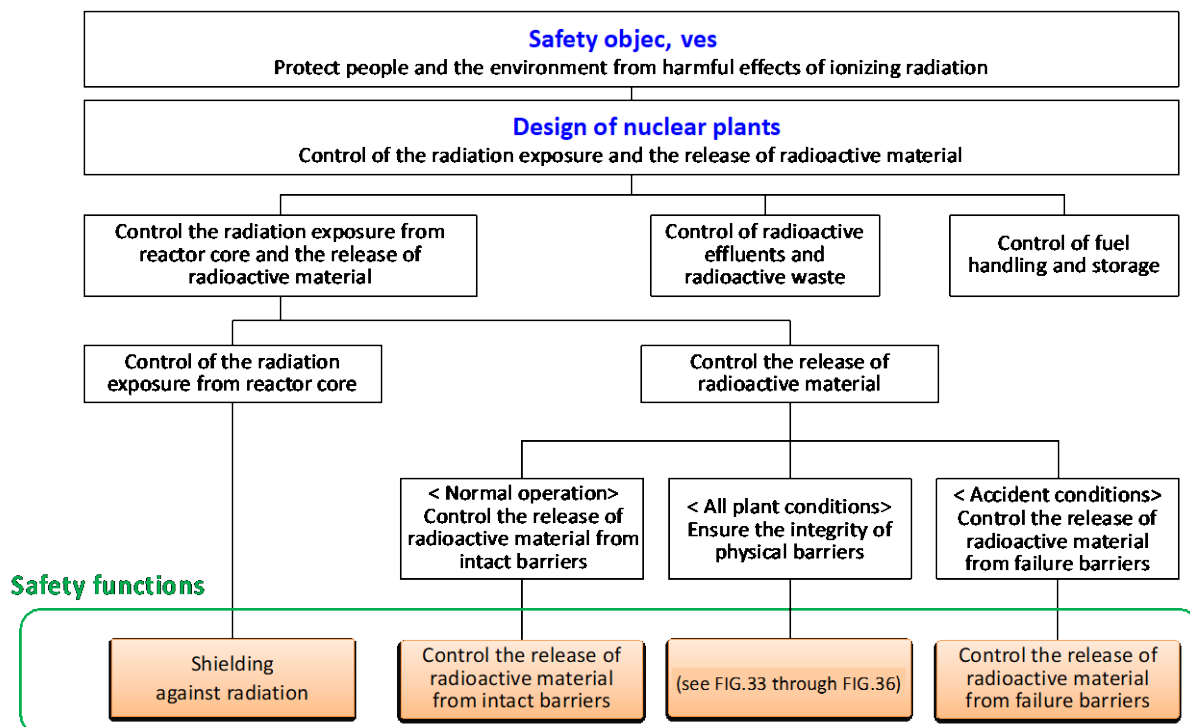


FIG. 31. Master logic diagram of top down functional analysis of the safety functions.

The safety functions to ensure the integrity of physical barriers were analyzed systematically using a similar manner to the objective provision tree methods as shown in Figure 32. The top

column of the diagram is indicating the physical barrier to retain the radionuclides (i.e., the coated fuel particle, the fuel element, the reactor coolant pressure boundary and the confinement). The comprehensive off-normal events were deterministically identified as challenges to the confinement function of physical barriers from a physical and chemical point of view as shown in the second column. It was determined by taking into account physical and chemical phenomena that degrade confinement function of physical barrier, mechanisms whose consequences create these challenges and its causes. Finally, the provisions which are measures to prevent the occurrence of the causes were determined and defined as the safety functions.

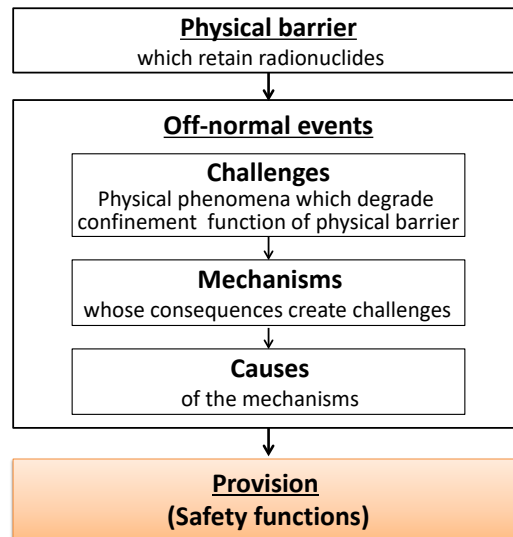


FIG. 32. Method to determine the safety functions to ensure the integrity of physical barrier.

The results of the safety function analysis for each barrier are shown in Figures 33, 34, 35 and 36. Comprehensive off-normal events are postulated such as a heat up, a core oxidation and an increase of load to each physical barrier. The analysis results of the safety functions to ensure the integrity of physical barriers are summarized in Table 15. The safety functions are categorized into the related barriers. The safety functions of control of reactivity, heat removal from core and reactor coolant pressure boundary (RPB), maintain core geometry and control stress are the same as those of LWRs. On the other hand, the safety function of the control of chemical attack and combustible gas, which are derived from the challenges of oxidation of the coating layer of CFP and fuel element, are determined as the modular HTGRs-specific ones.

TABLE 15. RELATIONSHIPS BETWEEN PHYSICAL BARRIERS AND SAFETY FUNCTIONS TO PROTECT THE INTEGRITY OF PHYSICAL BARRIERS

Safety functions	Physical barriers			
	Coated fuel particle	Fuel element	Reactor coolant pressure boundary (RPB)	Confinement
Control reactivity	O	-	O	-
Heat removal from core	O	-	O	-
Control chemical attack	O	O	-	-
Control combustible gas	O	O	O	O
Control load	O	O	O	O
Maintain core geometry	O	-	O	-
Heat removal from RPB	-	-	O	-

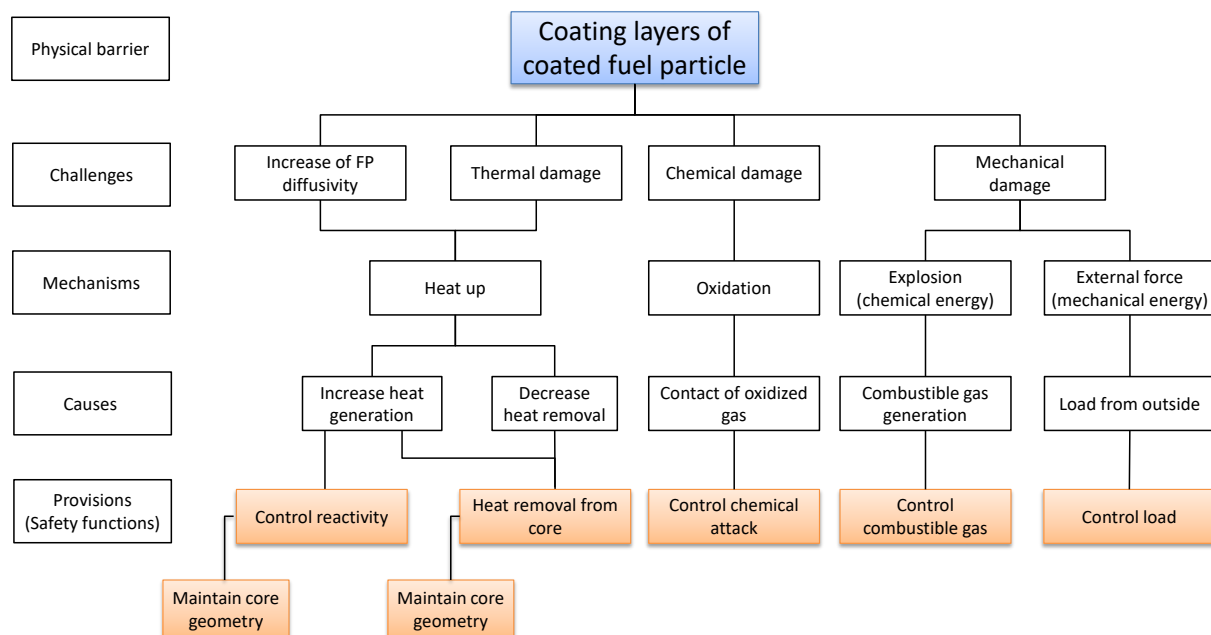
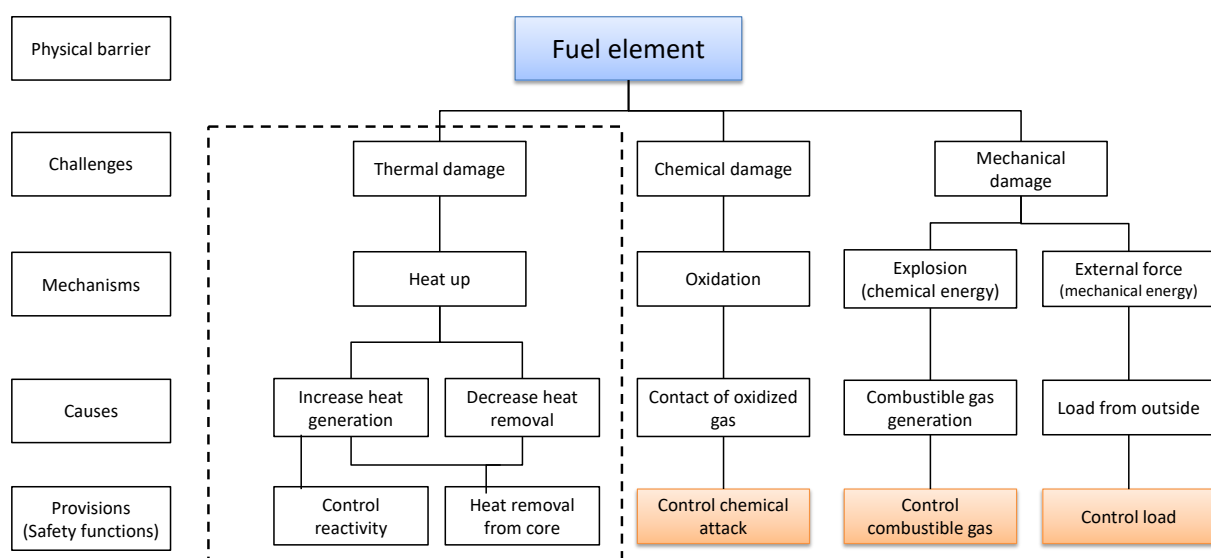


FIG. 33. Safety functions analysis results to ensure the integrity of the coating layer of the coated fuel particle.



* Safety functions for CFP against thermal damage covers those for fuel element, because the temperature limit of fuel element (core graphite) is higher than that of CFP.

FIG. 34. Safety functions analysis results to ensure the integrity of the fuel element.

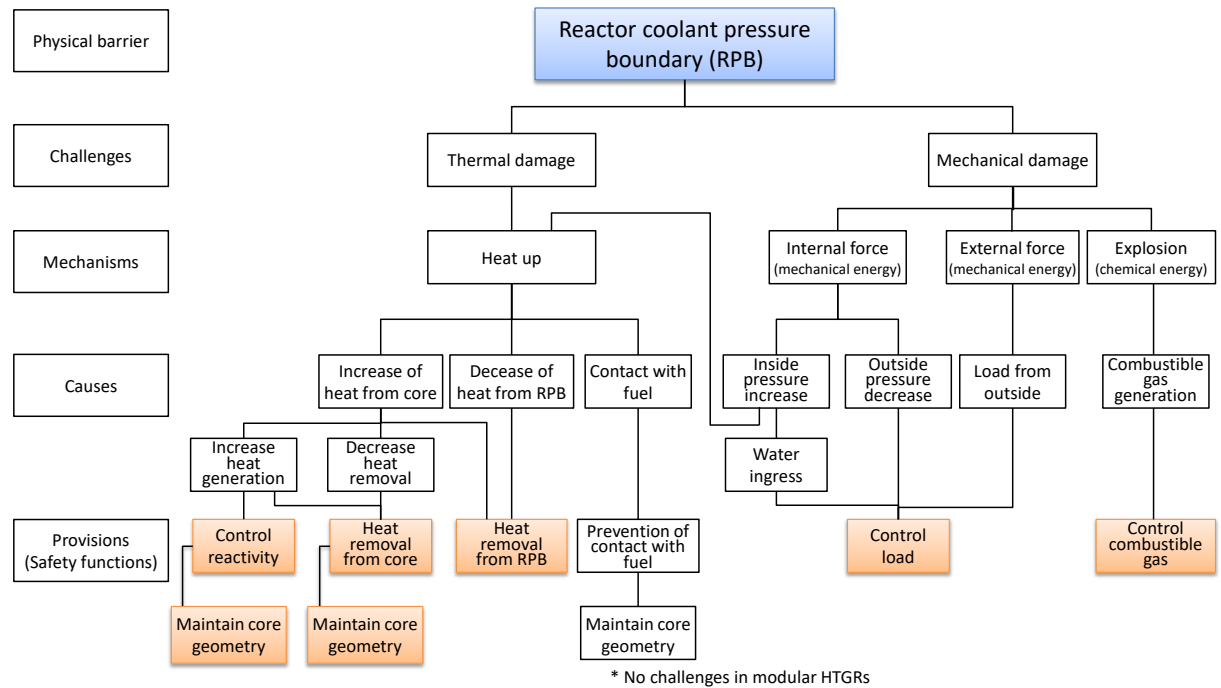


FIG. 35. Safety functions analysis results to ensure the integrity of the reactor coolant pressure boundary.

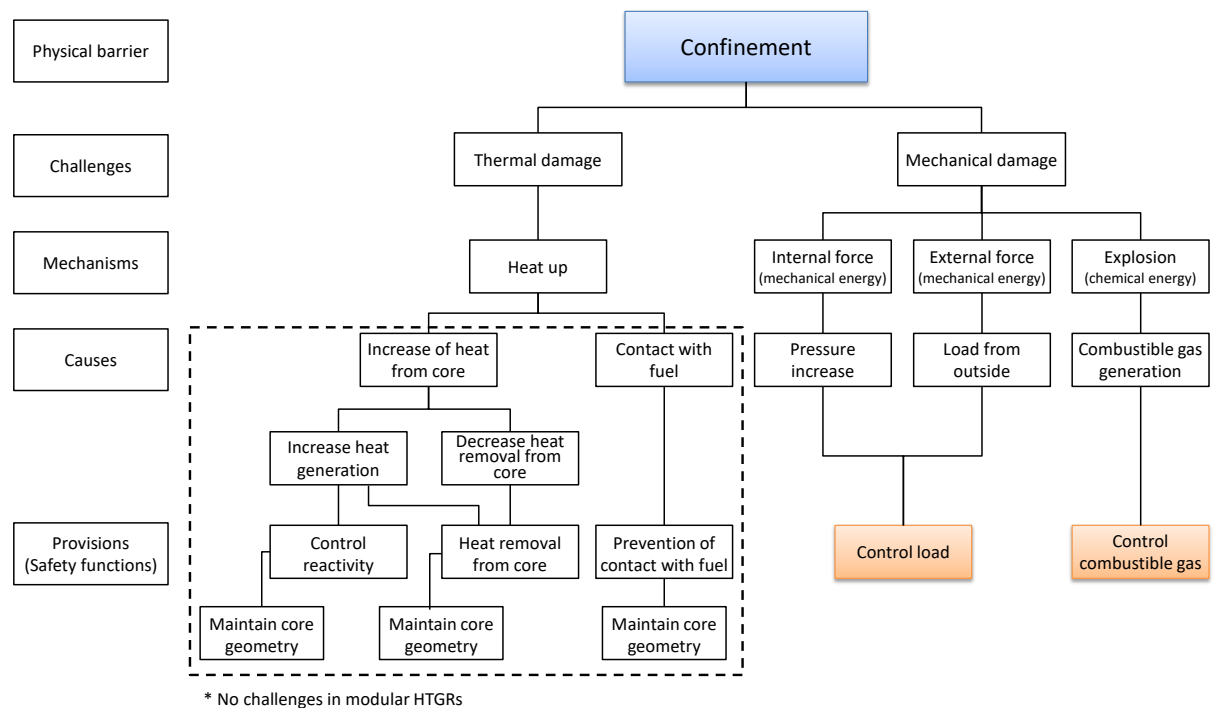


FIG. 36. Safety functions analysis results to ensure the integrity of the confinement.

4.2.3. Functional Requirements Analysis (Objectives Provisions Tree Analysis)

The functional requirements were analyzed using the objectives provisions tree method to draft the safety requirements. The challenges which have an impact on the intended performance of the safety functions and mechanisms whose consequences creates challenges to the performance of the safety functions were identified for each physical barrier and safety function as listed in Table 15. The mechanisms of challenges are considered as more detailed off-normal

events than those postulated in the safety function analysis. Note that the detail identification of off-normal events for the safety analysis will be performed during the design process for each individual plant. Then a list of provisions that should be implemented to prevent the mechanisms from the occurring and to prevent challenges to the safety functions were derived based on the safety design approach.

The objectives provisions tree analysis results are shown in Appendix I in Figure I.1 through Figure I.18. The provisions are corresponding to the functional requirements. The functional requirements obtained from the objectives provisions tree analysis were then categorized into related SSCs as listed in Table 16 of the first and second columns. Then the functional requirements, which can be described in the same safety requirement, are grouped. The last column represents the candidate title of requirements in the document of safety requirements which contains functional requirements in the second column of the Table 16.

TABLE 16. FUNCTIONAL REQUIREMENTS OBTAINED BY OBJECTIVES PROVISIONS TREE ANALYSIS AND ITS CATEGORIZATION INTO SAFETY REQUIREMENTS

SSCs	Functional requirements	Candidate title of requirements in the safety requirements for the design of modular HTGRs
General	To prevent missile caused by internal events and to mitigate its consequence	Internal and external hazards
	To maintain operational limits and conditions	Operational limits and conditions for safe operation
	To monitor plant parameter in normal operation	Provision of instrumentation
	To control the plant	Control systems
	To protect deviations from normal operational states	Protection system
Reactor core	To prevent release of radioactive materials	Performance of fuel particles
	To mitigate oxidation of coated fuel particle (CFP)	
	To mitigate oxidation of graphite structure	Scope (definition of graphite)
	To prevent contact of oxidation gases to CFP	Scope (definition of graphite) Performance of fuel elements
	To prevent occurrence of stress to CFP	Performance of fuel elements, Structural capability of the reactor core
	To assure the structural integrity for the heat removal from core	Structural capability of the reactor core
	To assure the structural integrity for reactor shutdown and the maintaining the reactor subcritical	
	To mitigate reactivity insertion by over cooling	Structural capability of the reactor core, Control of the reactor core
	To mitigate power increase	
	To prevent reactivity insertion	Control of the reactor core
	To mitigate reactivity insertion	
	To prevent unacceptable recriticality	
	To prevent xenon oscillations	
	To shutdown reactor	Reactor shutdown
Reactor coolant system	To prevent and mitigate release of radioactive material from fuel to the environment	Design of reactor coolant systems
	To prevent reactivity insertion by over cooling (related to gas circulator)	
	To mitigate air ingress (related to gas circulator)	
	To mitigate water ingress (related to gas circulator)	
	To protect reactor coolant pressure boundary	

	To protect reactor coolant pressure boundary from overpressure (pressure decrease outside reactor coolant pressure boundary)	
	To mitigate reactivity insertion by over cooling (related to gas circulator)	Operational limits and conditions for safe operation, Control systems
	To mitigate reactivity insertion by over cooling (pressure increase inside reactor coolant pressure boundary)	Overpressure protection of the reactor coolant pressure boundary
	To cleanup reactor coolant	Cleanup of reactor coolant
	To mitigate water ingress (related to secondary coolant system)	Design of secondary coolant systems using water or steam
	To protect reactor coolant pressure boundary from overpressure (pressure increase outside reactor coolant pressure boundary)	
	To prevent missile caused by internal events and to mitigate its consequence	Internal and external hazards.
	To mitigate core heat up	Structural capability of the reactor core
	To remove heat from core	Structural capability of the reactor core, Residual heat transfer from the reactor core to an ultimate heat sink
	To transfer heat to ultimate heat sink	
	To remove heat from reactor coolant pressure boundary	

4.2.4. Requirements for coupling heat application facility

The fundamental requirements for coupling heat application facility to nuclear facility are as follows [42] [7];

- i. Assurance of the safety of nuclear facility against postulated events initiated in heat application facility, and
- ii. Certification of heat application facility as a nonnuclear facility, that is, construction and operation of heat application facility under non-nuclear regulation.

6.1. Requirements to Assure Safety of Nuclear Facility

The following phenomena are postulated from safety viewpoint when heat application facility is coupled with the nuclear reactor [42] [7].

- Temperature and pressure transients induced by abnormal events in heat application facility
- Migration of chemicals (combustible gases and hazardous chemicals) from heat application facility to reactor
- Migration of tritium from reactor to heat application facility

The functional requirements related to above phenomena were analyzed using the objectives provisions tree methodology. It was confirmed that the functional requirements for the nuclear facility without coupling of heat application facility envelop that with coupling of heat application facility.

6.2. Requirements to Certificate Heat Application Facility as a Non-nuclear Facility

The criterion to certificate heat application facility as a non-nuclear facility is to exempt heat application facility from the safety-related SSCs of nuclear facility [42] [7]. This criterion leads the following detail criteria.

- Maintain normal operation of nuclear facility against temperature and pressure transients induced by abnormal events in heat application facility without relying on SSCs in heat application facility.
- Assure the reactor safety against chemicals (combustible gases and hazardous chemicals) would migrate from heat application facility to nuclear facility without relying on SSCs in heat application facility.
- Ensure tritium concentration in heat application facility below an allowable limit without relying on SSCs in heat application facility.

6.3. Safety Requirements to Couple Heat Application Facility

Based on the above discussions, the safety requirements for the design of HTGRs shall not be applied to the design of heat application facility if above criteria to certificate heat application facility as non-nuclear facility are satisfied. Under this condition, abnormal events in the heat application facility shall be defined as external hazards and, it is required to be physically separated from the nuclear facility to prevent harmful disturbances over the nuclear facility if they do occur. Vice versa, if normal operation and abnormal events in the heat application facility affect normal operation of the nuclear facility, the design for the heat application facility shall be such as to ensure that the safety requirements of nuclear facility are all met.

- [1] S. Saito, et al., “Design of High Temperature Engineering Test Reactor (HTTR),” *JAERI 1332*, (1994).
- [2] H. Ohashi, et al., “Safety Design Approach for the Development of Safety Requirements for Design of Commercial HTGR,” *Proceedings of the HTR 2014*, Weihai, China, October 27-31, 2014, Paper HTR2014-81150 (2014) (CD-ROM).
- [3] INTERNATIONAL ATOMIC ENERGY AGENCY, *Safety of Nuclear Power Plants: Design*, IAEA Safety Standards Series No. SSR-2/1 (Rev.1), IAEA, Vienna (2016).
- [4] INTERNATIONAL ATOMIC ENERGY AGENCY, *Assessment of Defence in Depth for Nuclear Power Plants*, IAEA Safety Report Series No. 46, IAEA, Vienna (2005).
- [5] INTERNATIONAL ATOMIC ENERGY AGENCY, *Fundamental Safety Principles*, IAEA Safety Standards Series No. SF-1, IAEA, Vienna (2006).
- [6] H. Ohashi, H. Sato, K. Kunitomi, et al., “Concept on Inherent Safety in High-Temperature Gas-Cooled Reactor,” *Transactions of the Atomic Energy Society of Japan*, 13 (1), 17 (2014) (in Japanese).
- [7] H. Sato et al., “Safety Design Consideration for HTGR Coupling with Hydrogen Production Plant,” *Progress in Nuclear Energy*, 82, 46 (2015).

Tables XX in APPENDIX III represent the overall comparison table which contains the Specific Safety Requirements No. SSR-2/1 (Rev. 1) as a reference and Specific Safety Requirements for Design of Modular HTGR (HTGR-SSR) initially provided by Japan (JAEA), reviewed and discussed in the IAEA CRP on Modular High Temperature Gas-cooled Reactor Safety Design.

5. SUMMARY OF SAFETY DESIGN CRITERIA COMPARISON FROM THE TWO APPROACHES

- [Draft CRP TECDOC on Blended Approach → (Action 1 (US))]

5.1. SUMMARY AND PATH FORWARD

Two approaches to development of SDC have been compared using two versions of modular HTGRs as examples. Approach 1 that is the primary focus of this report is consistent with IAEA NR 54. It begins with identifying the top level requirements for *what* must be met, uses risk insights to identify *when* the top requirements are to be met, determines the required safety functions that is how the design meets the top requirements during the off-normal events, and finally develops the functional qualitative statements that form the SDC for each safety function. Approach 2 has started with the IAEA Requirements Light Water Reactors in SSR (Ref) and utilizing experience and engineering judgement modified them to develop a set applicable to the modular HTGR.

To understand the differences between the two sets of SDC, input from other CRP participants from other countries for the Approach 1 steps was examined:

A comparison of the top requirements from three other countries showed large variations. The U.K. and U.S. both have requirements expressed as risks of the entire event frequency, while Germany uses a more deterministic approach that examines only the PIEs. This makes a direct comparison between all three countries difficult. There is not only disagreement between countries on the dose consequences, but also on what the design frequency should encompass. Generally, the U.K. and particularly Germany have requirements that are more restrictive than the U.S.

Whereas the top level safety requirements showed significant differences from country-to-country, the off-normal events that are designed for showed greater similarities, particularly, for the German HTR-Module and the U.S. MHTGR that both utilize a steam Rankine cycle.

Greater similarities between the two approaches were noted with the comparison of safety functions. For example, both approaches emphasize retention within the fuel particles/compacts. Both approaches retain the radionuclides within the fuel by controlling core heat generation with a strong negative temperature coefficient and high reliability shutdown systems and removing core heat passively from the reactor vessel to an ultimate heat sink, consistent with the definition of a modular HTGR. Finally, the Japan inclusion of deterministic BDBA/DEC leads to SSCs such as a confinement for retention of radionuclides and control of chemical attack that also will lead to differing SDCs.

With the above as a starting point, the path forward recommended is that the CRP members work to reach a blend of the two approaches with the following initial guidelines:

- The SDCs should first be written for the common features and safety functions of a modular HTGR, regardless of fuel type, reactor geometry, or power cycle. Use should be made of Ref (xx), which provides the modular HTGR definition.
- The SDCs should apply to those events that within the design basis: risk-informed AOOs and DBEs and deterministic DBAs. Design Extension Conditions may be added later.

- Risk-informed BDBEs and deterministic BDBAs should not be included in the SDCs since, by definition, they are beyond the design basis.
- The SDCs should be written with a clear explicit link to the modular HTGR safety functions and worded consistently, more along the lines of Approach 1 than the Approach 2 LWR requirements that are broader in nature and have evolved with time and event.

Table shows overlap of the 2 approaches

Example of table that shows comparison and provides suggestion

MHTGR SDCs Approach 1	MHTGR SDCs Approach 2	Comment/Suggestion
MHTGR SDC 1 - Control Radionuclides in Fuel: The reactor fuel shall be designed, fabricated, and operated such that radionuclides are retained within the fuel to the extent that releases to the primary coolant will not exceed acceptable values.	Requirement 42: Performance of coated fuel particles and fuel elements Coated fuel particles for the nuclear installations shall be designed to maintain their structural integrity, and to withstand satisfactorily the anticipated radiation levels and other conditions in the reactor core, in combination with all the processes of deterioration that could occur in all plant states. Fuel elements shall be designed to maintain their structural integrity in the operational states, and to prevent the occurrence of events that could lead to unacceptable loads to the coated fuel particles in accident conditions.	

6. DEFENCE IN DEPTH IN TERMS OF THE RADIONUCLIDE RETENTION ALLOCATION TO THE BARRIERS.

INL/EXT-16-38812 (A08)(US)

6.1. RADIONUCLIDE RELEASE BARRIERS

The barriers to radionuclide release that form of a functional containment system for modular HTGRs are as follows:

1. Fuel particle kernel
2. Fuel particle coatings (SiC and PyC)
3. Core graphite and carbonaceous materials
4. Helium pressure boundary (HPB)
5. Reactor building.

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

6.1.1. Fuel Particle Kernel

The first barrier to radionuclide transport and release is the fuel kernel itself. Under normal operating conditions, the kernel retains a substantial fraction (>95%) of the radiologically important, short-lived fission gases, such as Kr-88 and I-131. At elevated temperatures, the effectiveness of the fuel kernels for retaining fission gases can be reduced to a retention fraction of 80 - 90% at the peak temperature locations (Martin 1993).

The release of short-lived fission gases from heavy-metal contamination and from fuel kernels is typically expressed in terms of the release rate-to-birth rate ratio (R/B). At steady state, the R/B ratio is numerically equal to the fractional release. The fission gas release models give the R/Bs from heavy-metal contamination, bare kernels, and from failed particles under irradiation as a function of chemical element, isotope half-life, temperature, and burnup. These functional dependencies are determined experimentally.

Metallic radionuclides such as silver, cesium, palladium, and perhaps other noble metals, are diffusively released to a significant degree from the small percentage of fuel kernels at the upper end of the range of normal operating temperatures (typically > 1100 – 1200°C). The other fission metals, including radiologically important Sr-90, are only released from the kernel by fission recoil at normal operating temperatures. Under elevated temperature conditions, the retention in fuel kernels of long-lived, volatile fission metals such as Cs, Ag, and Sr is strongly dependent on temperature and burnup.

Fractional releases of fission gases from exposed fuel kernels under irradiation can be enhanced if the kernel is hydrolyzed by reaction with water vapor, which may be present in the helium coolant (e.g., because of a tube leak in a SG located in the primary helium loop). The magnitude of the effect depends first and foremost, on the amount of moisture in the helium coolant that penetrates the fuel element and the outer layers of the fuel particle coatings without reacting to reach the fuel particle kernels. Then, the radionuclide release depends upon the kernel composition, with UC₂ showing the largest enhancement and UO₂ showing the least. The

effect for UCO is intermediate. With kernels containing uranium carbide, the water reacts to convert the carbide phase completely to oxide along with kernel swelling and increased porosity. With UO₂ kernels, a hyperstoichiometric uranium oxide phase may be formed. In any case, kernel porosity is increased with enhanced fission gas release (INL 2010b).

The extensive international database on the radionuclide release from fuel kernels has been summarized in numerous review documents (IAEA 1997, Martin 1993, Hanson 2004).

6.1.2. Fuel Particle Coatings

The second and most important barrier to radionuclide release from the core, particularly during accidents, is the SiC and PyC coatings of each fuel particle. Both the SiC and PyC coatings provide a barrier to the release of fission gases. The SiC coating acts as the primary barrier to the release of metallic fission products because of the low solubilities and diffusion coefficients of fission metals in SiC. The PyC coatings are partially retentive of Cs at lower temperatures but provide little holdup of Ag and Sr (INL 2010a).

Coated particle in-service failure or degradation can entail failure of both the PyC layers and the SiC layer resulting in an exposed kernel (particle failure), or degradation of only the SiC layer such that the remaining intact PyC layers continue to retain fission gases. In-service failures are primarily due to manufacturing defects, such as a thin or missing buffer layer.

There are considerable international data on the transport of radionuclides in the SiC and PyC coatings of TRISO fuel particles (e.g., IAEA 1997). At accident temperatures, most of these data were obtained by heating irradiated particles, and effective diffusion coefficients were deduced from the observed time histories of fission product release. At temperatures typical during normal operation, data were obtained from irradiations.

6.1.3. Core Graphite and Carbonaceous Materials

For a prismatic core, the fuel compact matrix and the fuel block graphite are collectively the third fission product transport and release barrier. For a pebble bed core, the analog is the pebble matrix, including the unfueled outer shell of the spherical pebble fuel element. Radionuclide transport in fuel matrix and fuel element graphite is treated collectively since the experimental techniques to characterize radionuclide transport in them are the same, and the radionuclide transport mechanisms appear to be the same based on available data (INL 2010b).

The fuel matrix material is a relatively porous carbonaceous material that provides little holdup of the fission gases that are released from the fuel particles. The effect is generally neglected in calculations of fission gas transport in the fuel matrix as well as in the fuel block graphite. However, the fuel matrix is a composite material that has a high content of amorphous carbon, and this constituent of the matrix is highly sorptive of metallic fission products, especially strontium, europium, and actinides.

The graphite block of a prismatic fuel element, which is denser and has a more ordered structure than the fuel matrix material, is somewhat less sorptive of the fission metals than the matrix, but it is more effective as a diffusion barrier. The effectiveness of the graphite as a release barrier decreases as the temperature increases. Under typical steam-cycle core conditions, with helium coolant temperatures at the core outlet on the order of 750°C, the fuel element graphite attenuates the release of Cs from the core by an order of magnitude, and the Sr is essentially completely retained. The extent to which the graphite attenuates Ag release is less well-

characterized, and there is some evidence that the retention of Ag by graphite increases as the total system pressure increases, implying gas phase transport through the interconnected pore structure of the graphite. Fission metals that escape the core in either a prismatic or pebble bed reactor will be sorbed into upper and lower graphite reflectors in addition to being deposited onto metallic surfaces as the primary coolant circulates through the system.

The international database for radionuclide transport in matrix and graphite has been summarized previously (Hoinkis 1983, IAEA 1997). The database for nuclear graphite is large in recognition of its effectiveness as a release barrier in HTGR cores. Only cesium and silver nuclides effectively migrate through the fuel element graphite at normal operating temperatures. The other fission metals, including strontium, europium, and the actinides, are completely retained by the graphite during normal operation.

A fraction of the strontium and europium is released under core heat-up peak temperature conditions, but the actinides are still completely retained. Events entailing ingress of moisture into the reactor can result in limited graphite oxidation and mobilization of radionuclides contained in the oxidized graphite. However, as discussed in Section 6.3, measures are taken to limit these effects.

2.4.4 Helium Pressure Boundary

The fourth transport and release barrier is the HPB, which contains the primary circuit. Radionuclides that are transported from the core are transported throughout the primary circuit by the helium coolant. Although the primary purpose of the helium purification system (HPS) is to control chemical impurities in the helium, the HPS, if available, efficiently removes both gaseous and metallic radionuclides from the helium at a rate determined by the gas flow rate through the purification system (INL 2010b).

For the condensable radionuclides, 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 volatile radionuclides, and by the temperatures of the surfaces. Condensable radionuclides may also be transported throughout the primary circuit sorbed on particulates (“dust”), which may be present in the primary circuit. The distribution of these contaminated particulates may be considerably different from the distribution of radionuclides transported as atomic species.

The circulating, dust, and plateout activities in the primary circuit are potential sources of release to the environment in the event of helium leaks or as a result of the venting of helium in response to over pressurization of the primary circuit (e.g., in response to significant water ingress because of an SG tube leak in a steam cycle plant). The fraction of the circulating activity lost during such events is essentially the same as the fraction of the helium that is released, although 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 dust may be re-suspended 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 by the presence of friable surface films on primary circuit components, which could possibly spall off during a rapid depressurization.

Other mechanisms that can potentially result in the removal and subsequent environmental release of primary circuit plateout activity are “steam-induced vaporization” and “washoff.” In both cases, the vehicle for radionuclide release from the primary circuit is water that has entered the primary circuit. In principle, both water vapor and liquid water could partially remove plated out radionuclides. However, even if a fraction of the plated out radionuclides is removed from the fixed surfaces, there would be environmental release only in the case of venting of helium/steam from the primary circuit. For all but the largest water ingress events, the pressure relief valve does not lift. Moreover, the radiologically important nuclides, such as iodine and cesium, are expected, based on available data, to remain preferentially in the liquid water that remains inside the primary circuit.

6.1.4. Reactor Building

The reactor building is the fifth and final barrier to the transport and release of radionuclides to the environment. Its effectiveness as a release barrier is highly event specific. A vented low pressure reactor building is the baseline design for both prismatic and pebble bed modular HTGRs. Retention of radionuclides in the reactor building is influenced by several factors, including the extent to which the design of the building is compartmentalized, the action of the reactor building heating, ventilation, and air conditioning (HVAC) system, the action of the building overpressure relief system, and reactor building leakage (INL 2010b).

In the event of reactor helium depressurization transients, louvers in the reactor building open, and a significant portion of the released helium coolant is vented to the environment until the pressure in the reactor building is reduced to near atmospheric pressure, at which time the louvers close. Consequently, radionuclide retention in the reactor building is limited in the near term for rapid depressurization transients. However, if the event also involves the unavailability of all forced cooling systems, considerable retention is predicted during longer-term core conduction cooldown transients. Under such conditions, the natural removal mechanisms occurring in the reactor building, including condensation, fallout, and plateout, are expected to attenuate the release of condensable radionuclides, including the radiologically important iodine isotopes, by at least an order of magnitude.

The transport behavior of radionuclides during core conduction cooldown accidents in modular HTGRs is much simpler than that in LWR’s loss-of-coolant accidents that result in core melt. 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 aerosols are not expected to form. Dust present in the primary circuit during normal operation and liftoff of plated out radionuclides may add to the activity released from the primary circuit into the reactor building during rapid depressurization accidents, but the chemical and physical nature of this material is quite different from LWR aerosols.

The reactor building consists of the structures shown in the Figure 37 which illustrates a typical below-grade reactor building.

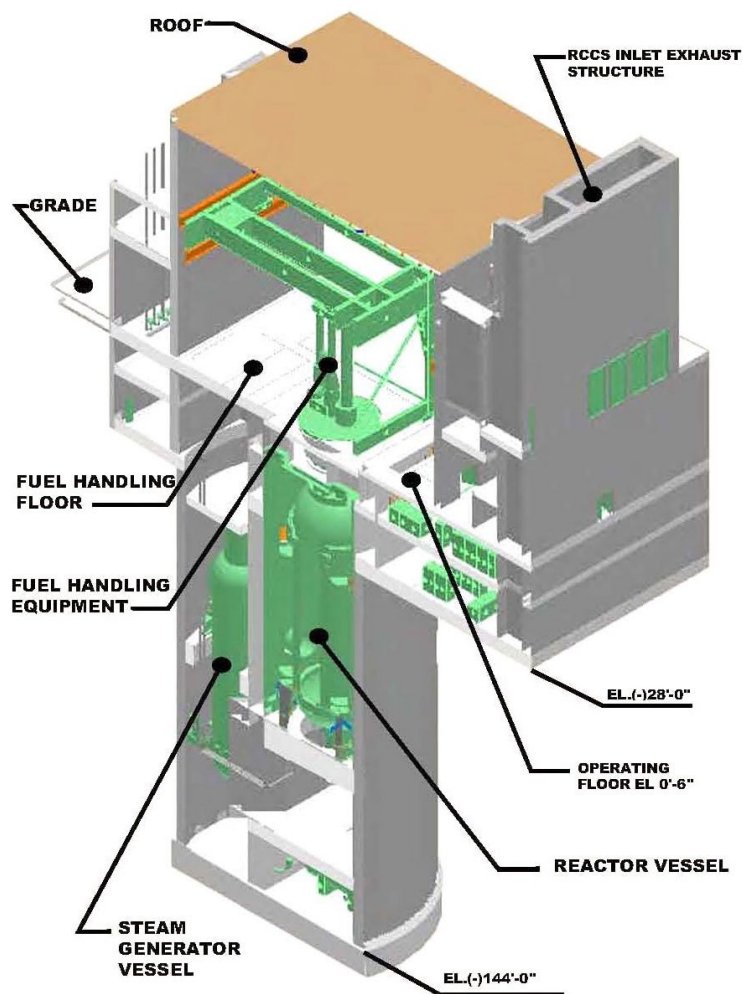


FIG. 37. Typical below-grade reactor building.

USA 2018 Draft DID Content for TECDOC - Rev 0

The objectives of this TECDOC section are to:

- Describe how the concept of protective strategies of DID are used to define DID attributes that are incorporated into the plant capabilities that support each layer of defense. The resolution of the general concept of protective strategies into a set of DID attributes is necessary to support an objective evaluation of DID adequacy. These DID attributes are reflected in the design features of the plant and the reliabilities and capabilities of structures, systems, and components (SSCs), including radionuclide

barriers¹ that contribute to multiple, functionally independent layers of defense, in the prevention and mitigation of accidents with adverse effects on public health and safety.

- Summarize the programmatic attributes of DID to provide adequate assurance that the DID plant capabilities in the design are realized when the plant is constructed and commissioned and are maintained during the plant design life cycle.
- Discuss the roles of programmatic attributes of DID to compensate for uncertainties, human errors, and hardware failures.
- Identify the importance of defenses against common cause failures and need to minimize dependencies among the layers of defense.
- Present guidelines for evaluating and establishing DID adequacy.

6.2. FRAMEWORK FOR ESTABLISHING ADEQUACY OF DEFENSE-IN-DEPTH (DID)

6.2.1. Defense-in-Depth Philosophy

According to the NRC glossary [43], defense-in-depth (DID) is described as:

..an approach to designing and operating nuclear facilities that prevents and mitigates accidents that release radiation or hazardous materials. The key is creating multiple independent and redundant layers of defense to compensate for potential human and mechanical failures so that no single layer, no matter how robust, is exclusively relied upon. Defense in depth includes the use of access controls, physical barriers, redundant and diverse key safety functions, and emergency response measures.

A graphic that describes the concept of layers of defense embodied in this philosophy taken from NUREG/KM-0009 [44] is shown in Figure 38. As discussed more fully in Reference [44], this framework is consistent with the “levels of defense” concept advanced by the International Atomic Energy Agency in Reference [45].

¹ In this paper, the term “barrier” is used to denote any plant feature that is responsible to either full or partial reduction of the quantity of radionuclide material that may be released during a Licensing Basis Event (LBE). LBEs are comprised of Anticipated Operation Occurrences, Design Basis Events, Design Basis Accidents, and Beyond Design Basis Events. “Barrier” includes features such as physical or functional barriers or any feature that is responsible as part of a layer of defense for mitigating the quantity of radionuclide material released from the plant including time delays during transport that permit radionuclide decay or provide extended response times for compensatory actions.

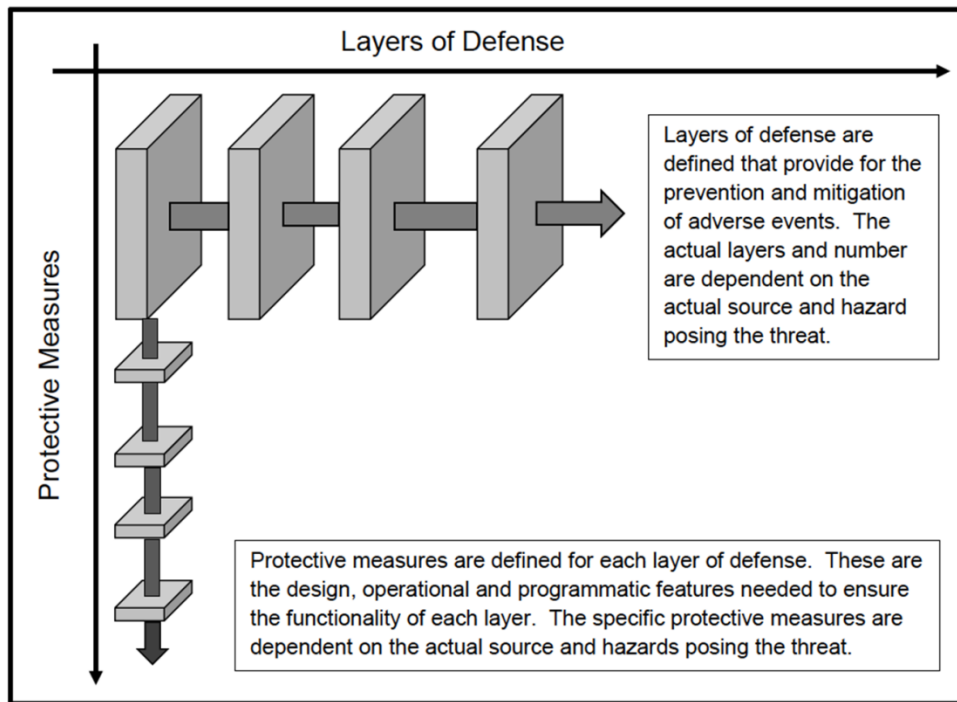


FIG. 38. U.S. Nuclear Regulatory Commission's Defense-in-Depth Concept [44].

6.3. FRAMEWORK FOR ESTABLISHING DID ADEQUACY

The process for using the layers of defense for performing the evaluation of plant capabilities and programs, which has been adapted from the IAEA "levels of defense" approach, is shown in Figure 39. This process is used to evaluate each LBE and the DID attributes that have been incorporated to prevent and mitigate accident sequences to incorporate adequate SSC reliability and capability.

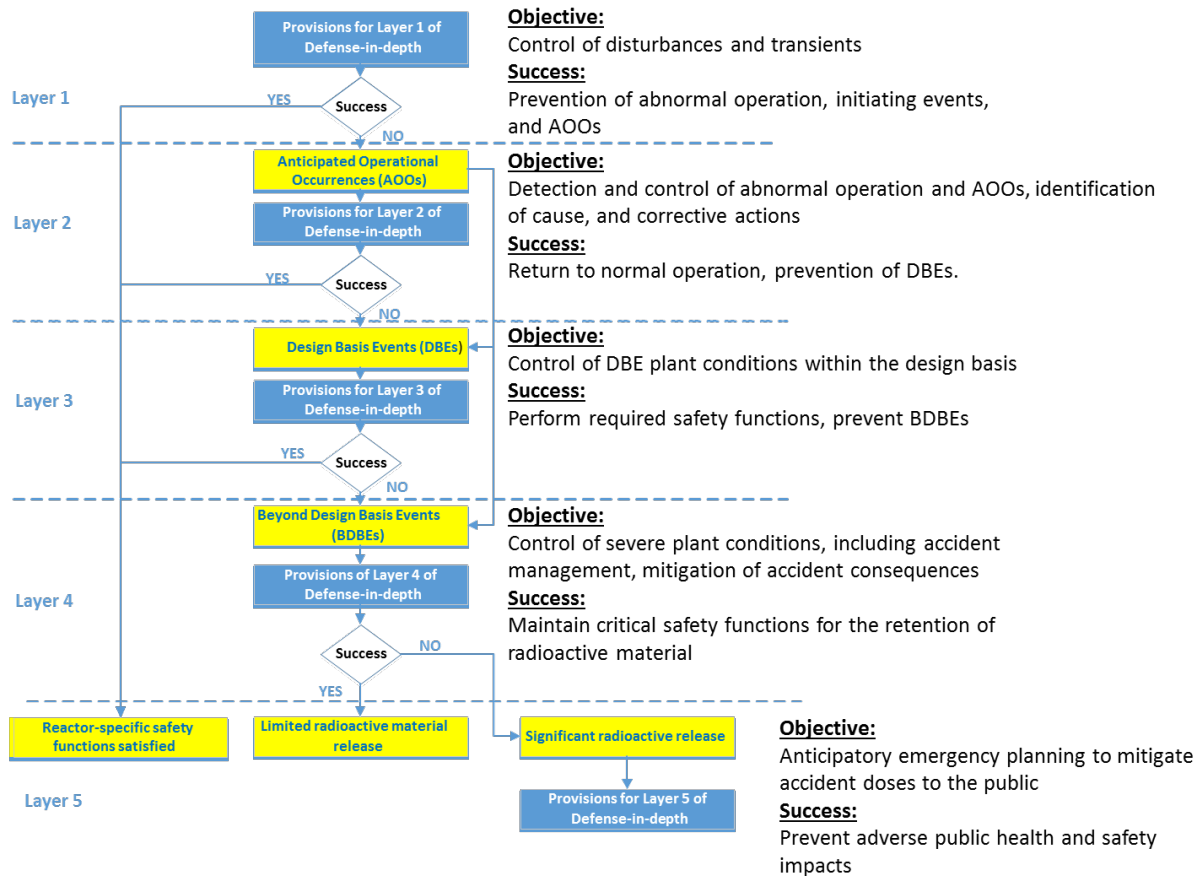


FIG. 39. Process for evaluating LBEs using layers of defense concept adapted from IAEA [45].

6.4. INTEGRATED APPROACH FOR INCORPORATION AND EVALUATION OF DID

DID is incorporated into all phases of defining the design requirements, developing the design, evaluating the design using applicable deterministic and probabilistic perspectives, and defining the programs that are to be implemented to ensure adequate protection. The execution of the DID elements is accomplished in the context of an integrated decision making process throughout the plant lifecycle.

6.5. COMPENSATORY ACTION SELECTION AND SUFFICIENCY

6.5.1. Choosing DID Compensatory Actions

Because the design, safety analyses, and PRA will be developed in phases and in an iterative fashion, the DID adequacy evaluation and baseline are updated as the design matures consistent with the chosen approach and options for implementing that approach. (It's noted that the PRA can provide key insights in performing these iterative adequacy evaluations when implementing either approach). The DID evaluation is developed in the design process to adjust the plant capability features or programmatic actions as the state of DID knowledge improves with the design evolution.

6.5.2. Plant or Programmatic Changes

The addition of new features, improved plant capabilities or additional programmatic controls or assurance activities should provide demonstrable improvements in predicted plant

performance, risk reduction, elimination or material reduction of significant uncertainties or greater assurance of plant performance. **At no point should programmatic actions alone be taken to solve a plant performance vulnerability associated with an event that can lead directly to exceedance of an applicable safety target, goal or regulation.**

Improve Plant Capability

During the development of the functional design (pre-conceptual, conceptual and preliminary design phases), DID insights that highlight significant adverse risks, smaller margins than desired or overdependence on certain design features should be addressed with a bias towards improvements in the plant capability. Consideration of the practicality of potential actions should include counterproductive safety impacts such as operational complexity increases, extended outage impacts, increased plant staff radiation exposures, waste disposal as well as business issues such as capital cost increases, delivery schedule impacts, plant output and availability.

Improve Plant Performance Assurance

Programmatic actions can be important elements of safety assurance and should be used to assure the construction and operations stay within the design envelope established for the plant. The application of special treatment is in part compensation for uncertainties in performance of SSCs associated with significant LBEs. Other special treatments are part of effective monitoring of plant and SSC performance over time to assure the realized performance remains within the design basis.

Programmatic controls such as initial in-plant testing, technical specifications, operating procedures for all modes and states, conservatively established alarm and control setpoints, performance monitoring programs and corrective maintenance programs should be put in place for risk significant SSCs.

6.5.3. DID Attributes to Achieve Plant Capability DID Adequacy

The evaluation of Plant Capability DID adequacy focuses on the completeness, resiliency and robustness of the plant design with respect to addressing all hazards, responding to identified initiating events, the availability of independent levels of protection in the design for preventing and mitigating initiating events progressions, and the use of redundant and diverse means to achieve the needed levels of protection sufficient to address different threats to public health and safety. Additionally, the Plant Capability DID adequacy evaluation examines whether any single feature is relied on to achieve public safety objectives, and if so identifies options to reduce or eliminate such dependency. The completion of the Plant Capability DID adequacy evaluation provides the necessary basis to conclude that there is “Adequate Protection” that public health and safety will be protected. Table 17 provides a listing of the Plant Capability DID attributes and principal evaluation focus included in this DID evaluation scope. The evaluation of Plant Capability involves the systematic evaluation of hazards that exist for a given technology and specific design over the spectrum of all modes and states including anticipated transients and potential accidents within and beyond the design basis.

TABLE 17. PLANT CAPABILITY DEFENSE-IN-DEPTH ATTRIBUTES

Attribute	Evaluation Focus
Initiating Event and Accident Sequence Completeness	PRA Documentation of Initiating Event Selection and Event Sequence Modeling
Layers of Defense	Multiple Layers of Defense
	Extent of Layer Functional Independence
	Functional Barriers
	Physical Barriers
Functional Reliability	Inherent Reactor Features that contribute to performing safety functions
	Passive and Active SSCs performing safety functions
	Redundant Functional Capabilities
	Diverse Functional Capabilities
Prevention and Mitigation Balance	SSCs performing prevention functions
	SSCs performing mitigation functions
	No Single Layer /Feature Exclusively Relied Upon

TABLE 18. EVENT SEQUENCE MODEL FRAMEWORK FOR EVALUATING PLANT CAPABILITIES FOR PREVENTION AND MITIGATION OF LBES

Standard Elements of Accident Sequence	Design Features Contributing to Prevention	Design Features Contributing to Mitigation
Initiating event occurrence	Reliability of SSCs supporting power generation reduces the initiating event frequencies; successful operation of the SSCs prevents the sequence	Capabilities of normally operating systems to continue operating to prevent initiating events serve to mitigate events and faults that may challenge these functions
Response of active SSCs supporting safety functions: successful and failed SSCs	Reliability and availability of active SSCs reduce sequence frequency; successful operation of these SSCs prevents the sequence	Capabilities of active successful SSCs reduce the impacts of the initiating events and reduce the challenges to barrier integrity.
Response of passive features supporting safety functions: successful and failed SSCs.	Reliability and availability of passive SSCs reduce sequence frequency; successful operation of these SSCs prevents the sequence	Capabilities of passive successful SSCs reduce the impacts of the initiating events and reduce the challenges to barrier integrity.

Standard Elements of Accident Sequence	Design Features Contributing to Prevention	Design Features Contributing to Mitigation
Fraction of source term released from fuel	None	Inherent and passive capabilities of the fuel given successful active or passive SSCs limit the release from the fuel.
Fraction of source term released from the coolant pressure boundary	None	Inherent and passive capabilities of the pressure boundary given successful active or passive SSCs and the capabilities of the fuel limit the release from the pressure boundary.
Fraction of source term released from reactor building barrier	None	Inherent and passive capabilities of the reactor building barrier conditioned on the successful response of any active or passive SSCs along the sequence and the capabilities of the fuel and coolant pressure boundary limit the release from the reactor building barrier.
Time to implement emergency plan protective actions.	None	Inherent and passive features and capabilities of the fuel, coolant pressure boundary, and reactor building barrier conditioned on the successful response of any active or passive SSC along the sequence dictate the time available for emergency response.

The attributes of Programmatic DID complement each other and provide overlapping assurance that the design plant capability is achieved in design, manufacturing, construction and operations lifecycle phases. The evaluation focus items in Table 19 should be answered for each Programmatic DID attribute (for risk significant LBEs when using Approach 1) to determine that the Programmatic DID provides sufficient confidence that there is reasonable assurance of adequate protection of public health and safety based on the design plant capability. The net result of the Programmatic DID evaluation is the selection of special treatment programs for all safety significant SSCs, which include those classified as Safety Related (SR) or Non-Safety Related with Special Treatment (NSRST). Examples of special treatment considerations are summarized in Table 20.

TABLE 19. PROGRAMMATIC DID ATTRIBUTES

Attribute	Evaluation Focus
Quality / Reliability	Performance targets for SSC reliability and capability
	Design, manufacturing, construction, operations and maintenance features or special treatment sufficient to meet performance targets

Attribute	Evaluation Focus
Compensation for Uncertainties	Compensate for Human Errors
	Compensate for Mechanical Errors
	Compensate for Unknowns
Off-Site Response	Emergency Response Capability

TABLE 20. EXAMPLES OF SPECIAL TREATMENTS CONSIDERED FOR PROGRAMMATIC DEFENSE-IN-DEPTH

- Engineering assurance programs:
 - Special treatment specifications
 - Independent design reviews
 - Physical testing and validation including integrated and separate effects tests
- Organizational and human factors programs:
 - Plant simulation and human factors engineering
 - Training and qualification of personnel
 - Emergency operating procedures
 - Accident management guidelines.
- Technical specifications:
 - Limiting conditions for operation
 - Surveillance testing requirements
 - Allowable outage (completion) times.
- Plant construction and start-up programs:
 - Equipment fabrication
 - Construction
 - Factory testing and qualification
 - Start-up testing.
- Maintenance and monitoring of SSC performance programs.
 - Operation
 - In-service testing
 - In-service inspection
 - Maintenance of SSCs
 - Monitoring of performance against reliability and capability performance indicators.
- Quality assurance program:
 - Inspections and audits
 - Procurement
 - Independent reviews
 - Software verification and validation.
- Corrective action programs:
 - Event trending
 - Cause analysis
 - Closure effectiveness.
- Independent Oversight and Monitoring Programs
- Equipment qualification
 - Seismic qualification
 - Adverse environment qualification
 - Physical protection
- Emergency Planning.

- A06_BriVaTech-HTR-026

The implementation of defense in depth (DID) for Modular HTGRs differs from that for traditional LWR strategy to achieve effective defense against radiological hazards. The safety of Modular HTGRs relies strongly on the inherent features, with the confinement of radionuclides being accomplished with minimal or no reliance on active systems or operator actions.

Defense in depth consists of a hierarchical deployment of different levels of equipment and procedures in order to maintain the effectiveness of physical barriers placed between radioactive materials and workers, the public and the environment.

The description of these barriers that can be identified in Modular HTGRs requires special attention because their importance to safety may vary relative to water reactors. A proposed definition of the barriers is as follows: the kernel, three particle coating layers, the matrix, the fuel element, the primary circuit, the plant civil/structural/confinement works, and the filtering systems.

6.6. HTR-MODULE BARRIER CONCEPT

- The minimization of radioactive releases during normal operation and accidents.
- Knowing the design of an HTR the accident analyses have to demonstrate with adequate safety margins that the radioactive releases are far below the governmental dose limits.
- So the question is:
What is the quality of each barrier and the quality of all together against radioactive releases?

6.6.1. First Barrier

Fuel particles:

-More or less a safe confinement of radioactivity (depending on burn up and temperature)

-Quality of this first barrier is given by the failed Particle Fraction Curve

In general during licensing procedures the data for calculation are about one magnitude higher than the expected values.

So this curve is the starting point for the discussion of barriers.

For HTR Module (Siemens design) the curve was based on the German fuel tests.

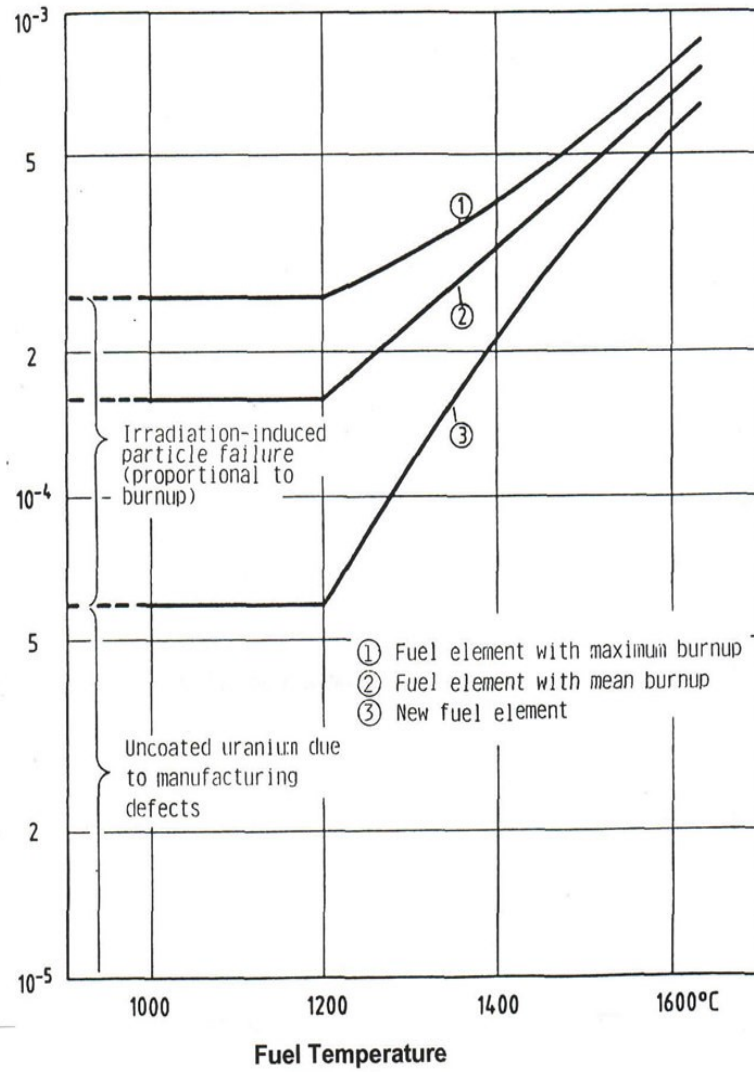


FIG. 40. Maximum failed particle fraction as a function of fuel temperature.

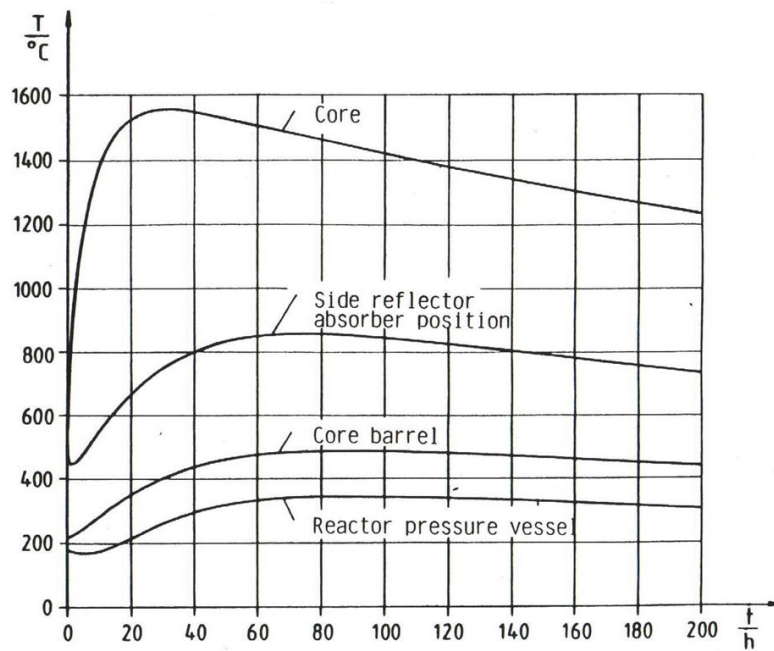


FIG. 41. Peak temperature versus time diagram.

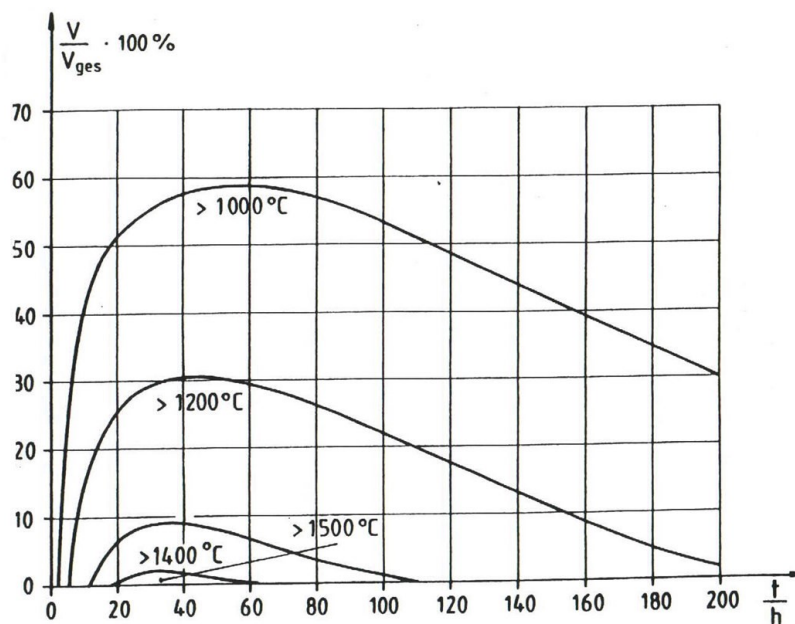


FIG. 42. Volumetric fractions of core at certain temperatures, core heat-up phase.

6.6.2. Second Barrier

Primary gas envelope (primary boundary):

More or less a good confinement of radioactivity (depending on the quality of the components and pipings)

Using the quality of LWRs (nuclear grade class 1 - whatever that means in different countries):

You can use the break postulations (state of the art):

- no through wall cracks in vessels
- 2A breaks in pipings with known probability

If you change the quality of the second barrier, you have to strengthen the first or the third barrier.

For the HTR-MODULE it was postulated (like PWRs in Germany)

- small breaks (DN10) - unisolable (Quality class for small piping)
- large breaks (DN65) - isolable (Quality class 2)
- large breaks (DN65) - unisolable (Quality class 1)
 - low probability
 - only a few connections to the vessel

In the Figure 43 the correlation between the component and system classification and the different radiological events are given.

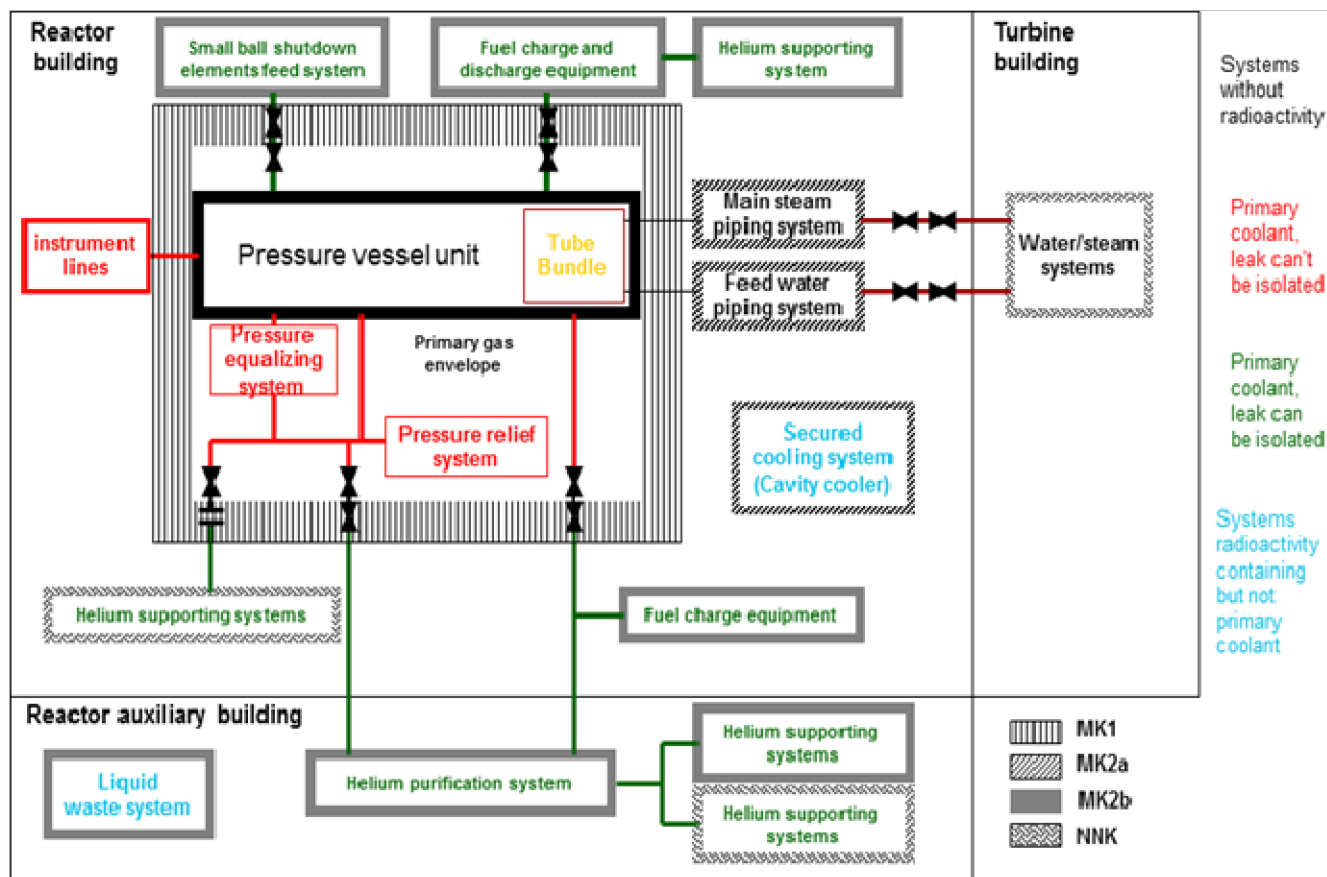


FIG. 43. Correlation between event classification and system classification, along with quality requirements. (MK1, MK2a, MK2b are quality classes and NNK means non-nuclear classified (see APPENDIX II))

6.6.2.1. Small Break (DN10)

Assumptions:

Scram signal delayed to the break.
 Time of pressure loss several hours.
 No dust release out of the core.
 No pressure build up in the building.
 Release by the stack (normal path).

Radioactive release:

	Filtered	Unfiltered
Noble Gases	6.2 E+11 Bq	6.2 E+11 Bq
Iodine	3.4 E+07 Bq	3.4 E+09 Bq
Sr, Ag, Cs	3.3 E+03 Bq	3.3 E+06 Bq

Radiological Impact (dose)

	Filtered	Unfiltered	Limit
Whole Body (adult)	8.42 E-07 Sv	2.43 E-06 Sv	0.05 Sv
Thyroid (child)	5.70 E-06 Sv	4.88 E-04 Sv	0.15 Sv

Result:

Impact far below the limits

Decision:

Filters are not safety related, so in the licensing procedure the reference case is the unfiltered one.

6.6.2.2. Large Break (DN65) - isolable

Assumptions:

Direct counter measures of reactor protection system (scram, actuation of isolation valves).
 Pressure build up in the building relatively low.
 Release by the stack (normal path).

Radioactive release:

Depending on the broken system, the helium purification system is covering all other systems.

Radiological Impact (dose)

	Unfiltered	Limit
Whole Body (adult)	6.68 E-06 Sv	0.05 Sv
Thyroid (child)	2.63 E-04 Sv	0.15 Sv

(Values coming from calculations for a break in the auxiliary building)

Result:

Impact far below the limits

Decision:

Filters are not safety related, so in the licensing procedure the reference case is the unfiltered one.

6.6.2.3. Large Break (DN65) - unisolable

Depressurization phase:

Assumptions:

Direct counter measures of reactor protection system.

Depressurization time of about 3 minutes.

Pressure build up in the building.

Relief dampers to the stack open.

Radioactive release:

- Content of the primary circuit
- Content of helium purification system incl. desorption of filters
- Desorption of surface activity in the primary circuit
- Dust (1 kg)
- No plate out in the building

	Unfiltered	Factor: Design/Expected
Noble Gases	3.3 E+12 Bq	~3
Iodine	9.1 E+09 Bq	~100
Sr, Ag, Cs	5.3 E+06 Bq	~50
Tritium	5.6 E+12 Bq	~2
C14	6.0 E+10Bq	~10

Radiological Impact (dose)

	Unfiltered	Limit
Whole Body (adult)	9.76 E-06 Sv	0.05 Sv
Thyroid (child)	5.45 E-04 Sv	0.15 Sv

TABLE 21. CONTRIBUTION TO THE SOURCE TERM "DEPRESSURISATION PHASE AFTER UNISOLABLE DN65 PIPE BREAK" (DESIGN VALUES), HTR-MODULE

Nuclide	Contribution (in percent)			
	Steady State Coolant Activity	Desorption	Dust Release	Helium Purification System
Kr 88	83.2	-	-	16.8
Xe 133	9.9	-	-	90.1
I 131	23.0	71.0	6.0	-
Cs 137	18.6	57.4	24.0	-
Sr 90	<0.1	<0.3	99.7	-
Ag 110m	9.3	28.8	61.9	-
H3/C14	2.0	-	-	98.0

Core heat-up phase

Assumptions:

All operating parameters very high (temperature, power)

Failure of the first protection signal (single failure in reactor protection system - not normal in licensing)

Combination (addition) of uncertainties result: about 130K to the calculated values.

Gas expansion in the vessel due to temperature increase will end after 160 hours with 9% vol. increase, end of release into the building.

No plate out in the building

Radioactive release to the building:

	Design		Expected	
	T (lic.)	T (nom.)	T (lic.)	T (nom.)
Iodine	1.3 E+10 Bq	5.3 E+09 Bq	4.2 E+09 Bq	1.5 E+09 Bq

Radioactive release to environment:

	Filtered	Unfiltered
Xe 133	2.7 E+11 Bq	2.7 E+11 Bq
I 131	1.3 E+08 Bq	1.3 E+10 Bq
Ag 110m	1.2 E+06 Bq	1.2 E+09 Bq
Cs 137	2.0 E+06 Bq	2.0 E+09 Bq
Sr 90	1.0 E+04 Bq	1.0 E+07 Bq

Radiological Impact (Dose):

Depressurization and Heat-up Phase:

	Filtered	Unfiltered	Limit
Whole Body (adult)	9.8 E-06 Sv	2.97 E-04 Sv	0.05 Sv
Thyroid (child)	6.22 E-04 Sv	1.23 E-02 Sv	0.15 Sv

Result:

Impact far below the limits

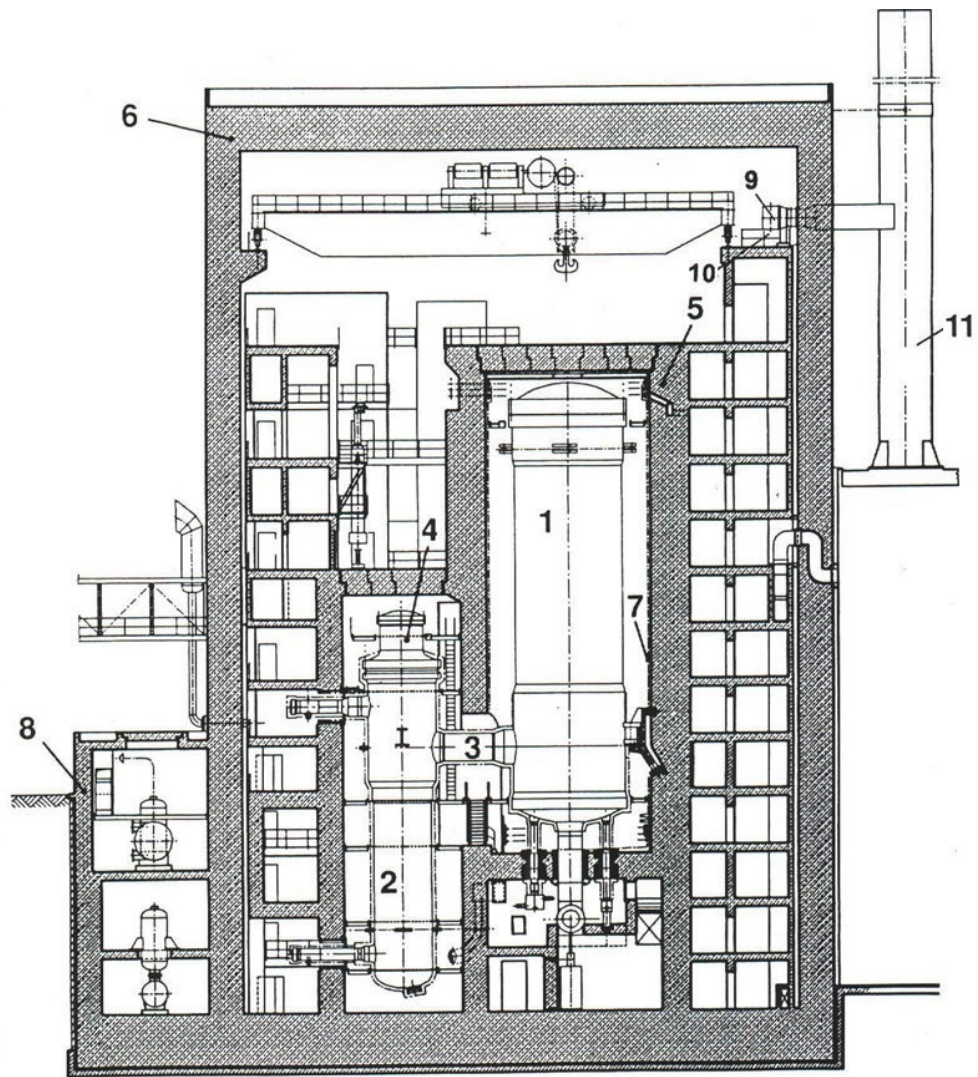
Decision:

Filters are not safety related, so in the licensing procedure the reference case is the unfiltered one.

6.6.3. Third Barrier

Confinement Envelope consists of:

- Reactor Building (leak tightness 50Vol.%/day)
- Building pressure relief system
- HVAC system isolation
- Subatmospheric pressure system (filter) as operational system



Legend:

- | | |
|------------------------------|-----------------------------------|
| 1 Reactor Pressure Vessel | 2 Steam Generator Pressure Vessel |
| 3 Connecting Pressure Vessel | 4 Primary Circuit Blower |
| 5 Primary Cell | 6 Protective Shell |
| 7 Surface Cooler | 8 Reactor Building Annex |
| 9 Relief Damper | 10 Isolation Damper (manually) |
| 11 Stack | |

Design Basis Accidents	SAR (1988)	Dose (TEDE) Sv	
		EAB (2 hour) ⁽¹⁾	NRC Limit ⁽²⁾
Break of a Large Connecting Pipe (DN 65) - LBLOCA short-term unfiltered release	6.2.3.1.1	unfiltered: 1.361E-04 (13.61 mrem)	2.5E-1 6.3E-2 2.5E-2
Break of a Large Connecting Line (DN 65) - LBLOCA long-term unfiltered release with core heat up	6.2.3.1.2	filtered: 2.858E-06 unfiltered: 2.214E-04 (22.14 mrem)	
Instrument Line Break Pressure release phase (DN <10)	6.2.3.3	filtered: 5.183E-05 unfiltered: 5.782E-05 (5.782 mrem)	
Steam Generator Tube Rupture with response of the Pressure Relief System	6.2.5.2	filtered: 2.245E-06 unfiltered: 3.464E-05 (3.464 mrem)	
Helium Purification System Pipe Break release via stack	6.2.6.1	unfiltered: 1.975E-04 (19.75 mrem)	
Non-Design Basis Accidents			
Leakage of Vessel Containing Radioactive Contaminated Water	6.2.6.2	Unfiltered: 2.443E-06 (0.2443 mrem)	10CFR20
Seismic Effects on the Reactor Auxiliary Building	6.2.7	Unfiltered: 3.961E-04 (39.61 mrem)	

Notes:

- (1) The worst two hour window is used with an atmospheric dispersion factor (X/Q) value of 3.35E-03 s/m³ corresponding to an EAB distance of 0.249 miles (400 m).
- (2) The 0.25 Sv criterion is used for evaluating design basis accidents of exceedingly low occurrence probability and low risk of public exposure to radiation. The criterion for events of moderate frequency is 25% of the 0.25 Sv, or 0.063 Sv. The criterion for events of higher probability of occurrence, the acceptance criterion is 10% of the full limit, or 0.025 Sv

7. FUKUSHIMA LESSONS LEARNED

- Discussion of how the process and its implementation to the selected designs accounts for the Fukushima lessons learned (e.g., events impacting more than one reactor, spent fuel, power supplies, active systems, operator actions, etc.).

USA 2017 INL/EXT-17-43155 Appendix B

Appendix B – Summary Discussion: Addressing Fukushima Lessons Learned

This appendix provides a summary discussion of how the implementation of the proposed safety design process addresses the key lessons learned from the events at Fukushima.

A primary focus of the June 2017 Research Coordination Meeting was to compare and contrast the performance-based and risk-informed approach to safety design criteria development proposed by the United States (“Approach 1”) versus a more prescriptive and deterministic method, starting from historical light-water-reactor-based criteria (“Approach 2”) to develop a clear understanding of the strengths and weaknesses of each and, if possible, to propose a blended approach to development of mHTGR safety design criteria. “Approach 1” has been largely developed directly from the process flow utilized by the United States Department of Energy’s Next Generation Nuclear Plant Project for mHTGR designs, including insights from the related dialogue and reviews provided by the U.S. Nuclear Regulatory Commission.

“Approach 1” proposed by the U.S. is characterized by two key concepts that relate directly to more clearly understanding and addressing the lessons learned from the events at Fukushima. Those two concepts include: 1) the use of a risk-informed and performance-based process for identifying the spectrum of licensing basis events (LBEs) to be evaluated and addressed by the design; and 2) the use of a mechanistic source term (MST) approach when evaluating the potential radiological releases that may occur from those events. These two concepts are summarized below.

Identification and Evaluation of LBEs

LBEs are a comprehensive set of event sequences used in development of the license application that form the basis for plant analysis and represent the plant’s characteristic performance in all analyzed frequency and consequence ranges and modes of operation.

Approach 1 is a systematic, performance-based and risk-informed methodology for selecting and classifying LBEs for the mHTGR, consistent with current Nuclear Regulatory Commission policies and guidance on the application of deterministic design criteria and the use of probabilistic risk assessment (PRA) techniques. The methodology integrates the use of deterministic safety principles and PRA insights as critical inputs into the selection of LBEs. A combination of deterministic and probabilistic analysis is used to identify these events and evaluate the event sequences. The LBE selection process 1) identifies event sequence families based on an identified set of initiating events, 2) establishes the frequency of each of these event sequences, and 3) assesses the consequences of the event sequences against offsite dose criteria.

LBE selection is also an integral part of the overall design process. The design attributes of the plant influences the type and sequence of events of LBEs, and the initial set of identified LBEs

can be used to improve the final design. Once the initial set of LBEs is identified, the design can be refined to reduce the frequency or consequence of a given LBE. This suggests an iterative design process where more design and analysis detail is available at each phase of the design process, and includes the following development sequence:

1. A deterministic approach is used to select an initial event set providing a starting point for a given phase of the design process. For example, a set of initial events developed from conceptual design provides the starting point for preliminary design.
2. The LBEs are updated as the design and analysis progress. The PRA is developed and revised as the design matures. This begins to risk inform the LBE event sequences with insights gained from the design phase PRA.
3. A review of the LBEs is performed at the end of the design phase to evaluate conservatism in the selected events.

This approach uses a blend of deterministic and probabilistic techniques, where deterministic evaluations provide initial identification of events and subsequent confirmation of margins through the evaluation of DBAs, and probabilistic components provide a systematic process to ensure all sequences are captured and properly classified.

Approach to Establishing MSTs

The mechanistic approach to source term development is needed to establish the technical basis and take credit for the radionuclide retention capabilities of the multiple barriers to radionuclide transport consistent with the mHTGR safety design. For each LBE identified using the process described above, MSTs are developed that evaluate the realistic response of the plant to the initiating event. The initial radionuclide inventories during the modes of normal operation will include, as appropriate those in the fuel, the circulating activity, the plate-out activity within the helium pressure boundary, the spent and used fuel, and radioactive waste systems. For each of these inventories, the response to the initiating event of the barriers and that of the passive and active SSCs that protect those barriers are modeled.

Several factors need to be considered in a mechanistic definition of event-specific source terms for mHTGRs. As these factors are defined and characterized, the influence of each on the calculated dose is established. This permits developing a target for each element in the source term calculation to meet the safety goals of the project. The development of these targets is addressed by the following process:

1. Establish the top level radionuclide control requirements to ensure the health and safety of the public and plant workers and to protect the environment.
2. Identify LBEs for which plant conditions and source terms are to be calculated and compared with the goals.
3. Identify and characterize the factors affecting radionuclide generation and transport for this reactor technology.
4. Scope the influence of each factor on the magnitude of the source terms and establish the principal parameters needed to characterize the effect of these factors on the generation and transport of radionuclides for the LBEs.
5. Establish a target for each factor to achieve the goal for each event.

6. Calculate source terms and dose rates based on the current understanding of generation and transport phenomena for the LBEs and compare with top level regulatory criteria (TLRC) requirements.
7. As needed to support meeting the TLRC requirements, identify how well each factor is currently characterized to validate its target in establishing the source terms and, where the current characterization is deficient, define the gaps between what is needed and what is known.
8. Develop and complete analytic and testing programs to fill those gaps, if needed.
9. Recalculate source terms and dose rates again based on the more fully characterized and validated generation and transport phenomena for the LBEs and compare with TLRC requirements.

This MST approach analyzes a mHTGR functional containment comprising several barriers that limit the release of radionuclides to the environment for each postulated event, including normal operating conditions, abnormal operating conditions and accident conditions. The multiple barriers include:

- Individual fuel particle kernels and coatings,
- The fuel matrix and fuel element graphite,
- The helium pressure boundary (primary circuit), and
- A vented low-pressure reactor building.

Design methods for determining radionuclide source terms, which include analytical tools used to calculate the performance of each of these barriers during radionuclide transport under event-specific conditions, are defined and supported by testing and analysis. These analytical tools are applied in calculations for normal operating conditions, abnormal operating conditions, design-basis accident conditions, and beyond-design-basis-accident conditions.

Summary of How Approach 1 addresses some of the more critical causes of the events at Fukushima Daiichi

1. Events impacting more than one reactor on a multi-reactor site

Proposed Approach 1 systematically evaluates all identified event sequences and event sequence families on a “per plant-year” basis. This means that all reactor units on a plant site are evaluated both individually, and in combination, for event sequences that may apply to multiple reactors simultaneously. This assures that the overall impact of the plant facility is evaluated and considered, rather than evaluating impacts to the public based on single reactor units only, as was the case at Fukushima Daiichi.

2. Interdependence of radionuclide release barriers

The developers of mHTGRs typically design and configure the various release barriers to be largely independent. Approach 1’s source term approach, combined with the LBE determination process, provides a tool for evaluation of those design choices with any related interdependencies, so that the adequacy of release barrier configurations can be confirmed, including considerations of defense-in-depth.

3. Reliance on active systems and operator actions

The mHTGRs being addressed by the safety design criteria under development within this Cooperative Research Project typically use the inherent high-temperature characteristics of tristructural-isotropic-coated fuel particles, graphite moderator, and helium coolant, as well as passive heat removal from a low-power density core with a relatively large height-to-diameter ratio within an uninsulated steel reactor vessel. These mHTGRs are designed in such a way to ensure during design-basis events (including loss of forced cooling or loss of helium pressure conditions) that radionuclides are retained at their source in the fuel. They generally do not rely on either active safety systems or operator actions to achieve these capabilities. However, this aspect of a particular design is evaluated and confirmed through the Approach 1 process.

4. Adequate cooling of spent fuel

Adequacy of spent fuel cooling, as well as all other critical cooling functions of any given mHTGR concept, are directly addressed through the event evaluation process summarized above. This includes a review of available heat removal systems and configurations to assure margins and capabilities.

Europe/ Wenra reports ½ page (Ewa and Gerd – 1 Aug)

Fukushima Lessons Europe/WENRA Reports

One of the objectives of the Western European Nuclear Regulators' Association (WENRA), as stated in its terms of reference, is to develop a harmonized approach to nuclear safety and radiation protection and their regulation. A significant contribution to this objective was the publication, in 2006, of a report on harmonization of reactor safety in WENRA countries. This report addresses the nuclear power plants (NPPs) that were in operation at that time in those countries.

Since then, the construction of new nuclear power plants has begun or is being envisaged in several European countries. Hence, it was considered timely for WENRA to develop the safety objectives for new nuclear power plants. A report "Safety objectives for new power reactors – study by RHWG – December 2009" and "WENRA statement on safety objectives for new nuclear power plants – November 2010" have been published by WENRA (www.wenra.org). The statement includes seven safety objectives, which are the basis for further harmonization work of WENRA. Based on these safety objectives, WENRA decided to develop common positions on selected key safety issues for the design of new nuclear power plants.

The work was initiated and also a major part of the work was carried out before the TEPCO Fukushima Daiichi accident. Therefore, the report discusses also some considerations based on the major lessons from the Fukushima Daiichi accident, especially concerning the design of new nuclear power plants, and how they are covered in the new reactor safety objectives and the common positions.

The WENRA safety objectives for new nuclear power plants were developed on the basis of a systematic review of the Fundamental Safety Principles (SF-1 document issued 2006 by the IAEA). Grounding the safety objectives on the fundamental safety principles has been explained in the December 2009 study by the RHWG. The WENRA Objectives cover the following areas:

- Normal operation, abnormal events and prevention of accidents

- Accidents without core melt
- Accidents with core melt
- Independence between all levels of Defence-in-Depth
- Safety and security interfaces
- Radiation protection and waste management
- Leadership and management for safety

The safety objectives address new civil nuclear power plant projects. However, these objectives should also be used as a reference to help identify reasonably practicable safety improvements for “deferred plants” and existing plants during Periodic Safety Reviews.

The safety objectives are formulated in a qualitative manner to drive design enhancements for new plants with the aim of obtaining a higher safety level than that expected from existing plants. The WENRA safety objectives call for an extension of the safety demonstration for new plants, consistent with reinforcement of Defence-in-Depth. Some situations that are considered as “beyond design” for existing plants, such as multiple failures conditions and core melt accidents, are taken into account in the design of new plants.

WENRA considers that these safety objectives reflect the current state of the art in nuclear safety and can be implemented at the design stage using the latest available industrial technology of nuclear power plants

8. KEY R&D CONSIDERATIONS (IDENTIFICATION OF ANY RESEARCH AND DEVELOPMENT GAPS)

8.1. IDENTIFICATION OF SIGNIFICANT RESEARCH & DEVELOPMENT GAPS AND ANALYSIS METHOD VERIFICATION AND VALIDATION NEEDS

8.1.1. United States of America

- [INL/EXT-17-43155 Appendix C](#)

The key research and development related activities that need to be considered and addressed in support of defining and confirming the safety case for the modular high-temperature gas-cool reactor were previously evaluated and reflected in a U.S. Department of Energy-sponsored activity within the Advanced Reactor Technology Program. PLN-4910, “ART Program Regulatory Technology Development Plan,” was originally issued in 2015. It is currently undergoing revision, which will be issued in the very near term. PLN-4910 should be referenced for a more comprehensive description of significant and higher priority research and development gaps or verification and validation needs, although the needs in those areas are briefly summarized below.

- **Fuel Qualification and Mechanistic Source Term**
 - Establish fuel service conditions and performance requirements for normal and off-normal operations
 - Demonstrate fuel performance requirements are met at normal operating conditions using irradiated fuel at design conditions, fuel irradiation performance monitoring, and post-irradiation examinations
 - Demonstrate fuel performance requirements are met for accident conditions using irradiated fuel at accident conditions and monitored fuel accident performance
 - Establish and validate models for fuel performance and radionuclide transport in fuel
 - Develop fuel product and fuel fabrication process specifications
 - Develop event-specific mechanistic source terms based on fuel test program results
 - Establish and validate models for radionuclide transport to the environment
 - Demonstrate mechanistic source term models in best estimate and conservative analyses of transients and accidents.
- **Core Heat Removal**
 - Confirm reactor core heat removal capabilities.
- **Materials Analysis**
 - Irradiation and property testing of advanced reactor materials and application development
 - Development of material codes and standards.
- **Analytical Codes and Methods**
 - Define calculational envelope required to analyze reactor systems
 - Define evaluation models capable of an analysis across the calculational envelope defined by the above

- Identify data or perform thermal fluid experiments to generate comprehensive database for validating design safety evaluation models.

8.1.2. Japan

- Japan to submit Dec 2018

The topics of key research and development related to the safety requirements for the modular HTGR, and current status mainly in Japan are described as follows.

(1) Confinement of radioactive materials

Confinement performance of coated fuel particle for radioactive materials in postulated operational state and accident conditions should be demonstrate by the irradiation test and post irradiated examination. There are many activities in the world in the past and at present. JAEA developed the HTTR fuel for 33 GWd/t and is currently developing the high-burnup UO₂ fuel for about 100 GWd/t [1]. The final target of the high-burnup fuel in Japanese design is about 160 GWd/t. Quality assurance program for the fabrication of coated fuel particle is very important items. It was already established during the HTTR fuel development.

The modeling for the evaluation of fuel failure mechanism and fission product transport behavior from the coated fuel particle to atmosphere should be developed. JAEA developed the numerical models and tools to estimate the fuel failure and fission product behavior for the HTTR licensing. The upgrade of the models to reduce the uncertainty and conservativeness are one of R&D items for the deployment of the modular HTGR.

(2) Reactor shutdown

The proposal to the safety requirements for the modular HTGR related to the reactor shutdown is the shutdown by inherent characteristics instead of a shutdown system. The reactor shutdown by relatively large negative Doppler temperature coefficient without the control rod insertion at 30% of full power was demonstrated by the safety demonstration test using HTTR [2]. This characteristic has also demonstrated by other HTGRs such as AVR and HTR-10.

The numerical tool to simulate the reactor behavior including reactivity and temperature transients has being validated using the HTTR data. The loss of force cooling test without the reactor scram by control rod during full power operation is planned. It is expected to provide additional evidence of the shutdown by inherent characteristics and experimental data for code validation.

(3) Heat removal from the core

The proposal related to the heat removal from the core in the safety requirement is heat removal from outside of the reactor pressure vessel. The core heat removal from outside the reactor pressure vessel during loss of forced cooling was demonstrated by the safety demonstration test using HTTR [2]. If passive cooling from outside of the reactor pressure vessel by either air or water is applied to the core heat removal, it is desirable to demonstrate the capability of passive cooling and validate a simulation tool.

(4) Safety case

Though there is a consensus that no core meltdown is postulated in the modular HTGR, there is argument about the necessity of the consideration of the plant state corresponding to the core

melt in LWR (i.e., DEC-B) such as significant fuel damage or core degradation in the design of the modular HTGR. It is very important to show the practical elimination of the significant fuel damage or core degradation.

(5) Safety analysis

The numerical models and tools for the safety analysis have been developed in the several countries and some of them were used for the licensing of HTGRs. The upgrade of the models to reduce the uncertainty and conservativeness are desired. The probabilistic safety assessment (PRA) method not only the internal events but also the internal and external hazards should be developed to provide the risk information for design, licensing, maintenance, etc.

(6) Code and standards for material

If new material is applied to the modular HTGR design, material property data non-irradiated and irradiated conditions should be obtained, and material codes and standards should be established.

(7) Coupling of high temperature heat application facility

The safety requirements related to the coupling a high temperature heat application facility with the nuclear reactor and the certification of the heat application facility as a non-nuclear facility should be demonstrated by a licensing process of a regulatory body. The HTTR-GT/H2 test facility [3], HTTR coupled with high temperature heat application facilities such as helium gas turbine and hydrogen production systems, is candidate for the licensing demonstration.

(8) Other topics related to the modular HTGR safety

Though it is out of scope of the safety design requirements, the method to determine the size of emergency planning zone for modular HTGR taking into account the safety feature of the modular HTGR is one of key R&D issues and closely related to the safety case of the modular HTGR.

References

- [1] S. Ueta, et al., Research and Development on High Burnup HTGR Fuels in JAEA, Proc. ICONE27, May 19-24, 2019, Tsukuba, ICONE27-2138 (2019).
- [2] K. Takamatsu, et al., Experiments and validation analyses of HTTR on loss of forced cooling under 30% reactor power, J. Nucl. Sci. Technol., Vol.51, No.11-12, pp.1427-1443 (2014).
- [3] X. Yan, et al., Design of HTTR-GT/H2 test plant, Nuclear Engineering and Design, Vol. 329, pp. 223-233 (2018).

8.2. TEST FACILITIES NEEDED FOR THE HTR-PM

- China (Test facilities needed for HTR-PM)

The design of HTR-PM began in 2001, based on the technology of HTR-10. For HTR-PM, several test facilities were built since 2009. The list of the test facilities can be found in Table 22. All test facilities, except for the TF-PBF3D (see Table 22), are finished already. Most of the facilities were built to show the operation performance of key components and system in full scale, in order to make sure that all components will work as expected in HTR-PM. These systems and components include the steam generator, the helium circulator, the control rod driving mechanism, the small absorber sphere system, the fuel handling system, the spent fuel storage system, the helium purification system, the distributed control system, the main control room, etc. Because size and capability of these systems and components are first of one kind,

the designer built the test facility again to test them in full scale, based on the support from the central government in the framework of national key science and technology project. Even though, this type of system and components were already used in HTR-10. Naturally, some of the test facilities are surveyed by NNSA as one of qualification process of safety related components and systems. Some of them can provide more data for the safety analysis; for example, the measurement of pebble flow and pebble bed equivalent conductivity coefficient. Based on the result of these facilities, hope is that no big test facilities in engineering scale are needed for near term deployment of HTR-PM and HTR-PM600; unless some key components are changed or improved, the outlet temperature is significantly increased, process heat application is connected, or gas turbine or hydrogen production facility is connected, or some new design or concepts are adopted. New facilities for new technology, new concepts, future applications will be proposed.

TABLE 22. LIST OF TEST FACILITIES BUILT TO DEMONSTRATE THE OPERATION PERFORMANCE OF KEY COMPONENTS AND SYSTEM OF THE HTR-PM.

<i>Abbreviation of the facility</i>	<i>Name of the facility</i>	<i>Key parameters</i>	<i>Function of the facility</i>
<i>ETF-HT</i>	<i>Engineering Test Facility- Helium Technology</i>	<i>10MWt test power, 7.0MPa, 250-750°C, helium</i>	<i>Heat source to verify steam generator</i>
<i>ETF-SG</i>	<i>Engineering Test Facility- Steam generator</i>	<i>10MWt test power, 13.25MPa, 205-570°C, water</i>	<i>Secondary loop and third loop to verify steam generator</i>
<i>ETF-HC</i>	<i>Engineering Test Facility- Helium Circulator</i>	<i>4.5MWe, 7.0MPa, 250°C, helium</i>	<i>Full scale verification of helium circulator</i>
<i>ETH-FHS</i>	<i>Engineering Test Facility- Fuel Handling System</i>	<i>7.0Mpa, 100-250 °C, helium, two chain</i>	<i>Full scale verification of fuel handling system</i>
<i>TH-FHS</i>	<i>Test Facility- Fuel Handling System</i>	<i>Full geometry size, air, 0.1MPa</i>	<i>Verification of the fuel movement in the FHS system</i>
<i>ETF-CRDM</i>	<i>Engineering Test Facility- Control Rods Driving Mechanism</i>	<i>1MPa, 100-250°C, helium</i>	<i>Full scale verification of Control Rods Driving Mechanism</i>
<i>ETF-SAS</i>	<i>Engineering Test Facility- Small Absorber Sphere System</i>	<i>7.0MPa, 100-250°C, helium</i>	<i>Full scale verification of small absorber sphere system</i>
<i>ETF-SFS</i>	<i>Engineering Test Facility- Spent Fuel System</i>	<i>Full geometry size, air, 0.1 MPa</i>	<i>Full scale verification of major components of spent fuel storage system</i>

<i>TF-SFCD</i>	<i>Test Facility- Spent Fuel Canister Drop</i>	<i>Full geometry size, Full height (30m), Full weight (17t)</i>	<i>Full scale drop verification of spent fuel canister</i>
<i>ETF-HPS</i>	<i>Engineering Test Facility- Helium Purification System</i>	<i>7.0MPa, 25-250°C, helium Purification flow rate: 40kg/h</i>	<i>Verification of purification efficiency (greater than 95% and system resistance less than 200kPa).</i>
<i>TF-PBEC</i>	<i>Test Facility- Pebble Bed Equivalent Conductivity</i>	<i>1600°C, helium/vacuum</i>	<i>Measurement of pebble bed equivalent conductivity</i>
<i>TF-PBF3D</i>	<i>Test Facility- Pebble Bed Flow 3D</i>	<i>0.1 MPa, room temperature, air</i>	<i>Three-dimensional simulation test for pebble bed flow (1:5 scale)</i>
<i>TF-HGM</i>	<i>Test Facility- Hot Gas Mixing</i>	<i>atm, 20-150°C, air</i>	<i>Reduced scale (1:2.5) verification of hot gas mixing at reactor core outlet</i>
<i>ETF-DCS</i>	<i>Engineering Test Facility- Distributed Control System</i>	<i>Reactor power control system, fuel cycle control system, VDU-based Man-Machine Interface</i>	<i>verification of DCS architecture and major control Systems</i>
<i>ETF-RPS</i>	<i>Engineering Test Facility- Reactor Protection System</i>	<i>Prototype of Reactor Protect System with 4 channels</i>	<i>Full scale verification of Reactor Protect System</i>
<i>ETF-MCR</i>	<i>Engineering Test Facility- Main Control Room</i>	<i>1:1 MCR control consoles, mimic panels, layouts and inner environments</i>	<i>Full scale verification of Man-Machine Interface</i>

8.3. EUROPEAN FRAMEWORK HTR PROGRAMS

- European R&D over the last years

HTR development in Europe started a long time ago before the European HTR programs. In parallel to the American efforts, at the same time, there was the Dragon project (UK)(1960-1970), a gas-cooled reactor development, with coated fuel particle and graphite characterization development. As well as the HTR development program Germany (1970-1990) implying TRISO fuel development, HTR pebble qualification, graphite qualification, AVR, THTR and HTR-MODULE.

The European projects (see Figure 44) started in the year 2000 with several programs (HTR-L, etc.) to restore the HTR knowledge. Later on, in 2005, the main program RAPHAEL (reactor for process heat, hydrogen and electricity generation) was initiated to provide R&D results for:

- Consolidating generic HTR/VHTR technologies
- Exploring advanced solutions for improving HTR performances (higher temperature > 900°C, higher fuel burn-up up to 15% FIMA, improved competitiveness, extending the domains of application (electricity → cogeneration of heat and electricity))
- Development of components for heat applications (IHX, blowers)

- Materials for very high temperatures
- Fuel (post irradiation examination and heat-up tests of irradiated fuel, development of fabrication processes for an alternative kernel composition (UCO) and an alternative coating layer (ZrC), development of fission product release modelling and statistical methods)

Then, project EUROPAIRS has been initiated to connect the HTR plants to possible end-users, while later on, the ARCHER program was built to continue the RAPHAEL program, subdivided in:

- System Integration (coupled system specification, primary system code integration)
- Safety Aspects (air ingress, water ingress, source term analysis chain, thermal safety issues, integrity concept of the helium pressure boundary)
- Fuel & Fuel Cycle (fuel basic properties, integral fuel element irradiation performance and safety testing, HTR fuel back end)
- Materials & Components (graphite, high temperature alloys and instrumentation, intermediate heat exchanger)

In 2013, the objective of NC2I-R was to structure the European public and private R&D capabilities for delivering a nuclear cogeneration demonstrator fully meeting the market needs, in support of the Nuclear Cogeneration European Industrial Initiative. Following the reference EUROPAIRS project and in close collaboration with the ongoing ARCHER project, national projects (e.g. Polish HTRPL, German SYNKOPE), non-EU HTR programs (US, China, South Korea, South Africa) and Generation IV International Forum, NC2I-R contributed to

- Structure the European public and private R&D capacities towards nuclear cogeneration
- Define the safety requirements to prepare for the future licensing process for a cogeneration demonstrator and limit the associated risk
- Define specifications for the demonstrator, ensuring its economic viability, its market fit, its future replicability and its safety, in particular of the coupling scheme, and limiting all construction project risks
- Managing the knowledge from past projects on HTR and nuclear cogeneration with a comprehensive experience feedback in order to identify potential points of attention and success factors
- Prepare for and organise the cooperation with non-European similar programmes to possibly share the demonstrator risk in line with the European interest.

The ongoing GEMINI+ project will provide a conceptual design for a high temperature nuclear cogeneration system for supply of process steam to industry, a framework for the licensing of such system and a business plan for a full-scale demonstration.

The objective is to further develop the safety approach for HTGR for nuclear cogeneration on the basis of the RAPHAEL, ARCHER and NC2I-R results, taking into account the lessons learned from the Fukushima accident and incorporating the requirements of the amended Euratom Safety Directive.

In this context, it shall contribute to a methodology for definition of severe accidents to be considered in a licensing process and shall evaluate existing European licensing frameworks with regard to potential licensing impediments specific for HTGR safety design solutions.

Furthermore, safety options developed by designers shall be reviewed from a TSO perspective and the safety features of a reference reactor proposed shall be established by safety related thermal hydraulic calculations and estimates of accidental fission product releases from the fuel.

European framework HTR programs

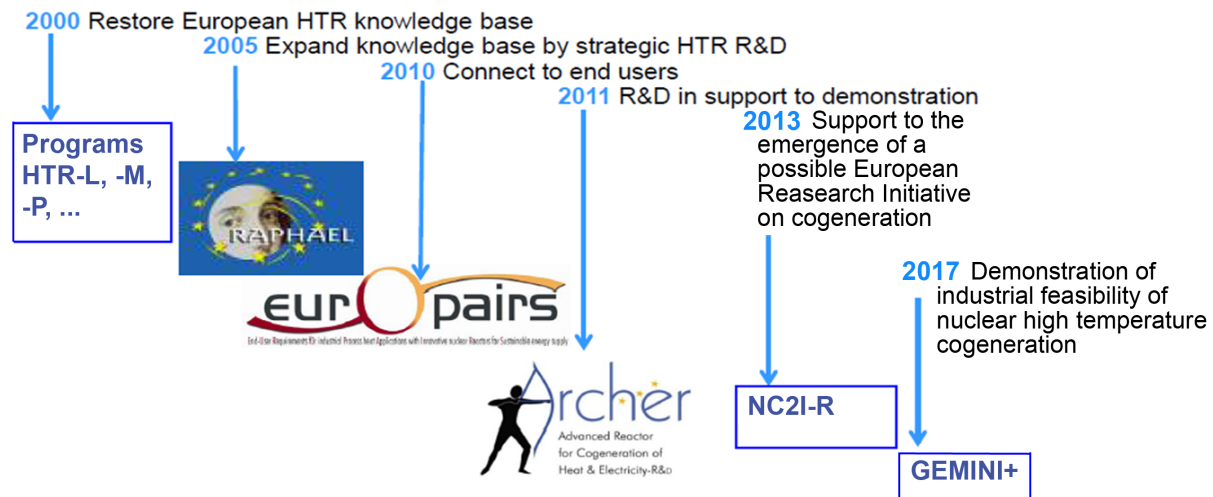


FIG. 44. European framework HTR R&D programs.

8.4. GENERATION IV INTERNATIONAL FORUM VHTR PROJECT FUTURE DEPLOYMENT

- GIF V-HTR project (reference research gap report) – future deployment.

The VHTR is the next generation in the development of high-temperature reactors and is primarily dedicated to the cogeneration of electricity, hydrogen, and process heat for industry. VHTR can supply nuclear heat and electricity over a range of core outlet temperatures between 700°C to 950°C, and potentially more than 1 000°C in the future.

In January 2014, Gen IV International Forum (GIF) issued “Technology Roadmap Update for Generation IV Nuclear Energy Systems”. This document pointed out that, in the near term, the R&D work for VHTR system within GIF should focus on the needs of lower outlet temperature (from 700 to 950°C) demonstration projects, especially with co-generation capability, future operation at higher outlet temperatures (up to above 1 000°C) requires development of high temperature alloys, qualification of new graphite type and development of composite ceramic materials. Also, improvement and validation of computational fluid dynamics and system models through theoretical and experimental benchmarks would be needed.

In more detail, the R&D outlook for VHTR include: design and system integration in support to demonstration projects, coupling with process heat end-users, design, manufacturing, qualification of several types of specific components for demonstration (e.g. safety instrumentation, heat exchanger, ducts, valves and associated heat transfer fluids), demonstration of passive safety and other licensing-relevant tests, waste minimization (e.g. graphite decontamination and recycling, fuel waste reduction, symbiotic fuel cycles), computer tools, codes and standards as engineering design tools and for licensing, R&D with the specific target of cost reduction.

More specifically, the R&D inside VHTR system are divided into 4 project management boards (PMBs): Material (MAT), Fuel and Fuel Cycle (FFC), Hydrogen Production (HP), Computational Methods Validation and Benchmarks (CMVB).

The MAT project bundles the efforts to develop, screen and qualify the materials required for a VHTR and its ancillary equipment including components such as pipework, gas circulators, heat exchangers, valves, graphite moderators or control rods. This encompasses graphite, advanced nickel-base alloys and ferritic-martensitic steels of the 9% Cr class, as well as composite ceramics.

In FFC project, cooperative work on TRISO fuel includes sharing irradiation experiments, characterization methods and facilities as well as the determination of materials properties. Advanced fuel particles such as UCO fuel and ZrC (instead of SiC) coated particles are also investigated. This includes several steps: Pre-irradiation characterization, irradiation testing, safety testing, code development.

For HP project, while process steam generation was rather recently identified as a large market opportunity for VHTR in the nearer term, the longer term objective and initial driver towards reactor outlet temperatures of the VHTR in the vicinity of 1000 °C was the thermo-chemical iodine-sulfur process for efficient large-scale hydrogen production, which involves a process step at 850 °C. Cooperation within GIF contributed to share the realization and results of laboratory scale experiments on the Sulfur-Iodine (S-I) and high-temperature steam electrolysis (HTSE) processes, to advance the development of catalysts and to share results of technical and economic assessments of several processes. Beyond experimental testing, significant analytical capabilities/methods were developed that can be used to evaluate hydrogen production in combination with a VHTR plant.

CMVB PMB focuses on ensuring the numerical models used for reactor system analysis are capable of calculating the reactor system behavior at normal operational conditions and for operational transients and accident scenarios. In CMVB project, collaborative research is done in area of:

- 1) Phenomena Identification and Ranking Table (PIRT) Comparison, Evaluation, and Update,
- 2) Computational fluid dynamics (CFD),
- 3) Reactor core physics and nuclear data,
- 4) Chemistry and transport,
- 5) Reactor and plant dynamics.

References:

1. Generation IV International Forum, Technology Roadmap Update for Generation IV Nuclear Energy Systems. Jan 2014
2. M. Fuetterer, et. al. Status of the very high temperature reactor system, Progress in Nuclear Energy. 77 (2014) 266-281

- OECD-NEA (new initiative)

9. SUMMARY AND CONCLUSIONS

9.1. SUMMARY

9.2. CONCLUSIONS

10. APPENDICES

APPENDIX I. OBJECTIVE PROVISIONS TREE ANALYSIS FROM APPROACH 2

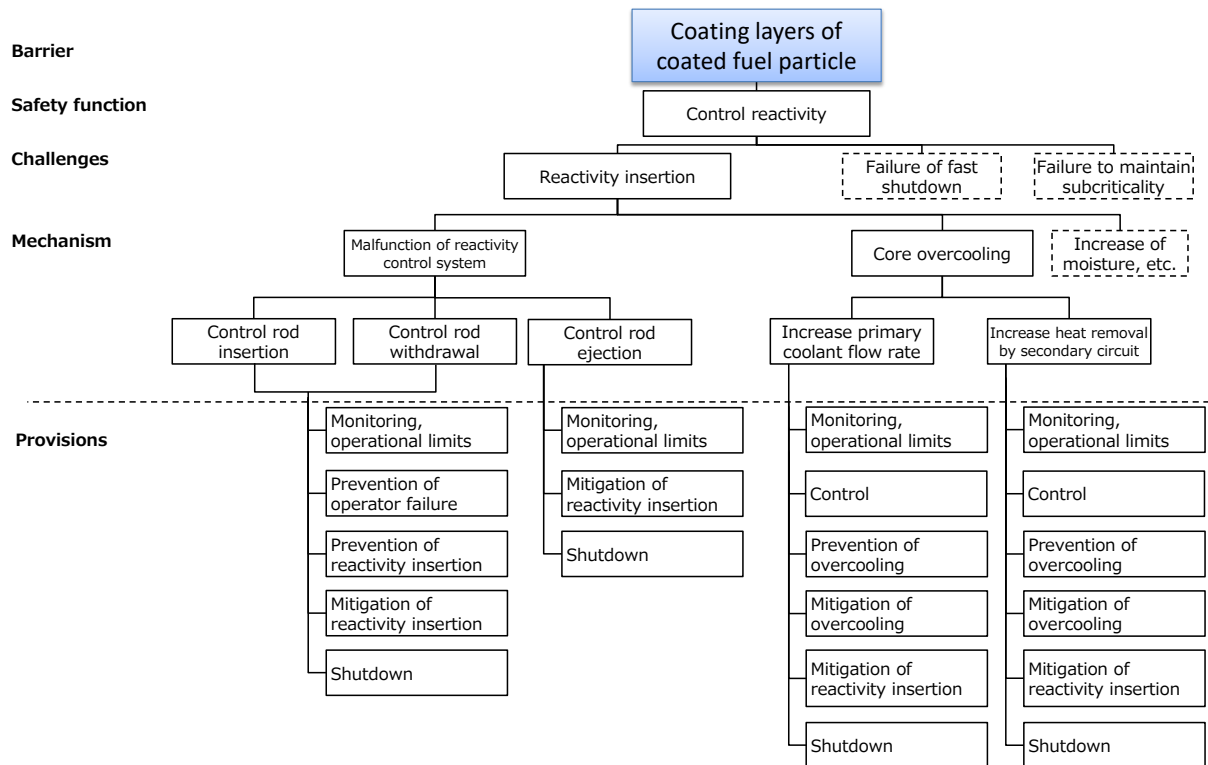


FIG. I.1. Objectives provisions tree analysis result for the coating layer of the coated fuel particle (1/11).

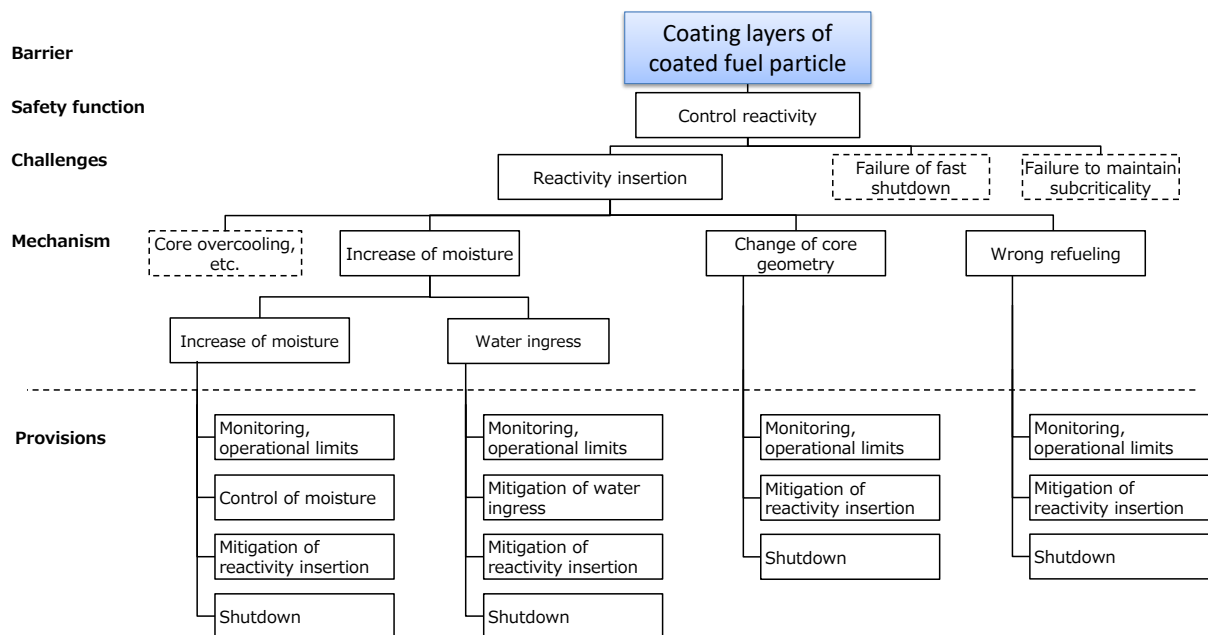


FIG. I.2. Objectives provisions tree analysis result for the coating layer of the coated fuel particle (2/11).

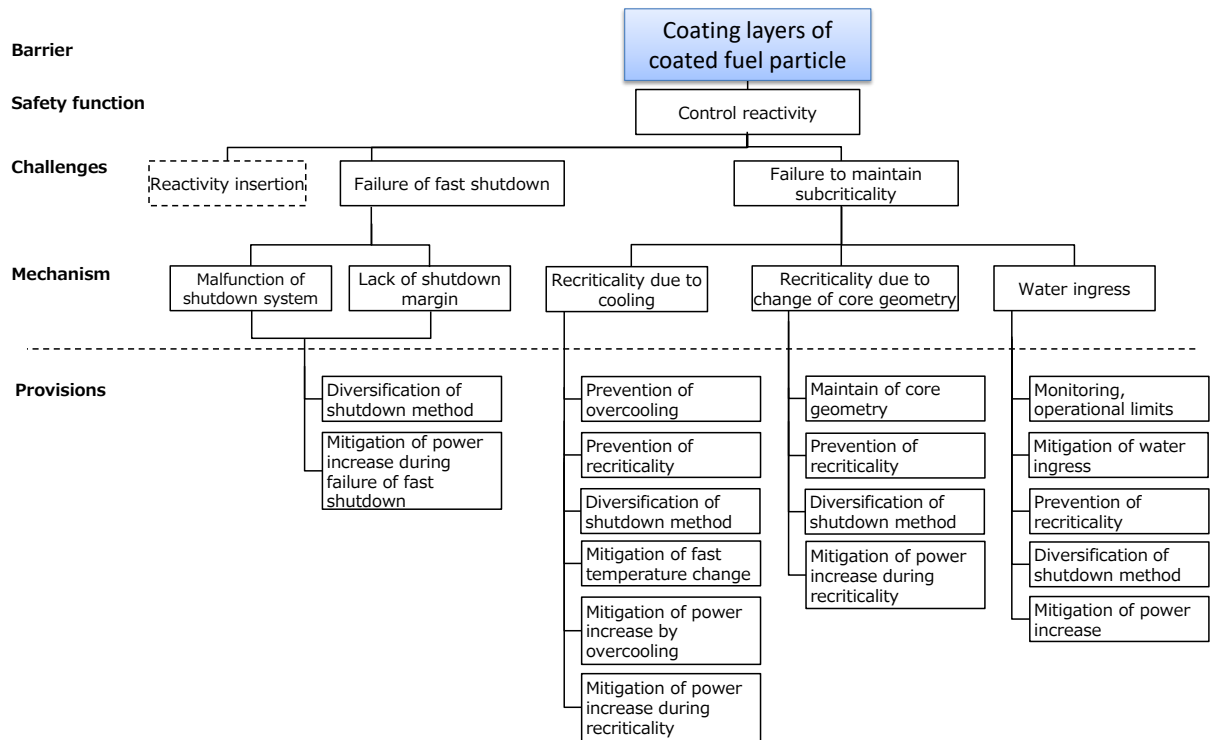


FIG. I.3. Objectives provisions tree analysis result for the coating layer of the coated fuel particle (3/11).

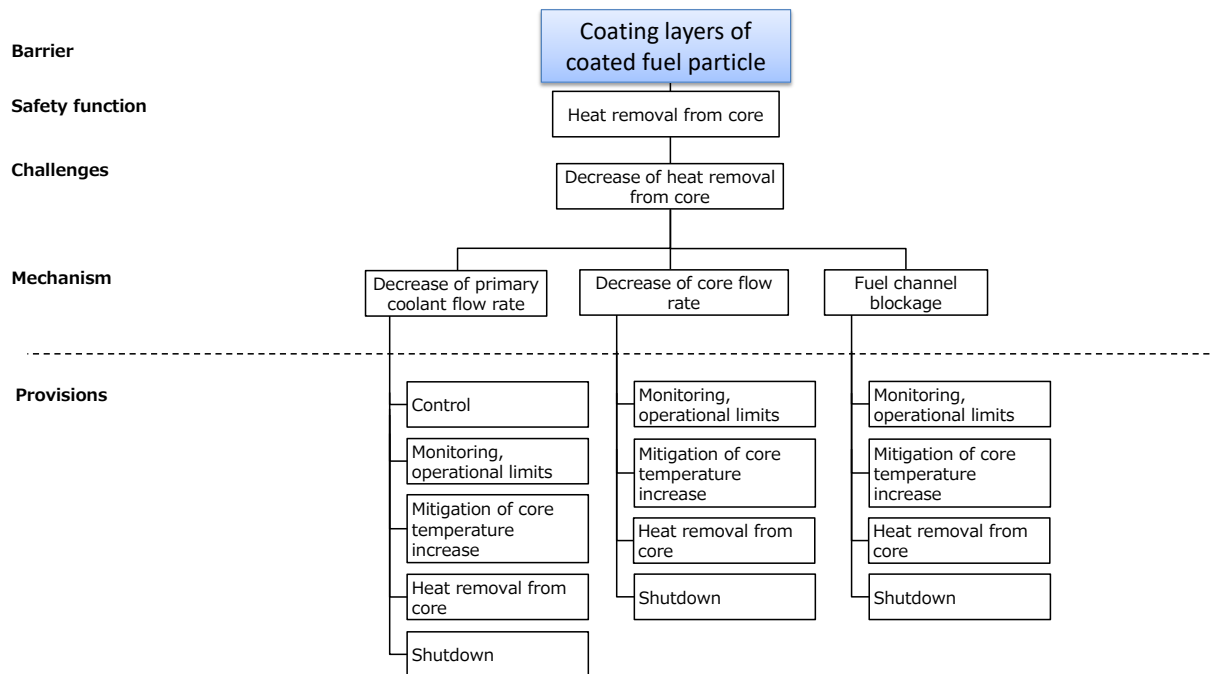


FIG. I.4. Objectives provisions tree analysis result for the coating layer of the coated fuel particle (4/11).

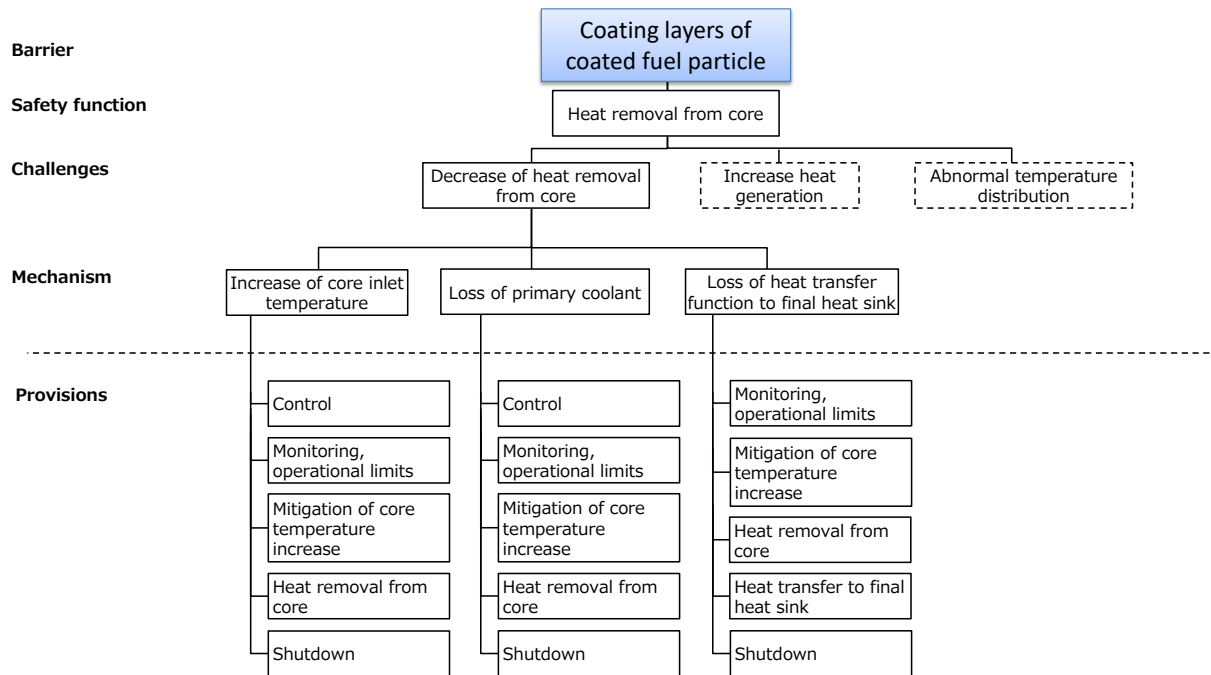


FIG. I.5. Objectives provisions tree analysis result for the coating layer of the coated fuel particle (5/11).

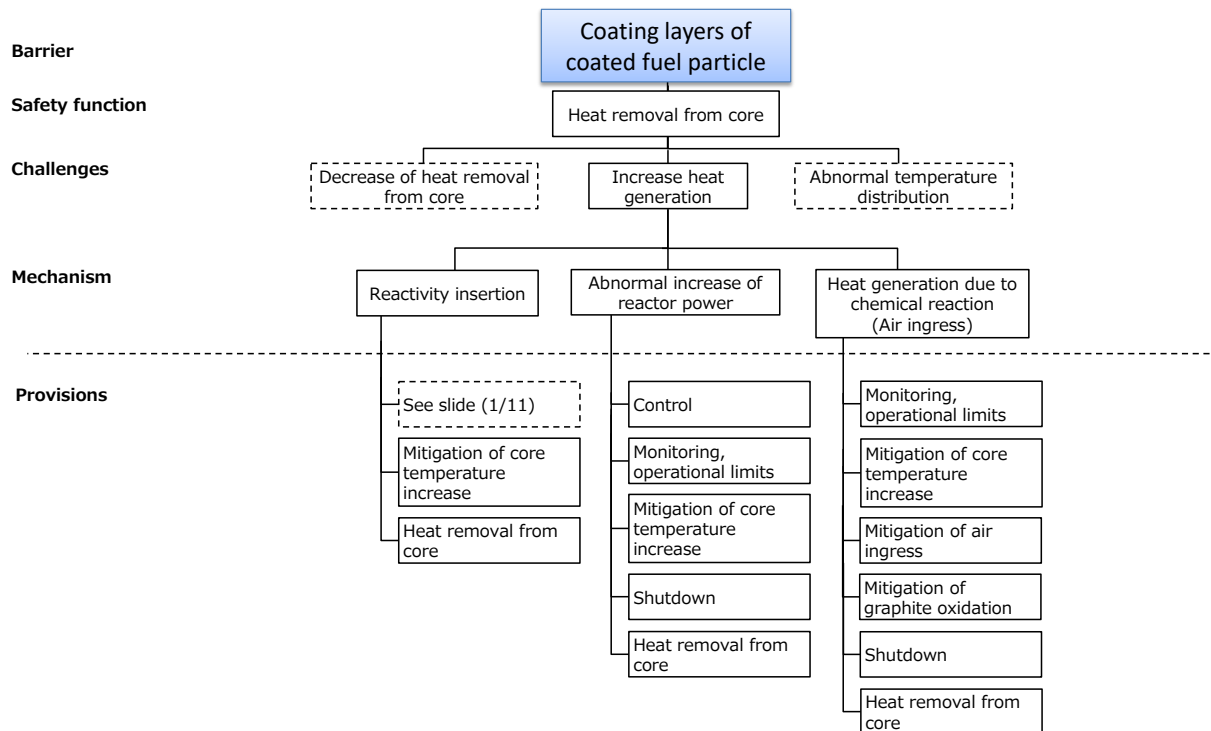


FIG. I.6. Objectives provisions tree analysis result for the coating layer of the coated fuel particle (6/11).

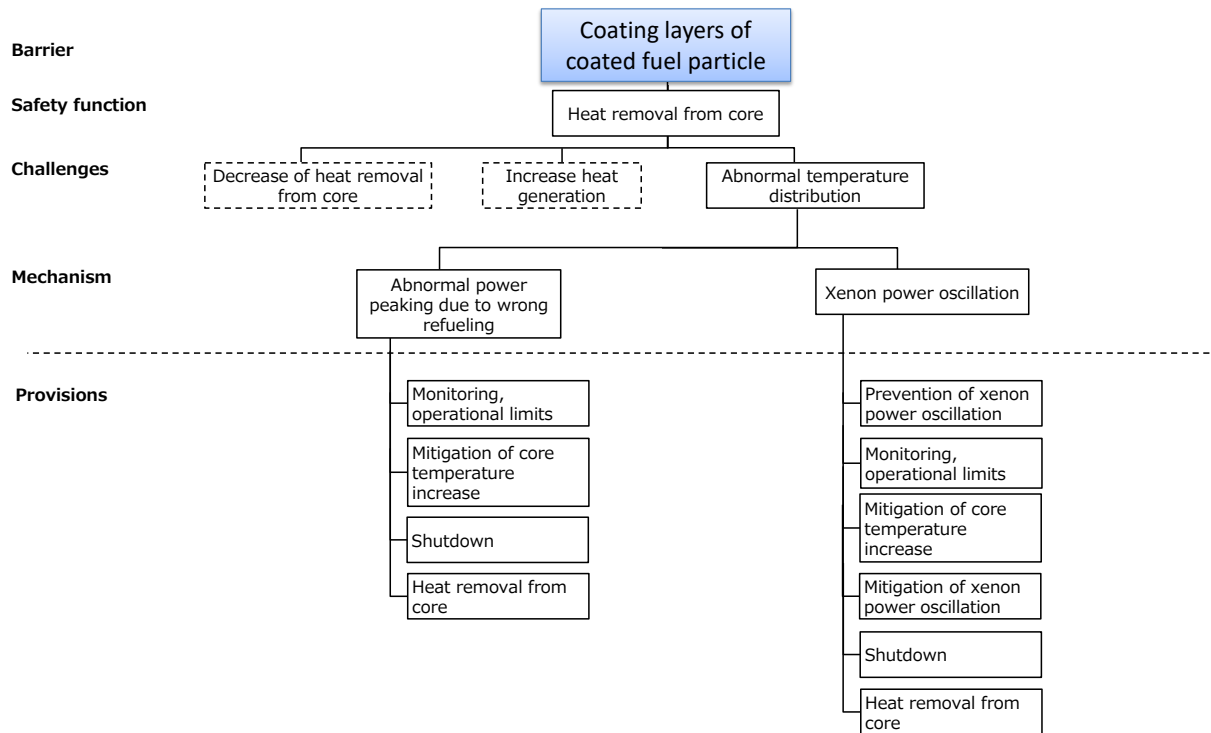


FIG. I.7. Objectives provisions tree analysis result for the coating layer of the coated fuel particle (7/11).

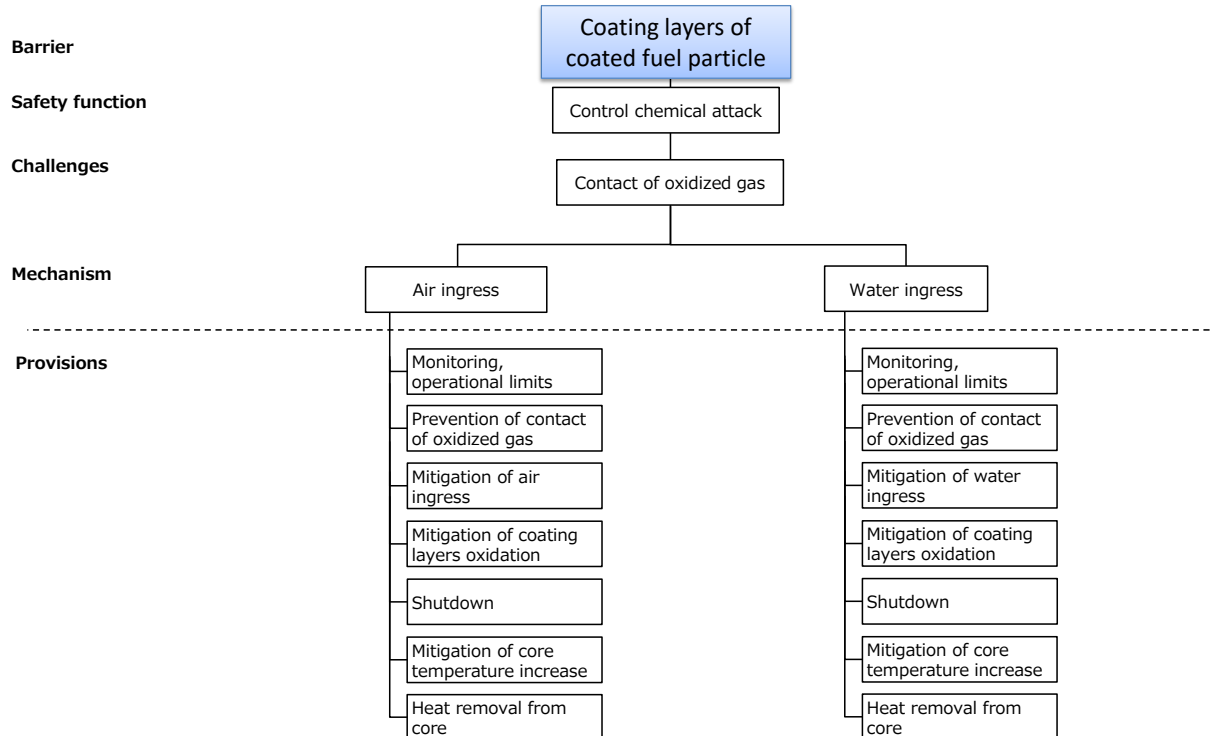


FIG. I.8. Objectives provisions tree analysis result for the coating layer of the coated fuel particle (8/11).

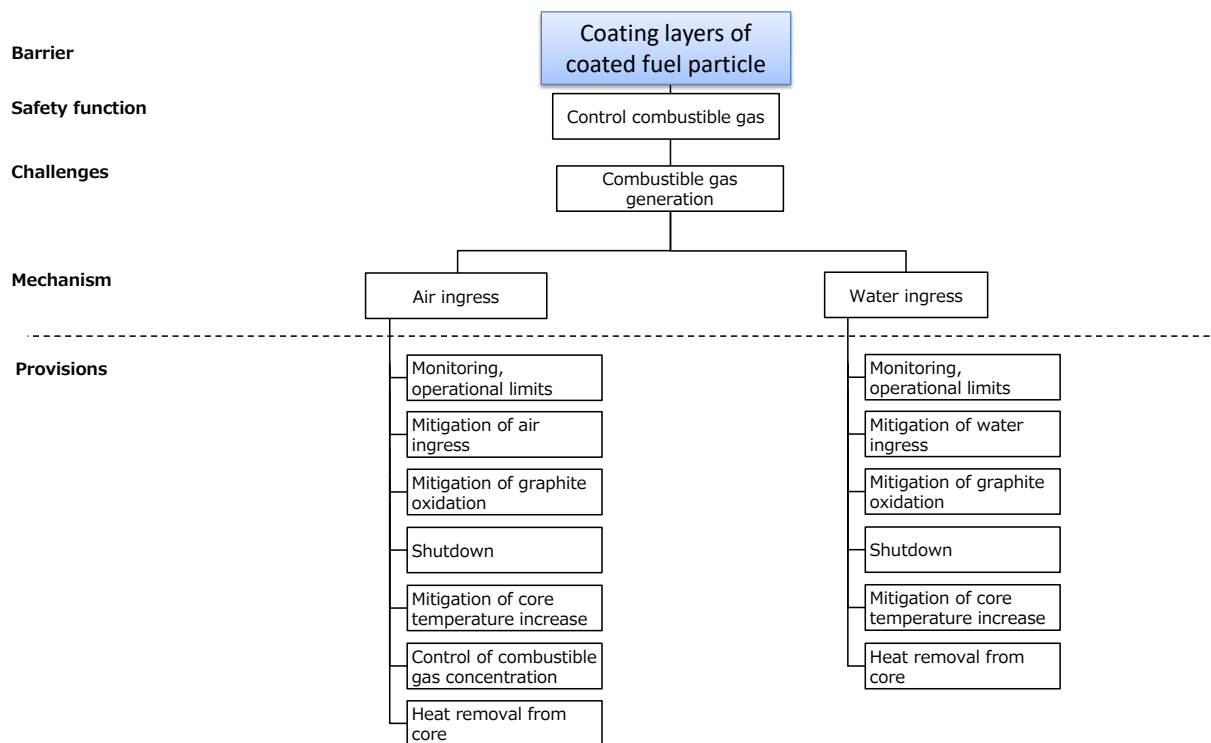


FIG. I.9. Objectives provisions tree analysis result for the coating layer of the coated fuel particle (9/11).

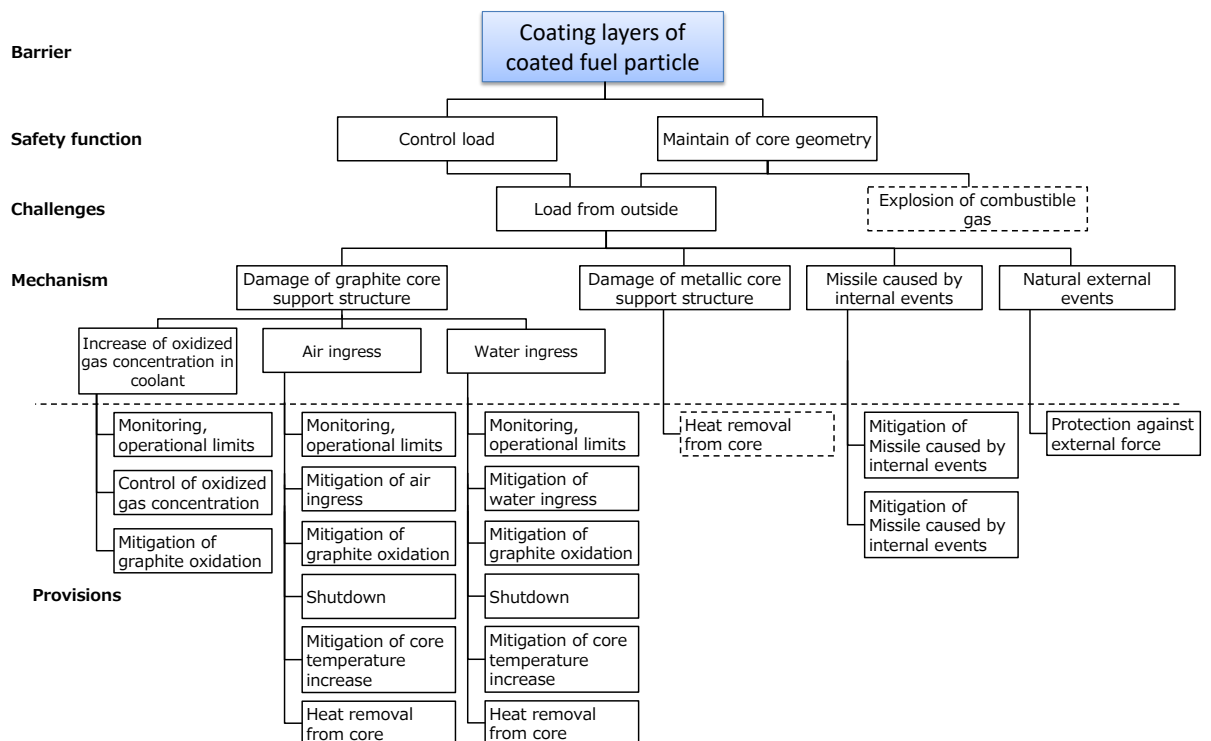


FIG. I.10. Objectives provisions tree analysis result for the coating layer of the coated fuel particle (10/11).

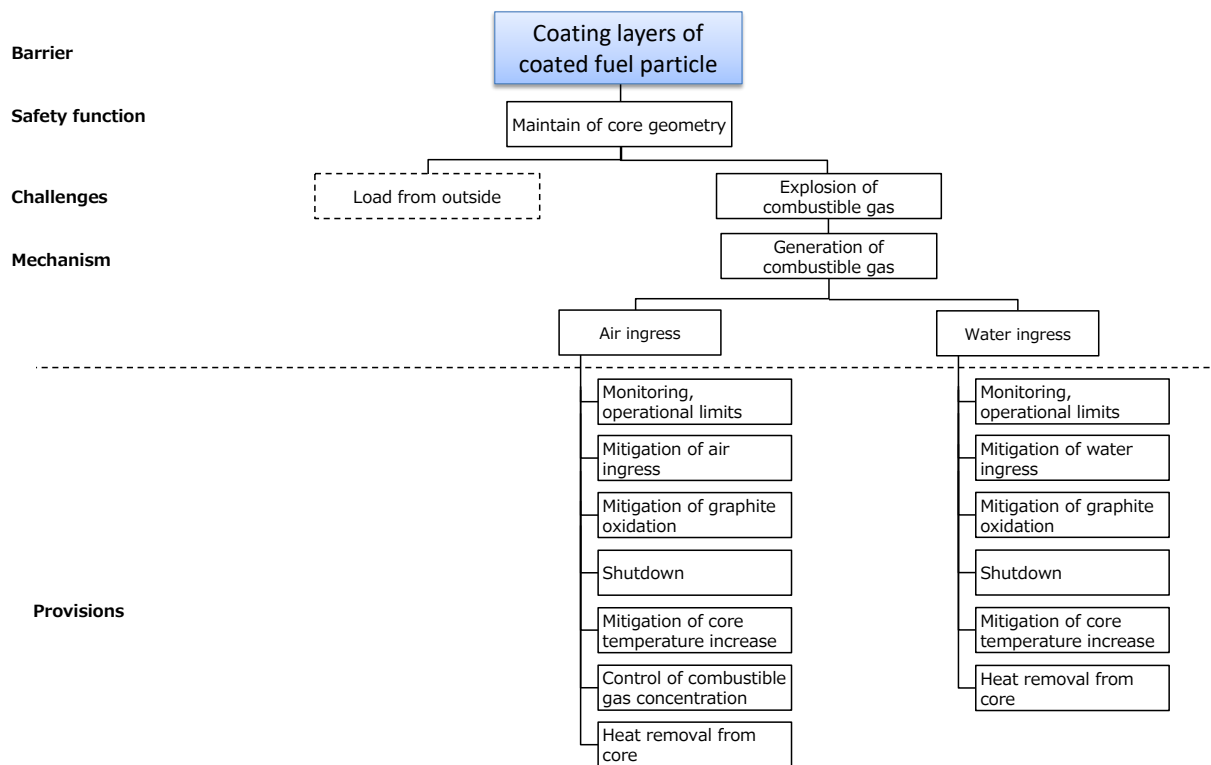


FIG. I.11. Objectives provisions tree analysis result for the coating layer of the coated fuel particle (11/11).

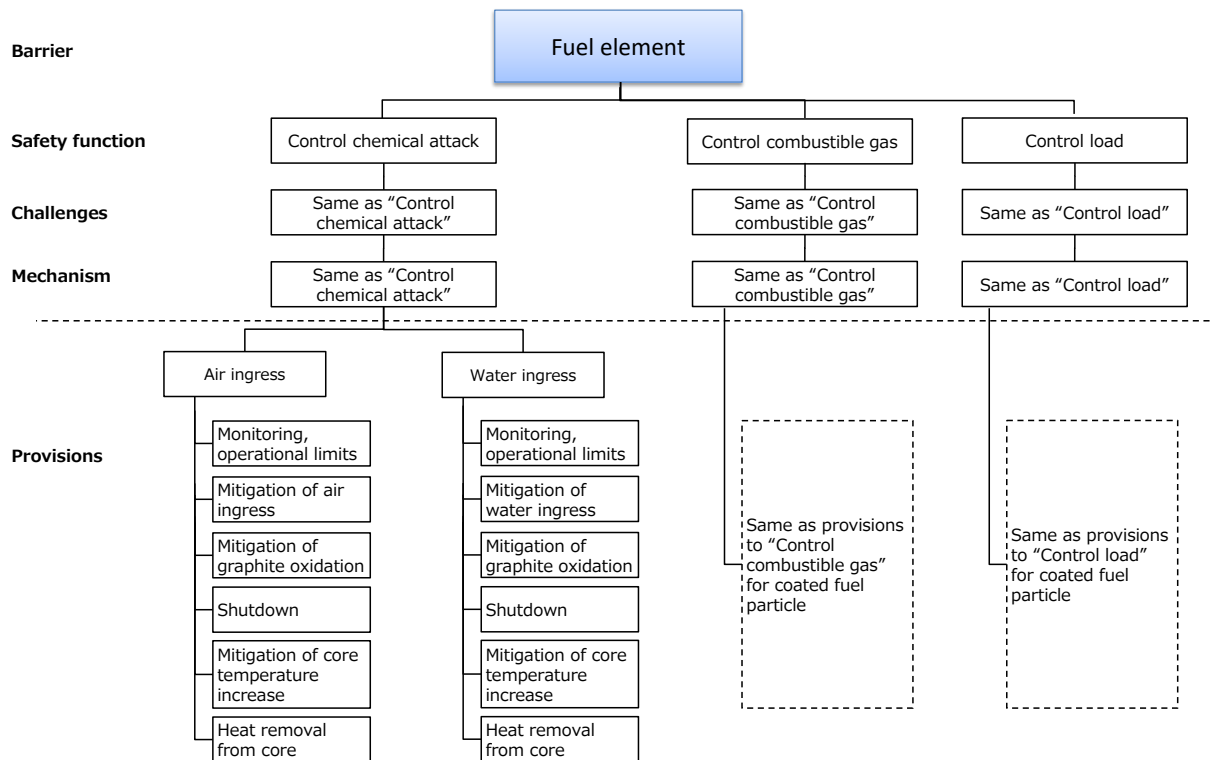


FIG. I.12. Objectives provisions tree analysis result for the fuel element.

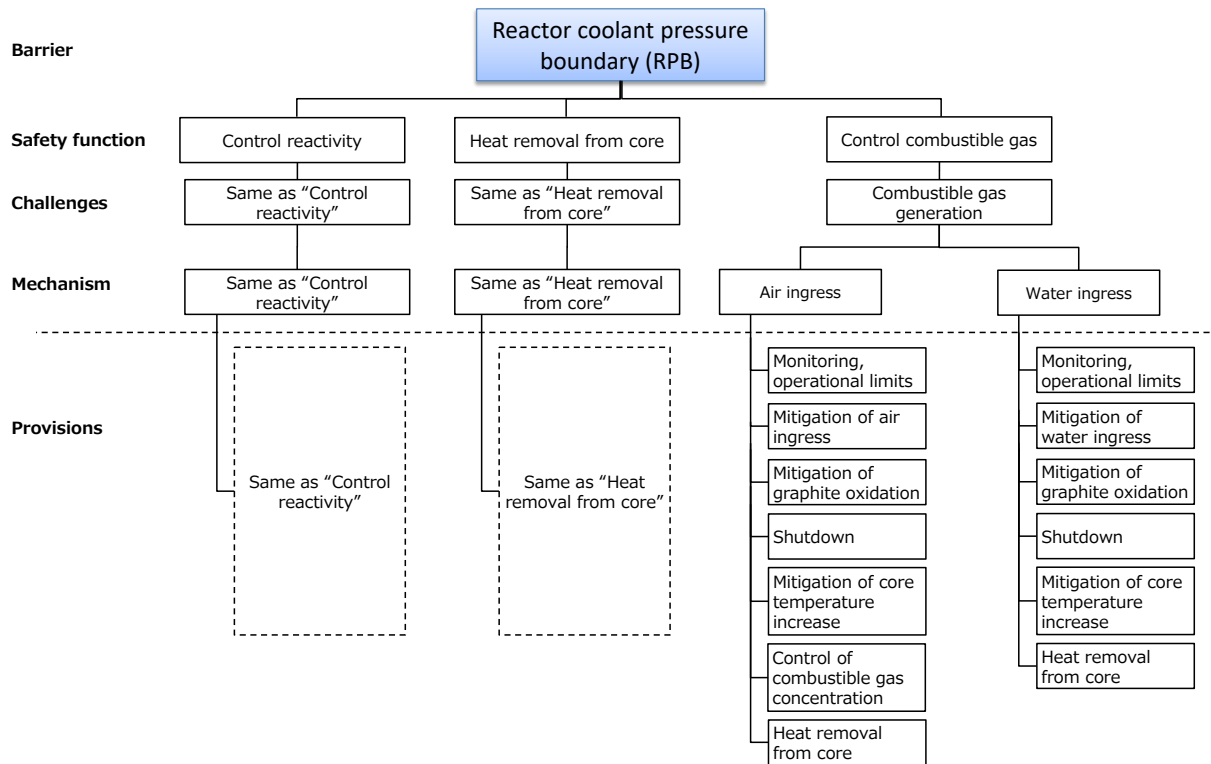


FIG. I.13. Objectives provisions tree analysis result for the reactor coolant pressure boundary (1/3).

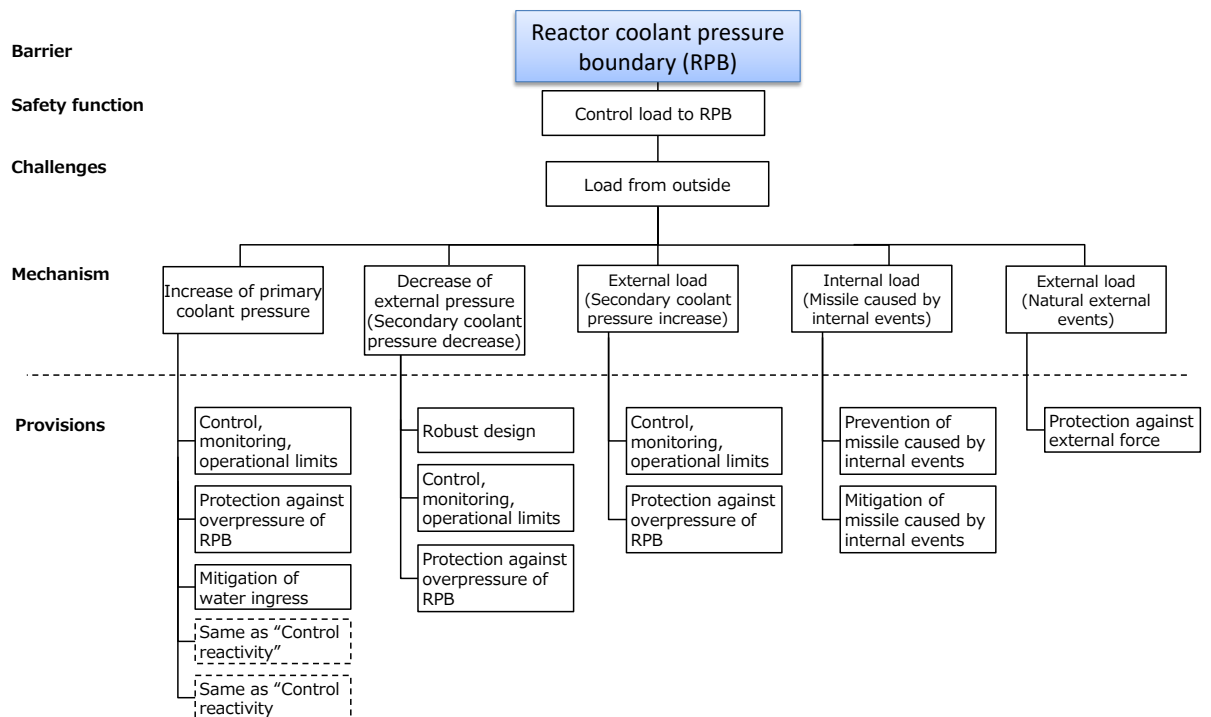


FIG. I.14. Objectives provisions tree analysis result for the reactor coolant pressure boundary (2/3).

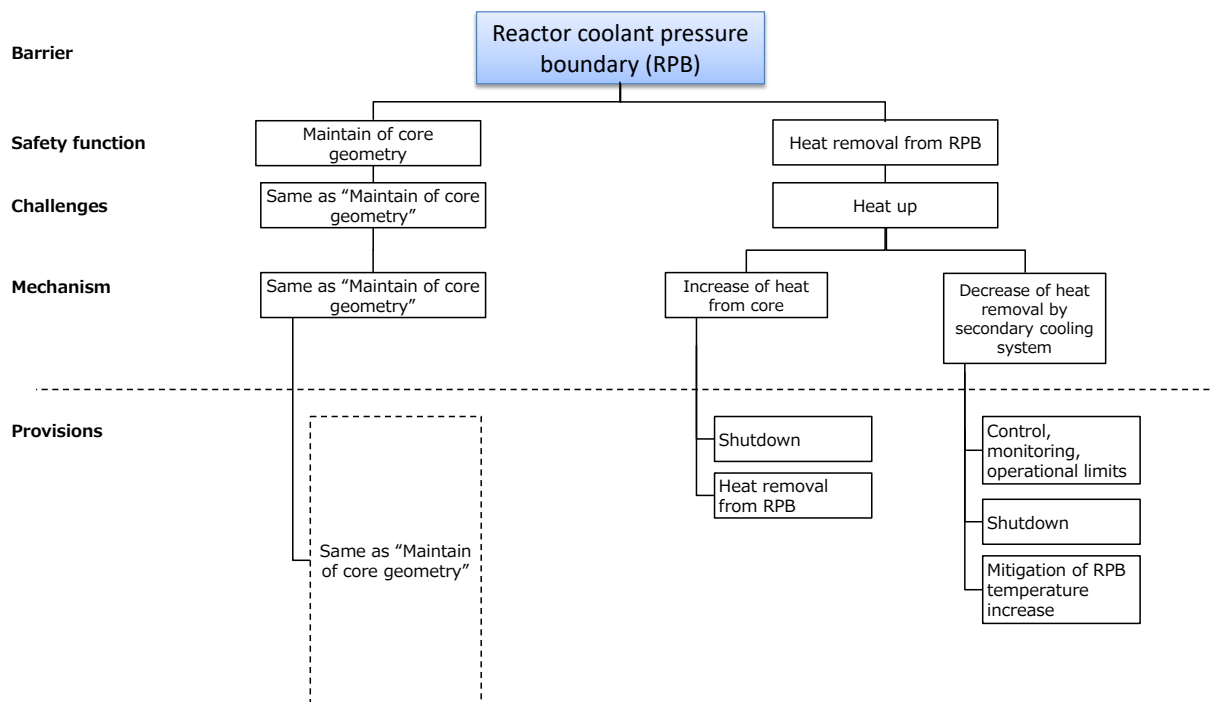


FIG. I.15. Objectives provisions tree analysis result for the reactor coolant pressure boundary (3/3).

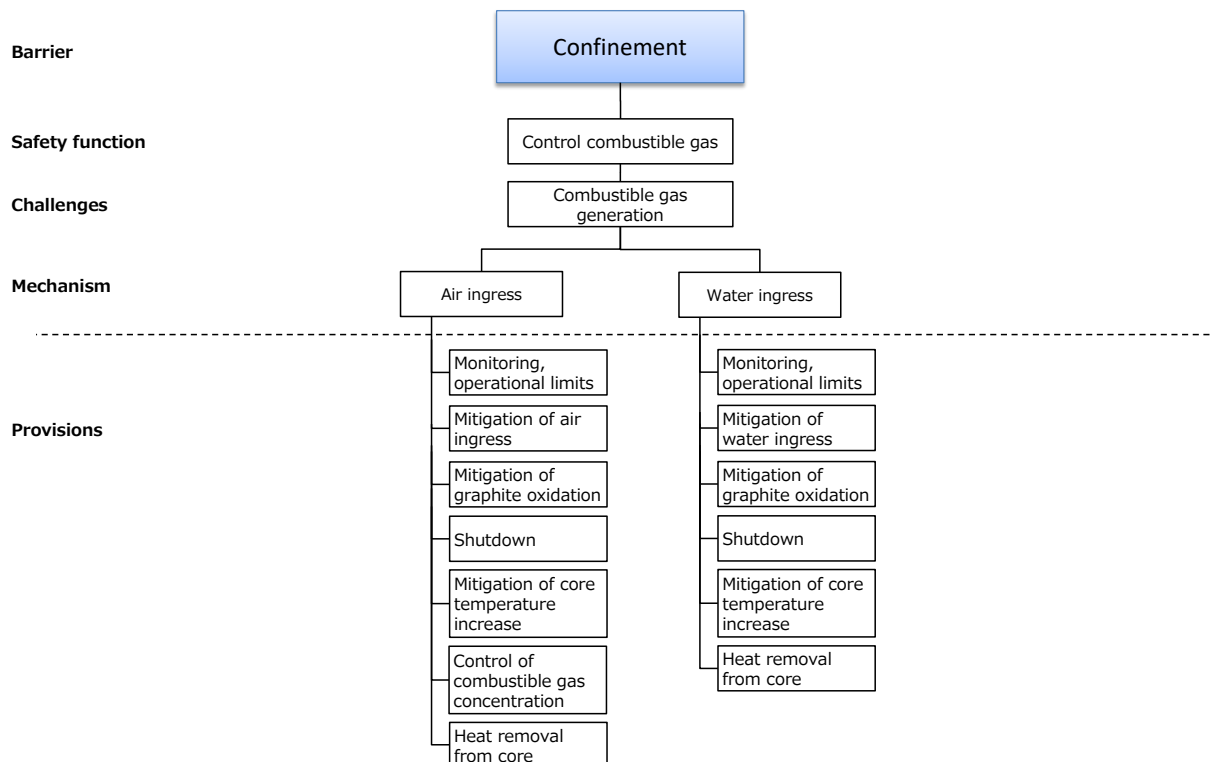


FIG. I.16. Objectives provisions tree analysis result for the confinement (1/2).

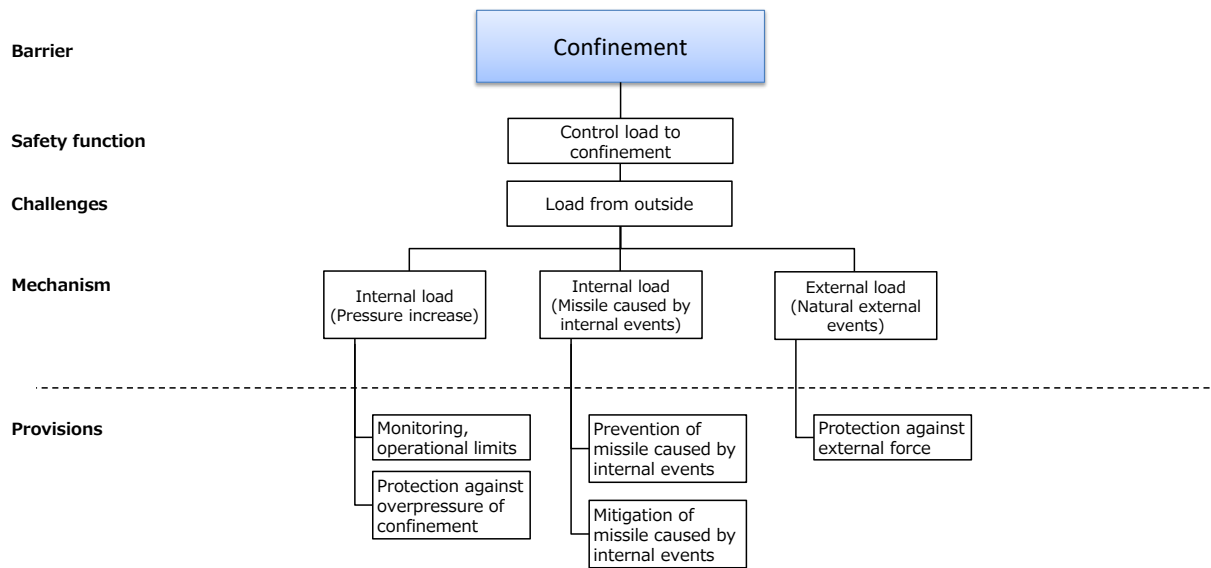


FIG. I.17. Objectives provisions tree analysis result for the confinement (2/2).

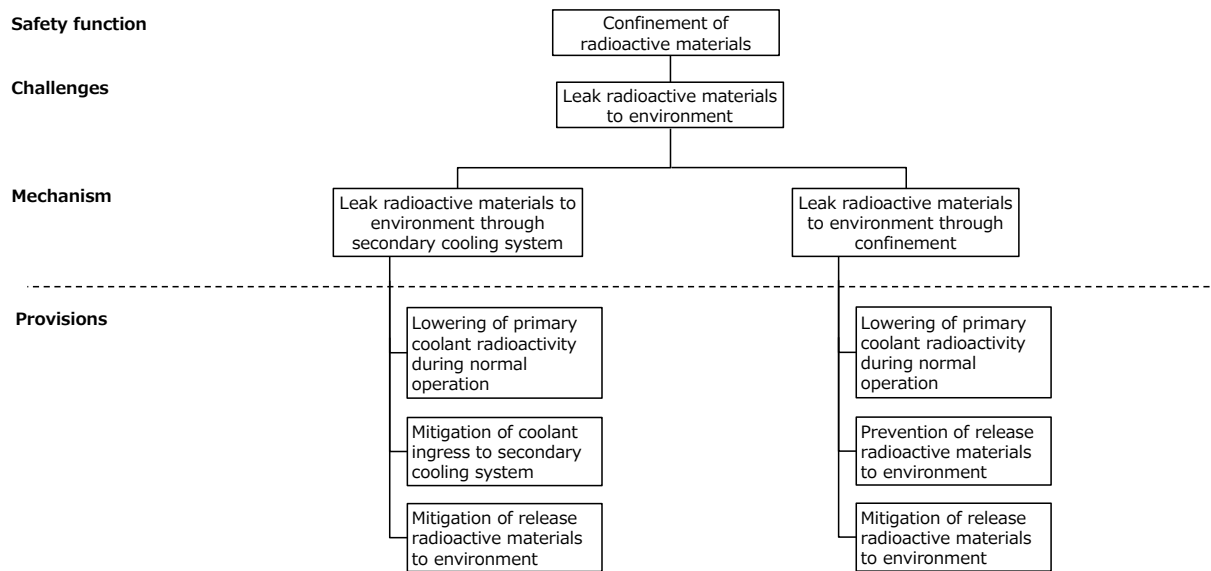


FIG. I.18. Objectives provisions tree analysis result for confinement function of radioactive materials.

APPENDIX II.

TECHNICAL REPORT: HTR-MODULE: CLASSIFICATION AND QUALITY REQUIREMENTS FOR SYSTEMS AND COMPONENTS

A05-Brivatech-Bericht HTR-020-2015

II.1. INTRODUCTION

The HTR-MODULE power plant is a thermal power plant for the cogeneration of electricity, process steam or district heating. The process steam can be used for a wide variety of applications in the chemical industry.

The modular HTR concept is characterized by the fact that standardized reactor units with power ratings of 200 MJ/s (so called modules) can be combined to form power plants with a higher power rating.

Each modular unit comprises one high-temperature reactor, one steam generator and one primary gas blower.

The heat generated by nuclear fission in the high-temperature reactor is transported from the reactor through a coaxial duct to the steam generator by the primary coolant, helium, which is circulated by the primary gas blower. In the steam generator, the heat is transferred to the water/steam conversion System which is designed and operated as a purely non-nuclear plant.

Auxiliary and supporting systems connected to the primary system are provided for operation of the reactor; furthermore, there are systems which fulfil the task of keeping loadings on components and structures within acceptable limits under accident conditions and which minimize the impact of accidents on the operating personnel and the environment.

The cooling loads in the power plant are served by closed cooling water systems which remove the rejected heat to service water systems.

II.2. NUCLEAR CLASSIFICATION AND QUALITY REQUIREMENTS

The systems and components differ in functional and safety-related importance for the overall plant and are classified accordingly. This basically applies to :

- Pressure and activity-carrying Systems
- HVAC Systems
- Hoists and Cranes
- Steelwork Items (system and component-specific)

The quality requirements relating to integrity and operability are graded according to nuclear classification.

II.2.1. Pressure and Activity-Carrying Systems

II.2.1.1. Classification

The classification of pressure and activity-carrying Systems mainly relates to the integrity of the pressure-retaining enclosure. Component internals, such as reactor pressure vessel internals and steam generator pressure vessel internals, are not covered by the classification; their specifications are based on their functional requirements only.

Quality Class MK 1

Class MK 1 covers systems and components, where postulated failures could lead to radioactive releases in excess of the dose limits stated in Article 28, Paragraph 3 of the German Radiation Protection Ordinance.

This class also covers systems and components, where postulated failures would lead to a non-isolable break in the primary gas envelope, even though the dose limits stated in Article 28, Paragraph 3 of the Radiation Protection Ordinance would not be exceeded.

In accordance with these criteria, the components of the pressure vessel unit and all connected primary coolant piping up to and including the primary system isolation valve are assigned to class MK 1.

Quality Class MK 2

- **Quality Class MK 2a**

This class covers systems which are necessary to limit loadings on components and structures for residual heat removal (such as cavity cooler for instance) and also systems and components which are necessary for module shutdown (for example, valves of feedwater and main steam system).

- **Quality Class MK 2b**

This class covers systems and components which limit the release of radioactivity to levels that do not exceed

To delimitate components of class MK 2 from classes MK 1 and NNC serve:

- Piping and components connected to class MK 1 items
- Valves with isolating functions which connect non-nuclear-classified Systems and components to class MK 2 items

Non-nuclear-classified (NNC)

All systems that are not assigned to classes MK 1 or MK 2 are non-nuclear classified. The main systems assigned to the classes are shown in Figure 43.

II.2.1.2. Quality Requirements

Component families are established within the quality classes and quality characteristics and verifications are specified for these families.

The pressure and activity-carrying systems are grouped in the following component families

- Vessels/heat exchanger
- Piping bigger than DN (nominal diameter) 80 (no MK 1 components)
- Piping less than or equal to DN 80
- Valves less than or equal to DN 80
- Pumps, blowers and compressors (no MK 1 components).

The quality characteristics of the component families conform to the rules of non-nuclear codes and Standards (e.g. Federal German Pressure Vessel Code, Federal German Technical Code for Steam Generating Installations). Additional requirements are placed on class MK 1 and MK 2 components, for example:

- Use of KTA nuclear safety Standards 3201 and 1401 for class MK 1 vessels/heat exchangers and valves bigger than DN 80

Preparation of special specifications and quality assurance by quality verifications (review of manufacturing documents) for MK 1 components and MK 2a components are carried out with the participation of the authorized experts appointed by the licensing authority.

MK 2b components and NNC components which could cause damage to safety related components on loss of integrity due to, for example, earthquake, are subject to an approval by the authorized experts.

II.2.2. HVAC Systems

II.2.2.1. Classification

Quality Class ML

This class covers HVAC components that have to be operated during or after accidents to minimize the radiological impact on the environment and thus function as activity-carrying components during such an operation, and HVAC components which ensure heat removal from compartments containing systems or components for accident control or monitoring.

Systems performing the functions described above are

- building pressure relief system
- secured subatmospheric pressure system
- secured air conditioning unit for control room, Computer and electronic equipment rooms, including the secured chilled water system
- secured air conditioning unit for the remote shutdown station.

Non-nuclear-classified (NNC)

HVAC components that are not assigned to class ML are non-nuclear-classified.

II.2.2.2. Quality Requirements

To reflect the system and component-specific tasks, the application of DIN 25 414 ("Ventilation Systems in Nuclear Power Plants") necessitates the following categorization

- Building pressure relief system assigned to category 3
- Secured subatmospheric pressure system assigned to category 3
- Secured air-conditioning unit for control room, computer and electronic equipment rooms and the secured air-conditioning unit for the remote shutdown station assigned to category 2.

Non-nuclear-classified HVAC Systems are assigned to category 3 or 4 as appropriate to their functional requirements.

Quality verifications (review of manufacturing documents) for HVAC components subject to class ML leak tightness requirements are carried out with the participation of the authorized experts appointed by the licensing authority.

II.2.3. Hoists and Cranes

II.2.3.1. Classification

Quality Class MH 1

Hoists and cranes are assigned to class MH 1 if, during load transport, failure of the hoists or cranes

- could lead to radioactive releases in excess of the dose limits stated in Article 28, Paragraph 3 of the German Radiation Protection Ordinance, or
- would lead to a non-isolable break in the primary gas envelope, even though the dose limits stated in Article 28, Paragraph 3 of the Radiation Protection Ordinance would not be exceeded.

This only applies to the following hoists and cranes:

- Reactor building crane RPV closure head transport rig
- Lift rig for shipping casks
- Slab lift rig
- Erection lugs, load attachment lugs in concrete slabs
- Hoist mechanisms and load attachment rigging for equipment handling casks.

Quality Class MH 2

Hoists and cranes are assigned to class MH 2 if, during load transport, failure of the hoists or cranes could lead to major radioactive releases inside the plant.

In the given concept of the HTR Module plant there is no hoist and crane assigned to this class.

Non-nuclear-classified (NNC)

Hoists and cranes that are not assigned to classes MH 1 and MH 2 are nonnuclear-classified.

II.2.3.2. Quality Requirements

The hoists and cranes listed above are designed in compliance with the stringent requirements of KTA Nuclear Safety Standard 3902, other hoists and cranes in compliance with non-nuclear codes and standards (Load Attachment Rigging for Hoist Operation; VBG 9a).

Quality verification is performed as appropriate to the items concerned in accordance with KTA Nuclear Safety Standard 3903 for class MH hoists and cranes, and VBG 9a for NNC hoists and cranes.

II.2.4. Steelwork (System-and Component-Specific)

The steelwork classification applies to the following items, provided that they serve systems or components:

- Steel platforms, steel stairways and steel landings
- Piping supports (including valve supports), e.g. piping anchors, guides, sliding supports, support frames as well as variable support spring hangers and variable spring supports, constant hangers and constant supports, snubbers and shock absorbers
- Component supports, e.g. structural steel frames, pump frames, lugs, support
- Protective and Special structures, e.g. bumpers and manipulator rails
- Anchoring items.

The various steelwork items are classified according to the following criteria.

II.2.4.1. Classification

Quality Class MS 1

This class covers steelwork items, where postulated failures

- could lead to radioactive releases in excess of the dose limits stated in Article 28, Paragraph 3 of the German Radiation Protection Ordinance
- would lead to a non-isolable break in the primary gas envelope, even though the dose limits stated in Article 28, Paragraph 3 of the German Radiation Protection Ordinance would not be exceeded
- could cause a simultaneous failure of all trains of the cooling systems in the primary cavity.

Quality Class MS 2

This class covers steelwork items, where postulated failures

- could degrade the operability of parts assigned to seismic class I
- could lead to loss of integrity of MK 2 components in the reactor building.

Non-nuclear-classified (NNC)

Steelwork items that are not assigned to class MS1 or MS 2 are non-nuclearclassified.

If steelwork items supporting differently classified components or piping, the classification of the overall structure is basically governed by the component class with the highest significance to safety.

II.2.4.2. Quality requirements

The quality characteristics of steelwork comply with rules of DIN 18 800 (Part 1: Steel Structures; Design and Construction - Part 7: Steel Structures; Fabrication, Verification of Suitability for Welding). Additional requirements are placed on class MS 1 and MS 2 steelwork (e.g. application of KTA Nuclear Safety Standard 3205.01 for the pressure vessel unit support). Quality verifications (reviews of manufacturing documents) for class MS 1 steel-work are carried out with the participation of the authorized expert appointed by the licensing authority.

Abbreviations

KTA Kerntechnischer Ausschuß

VBG Verband der Berufsgenossenschaften

APPENDIX III.
APPROACH 2 SPECIFIC SAFETY REQUIREMENTS FOR DESIGN OF MHTGRS

(SEE APPROACH 2 DOCUMENT)

REFERENCES
for Specific Safety Requirements for Design of Modular HTGR

- [1] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-R-3, IAEA, Vienna (2006).
- [2] INTERNATIONAL ATOMIC ENERGY AGENCY, Radiation Protection and Safety of Radiation Sources: International Basic Safety Standards (Interim Edition), IAEA Safety Standards Series No. GSR Part 3, IAEA, Vienna (2011).
- [3] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment for Facilities and Activities, IAEA Safety Standards Series No. GSR Part 4, IAEA, Vienna (2009).
- [4] INTERNATIONAL ATOMIC ENERGY AGENCY, Site Evaluation for Nuclear Installations, IAEA Safety Standards Series No. NS-R-3, IAEA, Vienna (2003).
- [5] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Commissioning and Operation, IAEA Safety Standards Series No. SSR-2/2, IAEA, Vienna (2011).
- [6] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GSR Part 7, IAEA, Vienna (in preparation).

REFERENCES

- [A] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1 (Rev.1), IAEA, Vienna (2016).
- [B] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1, IAEA, Vienna (2012).
- [C] Sato, H. , et al., Safety Design Consideration for HTGR Coupling with Hydrogen Production Plant, Progress in Nuclear Energy, doi: 10. 1016/j.pnucene.214.07.032 (2014).
- [D] Takamatsu, K. et al., Experiments and validation analyses of HTTR on loss of forced cooling under 30% reactor power, J. Nucl. Sci. Technol., Vol.51, No.11-12, pp.1427-1443 (2014).

REFERENCES

- [1] INTERNATIONAL ATOMIC ENERGY AGENCY Safety Standards Series No. SSR-2/1: Safety of Nuclear Power Plants: Design, IAEA, Vienna (2012).
- [2] INTERNATIONAL ATOMIC ENERGY AGENCY Safety Standards Series No. SSR-2/1 (Rev 1): Safety of Nuclear Power Plants: Design, IAEA, Vienna (2016)
- [3] https://www.gen-4.org/gif/jcms/c_42153/very-high-temperature-reactor-vhtr ; Accessed 15 December 2016
- [4] C.R. Fisher and D.D. Orvis, “Licensing of HTGRs in the United States”, Specialists meeting on gas-cooled reactor safety and licensing aspects; Lausanne, Switzerland; 1 - 3 Sep 1980, International Atomic Energy Agency, International Working Group on Gas-Cooled Reactors; p. 184-190; Vienna (Austria), Jan 1981.
- [5] Summary of the NRC delegation visit to Germany on safety aspects of high temperature gas cooled reactor design technology, August 2001.
<http://www.nrc.gov/docs/ML0411/ML041170039.pdf>
- [6] National Nuclear Regulator, RD-019, “Requirements for the Core Design of the Pebble Bed Modular Reactor” Revision 0, South Africa, October 2006.
- [7] P. Bester, “Licensing Framework for the Pebble Bed Modular Reactor and the Lessons Learnt with the licensing of a new reactor technology” Presented at the 1st RCM for the Modular HTGR Safety Design, 9-12 June 2015, Vienna, Austria.
- [8] F. H. Southworth, et.al. “The Next Generation Nuclear Plant (NGNP) Project” Proc. Global 2003, New Orleans, USA, 16-20 November 2003.
- [9] Draft Advanced Non-Light Water Reactor Design Criteria, NRC, ML16096A420; Accessed 21 December 2016
<http://www.nrc.gov/reactors/advanced/non-lwr-activities/adv-non-lwr-rx-dc.html>;
- [10] Hirofumi Ohashi, Hiroyuki Sato, Shigeaki Nakagawa, Yukio Tachibana, Tetsuo Nishihara, Xing Yan, Nariaki Sakaba, Kazuhiko Kunitomi, “Safety Design Approach for the Development of Safety Requirements for Design of Commercial HTGR”, HTR2014-81150, Proceedings of the HTR 2014, 27-31 October Weihai, China, (2014)
- [11] Hirofumi Ohashi, Hiroyuki Sato, Shigeaki Nakagawa, Kazumi Tokuhara, Tetsuo Nishihara, Kazuhiko Kunitomi, “Development of Safety Requirements for HTGRs Design”, Proceedings of the HTR 2016, Las Vegas, USA, 6-10 November, 2016.
- [12] INTERNATIONAL ATOMIC ENERGY AGENCY, Proposal for a Technology-Neutral Safety Approach for New Reactor Designs, TECDOC-1570, IAEA, Vienna, 2007.
- [13] INTERNATIONAL ATOMIC ENERGY AGENCY, Considerations in the development of safety requirements for innovative reactors: Application to modular high temperature gas cooled reactors, TECDOC-1366, IAEA, Vienna, 2003.
- [14] INTERNATIONAL ATOMIC ENERGY AGENCY, Accident Analysis for Nuclear Power Plants with Modular High Temperature Gas Cooled Reactors, Safety Reports Series No. 54, IAEA, Vienna, 2008.
- [15] F. Reitsma, P. Chellapandi, K. Tuček, N Tricot, Safety Requirements for Design and Safety Assessment of HTGR and Fast Reactors, Paper HTR2012-8-002, *Proc. HTR 2012*, Tokyo, Japan, 28 Oct. – 1 Nov. 2012.
- [16] INTERNATIONAL ATOMIC ENERGY AGENCY, Risk Informed Regulation of Nuclear Facilities: Overview of the Current Status, IAEA-TECDOC-1436, IAEA, Vienna (2005).
- [17] PROSEK, A., MAVKO, B., “BEPU methods and combining of uncertainties”, Updates in Best Estimate Methods in Nuclear Installation Safety Analysis (Proc. Int. Mtg Washington, DC, 2004), American Nuclear Society, La Grange Park, IL (2004).

- [18] INTERNATIONAL ATOMIC ENERGY AGENCY, Status of Advanced Light Water Reactor Designs — 2004, IAEA-TECDOC-1439, IAEA, Vienna (2002).
- [19] INTERNATIONAL ATOMIC ENERGY AGENCY, HWRs — Status and Projected Development, Technical Reports Series, IAEA-TRS-407, IAEA, Vienna (2002).
- [20] INTERNATIONAL ATOMIC ENERGY AGENCY, Current Status and Future Development of Modular High-Temperature Gas-Cooled Reactor Technology, IAEA-TECDOC-1198, IAEA, Vienna (2001).
- [21] INTERNATIONAL ATOMIC ENERGY AGENCY, Status of Liquid Metal Cooled Fast Reactor Technology, IAEA-TECDOC-1083, IAEA, Vienna (1999).
- [22] INTERNATIONAL ATOMIC ENERGY AGENCY, Innovative Small and Medium Sized Reactors: Design Approaches, Safety Features and R&D Trends, Final Report of IAEA Technical Meeting Convened in Vienna on 7–11 June 2004, IAEA-TECDOC-1451, IAEA, Vienna (2005).
- [23] INTERNATIONAL ATOMIC ENERGY AGENCY, External Human Induced Events in Site Evaluation for Nuclear Power Plants, Safety Standards Series, No. NS-G-3.1, IAEA, Vienna (2002).
- [24] INTERNATIONAL PANEL ON CLIMATE CHANGE, Special Report on Emission Scenarios, A Special Report of Working Group III, Cambridge University Press, Cambridge (2000).
- [25] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, Safety Standards Series No. NS-R-1, IAEA, Vienna (2000).
- [26] GASPARINI, M., “The IAEA Safety Standards for Design. Application to Small and Medium Size Reactors”, C&S Papers Series No. 14, IAEA, Vienna (2002).
- [27] "Development of Regulatory Technology for High Temperature Gas-Cooled Reactor for Hydrogen Production - Analysis of design and regulation characteristics of High Temperature Gas-Cooled Reactor", KINS Report, KINS/GR-280, 2005. (In Korean)
- [28] "Study on Status of Regulatory Technologies and Development of Safety Issues and Regulatory Technology for High Temperature Gas-Cooled Reactor for Hydrogen Production ", KINS Report, KINS/GR-327, 2006. (In Korean)
- [29] "Development of Licensing Technologies for Very High Temperature Gas-Cooled Reactors", KINS Report, KINS/RR-840, 2011. (In Korean)
- [30] "Establishment of direction for the development of Licensing procedures of regulation requirements for Gen-IV nuclear reactors", KINS Report, KINS/RR-613, 2008. (In Korean)
- [31] "Development of Licensing Technologies for Very High Temperature Gas-Cooled Reactors", KINS Report, KINS/GR-489, 2012. (In Korean)
- [32] "Development of Licensing Technologies for Very High Temperature Gas-Cooled Reactors", KINS Report, KINS/FR-566, 2015. (In Korean)
- [33] "A Study on Very High Temperature Gas-Cooled Reactor System Concept", KAERI Report, KAERI/RR-3869/2014, 2015. (In Korean)
- [34] H. Sato, et al., “Safety design consideration for HTGR coupling with hydrogen production plant,” *Progress in Nuclear Energy*, 82, pp. 46-52 (2015).
- [35] H. Ohashi, et al., “Safety Design Approach for the Development of Safety Requirements for Design of Commercial HTGR,” *Proceedings of the HTR 2014*, Weihai, China, October 27-31, 2014, Paper HTR2014-81150 (2014) (CD-ROM).
- [36] Donald E. Carlson, Sydney J. Ball, “Perspectives on understanding and verifying the safety terrain of modular high temperature gas-cooled reactors”; **NED 306** (2016) p117-123.
- [37] L.M. Lidsky, “Levels of Safety, Radiation Research,” *Nuclear Power*, **113**, 217 (1998).

- [38] H. Ohashi, H. Sato, K. Kunitomi, et al., “Concept on Inherent Safety in High-Temperature Gas-Cooled Reactor,” *Transactions of the Atomic Energy Society of Japan*, vol. 13, No. 1, p. 17, (2014) (in Japanese).
- [39] K. Kunitomi, S. Katanishi, S. Takada, et al., “Japan's future HTR-the GTHTTR300,” *Nuclear Engineering and Design*, vol. 233, p. 309, (2004).
- [40] K. Kunitomi, X. Yan, T. Nishihara et al., “JAEA’s VHTR for Hydrogen and Electricity Cogeneration: GTHTTR300C,” *Nuclear Engineering and Technology*, vol. 39, no. 1, p. 9, (2007).
- [41] IAEA INSAG DID INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, *Basic Safety Principles for Nuclear Power Plants*, 75-INSAG-3 Rev. 1, INSAG-12, IAEA, Vienna (1999).
- [42] Western European Nuclear Regulators Association, *Safety of new NPP designs*, WENRA (2013).
- [43] U.S. Nuclear Regulatory Commission Glossary, <https://www.nrc.gov/reading-rm/basic-ref/glossary/defense-in-depth.html>
- [44] U.S. Nuclear Regulatory Commission, NUREG/KM-0009, “Historical Review and Observations of Defense-in-Depth”, April 2016.
- [45] International Atomic Energy Agency, Safety Report Series No. 46, “Assessment of Defence in Depth for Nuclear Power Plants”, 2005.
- [46] S. Ball, “Overview of Modular HTGR Safety Characterization and Postulated Accident Behavior Licensing Strategy”, ORNL/TM-2014/187, Oak Ridge National Laboratory, May 2014.
- [47] MHTGR Fuel Performance and supporting Data base, report GA-A19877, General Atomics, October 1989.
- [48] DOE/NRC, 2008, *Next Generation Nuclear Plant Licensing Strategy - A Report to Congress*, Department of Energy/Nuclear Regulatory Commission, August 2008.
- [49] S. Saito, et al., “Design of High Temperature Engineering Test Reactor (HTTR),” *JAERI 1332*, (1994).

ANNEX I. IMPUTS FROM OTHER COUNTRIES ON APPROACH 1 ELEMENTS

[Draft CRP TECDOC on Blended Approach → (Action 1 (US))]

Participating countries in the IAEA CRP were asked for input on the top safety requirements, off-normal events, safety functions, and SDCs. This information was used to conduct a comparison study, described below, on the approaches used to develop HTGR SDCs.

I-1. TOP SAFETY REQUIREMENTS

In Section 4.1, an overview is provided of the approach used by the United States to meet the top level requirements. The main elements of Approach 1 are similar to those used to develop the top safety requirements in other countries. The United Kingdom and Germany have provided input to compare the top safety requirements between different approaches.

I-1.1. United Kingdom Top Safety Requirements

The United Kingdom (U.K.) Top Safety Requirements used in the comparison are derived from the Safety Assessment Principles for Nuclear Facilities. The Safety Assessment Principles (SAPs) are used to guide regulatory judgements and recommendations when undertaking technical assessment of nuclear site licensees' safety submissions. The 2014 SAPs provides frequency dose targets during accidents for any person off the site on an individual facility. The Basic Safety Objectives (BSOs) are benchmarks that reflect modern safety standards and expectations and are comparable to the NRC safety limits used in the U.S. Table I-1 provides the BSO during normal operation for any person off the site and Table I-2 provides both the event consequences and the frequency range for any person off the site during an accident over which the BSOs must be met. The metric for the event sequence frequency is for the entire plant, consisting of one or more reactors.

TABLE I-1. U.K. FREQUENCY DOSE TARGETS FOR NORMAL OPERATION

Normal operation – any person off the site		Target 3
The target and a legal limit for effective dose in a calendar year for any person off the site from sources of ionising radiation originating on the site are:		
BSL(LL):	1 mSv	
BSO:	0.02 mSv	
<i>Note that there are other legal limits to tissues and parts of the body (IRR99).</i>		

TABLE I-2. U.K. FREQUENCY DOSE TARGETS FOR ACCIDENTS ON AN INDIVIDUAL FACILITY

Frequency dose targets for accidents on an individual facility – any person off the site		Target 8
The targets for the total predicted frequencies of accidents on an individual facility, which could give doses to a person off the site are:		
Effective dose, mSv	Total predicted frequency per annum	
	BSL	BSO
0.1–1	1	1×10^{-2}
1–10	1×10^{-1}	1×10^{-3}
10–100	1×10^{-2}	1×10^{-4}
100–1000	1×10^{-3}	1×10^{-5}
>1000	1×10^{-4}	1×10^{-6}

Figure I-1 shows the comparison of the U.K. BSOs in red on the frequency-consequence curve derived from the U.S. NRC and EPA regulations, in blue, as derived in Section 4.1. In general, the U.K. BSO limits are more restrictive in both the acceptable frequency and consequences limits than those in the FC curve derived from the U.S. regulations. Although there is agreement that the design basis region begins below 1×10^{-2} per plant year, the U.K. BSOs lower frequency of the design basis region, 1×10^{-4} per plant year, extends an order of magnitude lower than the U.S. design basis event region. The U.S. design target is constant over orders of magnitude compared to the step pattern of the U.K. BSOs. This may present interpreting difficulties early in design process where uncertainties are large in frequency and/or consequence data relative to the steps.

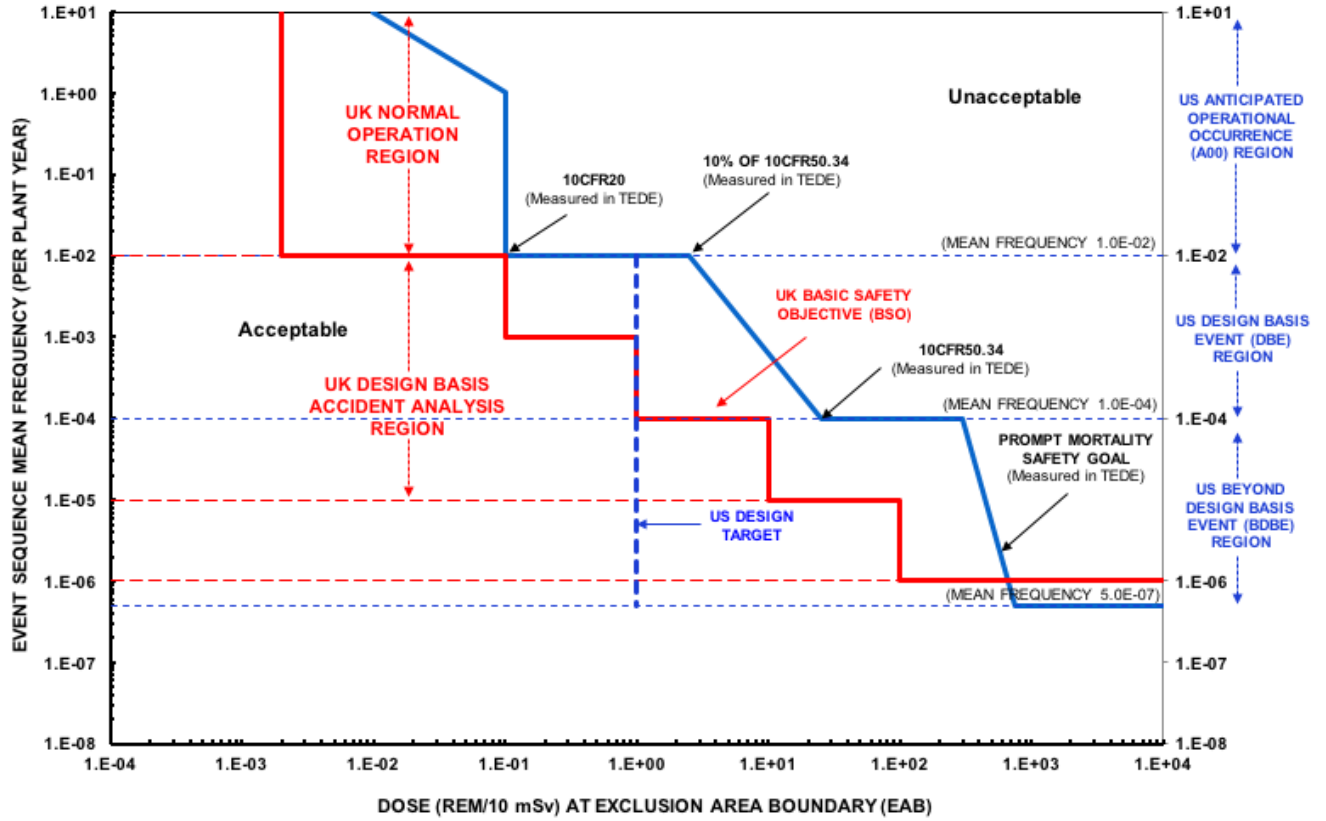


FIG. I-1. Comparison of frequency consequence curves for the United States and United Kingdom.

I-1.2. Germany Top Safety Requirements

The frequency consequence information for Germany is derived from the defense-in-depth safety concept for nuclear power plants provided in the Safety Principles Technical Report shown in Table I-3. For the HTR-Module, normal operation occurs when the postulated initiating event (PIE) frequency is greater or equal to 1×10^{-2} per plant year, accidents occur when the PIE frequency is between 1×10^{-2} and 1×10^{-6} per plant year, and special rare events occur at an event frequency higher than 1×10^{-6} per plant year.

Level of defense	Plant states, Events	Frequencies ^{a)} of plant states or events	Technical installations ^{b)} and measures	Radiation protection requirements	Design Basis Area/ Precaution
1	Normal Operation (including maintenance) and outage	continuous	Operational Systems and components	Radiation Protection Ordinance, e.g., 1mSv/a whole body	
2	Abnormal Operation (disturbances)	frequently	c)Monitoring of radiation Safety Information system, Limitation devices		
3	Accidents	rare ²⁾	Safety System	Radiation Protection Ordinance, e.g., 50mSv whole body	
4a	Special very rare events	very rare*	Special measures	Risk reduction Reduction of radiation exposure	Beyond Design Basis Area
4b	Plant states beyond design basis without severe core damage	very rare ³⁾	Measures to avoid severe core damage		
4c	Plant states with failure of all preventive measures, core damage	extremely rare ⁴⁾	Measures to reduce release of radioactive material		
Damage states with relevant effects on the environment			Disaster control and environmental protection		

a) Orientation values for frequency of events/states (per year and plant):

1) $\geq 10^{-2}$; 2) 10^{-2} - 10^{-5} ; 3) 10^{-5} - 10^{-6} ; 4) $< 10^{-6}$

*) Assignment due to special considerations; measures taken can partly not be justified by frequency of demand

b) Examples with classification according to safety relevance or design requirement

c) Individual safety installations may already apply to level of defense 2

TABLE I-3. DEFENSE-IN-DEPTH SAFETY CONCEPT FOR NUCLEAR POWER PLANTS FOR GERMANY

The comparison between the frequency-consequence curves of Germany, shown in green, and the U.S., shown in blue, is provided in Figure I-2. Note that since the frequency metric from

Germany is not the entire event sequence, but only the initiating event, the comparison is meaningful for only the higher frequency events. In addition to the more restrictive German frequency definition, the dose limits are also orders of magnitude more restrictive, closer to the U.S. design target than the doses taken from the U.S. regulations. The German consequence metric used is for the whole body rather than the more comprehensive total effective dose equivalent (TEDE) dose used in the U.S., which is weighted by the health effects to an offsite person. Therefore, a direct comparison between the countries' consequence data cannot accurately be made. The lower frequency of the U.S. Design Basis Event region and German Accidents region do not agree, with the German Accidents region extending two orders of magnitude further to a frequency of 1×10^{-6} per plant year. This major difference shows the disconnect between the U.S. and Germany on how low in frequency the design basis should extend.

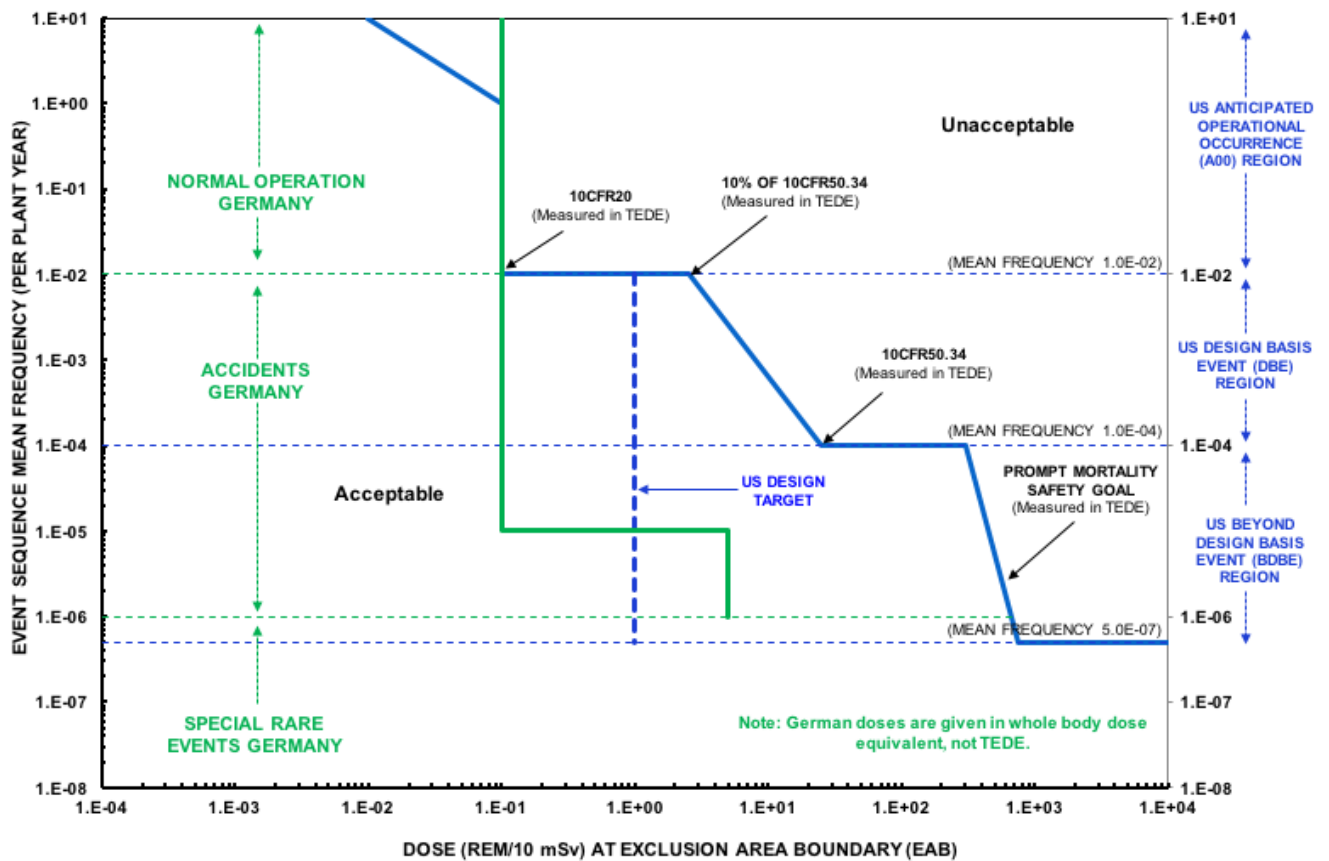


FIG. I-2. Comparison of frequency consequence curves for the United States and Germany.

I-1.3. Summary of the Comparison of Top Safety Requirements from the U.S., U.K., and Germany

At this point, it is difficult to conclude whether or not the major differences in top level requirements between the three countries will ultimately affect the SDCs. Figure I-3, shown

below, contains all three countries' top safety requirements. The U.K. and U.S. both have requirements expressed as risks of the entire event frequency, while Germany uses a more deterministic approach that examines only the PIEs. This makes a direct comparison between all three countries difficult.

There is not only disagreement between countries on the dose consequences, but also on what the design frequency should encompass. Generally, the U.K. and particularly Germany have requirements that are more restrictive than the U.S.

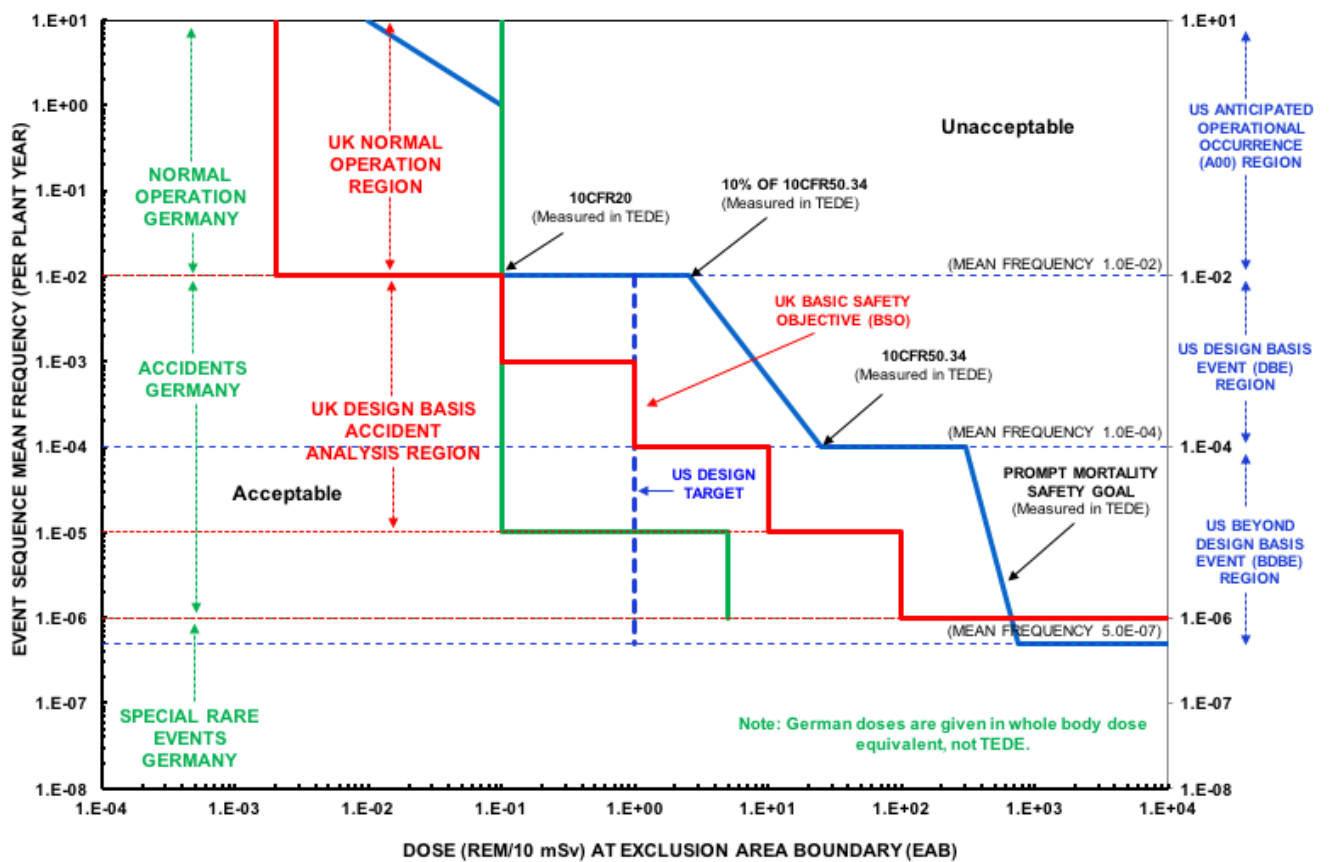


FIG. I-3. Comparison of frequency consequence curve for the United States, United Kingdom, and Germany.

I-2. OFF-NORMAL DESIGN EVENTS

Off-normal event input from other countries for their modular HTGR designs was received from Japan and Germany.

I-2.1. Japan Off-Normal Design Events

The AOOs (initiating events with frequencies greater than 10^{-2} /reactor year) from Japan for their Gas Turbine High Temperature Reactor (GTHTR) are listed in Table I-4. The GTHTR is

a modular HTGR that utilizes a Brayton cycle with a helium gas turbine within the primary system rather than a steam Rankine cycle with a steam generator within the primary system.

TABLE I-4. ANTICIPATED OPERATIONAL OCCURRENCES PROVIDED BY JAPAN FOR GTHTR

a) Transients
• Abnormal control rod insertion • Abnormal control rod withdrawal • Loss of load • Increase in rotation number of cooling water pump • Abnormal opening of safety valve in primary loop • Leakage in cooling water system piping • Abnormal opening of safety valve in shutdown cooling system • Abnormal opening in purge line of standpipe • Leakage in recuperator heat exchange part • Abnormal opening of turbine bypass control valve • Abnormal opening of recuperator inlet temperature control valve

A comparison of the five MHTGR AOOs in Table 8 with the eleven GTHTR AOOs in Table I-4 shows that there are several in common, for example, an abnormal control rod withdrawal and small leaks in the HPB. The others differ due to the MHTGR steam cycle and the GTHTR gas turbine cycle designs.

The PIEs from Japan are shown in Table I-5 categorized by type.

TABLE I-5. SINGLE FAILURE INITIATING EVENTS FOR DBAS PROVIDED BY JAPAN FOR GTHTR

a) Transients
• Abnormal opening of turbine bypass valve • Abnormal opening of discharge valve in helium supply and storage system • Abnormal opening of supply valve in helium supply and storage system • Leakage in pressure vessel of cooler in cooling water system • Leakage in piping of shutdown cooling system

• Turbine blade failure • Compressor blade failure • Failure in gas turbine shaft • Abnormal startup in helium circulator • Fuel coolant channel blockage
b) Air ingress
• Failure in outer piping of co-axial piping • Standpipe rupture • Leakage in reactor pressure vessel • Leakage in heat exchanger pressure vessel • Leakage in inner piping of co-axial piping • Rupture of co-axial piping
c) Water ingress
• Leakage in precooler heat transfer tube • Leakage in shutdown cooling system heat transfer tube
d) Radioactive material leakage
• Leakage in piping of helium purification system • Leakage in decay tank of gaseous radioactive waste treatment system • Leakage in waste liquid evaporator vessel of liquid waste treatment system • Leakage in demineralizer vessel of liquid waste treatment system

A comparison of the PIEs from Japan for the GTHTTR in Table I-5 with the DBEs from the US in Table 9 for the MHTGR is more complicated than only the differences in design but also in the deterministic versus risk-informed approach to event selection. The PIEs from Japan are from the traditional, deterministic approach of assuming a Postulated Initiating Event (PIE) followed by the response of preselected safety-related SSCs. Since the DBAs that correspond to the initiating events from Japan have only SSCs responding that are safety-related, a closer comparison would be expected with the US DBAs provided in the right hand column of Table 12, that also only rely on safety-related SSCs.

However, a further complication to the comparison is that the PIEs from Japan are categorized by transients, phenomena (air and water ingress) or non-reactor core sources. The phenomena may or may not be within the MHTGR DBAs depending on the DBE initiating event frequency and the non-reactor core sources were not yet examined in the conceptual design phase. Another difference may be the selection of piping versus pressure vessels. The MHTGR has a vessel system comprised of three highest quality ASME vessels including the cross vessel that

has an inner hot duct within the return of the cold helium to the reactor vessel from the steam generator vessel. Apparently, the GTHTTR design has coaxial piping in the Brayton cycle that has an outer pipe rather than a pressure vessel.

As a result of the above differences, it is difficult to identify even one DBA in common, although since both designs are modular HTGRs with passive core cooling from the reactor vessel to an outer passive system, the GTHTTR no doubt has DBAs that are pressurized and depressurized loss of forced cooling events DBE-1 and DBE-10/11 in Table 12.

I-2.2. Germany Off-Normal Design Events

The defense-in-depth framework utilized in Germany, shown in Table I-3, applied to the HTR Module results in Postulated Initiating Events (PIEs) that challenge the preselected safety systems. The HTR-Module is a pebble bed modular HTGR that like the MHTGR utilizes a steam Rankine cycle with a steam generator within the primary system.

The PIEs from Germany shown in Table 14 are categorized by type.

TABLE I-6. POSTULATED INITIATING EVENTS FOR DBAS PROVIDED BY GERMANY FOR HTR-MODULE

I.1 Primary system depressurization

- Catastrophic failure of the pressure vessel unit (RPV, gas duct pressure vessel, SG pressure vessel) can be ruled out thanks to quality assurance measures
- Break in a connecting pipe between reactor pressure vessel and primary system isolation valve
- Break in connecting pipe downstream of the primary system isolation valve inside the reactor building
- Break in a primary coolant-conveying instrument line
- Inadvertent opening of a safety valve and that valve stuck open

I.2 Damage to steam generator tubes

- Rupture of a steam generator tube
- Rupture of a steam generator tube concurrent with long-term failure of water separation equipment and the primary system pressure control system

I.3 Malfunctions of the helium purification system and liquid waste system

- Break in the largest primary coolant-conveying line outside the reactor building and closure of the primary system isolation valves
- Break in a vessel containing radioactively contaminated water

I.4 Earthquake

- Effects on the reactor building, switchgear and emergency supply building, and service water systems
- Effects on the reactor auxiliary building

II.1 Reactivity accidents

- Withdrawal of all reflector rods at different initial conditions
- Water ingress into the primary system

II.2 Malfunction in the main heat transfer system

- Failure of the auxiliary power supply
- Short-term failure of the auxiliary power supply (≤ 2 hours) and unavailability of both emergency diesels
- Long-term failure of the auxiliary power supply (≤ 15 hours) and unavailability of both emergency diesels

II.3 Secondary-side leaks and breaks

- Break of feedwater line
- Break of main steam line

II.4 In-plant fires and explosions

II.5 Failure of large components

- Effect of turbine failure

II.6 Other external events

- External fire
- High water
- Lightning

II.7 Load drop

- Failure of reactor building crane

A comparison of the PIEs from Germany for the HTR-Module in Table I-6 with the DBEs from the US in Table 9 for the MHTGR is not complicated by differences in the energy conversion as both are Rankine cycles utilizing a steam generator. However, the deterministic versus risk-informed approach to event selection. The PIEs are from the traditional, deterministic approach of assuming a PIE followed by the response of preselected safety-related SSCs. Since the DBAs that correspond to the initiating events from Germany have only SSCs responding that are safety related, a closer comparison is expected with the US DBAs provided in the right hand column of Table 12, that also only rely on safety related SSCs.

Another commonality between the MHTGR and HTR-Module is that the HPB is within a vessel system comprised of three high quality vessels including the cross vessel that has an inner hot duct within the return of the cold helium to the reactor vessel from the steam generator vessel. This is explicitly stated in the first entry under I.1 Primary system depressurization. Therefore,

the comparison of the MHTGR and HTR-Module DBAs shows notable commonality with primary system depressurization, SG leaks, and reactivity events.

I-2.3. Summary of the Comparison of Off-Normal Design Events from the U.S., Japan, and Germany

In summary, while the top level safety requirements in the prior section showed significant differences from country-to country, the off-normal events that are designed for show greater similarities, particularly, for the German HTR-Module and the U.S, MHTGR that both utilize a steam Rankine cycle.

ANNEX II. HTR-PM CONTAINMENT CONSIDERATIONS

Different HTR reactors have different implementation for the reactor building. Steel vessel type of containment in AVR and HTTR are special cases, prestressed concrete reactor vessel in THTR and Fort St. Vrain are also special arrangement. Nowadays, most of HTR have a reactor building with a rectangular shape, and is equipped with sub-atmosphere ventilation system, burst disc, and filtration system, with the concept of early direct release in depressurization accident and later filtration capability. This is different with PWR design, which normally has a leak-tight strong round reactor building (containment), combined with many associated supporting systems such as containment spray system. In the case of HTR, the reactor building, or part of this building (for example the reactor cavity), plus the sub-atmosphere ventilation system, burst disc, and filtration system, also carries out the function of third layer of barrier for radioactive retention, and the forth level of defense in depth, almost in same level as in PWR, although with different importance. Therefore, it also can be named as containment, or vented low pressure containment (VLPC) in China, or confinement in some cases.

In China, the main functions of VLPC are defined as: to provide shielding from reactor, to protect the power plant from external hazard, to provide suitable environment during normal operation, to reduce the radioactive release during and after accident by early direct release and later filtration. Although some functions for the building may be classified as safety related (for example radiation shielding, supporting of safety SSCs), the requirement for radioactive retention by VLPC is based on as low as reasonably achievable (ALARA) principle. This is mainly because of the release into the environment not exceeding the limit even if the filtration function failed, and the release being greatly reduced if filtration functions properly. The underline reason is, that most of the fission product is retained inside TRISO coated particle in the case of normal operation and accident condition, with excellent performance of TRISO fuel and proper design of reactor.

Different HTR plants can have different implementations of VLPC; for example, even in China, HTR-10, HTR-PM, and newly designed HTR-PM600 have slightly different implementations. In the case of HTR-PM600, corresponding to the fact that there are 6 Nuclear Steam Supply Systems (NSSS) modules in one large round reactor building. The new implementation of VLPC for HTR-PM600 is to treat the whole reactor building as the VPLC, and sub-atmosphere ventilation is applied to the whole reactor building, instead of each reactor cavity as in the case of HTR-PM and HTR-10. The reactor building also has the capability to withstand an air craft crash. Auxiliary systems for VLPC in HTR-PM600 will also be changed from that of HTR-PM accordingly.

ANNEX III.
SPENT NUCLEAR FUEL MANAGEMENT

(DELETED FOR THE PURPOSE OF GIF MEETING)

[III-1]

ANNEX IV.
**UK HAZARDS APPROACH: EXAMPLE USED ON SIZEWELL B AND THE
PROPOSED APPROACH TO COMBINED HAZARDS ASSESSMENT**

This report provides information on the UK Approach to Hazards as an example approach as used on Sizewell B, while in the following part the new approach to the Assessment of Combined Hazards is presented for information.

IV-1. EXAMPLE APPROACH AS USED ON SIZEWELL B

IV-1.1. Design Approach

The hazards design approach is to ensure that an NPP may be safely brought to, and maintained at a safe shutdown state following any design basis hazard. For internal hazards such as fire and flooding this is achieved by suitable segregation provisions. For external hazards such as earthquake and wind the requirement is to qualify the equipment to survive and function as required to achieve safe shutdown. The qualification level corresponds to the 10^{-4} p.a. return frequency for the external hazard.

The design approach adopted in the treatment of the design basis hazards is conservative such that the plant has the capability to withstand hazards more severe than the design basis hazard levels. This is achieved using conservative design methods and by the specification of conservative stress and deformation limits. Thus, in practice, the design has a capability to withstand greater than design basis internal and external hazards. The extent to which is achieved is addressed quantitatively by a Hazards Probabilistic Safety Assessment (PSA).

The safety case must demonstrate that sufficient plant is available during and following a hazard to achieve safe shutdown and post trip cooling. The systems, structures and equipment required are shown to have the capability to perform their safety related functions together with the occurrence of the specified hazard.

IV-1.2. Implementation of the Overall Design Approach

The design approach to hazard protection is based on the following principles.

- i. Prevention of the hazard.
- ii. Limitation of consequences of the hazard.
- iii. Mitigation of consequences of the hazard.

The overall design objectives are to ensure that any design basis hazard does not cause:

- i. A fault, or combination of faults which are beyond the design basis of the engineered safety features.
- ii. A plant fault or combination of faults in conjunction with a reduction in the redundancy of any of the systems required to perform the safety functions to such a degree that the frequency of an unsafe condition arising is unacceptable.
- iii. An unacceptable release of activity either due to a reactor fault, mal-operation or from stored fuel or radioactive waste.

- iv. A plant fault to be induced at a frequency significantly higher than it might occur independently of the hazard.

IV-1.3.General Hazard Principles

These objectives are addressed by implementing the following General Hazard Principles during the design process.

- i. Segregation and qualification of equipment must be adequate to allow safe shutdown with sufficient reliability following a design basis hazard. Exceptions to this criterion should not normally exceed a frequency of 10^{-8} p.a.
- ii. A hazard should not cause a significant increase in the frequency of a design basis or a beyond design basis fault.
- iii. A hazard should not cause a significant increase in the magnitude of a design basis or a beyond design basis fault.
- iv. A hazard should not cause two or more design basis faults.
- v. A hazard should not cause the loss of more than one train of hot and intermediate shutdown equipment.
- vi. A hazard should not cause the loss of more than one primary protection system train.
- vii. A hazard should not cause the loss of more than one half of the secondary protection system.
- viii. A hazard should not cause the loss of more than one half of category 2 systems which require segregation for that hazard.
- ix. A hazard should not prevent the short-term operation of more than one half of cold shutdown equipment (short term is up to 72 hours).
- x. A hazard should not prevent the long-term operation of more than one active hot shutdown components (long term is more than 72 hours).
- xi. Local hazard detection and mitigation features must be adequate for the frequency and magnitude of the hazard considered.
- xii. A local hazard must not propagate beyond a room unless the consequences can be shown to be acceptable.
- xiii. Equipment required to detect or mitigate a hazard or the consequence of that hazard must be provided with suitable protection or qualification.
- xiv. Hazards resulting from failures of non-safety items must not lead to safety classified equipment failing at a higher frequency or greater magnitude than otherwise assumed for the safety case.
- xv. A hazard must not cause safeguards equipment to fail at a higher frequency or greater magnitude than otherwise assumed for the safety case. (Note that consequential hazards were also considered.)
- xvi. Releases of activity into a room and potential contamination spread must be considered in the design of the plant.
- xvii. Protection of personnel must be considered in the design of the plant.

IV-1.4.Design Process

During the design process the hazards that are to be assessed are established using a screening process and those hazards that are considered to merit further assessment are defined.

As the design develops, the detailed implementation of hazard protection is refined and this is reflected back into the project design and construction process.

The strategy for protecting against hazards is intentionally conservative and utilises the defence-in-depth concept.

After the design of the station is essentially complete, a composite and extensive review process is undertaken to assess the compliance of the design.

In addition, a PSA for hazards should be undertaken and where applicable plant damage states identified in an equivalent fashion to plant faults. This will allow the contribution to station risk arising from hazards to be evaluated. This includes assessments for some hazards of beyond design basis hazard magnitudes to confirm the robustness of the deterministic design process.

IV-2. PROPOSED APPROACH TO THE COMBINED HAZARDS ASSESSMENTS

Presentation at the Institution of Mechanical Engineers Conference “Fit for Purpose Safety Cases in the Nuclear Industry”, Birmingham, 6th June 2017.

<https://events.imeche.org/ViewEvent?code=SEM6482>

ANNEX V. MHTGR FUNCTIONAL CONTAINMENT

Functional Containment Summary – FINAL(Jim)

Nuclear reactor designs include a containment, which must adequately retain radionuclides to meet the onsite and offsite radionuclide dose acceptance criteria for the event sequences identified for the design. Containment configurations must also have the capability to establish controlled leakage and controlled release of delayed accident source term radionuclides.

Modular HTGRs provide for this retention function through the use of a multiple barrier approach that can be referred to as a “functional containment”. A functional containment is defined as a set of barriers taken together, that effectively limit the physical transport and release of radionuclides to the environment. Functional containment is relied upon to ensure that radiological releases at the site boundary meet regulatory limits for the range of event sequences that are considered.

In addition to radionuclide retention, barriers within the functional containment are utilized to maintain the passive cooling geometry between the core and the ultimate heat sink, provide a pathway for the release of reactor helium in the event of depressurization accidents, and limit air ingress.

The modular HTGR functional containment consists of five barriers, as summarized below, including the primary attribute or purpose of each barrier:

1. Kernel
 - Retention
2. TRISO Coating
 - Retention
3. Fuel Element Matrix Graphite
 - Retention
4. Helium Pressure Boundary
 - Retention
 - Passive heat removal
 - Maintain core geometry
5. Reactor Building
 - Retention
 - Structural protection of passive heat removal configuration
 - Pathway for the release of reactor helium
 - Limit air ingress

An upper tier performance standard for the functional containment for modular HTGRs is that it should ensure the integrity of the fuel particle barriers (i.e., the kernel and coatings of the TRISO-coated fuel particles) rather than to allow significant fuel particle failures and then need to rely extensively on other mechanistic barriers (e.g., the helium pressure boundary and the reactor building). This standard is generally characterized by the following attributes:

- Ensuring during normal operation radionuclide retention within the fuel with relatively low inventory released into the helium pressure boundary (HPB).
- Limiting radionuclide releases to the environment to meet onsite and offsite radionuclide dose acceptance criteria and related regulatory requirements at the facility boundary, with margin, for a wide spectrum of off-normal event sequences.
- Maintaining the capability to establish controlled leakage and controlled release of delayed accident source term radionuclides.

REFERENCES TO ANNEX V

- [V-1] Functional Containment Performance Criteria for Non-Light Water Reactors, NRC SECY-18-0096, September 2018
- [V-2] Guidance for Developing Principle Design Criteria for Non-Light-Water Reactors, NRC Regulatory Guide 1.232 – Rev. 0, April 2018.

ANNEX VI. CONFINEMENT CONCEPT USED FOR HTR-MODULE

VI-1. CONFINEMENT ENVELOPE

The confinement envelope of the HTR-MODULE acts in conjunction with other barriers to the release of radioactive substances to minimize the radiological impact on the environment of accident conditions.

The following features fulfill confinement functions in the HTR-MODULE:

- Reactor building
- Secured subatmospheric pressure system
- Building pressure relief System, HVAC systems isolation

Because the fuel elements themselves provide reliable retention of radioactive fission products and because helium is used as the primary coolant, no special demands are made of the confinement envelope since compliance with the limits as stipulated in

the Federal German Radiological Protection Ordinance is assured even without additional fission product retention facilities.

In principle, it is possible to discharge the primary coolant unfiltered directly into the environment in the event of accident-induced depressurization of the primary system.

Nevertheless, it is intended to minimize the radiological impact on the environment of a depressurization accident by filtering the escaping primary coolant in the secured subatmospheric pressure system before discharge from the vent stack. The design basis for the system is a primary system break with a diameter less than or equal to 10 mm.

For larger postulated breaks which lead to a significant pressure build-up in the reactor building, building pressure is relieved by direct discharge of primary coolant into the environment. After depressurization, the pressure relief ports are closed; further discharges via the secured subatmospheric pressure system can be filtered.

VI-2. REACTOR BUILDING

No leaktightness demands are made of the reactor building as part of the confinement envelope or of its penetrations and entrances. The maximum leakage of the reactor building is 50 vol.-%/d with differential pressure of 2 mbar. A subatmospheric pressure system and a pressure relief system are provided in the reactor building merely to minimize the impact on the environment after a postulated break in the primary system. The entrances to the building consist of interlocked doors, which assure that a directional air flow in the building can be maintained at all times.

Since it is possible to relieve building pressure directly into the atmosphere in the event of a depressurization accident, it is unnecessary to design the building for high interior pressures.

The reactor building is designed for the pressures and temperatures which are postulated to occur in the event of a primary coolant pipe break or main feedwater line break and building pressure relief to the environment.

The primary cavities and outside walls of the reactor building are designed against a pressure of 0.3 bar. The shielding effect of the primary cells provides reliable protection of the environment from direct radiation.

VI-3. SECURED SUBATMOSPHERIC PRESSURE SYSTEM

Areas containing primary coolant pipes are monitored for helium leakage. If specified limits are exceeded, the affected area of the building is switched from the unfiltered air exhaust system to the secured subatmospheric pressure system.

The secured subatmospheric pressure system is designed for a volumetric flow rate of 2.5 m³/s and receives accident power back-up. The system is equipped with a High Efficiency Particulate Air (HEPA) filter and an activated-carbon adsorber.

Design of the secured subatmospheric pressure system for postulated external events is not envisaged.

VI-4. BUILDING PRESSURE RELIEF SYSTEM

The arrangement of the compartments in the reactor building and the HVAC Systems assure that air flows from rooms with low airborne activity levels into rooms with higher airborne activity levels in order to limit any spread of radioactive materials in the building under normal operating conditions.

As far as possible, the secured subatmospheric pressure system is used to minimize radioactive releases in the event of accidents.

Relief ports fitted with rupture discs or dampers which connect the modular units with the reactor hall are provided to control depressurization accidents (DN 65).

Building pressure itself is relieved into the environment via the vent stack. Each port is equipped with:

- A pressure relief damper which opens at a response pressure of approximately 0.1 bar and closes automatically after pressure equalization.
- An isolation damper which is normally open and can be closed manually after a depressurization accident in case the pressure relief damper sticks open.

Subatmospheric pressure can thus be restored after pressure relief.

ANNEX VII. **LICENSING PROCEDURE CONCEPT FOR THE HTR-MODULE**

VII-1. DESCRIPTION OF THE PLANT SUBJECT TO THE LICENSING PROCEDURE

The HTR-MODULE power plant is a thermal power plant for the cogeneration of electricity and process steam. The process steam can be used for a wide variety of applications in the chemical industry, for example, or for tertiary oil extraction.

The place of the fossil-fired heat source of conventional plants is taken in the HTR-MODULE by two nuclear steam supply systems (modular units). Each modular unit comprises one high-temperature reactor, one steam generator and one primary gas blower. The heat liberated by nuclear fission in the HTR is transported from the reactor through the coaxial duct to the steam generator by the primary coolant, helium, which is circulated by the primary gas blower. In the steam generator, the heat is transferred to the water/steam conversion system which is designed and operated as a purely non-nuclear plant. Auxiliary and supporting systems connected to the primary system are provided for operation of the reactor; furthermore, safety of the reactor is assured by systems which fulfil the task of keeping loadings on components and structures within acceptable limits under accident conditions and which minimize the impact of accidents on the operating personnel and the environment. The reactor auxiliary systems are installed in the reactor building and in the reactor auxiliary building. The cooling loads in the power plant are served by closed cooling water systems which remove the rejected heat to service water systems. Operation of the power plant is controlled and monitored from the central control room. Normal operation is largely automated by means of open- and closed-loop controls which correct minor deviations from required setpoints. In the event of major deviations, automatic operational limiting controls restore the plant to the condition requisite for operation. If trip limits set in the reactor protection system are reached, the necessary safety-related countermeasures are automatically initiated.

VII-2. LICENSING PROCEDURE/SAFETY CONCEPT REVIEW

The licensing procedure for the concept of the HTR-MODULE nuclear power plant was intended to confirm the licensability of the plant and thus to establish a solid legal basis for further planning work.

VII-2.1. Basis of Licensing Procedure

The construction and Operation of nuclear powerplants in the Federal Republic of Germany are subject to national legislation and ordinances such as the Atomic Energy Act (AtG), Atomic Licensing Procedure Code (AtVfV), Radiological Protection Ordinance (StrISchV) and are also governed by engineering rules and regulations. The licensing procedure for power plants is conducted in stages. At the first stage an application is submitted for a preliminary ruling on the concept pursuant to Article 7 of the AtG which would be preceded by a preliminary positive overall evaluation of construction of the plant and operation thereof pursuant to Article 18 of the AtVfV. If no actual site has been selected, the application for a preliminary ruling is based on Article 7a (basis of the licensing procedure for the HTR-MODULE power plant).

As in the case of an application for the construction and operation of a nuclear power plant (Article 7) the requirements of Article 3 of the AtVfV have also to be satisfied. For a preliminary ruling pursuant to Article 7a of the AtG, emphasis is placed on:

- the Safety Analysis Report,
- supplementary plans, drawings and descriptions, and
- information on measures provided for protection of the plant against sabotage.

VII-2.2. Time Schedule of the Licensing Procedure/Safety Concept Review

In April 1987 an application for a licence on the conceptual design was docketed by the State of Lower Saxony (FRG). In May 1987 the licensing authority nominated experts competent in the various fields of engineering. The main expert was the "Technischer Überwachungsverein Norddeutschland (TÜV Hanover) ", who subcontracted parts of the nuclear steam supply system and radiological issues to die "Technischer Überwachungsverein Rheinland (TÜV Cologne)". The work for the licensing procedure was then initiated in May 1987 on the basis of the Safety Analysis Report. By the end of 1987 about 100 supplementary reports, including detailed drawings, stress analysis reports, reports on seismic design and fuel technology, had to be submitted. Further additional reports and other documents (approx. 150) were supplied in 1988. The submitted Safety Analysis Report was reviewed and reconsidered in June-August 1988 in the light of the standpoint of the licensing authority and the experts and to incorporate changes in system design. The corresponding changes to die Safety Analysis Report to take into account the results achieved in the licensing procedure were agreed, the Safety Analysis Report was revised and submitted in September 1988. The draft review report was completed in mid-1989. However, the application for a preliminary ruling on the concept was withdrawn and the licensing procedure discontinued by the Lower Saxon Ministry for the Environment in April 1989 as the legal case for a non-site-specific licensing procedure in Lower Saxony was questionable.

The order placed with TÜV Hanover for the safety review was therefore cancelled by the Lower Saxon Ministry for the Environment. By this time the review had reached an advanced state of progress and great interest was expressed in the work being completed. Consequently, TÜV Hanover was retained in May 1989 to complete the safety concept review without reference to a specific licensing procedure as part of a research and development contract on behalf of the Federal Minister for Research and Technology (BMFT) and to document the results. The draft safety review report then followed in July 1989. The final version was completed in late 1989.

Excepted from this review were the fire protection concept and aspects of protection against sabotage. The Lower Saxon Ministry for the Environment placed orders for separate reviews for these topics. A review of the fire protection concept was performed by the Civil Engineering Institute (IBMB) of the University of Brunswick, and a review of the plant security concept by the Reactor Safety Association (GRS). These reports were completed within the scope of the licensing procedure in February and March 1989.

At the request of the Lower Saxon Ministry for the Environment, the Reactor Safety Commission (RSK) started reviewing the concept of the HTR-MODULE in late 1988. The concept was presented at numerous sessions of the RSK subcommittees for HTRs and electrical

engineering. These subcommittees completed their consultations in September and October 1989. The RSK announced its recommendation on the HTR-Module in March 1990 (published in "Bundesanzeiger" Nr. 81, dated 28.04.1990).

VII-3. SAFETY ANALYSIS REPORT

For light-water reactors the contents of Safety Analysis Reports are governed by a Bulletin of the Federal Ministry for the Interior (BMI) with the title "Contents Checklist and Format for a Standard Safety Analysis Report for Pressurized Water Reactor and Boiling Water Reactor Nuclear Power Plants". For the HTR-MODULE this "Contents Checklist" was modified to reflect:

- the lack of a site,
- the application for a preliminary ruling, and
- the new technology.

Table VII-1 shows the contents of the HTR Module Safety Analysis Report.

TABLE VII-1. CONTENTS OF THE SAFETY ANALYSIS REPORT.

1. Site
2. General Design Features of the HTR Module Power Plant
3. Power Plant
4. Radioactive Materials and Radiological Protection
5. Power Plant Operation
6. Accident Analysis
7. Quality Assurance
8. Decommissioning
9. Waste Management Provisions
10. Guidelines and Technical Rules

Since no decision on an actual site has yet been made, Section 1 of the Safety Analysis Report contains postulated site conditions to the extent necessary for evaluation of the concept and for arriving at a positive preliminary overall evaluation. The postulates made for this purpose are representative of numerous potential sites in Germany. Section 2 of the Report contains a collation of general design features of the HTR-MODULE power plant on which the application for a preliminary ruling on the concept pursuant to Article 7a of the AtG is based. Table VII-2 shows the contents of Section 2 of the Safety Analysis Report.

TABLE VII-2. CONTENTS OF SECTION 2 OF SAFETY ANALYSIS REPORT.

2 General Design Features of the HTR Module Power Plant
2.1 Introductory Remarks
2.2 Characteristic Safety Features
- Barriers against Release of Radioactivity
- Inherent Safety

2.3 Technical Design Features

- Reactor (fuel elements, reactor core, control and shutdown systems)
- Nuclear Steam Supply System (pressure vessel unit, primary System and steam generator isolation)
- Confinement Envelope
- Residual Heat Removal
- Emergency Power Supply
- Reactor Protection System
- Remote Shutdown Station

2.4 Nuclear Classification and Quality Requirements

2.5 Summary of Design Basis Events

2.6 Postulates and Measures for In-Plant Events

2.7 Postulates and Measures for External Events

Sections 3 to 9 of the Safety Analysis Report contain descriptions of the power plant and operation thereof in accordance with the requirements stated in the above mentioned "Contents Checklist" of the BMI, with modifications specific to the HTR-MOULE. For purposes such as providing a basis for a preliminary overall evaluation, these sections give greater details on the concept described in Section 2 for postulated, exemplary conditions of service. Since the HTR-MODULE has been designed as a universally usable energy source, detailing of the concept for actual conditions of service would in essence only have a bearing on:

- overall layout and non-nuclear structures,
- steam power conversion system, and
- electrical systems (grid connection).

In contrast, actual conditions of service and site conditions would hardly affect

- reactor core,
- nuclear steam supply system, and
- reactor auxiliary systems,

and, by definition, have no influence on the general design features described in Section 2. Section 10, titled "Guidelines and Technical Rules", gives a survey of the application or adaptation of the Bulletins of the BMI and of the KTA Safety Standards to the HTR-MODULE.

VII-4. RESULTS OF REVIEWS

VII-4.1. Fire Protection Review

In addition to the fire protection concept described in Section 2.6 of the Safety Analysis Report, a wide range of, in part, very detailed additional documents were submitted to the expert, in this case the Civil Engineering Institute (IBMB) of the University of Brunswick. The report, completed in February 1989, approves the fire protection concept. The few requirements and

recommendations can be fulfilled without problems and have no effect on plant technology and safety.

VII-4.2. Plant Security Concept Review

The plant security concept-the entirety of provisions for protection of the plant and operation thereof against sabotage-was reviewed by the Reactor Safety Association (GRS). The report, completed in March 1989, approves the concept and concludes that the inherent features of the HTR-Module warrant less stringent security precautions than those taken for LWRs.

VII-4.3. RSK Recommendation

In summary, the RSK concludes that the HTR-MODULE concept conforms to the state of the art and has positive safety features even in the beyond design realm. The HTR-MODULE is capable of fulfilling the safety related licensing requirements of the Federal Republic of Germany

VII-4.4. Safety Concept Review

The main document for the safety concept review by TÜV Hanover was the Safety Analysis Report, above all Section 2 which describes the general features of the HTR-MODULE central to the concept. The opinion of the expert as given in the Safety Concept Review and also special features and design principles are given below following the same breakdown as Section 2 (see Table VII-2).

Section 2.2 (SAR): Characteristic Safety Features

- The engineering configuration and nuclear design of the HTR-MODULE is such that, even in the event of postulated failure of all active shutdown and residual heat removal systems, the fuel temperature stabilizes at 1620°C. No appreciable release of radioactivity from the fuel elements occurs below this temperature.
- Active residual heat removal systems which limit the loadings on components and structures surrounding the core can fail for several hours without the allowable limits being exceeded.

Assessment in report: approved.

Section 2.3 (SAR): Technical Design Features

- Fuel element
 - Coatings (TRISO).
 - Enrichment ($8 \pm 0.5\%$).
 - 1620°C max. temperature, minimal release through SiC layer.
 - Particle failure curve (manufacturing defects: $< 6 \times 10^{-5}$, irradiation-induced: $< 2 \times 10^{-4}$, accident-induced: $< 5 \times 10^{-4}$).

Assessment in report: approved.

- Reactor core

- By virtue of core design, fuel temperature stays below 1620°C under all accident conditions even on loss of active residual heat removal.
- Due to uranium content of 7 g per fuel element the reactivity excursion on water inleakage is less than on inadvertent withdrawal of all reflector rods.
- Design for unrestricted load cycling between 50 and 100%.

Assessment in report: approved; restriction on part load operation below 50% and during the running-in phase (because no analyses submitted for this case): limits on absorber ball level in storage vessels.

- Shutdown systems

- Shutdown by absorbers in reflector holes.
- Shutdown by 6 rods and 18 absorber ball units.
- Location of rod drive mechanisms in RPV.
- Location of all absorber ball unit components needed for shutdown in RPV.

Assessment in report: design and configuration approved. Reactivity balances for equilibrium core approved but those for running-in phase up to several months have relatively small margins; consequences: reactor power might be below of 200 MW at first.

- Pressure vessel unit

- Consists of reactor pressure vessel, gas duct pressure vessel and steam generator pressure vessel inclusive of valve banks on RPV, nozzles of steam generator pressure vessel.
- Offset configuration, thus limiting natural circulation in the primary system.
- Leak before break, assured safety for entire pressure vessel unit.

Assessment in report: approved after discussion of dissimilar-metal weld and change of material for main steam nozzle. Requirement: preservice pressure test to include RPV nozzles.

- Primary and secondary system isolation

- Primary system by two valves in each line of which only one operated by reactor protection system(failsafe).
- Secondary system by two valves in each line (failsafe) both actuated by reactor protection system whenever reactor is shut down. Consequently, rest of secondary system outside reactor building has no functions important to safety.
- Primary System overpressurization protection: two safety valves; secondary System: one safety valve backed up by steam generator relief System.

Assessment in report: approved.

- Confinement envelope

- Consisting of reactor building and other features (secured subatmospheric pressure system, building pressure relief system, HVAC systems isolation).
- Normal Operation: no filtering.
- At overhauls: filtering by exhaust air filtering system(aerosols).

- During major depressurization accident (non-isolable DN 65 line): unfiltered venting through two dampers to vent stack.
- Other depressurization accidents: possibility of filtering by subatmospheric pressure system (iodine filter).
- Environmental impact of all accidents far below limits prescribed in Art. 28.3 of the Radiological Protection Ordinance even without active measures taken or filtering; consequently, no containment necessary.

Assessment in report: approved.

Requirement: higher grade exhaust air filtering system.

- Residual heat removal
 - Provided by secondary system, cavity coolers, helium purification system.
 - On loss of active cooling, residual heat removed from core to cavity coolers solely by thermal conduction, radiation and natural convection.
 - Secured component cooling system, two-train.
 - With cavity coolers intact and loss of core cooling, core can run hot for lengthy period of time (15 h) without design limits for RPV and concrete of reactor cavity being violated.
 - External supply can be connected to cavity coolers in the event of severe accident conditions.

Assessment in report: approved (see emergency power supply below for restriction).

- Emergency power supply
 - Two trains served by two diesel generator sets, started by operational sequencing controls or by hand.
 - DC buses (e.g. reactor protection system) battery buffered for two hours.
 - Reactor system can sustain loss of power for at least fifteen hours (loss of auxiliary power supply, failure of diesel generator sets) without design limits being violated.
- Assessment in report: approved. Restriction: quality assurance for diesels must be so strict that the diesel generators can certainly be started within the fifteen-hour period.

- Reactor protection system
 - Few process variables.
 - Three protective actions always actuated on shutdown (reflector rod drop, blower trip, steam generator isolation); additionally, steam generator pressure relief on tube failure and primary system isolation during depressurization accidents.
 - All actions failsafe.
 - Station blackout longer than two hours can be sustained since all protective actions are initiated, plant is transferred to safe condition, reactor protection system has no further tasks to fulfil.

Assessment in report: approved. Source-range neutron flux instrumentation to be of reactor protection grade.

- Remote shutdown station
 - Located in reactor building (designed for aircraft crash, blast wave).

- Power supply by diesels in switchgear building.
- On station blackout, single train battery power supply for fifteen hours, possibility of connecting up external power supply after that.
- Monitoring functions only, except for absorber ball shutdown system initiation by hand.

Assessment in report: approved

Section 2.4 (SAR): Nuclear Classification and Quality Requirements

- Definition of classification criteria and establishment of classes for
 - pressure-retaining and activity-carrying systems,
 - HVAC systems,
 - hoists and cranes,
 - structural steelwork,

- Assignment of systems to classes.

- Identification of quality requirements for classes.

Assessment in report: assignment criteria correctly selected; assignment of systems as correct as possible at the present status. Final assessment of assignment of systems and identification of quality requirements cannot be performed until construction licensing procedure.

Section 2.5 (SAR): Summary of Design Basis Events

- Listing of representative accidents by analogy with "Accident Guidelines for Pressurized Water Reactors".

Assessment in report: approved. Listing of all design basis events is complete, delimitation from hypothetical realm correct.

(Remark on BDBEs: BDBEs were not part of the SAR. They were discussed separately with the authorized experts.)

Section 2.6 (SAR): Postulates and Measures for In-Plant Events

- Break postulates:

Primary system: one DN 65 connecting line (2A)

Secondary system: main steam or feedwater line (2A)

Steam generator tubes: one tube (2A)

- Concurrent main steam line and steam generator tube rupture not postulated

Assessment in report: approved. Requirement: ISI of steam generator tubes

Section 2.7 (SAR): Postulates and Measures for External Events

- Building design for earthquake:
 - Reactor building
 - Reactor building annex
 - Switchgear building
 - Reactor auxiliary building; only sealed concrete pit and its main load-bearing structures

- Building design for aircraft crash, blast wave:
 - Reactor building
- System design for earthquake, aircraft crash,
 - Pressure vessel unit
 - Steam generator tubes
 - Reactor coolant piping as far as isolation valves
 - Secondary system inside reactor building
 - Remote shutdown station
 - Components of reactor protection system inside reactor building
 - Shutdown systems inside reactor pressure vessel
 - Cavity coolers
- System design for earthquake:
 - Secured closed cooling system
 - Secured service water System
 - Reactor protection System
 - Emergency power systems

Assessment in report: approved.

VII-5. NEW REGULATIONS SINCE 1980IES/ LESSONS LEARNED FROM FUKUSHIMA

VII-5.1. New Regulations since 1980ies

All the revisions of ordinances and rules in Germany would not lead to any major changes in the general concept of the HTR-MODULE. Of course, in detail depending on new materials and/or progress in engineering and construction changes in the component/system design would occur, especially I&C architecture would be different.

Regarding aircraft crash, the postulation of large civil aircraft crash, instead of military aircraft crash, may lead to changes in the building structure of the reactor building. The HTR-MODULE design of the 1980ies was capable to withstand the impact of a Boeing 747 type flying at moderate speed.

BDBEs have to be part of the SAR in contrast to the 1980ies, when they were discussed separately.

VII-5.2. 5.2 Lessons Learned from Fukushima

A common consensus is the autarky time of at least 72 hours for BDBEs regarding residual heat removal, etc. In the HTR-MODULE of the 1980ies this time span was given with 15 hours. The calculations in the 1980ies showed that no problems occur in residual heat calculations, including concrete temperatures, over the time up to 72 hours.

Only the capacity of the alternate power supply (batteries in the remote shutdown station) has to be enlarged to 72 hours.

ANNEX VIII. HTR-MODULE LICENSING BASIS EVENTS

In April 1987 the Company Siemens applied in the West German State of Lower Saxony for a concept licensing procedure to be initiated for an HTR-MODULE Nuclear Power Plant. In addition to a safety analysis report, numerous additional papers were submitted to the authorized experts. In April 1989 the proceedings were suspended for political and legal reasons. The safety concept review was continued by order of the Federal Minister for Research and Technology and completed at the end of 1989.

The classification of events for the HTR-MODULE has been incorporated into the safety concept evaluation as part of the Safety Analysis Report by the authorized experts. In summary, the experts came to the conclusion that the list of all design basis accidents is complete, the threshold against the hypothetical range has been selected correctly, and the measures for risk minimisation in the events of Class III have been met to the required extend.

According the German Atomic Energy Act, precautions have to be taken against damage arising from the construction and operation of nuclear installations, which are in compliance with the state of the art and science. In particular, it has to be ensured that in the event of activity release under accident conditions the design basis values specified in § 28 Section 3 of the Radiation Protection Ordinance are not exceeded. In addition to that, it has to be shown that in the event of accidents not only the radiation exposure of the plant personnel and environment is limited, but also that the following two fundamental protection objectives are met:

- Integrity of the barriers against activity release
- Operability of safety-relevant systems

For verifying that these requirements are met, all accidents relevant with regard to these protection objectives have to be analysed for the HTR-MODULE.

VIII-1. SPECIFICATION OF CLASSES OF EVENTS

In analogy to the German RSK Accident Guidelines for Nuclear Power Plants with pressurised water reactors issued on October 18, 1983, the accidents and events are classified as follows:

Class I events: Accidents which are relevant with respect to their radiological effects on the environment and for which technical precautions against damage have to be taken.

Class II events: Accidents for which technical precautions against damage have to be taken and which thereafter are no longer relevant with respect to their radiological effects on the environment.

Class III events: Events that are not classified as design basis accidents because of their low risk and thus are not covered by the accident guidelines, against which, however, nevertheless measures for risk minimization are taken.

VIII-1.1. Class III Events

These Class III events include:

- Aircraft impact
- External shock waves from chemical reactions
- Anticipated transients without scram (ATWS)

Event specific to the HTR-MODULE: (These events are not part of the Safety Analysis Report due to German Ordinances. They are discussed with the authorized experts separately.)

- Long-term failure of auxiliary power supply (> 15 hours) and not-availability of accident diesel power supply.
- Air ingress
- Water Ingress

In the event of external impacts, the protection objectives are met by the design of the reactor building and a few systems such as e. g. shutdown systems and cavity coolers. The measures which have to be taken after 15 hours, at the earliest, are limited to external feed of the cavity coolers and energy supply of the remote shutdown station. Even in case of long-term failure of the auxiliary power supply and non-availability of accident diesels only these two measures are required. The ATWS events are controlled solely by interruption of the primary coolant flow via the negative temperature coefficient of reactivity.

VIII-1.2. Class I and II Events

In analogy to the accident guidelines, it has to be determined under which aspects the events of Class I and II have to be considered. A distinction is made between categories:

- SI: Design of components and structures against accident loads required to ensure stability or integrity
- AS: Design of engineered safety systems or countermeasures required
- RA: Radiologically representative, consequences to be analysed

The accidents of the HTR-MODULE to be analysed under the aspect of "SI" mainly include:

- Seismic events: Design of buildings (e. g. reactor building, switchgear building) and systems (e. g. pressure vessel unit, core structure, shutdown systems, secondary circuit within the reactor building)
- Live steam line rupture: Mechanical stability of steam generator, integrity of the SG heat transfer tubes, pressure build-up in the reactor building.
- Rupture of an ND 65 helium line: Pressure build-up in the reactor building or in the reactor auxiliary building.

The AS events include several groups of events:

- Pressure loss in the primary system
 - ND 65 leak without possibility of isolation: Design of building depressurisation system.
 - Rupture of measuring line (ND 10): Design of secured subatmospheric pressure system (filter line).
- Damage of steam generator heat transfer tubes
 - Failure of one steam generator tube: Design of measures for limitation of water ingress into the primary system.
- Reactivity accidents
 - Withdrawal of all reflector rods: Reactor core design.
 - Water ingress: Reactor core design.
- Disturbances in the main heat transfer system
 - Failure of auxiliary power supply and operation of accident diesels: Design of intermediate cooling system.
 - Short-term failure of auxiliary power supply (< 2 hours) and non-availability of the accident diesels: Design of the batteries (instrumentation and control equipment of the switchgear building), design of cavity coolers.
- Long-term failure of auxiliary power supply (>15 hours) and non-availability of the accident diesels: Design of batteries (remote shutdown station), design of cavity coolers.

In order to limit the number of all radiologically relevant accidents to the representative ones (RA events), the following classification of possible events was adopted:

- Failure of non-radioactive systems:
 - Failure of heat transfer tubes in secondary system, loss of integrity of primary system in case of failure of helium purification system, response of primary system depressurisation system: Filtered activity release to the environment.
 - Rupture of live steam line in secondary system, integrity of primary system maintained: No activity release to the environment.
- Failure of radioactivity containing systems:
 - Systems carrying primary coolant - leak can be isolated from reactor pressure vessel: Activity release into the reactor building or reactor auxiliary building, release to the environment can be filtered.
 - Systems carrying primary coolant - leak cannot be isolated from reactor pressure vessel: Activity release into the reactor building, filtering of release to the environment in the initial phase not possible.
 - Liquid waste system - leak into the reactor auxiliary building: Activity release into the building, filtering of release to the environment not possible.
- External impacts
 - Consequential failure from seismic impact - leak inside the reactor auxiliary building, which can be isolated, and simultaneous leakage in the liquid waste system: Activity release into the building, ground release via building leakage.

Out of the number of radiologically relevant accidents resulting from this scheme the accidents which are representative in respect of initiating events, release point, release potential, release path (RA events) have been determined and analysed:

- Leak in a connection line between reactor vessel and primary circuit shut-off valve
- Leak in a measuring line carrying primary coolant
- Failure of a steam generator tube and long-term failure of helium purification system
- Rupture of a line of the helium purification system in the reactor auxiliary building
- Leakage of a tank of the liquid waste system
- Failure of helium purification system and liquid waste system in the reactor auxiliary building due to seismic impact.

Calculation on the radiation exposure of the environment after such accidents resulted in dose rates which even without consideration of the existing filter systems were far below the design reference values specified in § 28.3 of the Radiation Ordinance.