# Safety, Security, and Safeguards (3S) Interface

# Identification and Characterisation in

# Generation IV Advanced Modular Reactors

A Generation IV International Forum Case Study

|  |  |
| --- | --- |
| G. RENDA  European Commission Joint Research Centre  Ispra (VA), Italy  Email: [guido.renda@ec.europa.eu](mailto:guido.renda@ec.europa.eu) | G.G.M. COJAZZI  European Commission Joint ResearchCentre, retired  Ispra (VA), Italy |
| L. AMMIRABILE  European Commission Joint Research Centre  Petten, The Netherlands | D. HUMMEL  Canadian Nuclear Laboratories  Chalk River, Canada |
| L. CHENG  Brookhaven National Laboratory  USA | R. STEWART  Idaho National Laboratory  USA |
| C. CHWASZ  Idaho National Laboratory  USA | B. VAN DER ENDE  Canadian Nuclear Laboratories  Chalk River, Canada |
| B. CIPITI  Sandia National Laboratories  USA |  |

**Abstract**

The Generation IV International Forum (GIF) is a co-operative international endeavor that was set up to facilitate the research and development (R&D) needed to establish the feasibility and performance of the next generation (Gen IV) nuclear energy systems, establishing their performance goals and exploring technical feasibilities and designs, with the objective of making them available for industrial deployment by 2030s. Gen IV reactor technologies will have to excel in four main areas: safety, economics, proliferation resistance & physical protection, sustainability. With the development of Gen IV advanced modular reactor (AMR) designs, 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) are performing a bottom-up 3S (safety, security, and safeguards) exercise on a notional pebble-bed VHTR modular reactor. The objective of the exercise is to identify and characterize 2S and 3S interfaces on the reference system, and to abstract some technology neutral guidelines for 2S/3S interfaces identification and characterization. The paper will summarize the progress and experience emerging from this activity, together with some high-level findings and considerations.

## INTRODUCTION

The Generation IV International Forum (GIF) is an international initiative in which 13 Countries (Argentina, Australia, Brazil, Canada, China, France, Japan, Korea, Russia, South Africa, Switzerland, United Kingdom, United States of America) and Euratom co-ordinate research & development (R&D) activities aimed at supporting the feasibility and performance of fourth-generation nuclear energy systems. The initiative identified six reactor technologies (gas-cooled fast reactor – GFR, lead-cooled fast reactor – LFR, molten salt reactor – MSR, sodium-cooled fast reactor – SFR, supercritical water reactor – SCWR and very-high temperature reactor – VHTR) that will have to excel in four specific goals (safety, economics, proliferation resistance & physical protection, sustainability) [1]. Within the initiative, six (provisional) System Steering Committees –(p)SSC, one per reactor technology, and a number of horizontal working groups are coordinating and carrying out research activities aimed at investigating the potential and the performance of the six reactor technologies with respect to the four GIF goals. The Risk & Safety Working Group (RSWG) and the Proliferation Resistance & Physical Protection Working Group (PRPPWG) have a long-standing relationship in which activities of common interest are investigated, mainly at the interface of nuclear safety and security. Recently, a collaboration between the two working groups and the VHTR SSC started to investigate a method to identify the interfaces between safety, security and safeguards in a VHTR notional design, a bottom-up exercise aimed at providing designers and vendors potential guidance on how to approach this task.

## Safety, security and safeguards by design

Every nuclear energy system in non-nuclear weapon states (NNWS) will have to comply with the provisions of three different regimes: Nuclear Safety, Nuclear Security, and International Nuclear Safeguards. There are several different potential definitions for Nuclear Safety, Security, and Safeguards; Table 1 reports the definitions for safety, security and safeguards that will be here adopted.

*Table 1. Scope of nuclear safety, security and safeguards.*

|  |  |
| --- | --- |
| Discipline | Scope |
| 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 [2].  *Threat*: Accident due to system failure, human error, or natural disaster [3]. |
| 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 [2].  *Threat*: A person or group of persons with motivation, intention and capability to commit a malicious act [2] [3]. |
| 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 [4].  *Threat*: State actors with intent of acquiring or using nuclear material for proscribed purposes. |

While the three regimes have different origins, objectives and provisions, and are usually implemented independently from each other, they are all part of the same technical system and consequently they are inevitably interacting with each other. The current nuclear energy systems were not designed keeping in mind these interactions; for small and advanced modular reactors that are being designed and developed, there is the potential to explore increased efficiencies by addressing the interfaces between safety, security, and safeguards by designing the system to maximize synergies and minimising conflicts arising from the interaction of the three regimes’ activities.

## The GIF 3S Sub-group case study

In the line of their long-standing collaboration, the RSWG and the PRPPWG set up a bottom-up case study to start investigating the interfaces between safety, security and safeguards in Gen IV reactor technologies, with the final aim of providing some guidance to designers and vendors wishing to apply a 3S-by-design (3SbD) approach to the development of a Gen IV advanced modular reactor (AMR). The VHTR SSC made available a notional design of a very-high temperature pebble-bed small modular reactor, enabling the formation of a PRPPWG/RSWG/VHTR SSC sub-group to perform this activity. Some characteristics of the system selected for the analysis are of particular interest for an exercise like this one:

* The design is an online-fuelled, pebble-bed reactor, with a very large amount of small items 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, there are no pebble-bed reactors in commercial operation 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 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) fuel have the potential to be designed to be walk-away safe. While walk-away safety does not imply walk-away security, the safety-security interfaces will be influenced and potentially reduced.

The current sub-group involves 20 researchers among the three WG members and observers, representing 11 organisations and six member states that will collaborate on a two-year project. The following paragraphs will briefly describe the system and the current status of the activity.

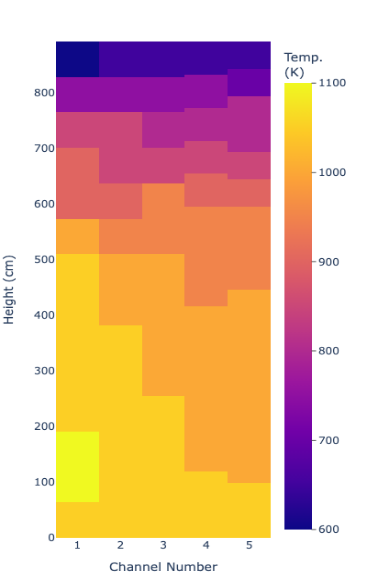
### System Description

The selected system (referred to as GPBR-200), provided by Idaho National Laboratory, consists of a pebble bed reactor (PBR) with a target power of 200 MWth [5]. The reactor's design includes a continuous fuelling regime, where fuel pebbles enter the core from the top and move through it to be finally discharged at the bottom for either disposal or recirculation. The primary coolant is helium, which is heated by flowing around the fuel spheres in the core and then transfers the heat to water in a steam generator to produce steam for electricity generation, co-generation, or industrial heat production. The GPBR-200 notional core is derived from previous designs and has a thermal power of 200 MWth, a primary system at a pressure of 6.0 MPa, and a flow rate of helium of 79 kg/s. The fuel pebbles have a diameter of 6.0 cm, a 1.0 cm thick graphite shell, and contain a graphite matrix mixed with TRISO particles. The fissionable nuclear material contained in the fuel pebbles is foreseen to have two different enrichment levels in 235U, of 5.0-wt% and 15.5-wt%. The core of the GPBR-200 has a radius of 1.2 m and an active height of roughly 8.93 m. Fresh fuel is stored on site in fresh fuel canisters. 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 pebble-bed reactor. The core has a relatively epithermal neutron energy spectrum when contrasted with typical light water reactors. The expected thermal temperature profile at equilibrium, together with an axial slice of the core region, is shown in Fig. 1.

The fuel handling system (FHS) is responsible for loading and unloading fuel pebbles, measuring burnup, removing defective pebbles, and extracting pebbles for post-irradiation examination. During normal operations, fresh fuel pebbles are loaded into the core, where they undergo a burnup process and are eventually discharged and replaced with new pebbles. The FHS also plays a crucial role in run-in and core defueling/refuelling processes.

The GPBR-200 safety design philosophy emphasizes inherent safety characteristics and passive systems to perform safety functions. The reactor's low power density, large heat capacity, and negative temperature coefficient of reactivity are some of the inherent safety features. In addition, the reactor has several passive and active safety systems, including the reactivity control system, reserve shutdown system, and safety shutdown system. These systems work together to ensure the reactor's safe operation and protect against severe core damage.

*Fig. 1. Axial slice of the GPBR-200 core region and temperature profile at equilibrium.*



The reactor is partially below grade, and the fresh, spent, and broken fuel pebbles are stored in below-grade facilities. The burnup measurement system, steam generator, and control room are attached to the reactor. The post-irradiation facility, fresh fuel storage, spent fuel storage, and broken fuel storage are also described. These areas are connected to the main fuel handling system for efficient pebble transport. The control room contains all necessary controls for safe reactor operation, and the shipping/receiving area is used for pebble shipments. The layout is designed to prioritize safety, security, and safeguards.

### Safety, Security and Safeguards Descriptions

After preparing the system’s description, the second phase of the activity has been to prepare notional safety, security and safeguards descriptions for the GPBR-200. A full-scope assessment was beyond the objective of the study, and the 3S descriptions address the identification of the key aspects needed to identify the interfaces between safety, security and safeguards. The 3S descriptions were performed starting from an open literature survey of pebble-bed VHTR reactors safety, security and safeguards that formed the basis for a tailoring to the GPBR-200 design features. Past WG assessments of the Gen IV VHTR system were also leveraged.

The GIF VHTR SSC and RSWG have previously examined the safety of the general VHTR system as documented, for example, in the VHTR risk and safety assessment white paper [6], VHTR safety assessment [7], and VHTR safety design criteria [8]. From a safety point of view, the main sources of radioactive material identified specifically for the GPBR-200 design are reported in Table 2, and the related barriers are summarized in Table 3, together with the main barriers to radionuclides transport per identified source.

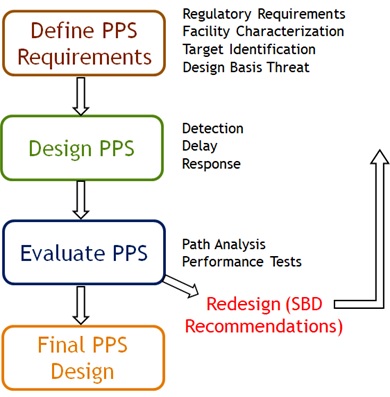
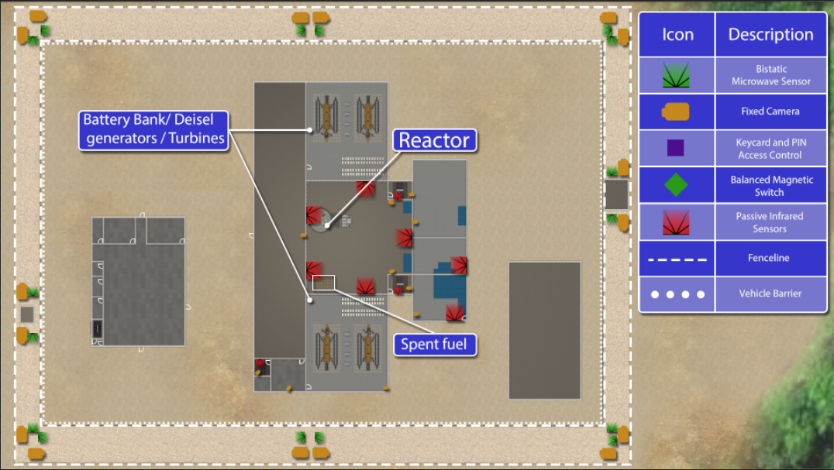
*Table 2. GPBR-200 sources of radioactive material.*

|  |  |  |
| --- | --- | --- |
| Sources within the main power system high 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 * Embedded/attached to graphite components |
| Plateout on HPB surfaces and dust |  |
| Circulating coolant activity |  |
| Sources outside the MPS HPB | Fuel spheres in storage systems |  |
| Solid and liquid radwaste systems |  |

*Table 3. GPBR-200 Sources and Barriers.*

|  |  |
| --- | --- |
| **Radioactive Material Source** | **Barriers to Radionuclide Transport** |
| Fuel spheres in the core | Coated particles, graphite matrix, helium pressure boundary, reactor building |
| Fuel spheres outside the core | Coated particles, graphite matrix, FHSS piping, spent fuel tanks (SFTs), used fuel tanks (UFTs), or new fuel tanks, reactor building |
| Non-core sources within the MPS | HPB, reactor building |
| Other sources | Various tanks, piping systems and containers, reactor building or ancillary buildings housing waste management equipment |

The security approach adopted for describing the security features of the GPBR-200 followed the Design Evaluation Process Outline (DEPO) [9], which involves defining physical protection systems (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. A revision to the original DEPO process includes security by design (SeBD) recommendations, which optimize facility costs by considering aspects early in the design process. Fig. 2 illustrates the DEPO process and a potential site layout identifying potential baseline Physical Protection features.



*Fig. 2. Scheme for the DEPO process* [9] *and a notional SMR baseline PPS layout* [10]*.*

During the DEPO process, the results from the evaluation are used to redesign the overall facility and site layout as needed, incorporating security by design recommendations. The "Define PPS Requirements" step of the DEPO process overlaps with the other S regimes, while the "Design" phase diverges due to the specificity of detection, delay, and response technologies and tactics. The "Evaluation" phase of DEPO is distinct from the other Ss due to the unique tools used for PPS analysis.

From a safeguards point of view, the description 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) [4]. There is little information about safeguarding PBRs [11]; for this description, suggestions for the HTR-10 and HTR-PM [12] in open literature has been used as a starting basis. Table 4 illustrates the main system elements and some of the key measurement points identified for this exercise.

*Table 4: Identified Sub-MBAs, System Elements and Key Measurement Points for the GPBR-200. KMPs with asterisks indicatING where item material counting is performed.*

|  |  |  |  |
| --- | --- | --- | --- |
| **SUB-MBA** | **System Element** | **Inventory Key Measurement Point** | **Flow Key Measurement Point** |
| MBA-1 | Receiving area |  | FKMP-1\*: Fresh Fuel receipt |
| Fresh Fuel Storage | IKMP-A\*: Fresh Fuel | FKMP-2: Recategorization of FF through transfer to pebble feed system |
| MBA-2 | Reactor System | IKMP-B: Irradiating items |  |
| Burnup Measurement System |  | FKMP 8: Irradiated fuel removed from burnup measurement system to spent fuel |
| MBA-3 | Spent Fuel Storage | IKMP-D\*: Spent Fuel | FKMP 9: Recategorization of spent fuel transferred to spent fuel storage |
| Broken Fuel Storage | IKMP-C\*: Broken Fuel | FKMP-5: Recategorization of broken fuel and waste transferred to broken fuel storage |
| Post-Irradiation Facility | IKMP-E\*: Post-irradiation facility items |  |
| Shipping Area |  | FKMP-12\*: Shipment of spent fuel, broken fuel, and waste (items) |

### Identifying and characterizing interfaces between the three regimes

Nuclear reactor designers have a strong safety culture, developed over several decades of experience, lessons learned, and regulatory requirements. Every nuclear reactor design is conceived having the safety requirements in mind and every design option routinely undergoes safety scrutiny, often in a structured, sometimes regulated way. A security culture is much less developed among designers, and a safeguards one is almost entirely absent. While a 3S by design (3SbD) approach would ideally benefit from a systems engineering, holistic approach, this would need a paradigm shift in terms of design culture and practice that will inevitably need many years and would risk missing the current window of opportunity related not only to the first Gen IV systems, but also to small modular reactors and advanced modular reactors. From a more pragmatic point of view, an intermediate step towards a fully integrated 3SbD culture is to leverage on the existing safety by design culture and complement it with a PR&PP culture that could be introduced via bilateral interfaces with the better-known safety domain. In practical terms, this would mean starting to introduce the security and safeguards needs in terms of relationship with the safety ones, through a 3x2S exercise. At the end of the identification of the 3x2S interfaces, an additional analysis would allow the identification of the ones that are proper 3S interfaces. For this exercise, the sub-group therefore opted to adopt this approach for the third phase of the activity – 3S interfaces identification – which is currently ongoing.

### Security – safety and security – safeguards preliminary interfaces

The choice of where to start with an identification process depends on the composition of the team performing the investigation. While safety is the best-known regime by designers, the easiest entry point to a 3x2S interfaces identification is probably security. Security has the advantage of having easy to identify links with both safety (concerning sabotage) and safeguards (concerning nuclear material theft) and the 3S sub-group composition makes it easier to work keeping security as a pivotal point. The first two interfaces that have been preliminary investigated are the safety-security and security-safeguards ones.

The safety-security interface is crucial in reactor design to ensure that security is not merely treated as an afterthought. By considering security alongside safety during the design process, building designs, delay features, and response force strategies can be created that are more efficient and elegant. This becomes particularly relevant in the context of nuclear reactors, where the primary concern is the risk related to sabotage, rather than theft.

Safety systems and physical security are closely intertwined. Any safety-significant system or control system must be protected as a vital area in the overall design of the physical protection system. For a PBR, this means ensuring that all such systems are included within the reactor building, thereby denying access to potential adversaries. Furthermore, safety and control systems should not be installed on the outside wall of a building structure, and the adversary path within the building should be carefully considered to avoid creating vulnerable targets.

Advanced reactors typically have longer timelines before core damage or other problems that occur in the event of loss of cooling systems. Passive safety is often incorporated into these designs, but it is essential to recognize that passive safety does not equate to passive security. The performance of safety systems should be considered in light of an adversary attack, and necessary design choices be made to increase the robustness of the plant safety response, for example, increase the diversity of safety systems that respond to adversary-initiated events, separate important safety systems to reduce interfacing adversary targets, or increase timelines to undesirable consequences. The longer timelines may have an advantage in how the response force strategy is applied, potentially allowing for the use of off-site response and mitigating safety actions for select scenarios.

Cybersecurity is another critical aspect of reactor design, as safety-significant systems must be robust to digital attacks. A defensive computer security architecture (DCSA) should be designed for any advanced reactor, defining the plant control systems and their respective cybersecurity levels [13]. The most critical plant systems require the most stringent cybersecurity protection measures and may even be isolated through an air gap from the rest of the systems.

The effect of radiation dose on responders must also be considered when designing the physical protection system. This may affect responder placement within the reactor building, as stations within a radiological area will have limitations on food and drink, making for a less desirable work environment.

Safety and security requirements must be considered in the design and layout of emergency exits. Shark cages or mantraps can be designed to slow down attackers while still allowing egress in the event of an emergency. Previous designs have also utilized "safe havens" that provide a delay for exiting a facility during an attack.

The safeguards-security interface is equally important and should be considered early in the design process. By designing optimal measurement and accounting systems that augment overall plant security, the need for international safeguards can be minimized. Theft is not a significant concern for PBRs due to the large number of pebbles required to accumulate a significant quantity (defined by the IAEA as “the approximate amount of nuclear material for which the possibility of manufacturing a nuclear explosive device cannot be excluded” [4]) of nuclear material and the dilute, material form of the fuel.

In the context of a PBR, the pebble handling system plays a crucial role in counting total numbers of pebbles but does not track or identify specific pebbles. All pebbles leaving the reactor undergo a burnup measurement to determine if they can be re-inserted into the core or if they need to be sent to spent fuel canisters upon reaching a burnup limit. This helps to inform the total actinide content in spent fuel canisters.

## preliminary conclusions and way forward

The GIF 3S sub-group set up a bottom-up case study to start investigating the interfaces between safety, security and safeguards in Gen IV reactor technologies, with the final aim of providing some guidance to designers and vendors wishing to apply a 3SbD approach to the development of a Gen IV AMR. The study is being performed on a notional pebble-bed VHTR , and is now in the phase of identifying the design’s 3x2S interfaces. The process highlighted that the concept of 3SbD and PR&PP by design are not new, but among designers there is the need to foster a security and safeguards by design to integrate the already existing safety by design culture. Through an intermediate 3x2S analysis of the existing interfaces, the ultimate goal of a 3SbD culture among designers could be achieved in a smother and quicker way, potentially allowing the industry to profit from the window of opportunity represented by AMRs. Indeed, AMRs provide opportunities to take a more integrated approach to the design of 3S systems: while a tighter 3S integration would be beneficial for all new reactor systems, it will be particularly relevant for small and advanced modular reactors (SMR/AMRs). Once the 3x2S exercise will be over, the identified interfaces will be characterized and further analysed to single out which of them are actual proper 3S interfaces.

references

|  |  |
| --- | --- |
| [1] | GENERATION IV INTERNATIONAL FORUM, [Online]. Available: https://www.gen-4.org/gif/. |
| [2] | INTERNATIONAL ATOMIC ENERGY AGENCY, “IAEA Nuclear Safety and Security Glossary: Terminology used in Nuclear Safety, Nuclear Security, Radiation Protection and Emergency Preparedness and Response, interim edition,” IAEA, Vienna, 2022. |
| [3] | K. Sanders, R. Pope, Y. Liu and J. Shuler, “Interfaces among Safety, Security, and Safeguards (3S) - Conflicts and Synergies,” in *Proceedings of INMM 56th Annual Meeting*, Indian Wells, CA, USA, 2015. |
| [4] | INTERNATIONAL ATOMIC ENERGY AGENCY, “IAEA Safeguards Glossary,” IAEA, Vienna, 2022. |
| [5] | 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. |
| [6] | J. Tong, F. Li, M. Futterer, H. Gougar, C. Sink and D. Petti, “Very High Temperature Reactor (VHTR) Risk and Safety Assessment White Paper,” GIF, Paris, 2015. |
| [7] | F. Chen and H. Gougar, “Very High Temperature Reactor (VHTR) Safety Assessment,” GIF, Paris, 2018. |
| [8] | GENERATION IV INTERNATIONAL FORUM, “Safety Design Criteria for Generation IV Very High Temperature Reactor System,” GIF, Paris, 2023. |
| [9] | M. Garcia, “Design and Evaluation of Physical Protection Systems, 2nd edition,” SNL, 2008. |
| [10] | A. Evans, J. Parks, S. Horowitz, L. Gilbert and R. Whalen, “U.S. Domestic Small Modular Reactor Security by Design,” Sandia National Laboratories, 2021. |
| [11] | GENERATION IV INTERNATIONAL FORUM, “GIF Very High Temperature Reactor Proliferation Resistance and Physical Protection White Paper,” GIF, Paris, 2022. |
| [12] | P. Becker, A. Rialhe, J. Whitlock and J. Doo, “Implementation of Safeguards Measures at the High Temperature Gas-Cooled Reactor Pebble-Bed Module (HTR-PM) in Chinq and proposed Safeguards by Design for Units to be exported to other States,” in *IAEA Symposium on International Safeguards*, Vienna, 2018. |
| [13] | G. Herdes, G. White and J. Sladek, “Defensive Computer Security Architectures for Facilities with Radioactive Materials,” in *Proceedings of the INMM/ESARDA Joint Annual Meeting*, Vienna, 2021. |
| [14] | INTERNATIONAL ATOMIC ENERGY AGENCY, “Fundamental Safety Principles,” IAEA, Vienna, 2006. |