TREASURE

Project Number 101164616

Deliverable D1.3

Non-proliferation issues, waste management of GFR

Lead Beneficiary: CTU

Due date: 30/09/2025 **Released on: 07/01/2026**

Authors:	**Radovan Stary, Sebastian Nyvlt, Petr Vacha**	
Version:	**1.3**	
For the Lead Beneficiary	**Reviewed by the Work package Leader**	**Approved by the Coordinator**
Pavel Zácha	**Jan Komrska**	**Boris Kvizda**

Dissemination level

PU	Public	X

Version control table

Version no.	Date of issue	Author(s)	Brief description of changes made
0.1	28/08/2025	See above	1st draft
1.0	05/11/2025	Petr Vacha	Review by the Lead Beneficiary
1.1.	10/11/2025	S. Bebjak, J. Heller	Review by the Coordinator and MST
1.2	20/11/2025	WP1 partners	Review by the partners Final version
1.3	25/11/2025	Members of SUJB	Detailed review by SUJB Integration of comments Final version

Funded by the European Union

Project information

Project number:	101164616
Project full title:	Towards reliable and safe GFR
Acronym:	TREASURE
Call:	HORIZON-EURATOM-2023-NRT-01
Type of action:	EURATOM Research and Innovation Actions
Project Coordinator Organization:	VUJE a.s.
Coordinator:	Boris Kvizda
EC Project Officer:	Cristina Fernandez-Ramos
Start date – End date:	01/10/2024 – 30/09/2028
Coordinator contact:	boris.kvizda@vuje.sk
Administrative contact:	jakub.heller@evalion.cz
Website:	www.projecttreasure.eu

Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the European Commission can be held responsible for them.

EXECUTIVE SUMMARY

Deliverable D1.3 provides an integrated assessment of non-proliferation considerations, nuclear security requirements, and waste-management implications associated with the fuel cycle of the ALLEGRO gas-cooled fast reactor (GFR) demonstrator under the TREASURE project. As ALLEGRO relies on MOX and UPuC fuels containing significant quantities of plutonium, its fuel cycle inherently falls within the highest categories of international safeguards and physical protection frameworks. The report therefore analyses the applicable safeguards obligations, the physical protection system (PPS) requirements, and design features that can strengthen proliferation resistance throughout the reactor's operational and post-irradiation stages.

From a non-proliferation perspective, the document reviews the fissile material inventories of candidate fuel assemblies, the IAEA timeliness goals, and the consequences of handling material that is classified as Category I nuclear material. While the first core will use HALEU fuel, the operational ALLEGRO cycle is based on MOX and UPuC fuels that contain plutonium compositions of proliferation relevance. Accordingly, the facility and its associated material flows must be subject to the highest level of safeguards, transparent accounting, and stringent control of undeclared activities.

The nuclear security analysis follows IAEA Nuclear Security Series guidance and outlines the process of designing a PPS tailored to a facility of this type. It describes the key steps of facility characterisation, threat definition, target identification, and PPS design and evaluation. The report presents a conceptual layout for a suitable multi-layered PPS based on defence-in-depth, including detection, delay, and response functions, supported by personnel reliability, access control, and robust organisational measures. Special consideration is given to the insider threat and the need for systematic personnel vetting and security culture. Given the presence of Category I material and the potential for high radiological consequences, the PPS must incorporate vital area identification (VAI) and meet the performance criteria for timely and effective response.

The deliverable also explores options to enhance the inherent proliferation resistance of ALLEGRO spent fuel. Because fast-spectrum irradiation leads to significant plutonium production and isotopic vectors of proliferation interest, the report outlines engineering and procedural strategies to make spent assemblies difficult to disassemble, divert, or process outside of industrial-scale facilities. These include structural design features that prevent non-destructive access to fuel pins, maintaining shielding and reflector masses during storage, and incorporating tamper-evident and forensic traceability measures. Such measures complement safeguards and reduce the attractiveness of the material for misuse.

Overall, the report concludes that while fast-reactor fuel cycles present unique proliferation and security challenges, these can be effectively mitigated by a combination of robust PPS design, strict regulatory oversight, and engineered proliferation-resistance features built into the fuel and storage systems. Deliverable D1.3 provides the technical and methodological basis for these measures within the TREASURE project and contributes to ensuring that the ALLEGRO GFR demonstrator can be developed and operated in compliance with European and international nuclear security and non-proliferation standards.

CONTENT

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

The issue of nuclear non-proliferation and the associated physical protection of nuclear materials are key pillars of international nuclear security. Particular attention is paid to facilities using MOX (Mixed Oxide Fuel) and UPuC (uranium-plutonium carbide) fuels, which contain fissile materials with a high proliferation potential. Effective control of the movement and security of these fuels is necessary not only to prevent their misuse to produce nuclear weapons, but also to minimize the risks associated with possible leaks, sabotage or terrorist threats. This report therefore focuses on the main aspects of nuclear non-proliferation and physical protection measures for the Allegro GFR reactor project.

2 FUEL CYCLE OF THE PROJECT FROM A NON-PROLIFERATION PERSPECTIVE

2.1 Fuel issue

The background materials [12] show that despite the innovative design, which could reduce the risk of misuse or proliferation of the material, the content of fissile materials is significant. From a non-proliferation perspective, the plutonium contained in MOX and UPuC fuels must be considered significant [5]. In the first core, HALEU fuel, which is a low-enriched nuclear material, is considered. However, the proposed approach from the perspective of non-proliferation and physical protection mainly considers the operational MOX and UPuC fuel. Existing procedures and regulations regarding the safeguards process and security do not distinguish among fissile materials in its form, but in its content. According to the background materials, the content of nuclear materials in standardized sets is as follows:

Initial fuel composition in 1 SA:	
isotope	mass (kg)
O16	6,33
U235	9,02
U238	37,995
total:	53,345

Tab. 1: Initial fuel compositions in 1 standard UOX assembly [12]

Initial fuel composition in 1 SA:	
isotope	mass (kg)
O16	4,178
U235	0,163
U238	22,812
Pu238	0,223
Pu239	4,618
Pu240	2,136
Pu241	0,61
Pu242	0,602
Am241	0,058
total:	35,4

Tab. 2: Initial fuel compositions in 1 standard MOX assembly [12]

From the above it follows that the U235 content in the UOX material will be 19.2%, which places it among the low-enriched material - LEU. In the case of MOX fuel, the share of plutonium in the total composition will be around 26%, while the share of Pu238 will be less than 3%.

2.2 Non-proliferation issue

The need for a systematic approach to account for and control access to nuclear materials drove states to form the foundations of a nuclear material accounting and systems in use for banking and industry, basic elements began to evolve for accountancy and control using ledgers to record, assay systems in determine utopic composition and weight, labels to identify contents, and secure locations to store and process these materials. The best parallel would be the precious metals industry where systems were put in place to not only account for and control the inventory but also to support deterrence and detection of both insiders and outsiders who intended to steal these materials [2].

2.2.1 Nuclear Material Accounting and Control

The State's regulatory framework should set forth requirements for the design and performance of NMAC systems at the nuclear facility level, including those related to nuclear security. Nuclear security requirements should be consistent with a graded approach similar to that applied to physical protection [3] regarding the stringency of measures to be taken based on the quantities and attractiveness of the nuclear material at facilities. The State may incorporate elements of this guidance, as appropriate, into the regulatory framework [15].

As in any system that is formed with specific goals in mind and where failure can result in severe negative consequences, extensive efforts are made to evaluate the system and address potential weakness so no single point of failure can result in a severe event. Within the nuclear community, this is referred to as defence in depth. While defence in depth is applied to many areas such as safety and physical security, it also plays a key role in NMAC All of the functions required by an NMAC will vary from state to state, but in general, key elements include:

- maintaining an up-to-date inventory of all nuclear material present:
- record of all receipts, shipments, and losses/gains;
- on each item is
    - unique identifier
    - location
    - isotopic composition
    - quantity
    - type of material

- access control to the facility and specific locations in the facility, as needed,
- initiate an alarm when specified measurement uncertainties are exceeded on items and mass balances, and when access controls are violated;
- identify the location of all alarms;
- in the case of missing nuclear materials, identify the specific items and their quantities and characteristics;
- assist in the timely resolution of any alarms, and
- provide the foundation for any investigation of serious events and for an emergency inventory to address potential missing items.

A comprehensive NMAC system should meet the goal of providing timely and accurate information on all nuclear material activities in the facility Through this capability, it should deter and, if necessary, detect any unauthorized access and/or activities to nuclear material [2].

2.2.2 Material Balance Area

Another function of NMAC management is the establishment of material balance areas MBA for the facility, An MBA is an area that is both a subsidiary account of materials at a facility and a single geographical area that has defined boundaries and is an integral operation [5]. It is used to desi the location and quantity of nuclear materials in a facility and is an area designated such that the quantity of nuclear material in each movement into and out of the area can be determined and is documented, and the physical inventory of the nuclear material within can be determined when necessary. To meet the requirement of determining the quantity of material moving into and out of the MBA and what is physically present, each MBA will have defined key measurement points (KMPs) for the MBA. A KMP is a location where nuclear material appears in such a form that it may be measured to determine material flow or inventory.

KMP is a location within an MBA where:

- Measurements of nuclear material flow or inventory are taken.
- These measurements form the basis for material accountancy.

KMPs are chosen based on:

- Accuracy and reliability of measurement instruments.
- Strategic points where material changes form (e.g., input/output of a process, storage).

KMPs will be included in the NMAC measurement control program to ensure that they are periodically calibrated and that their measurement precision and accuracy meet NMAC requirements [2].

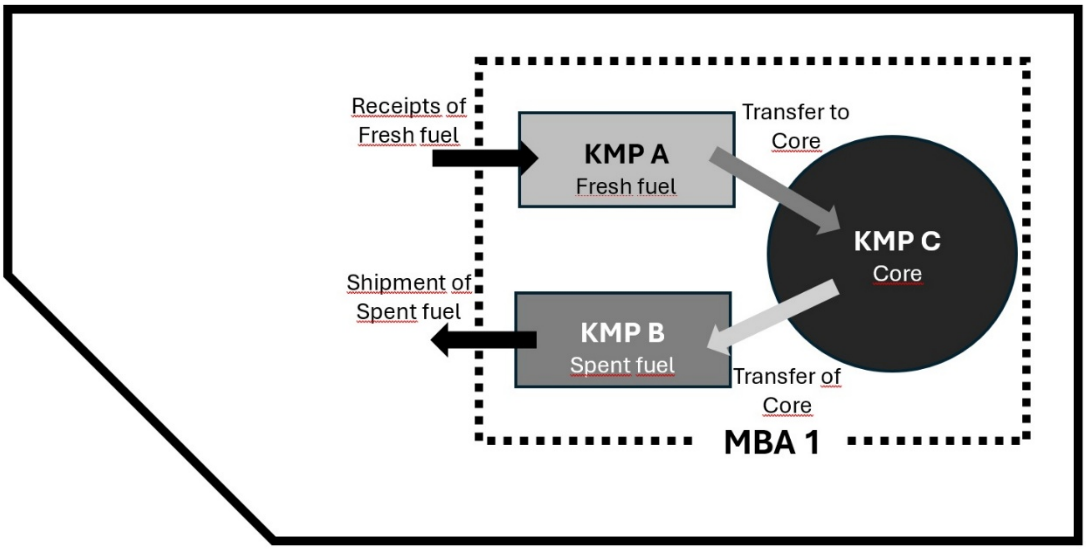

Figure 1: Example of MBA and KMP

2.2.3 MBA Categorization

For the purposes of determining MBA and KMP, the basic division of nuclear materials according to

- Material Type:

    - Direct-use material: Can be used for nuclear explosives without further enrichment or conversion (e.g., HEU, Pu).
    - Indirect-use material: Requires further processing before use in explosives (e.g., LEU, natural uranium).
- Physical Form:
    - Bulk material (powder, solution, etc.)
    - Itemized material (fuel assemblies, rods)
- Strategic Value:
    - Based on enrichment level, isotopic composition, and quantity.

For each MBA and the facility, the quantity and attractiveness of the nuclear material present will define the category of the MBA and/or facility. If under IAEA safeguards, the categorization of the facility and MBA used to establish inspection frequencies by the IAEA and to define various NMAC recommendations and other security recommendations are set forth in IAEA Nuclear Security Series documents. The categorization used by the IAEA is defined within Nuclear Security Series No. 13 [3] and is shown in Fig. 3

2.2.4 Interface NMAC with the Physical Protection

Coordination between Nuclear Material Accounting and Control (NMAC) and physical protection systems is essential for secure operations involving nuclear material. Both systems should complement each other, and some technical measures, such as surveillance cameras, can serve dual purposes. For these measures to be effective for material control, clear procedures and proper training are necessary to ensure personnel can distinguish authorized from unauthorized actions. Regular collaboration, such as during material relocation or access to secured areas, strengthens mutual support and improves information sharing between NMAC and physical protection teams [16].

When irregularities occur, investigations must involve both NMAC and physical protection personnel, with all relevant information documented and shared. Data from alarms, video surveillance, and access control should be reviewed alongside NMAC records to provide a comprehensive understanding of the situation. Facility procedures should define when immediate notification of physical protection is required and when initial investigation by NMAC personnel is appropriate. This structured approach ensures timely response and effective resolution of potential security issues.

2.3 The Project fuel and NMAC

From the perspective of the description of the proposed fuel given in Chapter 2.1, it is necessary to consider MOX and UPuC as significant. The use of MOX fuels and other fuels containing plutonium introduces several unique challenges for NMAC systems. These challenges arise because plutonium is a direct-use material under IAEA definitions, meaning it can be used in nuclear explosives without further enrichment. Here are the main issues NMAC addresses [15]:

1. **Higher Proliferation Risk**

- Plutonium is weapons-usable, so accounting must be extremely precise to prevent diversion.
- NMAC systems must ensure timely detection of any loss or unauthorized removal of even small quantities.

2. **Complex Measurement and Verification**

- MOX fuel contains uranium and plutonium, making isotopic composition more complex.
- Measurement techniques (e.g., NDA, calorimetry, neutron coincidence counting) are more challenging because:
  - Plutonium emits neutrons and gamma rays, complicating accurate mass determination.
  - High radiation fields require shielding and remote handling.

3. Material Categorization and MBA/KMP Design

- Plutonium-bearing materials fall under Category I (highest security level) [3].
- MBAs and KMPs must be designed to:
  - Separate plutonium streams from uranium streams.
  - Track material through fabrication, storage, and reactor loading.

4. Increased Uncertainty in Inventory

- MOX fabrication involves powders and scraps, which are hard to measure precisely.
- NMAC must address process losses, holdup in equipment, and account for residues.

5. Enhanced Physical Protection and Safeguards

- Because of the attractiveness of plutonium, NMAC systems integrate:
  - Tamper-indicating devices
  - Seals and surveillance
  - Frequent physical inventories and audits

The IAEA has established "conversion times" from estimates of the time required to convert different types and forms of nuclear material into forms suitable for weapons production. Table 3 provides background information on the estimates of the time required to convert nuclear material into a weapon. From these times, the IAEA has established the timeliness targets shown in the same table. The IAEA has assumed in these conversion times that, under INFCIRC/153 [5] safeguards, there is a possibility that clandestine facilities may exist and that material may be processed there. The introduction of the AP (additional protocol) by States has allowed additional factors to be considered to change this approach [2].

Nuclear Material	Material Form	Conversion Time	IAEA Timeliness Goals
Pu,HEU, or 233U	Metal	Few days (7-10)	1 month
Pure Pu components	Plutonium dioxide (PuO2	Few weeks (1-3	1month
Pure HEU or 233U compounds	Uranium dioxide (UO2	Few weeks (1-3)	1month
Mixed Oxide (MOX) of U and Pu	Unirradiated fresh fuel	Few weeks (1-3)	1 month
Pu, HEU, or 233U	In scrap	Few weeks (1-3)	1month
Pu,HEU, or 233U	In irradiated fuel	Few months (1-3)	3months
LEU, natural U, depleted U, and thorium	Unirradiated fresh fuel	Order of 1year	1year

Tab. 3: Definition of Timeliness Goals for IAEA Nuclear material Types [2]

The key reason for the safeguards is to ensure that undeclared facilities and activities do not exist. The timeliness and quantity targets, together with the safeguards activities, within the safeguards framework considered that such undeclared activities could not be excluded. With a broader conclusion, the IAEA could mitigate some of the activities, particularly where no special fissionable material was produced or stored for direct use, and apply less prescriptive, more individual safeguards. Thus, the IAEA could mitigate the time limit for spent fuel and fresh MOX fuel under integrated safeguards from 3 months to 1 year and from 1 month to 3 months, respectively.

3 THE PROJECT FROM A NUCLEAR SECURITY PERSPECTIVE

3.1 Physical protection in general

According to the recommendations of the International Atomic Energy Agency (IAEA), particularly the Nuclear Security Series documents (e.g. NSS No. 13 INFCIRC/225/Rev.5 – Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities), the physical protection system of nuclear facilities should meet general requirements and principles, which can be summarized in a few points [3]:

1**. Basic objectives**

- Protection against theft of nuclear material – preventing its misuse to produce a nuclear weapon or radiological device.
- Protection against sabotage of nuclear facilities or material – preventing acts that could lead to radiological consequences threatening the population and the environment.

2. Basic principles

- State responsibility – the state has the ultimate responsibility for establishing and controlling the physical protection system.
- Licensee responsibility – the operator bears the primary responsibility for the practical implementation and maintenance of protective measures.
- Nuclear safety and security culture – emphasis on the human factor, training and awareness.
- Defence-in-depth principle – a multi-layered system of physical protection (technical, organizational, administrative and personnel barriers).
- Threat assessment basis – the system is designed based on a defined set of threats (Design Basis Threat – DBT) or equivalent method.
- Minimization of internal and external threats – including insider risk.
- Flexibility and adaptability – the ability to respond to changes in threats and technologies.

3. Functional requirements

- Detection – the ability to identify unauthorized activities in a timely manner.
- Delay – measures that slow down intruders (physical barriers, checkpoints, technical systems).
- Response – prepared forces (armed forces, intervention units) that can stop the threat before it reaches the protected target.
- Access control – physical, administrative and electronic control of people and materials.
- Protection against cyber threats – securing control and monitoring systems.
- Redundancy and reliability – measures must work even if some parts of the system fail.

4. Supporting elements

- Personnel reliability and checks – to minimize the risk of insiders.
- Training and exercises – regular training of personnel and security forces.
- Emergency planning – coordination with the police, military, rescue services.

- Continuous improvement – revision of the system according to new knowledge and development of threats.

3.2 Physical protection system design

Designing an effective physical protection system (PPS) involves establishing PPS objectives, initial design or characterization of the PPS, evaluating the design, and in many cases, redesigning or improving the system. To establish objectives, the designer must begin by gathering information about the facility's operations and conditions, such as a comprehensive description of the facility, operating conditions, and physical protection requirements. The designer must then define the threat. This includes considering factors about potential adversaries such as class, capabilities, and range of tactics. Next, the designer should identify targets. Targets can be physical assets, electronic data, people, or anything that could impact business operations. The designer now knows the PPS objectives, i.e., what to protect from whom [1].

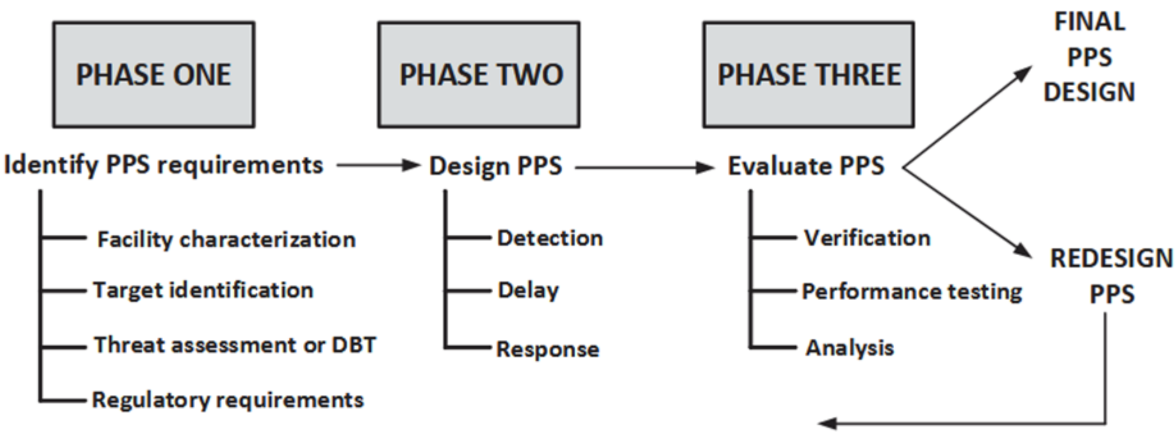

Figure 2: PPS design and evaluation process outline [7]

A graphical representation of the PPS methodology is shown in Figure 1. As mentioned above, the first step in the process is to establish the objectives of the protective system. To formulate these objectives, the designer must

- characterize (understand) the operation and conditions of the facility,
- define the threat,
- identify the targets.

3.2.1 Facility characterisation

Characterizing the operation and conditions of a facility requires developing a thorough description of the facility itself (location of site boundaries, building location, building interior plans, access points). It also requires a description of the processes within the facility and identification of all existing physical protection elements [1].

3.2.2 Threat definition

The State should define requirements based on the threat assessment or design basis threat for the physical protection of nuclear material in use, in storage, and during transport, and for nuclear facilities depending on the associated consequences of either unauthorized removal or sabotage [3]

In terms of defining and assessing the threat, it is necessary to gather information about the adversary for a given facility that answers three questions [1]:

1. What class of adversary should be considered?
2. What is the range of adversary tactics?
3. What are the adversary capabilities?

Adversaries can be divided into three classes: outsiders, insiders, and outsiders in collusion with insiders. For each class of adversary, a range of tactics (deception, force, stealth, or any combination thereof) should be considered. Deception is an attempt to defeat a security system by false authorization and identification; force is an overt, violent attempt to overcome a security system; and stealth is any attempt to defeat a detection system and secretly enter the facility. For any given facility, there may be multiple threats, such as an outside criminal, a disgruntled employee, a competitor, or some combination of the above, so the PPS must be designed to protect against all these threats. Selecting the most likely threat, designing the system to meet that threat, and then testing to verify the system's performance against other threats will facilitate this process. Finally, the target identification for the facility should be performer [8].

3.2.3 Target identification

Targets may include critical assets or information, people, or critical areas and processes. A thorough review of the facility and its assets should be performed. Questions such as "What losses will occur if this facility is sabotaged?" will help identify the assets or facilities that are most vulnerable or that create unacceptable consequences.

Target identification provides the basis for the design of a PPS, focusing on what to protect, while PPS design addresses how to protect. Target identification is the evaluation of what to protect, regardless of the threat or difficulty of providing physical protection. In other words, target identification determines the areas, assets, systems or activities to be protected, and generally those that have undesirable consequences in the form of loss to the business. The threats to these items and the ease or difficulty of protecting the items from a particular threat are considered after the items are identified.

Primary targets can be both nuclear materials and systems and equipment important to nuclear safety. Secondary targets can also include PPS components that can be attacked to reduce the effectiveness of the system and facilitate an attack. Identification of both types of assets is often necessary, depending on the objectives of the threat, its capabilities and motivation, and the consequences of losing the asset.

The primary factor in determining the physical protection measures against unauthorized removal is the nuclear material itself. Figure 2 categorizes the different types of nuclear material in terms of element, isotope, quantity and irradiation. This categorization is the basis for a graded approach for protection against unauthorized removal of nuclear material that could be used in a nuclear explosive device, which itself depends on the type of nuclear material (e.g. plutonium and uranium), isotopic composition (i.e. content of fissile isotopes), physical and chemical form, degree of dilution, radiation level, and quantity [3].

TABLE 1. CATEGORIZATION OF NUCLEAR MATERIAL

Material	Form	Category I	Category II	Category III[c]
1. Plutonium [a]	Unirradiated[b]	2 kg or more	Less than 2 kg but more than 500 g	500 g or less but more than 15 g
2. Uranium-235 (^{235}U)	Unirradiated[b] – Uranium enriched to 20% ^{235}U or more	5 kg or more	Less than 5 kg but more than 1 kg	1 kg or less but more than 15 g
	– Uranium enriched to 10% ^{235}U but less than 20% ^{235}U		10 kg or more	Less than 10kg but more than 1 kg
	– Uranium enriched above natural, but less than 10% ^{235}U			10 kg or more
3. Uranium-233 (^{233}U)	Unirradiated[b]	2 kg or more	Less than 2 kg but more than 500 g	500 g or less but more than 15 g
4. Irradiated fuel (The categorization of irradiated fuel in the table is based on international *transport* considerations. The State may assign a different category for domestic use, storage and *transport* taking all relevant factors into account.)			Depleted or natural uranium, thorium or low enriched fuel (less than 10% fissile content)[d, e]	

Note: This table is not to be used or interpreted independently of the text of the entire publication.

[a] All plutonium except that with isotopic concentration exceeding 80% in plutonium-238.

[b] Material not irradiated in a reactor or material irradiated in a reactor but with a radiation level equal to or less than 1 Gy/h. (100 rad/h) at 1 m unshielded.

[c] Quantities not falling in Category III and natural uranium, depleted uranium and thorium should be protected at least in accordance with prudent management practice.

[d] Although this level of protection is recommended, it would be open to States, upon evaluation of the specific circumstances, to assign a different category of physical protection.

[e] Other fuel which by virtue of its original fissile material content is classified as Category I or II before irradiation may be reduced one category level while the radiation level from the fuel exceeds 1 Gy/h (100 rad/h) at one metre unshielded.

Figure 3: Categorisation of Nuclear Material [3]

The categorization specified in Figure 2 is based on the attractiveness of material for the potential construction of a nuclear explosive device and cannot be directly applied to protection against sabotage. For each nuclear facility, an analysis, validated by the competent authority, should be performed to determine whether the radioactive inventory or safety system has the potential to result in unacceptable radiological consequences, assuming that the sabotage acts will be successfully completed while ignoring the impact of the physical protection or mitigation measures. From this perspective, we recognize the term vital area, which is defined as "Area inside a protected area containing equipment, systems or devices, or nuclear material, the sabotage of which could directly or indirectly lead to high radiological consequences" [3].

Sabotage can have serious consequences, and successful sabotage could lead to conditions that compromise safety and security objectives. Successful sabotage involves the successful destruction of not only the physical protection system but also the facility's safety systems and emergency management arrangements. Sabotage protection measures should therefore be designed and evaluated in collaboration with nuclear safety experts, nuclear security experts and emergency management experts, with the involvement of sabotage protection experts from various relevant authorities [6].

- Type 1 sabotage threat scenarios include criminal acts or other intentional unauthorized acts committed by insiders or external adversaries who gain access to the facility (with or without internal assistance). This category includes cyber threats combined with physical attacks.
- Type 2 sabotage threat scenarios include attacks initiated from outside the facility boundary that do not require an adversary to be present on site and have the potential to result in unacceptable radiation consequences or high radiation consequences. Examples of such attacks may include remote attacks, such as aerial attacks using drones, missiles, or aircraft, as well as attacks using directed energy weapons; chemical explosions; or remote destruction of a heat sink. Type 2 sabotage threat scenarios may include cyber-attacks.

For Type 1 sabotage threat scenarios that could lead to high or greater radiological consequence situations, a process should be used to identify sabotage targets and appropriately assign vital areas within the physical protection system to protect those targets.

If the design threat capabilities defined by the State are sufficient to cause a Type 2 sabotage threat, it should be analyzed whether the protection of sabotage targets in vital areas is sufficient against the potential effects of such sabotage threat scenarios [6].

To prevent radiological sabotage of a nuclear facility it is necessary to prevent significant safety system or core damage and spent fuel sabotage. Vital areas should be identified to protect a minimum set of the systems, personnel, and equipment needed to prevent these events.

Vital Area Identification (VAI) is the process of identifying the areas of a nuclear facility that must be protected to prevent malicious acts that could directly or indirectly endanger the public health and safety by exposure to radiation. VAI involves the use of logic models (see Figure 3) to systematically identify all the malicious acts or combinations of malicious acts that could lead to radiological sabotage. The models available in the plant probabilistic risk assessment and other safety analyses provide a great deal of the information and basic model structure needed for the sabotage logic model [13] [6].

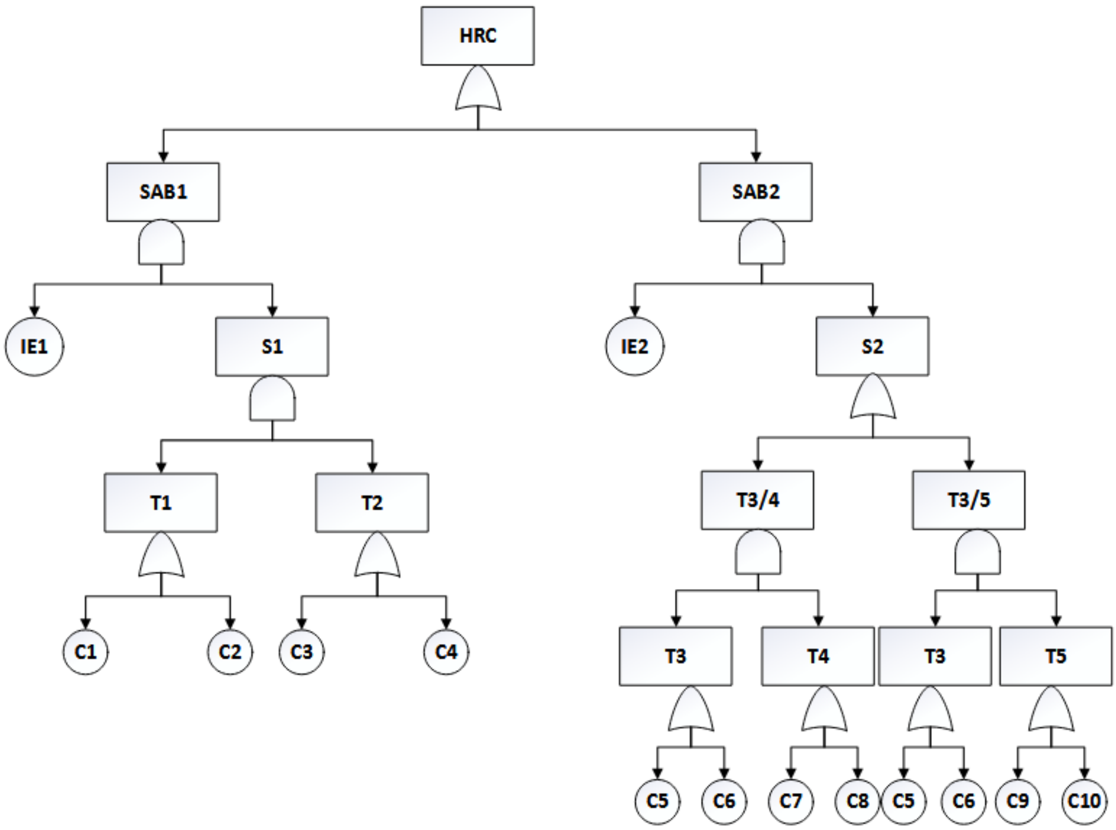

Figure 4: Example of logic model [6]

3.2.4 PPS design and evaluation

After Phase 1, where we have defined the basic system requirements, we can proceed to the design of the PPS itself. The design of the PPS must be such that all safety and security requirements are adequately met. During Phase 2, the designer determines how best to combine physical protection measures, such as physical barriers, sensors, procedures, video surveillance, communication equipment and responses, into a PPS that meets the protection requirements, taking into account other considerations such as the initial and life-cycle costs of the PPS and the potential impacts of the design on nuclear material accounting and control, safety and operations. The overall objective is to ensure that the PPS meets the protection requirements by providing an appropriate balance between detection, delay and response functions while allowing the facility to operate effectively. The nuclear facility security plan should reflect the final PPS design [7].

Once the objectives of the PPS and its design have been determined, it is necessary to conduct an analysis of the effectiveness of the design in meeting these objectives. This analysis can take two forms – quantitative or qualitative. To protect assets with unacceptably high consequences of loss, a thorough quantitative analysis is required, even if the probability of an adversary attack is low. This is characteristic of highly secure systems found in commercial nuclear power plants or other critical infrastructures.

4 OUTLINE OF A POSSIBLE PPS DESIGN FOR THE PROJECT

The initial project criteria in terms of a possible design of a physical protection system are not yet fully defined. The tender documents show that the aim is a facility with a cycle assuming lower demands from a non-proliferation perspective, which does not necessarily have an impact on ensuring the physical protection of the facility. It is clear from the supporting materials for the project that the Pu content will be significant, in forms and volumes that, according to the classification in table Figure 2, fall into Category I from a security perspective. Furthermore, according to the documents [14] and the PSA assessment carried out, a radiation extraordinary event with unacceptable radiological consequences is not excluded. For these reasons, it is necessary to count on the identification of a vital area according to the recommended methods (see 3.2.3). A possible scenario for the design of a physical protection system can therefore be proposed using the standard procedure according to IAEA recommendations [3].

4.1 Project Facility characterisation

The facility will be located on a smaller area of several hectares. It will consist of five basic parts (buildings), namely (due to the hypothetical nature of the project, it is greatly simplified):

- Reactor building
- Generator building
- Fresh fuel storage
- Spent fuel storage
- Administration, etc.

Regarding the operation and maintenance of the facility, it is assumed, as with the size of the facility, to be smaller in scale compared to a classic NPP. Operation will be continuous with campaigns lasting several months or years. The number of employees could be conservatively estimated at several hundred.

4.2 Project Target identification

Every PPS system is an integrated detection, delay and response system that should be effective against both tampering and sabotage. It should include people, procedures and equipment that provide defence in depth, with a graded approach [7]. For these reasons, it is necessary to identify targets in each area, categorize them and design the system based on this analysis. Basically, we distinguish 4 basic areas:

- Area outside the facility
- Limited area
- Protected area
- Inner area/vital area

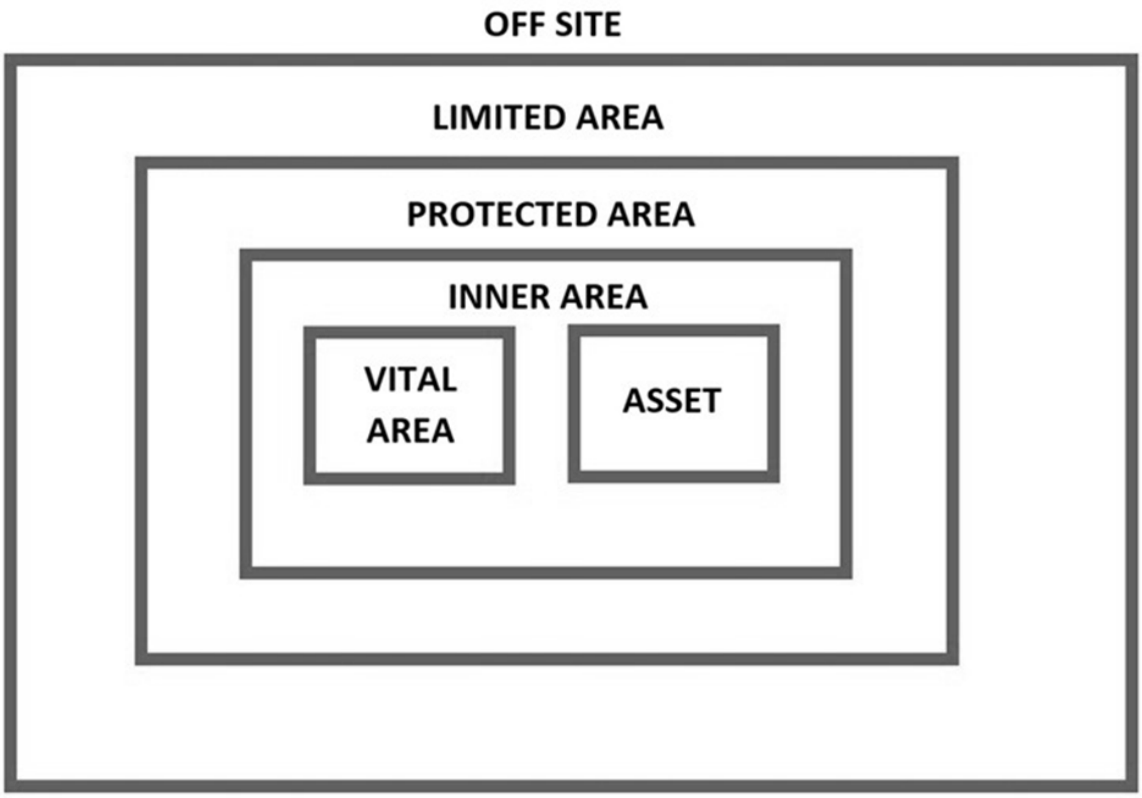

Figure 5: Physical protection Areas

It is true that within the framework of applying the rule of defence in depth, we place material or vital areas in areas (see Figure 4) according to their potential attractiveness or radiological consequences in the event of sabotage. In general, nuclear material of a lower category is placed deeper in the system than a higher category. That is, material of category I is usually placed in an internal area, category II in a protected area and category III in a guarded area. For vital areas, it is true that they are placed in an inner area.

Given the fuel composition for this type of reactor (MOX, UPuC), it can be classified as Category I according to Table 2. The initial charge of HALEU type fuel will have low enrichment (see Table 3), but the physical protection design must be based on the categorization of the operating fuel materials.

Nuclear material Category I should be used or stored within an inner area. An inner area could also be a vital area. An inner area should provide an additional layer to the protected area for detection, access control and delay against unauthorized removal. Inner areas should be appropriately secured and fitted with alarms when unattended [3]. An outline of the location of individual parts of the hypothetical GFR facility can be seen in the diagrams Figure 5.

4.3 Project Threat definition

Threat identification and the role of the Design Basis Threat (DBT) document is that it determines the reference threat to which the entire physical protection system of a nuclear facility is dimensioned. It is the regulator's basic tool for unifying requirements and ensuring that protection is adequate, effective and up to date. DBT is usually created by the regulator in cooperation with the police, military authorities and intelligence community. Given the hypothetical nature of the project facility, it will not be considered in this document.

4.4 Insider threat issue

The IAEA defines an insider threat as any individual with authorized access to nuclear material, associated facilities, sensitive information, or sensitive systems who could commit or facilitate a criminal or intentional unauthorized act, such as theft or sabotage [3]. This malicious act could be intentional or unintentional, and insiders leverage their unique access, authority, and knowledge to cause harm to the organization or its assets.

The specifics of the project are in its smaller size compared to the NPP and in the smaller number of employees. But here too, it will be necessary to pay attention to the division of the facility into individual parts into which a specific employee has the right to enter and what activities to perform. As in other critical infrastructure facilities, it is necessary to pay attention to a consistent control of the validity of security clearances and psychological tests and, last but not least, to quality management, safety culture and human resources issue.

4.5 Project PPS

The nature of the facility after the identification and categorisation of material and vital aeras in individual layers will require all measures of protection in depth with basic elements of physical protection.

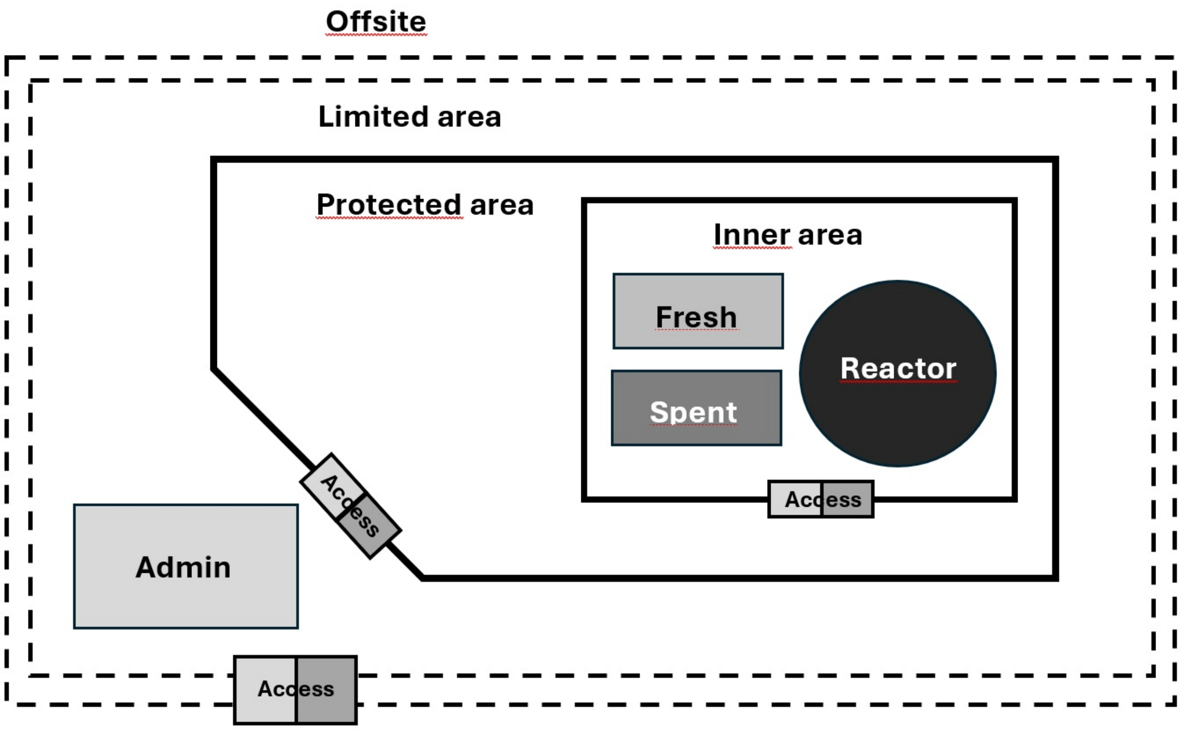

Figure 6: Schematic of a Project facility

Detection and its assessment will have to be at all layers to ensure timely information about an event of malevolent origin. The purpose of physical protection measures is not only to detect and evaluate the signal of the intrusion in time, but also to gain time to prepare a response through appropriate delay systems. In terms of delay elements, it is recommended to act tactically from the very beginning of the Limited area. Physical barriers and the regime at access points should be designed thoroughly to ensure not only thorough detection of activities, but also sufficient delay in the event of an attempt to overcome them. The purpose of delay is to extend the time to complete the action and gain time to prepare an adequate intervention. In the case of detection, we monitor its probability parameter and assessment P_D, and for delay elements, we monitor the delay time T (see Figure 6).

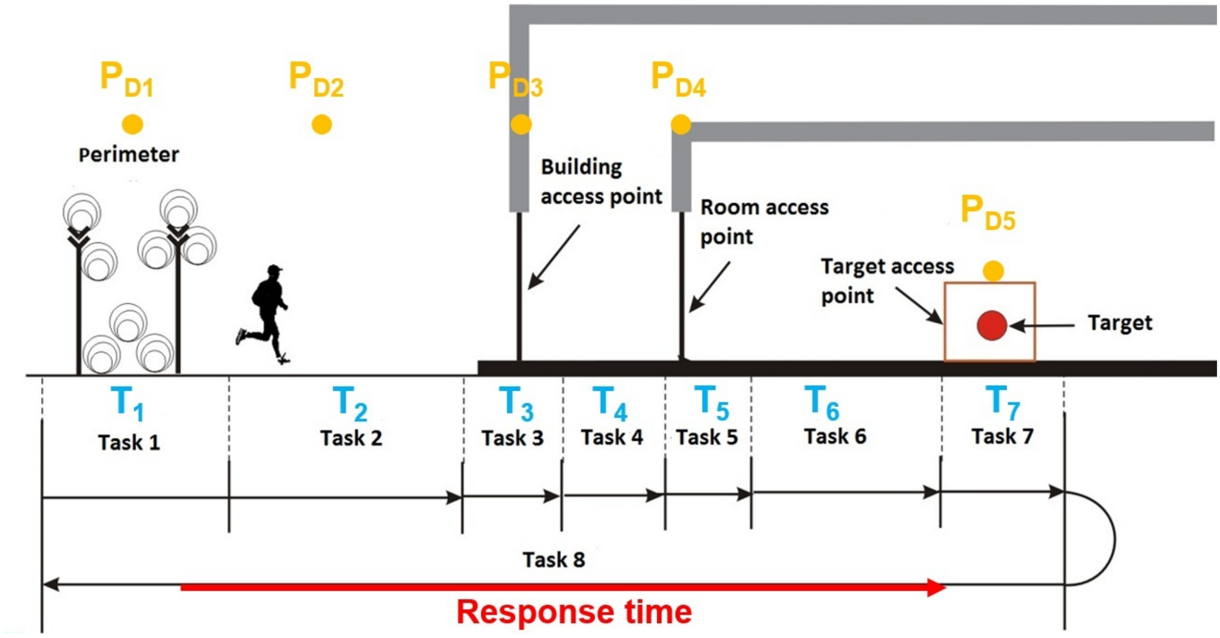

Figure 7: Potential adversary path (adapted according to [1]).

4.6 Evaluation

The basic metrics for evaluating the system are therefore the probability of detection and the delay time compared to the response force time. In the case of facilities with identified Category I material and vital areas, the intervention unit is usually deposited directly in the facility in addition to regular security. In these cases, due to the nature of the facility, care is taken to ensure that the intervention is timely and prevents the completion of theft or sabotage with unacceptable radiological consequences.

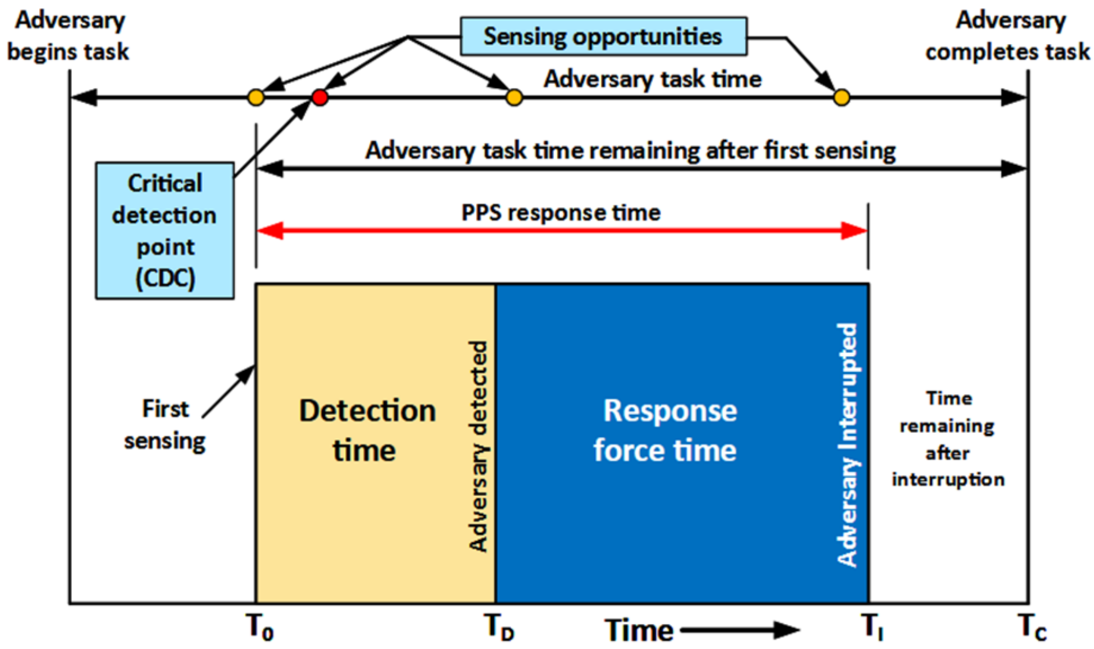

Figure 8: Comparison of adversary and response timelines [7].

After the PPS objectives have been established and a new or upgraded design has been developed, it is necessary to analyze the effectiveness of the design in meeting the objectives. This analysis can take one of two forms—quantitative or qualitative. A rigorous quantitative analysis is required for protection of assets with unacceptably high consequence of loss, even if the probability of an adversary attack is low. This is a characteristic of high-security systems found at commercial nuclear power plants, prisons, and some government or military installations [1].

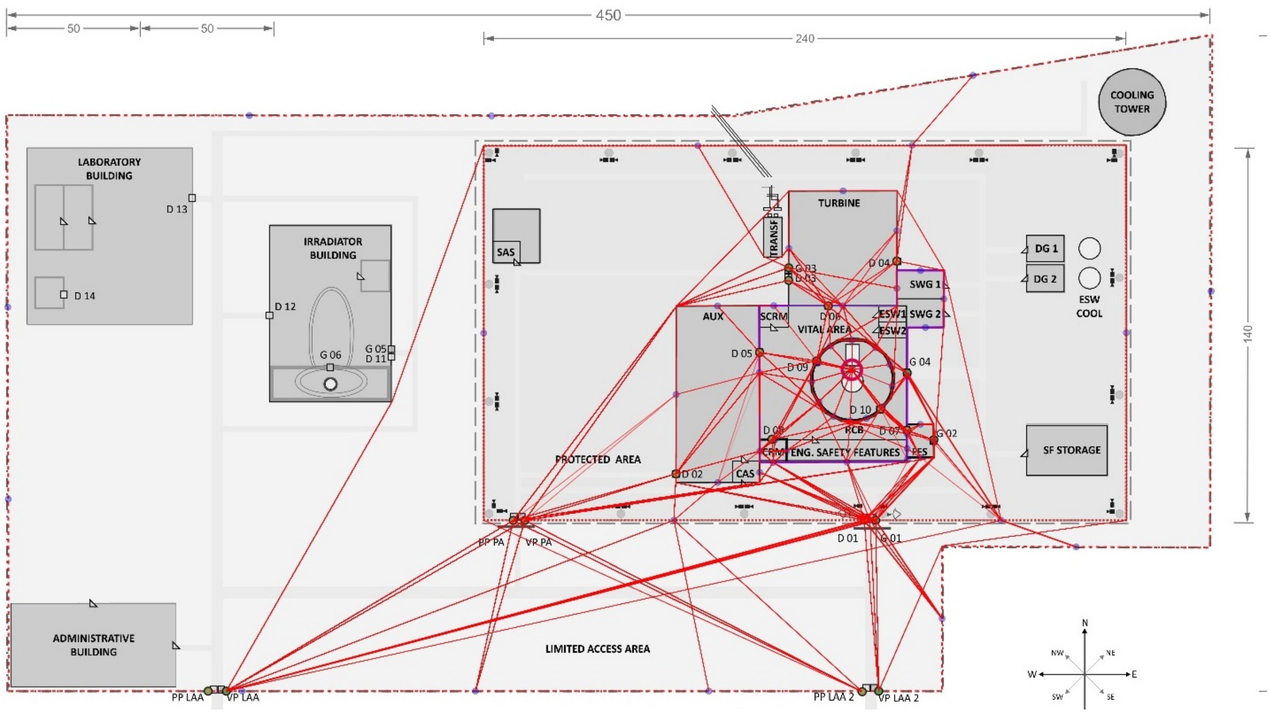

Figure 9: Examle of multi-path computer model ProEv

The evaluation of the PPS of a nuclear facility includes assessing their effectiveness against defined threats, ensuring that an integrated system of personnel, procedures and equipment can deter, detect, delay and respond to unauthorized activities and sabotage attempts. Key evaluation methods include testing performance against DBT, measuring detection probabilities, delay times and response capabilities, and ensuring timely intervention and neutralization of adversaries. The threat definition is not considered here, due to the hypothetical nature of the project, but it is one of the key starting points in the real design and evaluation of PPS. Multi-path computer models (see example on Fig. 8) are usually used to evaluate the effectiveness of PPS, based on probable scenarios of adversary progress based on the design threat. And, from testing detection probabilities and real times for overcoming delay barriers and response time.

5 CONSIDERANTIONS TO IMPROVE INHERENT PROLIFERATION RESISTANCE OF THE ALLEGRO FUEL

This section addresses measures to improve the inherent proliferation resistance of spent fuel produced by the ALLEGRO 75 MWth gas-cooled fast reactor demonstrator. The SafeG project has highlighted important neutronic and material characteristics of ALLEGRO's fuel cycle that must be taken seriously: both UOX and MOX irradiated in a gas-cooled fast reactor environment produce spent fuel streams containing substantial quantities of plutonium, and the plutonium isotopic composition tends toward quality very interesting for potential proliferators, because of the very hard fast-spectrum neutronics.

Given these realities, a combination of design choices, material management policies, and strengthened engineering controls must be adopted to reduce the attractiveness and the practical feasibility of diversion or misuse of the irradiated fuel. The following text summarizes a defensive design philosophy and concrete mitigation directions that will be incorporated in the spent fuel management approach and in the design of the fuel storage assemblies (SAs) themselves.

5.1 Design philosophy and objectives

The fundamental objective is to raise the technical, logistical, and institutional barriers to any attempt at illicit removal or separation of plutonium from ALLEGRO spent fuel to a level that makes proliferation impractical and easily detectable. Achieving that objective relies on three complementary strategies, in-line with information provided in Chapter 4:

1. **Reduce attractiveness through material form and context.** Where possible, spent fuel and associated components should be configured such that the plutonium is not readily accessible without large-scale, destructive processes and specialized facilities.
2. **Increase physical and procedural barriers.** Storage systems, handling equipment and site procedures must be designed to make unauthorized access, tampering, or covert removal extremely difficult, obvious, and traceable.
3. **Integrate safeguards, detection and forensic capabilities.** Robust monitoring, tamper-evident features, and forensic traceability must be incorporated so that any attempts at diversion are promptly detected and attributable.

These strategies are carried forward into specific choices for the spent fuel storage and the design of the storage assemblies (SAs).

5.2 Fuel sub-assembly design measures

A central feature of the ALLEGRO spent fuel strategy is to design the fuel sub-assemblies (SAs) so that they are intrinsically difficult to disassemble non-destructively and so that removing fuel pins (or other fissile-bearing subcomponents) cannot be accomplished without substantial, traceable disruption. The guiding principles for SA design are:

- **Make non-destructive disassembly infeasible.** Mechanical and material features of the SA will prevent mounting of clandestine operations that would remove only fuel pins. The SA in storage will incorporate integral structural components and closures that are either permanently sealed or require deliberate, high-effort, destructive actions to remove. Where seals or closures are not permanent for legitimate operational reasons, they will be secured by tamper-evident fastenings, encrypted locks, and continuous monitoring so that any opening triggers immediate alarms and creates an unequivocal forensic record.

- **Preserve integral mass and shielding in storage condition.** SAs will be stored complete, including the large portions of axial reflector and shielding. By retaining these components within the stored configuration, the mass, geometry and radiological signature of the stored assembly present a high barrier to covert handling. The need to remove substantial reflector or shielding to access fuel pins increases required equipment, time, and detectable activity; such requirements significantly elevate the complexity and detectability of any malicious attempt.

- **Forensic traceability of materials and components.** Where appropriate, components such as reflectors, shielding segments, and assembly structural elements will include unique markings, coded identifiers, or embedded forensic markers that enable authorities to trace any recovered parts and to link them to a given storage location and time. Such traceability discourages diversion and aids attribution if diversion is attempted.

The SA design choices are intentionally described here at a systems level; they are not instructions for circumvention or for illicit activity. The goal is to communicate the protective intent: to ensure that the path from a stored ALLEGRO spent assembly to separated plutonium requires industrial-scale processing that cannot be accomplished covertly on site or in improvised facilities.

6 CONCLUSIONS

The global nuclear non-proliferation regime is under increasing pressure as nuclear technologies evolve beyond the conventional uranium fuel cycle. Generation IV reactors using UPuC and mixed oxide MOX fuels present a dual challenge: they offer potential benefits for energy security and waste reduction, but they also increase proliferation risks due to their plutonium content. The current framework – enshrined in the Treaty on the Non-Proliferation of nuclear weapons (NPT) and protected by the IAEA – is not yet equipped to address these emerging realities. Ensuring effective oversight of UPuC and MOX facilities requires not only technological safeguards, but also legal instruments, transparent reporting mechanisms and international cooperation to maintain trust and compliance. The physical protection and security of this cycle must also be conservatively managed within existing international conventions and local legislation. This means that physical protection measures will be at the highest level necessary for the nuclear materials Category I and vital areas.

Resources

1. Garcia M. L. *The Design and Evaluation of Physical Protection Systems.* Butterworth-Heinemann 2008, ISBN 9780750683524.
2. Doyle J. (editor) *Nuclear Safeguards, Security, and Nonproliferation,* Edition 2. Butterworth-Heinemann 2019
3. IAEA Nuclear security series no.13 *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities.* IAEA Vienna 2011.
4. IAEA Nuclear security series no.16 *Identification of vital areas at nuclear facilities - Technical guidance.* IAEA Vienna 2012.
5. IAEA INFCIRC/153/Corr. *The Structure and Content of Agreements Between the Agency and States Required in Connection with the Treaty on the Non-Proliferation of Nuclear Weapons.* IAEA Vienna 1972
6. IAEA Nuclear security series No. 48-T *Identification and Categorization of Sabotage Targets, and Identification of Vital Areas at Nuclear Facilities - Technical guidance.* IAEA Vienna 2024.
7. IAEA Nuclear security series No. 40-T *Handbook on the Design of Physical Protection Systems for Nuclear Material and Nuclear Facilities.* IAEA Vienna 2021
8. IAEA Nuclear security series No. 10-G *National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements.* IAEA Vienna 2021
9. Hobbs C., Tzinieris S., Aghara S. K. (editors) *The Oxford Handbook of Nuclear Security.* Oxford University Press 2024
10. Crossland I. (editor) *Nuclear Fuel Cycle Science and Engineering.* Woodhead Publishing, 2012
11. Kenton J. Moody, Patrick M. Grant, Ian D. Hutcheon *Nuclear Forensic Analysis.* 2021 CRC Press, ISBN 9780367778040
12. SAFEG D1.3 *Assessment of Proliferation Resistance of ALLEGRO Spent Fuel Reprocessing Technology.* 2022
13. Varnado G.B., Whitehead D. W. *Vital Area Identification for U.S. Nuclear Regulatory Commission Nuclear Power Reactor Licensees and New Reactor Applicants.* Sandia National Laboratories 2008
14. Bassi C., Azria Ph., Balmain M. *Level 1 probabilistic safety assessment to support the design of the CEA2400 MWth gas-cooled fast reactor.* in Nuclear Engineering and Design 240, 2010
15. IAEA Nuclear security series no.25- G *Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities* . IAEA Vienna 2015.

16. IAEA Nuclear security series no.32-T *Establishing a System for Control of Nuclear Material for Nuclear Security Purposes at a Facility during Use, Storage and Movement.* IAEA Vienna 2019.