Nigerian Journal of Physics (NJP)
ISSN online: 3027-0936
ISSN print: 1595-0611
DOI: https://doi.org/10.62292/njp.v34i3.2025.405
Volume 34(3), September 2025

Small Modular Reactors: Physical Protection Considerations

***[1]Ojinnaka, C. A. S., [2]Emejiaka, E. E., [1]Osaisai, F. E. and [1]Kuye, A.**

[1]Centre for Nuclear Energy Studies, University of Port Harcourt, Port Harcourt, Nigeria.
[2]Nigeria Nuclear Regulatory Authority, Abuja, Nigeria.

[*]Corresponding author: cojinnaka@yahoo.com

ABSTRACT

It is no longer news that Nuclear Energy provides one of the best alternatives for clean energy. In this regard, and to ensure that energy generation from this source is safer and cleaner, advancements have been ongoing and one of such is the concept of Small Modular Reactors (SMRs). SMRs offer more economic, and passive safety features, flexibility, and far less radiological consequences from accidents. Although only the Akademik Lomonosov is currently in use, research and development for other more efficient SMRs are ongoing. This work aims to provide a technical overview of SMRs, evaluate some emerging threats associated with SMRs, and analyze how a robust and effective physical protection system (PPS) could mitigate against these threats using two case studies. The two case studies considered were Akademik Lomonosov and Spar-Type Platform Design for the Offshore Floating Nuclear Power Plant (OFNP). It was observed that one of the impacts of SMR on PPS would be a significantly lower cost for PPS than in the traditional large nuclear power plant, owing largely to the difference in size. Also, in SMRs, security would be more centralized and enhanced. Situating SMRs offshore provides a better physical protection system in terms of natural phenomena or extreme weather events. Areas for improving the PPS of SMRs for the two case studies were identified and the best possible solutions were proffered.

Keywords:
SMR,
Physical protection,
Intrusion detection,
Transport security,
Resilience.

INTRODUCTION

The overall objective of the State's Nuclear Security Regime comprises international legal instruments, conventions and codes of conduct and are supplemented by IAEA security services. The most important documents in the protection of nuclear material and nuclear facilities are the 2005 Amendment to the Convention on the Physical Protection of Nuclear Material (CPPNM) and the Code of Conduct for the Safety and Security of Radioactive Sources (IAEA, 2004, 2011; Rossi, 2015). The 2005 Amendment to the CPPNM entered into force on 8 May 2016, makes it legally binding for States Parties to protect nuclear facilities and material in peaceful domestic use, storage and transport. It also provides for expanded cooperation between and among States regarding rapid measures to locate and recover stolen or smuggled nuclear material, mitigate any radiological consequences of sabotage, and prevent and combat any related offences (IAEA, 2023; Müller, 2016).

The State's Physical Protection Regime elements include appropriate legislation and regulation; responsibility, authority, and sanctions; licensing and other procedures to grant authorization; analysis of threats; physical protection requirements for nuclear material in use and storage and during transport and for nuclear facilities; nuclear facility siting, layout, and design; trustworthiness program; reporting of information; confidentiality; and evaluation of the implementation of physical protection measures (Rossi, 2015). However, this work focuses primarily on physical protection system.

A good physical protection system (PPS) is designed to integrate people, equipment and procedures for the overall protection of facilities and assets against adversaries that have the intention of either theft, attacks, or sabotage (Tekinerdogan et al., 2020). Cheng & Bari, 2021) in their book defined physical protection as the characteristic of an SMR that impedes the theft of materials suitable for nuclear explosives or radiation dispersal devices (RDDs) and the sabotage of facilities and transportation by subnational entities and other nonhost state adversaries. PPS design applies a systematic and logical approach where the objectives of the PPS are weighed against resources that are available

and what is being protected. If a proper PPS design and analysis is not done, then valuable resources are bound to be wasted on the protection that is not necessary, or the PPS may fail to provide the required protection of facilities and assets. Theft, attack, or sabotage of a facility may be reduced or prevented either by deterring or defeating the adversary. To deter or defeat the adversary, the three PPS elements must be applied. These elements are detection, delay and response. Detection is simply the sensing and discovery of the adversary, who could either be covert or overt. The main function of the delay element is to slow down the progress of an adversary in other for the response team to mitigate the adversary's action. This can be accomplished using either passive or active delay and, in most cases, both. The third element of PPS is the response which is made up of activities taken to mitigate the adversary's success. PPS, as mentioned earlier, is used for the protection of critical facilities and assets. Such facilities can be an airport, nuclear power plant or even a small modular reactor (SMR). This paper will look at how PPS impacts small modular reactors.

Small Modular Reactors (SMRs), a global emerging technology, have peculiar security vulnerabilities due to their design and structure. It could be vulnerable to attack by adversaries or natural phenomena like extreme weather events (EWE) or issues arising from sitting in a remote location. Being in a remote location with limited access could reduce the likelihood of a physical attack, particularly by external adversaries, but on the other hand, it could give external response forces limited time, which could be a negative impact on the physical protection system. Also, most SMRs may be sited around urban areas, and this could expose them to more threats, thus the need for an adequate response force. With SMR, the threat is not only with nuclear or radiological materials but with the whole plant due to its size.

This study is aimed at highlighting the fundamentals of SMRs and assessing applicable physical protection systems.

Technical Overview of Small Modular Reactors

Small modular reactors (SMRs) are nuclear reactors that have power capacities of up to 300 MWe per unit, designed with modular technology using module factory-assembled systems and components and transported as a unit to a location for installation (Duguay, 2020; Liou, 2021). SMRs are expanding the nuclear energy portfolio options needed to meet our national goals on energy security and mitigation of climate change (Nuclear Energy Institute). They offer an enhanced safety performance through inherent and passive safety features, better upfront capital cost affordability and are suitable for cogeneration and non-electric applications. In addition, they offer options for remote regions with less developed infrastructures and the possibility for synergetic hybrid energy systems that combine nuclear and alternate energy sources, including renewables (Duguay, 2020).

According to Liou (2021), about 70 SMRs are being designed globally. Most of these designs are at an advanced developmental stage, and there are claims that most may be deployed in the near future. There is currently only one operational marine-based SMR, Akademik Lomonosov, and at least four other SMRs in their advanced stages of construction in Russia, Argentina, South Korea, and China, and several other nuclear energy countries are conducting SMR research and development.

There are multiple proposed designs for small modular reactors in which some are only a streamlined version of the conventional reactors, while others are entirely new technologies that are aimed at meeting the goals of Generation IV reactors (Oka & Mori, 2014). The new advanced reactors can be categorized into three types: Molten Salt, Triso-Based, and Fast Neutron Spectrum (Michelle, 2019). In molten salt-fueled reactors, the fuel consists of fissile materials (uranium fuel enrichment up to (but less than) 20% or thorium-based fuel) dissolved in a salt, a mixture that becomes liquid during operation. In a reactor with thorium-based fuel, ^{232}Th in the initial fuel inventory is converted during operation to the fissile isotope ^{233}U, which is then consumed as fuel.

Tristructural-isotropic (TRISO)-fueled reactors operate at a high temperature, using small, uniform microspheres of uranium oxycarbide coated with several layers of pyrocarbon and silicon carbide which are dispersed into graphite pebbles (e.g., billiard-ball sized) or prismatic, hexagonal graphite fuel blocks. The reactor uses graphite as a moderator. Some designs are helium-cooled, and some are molten fluoride salt cooled. High-temperature reactor SMRs using TRISO fuels can retain fission products to provide high proliferation resistance, but these fuels are impractical to reprocess (Black et al., 2020). On the other hand, Fast reactors use a fast neutron spectrum that can enable high fuel utilization, operational flexibility, and fuel recycling. Fast reactors can use liquid metal, gas coolants, or salt coolants.

Most envisioned SMRs use nuclear fission with designs of either thermal-neutron reactors, which require a moderator (light water or heavy water) to slow neutrons or fast neutron reactors, which rely on reactor fuel to absorb fast neutrons (Hidayatullah et al., 2015). Table 1 shows examples of SMR types that are being developed with their brief characteristics.

Table 1: Small Modular Reactor Types

	Small Modular Reactor Type	Description
1	Light Water Reactor (LWR)	Coolant: Light water Moderator: Light water Fuel: Uranium 235 Type: Pressurized water reactor (PWR) Boiling-water reactor (BWR) Supercritical water reactor (SCWR) Neutron Spectrum: Thermal-neutron
2	Heavy Water Reactor (HWR)	Coolant: Heavy water Moderator: Heavy water Fuel: Natural uranium Type: Pressurized heavy-water reactor (PHWR) Neutron Spectrum: Thermal-neutron
3	Gas-Cooled Fast Reactor (GFR)	Coolant: Helium gas Fuel: Uranium, thorium Neutron Spectrum: Fast-neutron Notes: The elevated outlet temperature of the helium coolant allows it to generate electricity, provide heat, and support hydrogen production (Gill et al., 2014). Currently, three GFRs are under design.
4	Sodium-Cooled Fast Reactor (SFR)	Coolant: Liquid sodium Fuel: Uranium dioxide Neutron Spectrum: Fast-neutron Notes: SFR closed fuel cycle enables the regeneration of fissile fuel and facilitates actinide management. Currently, nine SFRs are under design, and one is under construction (Hayafune et al., 2017).
5	Lead-Cooled Fast Reactor (LFR)	Coolant: Molten lead or lead-bismuth eutectic (LBE) Fuel: Nitride fuel Type: Pressurized heavy-water reactor (PHWR) Neutron Spectrum: Fast-neutron (Yun et al., 2021; Zohuri, 2020).
6	Molten Salt Reactor (MSR)	MSR is one of the Generation IV reactor systems. MSRs under development include nuclear fuel dissolved in molten fluoride salt as well as solid fuel with molten salt coolant. A lot of research and development efforts are being put into the MSRs to improve on thermal and fast-spectrum MSR concepts and combine the generic assets of fast neutron reactors with those relating to molten salt fluorides as fluid fuel and coolant. About nine MSRs are under design (Serp et al., 2014).

Emerging Nuclear Threats with Emphasis on SMRs

Worldwide, adversary groups are using innovative techniques and state-of-the-art technology to carry out terrorist activities, hence the need for robust and effective countermeasures. Although there has not been a record of an attack on an SMR facility, the emerging threat for a conventional NPP is almost similar to that of an SMR, especially for land-based SMRs. However, one of the greatest advantages of the SMRs over the NPPs is the decentralization of the energy supply.

Some of the characteristics of advanced reactors that can support improved nuclear security and prevent unauthorized radioactive release include below-ground placement, passive safety features, low operating pressures, and decreased external power dependence. However, there are security issues with the remote location of these reactors which includes how the siting may impact physical security and timely response in the case of a security event (Michelle, 2019). Nilsson et al. (2018) indicate that four key nuclear security challenges of SMRs are: (a) Physical Protection, (b) Facility Sabotage and Nuclear Terrorism, (c) Cyber and Emerging Technologies, and (d) Reactor Siting. These threats and others are discussed below.

Remote Locations with Limited Access

Remote location challenges require more analysis. The safety of nuclear materials can be guaranteed because the SMRs can be shop fabricated, fuelled, sealed and transported to the location of use for power generation.

The SMR will remain sealed until it is returned to the factory safely. This will reduce or stop the possibility of material misuse or diversion. The SMRs can be used in locations that are off-grid and at mining sites (Bentoumi et al., 2020). The SMR being in a remote location with limited access can reduce the probability of an external adversary attack. Staffing for SMRs is likely to be very small due to economic reasons. This can lead to less manpower at the site to fully protect and guard against sabotage attacks. Several SMR designs also propose installing the SMR core module underground. This presents further difficulty, cost, and technical challenges to access. Precisely, robust physical protection and internal guards should be prepared in case of a hostage attempt, as security forces from outside will have difficulties accessing the facility. This can be mitigated by having the control room above ground. Considering the fact that the SMRs will be situated in remote regions and over a vast geographical area, the development of remote monitoring capability is mandatory (Upadhyaya et al., 2015). Building on Upadhyaya et al.'s (2015) work, Kosai & Unesaki (2024) introduced a resilience-based vulnerability index that combines hazard exposure and critical-infrastructure dependencies, offering a quantitative tool to optimize SMR siting.

Reactor Siting

SMRs lend themselves to distributed operation, as it is feasible to deploy many SMR sites over a potentially large geographic region. This has strengths and weaknesses. While the number of potential targets for security breaches grows as the number of SMR sites increases, it becomes more justifiable to employ a sizable security task force that is available to a significant network of SMR sites through dispatch centres reasonably located to ensure timely response in case of an attack (Poudel et al., 2018).

Cyber Security

Cyber-attacks are targeted to gain information, compromise the integrity of data or affect the availability of computer systems used for the security of nuclear facilities. In today's digital world, cyber security incidents are a reality, whether targeted or not. The cost of not preparing for such incidents is significantly higher than the investment into the development and maintenance of a solid cyber security program from the onset. Digital systems with increased automation that goes with both remote supervisory control and remote maintenance can be very useful in the reduction of costs of SMRs, provided appropriate cyber security risk management is established and maintained throughout the entire SMR lifecycle from design through operation and decommissioning. Establishing a solid cyber security program upfront is imperative to ensure that no unauthorized changes find their way into the baseline and that the baseline does not contain any known vulnerabilities. A solid cyber security program will significantly contribute to managing risk and directing limited resources towards systems or assets based on their relative value or importance throughout their lifecycle. This is key when designing a licensable Instrumentation & Control (I&C) architecture with its corresponding concept of operations as it establishes a foundation for regulatory review through a defined cyber security classification scheme where security risks are categorized from low to high such that appropriate zoning and controls are incorporated into the design (Bentoumi et al., 2020). Possibly in the near future, quantum-secure key distribution will used over a 1 km reactor-control link, pointing toward eavesdropping-proof channels for next-generation SMR networks as demonstrated by Gkouliaras et al. (2025) .

Waste Risk

Consumed fuel rods from nuclear plants are radioactive waste. Most fuel rods are stored at the same site as the nuclear reactor that spent them. This has resulted in the numerous radioactive waste sites in different countries that must be maintained and funded for so many years, which is far longer than the lifetime of any nuclear power plant. The more these nuclear plants generate waste, the more the risk of radioactive leaks, which can affect the quality of water supply, crops, animals, and even humans. However, the emergence of SMR technology does not need on-site refuelling instead, the entire core is removed at the end of fuel life. This could significantly reduce and alleviate the fear and challenges of nuclear waste disposal, thereby addressing the issue of proliferation.

Insider Threat

An insider is someone who has authorized access to nuclear facilities or transport that is capable of unauthorized removal or sabotage or someone who could aid outsiders in causing damage or sabotage (IAEA, 2020a). These threats could stem from one or more persons with legitimate access to a facility and detailed knowledge of activities or source locations in that facility (IAEA, 2019). These individuals may be employees, contractors, or visitors who have authorized access and who could remove radioactive sources or vital information with malicious intent or conduct acts of sabotage on the premises. An insider could be categorized into a passive insider, one who doesn't participate directly either by giving information to an outsider under duress or an act of negligence of security protocols, or an active insider, one who participates directly in a malicious act and could either be violent or non-violent. These attributes of an insider can present a risk to the physical protection system of a nuclear facility due to their access, authority, and/or knowledge of the

system. The risk is difficult to quantify because of the type and number of parameters that determine the risk. However, the growing interest in licensing, constructing, and operating new advanced and small modular reactor (SMR) designs has created new opportunities for security cost savings and effectiveness by incorporating insider security measures into new reactor site designs using security-by-design principles. Faucett & Vierow Kirkland (2023) presented a review of existing security risk evaluation approaches for insider threats.

Figure 1: Akademik Lomonosov SMR (Spiler et al., 2015)

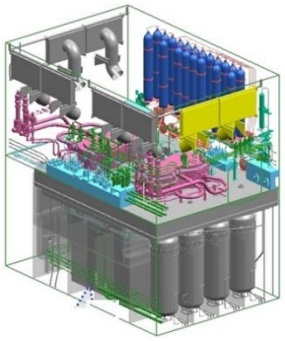

Figure 2: KLT-40S Reactor (Spiler et al., 2015)

On board the Akademik Lomonosov are two KLT-40S reactor (shown in Figure 2) systems, each having a capacity of 35MW. The vessel has an overall life cycle of 40 years, which can be extended up to 50 years, according to Rosatom, who designed it to work as part of the Floating Nuclear Thermal Power Plant (FNPP). Rosatom stated that the Akademik Lomonosov is part of a bigger plan to make energy accessible to remote regions in Russia and around the world. The vessel is made up of three decks, and each deck is divided into ten compartments, measuring 144 meters long by 30 meters wide by 10 meters in height. The vessel displaces about 21,500 tons of water. Akademik Lomonosov has living quarters that can house about 70 crew, and these crews are responsible for various operations on the vessel. The emergency cool-down system (ECS) for the KLT-40S reactor was developed to remove residual heat released when the power station is in a blackout (Lee et al., 2015). The Lomonosov is designed to operate in three 12-year operational cycles. At the end of each period, the vessel will be towed back to the Rosatom float shipyard in Murmansk for repairs, refuelling, refuelling, and radioactive waste removal. To ensure a constant supply of power, FNPPs can be operated in fleets, with a new FNPP arriving and replacing the old one before it departs.

Proliferation and Security Concerns

Russia's development of FNPPs has given rise to several proliferation concerns from experts and policymakers, mainly because of its plans to lease the plants abroad. The concerns are about the risk of material diversion when the plant is stationed in another state's territorial waters; the security of the plant, both when in transit and on lease to a state; and the security of FNPPs when it is stationed in Russia itself.

Leasing FNPPs and the risk of state-level proliferation:

If Russia is successful in leasing the plants, then the risk of proliferation regarding recipient states could be reduced by an arrangement known as "build-own-operate". Under this arrangement, Russia will be responsible for towing the plant to the designated location, providing the needed electricity and desalination services, and then towing it back to Russia at the end of the 12-year cycle for refuelling and maintenance. In this case, Russia will only be supplying electricity and not transferring ownership of the FNPP. This arrangement greatly reduces the risk of material diversion.

Non-state actors:

A regular criticism of the export of FNPPs is that it will require the vessels to travel over very large distances in the open and unsecured sea, thereby exposing them to the dangers of pirates and also sabotage.

While there could be mixed assessments over the security details of FNPPs, it is believed that the plants were designed with security in mind. For example, some Russian experts claim that the vessels will contain iris and fingerprint detection systems for entry into various sensitive areas, as well as underwater protection against threats from there. But it is currently not possible to verify this information, and there are questions about the availability of sufficient manpower to guard the stationary vessels. There is also confusion as to whether

Case Studies

Akademik Lomonosov– Russia

Akademik Lomonosov is the first ship of this kind which was named after 18th-century Russian scientist Mikhail Lomonosov. It is a nuclear plant (see Figure 1) that produces enough electricity to power a city of about 100,000 people.

Russian personnel will protect plants stationed abroad or if that will become the responsibility of host nations. If the latter is true, then some states may find it difficult to ensure adequate physical protection.

Spar-Type Platform Design for the Offshore Floating Nuclear Power Plant (OFNP)

The Offshore Floating Nuclear Plant (OFNP) is a new concept that comes with lots of economic attraction as well as an unparalleled level of safety. The designers of the OFNP combine state-of-the-art Light Water Reactors (LWRs) and oil and gas offshore floating platforms. These two technologies already have established for themselves a reputation for safety. The OFNP can be built within a shipyard and then moved to the site using a tug boat, where it can be fixed within a few miles off the coast.

Figure 3: Offshore Floating Nuclear Power Plant (OFNP)

The OFNP is designed to be able to withstand significant damage while remaining afloat, using designs from the U.S. Navy (Lee et al., 2015). A typical OFNP is shown in Figure 3. Since OFNP is a floating power plant, it is difficult for earthquakes caused by seismic loads from the ocean floor to affect the plant structures; therefore, earthquakes are eliminated as a safety concern. The platform can be designed to withstand extreme storms.

Security Concerns

Offshore siting makes it easier to monitor the plant's surrounding area and harder for prospective attackers to gather information about plant vulnerabilities (Buongiorno et al., 2016). However, in addition to attacks from surface and air, an offshore plant is potentially exposed to subsurface attacks. In developing the OFNP security plan, it is important to identify all possible threats and determine whether the primary responsibility to protect against each threat lies with the plant owner/operator or the government, that is, law enforcement or military personnel. Table 2 shows a preliminary categorization of security threats for the OFNP. For those threats that fall under the owner/operator's responsibility, the security forces at the plant must be able to fend off an attack until external intervention can occur.

Table 2: Security Threats for OFNP (Buongiorno et al., 2016)

	Host Nation – National Military	OFNP – Security Team
Air	Military aircraft	Drones
	Commercial aircraft	Light planes/Helicopters
	Missile	
Surface	Large tankers	Non-military boats
	Military surface vessels	
Subsurface	Large submarines	Mini-subs (torpedoes)
		Divers (explosives)

Transport Security for SMRs

The Akademik Lomonosov SMR and OFNP are emerging technologies that offer unique advantages in terms of flexibility and mobility for generating nuclear energy. However, ensuring the security of these mobile nuclear facilities during transport presents specific challenges, which include:

i. Vulnerability to Physical Attacks: The small size and mobility of SMRs and FNPPs can make them possible targets for physical attacks, which include theft, sabotage, or unauthorized access. It is very crucial to detect and mitigate vulnerabilities to be able to reduce these risks.
ii. Secure Transport Containers: A safe and secure transport of SMRs and FNPPs requires the use of secure transport containers designed to withstand accidents, extreme environmental conditions and resist potential attacks. These containers should

have features such as tamper-evident seals and real-time trackers to ensure the integrity and security of the transported nuclear materials.

iii. Secure Transport Routes: Establishing secure transport routes is important to reducing the risk of unauthorized access and ensuring the safe transportation of SMRs and FNPPs. Factors such as infrastructure suitability, road conditions, sea route conditions, potential security threats along the route, and coordination with relevant authorities should be considered to select the most secure, effective and efficient routes.

These challenges can be addressed by putting in place appropriate measures; some of these are:

i. Security by Design (SeBD) Approach: The security by design approach should be applied during the design and construction of SMRs and FNPPs. This involves integrating security features and measures into the design process, such as access controls, perimeter security, intrusion detection systems, and emergency response capabilities, to improve the overall security of these mobile nuclear facilities. SeBD is discussed further in Section VIA.

ii. Comprehensive Security Plan: Developing a comprehensive security plan specific to the transport of SMRs and FNPPs is crucial. This plan should include security assessments, threat and vulnerability identification, and the implementation of appropriate security measures to address potential risks during transport. Regular review and updates of the security plan are necessary to adapt to evolving threats.

iii. Layered Security Measures: Implementing a layered security approach is essential to protect SMRs and FNPPs during transport. This involves the deployment of multiple security layers, such as physical barriers, intrusion detection systems, surveillance technologies, access controls, and well-trained security personnel, to deter and respond to security threats effectively.

iv. To strengthen in-transit controls, the IAEA's Transport Standard now mandates tamper-evident seals, real-time GPS tracking, and enhanced container design tests for SMR modules, tightening both physical and procedural safeguards (IAEA, 2024).

By adopting the above procedures, it is possible to improve the security of SMRs during transport. It is also very important to note that it is the responsibility of the shipping or sending State to ensure that the nuclear material and other radioactive materials are adequately protected during transit in local or international routes and in the transit State until that responsibility is properly transferred to another State (IAEA, 2011, 2013, 2020b). Multiple response forces across these jurisdictions are crucial for the safe transportation of SMRs and FNPPs. This requires establishing a clear and strong chain of command, roles and responsibilities. Facilitating a coordinated response in emergencies through joint planning exercises allows response forces to understand each other's capabilities and to develop effective strategies. Communication plays a vital role in coordination; compatible communication systems enable real-time information sharing, while designated communication points facilitate direct and efficient communication during transport operations. Cooperation is vital for a secure transport environment. Mutual agreements facilitate resource sharing and support between States and jurisdictions, ensuring a synchronized response to emergencies. Information and intelligence sharing provides an understanding of risks and threats during transport (IAEA, 2020b).

Physical Protection Systems for SMRs

Although physical protection of radioactive material and nuclear facilities are state affairs, the Akademik Lomonosov SMR and OFNP are likely to move from one state to another as well as move on international waters. To proffer a solution, an international convention that is shared with the operator will need to be made to protect the FNPP in international waters. In addition to an international convention, the operator or licensee should be made to come up with their PPS in line with the state (regulator). The proposed approach below by Evans et al. (2021); Cheng & Bari (2021) can be used to come up with PPS for the Akademik Lomonosov SMR and OFNP or any FNPP.

i. A competent authority or regulator shall provide a design-based treat (DBT) and possible threats along with an effective PPS to the operator.

ii. A competent authority or regulator shall provide performance requirements with respect to the DBT and possible threats to the operator.

iii. The competent authority or regulator shall define the provided performance requirements to the operator.

iv. Plans should be made to avoid on-site storage of fresh and/or spent fuel.

v. A thought-out plan and consideration must be given to issues concerning access for adversaries, response forces and inspectors. This is important because of the isolation of the site

vi. Remote monitoring of the reactor that can transmit and evaluate data offsite. This must be discussed between the operator/state/IAEA.

Table 3 provides a proposed PPS for the various stages of physical protection (Evans et al., 2021; Sandt, 2021). It is important to note that since the full details of both the Akademik Lomonosov SMR and OFNP are in their experimental and developmental stages, their PPS, DBT and performance requirements are re-evaluated from time to time.

Table 3: Proposed Physical Protection for both Akademik Lomonosov SMR and OFNP

	Proposed PPS for both Case Studies
Target Identification	i. Identify and classify all radioactive materials (e.g. spent fuel). ii. Determine if direct dispersal of these radioactive materials is possible. iii. Identify events or malicious acts that can indirectly lead to the sabotage of radioactive materials. iv. Design a sabotage logic model (SLM) that represent combinations of procedures and event which can lead to indirect sabotage of radioactive materials. v. Remove procedures and events from the SLM that are outside of the DBT. vi. Identify paths and targets that correspond to events on the SLM and replace procedures and events with their related paths and targets. vii. Identify paths the adversary access to cause sabotage or theft. viii. Identify critical paths and combinations of paths that must be protected in other to avert sabotage and protect these paths.
Threat Assessment/Characterization	i. A competent authority or regulator shall provide a DBT and possible threats along with an effective PPS to the operator. ii. A competent authority or regulator shall provide performance requirements with respect to the DBT and possible threats to the operator. iii. The competent authority or regulator shall define the provided performance requirements to the operator.
Intrusion detection systems	Exterior Detection System i. A continuous line of detection is required around the FNPP. In reality, this may require configuring the sensors in such a manner that the detection zone from one part of the FNPP must overlap the detection zones of other parts of the FNPP. ii. Balanced detection should be put in place so that when an adversary tries to achieve their goal, effective elements of the PPS will be met. iii. Defence-in-depth and protection-in-depth involve the use of different layers of detection. iv. Priority schemes – This allows alarms to be evaluated with the aid of computers by the system operator. The priority scheme establishes the time order of assessment for multiple simultaneous alarms. The computer then sets a priority for all alarms based on the probability that an alarm event corresponds to a real intrusion.
Access controls	i. It is very important to consider designing access controls for target areas and locations that may need them. These areas may include the area housing the reactors, spent fuel pool, other areas housing radioactive materials and the control room. ii. FNPPs are designed to have minimal personnel and security staff during normal operations. This simply means that a complex access control system may not be necessary because of the fewer staff that would be onboard. With fewer personnel onboard, the access control system may only be required at target area access points. iii.
Access Delay	i. The use of active delay elements should be deployed in the PPS. For higher efficiency and cost-effectiveness, delay capability should be increased on the path to the target area, with the best active and dispensable delays installed in the target location. ii. Remotely Operated Weapon Systems (ROWS) can be installed and deployed around FNPP in other to delay the adversary before the response force arrives.

	Proposed PPS for both Case Studies
Guard and Response Force	Guard i. Implement the two-man rule ii. Provide access control roles iii. Conduct searches for prohibited items iv. Conduct alarm assessment v. Conduct alarm station monitoring vi. Provide escorts when and where necessary Response Force i. Familiar with either vessel or platform layout ii. Know the locations of the target area iii. Adequate training on contingency plans and measures iv. Adequate training in emergency plans v. Adequate training on facility access control procedures vi. Adequate training on the security plan vii. Adequately equipped with the necessary equipment viii. FNPP and PPS designers should consider and understand how the response force will be implemented as part of the PPS strategy. An onboard response force is likely to deliver a quick response. This would increase the probability of the response force's success in interrupting an adversary. ix. Response forces should be up-to-date with the regulations regarding the use of force and the ability to disarm and perform an arrest.

Security by Design

Security by design (SeBD) is a concept that incorporates security into all phases of facility design, construction, operations, and decommissioning (Snell & Jaeger, 2014). It should be part of a holistic approach, integrated with operations, safety, and nuclear material accounting and control, so they are mutually supportive and avoid conflicts. SeBD is also a risk-informed approach that requires multi-disciplinary teamwork and a clear security strategy. SeBD is a concept that is sometimes referred to as "intrinsic security," meaning that it is permanent, inseparable, or built-in. Implementing SeBD can reduce the risk of major security incidents and associated costs (WINS, 2019). A good SeBD should:

i. Minimize insider access to nuclear material and the opportunities for and risks associated with malicious acts
ii. Provides flexibility to respond to a changing threat environment
iii. Decreases operational security costs by reducing the reliance on the Protective Force
iv. Increases efficacy of Protective Force (e.g., on-site security guards) in the event of an attack

Three effective strategies for SeBD are described by Jaeger et al. (2013) . SeBD can be considered the output of an integrated security system design process. This process is well established within the Design and Evaluation Process Outline (DEPO) methodology for physical protection systems (Garcia, 2008)**,** and a refined version is shown in Figure 4.

SeBD principles applicable to SMRs and Nuclear Facilities include (Duguay, 2020):

i. Integrated approach: working with engineering and safety specialists to achieve integrated security systems; for example: integrating physical and cyber security specialists in the design process
ii. Inherently secure: design plants, facilities, buildings, and systems with security in mind at the beginning of the process
iii. Passive security: reduce reliance on active security and human measures to counter a security event
iv. Evolving response: the ability to provide a flexible response to changing threat levels and security.
v. Defense in Depth and Balanced Protection: the use of multiple security layers and measures that an adversary must defeat to access nuclear or other radioactive materials.

Further details on SeBD design principles and its international perspective for new nuclear facilities and SMRs, as well as examples of how SMR design could integrate threat information in countermeasures, are presented in Duguay's (2020) work.

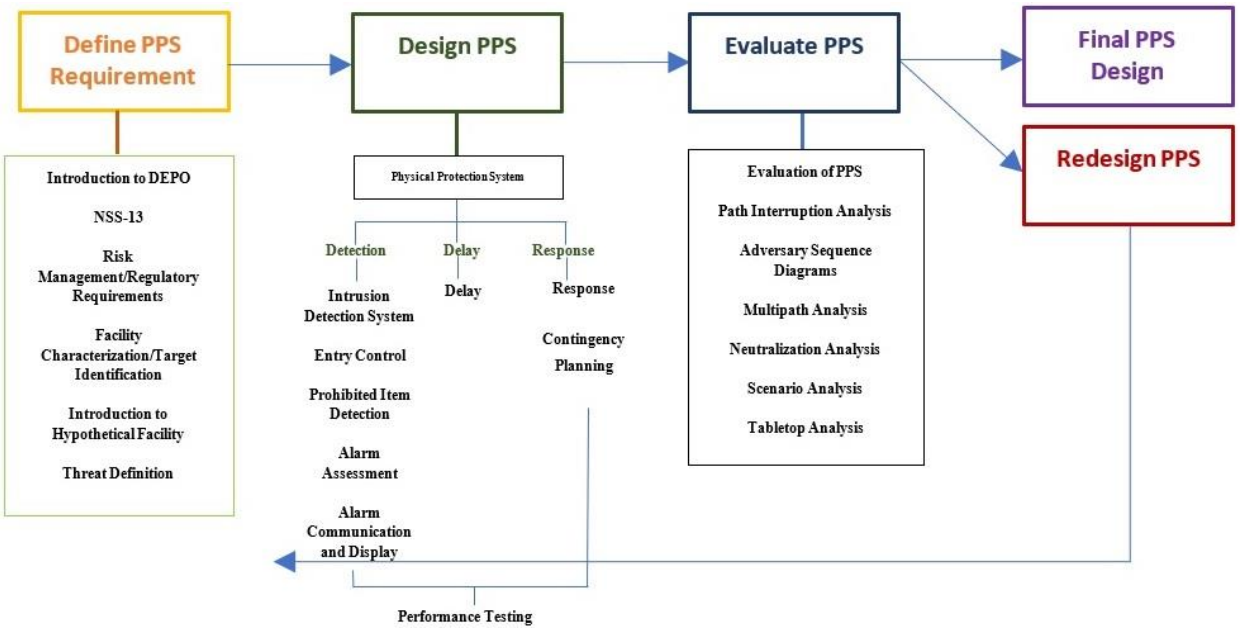

Figure 4: The Design and Evaluation Process Outline (DEPO) [Source: (Duguay, 2020)]

Target Identification

i. Identification of targets that must be protected from adversary attack: Target sets may differ for SMRs due to the decreased complexity of safety systems, especially safety systems that are external to the reactor.
ii. Vital Area Identification: A vital area is an area containing equipment, systems, devices, or nuclear material, the sabotage of which could directly or indirectly lead to high radiological consequences (Kwak & Jung, 2021).

Threat Assessment/Characterization

The complexity of the adversary and threats are ever-changing. This is particularly true for facilities that process or possess highly enriched uranium or plutonium. SMRs have a different threat environment than traditional NPPs may have. SMRs are being considered for deployment in urban environments, which may change the types of adversaries that may be considered in the design basis threat (DBT).

These threats may range from terrorist groups to environmentalist activists to petty criminals, but for Offshore SMR, it would most likely be terrorist groups, sea pirates or an Insider (employee) due to limited accessibility.

Tables 4a and 4b depict some adversary threat spectrum in Akademik Lomonosov and Spar-Type Platform Design for the Offshore Floating Nuclear Power Plant (OFNP) respectively, and a few countermeasures that could be applied to neutralize those threats.

Due to the wide publicity already of SMRs and their inherent safety, especially for the Akademik Lomonosov, which is operational, the threats include Insider threats, pirate raids, underwater attacks, and aerial attacks. Others include collision with another floating object or tsunamis. For the OFNP, the threat remains the same except for the fact it is stationary. Its threat is more predictable than the mobile facility, which could encounter a different kind of threat along its path depending on its location, for instance, pirate raid or extreme weather events.

Table 4a: Adversary Threats and Countermeasures of Akademik Lomonosov

Topic	Possible Countermeasures
Hypothetical challenges in capabilities to any threat attempting to commit	
i. Sabotage	A reduction in the number of critical areas subject to sabotage. Adoption of safety concepts such as inherently safe designs. Proper inventory management system.
ii. Theft	Application of the two-man rule. Steel vaults. Availability of CCTVs.
iii. Hijacking	Active automatic lockdown system.

Hypothetical changes to external threat	
i. Better weapons and/or weapon training	More sophisticated weapons and well-trained security personnel.
ii. More adversaries and/or better tactics	Availability of long-range cameras for early detection and preparedness. Well-trained personnel.
iii. Cyber-attack capabilities	Placement of updated cyber protection system like the wavy-attention neural network which was demonstrated by Ayodeji et al. (2024).
Hypothetical changes to an internal threat	
i. More active and/or more violent insider adversaries	Two-man rule. Compartmentalize facility and responsibility. Limit access, knowledge, and authority to the security system. Human reliability program.
ii. Cyber-attack capabilities	Placement of updated and effective cyber security system.

Table 4b: Adversary Threats and Countermeasures of Spar-Type Platform Design for the Offshore Floating Nuclear Power Plant (OFNP)

Topic	Possible Countermeasures
Hypothetical challenges in capabilities to any threat attempting to commit	
i. Sabotage	A reduction in the number of critical areas subject to sabotage. Adoption of safety concepts such as inherently safe designs. Mini submarines and divers for an underwater attack.
ii. Theft	Proper inventory management system. Application of the two-man rule. Active surveillance cameras. Availability of CCTVs.
Hypothetical changes to external threat	
i. Better weapons and/or weapon training	More sophisticated weapons and well-trained security personnel.
ii. More adversaries and/or better tactics	Availability of long-range cameras for early detection and preparedness. Well-trained personnel.
iii. Cyber Attack capabilities	Placement of updated cyber protection system.
Hypothetical changes to an internal threat	
i. More active and/or more violent insider adversaries	Two-man rule. Compartmentalize facility and responsibility. Limit access, knowledge, and authority to the security system. Human reliability program.
ii. Cyber-attack capabilities	Placement of updated and effective cyber security system.

Facility Characterization

Facility characterization is as follows:

i. Physical conditions include; Building Structure (construction materials, heating and ventilation cooling system), room location, site boundaries, access point, and processes within the facility.
ii. Operation conditions (working hours, off-hours, and potential emergencies), types and numbers of employees, facility policies and procedures, regulatory requirements, legal issues, cooperative goals, and objectives.

Intrusion Detection Systems

Intrusion detection systems (IDSs) aggregate various components that sense adversary activity and transmit a signal to the monitoring station, where the operator performs the assessment and initiates a response if necessary. These devices include magnetic door switches, motion sensors, capacitance sensors, vibration

sensors, etc. The IDSs may be passive (the device listens or searches for energy coming from the adversary, an infrared sensor) or active (the device emits energy to detect the adversary, a break beam sensor). These devices may be covert (hidden from view) or overt (visible) and can be volumetric (cover height, width, and length) or line detection (provide coverage of a narrow, two-dimensional area).

Vaults, vital locations, and target areas should have some sort of volumetric or boundary IDS coverage. Volumetric sensors cover an area including length, width, and height. Boundary coverage includes walls, ceilings, floors, etc. Different types of sensors can be used to achieve the goals of the security system.

Exterior Detection System

This enables timely detection of the adversary at the facility perimeter and increases the amount of time available for the response to get into position. Detection of the adversary at the area boundary rather than at the target entrance will increase the effectiveness of the security system. An example of Exterior detection is a long rage searchlight and effective night vision cameras. Different types of devices may operate differently under varying environmental conditions. Specific concerns are rain/storms, lightning frequency, annual temperature range, and humidity. Consideration should also be given to the size of the perimeter. A 2 km perimeter may not be difficult to cover with sensors and cameras. A 20 km perimeter would be much more complex and much more expensive. Therefore, it's good that SMRs are small compared to NPPs which means a smaller perimeter range. Technologies that have been applied to the transportation security of maritime vessels, such as SONAR (system of detection of objects under water by emitting sound pulse), RADAR, and LIDAR (light detection and ranging) may also apply to offshore SMRs that are placed on ships

Access Controls

Access control tends to be differentiated using what you have (Peripheral Interface Controller - PIC), what you know (Personal Identification Number) and what you are (Fingerprint, biometric). Defeating a system that has combined all three is very difficult (PIN, coded badge, and hand geometry).

Biometric access that should be used are:

i. Eye features like retina or iris
ii. Hand and finger features like palm print, fingerprint, or subcutaneous infra-red mapping
iii. Facial recognition
iv. Voice Biometrics based on measurable physical or behavioural features.

Access Delay

With any type of attack, it becomes a race between the response force and the adversary unless the adversary is not detected or not assessed, or the response force is not notified of the intrusion. To increase the response force's likelihood of interrupting and neutralizing the adversary after attack notification, a balanced delay should be implemented for all viable attack paths, and the delay should be sufficient to expend all the DBT attack tools. Access delay technologies and physical barriers should be designed and constructed to protect against radiological sabotage. Physical barriers should provide delay and support detection, assessment, access controls, and mitigate the insider threat.

Guard and Response Force

Deployment of SMRs may reduce costs for power production. One way these costs may be reduced is by minimizing the guards present onsite or removing all onsite. SMR facility designers, operators, and security managers need to determine and understand how guard and response force members will be implemented as part of the security system. Guards should have up-to-date weapons and adequate experience and training to repel adversaries before external response forces arrive. Response forces should be well equipped and have means of responding quickly, like helicopters that could arrive at the facility in time before adversaries get to the target. There are new revolutionary technologies and advanced PPS that should be considered during the design phase that could be used to deter, detect and respond to a potential attack on an offshore floating SMR facility. Listed below are some solutions for an effective PPS for floating SMRs:

i. Long-range acoustic device: This is a non-lethal anti-piracy device that uses pain-inducing sound beams to prevent intrusion. The sonic weapon produces a high-pitched noise that is above human tolerance. This device could be used as a deterrence for potential invaders
ii. Underwater sonar detection system: This is used against an underwater attack. It tracks and identifies divers and underwater vehicles approaching a Floating SMR from any direction using heat and magnetic sensors and triggers an alarm to alert in-house security personnel
iii. Anti-drone detection system: the anti-drone device detects and identifies commercial drones in about 20km range, and it also provides the GPS location of both the drone & pilot together with the drone's speed and direction the drone is heading.
iv. Cloaking system: The cloaking system creates an organic smoke that reduces visibility to less than a foot. This could act as a delay system to increase adversary task time and provide external response less time to arrive at the facility

v. Lockdown System: This is an automatic lockdown system that could be triggered in an attempt to breach vital areas without authorized access
vi. Night vision goggles: These could aid night vision for security personnel
vii. Vibration sensors: These sensors should be around the Floating SMR and underneath for detection of intrusion.
viii. New drones equipped with cameras, radiation or heat sensors, and firing capabilities, for perimeter surveillance, radiation detection, and response to an attack.

CONCLUSION

One of the greatest impacts of SMRs on PPS would be a significantly lower cost for PPS than in large nuclear reactors or conventional power plants, owing largely to the difference in the size of both facilities. Also, in SMRs, safety would be more focused and enhanced because of their smaller size and fewer critical areas. This work supports one of the major advantages of SMRs over the traditional NPP, which is that their PPS is easier to manage due to their size which implies less vital areas which could be easily managed. They are also less prone to target than the conventional NPP because adversaries would rather put in more effort to carry out an attack or sabotage a facility that would yield more devastating radiological consequences. The security system of an SMR is designed by experts based on a thorough evaluation of threat assessment and various potential adversary attack scenarios. Although there might not be a defined adversary pathway, adversary scenarios for Floating SMRs are more likely from underwater or by air. Offshore SMRs have a significant advantage as they are far from human habitation therefore, the threats are low since they are neither easily assessable nor provide an easy escape route for adversaries, and the radiological consequences are less harmful. During this research, it was discovered that there wasn't adequate information on the physical protection system of the Akademik Lomonosov, which is believed to be due to security reasons as it is the first of its kind in existence. However, this work has analysed and proffered applicable effective PPS suitable for Akademik Lomonosov and Spar-type design of Offshore floating Nuclear Power Plant SMRs.

REFERENCES

Ayodeji, A., Di Buono, A., Pierce, I., & Ahmed, H. (2024). Wavy-attention network for real-time cyber-attack detection in a small modular pressurized water reactor digital control system. *Nuclear Engineering and Design*, *424*, 113277. https://doi.org/10.1016/j.nucengdes.2024.113277

Bentoumi, G., Van Der Ende, B., Chaudhuri, A., & Trask, D. (2020). SAFETY AND SECURITY OF SMALL MODULAR REACTORS IN CANADA. *Third International Conference on Nuclear Security: Sustaining and Strengthening Efforts (ICONS 2020)*.

Black, G., Shropshire, D., & Araújo, K. (2020). Small modular reactor (SMR) adoption: Opportunities and challenges for emerging markets. In *Handbook of Small Modular Nuclear Reactors: Second Edition* (pp. 557–593). Elsevier. https://doi.org/10.1016/B978-0-12-823916-2.00022-9

Buongiorno, J., Jurewicz, J., Golay, M., & Todreas, N. (2016). The Offshore Floating Nuclear Plant Concept. *Nuclear Technology*, *194*(1), 1–14. https://doi.org/10.13182/NT15-49

Cheng, L., & Bari, R. A. (2021). Proliferation resistance and physical protection (PR&PP) in small modular reactors (SMRs). In D. T. Ingersoll & M. D. Carelli (Eds.), *Handbook of Small Modular Nuclear Reactors* (pp. 217–238). Elsevier Ltd.

Duguay, R. (2020). Small Modular Reactors and Advanced Reactor Security: Regulatory Perspectives on Integrating Physical and Cyber Security by Design to Protect Against Malicious Acts and Evolving Threats. *International Journal of Nuclear Security*, *7*(1), 2. https://doi.org/https://doi.org/10.7290/ijns070102

Evans, A., Byrum, C., Stanford, D., Sandt, E., & Goolsby, T. (2021). *Physical Protection Recommendations for Small Modular Reactor Facilities*. https://doi.org/10.2172/1837151

Faucett, C., & Vierow Kirkland, K. (2023). State-of-the-Art in Evaluation Approaches for Risk Assessment of Insider Threats to Nuclear Facility Physical Protection Systems. *Nuclear Science and Engineering*, *197*(sup1), S1–S12. https://doi.org/10.1080/00295639.2022.2130635/ASSET/2C4CA4CC-512C-4629-9FAF-73944B4210B7/ASSETS/IMAGES/UNSE_A_2130635_F0001_B.GIF

Garcia, M. L. (2008). Design and Evaluation of Physical Protection Systems. In *Design and Evaluation of Physical Protection Systems* (pp. 1–11). Elsevier. https://doi.org/10.1016/B978-0-08-055428-0.50005-1

Gill, M., Livens, F., & Peakman, A. (2014). Nuclear Fission. In *Future Energy* (pp. 135–149). Elsevier. https://doi.org/10.1016/B978-0-08-102886-5.00007-4

Gkouliaras, K., Theos, V., Miller, T., Jowers, B., Kennedy, G., Grant, A., Cronin, T., Evans, P. G., & Chatzidakis, S. (2025). Demonstration of Quantum-Secure Communications in a Nuclear Reactor. *Arxiv*. https://arxiv.org/pdf/2505.17502

Hayafune, H., Ruggieri, J., Kim, Y., Ashurko, Y., Hill, R., Glatz, J., & Yang, H. (2017). Current status of GIF collaborations on sodium-cooled fast reactor system. *International Conference on Fast Reactors and Related Fuel Cycles*, 132–132. https://inis.iaea.org/records/xnk4t-td006

Hidayatullah, H., Susyadi, S., & Subki, M. H. (2015). Design and technology development for small modular reactors – Safety expectations, prospects and impediments of their deployment. *Progress in Nuclear Energy*, *79*, 127–135. https://doi.org/10.1016/j.pnucene.2014.11.010

IAEA. (2004). Code of Conduct on the Safety and Security of Radioactive Sources. In *Code of Conduct on the Safety and Security of Radioactive Sources*. International Atomic Energy Angency. https://www.iaea.org/publications/6956/code-of-conduct-on-the-safety-and-security-of-radioactive-sources

IAEA. (2011). Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5). *IAEA Nuclear Security Series*, *No.13*. www.iaea.org/books

IAEA. (2013). *Objective and Essential Elements of a State's Nuclear Security Regime*. INTERNATIONAL ATOMIC ENERGY AGENCY. https://doi.org/10.61092/iaea.ajrj-ymul

IAEA. (2019). Security of Radioactive Material in Use and Storage and of Associated Facilities. *IAEA Nuclear Security Series*, *No.11-G (Rev. 1)*.

IAEA. (2020a). Preventive and Protective Measures against Insider Threats. *IAEA Nuclear Security Series*, *No. 8-G (Rev. 1)*. www.iaea.org/publications

IAEA. (2020b). Security of Radioactive Material in Transport. In *Security of Radioactive Material in Transport*. INTERNATIONAL ATOMIC ENERGY AGENCY STI/PUB/1872. https://www.iaea.org/publications/13400/security-of-radioactive-material-in-transport

IAEA. (2023). *Nuclear security conventions*. https://www.iaea.org/topics/nuclear-security-conventions

IAEA. (2024). *Security of Nuclear and Other Radioactive Material in Transport*. INTERNATIONAL ATOMIC ENERGY AGENCY. https://doi.org/10.61092/iaea.4umu-2uji

Jaeger, C. D., Snell, M. K., Jordan, S. E., Scharmer, C., Tanuma, K., Ochiai, K., & Iida, T. (2013, May 1). Security-by-Design Handbook. *International Conf on Nuclear Security: Enhancing Global Efforts*.

Kosai, S., & Unesaki, H. (2024). Nuclear power, resilience, and energy security under a vulnerability-based approach. *Cleaner Energy Systems*, *7*, 100107. https://doi.org/10.1016/j.cles.2024.100107

Kwak, M. W., & Jung, W. S. (2021). Vital area identification for the physical protection of NPPs in low-power and shutdown operations. *Nuclear Engineering and Technology*, *53*(9), 2888–2898. https://doi.org/10.1016/j.net.2021.03.031

Lee, K. H., Kim, M. G., Lee, J. I., & Lee, P. S. (2015). Recent Advances in Ocean Nuclear Power Plants. *Energies 2015, Vol. 8, Pages 11470-11492*, *8*(10), 11470–11492. https://doi.org/10.3390/EN81011470

Liou, J. (2021). *What are Small Modular Reactors (SMRs)?* International Atomic Energy Agency. https://www.iaea.org/newscenter/news/what-are-small-modular-reactors-smrs

Michelle. (2019). *Advancing Nuclear Innovation: Responding to Climate Change and Strengthening Global Security*. Global Nexus Initiative (GNI). https://globalnexusinitiative.org/results/reports/advancing-nuclear-innovation-responding-to-climate-change-and-strengthening-global-security/

Müller, H. (2016). *WMD Arms Control in the Middle East*. Routledge. https://doi.org/10.4324/9781315546988

Nilsson, A., Jorant, C., Redmond, E., & Luongo, K. (2018). *GNI Advanced Reactors Security Analysis & Findings*.

Oka, Y., & Mori, H. (2014). Supercritical-pressure light water cooled reactors. In *Springer* (Vol. 9784431550259). Springer Japan. https://doi.org/10.1007/978-4-431-55025-9

Poudel, B., Joshi, K. A., & Gokaraju, R. (2018). Analysis for Siting and Sizing of a Small Modular Reactor — A Case Study in Canada. *2018 20th National Power Systems Conference (NPSC)*, 1–6. https://doi.org/10.1109/NPSC.2018.8771710

Rossi, F. (2015). Safety, Security And safeguards In GEN IV sodium fast reactors [Ima Mater Studiorum Università di Bologna]. In *Dottorato Di Ricerca In Ingegneria Energetica, Nucleare E Del Controllo Ambientale, Alma Mater Studiorum*. https://amsdottorato.unibo.it/id/eprint/6836/

Sandt, E. (2021, May 1). How STPA can be used for target set and vital area identification. *How STPA Can Be Used for Target Set and Vital Area Identification*.

Serp, J., Allibert, M., Beneš, O., Delpech, S., Feynberg, O., Ghetta, V., Heuer, D., Holcomb, D., Ignatiev, V., Kloosterman, J. L., Luzzi, L., Merle-Lucotte, E., Uhlíř, J., Yoshioka, R., & Zhimin, D. (2014). The molten salt reactor (MSR) in generation IV: Overview and perspectives. *Progress in Nuclear Energy*, *77*, 308–319. https://doi.org/10.1016/J.PNUCENE.2014.02.014

Snell, M. K., & Jaeger, C. D. (2014, June 1). Incorporating Security-by-Design in both Planned and Operational Nuclear Facilities. *Institute of Nuclear Materials Management 55th Annual Meeting*.

Spiler, J., Kim, S.-B., Feron, F., Jaervinen, M.-L., Husse, J., Ferraro, G., Bertels, F., Denk, W., Tuomisto, H., Golay, M., Buongiorno, J., Todreas, N., Adams, E., Briccetti, A., Jurewicz, J., Kindfuller, V., Srinivasan, G., Strother, M., Minelli, P., … Organisation for Economic Co-Operation and Development, N. E. A.-O. L. S. S.-G. 12 boulevard des I. F.-92130 I.-M. (France). (2015). Proceedings (slides) of the OECD/NEA Workshop on Innovations in Water-cooled Reactor Technologies. *OECD/NEA Expert Workshop on Innovations in Water-Cooled Reactor Technologies*. https://inis.iaea.org/records/1azaq-fx413

Tekinerdogan, B., Yagiz, S., Özcan, K., & Yakin, I. (2020). Integrated Process Model for Systems Product Line Engineering of Physical Protection Systems,. In B. Shishkov (Ed.), *Business Modeling and Software Design* (10th ed. Cham, pp. 137–151). Springer. https://www.scribd.com/document/807986335/Business-Modeling-and-Software-Design-10th-International-Symposium-BMSD-2020-Berlin-Germany-July-6-8-2020-Proceedings-Boris-Shishkov-all-chapte

Upadhyaya, B., Hines, J. W., Damiano, B., Mehta, C., Collins, P., Lish, M., Cady, B., Lollar, V., De Wet, D., & Bayram, D. (2015). *In-situ Condition Monitoring of Components in Small Modular Reactors Using Process and Electrical Signature Analysis. Final report, volume 1. Development of experimental flow control loop, data analysis and plant monitoring*. https://inis.iaea.org/records/jfef8-fyz64

WINS. (2019). Implementing Security by Design at Nuclear Facilities. *WINS International Best Practice Guide*.

Yun, D., Lu, C., Zhou, Z., Wu, Y., Liu, W., Guo, S., Shi, T., & Stubbins, J. F. (2021). Current state and prospect on the development of advanced nuclear fuel system materials: A review. *Materials Reports: Energy*, *1*(1), 100007. https://doi.org/10.1016/J.MATRE.2021.01.002

Zohuri, B. (2020). Generation IV nuclear reactors. In *Nuclear Reactor Technology Development and Utilization* (pp. 213–246). Elsevier. https://doi.org/10.1016/B978-0-12-818483-7.00006-8