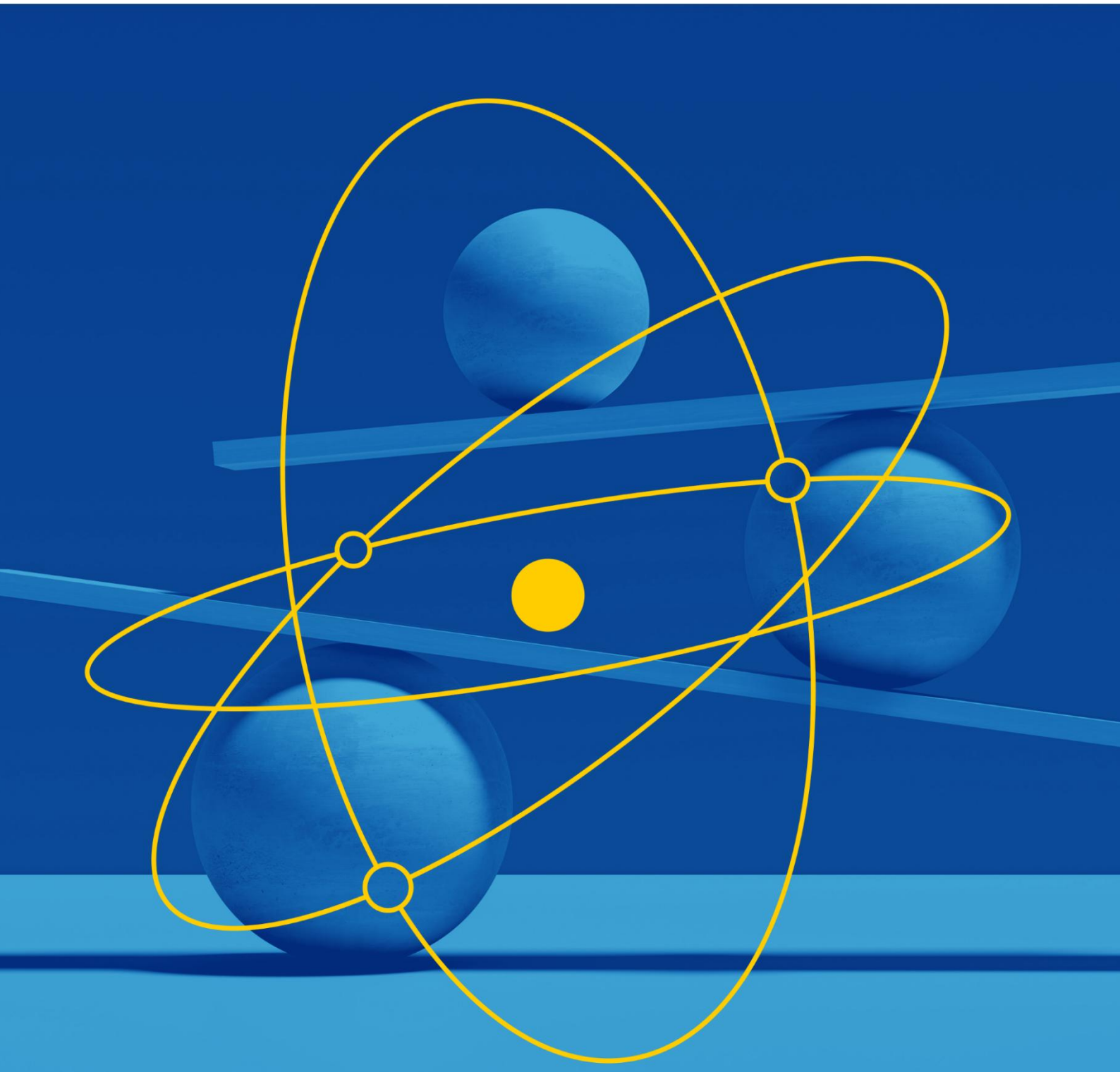
GEN IV International Forum
Expertise | Collaboration | Excellence

Case Study of Safety, Security and Safeguards (3S) Interfaces for a Very High Temperature Reactor System



December 2025

GIF/PRPPWG/2025/002

(This page has been intentionally left blank)

DISCLAIMER

This report was prepared by the GIF 3S collaborative sub-group composed by members of PRPPWG, RSWG and the SSC of the VHTR. Neither GIF nor any of its members, nor any GIF member's national government agency or employee thereof, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by GIF or its members, or any agency of a GIF member's national government. The views and opinions of authors expressed therein do not necessarily state or reflect those of GIF or its members, or any agency of a GIF member's national government.

(This page has been intentionally left blank)

Abstract

The Generation IV International Forum (GIF) [1] was established as a co-operative international endeavour aimed at developing the research necessary to evaluate the feasibility and performance of fourth generation nuclear systems (Gen-IV systems), with the objective of making them available for industrial deployment by 2030. The potential conflicts and synergies at the interfaces between the regimes of safety, security, and safeguards (2S and 3S interfaces) in nuclear facilities are increasingly apparent. With Gen-IV systems seeking to move towards deployment, it is an opportune moment to further develop guidance on how to effectively identify and address these 2S and 3S interfaces during the earliest design stages. To this end, the GIF Proliferation Resistance & Physical Protection Working Group (PRPPWG), the GIF Risk & Safety Working Group (RSWG) and the GIF Very High Temperature Reactor System Steering Committee (VHTR-SSC) conducted a bottom-up 3S interface case study exercise on a notional pebble bed VHTR modular reactor. The objective of this exercise was to identify and characterize the 2S and 3S interfaces on the reference system, thereby developing some technology-neutral guidelines for the identification and characterization of 2S and 3S interfaces. This report presents a summary of the outcomes of this work.

The primary objective of the bottom-up case study is to offer some guidance to designers and vendors interested in implementing a 3S-by-design (3SBD) approach to the development of a Gen-IV advanced modular reactor. The 3S interfaces can be analysed pairwise (3 x 2S), or in an integrated fashion at the simultaneous intersection of all three regimes (3S). Although the concept of 3SBD is not novel, there is a need among designers to foster both security and safeguards by design to integrate with the already existing safety by design culture. An intermediate analysis of the existing interfaces using a 3 x 2S framework can facilitate the realization of 3SBD culture among designers more effectively and expeditiously. Consequently, the case study considers both 2S and 3S interfaces.

Among the most critical aspects of the interfaces considered are those that would compromise the objectives of each S regime, potentially leading to conflicts between each regime. This typically arises from the sharing of space, time, or resources between the regimes. Equally, analysing how each interface shares space, time, or resources can either mitigate these conflicts or bring positive synergistic outcomes. The optimized sharing of space, time and resources holds special relevance for small or advanced modular reactors that occupy smaller spaces and/or utilize fewer resources compared to traditional large nuclear installations. These critical aspects distilled from the case study, are summarized in this report. Those interested in a “quick-start guide” to this case study can jump to the tables provided in Section 8.2 which summarize the critical aspects of the interfaces identified in the case study; the sections in Chapter 7. provide in-depth explanation of these interfaces. Further, more general characteristics of the interfaces are found in Section 8.3 that provide principles for identifying interfaces in a nuclear facility.

It has been observed that many of the interfaces identified in this report, except for a security-safeguards interface particular to the fuel pebble handling system, possess generic characteristics that can be readily applied to other Gen-IV energy systems. Although this study is not completely comprehensive in coverage of all 3S interfaces of a pebble bed VHTR reactor system, many of the critical aspects of the 3S interfaces identified should be easily generalizable to other reactor types.

List of Authors

Bryan van der Ende	PRPPWG	Canadian Nuclear Laboratories, Canada
Luca Ammirabile	RSWG	European Commission Joint Research Centre
Lap Cheng	PRPPWG	Brookhaven National Laboratory (retired), United States
Chris Chwasz		Idaho National Laboratory, United States
Benjamin Cipiti	PRPPWG	Sandia National Laboratory, United States
Giacomo Cojazzi		European Commission Joint Research Centre (retired)
Thomas DeGuire		Sandia National Laboratory, United States
David Hummel	RSWG	Canadian Nuclear Laboratories, Canada
Guido Renda	PRPPWG	European Commission Joint Research Centre
Ryan Stewart		Idaho National Laboratory, United States
Gerhard Strydom	VHTR-SSC	Idaho National Laboratory, United States

Acknowledgements

Members of the GIF 3S collaborative sub-group are to be thanked for their contributions to this work. Special thanks are due to GIF Technical Secretary Seoyeong Jeong (OECD-NEA) for detailed record-taking of 3S sub-group meetings, and to GIF Technical Secretary Alexiei Ozeretzkovsky (OECD-NEA) who ably readied the final manuscript for publication. The authors accept full responsibility for the content of this report, which does not necessarily reflect the views of the reviewers of this document. Nevertheless, the feedback from reviewers and the resulting discussions were instrumental in refining the quality of this work. The reviewers include members of GIF (Tanju Sofu – RSWG, Argonne National Laboratory), members of the IAEA (Shahen Poghosyan, Carolynn Sherer), and members of the nuclear industry (Eben Mulder – X-Energy, Margaret Ellenson – Kairos Power).

Table of Contents

List of Figures

List of Tables

List of Acronyms

3S	Safety, Security, Safeguards
3SBD	3S by Design
ACS	Active Cooling System
ALARA	As Low As Reasonably Achievable
AOO	Anticipated Operation Occurrence
BDBE	Beyond Design Basis Event
BUMS	Burn-Up Measurement System
CAS	Central Alarm Station
C/S	Containment and Surveillance
DBA	Design Basis Accident
DBE	Design Basis Event
DBT	Design Basis Threat
DCSA	Defensive Cybersecurity Architecture
DEC	Design Extension Conditions
DEPO	Design and Evaluation Process Outline
DIQ	Design Information Questionnaire
ECP	Entry Control Point
EPCC	Equipment Protection Cooling Circuit
ET	Event Tree
FT	Fault Tree
FHS	Fuel Handling System
FHSS	Fuel Handling and Storage System
FKMP	Flow Key Measurement Point
GIF	Generation-IV International Forum
HPB	Helium Pressure Boundary
HTR	High Temperature Reactor
HTR-PM	High-Temperature Gas-cooled Reactor Pebble-Bed Module
HX	Heat Exchanger
IAEA	International Atomic Energy Agency
IKMP	Inventory Key Measurement Point
LBE	Licensing Basis Event
LEU	Low Enriched Uranium
MBA	Material Balance Area
MHSS	Main Heat Sink System
MPS	Main Power System

MPS-HPB	Main Power System Helium Pressure Boundary
NMAC	Nuclear Material Accounting and Control
NNSA	National Nuclear Security Administration
PBMR	Pebble Bed Modular Reactor
PBR	Pebble Bed Reactor
PCU	Power Conversion Unit
PIDAS	Perimeter Intrusion Detection and Assessment System
PIN	Personal Identification Number
PPS	Physical Protection System
PRA	Probabilistic Risk Assessment
PRPPWG	Proliferation Resistance & Physical Protection Working Group
PRS	Pressure Relief System
RCS	Reactivity Control System
RCCS	Reactor Cavity Cooling System
RPV	Reactor Pressure Vessel
RSS	Reserve Shutdown System
RSWG	Risk and Safety Working Group
SAS	Secondary Alarm Station
SCRAM	Safety Control Rod Axe Man
SeBD	Security By Design
SMR	Small Modular Reactor
SQ	Significant Quantity
SSC	Structures, Systems, and Components
SSS	Startup/Shutdown System
TRISO	TRi-structural ISOtropic
UCO	Uranium oxicarbide
VAI	Vital Area Identification
VHTR	Very-High-Temperature Reactor
VHTR-SSC	Very High Temperature Reactor System Steering Committee

(This page has been intentionally left blank)

1. Introduction

The Generation IV International Forum (GIF) was established as a co-operative international endeavor aimed at developing the research necessary to evaluate the feasibility and performance of fourth generation nuclear systems (Gen-IV systems), with the objective of making them available for industrial deployment by 2030. In many cases, these Gen-IV systems are intended to be deployed in non-nuclear weapon states which must adhere to the provisions of three regimes: nuclear safety, nuclear security, and international safeguards[1]. The scope definitions of each of these regimes can be found in relevant glossaries of the International Atomic Energy Agency (IAEA) [1] [2]. Given that these regimes rely on the same technical system, they invariably interact with one another. These interactions give rise to potential conflicts and synergies in interfaces between the regimes of safety, security, and safeguards (2S and 3S interfaces). These conflicts and synergies are discussed, for example, in Refs. [3], [4] and [5]. Minimizing the conflicts and leveraging the synergies will be most efficiently achieved by considering the interfaces in the earliest design stages. With Gen-IV systems moving towards deployment, it is an opportune moment to further develop guidance on how to effectively identify and address these 2S and 3S interfaces during the earliest design stages.

To this end, a sub-group of the GIF Proliferation Resistance and Physical Protection Working Group (PRPPWG), the GIF Risk and Safety Working Group (RSWG), and the GIF Very High Temperature Reactor System Steering Committee (VHTR-SSC) conducted a bottom-up 3S interface case study exercise on a notional pebble bed Very-High-Temperature Reactor (VHTR) modular reactor. In GIF, the RSWG plays a key role in providing methodologies and analysis that supports the Generation IV goal of improved safety of Generation IV Nuclear Energy Systems. Similarly, the PRPPWG was established to develop, implement, and foster the use of an evaluation methodology to assess Gen-IV Nuclear Energy Systems with respect to the proliferation resistance (PR) and physical protection (PP) goal. Through its activities, the PRPPWG aims to foster a “PR&PP by Design” culture among Gen-IV designers and policy makers. The VHTR SSC oversees projects in GIF that cover a broad range of topics related to VHTRs. The alignment of the goals of each of these three groups under the GIF umbrella with the content of the proposed 3S case study made the groups ideal collaborators in this work.

The objective of the 3S case study was to identify and characterize the 2S and 3S interfaces on the reference system, thereby potentially developing some technology-neutral guidelines for the identification and characterization of 2S and 3S interfaces. The bottom-up approach of this case study focused on identifying these interfaces for a particular reactor type by starting with established details of a VHTR reference design, uniquely contrasting with many top-down 3S interface studies from the past that have focused on no particular reactor type (see, for example, Refs. [4] to [7]). This case study relied upon open literature data regarding VHTR-type reactors for its reference design information (see, for example, Ref. [7]), as well as associated data required for safety, security and safeguards assessments applied to the reference design. The study aimed to answer questions such as:

- What are the critical aspects of the identified interfaces?
- What are the differences and commonalities among the interfaces in their conflicts and synergies?
- Can technology-neutral bottom-up guidelines be formulated for identifying and characterizing these interfaces?

[1] Nuclear weapon states signatory to the non-proliferation treaty have only very limited international safeguards requirements, typically through voluntary offer agreements.

By answering such questions, it is intended to provide guidance to reactor vendors and designers wishing to apply a 3S-by-design approach to the development of Gen-IV systems.

There are some characteristics of the pebble bed VHTR system that are of particular interest for an exercise such as this case study:

- The design is a continuous refuelling, pebble-bed reactor, with a very large number of small fuel pebbles and a non-static inventory. From a safeguards perspective, this characteristic makes it a quasi-bulk-handling facility instead of an item facility like almost the entirety of today's power reactor fleet. In addition, the quasi-bulk-handling nature of the system has the potential to influence how the Nuclear Material Accounting and Control (NMAC) system of the facility – a security-safeguards interface – will be designed and operated.

- While prototypes have been built and operated, pebble-bed reactors in commercial operation are only in China today, and operational experience in safeguards and security for these systems is fairly limited compared to traditional designs. On the other hand, the design has been studied for many years [8], and there is some past operational experience on technological demonstrators providing a sound literature and documental basis for the 3S sub-group exercise.

- VHTR pebble-bed reactors running on TRi-structural ISOtropic (TRISO) particle fuel have the potential to be designed with inherent safety features. While inherent safety does not remove the need for robust security and safeguards measures, it does influence and potentially reduce the scope of safety-security and safety-safeguards interfaces. For example, it has been seen how security timeline analysis and response force strategy is influenced by the length of the grace period for loss of forced cooling: the longer grace period provided by the pebble bed VHTR affords a longer response time to safety and security responders. It has also been seen that some intrinsic features of the pebble bed VHTR that enhance safety have the potential to reduce possible diversion and misuse strategies of relevance to safeguards.

- A unique aspect of VHTR pebble-bed reactors is that in the course of normal operations, the pebble fuel elements may become damaged through friction and mechanical movement in the continuous flow of the fuel elements in the reactor core. As such, means must be put into place to identify damaged fuel elements, separate them out before they are recirculated in the reactor, and stored separately from spent fuel elements [9]. This consideration has implications for both safety and safeguards.

In chapter 2 of this report, the scope and definitions of each "S" regime of safety, security, and safeguards are carefully defined, along with some further details concerning the approach of this study. This is followed by chapter 3, providing details of the chosen reference design, based largely on a notional design of a VHTR pebble bed reactor (PBR) provided by the GIF VHTR-SSC [10]. Chapters 4 through 6 describe individual safety, security and safeguards assessments of this reference design carried out by the 3S interfaces case study sub-group, prior to examining the 3S interfaces of the reference design. These individual assessments were used as input for identifying and characterizing 2S and 3S interfaces, described in chapter 7. Chapter 8 summarizes key insights learned from this study, addressing the questions mentioned above. Chapter 9 provides conclusions and final remarks.

2. Safety, Security, Safeguards and their Interfaces: Scope and Interfaces Identification Approach

Nuclear safety, security, and safeguards are three distinct disciplines that play a crucial role in the operation of nuclear energy systems. According to the IAEA, nuclear safety refers to "the achievement of proper operating conditions, prevention of accidents and mitigation of accident consequences, resulting in protection of workers, the public and the environment from undue radiation risks" [1].

Nuclear security is defined as "the prevention and detection of, and response to, criminal or other intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities or associated activities" [1].

Lastly, nuclear safeguards are defined as "a set of legal instruments, technical measures and administrative procedures implemented by the IAEA … to verify that nuclear material, nuclear facilities and/or other items subject to safeguards are not acquired or used for proscribed purposes" [2].

The three regimes of nuclear safety, security, and safeguards have different backgrounds, legal mandates and manners of implementation. Nuclear safety has been a primary concern since the inception of nuclear energy, with a strong focus on preventing accidents and mitigating their consequences. Nuclear security, while existing since the very beginning of nuclear energy exploitation, gained additional prominence in the post-9/11 era, with an increased focus on preventing intentional unauthorized acts involving nuclear material. Nuclear safeguards, which date back to the 1960s, was usually considered during or immediately prior to the construction phase, but only marginally during early design stages.

In considering nuclear safeguards and nuclear security, a careful distinction should be made between international safeguards, international security, and domestic safeguards and security in some countries like, e.g., the United States. Table 2.1 below, produced by the US National Nuclear Security Administration (NNSA), summarizes key parameters involved in this distinction. In this document, “security” and “safeguards” will refer to international security and international safeguards, respectively.

Table 2.1. Aspects to each of international safeguards, international security, and domestic safeguards & security in the U.S. [12]

	International Safeguards	Domestic Safeguards & Security in the U.S.	International Security
Goals	Ensure peaceful uses of nuclear material & facilities, and detect and deter diversion or misuse	Prevent, detect, and respond to theft of nuclear materials or facility sabotage	
Threats	Country (State actors)	Malicious actors (e.g., terrorists) / individuals	
Legal Basis	Atomic Energy Act, Nuclear Nonproliferation Act, Nuclear Non-Proliferation Treaty, Safeguards Agreements, Nuclear Suppliers Group guidelines	U.S. law and Code of Federal Regulations	Local laws, and regulations, the Convention on the Physical Protection of Nuclear Material and its Amendment, UNSCR 1540, INFCIRC/225/Rev5
Lead Agency	IAEA	U.S. NRC	Country’s regulatory authority
Provision of MC&A Data	Provided by the country to the IAEA	Provided by the licensee/operator to the U.S. Nuclear Materials Management Safeguards System (NMMSS)	Provided by the licensee/operator to the country’s regulatory authority
Methods	Material Control and Accounting (MC&A)		
	Containment and surveillance, design information verification, and inspections	Physical security, cybersecurity, and personnel security	
	Safeguards by Design (SBD)	Security by Design (SeBD)	

The fundamental nuclear safety objective is to protect people and the environment from harmful effects of ionizing radiation [13]. Each of nuclear security and safeguards share this common objective. However, each of these regimes, also has its own focus and measures.

Understanding the scope and measures of each discipline is essential when considering the interfaces between the disciplines. Table 2.2 summarizes the scope and measures of each regime.

Table 2.2 Scope and measures of safety, security, and safeguards.

Discipline	Scope	Measures
Safety	The achievement of proper operating conditions, prevention of accidents and mitigation of accident consequences, resulting in protection of workers, the public and the environment from undue radiation risks [1]. *Challenge* Accident due to system failure, human error, or natural disaster [14].	Safety measures are designed to [13]: 1. Control both the radiation exposure of people and the release of radioactive material to the environment. 2. Restrict the likelihood of events that might lead to a loss of control over a nuclear reactor core, nuclear chain reaction, radioactive source or any other source of radiation. 3. Mitigate the consequences of such events if they were to occur.
Security	The prevention and detection of, and response to, criminal or other intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities or associated activities [1]. *Challenge* A person or group of persons with motivation, intention and capability to commit a malicious act [1][13].	Security measures are intended to [1]: 1. Prevent a nuclear security threat from completing criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities, or associated activities. 2. Detect or respond to nuclear security events. An integrated set of nuclear security measures forms a nuclear security system.[2]
Safeguards	A set of legal instruments, technical measures and administrative procedures implemented by the IAEA … to verify that nuclear material, nuclear facilities and/or other items subject to safeguards are not acquired or used for proscribed purposes [2].	Safeguards measures seek to [2][16]: 1. Verify the correctness and completeness of state's declarations. 2. Deter the spread of nuclear weapons by the early detection of the misuse of nuclear material or technology. Safeguards measures include [2]:

[2] The phrasing for the intention of security measures reflects the view of light water reactor technology in which site recovery after a security event is not considered timely compared to radioactive release. Advanced reactor technologies can have different timelines that can include site recovery in security strategies. As such, preventing damage in a security event need no longer be a metric for success. Rather, a useful design metric is to maintain radioactive releases from a security event below an established threshold [15].

Discipline	Scope	Measures
	Challenge State actors with intent of acquiring or using nuclear material for proscribed purposes.	1. Nuclear material accountancy. 2. Containment and surveillance. 3. Design information verification. 4. Inspections and reports. 5. Complementary access.

Despite their different histories and implementation, the three regimes will interact with each other, as they rely on the same technical infrastructure. It is essential to consider these interactions early in the design stages of new nuclear energy systems to ensure that the 3S interactions maximize potential synergies and minimize conflicts among the three regimes. In this “3S by Design” (SBD) process, the requirements of each of safety, security, and safeguards are considered as design inputs to ensure a proper integration in the plant system design. As design and construction planning decisions are made in the 3SBD process with such inputs considered, tensions as well as synergies between these input requirements become evident in how time, resources, and facility space are allotted in the facility deployment design and planning. It is important to be aware of these synergies and tensions in the early design stages so that the synergies can be capitalized upon, and potential conflicts are mitigated in the design and planning decisions that are made.

Interfaces between each of safety, security, and safeguards can be considered as decision points where issues from at least two of these disciplines should be considered. The issues include potential consequences of both unintentional events and intentional acts, and the interests of each involved discipline in providing preventative and protective elements against those events and acts. The activities involved in interface management can occur at strategic and operational levels [17]. The 3S interfaces can be considered pairwise (as 2S interfaces: safety – security, security – safeguards, safety – safeguards), or with all three disciplines simultaneously. The interests of each discipline at each decision point can work together synergistically or be in conflict with each other. In resolving conflicts, a risk-informed, balanced approach should be taken to ensure the best overall solution for all three disciplines [17].

In considering these interfaces and resolving potential conflicts, the fundamental objectives of nuclear safety, security and safeguards need to be met. The fundamental objective of nuclear safety, which was previously described and is ultimately shared by nuclear security and safeguards, cannot be neglected or sacrificed under any circumstance. That is to say, the manner in which interface issues are managed must ensure that the consequences of the issue at hand and how any response to it is managed do not result in exceeding acceptable radiological risk to facility workers, the public, and the environment. In particular, when considering the consequences of potential safety or security events, the acceptable radiological risk to facility workers, the public, and the environment cannot be different, irrespective of the cause of the initiating event of a radiological release. As such, an established acceptable level of radiological exposure to facility workers, the public, and the environment can serve as a starting point to define an acceptance criterion for 3S interface management, while aiming at continuous improvement in line with the ALARA (As Low As Reasonably Achievable) principle [18].

Early consideration of 3S interactions is crucial to ensure that the design of new nuclear energy systems takes into account the potential synergies and conflicts among the three regimes. This can be achieved through an integrated approach, where safety, security, and safeguards are considered simultaneously. However, this would require a complete paradigm change in the designers' safety-focused culture, which is typically very strong in safety, strong in security but usually considered only at later design stages, and weak in international safeguards, which are often overlooked. This will differ from the perspective of a designer that prioritizes each of

three regimes in an integrated fashion that is consistent with the deployment strategy for the design.

A practical way to transition towards an integrated approach is to adopt a 3×2S approach. This approach involves leveraging on a designers' strong safety culture and introducing security and safeguards considerations starting from their interaction with safety. The safety-security, safety-safeguards and security-safeguards interfaces can then be analysed to identify proper 3S interfaces.

The 3 x 2S approach offers several advantages over an integrated approach in the interim. Firstly, it allows designers to leverage on their existing safety culture. Secondly, it ensures that the design of new nuclear energy systems that aim at hitting the market in the near future takes into account the potential synergies and conflicts among the three regimes, which is essential for ensuring their efficient operation. Lastly, it provides a practical way to transition towards an integrated approach, which can be achieved in a graded manner.

Some efforts have sought the direct integration of security considerations into the safety organization, such as the concept of cyber-informed engineering [19]. Cyber-informed engineering is the integration of cybersecurity in the early stages of the design process and the engineering life cycle to include cybersecurity in the conception, design, development, and operation of physical systems to prevent or mitigate cyber-enabled attacks. In this way, cybersecurity is intended to be another metric of success for designers when developing facility instrumentation and control architecture, without the necessary integration of a cybersecurity staff member into the design team.

There are many contexts in which these 3S interfaces arise. These contexts can include management systems, site selection and justification, emergency response, normal operating procedures, defence in depth and designation of system safety components, reactor design, irradiated fuel storage system, fuel design manufacturing and management, instrument and control systems design, human factors engineering, access control, and use of risk-informed approaches. In this work, a generalized PBR serves as a case study to enable consideration of as many of these contexts as possible within the extent of information available for this study.

In chapter 1, it was mentioned that this case study follows a bottom-up approach. In general, a bottom-up approach begins with a detailed examination of individual components, systems, and processes. It examines specific operational practices and facility-level requirements, which are then synthesized to develop higher-level policies and objectives. The focus is on building an understanding from the ground up, ensuring that all elements contribute effectively to the overall objectives of each regime of safety, security, and safeguards. In the context of the present case study, this method allows the examination of each regime separately, followed by an analysis of their interfaces sequentially by examining each pair of the three regimes. It is anticipated that certain aspects of a generic pebble bed VHTR reference design will reveal interfaces connected to all three regimes.

In contrast, a top-down approach for a case study begins with a high-level analysis of the overall system and its objectives. This method emphasizes a comprehensive understanding of the overall system and the coordination between different components to achieve the desired outcomes. The aim of a top-down approach is to identify key safety, security, and safeguard requirements and then drill down into specific components and processes to ensure these requirements are met. Due to the absence of a complete design for a pebble bed VHTR in this study, as well as the absence of a well-defined framework or regulatory requirement for 3S interfaces to work with, a bottom-up approach for this case study was chosen over the top-down approach.

In keeping with this bottom-up approach, chapter 3 will provide a general description of the GPBR-200 for this case study. This will be followed by informed assessments on the safety,

security, and safeguards aspects of this facility. Each of these assessments will first be conducted individually in chapters 4 through 6 to ensure an in-depth understanding of the goals, measures, and aspects for each regime. Following these individual assessments, the 2S and 3S interfaces are explored more thoroughly in chapters 7 and 8.

3. Reference Design

This work utilizes a generalized PBR with a target power of 200 MWth (denoted as the GPBR-200), approximately 100 MWe, to provide a reference for determining safety, safeguards, and security by design (3SBD). Its design has the characteristic of a continuous fuelling regime where fuel spheres, which are also called pebbles, enter from the top of the reactor and move through the core to be discharged at its bottom. The primary coolant is helium that is heated by flowing downward (from top to bottom of the core) around the fuel spheres in the core and then moves to the steam generator where it transfers the heat to the water before being circulated back into the reactor core to be heated again. The heat transferred from the hot helium to the water in the steam generator converts said water into steam that can then be used for electricity generation, co-generation or other processes.

3.1. Core Description

The GPBR-200 core is derived from previous work described in Refs. [20] and [21], which draws its geometry and material properties from current and past designs found in the literature, including the HTR-PM [22], Xe-100 [23], and PBMR-400 [24] . Reactor specific information will be provided in this document as well as contextual ranges to allow for a comparison across multiple designs. Operating parameters for the GPBR-200 are shown in Table 3.1.

Helium is used as the primary coolant, where typical inlet and outlet temperatures are 260 °C (533 K) and 750 °C (1023K) respectively, and a pressure of 6.0 MPa is assumed in the primary cooling loop. Under these conditions, the necessary flow rate of helium through the core would be around 79 kg/s.

Table 3.1. GPBR-200 Design parameters.

Parameter	**Value**
Thermal Power (MW_{th})	200
Pressure (MPa)	6
Helium $T_{in,core}$ (°C)	260 (533 K)
Helium $T_{out,core}$ (°C)	750 (1024 K)
He mass flow (kg/s)	79
Active core height (m)	8.93
Core radius (m)	1.2

PBRs utilize fuel pebbles, which encapsulate thousands of smaller coated fuel kernels within them. The GPBR-200 fuel kernels utilize a uranium oxicarbide (UCO) TRISO fuel. Pebbles within a PBR typically have a constant diameter, which has been fixed at 6.0 cm in recent years. For the GPBR-200, the fuel pebbles have a diameter of 6.00 cm, including a 1.0 cm thick graphite shell. The graphite shell surrounds a graphite matrix with TRISO particles randomly dispersed throughout the matrix. Figure 3.1Figure 3.1 shows the progression from the fuel kernel to the fuel pebbles. Each TRISO particle contain five layers, detailed in Table 3.2, where the multiple layers help mitigate the diffusion of fission products out of the pebble.

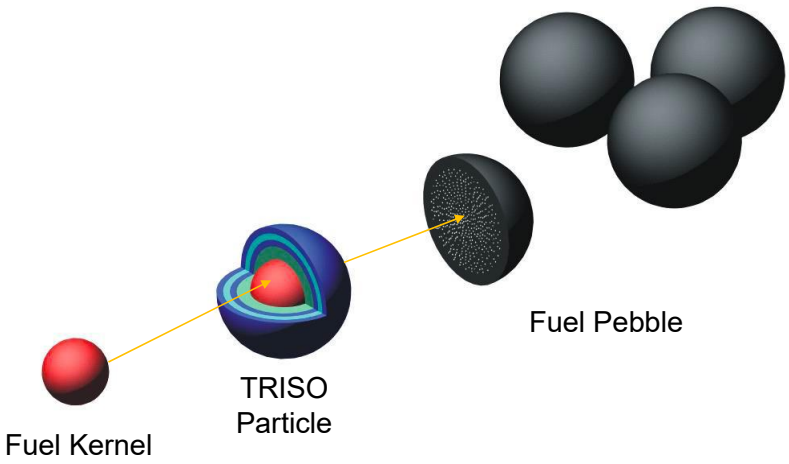


Figure 3.1. Fuel description from fuel kernel to fuel pebble.

Table 3.2. GPBR-200 TRISO geometry and material description.

Name	Outer Radius (cm)	Material
Fuel Kernel	0.0425	UCO
Carbon Buffer	0.0625	Carbon
Inner PyC	0.0705	Pyrolytic Carbon
SiC	0.0775	Silicon Carbide
Outer PyC	0.0855	Pyrolytic Carbon

For the GPBR-200, two fuel-pebble type exist: startup fuel and equilibrium fuel. Startup fuel utilizes an enrichment of 5.0-wt% U-235; this fuel is only used during the run-in phase of the reactor. Equilibrium fuel is enriched to 15.5-wt% U-235, which is used as equilibrium fuel for normal operations. The GPBR-200 model utilizes fuel pebbles with 18,687 fuel kernels (TRISO particles) in the graphite matrix; an assumption of the model is that the number of TRISO particles and their positions are fixed. This results in a TRISO packing fraction of 9.34% in each pebble. The masses of uranium and U-235 in an equilibrium fuel pebble intended for normal operation are 7.0 g and 1.085 g, respectively. The total number of pebbles in the GPBR-200 core is 208,997. Table 3.3 provides an overview of the special fissionable material data for the GPBR-200 along with ranges for contemporary and historical PBRs.

Table 3.3. Special nuclear material data for the GPBR-200 and contemporary PBRs.

	GPBR-200 Value	Contemporary Ranges
Fuel Form	UCO	UO_2, ThO
Mass of Uranium per Pebble (g)	7	6 – 8
Enrichment (wt%)	15.5	8.0 – 19.9
TRISO particles per pebble	18,687	15,000 – 20,000
Pebbles per core	208,997	200,000 – 500,000
Mass of U-235 in Core (kg)	226.8	150 – 275
Discharge Burnup (MWd/kg)	160	90 – 160
Average Number of Passes	6	6-17

During equilibrium operations, the core is a mixture of fresh fuel pebbles and fuel pebbles which have passed through the core multiple times. The average number of passes a pebble takes through the core before being removed from circulation and the discharge burnup of pebbles can have significant implications on 3SBD. For the GPBR-200 it is assumed that pebbles will, on average, pass through the core six times and achieve a discharge burnup near 160 MWd/kg. However, it is noted that other designs utilize upwards of 17 passes [25].

The pebble flow rate through the reactor results in an average of 1,300 pebbles exiting the active core region per day. Of these pebbles, roughly one sixth of them (approximately 220 pebbles) will have reached their maximum burnup and will be removed from the core and placed in spent fuel containers [20]. This means that roughly 220 fresh pebbles will need to be added to the core per day to make up for the discharged fuel. For the GPBR-200, the plutonium isotopes at discharge are given in Table 3.4.

Table 3.4. Plutonium vector for discharged fuel for the GPBR-200.

	Pu-238	**Pu-239**	**Pu-240**	**Pu-241**	**Pu-242**
Atom fraction	0.33	53.44	28.34	13.32	4.58

Fresh fuel would be stored on site, where it is assumed for this work that one year's worth of fresh fuel will be stored at a time. This results in approximately 80,000 pebbles being stored on site at a time. The storage of these fuel pebbles would be in fresh fuel canisters, where we assume each canister can hold 5,000 pebbles, resulting in 16-17 fresh fuel canisters being stored on site.

The GPBR-200 has an inner core radius of 1.2 m and an active core height of roughly 8.93 m, which feeds directly into a lower conus and finally a discharge chute which allows for pebbles to be passed to the fuel handling system. The height and diameter for PBRs can change, but these typically have a large height to diameter ratio to ensure optimal heat removal during accident scenarios. Along with this, some cores utilize a central graphite column, where pebbles pass through an annular cylinder.

The GPBR-200 has been used to model the run-in phase, determine equilibrium operations, calculate the decay heat, and determine transient behaviour for a PBR. To help provide context for the GPBR-200, Figure 3.2 shows an axial cut of the Serpent [26] model of the core. The reflector region of the core was segmented into 18 equal sub-regions, each containing a control guide tube or a safety guide tube, a helium riser channel, and dimples on the interior core area. The helium risers were located in the core to maintain a degree of realism in modelling the potential neutron streaming paths.

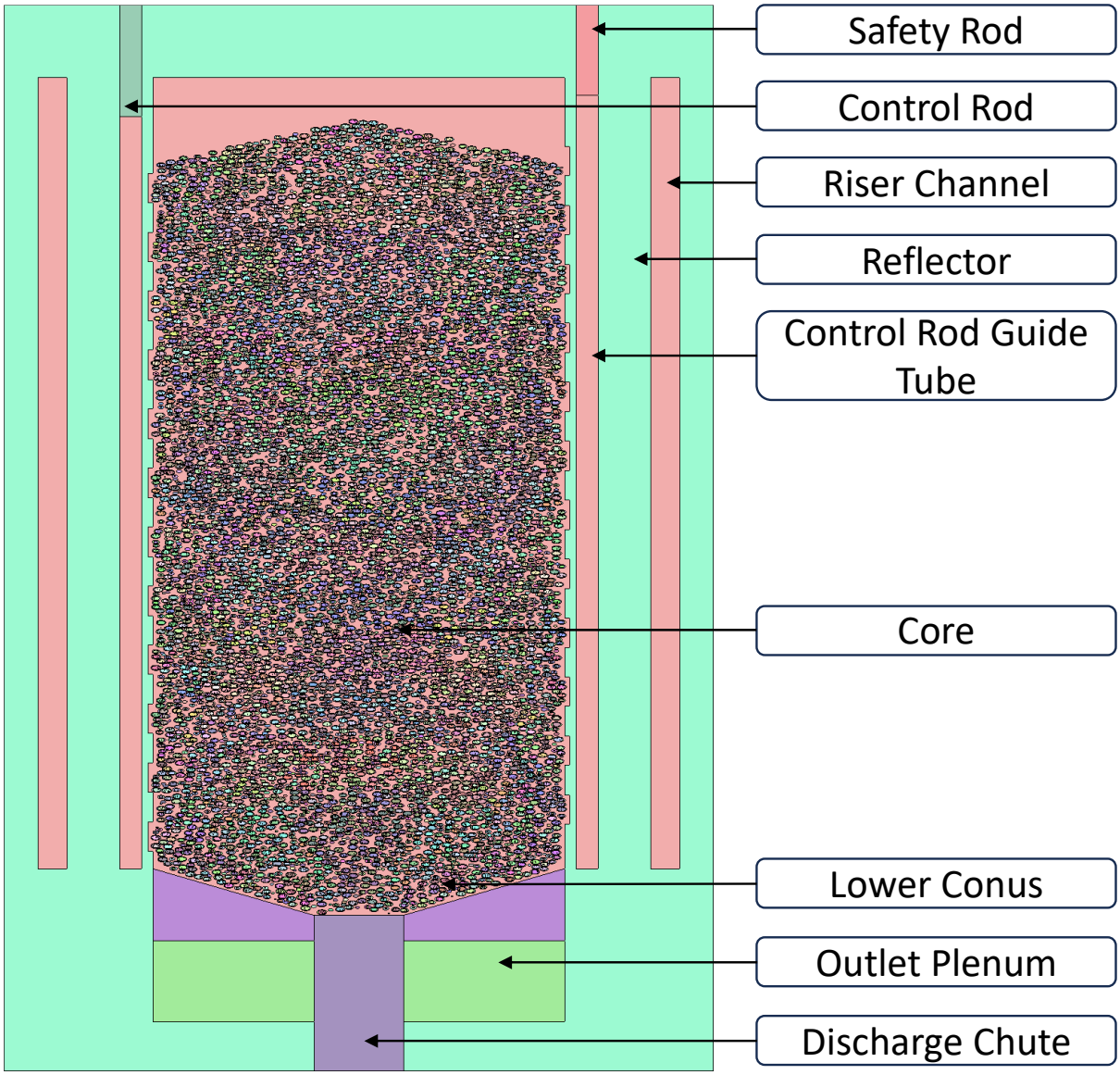


Figure 3.2. Axial slice of the GPBR-200 core region.

The GPBR-200 core has a relatively epithermal neutron flux when compared with traditional light water reactors. The normalized neutron spectrum can be seen in Figure 3.3 (flux is normalized to the total flux) and Figure 3.4 (normalized flux per unit lethargy). A further breakdown of this is given in Table 3.5, which shows the average neutron flux for the thermal, epithermal, and fast groups.

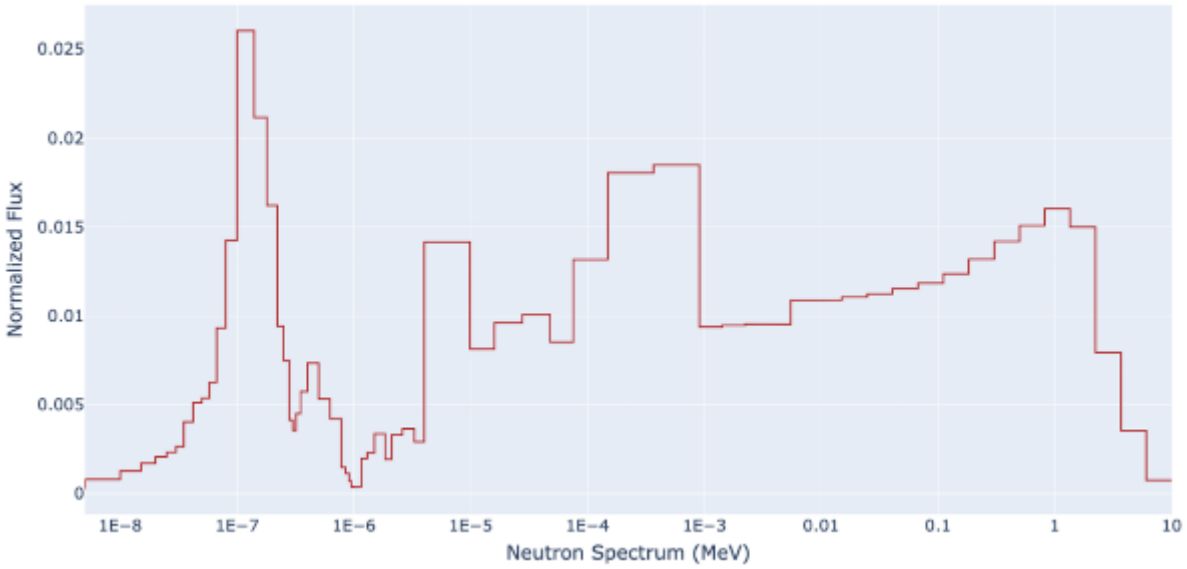


Figure 3.3. Normalized neutron spectrum for the GPBR-200.

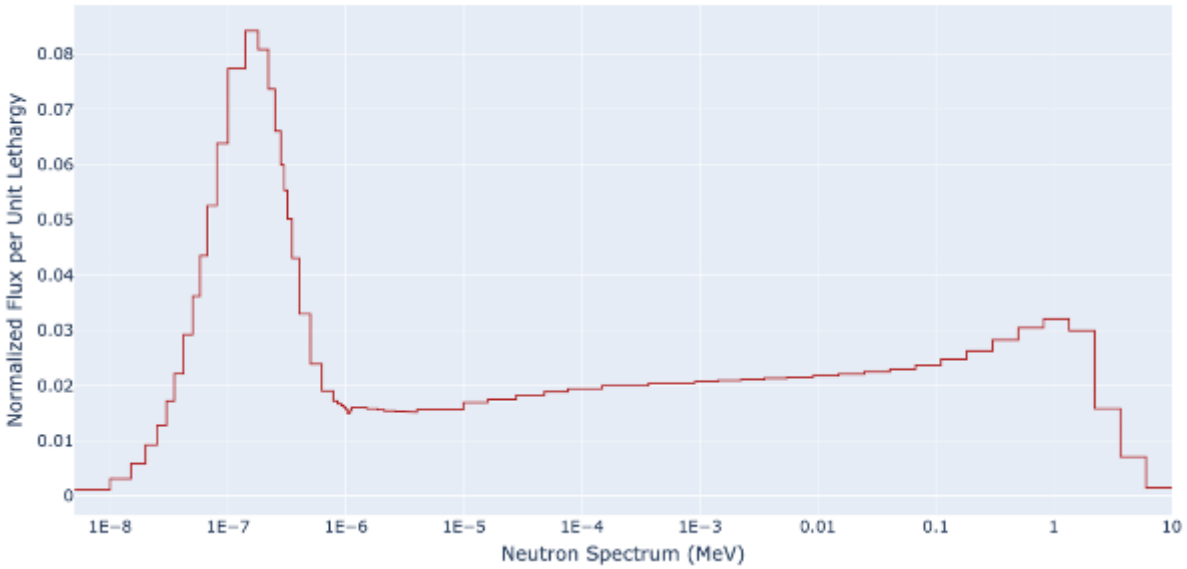


Figure 3.4. Lethargy averaged neutron spectra for GPBR-200.

Table 3.5. Average neutron flux for GPBR-200.

Energy Range (MeV)	**Flux (n/cm^{2}s)**
1E-11 – 6.25E-7	5.15E+19
6.25E-7 – 8.21E-1	5.07E+19
8.21E-1 – 1.00E+1	6.82E+19
Total	5.68E+19

The final aspect to describe in the GPBR-200 core is the expected thermal temperature profile. Given the thermal-epithermal energy spectrum and high temperature in the core, the temperature profile will have a large effect on core operations. This is due to the large Doppler reactivity coefficient, where increases in temperature will cause a subsequent decrease in

reactivity. Figure 3.5 shows an estimated temperature profile for the GPBR-200 [27]. The core has been axially and radially discretized for ease of comparison; upper and lower coni have been normalized to allow for a rectangular shape.

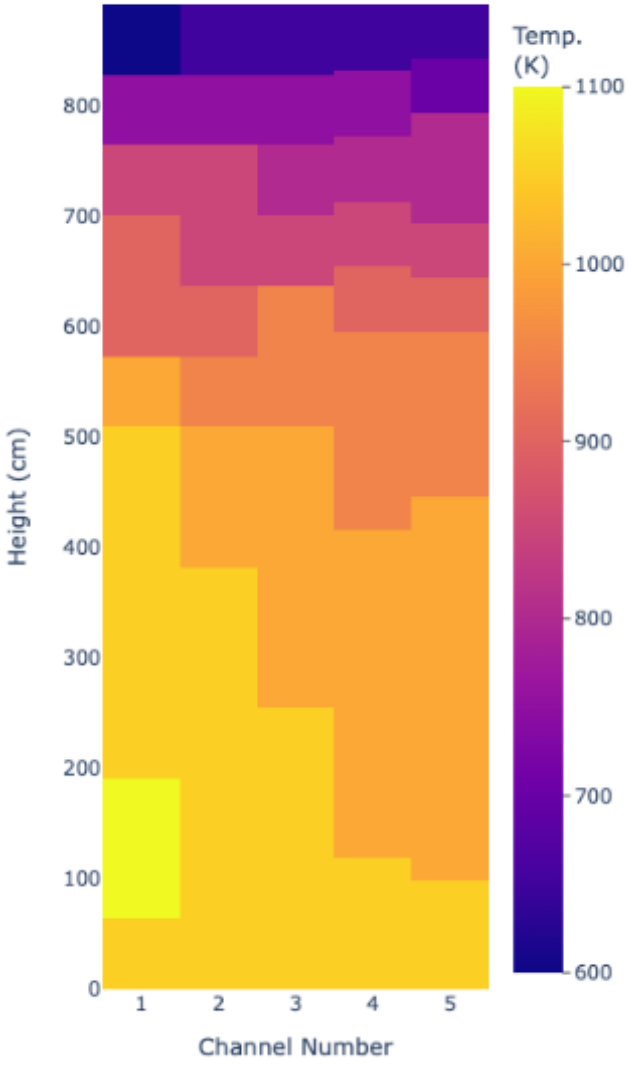


Figure 3.5. Temperature profile for the GPBR-200 at equilibrium.

3.2. Fuel Handling System

The Fuel Handling System (FHS) is one of the primary components for an operating PBR. The FHS described in this section is based on the technologies developed by HTR-10 and HTR-PM, where it is envisioned that the operation and maintenance of this system will be similar between reactor designs [28]. The FHS has several major tasks associated with it during equilibrium operations:

1. Perform fuel pebble loading (insertion) and unloading (removal)
2. At removal from the core, measure the burnup for each pebble
    a. Discharge spent pebbles (pebbles which reached a threshold burnup limit)
    b. Recirculate non-spent pebbles
3. Remove defective or undersized pebbles
    a. Discharge these to a separate area than spent pebbles
4. Extract pebbles for post irradiation examination (PIE)
5. Load fresh pebbles (compensates for the loss of discharged and extracted pebbles)

Along with normal operations, the FHS is also utilized in a similar, but unique, manner for the run-in process, core defuelling and core refuelling. These tasks are highlighted below:

1. Initial loading of graphite pebbles into the core
2. Loading of fuel and graphite pebbles during run-in
3. Replacing graphite pebbles and startup fuel with equilibrium fuel
4. Core defuelling and refuelling for shutdown or maintenance

During normal operations, fuel is taken from fresh fuel drums, and it enters a fuel loading section, which serves as a temporary storage location until fuel is needed for the core. From the loading section station, a fuel pebble is sent to the top of the core where it passes downward through the core until it reaches the discharge chute. Upon being discharged from the core it undergoes two tests. The first test ensures the pebbles are structurally sound and are not deformed in any way; upon passing this test, pebbles are passed to the burnup measurement system. The second test is conducted by the Burn-Up Measurement System (BUMS) which determines the burnup level of the pebbles, typically by examining the caesium peaks. If the burnup is below a specified threshold, pebbles are sent back to the fuel loading section along with any fresh fuel that has been placed there. This process repeats until the pebble has reached the threshold burnup, at which point it is instead sent to the fuel discharge section, where it will eventually be sent to a discharge fuel drum. Figure 3.6 shows a high-level overview of the FHS during normal operations, the process of fuel loading and unloading is provided in more detail below as is based off data provided in Ref. [28].

Loading fresh fuel into the core is known as the fresh fuel supplement process (see Ref. [20] for details). This process involves three segments of piping in the FHS: preparing buffering, atmosphere switching, and preloading buffering. The first segment, preparing buffering, loads individual fresh fuel pebbles from the fresh fuel drums into the FHS. Typically, this segment can hold approximately 40 pebbles. The HTR-PM discharges pebbles at a significantly faster rate; as such, the FHS has been scaled to approximately 20% of the HTR-PM design. These pebbles are then passed to the atmosphere switching segment where the atmosphere is purged and replaced with helium at pressure. The atmosphere switching segment can hold approximately 40 pebbles. Once the pebbles are placed in a helium environment, they are passed to preloading buffering section. This section has two parallel pipes, each of which can hold 40 pebbles. The preloading buffering section holds pebbles before they are finally sent to the core. Table 3.6 shows the corresponding pebble counts for each section.

Fuel discharge follows the same process in the fuel supplement process, but in reverse. Pebbles are discharged and are passed individually to the preparing buffering section. After this, pebbles are sent to the atmosphere switching section, where the helium is replaced with a normal atmosphere. Discharged fuel is then sent to the predischarge buffering pipe, where pebbles are discharged into spent fuel storage drums upon leaving the predischarge buffering pipe. If a constant rate of pebbles flow into and out of the discharge fuel section, it is expected that pebbles will spend on average 10.5 hours in the discharge system before being discharged into the spent fuel storage drums. Table 3.7 shows the pebble counts for each section for the fuel discharge.

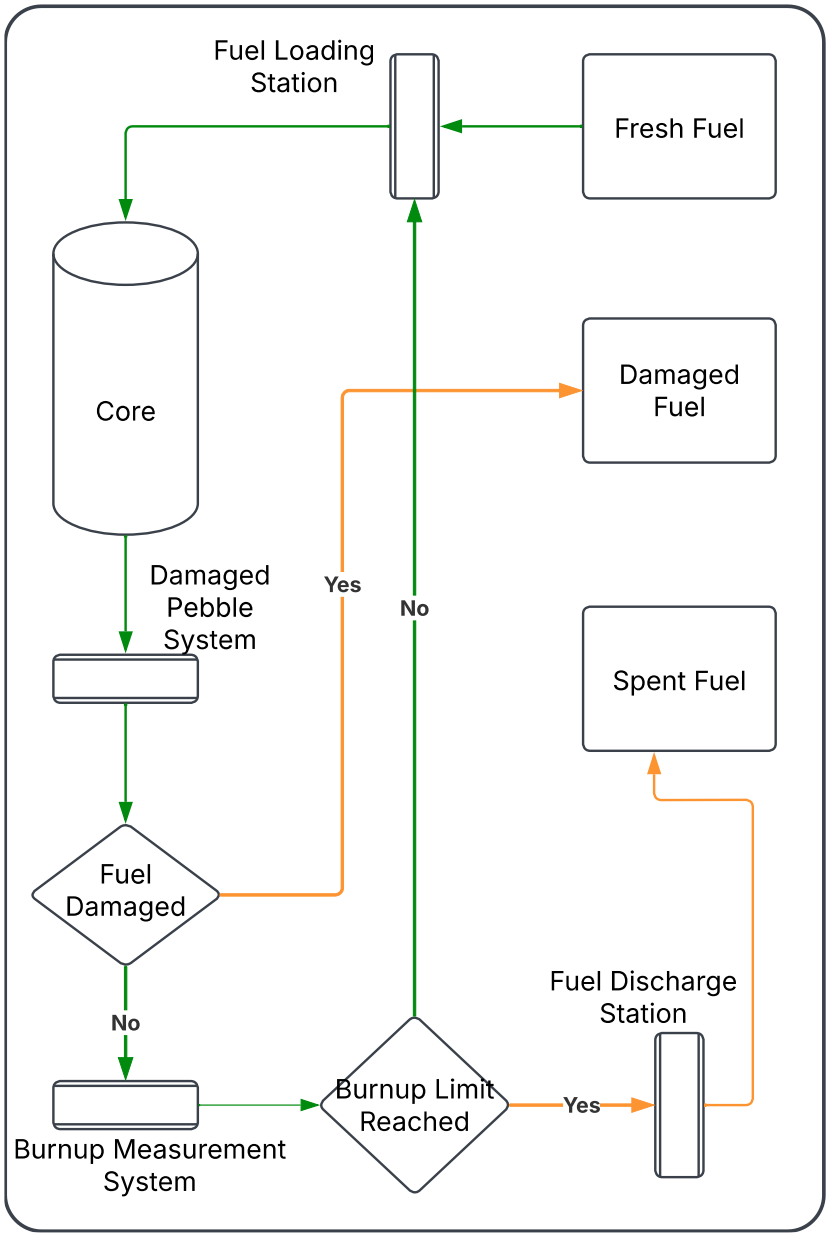


Figure 3.6. Simplified flow scheme for the FHS during normal operations.

Table 3.6. Pebble count in the FHS for fuel loading.

Section	Number of Pebbles
Preparing buffering	40
Atmosphere switching	40
Preloading buffering	80 (40 in two parallel pipes)
Total pebbles	160

Table 3.7. Pebble count in the FHS for fuel discharge.

Section	Number of Pebbles
Preparing buffering	96 (48 in two parallel pipes)
Atmosphere switching	40
Predischarge buffering	40
Total pebbles	176

3.3. Safety Features

The GPBR-200 safety design philosophy follows the same safety principles of Gen-IV VHTR concepts [29]. It strongly relies on inherent safety characteristics and passive systems to perform the required safety functions. Inherent safety features include low power density, a large heat capacity of ceramic core internals, strongly negative temperature coefficient of reactivity, large height-to-diameter ratio of the reactor core to promote passive heat removal, and the use of coated fuel particles (TRISO) that act as the primary barrier to radionuclide release. This combination of features allows the GPBR-200 to control the reactivity inherently (in a loss of helium flow scenario) and reject decay heat passively at a rate sufficient to avoid severe core damage. However, in the event of restarting helium flow after a shutdown, the reactivity will increase, thereby incurring a possible reactivity event. Active systems are also provided, but their goal is mainly for supportive safety functions and to assure plant investment protection and performance criteria. The ensemble of inherent safety features, passive and active systems constitute the safety architecture of GPBR-200.

3.3.1. Control of Reactivity

The primary mechanism for the control of reactivity is the strong negative temperature coefficient at all conditions [30].

Two additional diverse, independent systems are envisaged: the reactivity control system provides means to shut the reactor down by neutron absorbing rods inserted into channels in the side reflector, and the diversely actuated reserve shutdown system (for release of shutdown control rods). Another means to shut down, which takes a longer time, is to keep on shuffling fuel out of the pebble bed core, without adding fresh fuel back, so within a week or two, the core will not be able to remain critical in any case, even in the absence of any reactivity systems functioning.

3.3.2. Control of Heat Removal

The intrinsic design features of low power density, a high heat capacity of ceramic core internals, and a long and narrow core ensure the passive evacuation of decay heat under the worst accident conditions, including the loss of a heat sink, by evacuating heat through the reactor building and surrounding soil, thus preventing any significant core damage. The reactor pressure vessel is not expected to fail but nonetheless may sustain damage; likewise, the surface of the concrete reactor building may undergo spalling due to the overheating, which puts the future operability of the plant at risk.

Therefore, diversified active and passive safety systems are designed to provide backup safety functions of the reactor and serve as part of the reactor protection system.

3.3.3. Startup/Shutdown System (SSS)

The purpose of the SSS [31] is to provide secondary heat removal when main loop cooling capabilities are unavailable.

3.3.4. Reactor Cavity Cooling System (RCCS)

The RCCS [31] is designed as a passive air-cooled system that can operate without station power to protect the reactor core and surrounding plant structures from overheating. It is a safety related system that is expected to operate during all transients. The associated Structures, Systems, and Components are able of controlling heat removal for all accident scenarios. The RCCS is designed to limit the maximum concrete temperature to maintain its integrity.

3.3.5. Control of Chemical Attack

In graphite moderated reactor designs, graphite at high temperatures may oxidise in the presence of air or water. Nuclear grade graphite does not burn but will oxidize if oxygen is available continuously and in sufficient concentration [29]. Consequently, the most exposed graphite components may eventually lose structural integrity. The oxidation process itself generates volatile combustible compounds such as carbon monoxide. The reactor should be designed to minimize these phenomena.

During normal operation, the Helium Purification System ensures that the coolant contains minimal impurities capable of reacting with the graphite of the fuel and structures. However, potential steam generator leaks can allow water to enter the core and attack the high temperature graphite [30]. The oxidation produces carbon monoxide and hydrogen, which are both flammable in air. The graphite oxidation can trigger a release of radioisotopes embedded within the graphite.

To prevent these scenarios, the reactor protection system will act to stop the circulator as soon as moisture is detected by opening passive pressure relief valves. Additional measures include dumping (draining) water from secondary cooling loop until the pressure is equalised, in addition to stopping the feedwater pumps.

The other major risk of chemical attack is air ingress through a breach in the pressure boundary [30]. GPBR-200 is designed so as to prevent large amounts of air and water from entering the primary loop (relief valves, pipe diameters, steam generator design). The inventory of helium in the primary circuit is large compared to that of the air within the low-pressure containment and the gas released from the core would be vented and filtered in the event of a severe depressurization accident. The reactor building itself is designed to take advantage of the density difference between air and helium to minimize the air concentration near the break.

The reactivity effect of air ingress is negative due to neutron capture in nitrogen.

3.3.6. Confinement of Radionuclides

The GPBR-200 has multiple barriers to prevent the release of fission products: the coated fuel particles, the helium pressure boundary and the low-pressure reactor containment building [28]. The coated fuel particles are the most effective barrier because they remain intact with a very low rate of diffusion of fission products up to temperatures ~1600°C where the particle failure rate increases [32]. The value of 1600°C is not a ‘cliff-edge’ limit since the fuel needs to exceed this temperature for extended periods of time (tens to hundreds of hours) and in significant volumes of the core before significant core damage with radionuclide release would be expected to occur. Due to the low release rates, the surrounding graphite matrix is capable of retaining much of fission products resulting in a very low helium activity, even including the circulating graphite dust that builds up during PBR operation.

A dedicated helium purification system is also designed to keep the circulating activity at extremely low levels. Outside of the primary coolant boundary, the low-pressure reactor containment building ensures that the radiological releases that might leak from the primary coolant loop are kept again at very low levels, by filtered release during normal operation.

3.4. Plant Layout

The last aspect of the GPBR-200 examined in this work is a description of the plant layout. A notional layout was used for the security assessment described in section 5; this layout can be considered generic. The main rationale was to avoid supporting a particular plant design; this also prevents the development of an in-house design which is reactor and designer specific. Instead, a description of common facilities deemed necessary for operations will be described and accounted for. One assumption for this work is that the GPBR-200 is a single unit, meaning there is one reactor attached to a single turbine. Future facilities would likely take advantage of multiple reactors at the same site; however, for simplicity a single reactor is modelled. The results obtained from this study would likely be expanded to a multi-unit study.

For most advanced reactors, the reactor, fresh fuel, spent fuel, fuel handling, and steam generators are all housed in a single reactor building. For reference, HTR-10 had a similar structure, where the total dimensions of the facility footprint were approximately 24 m x 30 m. For this work, it is assumed that the reactor is partially below grade, and the fresh, spent, and broken fuel pebbles are stored in below-grade facilities.

For a general PBR, there are a few major system elements that would be required to discuss for their implications on reactor safety, facility security, and facility safeguards. A list of these system elements and their associated “S” regimes is provided in Table 3.8.

Table 3.8. Areas of interest for the GPBR-200 facility layout.

System Elements	**Potential Associated S**
Reactor	Safety, Security, Safeguards
Heat Removal System	Safety, Security
Burnup Measurement System	Safety, Safeguards
Secondary Circuit	Safety, Security
Post-Irradiation Facility	Safety, Security, Safeguards
Fresh Fuel Storage	Safety, Security, Safeguards
Spent Fuel Storage	Safety, Security, Safeguards
Broken Fuel Storage	Safety, Security, Safeguards
Control Room	Safety, Security
Shipping/Receiving	Safety, Security, Safeguards

The reactor was described in the previous section, and it would likely be the centre of the facility. The reactor would house the major core structure along with the pebbles currently being irradiated. Closely connected to the reactor is the heat removal system, described in the above Safety Features section, which is critical for the safe operation of the reactor. Also attached to the core would be the secondary circuit (including a steam generator) and the burnup measurement system. The steam generator uses the hot-leg helium to drive a steam turbine for power production. Specifics of the conversion process are not necessary for this study. In Section 3.2 it was noted how discharged pebbles are monitored by the and sent to the spent fuel storage area when their burnup exceeds a defined threshold. The BUMS (or some associate system) would also monitor the pebbles for defects and discharge pebbles that are deemed broken to the broken pebble storage. Likewise, pebbles can also be extracted and sent to a post-irradiation facility for additional analysis.

The post-irradiation facility, fresh fuel storage, spent fuel storage, and broken fuel storage are all likely to contain fuel pebbles. It is envisioned that these areas would be connected to the

main fuel handling system to facilitate passage of pebbles throughout the facility without the need for human intervention. The fresh fuel storage would contain shipments of fresh fuel pebbles that were shipped to the plant to ensure its continual operation. Fresh fuel shipments will likely contain hundreds or thousands of pebbles in a single tank. We note that the enrichment of the pebbles will likely be constant at equilibrium; however, during the run-in of the facility, lower-enriched fuel pebbles will also be present. The spent fuel storage would likely be similar to the fresh fuel storage, with the exception that the pebbles would be highly radioactive, resulting in a likely high radiation field in the area. Spent fuel pebbles would be stored in tanks as well, where the number of pebbles in a tank would likely be dependent on the decay heat. Broken fuel storage is imagined having much of the same structure as the spent fuel storage, where the major difference is the likelihood of contamination in the room due broken pebbles dispersing contaminated graphite or other products. The final aspect of the fuel would be the post-irradiation area where some subset of pebbles are sent to perform more detailed examination. This area is envisioned to be used by both the state and potentially by the IAEA to examine nuclide content of a pebbles.

The control room will contain all controls necessary to ensure safe operations of the reactor. This would include the ability to perform control rod movement, SCRAM (Safety Control Rod Axe Man) the reactor, and adjust the inlet helium temperature. Along with this, sensors in the reactor would have corresponding read outs for the reactor operators to examine and understand the current state of the reactor.

The last area of interest for the plant layout is the shipping and receiving area. Due to the continual operation of a PBR, shipments of pebbles are expected on a semi-regular basis. Pebbles shipped to the facility would likely be ingested at the receiving area and afterwards sent to the fresh fuel storage. Depending on the state of a final or temporary repository, spent fuel pebbles could also enter the shipping and receiving area to be loaded onto a transport and sent out.

4. Safety Description

A full-scope safety assessment goes beyond the scope of this study. Here, we only present the key elements in the design of the safety architecture while keeping in mind the final goal to identify the interfaces of safety with safeguards and security. To support this, there exist several documents addressing the development of a probabilistic risk assessment (PRA) for a PBR which discuss risk-informed approaches to safety by combining probabilistic and deterministic elements (Refs. [33] to [39]).

A first important step is the systematic approach towards the identification of initiating events to be considered in safety analysis (both using probabilistic and deterministic approaches). The initial conditions for the selection of initiating events cover all operating states (including shutdown) expected during the operating life of the reactor, including the expected shutdown configurations for maintenance and refuelling. Several systematic processes have been developed for this, such as the Master Logic Diagram, Failure mode and effects analysis, Hazard and operability study or the Objective Provision Tree (see for example recommendations provided in paragraph 5.13 of IAEA SSG-3 (Rev. 1) [38]).

4.1. System Overview

The process starts with the identification of the sources of radioactive material, barriers, safety functions, and initial plant operating states.

The following sources of radioactive material can be considered in the GPBR-200, along the line in [33]:

a) Sources within the Main Power System Helium Pressure Boundary (MPS-HPB):
   - Fuel spheres in core/Fuel Handling and Storage System (FHSS)
     - Intact coated particles
     - Failed or defective coated particles
     - Uranium contamination outside coated particles
     - Imbedded/attached to graphite components
   - Plate out on Helium Pressure Boundary (HPB) surfaces and dust
   - Circulating coolant activity

b) Sources outside the MPS-HPB
   - Fuel spheres in storage systems
   - Solid and liquid radwaste systems

The principal barriers to each of these sources that would be typical for a PBR such as the GPBR-200 are summarized in Table 4.1 [33].

Table 4.1. PBR sources and barriers [33].

Radioactive Material Source	**Barriers to Radionuclide Transport**
Fuel spheres in the core	Coated particles, graphite matrix, HPB, reactor building
Fuel spheres outside the core	Coated particles, graphite matrix, FHSS piping, Spent Fuel Tanks, Used Fuel Tanks, or new fuel tanks, reactor building
Non-core sources within the Main Power System (MPS)	HPB, reactor building
Other sources	Various tanks, piping systems and containers, reactor building or ancillary buildings housing waste management equipment

Additionally, a set of reactor-specific safety functions are identified that will define the GPBR-200 Structures, Systems, and Components (SSC) that are available or potentially available to perform these safety functions. Safety functions have been defined in the context of a top-down logical structure, starting with the high-level function of controlling the transport of radionuclides. Such transport is fundamentally controlled in the safety design approach by preserving the integrity of the radionuclide transport barriers. The safety functions are presented in Table 4.2, along the lines of Ref. [33].

Table 4.2. GPBR-200 safety functions

Safety Functions
Confinement of radionuclides
Control of reactivity
Removal of heat
Limiting chemical attack
Maintain core and reactor vessel geometry

Both inherent and engineered safety provisions and SSC are included in the design to perform the safety functions. Engineered safety provisions include both passive and active SSC. Consistent with good PRA practice, the GPBR-200 safety functions modelled in the PRA include those that are required to meet the minimum safety requirements, i.e., the ‘required safety functions’, as well as ‘supportive safety functions’. Supportive safety functions are performed by SSC that are included to meet investment protection needs and serve defense-in-depth roles by preventing and mitigating challenges to barriers to radionuclide transport.

Table 4.3 summarizes, along the lines of Ref. [33], the inherent provisions and SSC (both passive and active) that support or provide defense-in-depth for the safety functions for the GPBR-200.

The nature of the challenge to the safety functions defines the functional initiating event categories that are used to decide which different event sequence models need to be developed. Examples of functional initiating event categories are:

1) Power Conversion Unit (PCU) transients with intact HPB
2) PCU transients with intact HPB and reactivity addition
3) HPB Leaks and Breaks (excluding HPB Heat Exchanger (HX) failures)
   a) Small HPB failures resulting in slow depressurization < 10 mm break size
   b) Moderate HPB failures resulting in rapid depressurization with break size > 10 mm and< 230 mm
   c) Large HPB failures resulting in rapid depressurization with break size > 230 mm
4) HPB HX Failures

Table 4.3. GPBR-200 major structures, systems and components (adapted from Ref. [33]).

Safety Function	Inherent Features and Passive SSC	Active SSC
Confinement of radionuclides	• Fuel barrier - Coated particle barrier - Graphite matrix • Helium Pressure Boundary (HPB) barrier • Reactor building barrier - Confinement functions of reactor building - Reactor building PRS blowout panels	• Pressure Relief System (PRS) dampers • Reactor building Heating, Ventilation and Air-conditioning (HVAC) filtration system
Control of reactivity	• Strong negative temperature coefficient of reactivity • Reduced excess reactivity due to continuous refuelling • Gravity fall of control rods	• Control and protection systems - Operational Control System - Equipment Protection System - Reactor Protection System • Reactivity control systems (RCSs) - RCS trip release of control rods - Alternative Reserve Shutdown System (RSS) release of shutdown rods
Removal of heat	• Large thermal heat capacity • Passive core heat removal • Core size, power density, geometry • Core, un-insulated reactor vessel, and reactor cavity configuration • Passive RCCS • PRS blow-out panels	• PCU - Steam Generator → Active Cooling System (ACS) → Main Heat Sink System (MHSS) - Motored Turbine Generator (TG) → ACS → MHSS • Startup/Shutdown System (SSS) - Equipment Protection Cooling Circuit (EPCC) → MHSS - EPCC → Cooling Tower
Limiting chemical attack	• HPB high reliability piping and pressure vessels • HPB design minimize penetrations in top of reactor vessel • High purity specifications for inert helium coolant • All interfacing systems at lower pressure than MPS • Lack of HPB pressurization mechanisms to open PRS valves • ACS rupture discs protect against MPS HX leaks • PRS relief blowout panels	• PRS exhaust duct dampers limit air ingress • Isolation valves in MPS interfacing systems • Helium Purification System maintains high purity levels of Helium coolant

Safety Function	Inherent Features and Passive SSC	Active SSC
Maintain core and reactor vessel geometry	• Reactor core and structures • Reactor pressure vessel and structures • Reactor cavity citadel • Reactor building structure • Passive RCCS maintains acceptable reactor vessel support temperatures	

4.2. Event Sequences

In line with the risk-informed approach, the performance of a PBR [33] is assessed through the development of event trees (ETs) based on categories of initiating events. These categories help define the event sequences that result from each initiating event and initial condition to be modeled. The development process involves identifying all potential initiating events that could impact the nuclear power plant's safety and categorizing them according to their functional characteristics, i.e., how they affect the safety functions (reactivity insertion, breaks, cooling transients).

Once the initiating events are categorized, ETs are constructed for each specific initiating event that is representative of that category. This involves quantifying the ETs to account for significant dependencies between the causes of the initiating event and the failure probabilities of the modeled SSC (in short, plant provisions, or mitigating functions). Quantification ensures that the event trees accurately reflect the frequency (measured in occurrences per year) of various outcomes based on the interaction between initiating events and SSC failures.

The top events in the ETs are derived by considering the SSCs expected to fulfill the necessary safety functions. These top events represent critical points in the event sequence where the success or failure of an SSC can significantly influence the overall outcome. By analyzing these top events, the ETs can provide a detailed understanding of how each SSC contributes to the plant's safety.

Event sequences are then analyzed to determine the possible successes and failures of each SSC in implementing the required safety functions. This analysis is crucial for assessing whether the SSCs can perform their intended functions effectively under different conditions. The goal is to evaluate the extent to which each SSC can maintain safety functions and to identify the end states of the event sequences, which represent the final outcomes of the modeled scenarios.

The event sequence modelling framework includes the following elements:

- Initiating event.
- Plant response to initiating event.
- Response of the reactor building and associated SSC.
- Factors influencing the end state, including achievement of success criteria and mechanistic source terms.

Event sequences are also defined in terms of the characteristics of any radionuclide release (for instance, such as

Table 4.4).

Table 4.4. Example PRA release categories [33].

Code	Definition
RC-I	No release with an intact HPB
RC-II-F	Filtered release of all or part of circulating activity only
RC-II-U	Unfiltered release of all or part of circulating activity only
RC-III-F	Delayed filtered release from failed fuel with MPS pump-down
RC-III-U	RC-III-U Delayed unfiltered release from failed fuel with MPS
RC-IV-F	RC-IV-F Delayed filtered release from failed fuel without MPS
RC-IV-U	RC-IV-U Delayed unfiltered release from failed fuel without MPS
RC-V-F	Delayed filtered fuel release with oxidation from air ingress and lift-off of plated out radionuclides
RC-V-U	Delayed unfiltered fuel release with oxidation from air ingress and lift-off of plated out radionuclides
RC-VI	Loss of structural integrity in core, reactor vessel, or HPB with unfiltered release

Two or more event sequences are grouped together into an event sequence family when the sequences have a common initiating event, safety function response and end state. In risk-informed approach, these event sequence families will then lead to the selection of Licensing Basis Events (LBEs) and classification into plant states.

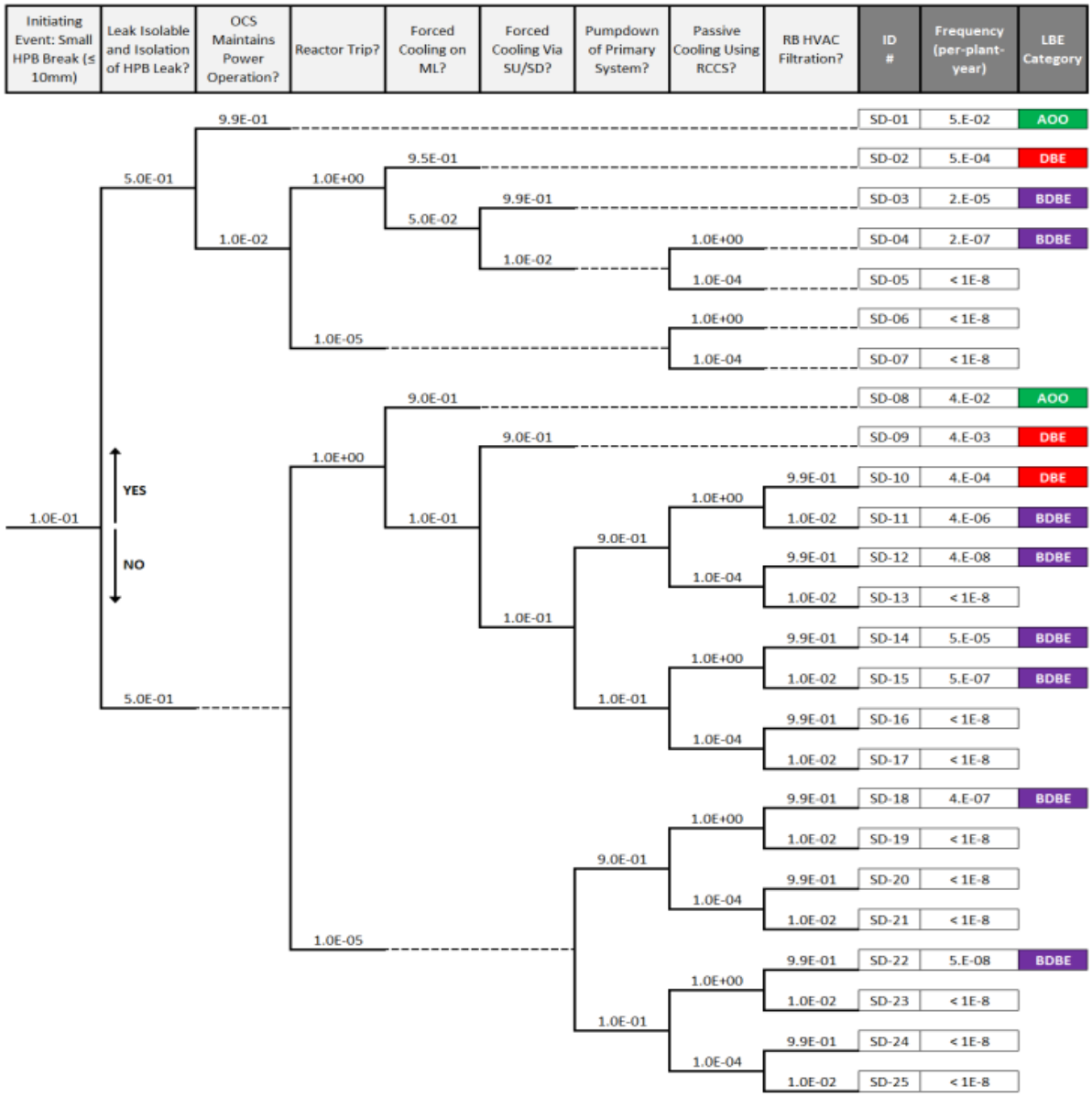


Figure 4.1. Example event tree for a small HPB break [34].

Figure 4.1 shows an example of Pebble Bed Modular Reactor (PBMR) event sequence model of MPS Heat Exchanger Tube Break, using the PBMR design assumptions and PRA models used to develop these examples based on an early design of the PBMR [34].

The typical event tree starts with the initiating event on the left, with its frequency provided in units of (occurrences) per-plant-year for the four-reactor module plant and subsequently lists each of the branch points sequentially across the top to describe the plant response. Note that the GPBR-200 is a single module plant, which may entail the modification of some of the frequency numbers in Figure 4.1, in the application of such an event tree to the GPBR-200. For each branch point question, the Yes-No branches are shown with their estimated probability (no units). The final columns provide the overall event sequence frequency and the associated risk-informed LBEs in the three frequency ranges: Anticipated Operation Occurrence (AOO), Design Basis Event (DBE), and Beyond Design Basis Event (BDBE). The above is based upon categorisations provided in Ref. [34]. It should be noted that the IAEA proposes different categorisations, including AOO, Design Basis Accident (DBA) instead of DBE, and Design Extension Conditions (DEC) instead of BDBE [37].

The above example identifies 25 accident sequences: 12 sequences are “discarded” (not considered further) due to having frequencies less than 10^{-8} per plant-year, 2 are classified as AOO, 3 as DBE and 8 as BDBE. The consequences of event sequences are assessed separately from calculating the frequencies of the sequences. The assessment done in [34] shows that only a few of the thirteen AOO, DBA and BDBA event sequences lead to releases of total effective dose equivalent at exclusion area boundary greater than 10^{-5} rem. This is important as licensing authorities usually specify dose limits at the exclusion area boundary for emergency and planning purposes.

4.3. 3S Observations

The event trees provide a clear image of the reactor safety architecture showing the set of plausible accidental challenges (whose set of mechanisms is represented by the initiating events) to the safety related barriers’ integrity and to the safety functions.

Sequences that are discarded as highly unlikely with a cut-off frequency of less than 10^{-8} per plant-year should be reintegrated in the analysis when addressing the possible interface with the other 2S.

The frequency of each sequence (whether discarded or not) is linked to the reliability of the individual provisions. However, the impact of security and safeguards interference with the safety provisions will affect such reliability by potentially increasing the failure probability of a safety provision up to the extreme value of 1.0 (100%) in the case of an active sabotage.

At the more detailed design level, the systems are designed together with their components. Fault Trees (FTs) are then developed to estimate the failure of the systems by means of the components failures. Its failures of components can be estimated by statistical data. In the case of sabotage, the probability of failure of the components can be reached at the level of 1.0.

5. Security Description

The security assessment for a nuclear facility relies on evaluating the performance of the facility's physical protection system. The Design and Evaluation Process Outline (DEPO), which is shown in Figure 5.1, has been used for several decades for the design of a physical protection system [40]. The process begins by defining the Physical Protection System (PPS) requirements, which involves determining regulatory requirements, characterizing the facility, identifying targets, and defining threats. Next, the PPS is designed with appropriate elements for detection, delay, and response. Then various tools are used to evaluate the PPS, including both path analysis and performance testing. Over the past several years, these tools have increasingly moved toward single-analyst modeling capabilities. Based on performance and identified gaps or vulnerabilities, the PPS will be redesigned. One revision that has been made to the original DEPO process is to include Security by Design recommendations. Security By Design (SeBD) means not just adding more guns, guards, and gates, but considering security aspects early in the design process and implementing design-related decisions which enhance the security of the facility to help optimize facility costs. The PPS design will be iterated until satisfactory results (from performance tests) are obtained.

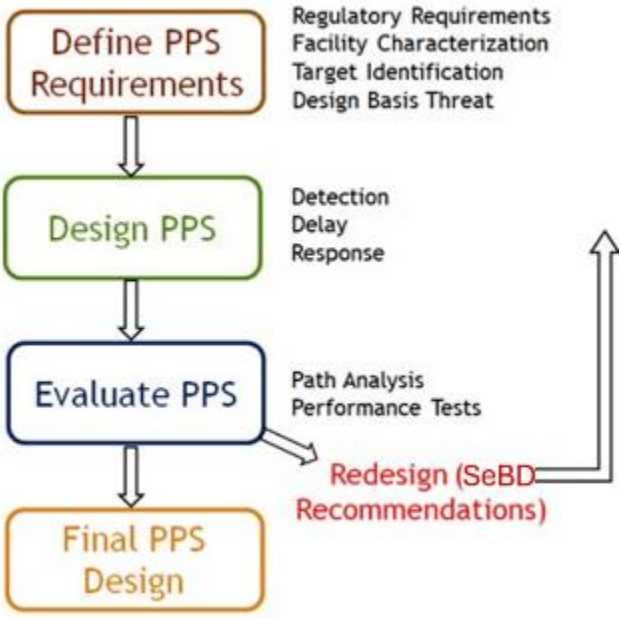


Figure 5.1. DEPO process [40]

5.1. Regulatory Requirements and Design Basis Threat

The regulatory requirements for advanced reactors vary slightly from country to country. The security program goals against radiological sabotage may be set to prevent fuel damage, prevent any offsite release, or only allow offsite releases during or after a security event within a defined dose threshold. Additionally, regulatory bodies may define the available equipment, operator actions, and the timeline of the security event to define the available resources of the safety organization to prevent or mitigate radiological sabotage. These differences can result in different sabotage logic models for the same facility in two different countries, just as different Design Basis Threats (DBTs) would result in different PPS designs.

However, physical protection design for nuclear reactors is fairly standard around the world, partly due to the efforts of the IAEA [41] and other organizations like the World Institute for Nuclear Security [42]. Regulatory requirements are typically based around a DBT that defines a reasonable threat against which the PPS must protect its facility. The DBT helps define the number of adversary attackers, inclusion of insiders, attacker capabilities and training, and attacker tools. This information is sensitive and is specific to each regulatory body. An example

open source, hypothetical DBT is provided in Ref. [43], which defines the adversary team against which to defend as having the following characteristics:

- Group size of 4-to-8 individuals
- Ability to conduct a determined, violent external assault
    - Attack by stealth or deceptive actions
    - Operate in groups through a single entry point
    - Have multiple groups attacking through multiple entries
- Military training and skills, willing to kill or be killed, enough knowledge to identify specific equipment or locations necessary for a successful attack
- Information/access from an active or passive insider
- Land or water vehicles, which could be used for transporting personnel and their hand-carried equipment to the proximity of vital areas.
- Land vehicle bomb assault, which may be coordinated with an external assault
- Ability to conduct a cyber-attack
- Ability to perform any of the tasks needed to steal or sabotage critical assets
- Armed with a 7.62-mm rifle and a 9-mm pistol; ammunition; grenades; satchel charges containing bulk high explosives, not to exceed 10 kg total; detonators; bolt cutters; and miscellaneous other tools
- Each able to carry a man-portable total load of 29.5 kg (65 lb)
- Assumed run speed of 3 m/s
- One passive non-violent insider (not included in the adversary group of 4-to-8 individuals)

DBT information such as that exemplified above help define the requirements and scope for the PPS. With the requirements and scope for the PPS defined, the manner in which the PPS will interface with safety and safeguards requirements also becomes clearer.

Following the guidelines of Ref. [42], the overall objectives of a state's nuclear security regime is to protect against unauthorized removal of nuclear material, locate and recover missing nuclear material, protect against sabotage, and mitigate or minimize the effects of sabotage. Physical protection responsibilities for an operator include the following:

- Security management structure and plan
- Designation of a limited access area
- Designation of a protected area with an intrusion detection system
- Designation of vital areas containing high-consequence equipment or material
- Central Alarm Station (CAS) and Secondary Alarm Station (SAS) for monitoring, assessment of alarms, and direction of responders during a security event

- Delay features and physical barriers including vehicle barriers to slow adversary progress toward a target
- Design of response forces and tactics
- Integration with plant safety systems
- Integration with nuclear material accounting and control systems
- Containment and surveillance systems
- Protection of computer systems (cybersecurity best practices)
- Alarm resolution and reporting
- Recovery from theft or sabotage and contingency plans
- Equipment maintenance, updating, and performance testing
- Response force training and testing including force on force exercises
- Protection against the insider threat including access control and background checks
- Compensatory measures to compensate for degraded or unique facility states

5.2. Facility Characterization

Facility characterization includes understanding the design and layout of the facility, including the overall site layout and location of targets. Both theft and sabotage targets should be included in this characterization. Theft targets will include any nuclear material and potentially nuclear technology as well. Sabotage targets may also include nuclear material as well as critical equipment or systems which could be compromised as a result of a sabotage event at the facility.

A generic reactor building layout for a pebbled bed reactor (the HTR-10) is provided in Ref. [44] and is reproduced in Figure 5.2. The reactor, fresh fuel, spent fuel, fuel handling, and steam generation are all housed in a single reactor building, of dimensions 23.6 m x 29.4 m. The entire reactor is below grade, and the reactor and steam generator are housed in a confinement structure within the reactor building. Fresh fuel, spent fuel, and storage of broken pebbles are stored 15 m below grade. Spent fuel storage is surrounded by shielding walls.

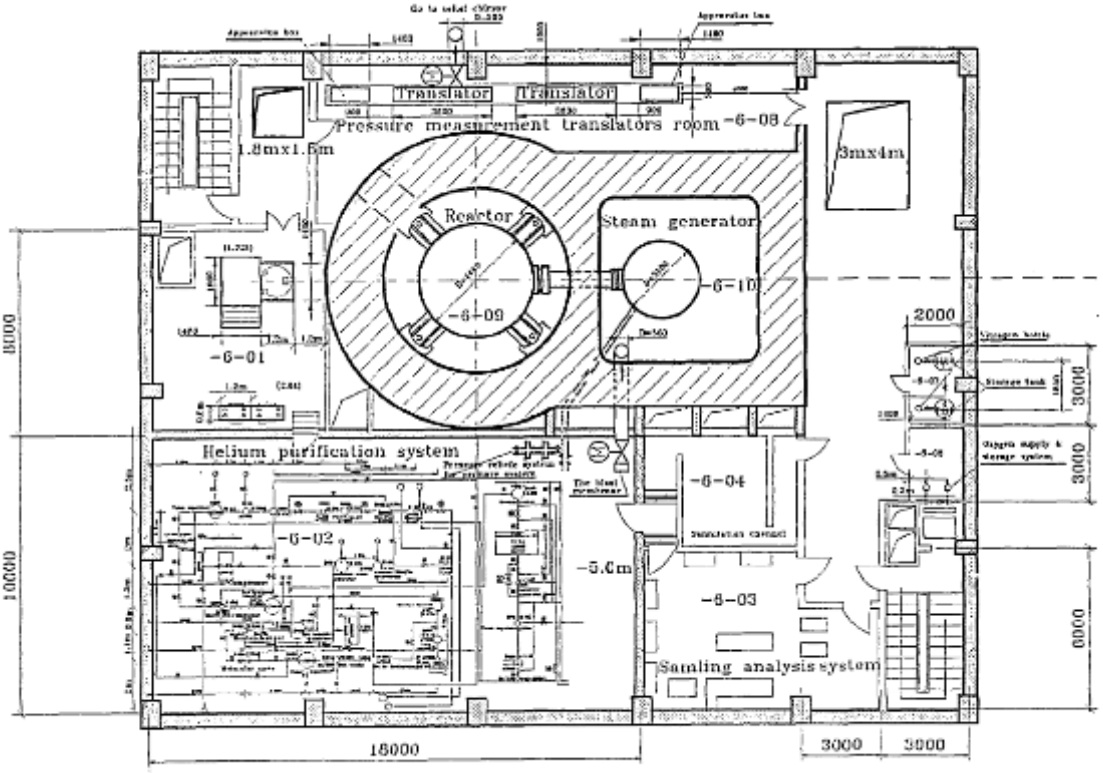


Fig.5 HTR-10 Systems Layout in -6.0m Floor

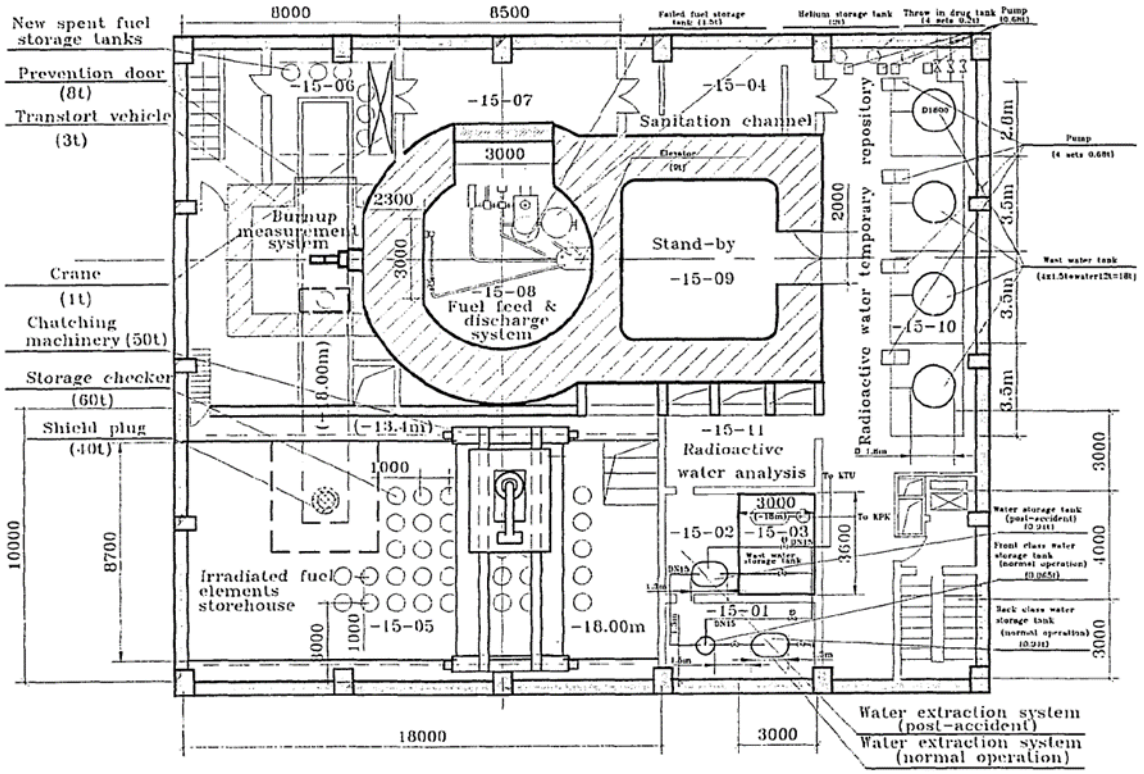


Fig. 6 HTR-10 Systems Layout in -15.0m Floor

Figure 5.2. Reproduction of HTR-10 building layout [44].

An example site layout for a generic Small Modular Reactor (SMR) is shown in Figure 5.3 [45]. The work in Ref. [45] was loosely used as a reference and a baseline PPS design for a generic

SMR not based on any particular vendor design. The design shown in Figure 5.3 assumes a site with one PBR. One building houses the reactor, all control systems, a CAS, and all storage of spent fuel and wastes. The protected area includes the reactor building, an office building, switchyard, and entry control points. There are two Entry Control Points (ECPs), one for vehicle access, and one for pedestrians. This design assumes the use of a Perimeter Intrusion Detection and Assessment System (PIDAS) [46] [47] around the protected area. The PIDAS incorporates microwave sensors and cameras to detect and assess intrusion into the protected area. Other sensors inside the facility may include passive infrared sensors, cameras, balanced magnetic switches on doors, and keycard and Personal Identification Number (PIN) access control on doors.

The entire reactor building will be considered a vital area. Some key theft targets would include fresh fuel and spent fuel canisters. The level of protection required for the fuel depends on the nature of the fuel and into what category of nuclear material it would be considered for security purposes (see Table 1 in Ref. [48]). Other targets include the reactor and fuel handling system, spent fuel canisters, plant safety systems (including decay heat removal, batteries, and diesel generators), control room, CAS, and any other radioactive wastes like filters or spent components that may be stored on site. External access to decay heat removal is a particular vulnerability that should not be ignored. The co-location of all targets in one building simplifies the protection strategy.

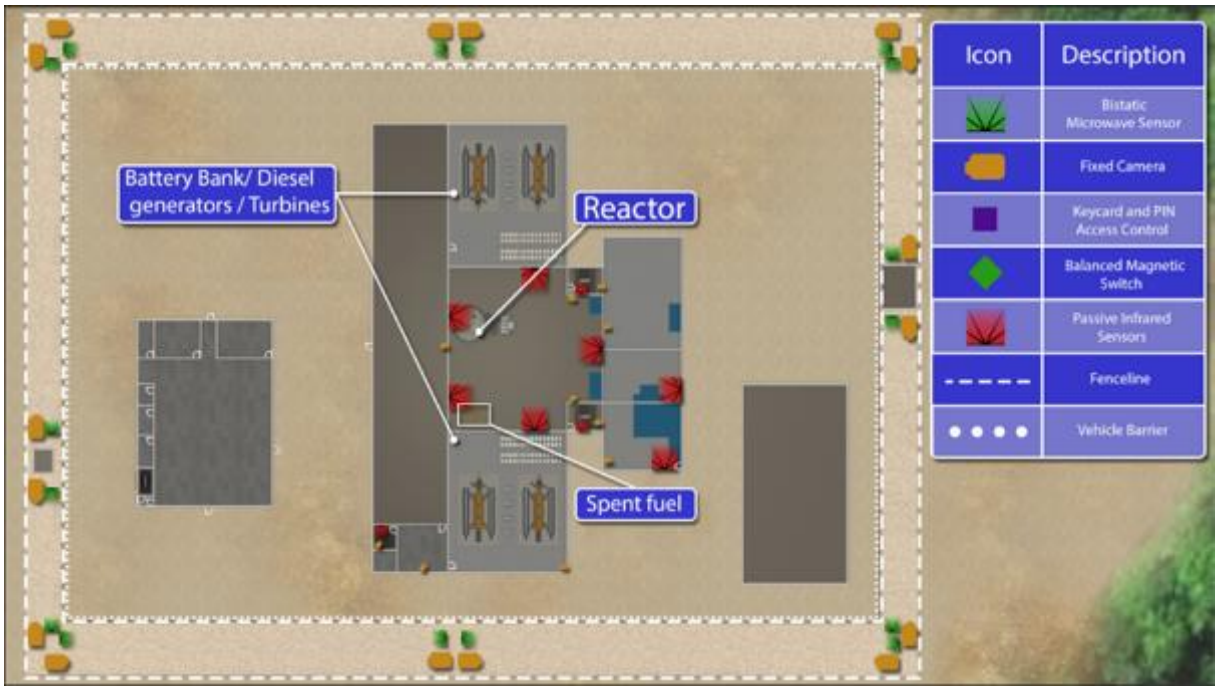


Figure 5.3. Notional SMR Site Layout and Baseline PPS Design.

5.3. Identification of Targets and Vital Areas

Target identification from both a PR and PP standpoint is outlined in the GIF PR&PP Evaluation Methodology [49]. The key theft targets would include the fresh, spent, and damaged fuel. It takes the theft of thousands of fresh or spent pebbles (over 69,000 GPBR-200 pebbles) to acquire one Significant Quantity (SQ) of uranium (75 kg of U-235). Further, processing of TRISO fuel requires a significant undertaking. Therefore, theft of fuel to accumulate significant quantities of uranium is a less likely scenario. On the other hand, one spent pebble can represent a significant source of radioactivity for a radioactive dispersal device (if intentionally destroyed); so, the spent fuel must be protected from theft accordingly. The storage on the

bottom of the reactor building deep below grade provides the opportunity to install additional delay barriers in the PPS design.

Direct sabotage targets include the reactor core itself, spent fuel, and wastes (including off gases, filters, and spent reactor components). Indirect sabotage targets may include decay heat removal systems, reactivity control systems, the control room, power supply systems. Additional targets, such as the CAS, could benefit the success of an adversary. Figure 5.2 does not show the location of all control systems, but it is generally a safe assumption that an unauthorized outsider should be prevented from accessing the reactor building.

The discussion in chapter 3 of this report, as well as equipment combinations determined from the safety analysis, as outlined in chapter 4, would give the list of targets for an adversary force intent on accomplishing radiological sabotage and causing a release from the GPBR-200 facility that could endanger public health and safety. Thus, a key tie between safety and security is the use of the PRA to help inform sabotage targets and to protect them. These equipment combinations result in sabotage logic models, and define the equipment required to be protected though vital area designations and the protective strategy implementation for the prevention of sabotage.

The PRA as used in safety assumes probabilities of failure based on experience with equipment and operator actions. For security assessments, the paradigm is different, in that in many cases the probability of failure is increased much higher, up to 1 as a consequence of an intentional adversary action. Probability of simultaneous failures of redundant components may be also increased, as well as probability of failures of passive components (walls, fire barriers, doors, pipes, vessels, etc.). However, rather than re-working a full FT analysis for security, the process may be made more efficient by protecting all safety systems in a denial of access strategy. In other words, the building or rooms that contain these systems or access to these systems are identified as vital areas. This significantly reduces the workload of the security analyst to then only consider systems that would be outside vital areas.

Vital Area Identification (VAI) is an important part of the PPS design, and advanced reactors, such as SMRs and microreactors, are likely to have a relatively small number of vital areas due to their more compact design. A smaller number of vital areas helps to make the protection strategy more efficient. Ref. [50] provides additional details on the VAI process.

5.4. Design of PPS

Once the facility is characterized and regulatory requirements, targets, and DBT are understood, the design process begins. There are usually well-accepted standards for the PPS design to use as a baseline which are also informed by regulatory requirements (fences, perimeter intrusion detection, lighting, berms or other barriers to prevent vehicle bombs, entry control points, and response forces). However, the facility operator ideally wants to tailor the specifics of the PPS in order to optimise the cost and footprint as much as possible while maintaining an acceptable level of performance to provide a cost-effective PPS design. In general, PPS systems seek to detect adversaries as early as achievable, delay them as long as possible, and respond to them as quickly as possible.

Detection systems are designed to detect adversaries and may include the PIDAS, cameras both external to and internal to the facility, balanced magnetic switches on doors or hatches to processing areas, and portal monitors (which may include metal detectors and radiation detectors) both for personnel and vehicles. These technologies are built up around and inside the facility containing the targets of interest. It is considered best practice to have redundancy and varying means of detection, thus making the system more robust.

Delay technologies are designed to slow down or stop adversaries and include robust walls and ceilings, underground siting, vehicle barriers, man-traps on entry points, hardened doors, ankle breaking rock, and access control. In addition to passive delay measures which are always present, active delay measures can be deployed against a suspected or known

adversary. Active delay may include slippery agents or foggers to make it difficult for an adversary to carry out an attack once in the building.

Response features are designed to neutralize an adversary and recover material if necessary and includes people or weapons and tactics to prevent or slow down access to a site. Both on-site and off-site response may be considered depending on a number of factors. For small modular reactors such as the GPBR-200, there is generally a desire to reduce the number of on-site responders as much as possible while still achieving adequate system effectiveness against attack scenarios. Responders may either be located in guard towers, in roving patrols, or in hardened fighting positions on top of or inside the reactor building.

The design of all three systems is interconnected and is based on the specific optimization approach a facility chooses for its PPS. For instance, the ability to detect an adversary more quickly or to delay an adversary for an extended period of time gives response forces more time to respond. Likewise, more effective means of detection may reduce nuisance alarms, which in turn reduces the number of resources that need to be dedicated to investigating alarms. The PPS must be considered and evaluated as a whole to understand how the various aspects work together.

5.5. Evaluation

Once a preliminary design is completed, the evaluation step includes utilizing various modeling tools or table-top exercises to determine if system effectiveness is high enough. In this case, system effectiveness is the probability that the response force can neutralize the attack. Both path analysis and force-on-force adversary modeling tools can be used for the evaluation step. Historically, much of this evaluation work was carried out using table-top exercises; today single-analyst computer modeling tools can be used to run through hundreds of scenarios and determine metrics for system effectiveness by running multiple simulations of the same attack.

Before attack scenarios can be modeled, path analysis is used to determine how an adversary may reach various targets at the facility as well as the delay time associated with those attacks. The most consequential attack is usually identified along with the adversary task time to steal material or sabotage the facility. Based on the response force design and muster times, the designer will determine if more delay time or earlier detection capabilities are required and may make changes to the facility.

Once several iterations on the baseline design are completed, and there is a degree of confidence in the performance of the PPS, force-on-force adversary modeling will be used to test the system against the DBT. Multiple scenarios will be analyzed to help assess whether the design is effective. Based on the system performance in these scenarios, changes may be made and the scenarios tested again. This testing and redesigning are expected as the DEPO process is inherently iterative.

5.6. Redesign

During the design iterations, the results from the evaluation will be used to redesign the overall facility and site layout as needed. This step is where SeBD recommendations are identified and may be implemented. Instead of assuming a fixed facility and only modifying aspects of the PPS, designers may include changes to the building or site layout to make the PPS more effective in addition to changing the PPS design.

5.7. 3S Observations

It should be noted that the PPS does not exist in a vacuum. Design choices for the PPS may have implications for the safety and safeguards of the facility. The “Define PPS Requirements” step of the DEPO process (see Figure 5.1 above) is the area with the most overlap with the other S regimes. Analysis of system design for each of safeguards, safety, and cybersecurity requires understanding the facility characterization, targets, threats, and regulatory requirements. An integrated 3S approach can be more efficient when these facility characteristics are examined in parallel through all of the S regimes. An integrated approach

allows designers to more aptly understand and balance how changes made to benefit one of the S regimes impact the other two. This can allow for maximizing synergies between systems and minimizing conflicts, which may reduce the need for costly retrofitting in the future.

The “Design” phase of DEPO starts to diverge from the other S regimes because the detection, delay, and response technologies and tactics are more specific for physical protection. However, understanding the safety systems and operations in the plant is vital to properly designing the PPS in order to protect the plant, especially if considering indirect sabotage scenarios. All decay heat removal systems, passive safety systems, and ultimate heat sink need to be considered as possible sabotage targets. Likewise, systems designed to delay an adversary should not impede the ability of site personnel to carry out safety related activities. There are also areas where safeguards or materials accountancy measurements can be useful to provide timely detection of anomalies that should be reported to responders. Cybersecurity is woven throughout all systems and in particular must be considered to provide robustness against cyber-physical attacks.

The “Evaluation” phase of DEPO diverges even more from the other S’s because the tools used for PPS analysis are very distinct from tools used in the other areas. Path analysis, force-on-force adversary modeling, and tabletop exercises are important aspects of the evaluation and testing of a PPS design. The use of such regime-specific tools can increase the difficulty in understanding how security design choices impact safety and safeguards, thus making a 3SBD approach difficult to implement. Future work should strive to see more integration of modeling capabilities from the other domains.

In the case of an SMR such as the GPBR-200, all key safety systems will likely be located within the reactor building which also contains spent fuel storage. One physical protection approach is to deny access to the reactor building, in which case the location of specific safety systems becomes less important. However, external access to decay heat removal systems is a specific vulnerability which needs to be considered. Additional strategies may focus on layered defense, use of active delay features, or hardening the facility (to include subsurface installation) to protect the facility against external threats. SMRs may have different operational regimes that result in minimal access required for regular maintenance or refuelling, allowing different PPS design architectures. PBRs may also have different opportunities to employ 2S integration to increase the facility robustness to attack, as will be discussed in chapter 7 of this report.

Historically, PPS design is somewhat agnostic to the specific reactor design and instead more focused on the location of targets and vital areas. Many generic design recommendations can be developed for SMRs and microreactors that do not depend on the specific technology. For a PBR, specific differences include the fuel handling system which has some unique interfaces between safeguards and security. Decay heat removal systems are all slightly different between reactor classes; such differences also need to be considered for the effective protection strategy. Protecting the one building with a denial of access strategy eliminates many of the PPS design differences that may exist between different reactors due to each unique set of operations.

6. Safeguards Description

The IAEA's safeguards approach for a facility consists of a set of safeguards measures and safeguards activities for the facility, along with their corresponding intensity and frequency; it is based upon nuclear material accountancy as a safeguards measure, complemented by containment and surveillance measures and monitoring. Very pertinent to the design of these measures is design information, which concerns nuclear material of a facility that is subject to IAEA safeguards, as well as features of the facility that are relevant to safeguarding such material [2].

Facility design information for safeguards includes the following [2]:

- form, quantity, location and flow of nuclear material to be or being used;
- facility layout and containment features;
- procedures for nuclear material accountancy and nuclear material control.

The design information is used by the IAEA to design the facility safeguards approach, to determine material balance areas (MBAs) and key measurement points, to develop a design information verification plan, and to establish an essential equipment list. This information is captured in a design information questionnaire (DIQ), which is a document submitted by States to the IAEA to provide safeguards design information of a facility. The IAEA provides States with standard DIQ forms to record and submit the design information required by it for the different facility types and for locations outside facilities [2]

The following assessment summarizes safeguards-relevant information pertinent to the GPBR-200, following the structural content of an IAEA DIQ checklist [2] [51]. The rationale for doing so is that the DIQ conveniently summarizes all of the major element of the GPBR-200 facility that are relevant to safeguards as well as the 3S interface discussion of this case study.

6.1. Facility Information

From a safeguards perspective, the portions of the GPBR-200 facility that are of the most interest are those where nuclear material is located, locations where nuclear material passes through, or pieces of equipment used to move nuclear material. The layout of the GPBR-200 is assumed to have a single reactor unit coupled with a single turbine. Other safeguards-relevant components of the facility include a burnup measurement system, a post-irradiation facility, shipping and receiving areas, as well as storage areas for fresh fuel, spent fuel, and broken fuel, and shipping and receiving area. These components are all discussed in further detail in section 3.4 above.

6.1.1. Core Description

The Core Description section of the system description in chapter 3 gives information addressing a number of aspects of an IAEA DIQ checklist, as shown in

Table 6.1 below.

Table 6.1. Summary of GPBR-200 DIQ information related to the description of the reactor core.

DIQ Item	GPBR-200 Information Provided
Uranium enrichment range of the reactor core	5.0 wt% to 15.5 wt% U-235
Neutron moderator	Graphite matrix of each pebble encapsulating TRISO particles
Coolant	Helium gas, pressurized at 6.0 MPa, flowing at the rate of 79 kg/s
Nominal weight of fuel in elements or assemblies	7.0 g of U, and 1.085 g of U-235 in each equilibrium fuel pebble
Physical and chemical form of fresh fuel	Uranium oxicarbide (UCO) tri-structural isotropic (TRISO) fuel kernels embedded in graphite of each pebble
Description of fresh fuel elements	6.0 cm pebble diameter, with 1.0 cm thick graphite shell surrounding a graphite matrix containing 18,687 TRISO particles; structure of TRISO particles is given in Table 3.2 of chapter 3
Basic accounting units	The number of fuel pebbles, or the aggregate nuclear material mass encased in the collection of fuel pebbles
Expected inventory/capacity of the reactor core	Approximately 220,000 fuel pebbles
Average neutron flux in core	Average neutron flux for each of the thermal, epithermal, and fast groups are 5.15E+19 n/cm^{2}s, 5.07E+19 n/cm^{2}s, and 6.82E+19 n/cm^{2}s, respectively

6.1.2. Fuel Handling System

The FHS section of the system description in chapter 3 gives information addressing a number of aspects of an IAEA DIQ checklist, including:

- Fuel burnup (average, maximum),
- Routes followed by nuclear material, including transfers,
- Staging areas, and
- Diagrams for the flow of nuclear material.

The text below summarizes these elements, extracting relevant portions from the FHS section of chapter 3, and consolidating the information here for convenient reference. As there is considerable fuel handling in the operation of a PBR such as the GPBR-200, the information bears revisiting here.

The FHS has several tasks during equilibrium operation, as described in chapter 3. During normal operations, fuel is taken from fresh fuel drums and enters a fuel loading section until fuel is needed for the core. Once in the loading section station, the fuel pebble is sent to the core where it passes through the core until it reaches the discharge chute. Upon being

discharged from the core it undergoes two tests. The first ensures the pebble is structurally sound and is not deformed in any way. Upon success, it is passed to the BUMS system. The BUMS system determines the burnup level of the pebble, typically by examining the cesium peaks, where if the burnup is below a specified threshold, it is sent back to the fuel loading section along with any fresh fuel that has been placed there. This process repeats until the pebble has reached the threshold burnup near 160 MWd/kg, when it is instead sent to the fuel discharge section and eventually sent to a discharge fuel drum. Each pebble in the GPBR-200 will have on average passed through the core six times.

Loading fuel into the core is known as the fresh fuel supplement process. During normal operations, as spent fuel is discharged from the core and sent to spent fuel storage, fresh fuel pebbles are added to the core to maintain constant reactivity. The continual addition of fresh fuel pebbles provides an opportunity for material diversion. A basic mass flow rate has been derived to understand the time required to obtain 1 SQ[3] of uranium (75 kg of U-235), details of which are provided in chapter 3.

This fresh fuel supplement process involves three segments of piping in the FHS: preparing buffering (loading 40 fresh fuel pebbles at a time from fresh fuel drums into the FHS), atmosphere switching (the atmosphere around 40 fresh fuel pebbles is purged replaced with helium at operating pressure), and preloading buffering (holding 40 pebbles in each of two parallel pipes prior to loading in the core).

Fuel discharge follows the same process in the fuel supplement process, but in reverse. Pebbles are discharged and are passed individually to the preparing buffering section, which can hold up to 96 pebbles (48 each in two parallel pipes). After this, the helium atmosphere of up to 40 pebbles at a time is replaced with a normal atmosphere. The 40 discharged fuel pebbles are then sent to the pre-discharge buffering pipe, where pebbles are discharged into spent fuel storage drums upon leaving the pre-discharge buffering pipe.

6.1.3. Example Calculation: Mass Flow of Fresh Fuel

To illustrate the rate of nuclear material flow through, the following simplified mass flow calculation for fresh fuel is provided.

During normal operations, spent fuel is discharged from the core and sent to spent fuel storage, where it is transferred to spent fuel drums. To maintain a constant reactivity, the discharged spent fuel is offset by adding fresh fuel pebbles. The continual addition of fresh fuel pebbles provides an opportunity for material diversion. A basic mass flow rate has been derived to understand the time required to obtain 1 SQ of uranium (75 kg of U-235).

Discharge Pebbles per day: $N_f = \frac{D}{P}$
Mass of fresh fuel per drum: $M_D = M_u * e * N_D$
Time to achieve 1 SQ: $t_{sq} = \frac{M_{SQ} * N_D}{M_D * f * N_f}$
In the above equations,
N_f = discharge rate from reactor circulation (pebbles per day)
D = total discharge rate from the reactor vessel to the FHS (pebbles per day)
P = number of passes
M_D = U-235 mass per drum
M_u = uranium mass per pebble (g)
e = enrichment

[3] The IAEA Safeguards Glossary [2] defines Significant Quantity (SQ) as “the approximate amount of nuclear material for which the possibility of manufacturing a nuclear explosive device cannot be excluded”. For Pu (containing less than 80% 238Pu) and for 233U, a SQ corresponds to 8 kg. A SQ is 25 kg for U enriched in 235U at 20%, or above, 75 kg for U enriched below 20% in 235U (or 10 t for natural U, or 20 t for depleted U) and 20 t for Th

N_D = pebbles per fuel drum
t_{SQ}= time to acquire 1 SQ (days)
M_{SQ} = mass of SQ desired
f = fraction of pebbles diverted per drum

This simplified algebraic representation of the fresh flow of fuel allows for an understanding of the quantity of fuel pebbles required for diversion scenarios. This representation does not consider the effects on core operations, which would likely require the reactor to be operated in a significantly different manner to maintain reactivity. In an example using the GPBR-200, where 1,300 pebbles are discharged per day, there are on average six passes, seven grams of uranium per pebble, an enrichment of 15.5-wt%, assuming 1,000 pebbles per drum (as per literature [52]) or 350 pebbles to each VP55 drum [53], and a requirement of 75 kg of uranium-235 to achieve 1 SQ. Given these requirements, 69 drums (or 197 VP55 drums) are required to reach 1 SQ. If we assume 50% of the pebbles were diverted from each drum holding 1,000 pebbles, it would take 21.2 months to acquire 1 SQ. A diversion rate of 50% of the pebbles would be relatively easy to detect within the established timeliness component of the IAEA inspection goals which would ensure that there has been no abrupt diversion of 1 SQ in a calendar year [2]. At the end of a calendar year, at most 57% of 1 SQ would be diverted, but a 50% diversion rate would likely be detected much sooner than one calendar year.

6.2. Plant Layout, Material Balance Structure, and Key Measurement Points

A description of the plant layout for the single unit GPBR-200 facility is provided in chapter 3 of this report. Table 3.7Table 3.8 of chapter 3 lists ten areas of interest for this 3S study, seven of which are relevant for safeguards considerations; these include:

- Reactor system
- Burnup Measurement System
- Post-Irradiation Facility
- Fresh Fuel Storage
- Spent Fuel Storage
- Broken Fuel Storage
- Shipping and Receiving

These seven areas can be considered as system elements within the GPBR-200 where nuclear material diversion and facility misuse could take place, being areas of concern for nuclear safeguards. The material accountancy system for the GPBR-200 should encompass the above facility areas. A few material balance area architectures have been proposed for PBRs in the past, such as in Ref. [54]. More recent reports in Refs. [53] and [55] propose a hybrid of item-counting and bulk-handling accountancy. It is proposed that the entire PBR facility be included in a single MBA, due to the continual movement of fuel pebbles through the facility during operation. However, the MBA can be segmented into sub-MBAs, as some areas are best handled with item-counting accountancy while others with bulk-handling accountancy. In this proposal, the item-counting is based upon counting of well-defined and characterized fuel pebble containers, while the bulk-handling accountancy is based upon accounting for the overall depletion (loss) of uranium and production (gain) of plutonium as pebbles flow through the operating core. More details about this approach can be found in Section 6.3. Following the example of Ref. [55], the organization of sub-MBAs could be broken down as follows:

- Sub-MBA-1
    - Receiving
    - Fresh Fuel Storage
- Sub-MBA-2
    - Reactor System
    - Burnup Measurement System
- Sub-MBA-3

- Spent Fuel Storage
- Broken Fuel Storage
- Post-Irradiation Facility
- Shipping

With this organization, sub-MBA-1 and sub-MBA-3 would maintain item-based accountancy strategies based upon fresh and irradiated fuel pebble storage containers, whereas sub-MBA-2 would employ bulk-handling accountancy strategies that deal with the flow of fuel pebbles through the reactor system. The demarcation of sub-MBAs, each with a single type of accounting strategy, provides for simplified inventory accounting within each sub-MBA. The accountancy information from each sub-MBA can be then combined for the overall MBA at the end of each material balance period. With the above demarcation of sub-MBAs, Inventory Key Measurement Points (IKMPs) and Flow Key Measurement Points (FKMPs) can be established, as follows:

- Inventory Key Measurement Points
  - IKMP A: Fresh Fuel Storage (items)
  - IKMP B: Reactor System
  - IKMP C: Broken Fuel Storage (items)
  - IKMP D: Spent Fuel Storage (items)
  - IKMP E: Post-Irradiation Facility (items)
- Flow Key Measurement Points
  - FKMP 1: Fresh fuel receipt (items)
  - FKMP 2: Recategorization of fresh fuel through transfer to pebble feed system
  - *FKMP 3: Fresh fuel insertion into reactor core
  - *FKMP 4: Irradiated fuel removal from reactor core
  - FKMP 5: Recategorization of broken fuel and waste transferred to broken fuel storage
  - *FKMP 6: Irradiated fuel transfer to burnup measurement system
  - *FKMP 7: Irradiated fuel reinsertion into reactor core from burnup measurement system
  - FKMP 8: Irradiated fuel removed from burnup measurement system to spent fuel transfer
  - FKMP 9: Recategorization of spent fuel transferred to spent fuel storage
  - *FKMP 10: Transfer of spent fuel between storage and post irradiation facility (items)
  - *FKMP 11: Transfer of broken fuel between storage and post irradiation facility (items)
  - FKMP 12: Shipment of spent fuel, broken fuel, and waste (items)

In the above, FKMPs marked with an asterisk (*) are for recording internal flows, not required for material accountancy reporting. IKMPs and FKMPs to which item-counting material accountancy applies are indicated above as such.

6.3. Source Data, Reporting, Loss and Production of Nuclear Material

The source data will vary depending on whether item accountancy or bulk handling accountancy applies at the segment in question. For fresh, spent, and broken fuel storage, item accountancy will be based on standardized containerization of the pebbles [55]. Item accountancy of pebbles selected for post-irradiation examination can be based upon individual pebbles. For the nuclear material quantities in the reactor vessel and potential scrap flows, a material balance based on measured inventories and flows would need to be established. The initial reported quantity of pebbles within the vessel would be based upon the quantity of pebbles used to fill the reactor vessel before the reactor went critical. Subsequent reporting of

nuclear material in the reactor would be based upon the quantity of unirradiated nuclear material representing the current number of pebbles in the reactor. The quantity of nuclear material transferred into spent fuel containers for the physical inventory taking would also be based upon fresh fuel values, for direct balancing with input quantities. Final balancing for the reactor and exiting spent fuel would factor in plutonium buildup and depletion of uranium, with these values being determined based upon burnup calculations and measurements. Source data would also include that information which is pertinent for physical inventory taking of the quantity of nuclear material in damaged or broken pebbles collected into a container and collected waste [55].

Nuclear material records and declarations of a licensee must be periodically compared and reconciled with those of the responsible regulator. The reconciliation is organized by material type and various subgroupings of interest within each material type. Values must match gram for gram or kilogram for kilogram in transactions and inventory; discrepancies are corrected during the reconciliation process. As discussed in Ref. [56], how transactions are grouped and summed for a PBR such as the GPBR-200 will determine what type of rounding bias will occur and their magnitude. Example physical groupings include:

- Discrete pebbles: the smallest integral nuclear material object within a PBR at one pebble.
- VP55 fresh fuel container: a certified shipping container for pebbles that holds approximately 350 fresh fuel pebbles.
- Truck: projected to hold 71 VP55 containers per truck, amounting to 24,850 pebbles per truck.
- Spent fuel container: current designs hold about 2000 pebbles.

In the case where one employs physical group based upon VP55 containers, it is conceivable that a container will only be partially loaded at the time of inventory. In such a case, an opened, partially full fresh fuel container could be inventoried either by the number of discrete pebbles held within the container, or by comparing the pebble mass held within the opened container with the pebble mass held within a full container.

The loss and production of fissile material during the operation of a nuclear reactor results from transmutation of actinides while using the nuclear fuel to produce power. In a U and Pu fueled systems, uranium is consumed, and plutonium is produced. A nuclear materials accountancy system must track the depletion (loss) of uranium and the production (gain) of plutonium to account for fissile and fissionable material. For a PBR facility such as the GPBR-200, several relevant factors should be considered for determining loss and production:

1. Determine when to record loss and production as each fuel pebble circulates within the reactor system several times.
2. Each pebble’s pathway through the reactor and its position at any given time is unknown.
3. The number of passes and length of time each pebble resides in the reactor is not directly known, only estimated from pebble flow characteristics and burnup measurements.
4. Overall loss and production are affected by the range of burnup values for determining when pebble should be discharged from the reactor.
5. The enrichment of pebbles is different during start-up than during equilibrium operations, and non-fuel graphite moderator pebbles are used throughout operations.

The above factors can be addressed using modeling tools for estimating isotopic content related to fuel burnup. The burnup estimations are based on variations in flow path and different residency times in order to determine the uranium and plutonium content of spent-fuel pebbles in spent fuel containers. In this way, the overall loss and production of fissile and fertile material can be determined [57].

6.4. Shipping/Receiving

Fresh fuel is to be received at the reactor in containers which are sealed after filling prior to shipment; the VP55 container is currently assumed to be the container used for shipping fresh fuel. Considering that the containers can hold pebbles of differing enrichment or even non-fuel moderator pebbles, handling and inventory procedures should clearly state how these containers and their contents are identified, stored and managed for operations and inventory. Receipt verification can follow one of a few options:

1) verify the container and serial number of the container's tamper-indicating device (TID);
2) open the container and count all pebbles;
3) open the container, count all pebbles and measure a sample of pebbles; or
4) open the container and individually measure each pebble.

When there is high confidence in the transfer process, option (1) is acceptable, and it could be coupled with a weight measurement or enrichment measurement to confirm the expected degree of enrichment. High confidence would entail that there was no evidence of diversion during transfer and storage, and that processes followed by the fuel fabricator and reactor operator involved little to no discrepancies. Subsequently, the number of pebbles and nuclear material content within the pebbles would be placed into inventory based upon shipper's values, and maintained until the container is opened for pebbles to be fed into the reactor [56].

In cases where there is lower confidence that diversion is not taking place, or there are performance violations in transfer and storage processes, one of options 2 through 4 could be followed, depending on the degree of lack of confidence [56].

6.5. Physical Inventory, Containment and Surveillance and Monitoring Features

Verification of fresh fuel pebble receipts and inventory performed by IAEA inspectors entails verifying the seals of fresh fuel containers, checking for tampering, and inspecting the storage of sealed fuel containers. The number and identification of the fresh fuel containers, as well as their storage location, are confirmed to be as declared by the facility operator. In the case of unsealed fresh fuel containers, the nuclear material content is verified using non-destructive assay instruments including gamma spectroscopy, passive or active coincident neutron counting, and mass measurements using a load cell balance system or mass scale which has been calibrated and verified by the inspector. The frequency of physical inventory verification of fresh Low Enriched Uranium (LEU) fuel is typically conducted annually in order to meet IAEA timeliness goals, but is more frequent (3 months) for plutonium-bearing spent fuel [2].

Seals, surveillance, and fuel flow monitoring systems would be used to detect and verify the transfer of pebble fuel to and from the reactor core. The IAEA would seal hatches, covers, or ports that access the reactor core. Seals are periodically replaced by the inspector to detect potential tampering, while video surveillance systems are reviewed to detect undeclared removal of pebble fuel. Fuel flow monitors serve to verify the transfer of pebble fuel to and from the core, which is otherwise difficult to access. It is possible in principle for the facility operator and the IAEA to share the fuel flow monitoring system provided that the IAEA can independently verify the safeguards data collected by the system. In principle, successful operation of seals, surveillance, and fuel flow monitoring systems may permit the IAEA to indirectly verify the pebble fuel in the reactor core by deduction. However, means to directly re-verify the pebble fuel and volume of fuel in the reactor core should also be provided; this may be accomplished by installing an instrumentation well adjacent to the reactor vessel for IAEA gamma and neutron detection probes, which can verify gross attributes of partly irradiated pebble fuel in the core as well as the fuel fill-height or volume in the core [54].

The IAEA also compares the data of installed instruments with facility operating and accounting records to ensure there are no undeclared reactor shutdowns or outages. Further, the IAEA

verifies declared nuclear material content of spent fuel using a suitable fuel burn-up analysis code, based upon the fuel irradiation history [54].

Fuel flow monitoring systems would be used to verify and count spent pebble fuel transferred from the reactor core to spent fuel storage, broken fuel storage, or to the post-irradiation facility. Seal and surveillance systems can also be used to detect the removal of spent fuel from storage as well as shipments of spent fuel containers from the facility. The IAEA may verify the shipment at the receiving location or prior to shipment using non-destructive assay measurement techniques such as gamma spectroscopy. Video surveillance and radiation fuel flow monitors would be reviewed to further verify that the shipments of spent fuel pebbles are as declared by the facility operator [54].

Staging areas for preparing loading of pebbles into the reactor, or receiving discharged pebbles into spent fuel storage, are integral to fuel flow lines monitored by the fuel flow monitoring system. In a recent implementation [58], the fresh fuel loading area is monitored via gamma spectroscopy calibrated to a fixed geometry. Operational information on material going to the core, circulating through the reactor system, or discharging to spent fuel storage is proposed to be available to the IAEA via secure, authenticated remote data transmission. Upon discharge from the burnup measurement system, spent fuel containers are loaded, sealed once filled, and transported to silos via a cask transportation machine. A neutron detector installed on the cask transportation machine monitors the silo loading and unloading activities, and a collimated gamma spectrometer can determine the radiation profile of the nuclear material as well as the number of spent fuel containers loaded in each silo [58].

6.6. Measurement Methods and Level of Accuracy

Some measurement methods have been mentioned above, including the use of load cells or scales for mass measurement, gamma spectroscopy, and neutron passive and active coincidence detection. From literature, the relative uncertainties associated with these measurement techniques are 0.07% for load cell mass measurement [58], 4% (for U) [60] or 1% (for Pu) [61] using multigroup analysis of gamma spectroscopy, 1-2% for passive neutron burnup measurement (based on Cm-244 spontaneous fission), and 5-10% for active neutron interrogation or neutron coincidence multiplicity [62]. The time latency for these measurement techniques also needs to be considered, with the required timings being seconds for mass measurements, minutes to hours for passive gamma and neutron measurements, and hours for active neutron interrogation or neutron coincidence multiplicity [62].

The burnup measurement system is an integral part of the material accountancy system for the PBRs such as the GPBR-200. Burnup measurements can be conducted either with gamma spectroscopy or neutron coincidence counting. For the gamma measurements, the cooling time of the irradiated pebble sample is a very important factor to the accuracy of burnup determination, as cooling allows time for short-lived fission products to die away and results in a cleaner spectrum [56]. Assuming a cooling time of 100 hours, burnup can be best estimated from gamma spectroscopy using the integral of the 661.6 keV line of Cs-137, for which measurement precision of up to 2.5% in 30 s can be expected [57]. Neutron measurements are usually more sensitive to the burnup of fuel than gamma spectroscopy measurements. Cm-244 is a dominant neutron emitter in spent fuel, and its concentration trends with the fourth power of the fuel burnup [57].

6.7. Access to Nuclear Material, Nuclear Materials Testing Areas

Safe engineered access should be provided for IAEA inspectors to service seals, surveillance systems, and fuel flow monitoring systems. Access is also required for the fresh fuel pebble storage area, fresh fuel containers, and feed hoppers employed for loading the reactor. Safe access should also be provided up to the access hatches for the reactor vessel and spent fuel storage areas [53]. To ensure the validity of safeguards provided by seals, which are used to hold accountable nuclear material, their issuance, movement, application, and removal must

be documented. Typically, seal management is integrated into the management of functions utilizing seals such as shipment, receipt, physical inventory and containerization [63].

The GPBR-200, much like current PBR designs, includes a post-irradiation examination facility for evaluating the mechanical and physical properties of pebble fuel specimens during reactor operation, enabling verification of the accuracy of burnup measurements, and confirming the mechanical integrity. This is a hot cell facility that would enable destructive and non-destructive measurements on statistically selected, pneumatically transferred samples. It is likely the IAEA would evaluate the capability of such a facility for the potential of producing separated nuclear material such as plutonium during Design Information Verification [53].

6.8. 3S Observations

In the compilation of this assessment, some areas of overlap of safeguards with safety and security have been observed.

For example, the physical inventory verification of the GPBR-200 reactor vessel is an integration point with safety, as the reactor core fissile material inventory directly impacts reactivity in the core; monitoring reactivity is a primary safety function [56].

Likewise, measures for physical protection are closely tied with the facility spatial site layout, which is dictated by flow of nuclear material. This flow of material is simultaneously monitored for purposes of international safeguards accountancy as well as security concerns. The safeguards monitoring measures described in this chapter will need to be implemented in harmony with the details of chosen physical protection measurements.

7. Interfaces Identification and Assessment

Safety, Security, and Safeguards have each been discussed in depth individually in chapters 4, 5, and 6.

The safety assessment in chapter 4 provided an overview of the GPR-200 system from a safety point of view, summarizing the radioactive material sources along with their barriers to radionuclide transport, and reviewing the safety SSCs of the system (both active and passive) that support the primary safety functions of the GPBR-200. This assessment sets the scene for understanding the safety aspects of the safety-security and safety-safeguards interfaces discussed in this chapter. Further, the example PRA event sequence shown in chapter 4 also provides context to further PRA-related discussion in chapter 5 (security assessment), safety-security, and 3S interface discussion in this chapter.

The security assessment in chapter 5 followed the structure of the DEPO process, a method of performing SeBD. The process involves defining PPS requirements, designing the system with detection, delay and response elements, evaluating it using path analysis and performance testing, and iterating the design based on identified gaps or vulnerabilities. The DEPO process includes SeBD recommendations, which optimize facility costs by considering aspects early in the design process. The "Define PPS Requirements" step of the DEPO process overlaps with the other S regimes, as is seen in the safety-security, security-safeguards, and 3S interfaces described below. From the "Design" phase onwards, the process diverges in overlaps with the other S regimes due to the specificity of detection, delay, and response technologies and tactics.

The safeguards assessment in chapter 6 was based on the information coming from existing literature studies on safeguards for pebble-bed reactors, adapted and organized according to the data requested by the International Atomic Energy Agency (IAEA) in its Design Information Questionnaire (DIQ). The DIQ content conveniently summarizes all of the major elements of the GPBR-200 system that are relevant to safeguards, which come into play in the safety-safeguards, security-safeguards, and 3S interfaces discussed below.

This chapter will further explore these areas of overlap. The chapter begins with focusing on 2S interfaces identified in the GPBR-200 system, discussed in sections 7.1 to 7.3. This is followed by section 7.4 which examines 3S interfaces that have been identified in the GPBR-200 system.

7.1. Safety-Security Interfaces

Safety-security interfaces are not new in reactor design, but a key aspect of 3SBD is to consider all the requirements early in the design process to avoid treating security as a “wrapper” that is added to a facility after design completion. Consideration of security with safety earlier in the design process can lead to building designs, use of delay features, and response force strategies that are more refined and efficient. Similarly, consideration of safety with security in mind during the design process can lead to more robust safety systems that can be more resistant to adversary physical or cyber-attacks. Sabotage events (as opposed to theft), aimed at safety systems and ultimately release of radioactive material, lend a natural interface between safety systems and security. Safety-security implications may also arise from theft attempts if, for example, fuel elements are damaged or there is undue radiation exposure during the act. In safety, one seeks to practically eliminate event sequences that are considered highly unlikely with a high degree of confidence due to robustness of prevention measures: in the example of the GPBR-200, through inherent characteristics and passive systems. While such event sequences can be ruled out and thereby be not considered in the design, security vulnerabilities may bring such sequences back into design considerations. In the safety-security interface of the nuclear facility design process, one can identify these specific event sequences and pay special attention to them in the security domain.

The interfaces between safety and security have several dimensions. The following examples are not comprehensive but provide some key considerations for safety-security interfaces:

- Safety Systems and Physical Security
- Safety Systems and Cybersecurity
- Timeline Analysis and Response Force Strategy
- Effect of Radiation Dose on Responders
- Emergency Exits

The following sections describe these interfaces as they pertain to the GPBR-200 system.

7.1.1. Safety Systems and Physical Security

The plant's PRA is utilized in both safety and security assessments. Any safety significant system or control system pertaining to safety must be protected within a vital area in the overall design of the physical protection system. As an example of this, reactor control rooms are considered as vital areas, for the access they provide to various reactor safety controls. Regulatory requirements would define the sabotage logic model and thus the targets for the PPS to protect.

As mentioned in section 3.4, the control room for the GPBR-200 will contain all controls necessary to ensure safe operations of the reactor. This would include the ability to perform control rod movement, SCRAM the reactor, and adjust the inlet helium temperature. Along with this, sensors in the reactor would have corresponding read outs for the reactor operators to examine to understand the current state of the reactor. As such, the control room of the GPBR-200 represents the nerve centre of its operations, where maintaining safety and security is crucial. Integrating these two critical aspects is essential to protect both the facility equipment and the operators responsible for their efficient operation. In the control room environment, implementing adequate security measures is essential to prevent sabotage or malicious actions that could jeopardize the plant's operations and safety. Furthermore, security and safety measures for the control room should ensure optimal survivability of control room operators during events such as fires or radiological release that may fall out from sabotage or malicious actions.

In the GPBR-200 reference design, all these systems for the reactor core are included within the reactor building, and so denial of access to the building will prevent physical attack or compromise (malevolent misuse) of these systems. Other sources of radioactivity may fall under the responsibility of the security program to prevent radiological sabotage.

For the GPBR-200 reference design, several other radionuclide sources should be evaluated if they fall under the security program. The fuel handling system, as it controls the flow of pebbles through the core, will contain a significant source term. Similarly, used or broken fuel storage containers will also possess significant source terms. The helium purification system is responsible for the removal of impurities from the coolant loop. These impurities may include chemical impurities (e.g., oxygen) and gas-born fission products such as iodine, bromine, strontium, ruthenium, cesium, xenon, and krypton. Cesium may be a large dose contributor from the sabotage of the helium purification system [64]. The waste streams of the facility may also accumulate sufficient qualities of radionuclides to be a sabotage concern, especially those that process wastes from the helium purification system. The protection of these non-core sources of radioactivity should be considered alongside the protection of the core from radiological sabotage, and should be located within the facility, with provisions for the necessary cooling and layers of retention to prevent or mitigate the release of those sources. However, there are some key lessons learned from the physical protection space that should be applied here.

Safety and control systems should not be installed on the outside wall of a building structure to avoid ease of sabotage from the outside. The adversary path within the building should also be considered to avoid generating more vulnerable targets. The placement of decay heat removal systems, due to their linkage to air or water sources, should also be considered to avoid easy targets for an outside adversary. In the GPBR-200, there are not many energetic

mechanisms that can be exploited for sabotage. In particular, the GPBR-200 features effective passive cooling for decay heat removal, removing the need for reliance on sources of water or pressurized air for cooling. The regulatory requirements that define the sabotage logic model may include provisions for the length of security events, and that preventable, mitigatable, or reversible releases beyond this timeframe may be assumed to be negated given an expected offsite emergency response. In this case, the design of safety systems may favor measures to delay or mitigate releases in order to reduce the scope of SSCs required to be protected by the PPS. The design and performance of the SSCs included within the sabotage logic model directly relates to the required performance of the PPS. Integrating PPS goals within the safety design process may result in a more robust and easier to protect facility.

7.1.2. Safety Systems and Cybersecurity

Any safety significant system must also be robust to digital attacks. For example, the cybersecurity of the control room is very important. The interconnected nature of modern digital control systems found in the control room exposes them to potential cyber-attacks that can disrupt operations and cause safety incidents. The requirements for cybersecurity tend to be more prescriptive as opposed to performance-based since modeling cyber-attacks is currently difficult. The control systems must be appropriately protected depending on the degree of consequence of compromising the system under cyber-attack.

A Defensive Cybersecurity Architecture (DCSA) system [65] should be designed for any advanced reactor, such as the GPBR-200. The DCSA will define all the plant control systems and where they should fall in terms of cybersecurity level. The most critical plant systems (typically identified through vulnerability analysis of the facility) need the most stringent cybersecurity protection measures and may include an air gap from the rest of the systems. The security level will depend on the potential consequence if that system is compromised, so safety and cybersecurity have a natural linkage.

The cybersecurity program should have close ties with the physical security program and the safety program, to ensure the inclusion of physical security controls on cyber assets, and the consideration of cyber-physical sabotage attacks on the facility. As advanced and small modular reactors move to digital architectures and simplified safety systems, key instrumentation and control SSCs can play a large role in the safe and secure operation of the reactor. For example, passive core cooling systems may be designed to always have a flow path open, even during operation. These cooling paths may possess valves or dampers to facilitate reactor performance or maintenance. The control of these valves and dampers may present as sabotage targets for destruction, delay, disablement, or compromise by an adversary. Instrumentation and Control (I&C) connectivity may be undesirable to such high-value security targets, thus necessitating an adversary to directly access the SSCs, instead of through a cyber-attack.

In the case of remote deployment, some operators and vendors are seeking to reduce the required number of on-site personnel. Reactor designs for this deployment scenario often claim enhanced passive safety features and may even utilize remote operations if approved by the regulator. Such a scenario would likely mean safety systems can be operated remotely, which opens up new cyber threat vectors that need to be addressed. Thus, cybersecurity may play an even more essential role in remote deployment [4].

7.1.3. Timeline Analysis and Response Force Strategy

Advanced reactors such as the GPBR-200 generally have been designed with extended coping time, that is longer timelines before problems occur in the event of loss of cooling systems. Passive safety is also often worked into these designs. These enhanced safety features may provide value in the design of physical protection systems, but it is important to recognize that passive safety does not equate to passive security. Passive safety systems will not prevent a determined adversary from causing damage to a reactor and also are likely targets for adversary attack.

A VHTR core such as the GPBR-200 features low power density, high heat capacity, and a slender core shape (large height-to-diameter ratio). These features help ensure that transients that result from Loss of Forced Cooling events develop and occur over tens or hundreds of hours, providing a long 'grace period' in comparison with contemporary Gen-III reactors. Decay heat removal is facilitated by the presence of a RCCS to absorb heat from the outer surface of the Reactor Pressure Vessel (RPV) and carry it via natural circulation of air or water to external cooling panels. In case that an adversary disables the RCCS in an act of sabotage, the reactor building and surrounding soil become the ultimate heat sink, which however does not absorb heat as well as the functioning RCCS. In such a case, the RPV will not fail, but may sustain damage, eventually requiring repair or replacement. While massive fuel failure should not occur in the event of a failed RCCS, higher temperatures in the core may drive release of fission products from some parts of the core, potentially challenging dose limits to workers and at the site boundary. However, the core heat-up and cool-down takes place over many days, providing opportunity for mitigating actions to take place before fission products are released [29]. These longer timelines may allow for use of off-site response (both security and safety) for select scenarios to secure and make safe the facility.

In remote locations, the need for reduced onsite workforce and the potential long time for off-site response might represent a security issue: the reduced onsite workforce may be less effective in preventing adversary success in some attack scenarios, and the longer response time for off-site response may provide attack adversaries additional time to overcome delay measures of the physical protection system. Proper risk-based analyses should be applied to inform the relevant players about the optimal tradeoff between the need for onsite personnel and the reliance on off-site response.

7.1.4. Effect of Radiation Dose on Responders

Onsite responders typically are deployed either in towers, hardened fighting positions, the CAS, or within the reactor building itself. Generally, response is more effective when the armed responders are located closer to the targets. The radiation dose within the building should be considered because it will affect responder placement. For example, stations within a radiological area will not allow any food or drink which would make a less desirable work environment for the responders. These considerations should be part of the design and layout of the physical protection system. The GPBR-200 features highly automated processes in its fuel handling system that would be a part of the facility vital areas. Since such areas would require minimal human presence, the facility structure around them can be designed to minimize radiation dose to responders when they are in proximity to these areas.

7.1.5. Emergency Exits

In the establishment of location and the number of emergency exits, safety and security tend to have a natural tension about what is required. The need for more than one building exit for emergency events presents more doorways that need to be guarded in the event of an attack. Shark cages or mantraps can be designed to slow down attackers attempting to enter a facility, while still allowing egress in the event of an emergency. Previous designs have also used "safe havens" that allow workers to get to a protected area where they can seek temporary refuge and delay an immediate evacuation. The building design should consider safety and security requirements up front to optimize the design of emergency exits. In particular, any entrance or exit to or from vital areas needs to be securely protected even during emergencies. Applying these observations more particularly to the GPBR-200 would require a detailed design of the facility layout. However, noting again the minimal human presence that would be needed in the vital areas of the GPBR-200 that include highly automated processes such as the fuel handling system, such areas would correspondingly require minimal routes of egress as there is a reduction in the presence of staff, which would help mitigate this particular tension between safety and security.

7.2. Safeguards-Security Interfaces

Safeguards-security interfaces should also be considered early in the design process to help design optimal measurement and accounting systems that help to augment overall plant security. Given the GPBR-200 system characteristics, abrupt diversion of nuclear material for proliferation purposes is more challenging for the proliferator because several thousand pebbles are required to accumulate enough nuclear material for an IAEA significant quantity and because the fuel is so dilute and in a material form that is difficult to reprocess. On the other hand, protracted diversion of fuel pebbles (diverting smaller amounts of pebbles over an extended period of time to obtain 1 SQ of nuclear material) is less of a challenge for a proliferator, and very much a concern for nuclear safeguards. From a security perspective, theft of even small quantities of nuclear material would represent an economic loss for the operator and a huge mediatic event able to damage the nuclear sector with regards to public opinion. Four example safeguards-security interfaces are important to consider in developing efficient plant systems:

- Fuel Handling System and Containment/Surveillance
- International Safeguards and Physical Protection
- Remote Data Transmission
- Surveillance Systems

The following sections describe these interfaces as they pertain to the GPBR-200 system.

7.2.1. Fuel Handling System and Containment/Surveillance

The fuel handling system is an operator-controlled system that helps to count total numbers of pebbles but does not track or identify specific pebbles. The flow of the pebbles is of interest for both safeguards and security because it represents one of the key sub-systems where diversion of fuel pebbles could occur. All pebbles leaving the reactor go through a burnup measurement to determine if they can be re-inserted into the core or if they need to go to spent fuel canisters upon reaching a burnup limit. The burnup measurement helps to inform the total actinide content in spent fuel canisters. This system could be misused to remove fuel pebbles or specific target pebbles that maximize Pu content for diversion. Along with this, pebbles which are declared as damaged are removed and stored in separate spent fuel canisters, thus leading to an additional avenue for material diversion or reactor misuse. IAEA Containment and Surveillance (C/S) systems may need to be installed in these areas as part of their verification activities.

From either a domestic or international NMAC standpoint, accountancy of fresh or irradiated fuel in storage at a GPBR-200 facility is likely to be done on sealed canisters as opposed to individual pebbles. As pebbles which are damaged or broken are not necessarily identical to each other, their accountancy may be best handled by item or mass, instead of counting by sealed containers. However, from a physical protection standpoint, even the loss of one pebble could present enough radioactive material for a radioactive dispersal device. Therefore, containment and surveillance are important parts of maintaining control of all pebbles without identification of individual pebbles. Diversion pathway analysis may be utilized to determine ways to remove pebbles and to provide mitigation measures to make pebble removal very difficult.

7.2.2. International Safeguards and Physical Protection

While aspects of NMAC are utilized by physical protection systems and by domestic and international safeguards, additional, independent verification measurements will need to be added to the system for international safeguards requirements. These additional measures are to ensure that the host state is not diverting material for clandestine uses. In the context of the GPBR-200, there is nevertheless potential for security-safeguards synergies in shared technology since burnup measurements, reactor physics codes, pebble counting systems, and

containment and surveillance used for accountancy in physical protection systems may also be used for international safeguards verification.

In many reactors (beyond just the PBR design), there can be a tradeoff between security containment and safeguards inspector actions. While increased containment for the purpose of preventing or controlling the release and dispersion of radioactive substances can make it more difficult for an adversary to access a core, it also makes it more difficult for a safeguards inspector to perform checks and measurements of systems or material when needed. These tradeoffs in the safeguards-security interface should be considered when designing an advanced reactor for international deployment.

7.2.3. Remote Data Transmission

For a PBR which has large amounts of fuel constantly moving throughout the facility, some form of remote unattended monitoring may appeal to the IAEA to better account for the flow of material throughout the facility. However, the data being sought by safeguards practitioners may also be deemed sensitive from a security standpoint. Safeguards and security may be in conflict over what information leaves the facility remotely and how the remote data is transmitted [4]. However, in a future context where remote operation of the reactor is in place, facilities are made for the transmission of data for operational purposes, in which case there are potential synergistic avenues for data transmission for safeguards purposes. Efforts should be made to see if data can be collected and transmitted in a way that is beneficial to safeguards while minimizing or eliminating any security concerns that remote data transmission generates. The GPBR-200 in principle does not present difficulties different from any other nuclear facility subject to safeguards-relevant remote data transmission.

7.2.4. Surveillance Systems

Surveillance systems have long been a cornerstone of both safeguards and security. While the surveillance systems used by the IAEA and security personnel often differ in purpose, they may be similar in terms of equipment and functions. Notably, both groups heavily make use of cameras. For a variety of reasons, the IAEA does not utilize camera or other surveillance equipment that are designed for domestic security. Thus, designers should ensure that where locations in the facility could support both domestic and (independent) international surveillance systems, the implemented surveillance systems do not interfere with each other [4]. For example, safeguards and security surveillance systems may be competing for the same viewing angles, space, and power supplies. Including safeguards and security by design in an integrated fashion can seek to identify and address overlapping concerns early in the process to avoid complicated retrofitting later on. In the GPBR-200, surveillance of the automated fuel handling system will be important to implement for both safeguards and security purposes, in addition to surveillance of more traditional facility areas, such as fresh and irradiated fuel storage locations. The use of shared, innovative spatial awareness techniques may help further exploit potential synergies here.

7.3. Safeguards-Safety Interfaces

Safeguards-safety interfaces are often less discussed and written about than the other two types of interfaces. While the connections between safeguards and safety may be more difficult to make relative to the other interfaces, they are just as important and should be considered early on in reactor design to reduce any potential tensions which may arise later on and to maximize synergy between these two regimes. Some example safeguards-safety interfaces to consider include the following:

- Fuel Movement During Accidents or During Safeguards Inspections
- Access Restrictions
- Equipment Failure
- Damaged Fuel Elements

The following sections describe these interfaces as they pertain to the GPBR-200 system.

7.3.1. Fuel Movement During Accidents or During Safeguards Inspections

The way an accident progresses at a nuclear reactor can have important safeguards implications. In the event of a beyond design basis accident, some form of fuel movement, such as through melting, may occur. Such movement has both safety and safeguards implications. From a safety perspective, even during a beyond design basis accident, the spread of radioactivity and contamination should be minimized, which in turn helps to minimize the risk to workers, the public, and the environment. Thus, the goal of safety would be to keep any nuclear material movements confined to a small region which is ideally within the reactor vessel. This desire to limit fuel movement also has benefits for nuclear safeguards; the occurrence of an accident does not immediately remove the safeguards obligations of a state to the IAEA [4]. If the nuclear material spreads as the result of an accident, the task of accounting for said material is greatly complicated. Thus, enhanced reactor safety and reduced probability of a breach of containment layers by nuclear material also enhances the ability to ensure safeguards are maintained over said material until the IAEA and relevant authorities can negotiate how the material should be handled post-accident [4]. This interface synergy is exemplified in the case of the GPBR-200; the stability of TRISO kernels and fuel pebbles makes major losses of fuel integrity during an accident to be very unlikely.

In normal operating conditions, safeguards inspections might require the movement of nuclear material items in order to perform the necessary characterization measurements. Any nuclear material movement carries a potential safety risk. Therefore, a system design where nuclear material movement for safeguards purposes is minimized or—if unavoidable—duly addressed, would represent a positive interaction at a safety-safeguards interface. This is exemplified in the GPBR-200, in that the fuel handling process is highly automated, and nuclear material in storage is enclosed in canisters, which minimizes the manual movement of fuel during safeguards inspections.

7.3.2. Access Restrictions

Because PBRs have on-line refuelling, there may be little reason to intentionally shut down the reactor other than for maintenance purposes. As a result of this minimal down time, some areas where elevated radiation fields are present during reactor operations may be inaccessible due to safety reasons for extended periods of time. However, it is possible that a lack of access to some of these regions may increase the difficulty in applying safeguards to the facility, particularly those safeguards measures which need to be carried out by safeguards inspectors. By considering safeguards applications in the design phase, designers can work to ensure safeguards inspectors will be able to safely access relevant areas of the facility without impacting reactor operations nor jeopardizing the safety of any personnel. In the case of the GPBR-200, where nuclear material is almost always in difficult to access areas, facilities will need to be considered in the design stages that will enable dual containment and surveillance systems for safeguards purposes, along with a remote means to restore continuity of knowledge in case of containment and surveillance failures.

7.3.3. Equipment Failure

For a reactor design such as the GPBR-200, one can see the safeguards-related benefits of allowing the IAEA to utilize operator systems such as the FHS to make safeguards related measurements. However, when these devices perform tasks with a high degree of safety relevance, such as measuring and moving fuel, potential failures of the system may have safety-related consequences. Therefore, concerns may arise that the failure of safeguards equipment attached to operator equipment could impact the safety of the facility, which would be an unacceptable outcome. Thus, when considering options for safeguards practitioners to potentially utilize safety relevant facility equipment, it needs to be ensured that the failure of any safeguards-related equipment does not negatively impacts the safety of the facility [4].

Conversely, safety failures could also impact safeguards equipment; as such, there is some merit to considering the placement of safeguards equipment near safety equipment with lowest failure rate and/or lowest consequence of failure.

7.3.4. Damaged Fuel Elements

In the operation of any reactor type, there is the eventual possibility of encountering damaged or failed fuel. Typically, damaged or failed fuel may arise from the harsh temperature and radiological conditions in which the reactor operates. The occurrence of damaged or failed fuel is minimized by the application of high-quality assurance standards to the fuel fabrication process, to ensure the fuel is resilient to such conditions. VHTR pebble-bed reactor designs such as the GPBR-200 are unique in that the fuel elements undergo mechanical movement, rubbing against each other as they circulate through the reactor core. In such a design, the occurrence of damaged fuel can arise in normal operation conditions through friction and impacts in their mechanical movement through the reactor core, under a high temperature and harsh radiological environment. At the point that a fuel element leaves the bottom of the reactor core, installed devices should be present to recognize when fuel is damaged, and when so identified that the fuel element is removed from circulation in the core, and put in separate storage [9]. The need for recognizing as early as possible when fuel elements are damaged is motivated by safety concerns, to ensure that fission products are retained within the fuel elements. This safety concern also works synergistically with the simultaneous safeguards concern that the nuclear material be retained within the fuel elements for ease of nuclear material accounting. The separate storage of damaged fuel elements from other spent fuel elements is necessitated from a safety perspective, as the fuel elements may already be broken at the time of transit to storage or may have a propensity to break in further storage and handling. The strategy of separate storage again works synergistically with the needs of safeguards, in that damaged fuel elements that may have suffered loss of nuclear material cannot be accounted for as individual standardized items. Likely, the damaged fuel elements in general would need to be accounted for with bulk or non-destructive assay measurements, necessitating a different accountancy approach than through item counting that would be used in storage of intact spent fuel items.

7.4. 3S Interfaces

Interfaces between only two aspects of safeguards, security, and safety are often easier to identify and discuss given the more limited scope of considerations compared to a 3S interface. By defining these 2S interfaces, the commonalities across them can also be used to identify potential 3S interfaces. In looking across the various interfaces, the following topics have been noted as key interfaces between all three S regimes:

- Digital Connectivity
- Nuclear Material Containment and Access
- Plant Operations
- Reactivity Control and NMAC
- Fuel Characteristics
- Facility Layout Constraints for Equipment/Design Feature Installation

The following sections describe these interfaces as they pertain to the GPBR-200 system.

7.4.1. Digital Connectivity

As technology advances and the perceived deployment scenarios for nuclear reactors expand, there is an increased desire to make use of digitally connected technologies within the nuclear facility. This may include technologies which enable remote operation and monitoring of a reactor, autonomous or remotely controlled security features, and remote unattended monitoring systems for safeguards. While the individual systems may not be relevant to all three S regimes, they may all be linked via their connection to the cyber domain. Thus, potential

hacking of one system could cascade across platforms and lead to the compromising of other, unrelated systems. A single integrated cyber strategy as each regime may have different concerns regarding accessing and authenticating signals from their relevant equipment; however, nuclear facilities should focus on developing a robust digital network connectivity and response capability to ensure there are no weak points in one regime that could lead to compromises in the other. In the GPBR-200, there is a high potential for data sharing between systems for each of safety, security, and safeguards. Mechanisms for such data sharing and remote data transmission should be carefully designed and implemented in the context of digital connectivity to avoid weak points that would lead to compromises to the broader infrastructure. In particular, one should consider mechanisms for isolating cyber incursions from other components of the network without inhibiting the sharing of data between different systems.

A vital component of an effective cyber-security program is to account for the supply chain security for digital components: neglecting this may result in installing digital components that become a weak point that could lead to compromising the broader facility infrastructure. Where cloud-based monitoring the facility is employed, the security of its implementation and the components that consist in such a monitoring scheme must also be scrutinized. There is increasing interest in the use of artificial intelligence (AI) in nuclear energy systems, wherein the parameters, training, and behavior of the AI system must be carefully validated for secure implementation in its role in the nuclear facility.

7.4.2. Nuclear Material Containment and Access

All three regimes are also concerned about the location of nuclear material, how it can be accessed, and who can access it. Broadly speaking, it is the objective of the safety regime to ensure robust containment measures for the nuclear material to minimize the possibility of any release or spread of radioactivity that could present a danger to workers, the public, or the environment. This objective is largely supported by the security and safeguards regimes as well [66] The desire to bolster safety can lead to increasing numbers of barriers to reach the nuclear material, as well as using stronger barriers which have a lower probability of failure. These safety concerns largely align with security concerns as well; more barriers between the material and an adversary as well as harder to breach barriers leads to increased delay times, which improves the security of the facility. The security regime also favors increasing the difficulty of accessing the material through methods such as increasing the thickness of facility walls or limiting the number of entry points to the facility. These more robust barriers and reduced pathways to access the material may make the facility more resistant to accidents, which ultimately reduces the probability of a release. In the context of insider threats, however, more robust security measures might make it difficult for response forces to interdict insiders that are familiar with these measures. Likewise, this approach may benefit the safeguards regime as well. Nuclear material that is more difficult to access may be more difficult to divert or misuse, and having a reduced number of pathways to reach the nuclear material reduces the surveillance burden of the facility. However, making nuclear materials more difficult to access may also be problematic for some regimes. For instance, as mentioned previously, reducing the number of doors in the facility may increase the risk for plant workers during an emergency. Moreover, this may also hamper the safeguards regime; the harder the nuclear material is to access, the more difficult it may be to verify via in-person inspections. The appropriate balance needs to be struck between the three S regimes. Having all stakeholders involved in the discussion early on regarding nuclear material containment strategies and potential access limitations can enable the maximization of synergies between safeguards, security and safety while ensuring that tensions are minimized, and safety requirements are being met [66].

In the GPBR-200, most of the nuclear material inventory is in areas that are difficult to access, where a large fraction of the nuclear material is in a non-static configuration. The high level of automation of the GPBR facility should facilitate the required access arising from the needs of

safety, security, and safeguards. Further, the use of dual containment and surveillance systems and the sharing of required data on a need-to-know basis has the potential to support the needs of each regime.

7.4.3. Plant Operations

Planned operational programs should consider each of safety, security and safeguards in the design of operational procedures. Operating procedures, by their nature, are typically aligned with the configuration of the facility in terms of safety; however, procedures should not impact aspects of each of security, and safeguards systems. Similarly, procedures for each of security and safeguards should not impact systems of the other two regimes. By including operational considerations of each regime early in the design stages, conflicts between procedures for each regime can be mitigated. Similar considerations would apply to emergency response procedures. For emergency response plans, it is notable how nuclear material accountancy information maintained for safeguards purposes can be utilized for development of both safety and security emergency response plans: such information provides a statement of what materials a site holds, and where it is located, which is a key component of safety and security emergency response plans.

In the GPBR-200, the high level of automation of the facility, coupled with strong systems integration offers opportunities to define plant operation to be synergistic with the needs of the safety, security, and safeguards regimes.

7.4.4. Reactivity Control and NMAC

In the GPBR-200, information for reactivity control for safety purposes involves key components such as burnup measurements, reactor physics codes, and pebble counting systems. This is unique to PBR systems, as the burnup measurements and reactor physics codes will determine when to add fresh fuel or recirculate irradiated fuel as part of an online refuelling process for maintaining appropriate reactivity. These same components are part of the fuel handling system, which can also play a role in maintaining accountancy and control of the nuclear material for security and safeguards purposes, as noted above in the Security-Safeguards section. As such, there should be appropriate sharing of information, and the technology involved for synergistically accomplishing the goals of all three S regimes.

7.4.5. Fuel Characteristics

As mentioned in section 3.3.2, low power density of the reactor core is a characteristic of the GPBR-200 which helps ensure passive evacuation of decay heat under severe accident conditions. The low power density is in part made possible by the small amount of nuclear material (7 g of uranium; see Table 3.3) present in each pebble. From a safeguards point of view, this fuel characteristic means that a large number of pebbles must be acquired to amount to a significant quantity of nuclear material (75 kg of uranium, or 8 kg of plutonium) [10]. This would have the impact of reducing the number of possible proliferation pathways. Therefore, the application of safeguards could be more focused, which possibly reduces the number of resources required to apply safeguards to the reactor facility. Discussions between designers and the IAEA could bring out such synergies and determine how safeguards approaches might capitalize on these synergies. Similarly, from a security point of view, this same fuel characteristic can reduce the attractiveness of the fuel pebbles as targets for would-be thieves and could reduce theft pathways for stealing a desired amount of nuclear material.

Another fuel characteristic of the GPBR-200 is the high degree of burn up that can be achieved. As explained in section 3.1, the GPBR-200 can on average achieve a discharge burnup near 160 MWd/kg, corresponding to a Pu vector shown in Table 3.4 that features significant percentages of even-numbered Pu isotopes that reduce the material attractiveness of the spent fuel for proliferation purposes. The self-protecting nature of these Pu isotopes from their significant specific radioactive activities can also reduce the attractiveness of fuel for thieves or saboteurs, or delay or deter the success of the adversary. In order to achieve high pebble

burnup, certain safety characteristics must be satisfied, such as maintaining pebble integrity under a specified maximum power density while keeping a desired core power and reducing the core height [67].

A further characteristic of fuel pebbles in a PBR such as the GPBR-200 is that the fuel pebbles have tight control over the quantity of uranium in each pebble. Tight quality control during fuel fabrication is necessary for safe, controlled operation of the reactor. This tight quality control is useful for accountancy purposes in NMAC programs in security and safeguards downstream of fuel fabrication.

7.4.6. Facility Layout Constraints for Equipment/Design Feature Installation

The design of a nuclear facility may be compact, or complex, particularly for advanced modular reactors in comparison with existing nuclear power plants. Careful consideration must be made of how and where equipment and/or design feature installation required for each regime of safety, security and safeguards will be laid out in a manner that fulfills requirements for each regime while not negatively affecting the other two regimes. This should be done in the earliest design stages, to avoid costly retrofitting for any one regime, in order to avoid negative impacts on the other two regimes [4].

In the GPBR-200 for example, the FHS is a central aspect of the facility. As described in section 3.2, the FHS is a complex, dynamic system that continuously moves fuel within a physically constrained geometry while the reactor is operating. Each regime figures prominently in this system, with design features in place for ensuring criticality safety during operation, security of the fuel pebble system against theft or sabotage, and the safeguarding of the fuel through proper accountancy of the fuel pebbles with facilities for their verification by safeguards inspectors. Early discussions of what these design features entail for each of the regimes may prevent the need to make changes later in the design phase, and particularly after the facility construction has already commenced or is completed. These early discussions will also enable easy deployment of the features so as to reduce tensions between the regimes.

8. Key Insights

In this chapter, a summary and discussion of key insights learned from this work is provided. This chapter will compare the approach of triple pair-wise 2S interface identification vs. 3S interface identification and examine some critical aspects of the interfaces identified. This chapter will also discuss differences and commonalities among the interfaces identified, in terms of their conflicts and synergies, and further consider how this case study extends to other reactor types.

8.1. 3x2S by Design vs. 3S by Design

In the context of the design stages of nuclear reactors, reactor designers have traditionally had a strong safety culture, which has been developed over several decades of experience in compliance with regulatory requirements and capitalizing upon lessons learned in the past. In this context, reactor design has traditionally had a “safety-first” mindset. As such, it is not realistic to shift from a solely safety-focused culture to a comprehensive 3S by design approach in a single step for the nuclear systems that are already currently under design. A more practical approach would be to leverage the existing safety by design culture and complement this with a culture focused on proliferation resistance and physical protection via their bilateral interfaces with the more familiar safety domain. This can be accomplished by introducing each of the needs of security and safeguards in terms of their relationship with the needs of safety, leading to examination of safety-security and safety-safeguards interfaces. Including also the security-safeguards interfaces leads one to a triple pair-wise (3 x 2S) interface analysis. Additional analysis as a subsequent step beyond the 3 x 2S interfaces allows one to identify interfaces that are proper 3S interfaces. This approach is reflected in this case study, where in the previous chapter each of the pair-wise safety-security, safety-safeguards, and security-safeguards interfaces were considered, before discussing the proper 3S interfaces.

8.2. Critical Aspects of the Identified Interfaces

Among the most critical (or important) aspects of the interfaces considered are those that would compromise the aims of each S regime, resulting in potential conflicts between the regimes. This usually comes about through the sharing of space, time, or resources between the regimes. Equally, the consideration of each interface in how they share space, time, or resources can either mitigate these conflicts, or bring positive synergistic outcomes. The optimized sharing of space, time and resources is of particular relevance for small or advanced modular reactors that occupy smaller spaces and/or utilize fewer resources than traditional large nuclear builds. These critical aspects are summarized in Table 8.1 through Table 8.4 below.

Table 8.1. Critical aspects of identified safety-security interfaces.

Interface	**Shared Space/ Time/ Resources**	**Critical Aspects/ Recommendations for Industry**	**Consequences of Not Considering the Interface**
Safety Systems and Physical Security	Space/ Resources	• Safety and control systems should be in protected areas. • Adversary paths should avoid vulnerable targets, particularly decay heat removal.	Unforeseen vulnerabilities may arise that may need to be resolved through costly retrofits.
Safety Systems and Cyber-security	Resources	• Safety and control systems should be appropriately protected. • Remote operations can present security and safety vulnerabilities.	There may be inadequate protection against cybersecurity threats to safety systems.
Timeline Analysis and Response Force Strategy	Time/ Resources	• Longer timelines before core damage in loss of cooling enables longer response times in case of attack. • Need to protect from intentional sabotage.	There can be an imbalance between on-site and off-site response: too many on-site responders if off-site response can be utilized, or too few on-site responders if off-site response is not adequate.
Effect of Radiation Dose on Responders	Space/ Time/ Resources	• Need to minimize dose to responders in normal and emergency operations. • Automation/remote handling minimizes human presence in vital areas.	Plant protection may not be optimized or additional costs for shielding may be incurred.
Emergency exits	Space/ Time/ Resources	• Entrance/exit to/from vital areas need to be adequately protected, even during emergencies.	Security costs may escalate due to too many exits needing protection.

Table 8.2. Critical aspects of safeguards-security interfaces.

Interface	**Shared Space/Time/ Resources**	**Critical Aspects/ Recommendations for Industry**	**Consequences of Not Considering the Interface**
FHS and C/S	Space/Time/ Resources	• FHS does not track/identify specific pebbles; even the loss of one pebble is a security-relevant event. • C/S is needed in absence of tracking individual pebbles; diversion pathway analysis may provide mitigation of individual pebble loss.	Not making use of an integrated approach will reduce efficiency in complying with the security and safeguards regimes, potentially leading to more downtime and higher costs.
International safeguards and physical protection	Resources	• Aspects of NMAC are utilized by both security and safeguards; further independent verification needed for safeguards purposes. • Potential synergy in using shared signals from operator while maintaining independent verification.	Cost of NMAC and international verification may increase if shared use and synergies are not utilized.
Remote data transmission	Time/ Resources	• Data should be collected and transmitted in a way that is beneficial to safeguards while mitigating security concerns.	Being aware of potential implications safeguards remote data transmission to security will help to create a more efficient system design.
Surveillance systems	Space/ Resources	• The facility needs to accommodate security and safeguards surveillance systems.	Not considering the surveillance needs of security and safeguards early in design stages could lead to costly retrofits.

Table 8.3. Critical aspects of identified safeguards-safety interfaces.

Interface	Shared Space/Time/ Resources	Critical Aspects/ Recommendations for Industry	Consequences of Not Considering the Interface
Fuel movement during accidents or safeguards inspections	Space/Time/ Resources	• Fuel movement may occur in a beyond design basis accident; fuel damage may occur in movement for safeguards inspection. • Fuel movement has safety and safeguards implications.	Increased inspection time or safety issues for inspectors may ultimately induce operational inefficiency.
Access restrictions	Space/Time/ Resources	• Reactors with minimal downtime will potentially have areas with elevated radiation that are difficult to access.	Difficulty of access of non-static nuclear material inventory will increase inspection complexity in which inventory verification is required in the event of loss of continuity of knowledge.
Equipment failure	Resources	• Failed equipment that is under shared use can impact safeguards and safety.	The impact of failed equipment under shared use can result in severe incompliances in safety and safeguards.
Damaged fuel elements	Space/ Resources	• Safety and safeguards concerns work synergistically here to ensure that damaged fuel pebbles be identified early for adequate handling.	Failing to identify damaged fuel as early as possible can result in incompliances in safety and (if the element breaks apart) in nuclear material accountancy for safeguards.

Table 8.4. Critical aspects of identified 3S Interfaces.

Interface	Shared Space/ Time/ Resources	Critical Aspects/ Recommendations for Industry	Consequences of Not Considering the Interface
Digital Connectivity	Resources	• Robust, secure digital connectivity and response capability needed for ensuring no weak points in one regime would cascade across platforms and compromise other unrelated systems.	Unidentified vulnerabilities may increase the likelihood of attack, loss of revenue, failure of plant, and loss of trust in capabilities.
Nuclear material containment and access	Space/ Resources	• All three regimes are concerned about the location of nuclear material, how it can be accessed, and who can access it. • Potential conflicts can arise in terms of accessibility to safety systems, vital areas and nuclear material locations.	Cost of international verification may increase if containment can not be applied, or security vulnerabilities may increase if access is not adequately protected.
Plant operations	Space/Time/ Resources	• Planned operational programs should consider security and safeguards in the design of the procedures. • Procedures for each S regime should not jeopardize aspects of the other S regimes.	Can lead to inefficiencies in the overall system design or wasted resources when operational changes (design/procedure) to address events are not properly communicated among the 3S regimes.
Reactivity control and NMAC	Resources	• Sharing of information and technology for reactivity control and NMAC should be implemented synergistically.	This is not current practice but is possible in the future, with potential benefits in efficiency.
Fuel characteristics	Resources	• Some fuel characteristics that enhance safety also serve to reduce material attractiveness for diversion, theft or sabotage, as well as to reduce the number of possible proliferation pathways.	Not recognizing the potential opportunity for synergistically enhancing the effectiveness of security and safeguards approaches may incur future costs involved with the implementation of these approaches.
Facility layout constraints for equipment/ design feature installation	Space/ Resources	• Careful consideration must be made of how and where equipment and/or design feature installation required for each regime of safety, security and safeguards will be laid out in a manner that fulfills requirements for each regime while not negatively affecting the other two regimes.	Not considering this interface in the early design stages may incur costly retrofitting later in the operating life of the facility.

8.3. Differences and Commonalities of the Interfaces

Discussion about the differences and commonalities of the 2S interfaces considered can focus on some general characteristics summarized in Figure 8.1.

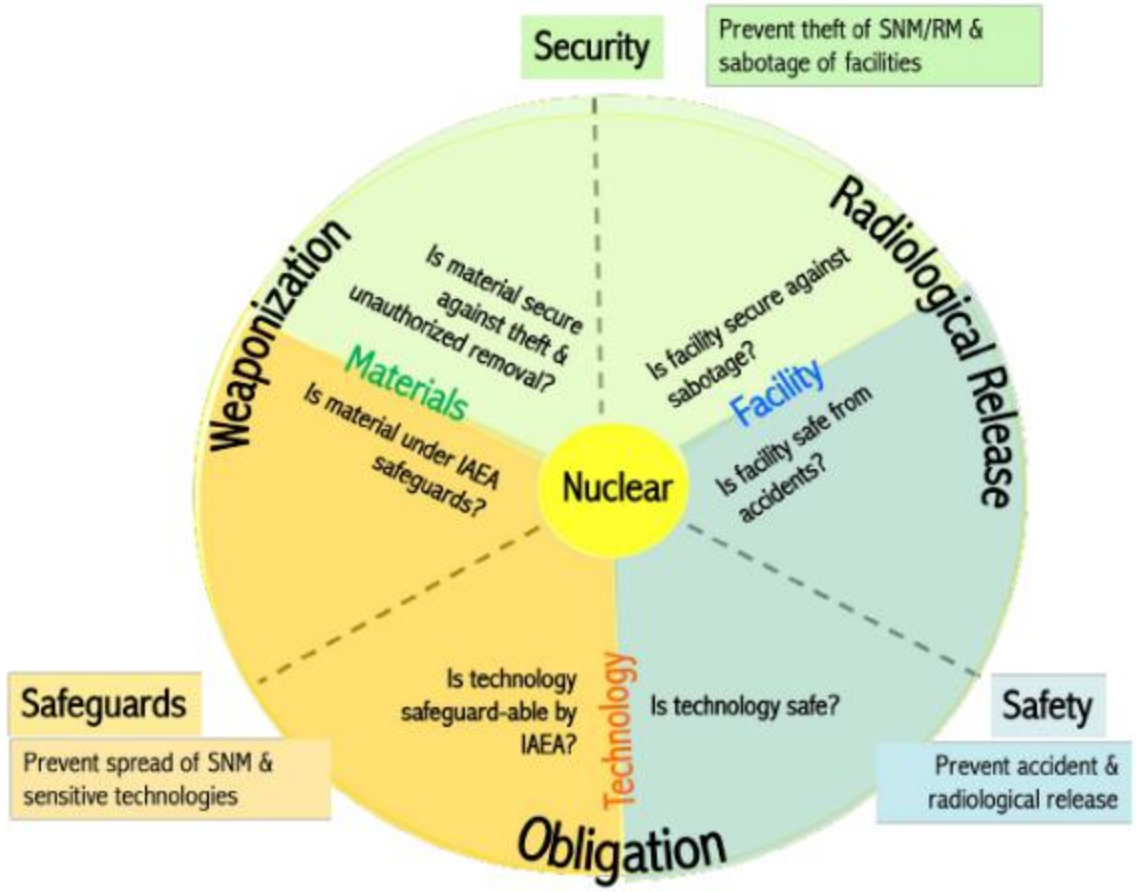


Figure 8.1. Some general characteristics of the three 2S interfaces [68].

In the safety-security interfaces, for example, there is a focus around the facility as a whole. The safety side of each interface asks, “Is the facility safe from accidents?” The security side of the same interface asks, “Is the facility secured against sabotage?” In this analysis, a few safety-security interfaces have been identified (see Table 8.1), where one sees these questions being addressed. The interfaces of safety systems with each of physical security and cybersecurity certainly have a focus of protecting the facility as a whole through the careful construction of each of these respective systems. In the matter of timeline analysis and response force strategy, one sees the safety interface in how the timeline for response is dependent upon the timeline before core damage or other problems in the event of loss of cooling, but the inherent safety features for the facility do not take away from the need to protect from intentional sabotage leading to radioactive release. Facility design also plays a role in how radiation dose is minimized to responders, and in how entrances and exits to and from vital areas are protected even during emergencies.

In the security-safeguards interfaces, there is a focus around the nuclear materials in the facility. The security side of each interface asks, “Is the nuclear material secure against theft and unauthorized removal?” The safeguards side of the same interface asks, “Is the nuclear material properly safeguarded?” In this analysis, a few safety-safeguards interfaces have been identified (see Table 8.2), where one sees these questions being addressed. For example, the inability of the fuel handling system (FHS) to track or identify specific fuel pebbles is a security concern (as the loss of one pebble is a security event). This concern signals the need for surveillance measures, where safeguards C/S systems could synergistically address that

need. By extension, this calls for the utilization of shared, innovative spatial awareness techniques to fulfill surveillance needs of both security and safeguards. Further, this surveillance data when remotely transmitted for security and/or safeguards purposes should be transmitted in a way that mitigates security concerns. Finally, aspects of NMAC are utilized by both security and safeguards, while safeguards do require further independent verification measures to ensure that the host state is not diverting nuclear material for clandestine purposes.

In the safety-safeguards interfaces, there is a focus around the technology employed in the facility. The safety side of each interface asks, “Is the technology safe?” The safeguards side of the same interface asks, “Does the technology surrounding the nuclear material make the facility safeguardable?” In this analysis, a few safety-safeguards interfaces have been identified (see Table 8.3), where one sees these questions being addressed. On the topic of fuel movement during accidents or safeguards inspections, technology plays a role in the fuel handling process and enclosed material storage strategies to ensure there are no major possibilities for an inspector to manually move fuel. Further, the technology behind the design of TRISO kernels and fuel pebbles makes major losses of fuel integrity to be very unlikely. The access restrictions discussed in Table 8.3 come about from the technology of the nuclear fuel cycle in the facility, making nuclear material in the facility difficult to access from a safety point of view, which has implications for the safeguards approach. Technical equipment can also fail, and where that equipment is shared, it can have implications for safety and safeguards. Further, technical features that intrinsically enhance safety can also synergistically have the potential to reduce possible nuclear material diversion and misuse strategies.

8.4. Applying a Generic 3S Approach to Advanced Reactors

Having performed the case study for the pebble bed VHTR design type, it is useful to think about what a generic 3S approach to advanced reactors would like. It can be seen from the summary of the identified interfaces shown in Table 8.1 through Table 8.4 above that the critical aspects of almost all of the interfaces discussed in this case study would apply generically to each of the six advanced reactor types considered by the Generation IV International Forum. In fact, just one security-safeguards interface (the first entry in Table 8.3), concerning the fuel handling system and containment and surveillance, would apply uniquely to the pebble bed VHTR design type. All of the other interfaces identified are concerned with reactor design facets that can be applied to other reactor design types. It should be kept in mind that the 3S interfaces identified in this study are examples, and not comprehensive in coverage; hence it is possible that this study may overlook some broader systemic issues. Nevertheless, it has been seen that many of the critical aspects of the 3S interfaces identified should be easily generalizable to other reactor types.

It should be noted that 3S interfaces should be accounted for through the various stages of the life cycle of a nuclear reactor facility, including design, construction, operation, and decommissioning. As has been mentioned in this report, 3SBD occurs in the earliest design stages, where 3S interfaces must be considered in plans for design, construction, and operation of the facility. While it is clear that 3S interfaces certainly come into play in design planning and during operation, they also come into play during aspects of construction and decommissioning where nuclear material is present on the site, wherein nuclear material security and safeguards must be executed in their interplay with nuclear safety.

8.5. Limitations of this Case Study: Additional Considerations for Adoption of 3SBD by Industry

This case study has followed a bottom-up approach. This approach is advantageous in that it allows for tailored 3S measures that address needs of the specific pebble bed VHTR reference design and focuses on the practical implementation of 3S measures and their resolution, to the extent that available information allows. The 3S interfaces identified in this study are examples and not comprehensive in coverage; hence it is possible that this study may have

overlooked some broader systemic issues. Nevertheless, it has been seen that many of the critical aspects of the 3S interfaces identified should be easily applied to other reactor types.

The value of this bottom-up case study is that it can significantly facilitate a future top-down 3S case study. The detailed insights and data collected from the bottom-up approach can inform the high-level analysis and strategic planning in a corresponding top-down case study. An advantage of a top-down approach is that it is comprehensive in nature, ensuring a integrated view of the case study system, and further ensuring alignment with standards and guidelines across different reactor types. The integration of a bottom-up case study with a top-down case study ensures that the strategic goals are grounded in practical, operational realities, leading to a more robust and effective 3S framework. An integration of these two approaches could be a topic for future work, wherein a structured approach to properly harmonize the two approaches together is essential.

It should be recognized that comprehensive 3S integration requires some up-front investment, for which one would desire significant cost savings over the life of the facility. To date, there has been no study (to the knowledge of the contributors to this case study) that quantifies potential long-term cost savings for implementing 3SBD. Such a study could employ quantitative case studies with cost-benefit analyses that demonstrate what significant return on investment there is from early 3S integration in comparison with post-construction retrofitting. A significant barrier in the past to undertaking such a study in a reliable manner that is relevant to deployment of advanced reactors in today's international markets is having access to detailed information relevant to the cost of deployment, operation, and decommissioning. As Generation IV nuclear energy systems come closer to deployment and more detailed information becomes available, the time also draws near for such a study to be undertaken. It is anticipated that a positive demonstration of cost savings when implementing 3SBD should catalyse more wide-spread adoption of 3SBD by the nuclear industry.

Another potential topic of future work is to develop a maturity model for 3SBD implementation, to the end of providing a benchmark to industry that could be used for ensuring that 3SBD is being followed in a comprehensive and effective manner. Such follow-on work could draw upon previous experience in actual 3SBD work, which continues to grow with time.

It should also be recognized national regulatory bodies vary widely in their approaches to nuclear security, and hence in their approaches to 3S integration. This is a particularly relevant point for industrial vendors looking to serve multiple international markets. The harmonization of regulatory approaches to nuclear security is an ongoing topic of discussion outside of the Generation IV International Forum, such as in efforts being undertaken by the IAEA's Nuclear Harmonization and Standardization Initiative [69]. The Working Group on Design and Safety Analysis from the IAEA's SMR Regulators' Forum has also considered 3S interfaces from a regulatory perspective [4].

It should be recognized that this case study has confined its attention to the reactor facility of VHTR PBRs such as the GPBR-200. No attention has been paid to, for example, security and safeguards aspects of fuel fabrication and how they would interface with each other and with relevant safety aspects. This is in part by design, as the Generation IV International Forum has traditionally confined attention to Generation IV reactor technology that is otherwise recognized to be part of a larger fuel cycle involving other aspects such as fuel fabrication, fuel recycling, and fuel waste management. One could extend this study to consider 3S interfaces that come into play in other aspects of the associated fuel cycle, such as fuel fabrication. For instance, the specialized TRISO fuel manufacturing ecosystem has security and safeguards implications with the supply chain in that ecosystem; one could pursue an in-depth look at the 3S interfaces in the upstream supply chain and fuel manufacturing process.

9. Conclusions

This report has summarized a case study of identifying and characterizing 3S interfaces in a notional VHTR pebble-bed reactor design. This bottom-up case study has sought to provide some guidance to reactor designers and vendors wishing to apply a 3S-by-design approach to the development of Gen-IV systems, by showing how to identify and characterize 3S interfaces. This is a foundational step to learning how to minimize conflicts between 3S interfaces and simultaneously exploit synergies among them. The case study began with a reactor reference design used to carry out assessments in each area: safety, security, and safeguards. These assessments provided the needed data for identifying and characterizing the 3S interfaces. In the identification process, both 2S and 3S interfaces were examined. In the process of this study, it was noted that among reactor designers there is typically a need to foster a security and safeguards by design approach to integrate with the already existing safety by design culture. Through an interim 3 x 2S analysis of the existing interfaces, the ultimate goal of a 3SBD culture among designers could be achieved in a smoother and quicker way, potentially allowing the industry to profit from the window of opportunity represented by Gen-IV systems. After completing the 3 x 2S exercise, the characterization of identified interfaces aids in determining which of them are actual proper 3S interfaces.

From the interface characterizations, some critical aspects to these interfaces were identified and summarized in chapter 8. Further, some commonalities and differences between these interfaces in how they interact with each other were summarized, giving generalizable insights into conflicts and synergies that are present among them. It was also observed that many of the interfaces listed in this report, except for the security-safeguards interface particular to the PBR fuel handling system, possess generic characteristics that can be readily applied to other Gen-IV energy systems. Consequently, numerous insights gained from this study can be readily applied by a variety of vendors and designers to their Gen-IV energy systems, beyond the VHTR pebble-bed design type. Also provide are some discussion outlining the limitations of this case study along with topics of potential future work.

10. References

[1] International Atomic Energy Agency, “IAEA Nuclear Safety and Security Glossary, 2022 (interim) edition”, IAEA, Vienna, 2022.

[2] International Atomic Energy Agency, “IAEA Safeguards Glossary”, IAEA, Vienna, 2022.

[3] International Atomic Energy Agency, “Applicability of IAEA Safety Standards to Non-Water Cooled Reactors and Small Modular Reactors”, Safety Reports Series No. 123, Vienna, Austria, 2023.

[4] Working Group on Design and Safety Analysis, “Safety, Security and Safeguards from a Regulatory Perspective: An Integrated Approach”, Phase 3 Report, IAEA SMR Regulators’ Forum, 2023.

[5] R. Peel, G. Foster, S. Aghara, “Nuclear Security and Safeguards Considerations for Novel Advanced Reactors”, King’s College London, 2022.

[6] A. D. Williams, B. Cipiti, A. Evans, “A Systems-Theoretic Framing for an Integrated Nuclear Energy Safety, Safeguards, and Security (3S) Approach”, Proceedings of INMM & ESARDA Joint Virtual Annual Meeting, 2021.

[7] B. D. Middleton, C. Mendez, “Integrating Safety, Operations, Security and Safeguards into the Design of Small Modular Reactors”, Proceedings of the ASME 2014 Small Modular Reactors Symposium, SMR2014, April 15-17, 2014, Washington, DC, USA.

[8] Z. Qin, “General Design of the _10 MW HTR”, 3rd JAERI Symposium on HTGR Technologies, JAERI, Japan, 1996.

[9] International Atomic Energy Agency, “Applicability of IAEA Safety Standards to Non-Water Cooled Reactors and Small Modular Reactors”, Safety Report Series No. 123, IAEA, Vienna, Austria, 2023.

[10] Generation IV International Forum, “GIF Very High Temperature Reactor Proliferation Resistance and Physical Protection White Paper,” GIF/PRPPWG/2022/005 , GIF, Paris, 2022.

[11] R. Stewart, P. Balestra, D. Reger, E. Merzari and G. Strydom, “High Fidelity Simulations of the run-in process for a pebble-bed reactor,” Annals of Nuclear Energy, vol. 195, 2024.

[12] A. Iyengar, National Nuclear Security Administration, Personal Communication, 2023 May 11.

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Fundamental Safety Principles, IAEA Safety Fundamentals SF–1, Vienna, 2006.

[14] SANDERS, K. E., POPE, R. B., LIU, Y. Y., SHULER, J. M., Interfaces among Safety, Security, and Safeguards (3S) – Conflicts and Synergies, Proceedings of INMM 56th Annual Meeting, Indian Wells, CA, USA, (2015).

[15] Margaret Ellenson, Kairos Power, Personal Communication, 2025 July 7.

[16] International Atomic Energy Agency, “Basics of IAEA Safeguards”, iaea.org, https://www.iaea.org/topics/basics-of-iaea-safeguards#:~:text=The%20objective%20of%20IAEA%20Safeguards,used%20only%20for%20peaceful%20purposes (accessed July 5, 2024).

[17] P. Karhu, M. Schraver, B. Stauffer, T. Hack, “Management of the interface of nuclear security and nuclear safety: what, why, and how”, IAEA-CN-278/185, IAEA International Conference on Nuclear Security: Sustaining and Strengthening Efforts, 2020 February 10-14.

[18] A. W. K. Yeung, “The ‘As Low As Reasonably Achievable’ (ALARA) principle: a brief historical overview and a bibliometric analysis of the most cited publications”, Radioprotection, 54:103-109, 2019.

[19] Idaho National Laboratory, “Cyber Informed Engineering”, inl.gov, https://inl.gov/national-security/cie/

[20] R. Stewart, P. Balestra, D. Reger, E. Merzari, G. Strydom, “High-Fidelity Simulations of the Run-In Process for a Pebble-Bed Reactor,” Annals of Nuclear Energy, vol. 195, p. 110193, 2024.

[21] Z. M. Prince, P. Balestra, J. Ortensi, S. Schunert, O. Calvin, J. T. Hanophy, K. Mo, G. Strydom, “Sensitivity analysis, surrogate modeling, and optimization of pebble-bed reactors considering normal and accident conditions,” Nuclear Engineering and Design, vol. 428, p. 113466, 2024.

[22] J. Zhang, F. Li, Y. Sum, “Physical Analysis of the Initial Core and Running-In Phase for Pebble-Bed Reactor HTR-PM,” Science and Technology of Nuclear Installations, 2017.

[23] E. Mulder, W. Boyes, “Neutronics characteristics of a 165 MWth Xe-100 reactor,” Nuclear Engineering and Design, vol. 357, p. 110415, 2020.

[24] P. Balestra, S. Schunert, W. Carlsen, A. Novak, M. D. DeHart, R. Martineau, “PBMR-400 benchmark solution of exercise 1 and 2 using the moose based applications: MAMMOTH, Pronghorn,” in Proceedings of PHYSOR 2020: Transition to a Scalable Nuclear Future, Cambridge, 2020.

[25] F. Vitullo, J. Krepel, J. Kililainen, J. Prasser, A. Paultz, “Statistical Burnup Distribution of Moving Pebbles in the High- Temperature Reactor HTR-PM,” Journal of Nuclear Engineering and Radiation Science, vol. 6, 2020.

[26] J. Leppänen, M. Pusa, T. Viitanen, V. Valtavirta, T. Kaltiaisenaho, “The Serpent Monte Carlo code: Status, development and applications,” Annals of Nuclear Energy, vol. 82, pp. 142-150, 2015.

[27] R. Stewart, J. Cavaluzzi, P. Balestra, G. Strydom, “Capturing the Run-In of a Pebble-Bed Reactor by Using Thermal Feedback and High-Fidelity Neutronics Simulations,” Annals of Nuclear Energy, vol. 207, p. 110697, 2024.

[28] H. Zhang, X. Wang, H. Li, J. Nie, J. Liu, “Design and engineering verification of HTR-PM fuel handling,” Advanced Materials Research, vol. 621, pp. 317-325, 2012.

[29] F. Chen, F. Li, H. Gougar, “Very High Temperature Reactor (VHTR) Safety Assessment, Revision 2.1,” Generation IV International Forum, 2018.

[30] IAEA ARIS, “Status Report 70 - Pebble Bed Modular Reactor (PBMR),” International Atomic Energy Agency, Vienna, 2011.

[31] C. DeDeaux, “Xe-100 Licensing Topical Report GOTHIC and Flownex Analysis Codes Qualification, Document no. 008585,” X-Energy LLC, 2023.

[32] J. Andrus, L. Nelson, J. Phillips, J. Wheelwright, “TRISO Fuel’s Safety Functions, Contributions to Reactor Safety, and Necessary Safety Limits”, Nuclear Technology, 2431779, 2024.

[33] K. Fleming, PROBABILISTIC RISK ASSESSMENT APPROACH FOR THE PEBBLE BED MODULAR REACTOR, Doc no. 039144, May 1st 2006.

[34] B. Waltes, K. Fleming, F. Silady, Alex Huning, and J. Redd, Modernization of Technical Requirements for Licensing of Advanced Non-Light Water Reactors High Temperature, Gas-Cooled Pebble Bed Reactor Licensing Modernization Project Demonstration Project Report, SC-29980-200 Rev 0, August 2018.

[35] M. Hamza, N. Joslin, G. Lawson, L. McSweeney, H. Liao, A. Vivanco, M. A. Diaconeasa, Identifying and Quantifying a Complete Set of Full-Power Initiating Events During Early Design Stages of High-Temperature Gas-Cooled Reactors, Reliability Engineering & System Safety, https://doi.org/10.1016/j.ress.2023.109688, Vol. 242, Feb 2024.

[36] F. Silady, LICENSING BASIS EVENT SELECTION FOR THE PEBBLE BED MODULAR REACTOR, Doc no. 040251, June 30th 2006.

[37] International Atomic Energy Agency, “Deterministic Safety Analysis for Nuclear Power Plants”, Specific Safety Guide No. SSG-2 (Rev. 1), IAEA, Vienna, Austria, 2019.

[38] International Atomic Energy Agency, “Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants”, Specific Safety Guide No. SSG-3 (Rev. 1), IAEA, Vienna, Austria, 2010.

[39] International Atomic Energy Agency, “Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants”, Specific Safety Guide No. SSG-4, IAEA, Vienna, Austria, 2010.

[40] M. L. Garcia, Design and Evaluation of Physical Protection Systems, 2nd edition, Sandia National Laboratories, 2008.

[41] International Atomic Energy Agency, “Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5”, IAEA Nuclear Security Series No. 27-G, Vienna, 2018.

[42] World Institute of Nuclear Security, “Implementing Security by Design at Nuclear Facilities”, WINS Best Practice Guide 4.1, Vienna, 2019.

[43] A. Evans, S. Sweet, D. Abell, B. Stromberg, M. McCullough, “Modularization of Small Modular Reactor Facilities: Physical Protection Recommendations”, Sandia National Laboratories, SAND2025-11085R, 2025.

[44] Zhenya Qin, “General Design of the 10MW HTR”, 3rd JAERI Symposium on HTGR Technologies, Feb. 15-16, JAERI, Japan, JAERI-Conf 96-010, pp.149-160 (1996).

[45] A. Evans, et al. “U.S. Domestic Small Modular Reactor Security by Design,” Sandia National Laboratories, SAND2021-0768 (2021).

[46] J. Russell, C. Stems, P. Blemell, A. Woo, “Deliberate Motion Analytics Fused Radar and Video Test Results Deployed Beyond the Perimeter Fence in a High Noise Environment”, Sandia Report SAND2021-5413 (2021).

[47] Lin, H., Ross, M., Mack, T., “Design of a physical security perimeter fencing system”, Proceedings - International Carnahan Conference on Security Technology, pp. 205–210, 5678719 (2010).

[48] International Atomic Energy Agency, “Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)”, IAEA Nuclear Security Series No. 13, IAEA, Vienna, Austria, 2011.

[49] Generation IV International Forum, “Evaluation Methodology for Proliferation Resistance and Physical Protection of Generation IV Nuclear Energy Systems”, Revision 6, GIF, Paris, 2011.

[50] International Atomic Energy Agency, “Identification and Categorization of Sabotage Targets, and Identification of Vital Areas at Nuclear Facilities,” IAEA Nuclear Security Series No. 48-T, Vienna, 2024.

[51] IAEA Form N-92 – IAEA Design Information Questionnaire Research and Development Facilities (Locations of Nuclear Material in Amounts Greater Than One Effective Kilogram). Online: https://www.nrc.gov/reading-rm/doc-collections/forms/iaea_n92info.html

[52] A. Torres, K. Him, T. Newton, J. Lee, C. Portaix, M. Cronholm and I. Antonelli, "A Safeguards Perspective on Pebble Bed Modular Reactors (PBMR) – Considerations, Approaches and Challenges," in Proceedings of the INMM/ESARDA Joint Annual Meeting, Vienna, 2023.

[53] D. Kovacic, P. Gibbs, L. Worrall, R. Hunneke, J. Harp, J. Hu, "Advanced Reactor Safeguards: Nuclear Material Accounting and Control," ORNL/SPR-2020/1849, Oak Ridge, TN, 2021.

[54] P. Durst, "Safeguards-by-Design: Guidance for High Temperature Gas Reactors (HTGRs) With Pebble Fuel," INL/EXT-12-26561, Idaho Falls, 2012.

[55] P. Gibbs, J. Hu, D. Kovacic, L. Scott, “Pebble Bed Reactor Domestic Safeguards: FY21 Summary Report”, ORNL/SPR-2021/170396, Oak Ridge, TN, 2021.

[56] D. Kovacic, P. Gibbs, J. Hu, D. Hartanto, W. Wieselquist, C. Ball, R. McElroy Jr., “Fuel Burnup and Fissile Material Loss and Production for Pebble Bed Reactor Nuclear Material Accounting”, ORNL/SPR-2022/2635, Oak Ridge, TN, 2022.

[57] P. Becker, A. Rialhe, J. Whitlock, J. Doo, B. Xia, J. Guo, H. Wang, “Implementation of Safeguards Measures at the High Temperature Gas-cooled Reactor Pebble-Bed Module (HTR-PM) in China and Proposed Safeguards by Design for Units to be Exported to Other States”, 2018 IAEA Symposium on International Safeguards, Vienna, Austria, 2018 November 5-8.

[58] International Atomic Energy Agency, “International Target Values 2010 for Measurement Uncertainties in Safeguarding Nuclear Materials”, STR-386, Vienna, 2010.

[59] H. Yücel, E. Yeltepe, A. Ö. Yüksel, H. Dikmen, “235U isotopic characterization of natural and enriched uranium materials by using multigroup analysis (MGA) method at a defined geometry using different absorbers and collimators”, Nukleonika, 60:615-620, 2015.

[60] C. K. Kim, D. Nakazawa, G. Duhamel, K. Raptis, A. Ruas, “Improved combined HRGS-TIMS method for rapid determination of Pu in nuclear material samples collected in the Rokkasho reprocessing plant”, Journal of Radioanalytical and Nuclear Chemistry, 328:49-63, 2021.

[61] J. B. Coble, S. E. Skutnik, S. N. Gilliam, M. P. Cooper, “Review of Candidate Techniques for Material Accountancy Measurements in Electrochemical Separations Facilities”, Nuclear Technology, 206:1803-1826, 2020.

[62] P. Gibbs, “Material Control and Accounting Systems – Requirements and Concepts”, ORNL/SPR-2022/2660, Oak Ridge, TN, 2022.

[63] H. Büker, “A Safeguards-System for Pebble Bed Reactors”, Journal of Nuclear Materials Management, pp. 391-399, Fall 1976.

[64] GA Technologies. Probabilistic Risk Assessment for the Standard Modular High Temperature Gas-Cooled Reactor. Report No. DOE-HTGR-86-011, Rev. 3, Vol. 1, 1987. https://www.nrc.gov/docs/ML1113/ML111310342.pdf.

[65] L. T. Maccarone, A. S. Hahn, M. T. Rowland, “System-Level Design Analysis for Advanced Reactor Cybersecurity”, Sandia Report SAND2023-11782, Sandia National Laboratories, 2023.

[66] D. Hanks, “Managing Safety, Security, and Safeguards (3S) Relationship: A National Regulatory Authority Perspective United States Nuclear Regulatory Commission”, Proceedings of the Institute of Nuclear Materials Management 54th Annual Meeting, 2013.

[67] T. Setiadipura, D. Irwanto, Zuhair, “Preliminary Neutronic Design of High Burnup OTTO Cycle Pebble Bed Reactor”, Atomic Indonesia, 41:7-15, 2015.

[68] J.-S. Choi, presented at an annual meeting of the Generation IV International Forum Proliferation Resistance and Physical Protection Working Group, 26 January 2023, updated 6 November 2024.

[69] International Atomic Energy Agency (IAEA), Nuclear Harmonization and Standardization Initiative (NHSI) [Online] https://nucleus.iaea.org/sites/smr/SitePages/Nuclear-Harmonization-and-Standardization-Initiative.aspx, accessed 2025 September 28.

(This page has been intentionally left blank)

THE GENERATION IV INTERNATIONAL FORUM

Established in 2001, the Generation IV International Forum (GIF) was created as a co-operative international endeavor seeking to develop the research necessary to test the feasibility and performance of fourth generation nuclear systems, and to make them available for industrial deployment by the 2030s. Under the new 2025 GIF Framework Agreement, GIF brings together countries, as well as Euratom, representing 27 EU member states, to co-ordinate research and develop these systems. GIF has selected six reactor technologies for further research and development: the gas-cooled fast reactor (GFR), the lead-cooled fast reactor (LFR), the molten salt reactor (MSR), the sodium-cooled fast reactor (SFR), the supercritical-water-cooled reactor (SCWR) and the very-high-temperature reactor (VHTR).

A report produced by

GEN IV International Forum

Expertise | Collaboration | Excellence

www.gen-4.org