NUCLEAR HARMONIZATION & STANDARDIZATION INITIATIVE

Security by Design Considerations for SMRs

December 2025

Working Paper[1] produced by the NHSI Regulatory Track Nuclear Security Working Group

1. Background

As part of International Atomic Energy Agency (IAEA) efforts to raise awareness of the importance of nuclear security for global deployment of new reactor technologies, the Nuclear Security Working Group (NSWG) was established under the IAEA Nuclear Harmonization and Standardization Initiative's (NHSI) Regulatory Track. One of the primary objectives of the Nuclear Security Working Group is supporting the development of guidance and other deliverables for consistent and risk-informed approaches to nuclear security of advanced novel reactors and Small Modular Reactors (SMRs) for both regulators and industry. The NHSI Nuclear Security Working Group members consider Security by Design approaches to support the harmonization of regulatory practices by encouraging consideration of key international nuclear security recommendations, at the earliest stages of SMR design.

This Working Paper addresses benefits and application of Security by Design, particularly for advanced novel reactors and SMR designs. The deployment of advanced novel reactors and SMRs to States worldwide, both with existing and potentially new nuclear power programmes, provides an opportunity for SMR developers (e.g., designers and vendors) to 'build in' financial and operational efficiencies through the implementation of Security by Design. The IAEA considers 'Security by Design' to be design approaches that take into account the needs of nuclear security. Implementing such approaches may lead to reduced physical protection costs over the lifetime of the nuclear facility and may simplify the task of maintaining an effective physical protection system over that lifetime. Security by Design is best implemented through a structured approach in which a State's nuclear security objectives are considered and fully taken into account in design decisions for the entire lifetime of the facility, starting with the planning of the facility and continuing through the design, construction, operational and decommissioning phases.[2] In the SMR context, Security by Design can be understood as a risk-informed approach to integrating nuclear security principles early into the design process of new SMR facilities in ways that are cost-effective and easily compatible with operations. Security by Design also allows to leverage the nexus between safety and security; for example, by optimizing safety systems and operational programmes to increase the resistance of the facility to sabotage and to reduce potential dose consequences to the public and/or the environment. By incorporating Security by Design principles, the nuclear industry can optimize the effectiveness of security measures and reduce the need for costly upgrades or additions later on. Early integration of these principles also supports multilateral cooperation and harmonization by encouraging designers and vendors to demonstrate security considerations, including any interfaces, from the earliest stages of design. The NHSI Nuclear Security Working Group also encourages further analyses and efforts to

[1] This paper is not an IAEA publication. It reflects the consensus opinion of the individual members of the NHSI Regulatory Track Nuclear Security Working Group. The views expressed do not necessarily reflect those of the IAEA or its Member States. A forthcoming IAEA Nuclear Security Series publication, "*Concepts and Application of Security by Design, Nuclear Security Technical Guide No. 071*", currently under development, will provide technical guidance on concepts and application of Security by Design to, at the design stage, reduce security vulnerabilities, improve security efficiency and effectiveness related to facility design, layout, operations, maintenance.

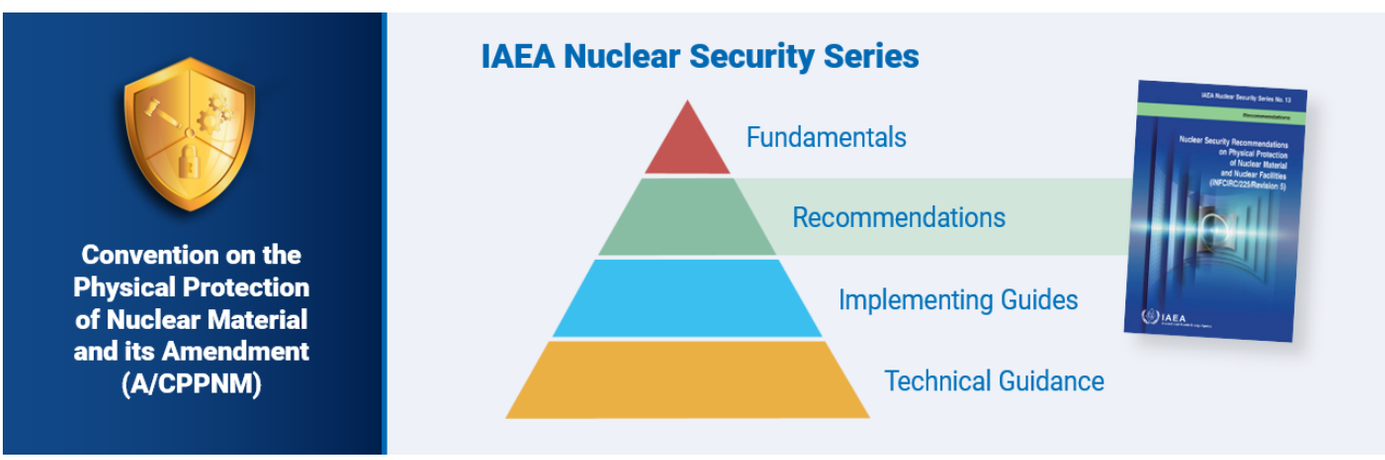
[2] INTERNATIONAL ATOMIC ENERGY AGENCY, *Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5), Nuclear Security Series No. 27-G, IAEA, Vienna (2018)*

validate specific security by design approaches, particularly with respect to initial construction and operational costs.

2. Providing Insights on Nuclear Security Regulatory Expectations: An International Nuclear Security Regime Perspective

Different national level requirements will shape nuclear security requirements for new nuclear energy facilities. These requirements may be prescriptive or performance-based, and underpinned by international guidance from the IAEA. Additionally, risk-informed design decisions must take into consideration threats, vulnerabilities, and consequences associated with nuclear material theft or sabotage of nuclear facilities and transports. While national security requirements may vary, baseline nuclear security requirements are largely based on an international framework that includes relevant legal instruments and international recommendations and guidance documents:

The Convention on the Physical Protection of Nuclear Material and its Amendment (A/CPPNM) requires States Parties to establish, implement and maintain an appropriate physical protection regime with the aim of: protecting against theft or other unlawful taking of nuclear material; ensuring implementation of rapid measures to recover missing or stolen material; protecting facilities and material from sabotage; and mitigating or minimizing radiological consequences of sabotage. To implement this regime, States Parties are obliged to: establish and maintain a legislative and regulatory framework for physical protection; designate a competent authority responsible for implementing this framework; and take other appropriate administrative measures necessary for the physical protection of nuclear material and facilities.



The IAEA's Nuclear Security Series (NSS) publications provide comprehensive non-legally binding guidance to States on nuclear security related topics. These publications are consistent with, and complementary to, international nuclear security instruments. IAEA Nuclear Security Series No. 13, *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities* (INFCIRC/225/ Revision 5) is the document that forms the basis for States' nuclear security regulations for nuclear material and nuclear facilities, providing guidance on the implementation of the legally binding A/CPPNM. Nuclear Security Series No. 13 also encourages the implementation of Security by Design approaches, as Section 3.18 states "…the site selection and design should take physical protection into account as early as possible…"

Furthermore, IAEA Nuclear Security Series No. 19, *Establishing the Nuclear Security Infrastructure for a Nuclear Power Programme* provides guidance on the actions to be taken by a State in implementing an effective nuclear security infrastructure for a nuclear power programme, consistent with the IAEA Nuclear Energy Series No NG-G-3.1 (Rev.1), *Milestones in the Development of a National Infrastructure for Nuclear Power*[3].

[3]INTERNATIONAL ATOMIC ENERGY AGENCY, Milestones in the Development of a National Infrastructure for Nuclear Power, IAEA Nuclear Energy Series No NG-G-3.1 (Rev.1), IAEA, Vienna (2024).

IAEA Nuclear Security Series publications provide useful guidance and technical recommendations for effective nuclear security of SMRs. The most directly relevant to a Security by Design approach, to ideally be implemented as early as possible in the design process, include:

1. **NSS No. 20,** Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Series
2. **NSS No. 13,** Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities *(INFCIRC/225/Revision 5)*
3. **NSS No. 7,** Nuclear Security Culture
4. **NSS No. 8-G,** Preventive and Protective Measures Against Insider Threats
5. **NSS No. 10-G, (Rev 1)** National Nuclear Security Threat Assessment, Design Basis Threats and Representative Threat Statements.
6. **NSS No. 19,** Establishing the Nuclear Security Infrastructure for a Nuclear Power Programme
7. **NSS No. 25-G,** Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities
8. **NSS No. 27-G,** Physical Protection of Nuclear Material and Nuclear Facilities *(Implementation of INFCIRC/225/Revision 5)*
9. **NSS No. 42-G,** Computer Security for Nuclear Security
10. **NSS No. 17-T,** Computer Security Techniques for Nuclear Facilities
11. **NSS No. 32-T,** Establishing a System for Control of Nuclear Material for Nuclear Security Purposes at a Facility During Use, Storage and Movement
12. **NSS No. 33-T,** Computer Security of Instrumentation and Control Systems at Nuclear Facilities
13. **NSS No. 35-G,** Security during the Lifetime of a Nuclear Facility
14. **NSS No. 39-T,** Developing a Nuclear Security Contingency Plan for Nuclear Facilities
15. **NSS No. 40-T,** Handbook on the Design of Physical Protection Systems for Nuclear Material and Nuclear Facilities
16. **NSS No. 48-T,** Identification and Categorization of Sabotage Targets, and Identification of Vital Areas at Nuclear Facilities
17. **NSS No. 49-T,** Evaluation of Physical Protection Systems at Nuclear Facilities

IAEA Nuclear Security Series No. 35-G, *Security during the Lifetime of a Nuclear Facility* is an implementing guide that supports IAEA Nuclear Security Series No. 13, and provides actions for the State, Competent Authority, and the Operator to implement security throughout the nuclear facility lifecycle as outlined in stages. As such, NSS No. 35-G is a valuable reference for industry in understanding potential nuclear security requirements and guidelines for the implementation of Security by Design for nuclear material and nuclear facilities, as follows:

Key Security by Design Steps	Relevant Actions per NSS 35-G
1. Identify applicable regulatory requirements based on material to protect	Actions 1-15, 1-16, 3-8
2. Establish Information Security Program	Actions 1-22, 2-7, 3-7
3. Ensure preparation and training of appropriate Operator management, licensing, and design personnel to implement security within the design of the facility	Actions 1-18, 2-9
4. Define security design strategy	Action 3-6
a. Deployment type and location	Action 2-6, 2-8
b. Regulatory Requirements	Actions 1-17, 1-23, 2-10
c. Physical protection system strategy	Actions 1-21
5. Define security design parameters important in the design (facility layout, safety system components of security interest, nuclear and other radioactive material inventory limits, etc..) and include security parameters within the facility design goals and planning	Actions 1-19, 3-9
6. Include security within the design change control process	Actions 1-20, 3-10
7. Design physical protection system (PPS) for regulatory requirements	Actions 3-11
8. Assess PPS design via tabletops / modeling and simulation tools	Action 3-13
9. Review and update PPS design throughout the design of the facility	Action 3-12

3. A Method for SMR Security by Design: Incorporating Nuclear Security at Different Stages of the Design Lifecycle Process

Relevant Stages of the SMR Design Process

Conceptual design	Initial design	Detailed design	Construction	Commissioning
Identify security regulatory requirements. Define security design strategy	Integral aspects of nuclear reactor and facility design	Preparation for regulatory approval Implement security design strategy Integration of security design	Operators employ security by design methods and meet licensed commitments and design parameters	Ensure all elements of the security programme are installed as designed and operate as intended

Although different technologies and different applications will require some variability in how nuclear security is implemented across the spectrum of SMRs, one recommendation for a consistent approach to Security by Design is for industry to consider the overall life cycle of a design process and how nuclear security can be incorporated into different stages of that process, including the feasibility analysis. Designers and vendors are encouraged to work with Competent Authorities and operators, as appropriate, to understand and balance prescriptive and performance-based requirements during the different stages, as well as the means to evaluate their security systems. Security by Design can also be identified as "intrinsic security" (as described in IAEA Nuclear Security Series No. 40-T, *Handbook on the Design of Physical Protection Systems for Nuclear Material and Nuclear Facilities*), that is, the inclusion of security considerations in the planning and design stages of reactor systems and facility for more effective and efficient security measures, as compared to extrinsic security that considers security after the facility design is complete. Below are some examples of how Security by Design can be integrated into the different stages of the design process starting at the conceptual design through construction and commissioning:

Conceptual Design Stage

The conceptual design stage is the initial phase of a project where the foundational attributes of the facility are explored and determined: determination of reactor technology (e.g., fuel, coolant, total power), the initial concept of deployment and operations (e.g., factory manufactured, floating, process heat, hydrogen production), and the planned market or deployment locations This stage could take into account options for flexibility and scalability of nuclear security measures as well as early consideration of relevant threat scenarios.

The conceptual design stage would identify the security regulatory requirements and then define the security design strategy. The security design strategy would enable actions such as:

- Incorporating considerations for values regarding High Radiological Consequences and Unacceptable Radiological Consequences, as defined by national regulations, in the design goals of the nuclear facility. The intent is that the design goals for both safety and security are integrated in the design of facility operational and safety systems.
- Incorporating security planning personnel within the facility design organization, so that facility design changes consider security requirements and do not unduly impact security, and security designs do not unduly impact safety.

- Including security in the planning for the concept of operations and deployment. This would inform functional design of the nuclear facility to reduce security vulnerabilities and make decision-makers aware of security requirements and costs for concepts of operations that differ from traditional nuclear power facilities. Deployment considerations may allow for reduced security requirements in specific circumstances (e.g. underground siting).
- Including security in the deployment location planning. The unique location of urban or remote facilities could impact security strategies involving offsite response organizations. Additionally, differences in security requirements between States may result in extensive and costly security design modifications if not considered in the design of the facility. Moreover, social, economic, and political conditions can also impact the security design, making it essential to consider these factors during the planning phase to avoid potential risks and complications.

Initial Design Stage

The initial design stage is characterized by work on the most integral aspects of the nuclear reactor and facility design: reactor core, fuel, coolant systems, primary heat transport system for energy production, and reactor island building. The initial design stage possesses the greatest flexibility for interfaces between safety and security, as the reactor systems have not yet been finalized within the facility design. Notably, incorporating advanced safety features at this stage can have a positive impact on reducing security requirements, making it an ideal time to consider safety and security interfaces that can enhance the overall safety and security of the facility. The design of reactor safety needs to consider an adversary's direct, indirect or computer aided attack on nuclear and other radioactive material. Safety systems should exhibit defense in depth properties to guard against an adversary attack, reduce reliance on active systems (e.g., electrical power, instrumentation and control, cooling), physical and electrical separation, redundancy, and minimize the potential for or consequences from compromise (malicious misuse by an adversary).

- The design and planning for nuclear and other radioactive material and reactor safety systems needs to consider security of these materials and systems against an adversary direct, indirect, and blended (i.e., computer system-aided) attack. This may include multiple and independent security barriers within the facility, minimization of safety system control interfaces that could be exploited, and considerations for computer-physical phenomenon to prevent or mitigate computer-aided sabotage and theft (i.e., physical separation or interlocks on computer-controlled actions).
- The initial design needs to also consider insider threat mitigation measures, ensuring that access controls, surveillance, and accountability features are incorporated to minimize opportunities for unauthorized actions (i.e., two-person rule).

Detailed Design Stage

The detailed design stage is where the largest share of design work occurs in preparation for regulatory approval to construct a nuclear facility. Detailed design of the reactor safety systems, supporting systems, facility layout, piping, cabling, and planning for maintenance and operational activities occur to ultimately support submission of a construction authorization application. At this stage, supply chain considerations are also important.

The design stage entails implementation of the security design strategy, and continued integration of the security design team within the design of the reactor facility. As the design matures, different opportunities for Security by Design and planning for physical protection systems and measures would become available:

- Computer security needs to be included in the design of the facility instrumentation and control systems, computer networks, and security systems including information security protocols.
- Planned maintenance and operational procedures need to consider security needs, to include insider threat mitigation, computer security, access control and searches.
- Nuclear material storage and operational procedures need to be planned at this stage to consider nuclear material accounting and control requirements and other security measures to prevent theft.
- Access points to vital areas and to the reactor building need to be minimized, and barriers to delay unauthorized access (to include unattended pathways and building structural materials) need to be incorporated.
- Limited access areas, protected areas, inner areas and vital areas, if applicable, need to be designed to facilitate detection and assessment.
- Delay elements need to be used to funnel adversaries toward predetermined locations where they can be delayed or interrupted, in order to maximize the response force's likelihood of neutralizing them.
- Response force positions need to be designed to be effective and efficient for adversary interruption.
- The facility layout needs to support effective detection, delay, and response, to include reduction or elimination of obstructions in the intrusion detection zones, protected area, and planned engagement areas, including contingency efforts as well as protection of equipment and personnel from adversary initiated offsite hazards or explosive devices as required.
- Where applicable, safety systems may be utilized to support nuclear security functions, for example by employing physical barriers that provide both delay against unauthorized access as well as radiation shielding or the application of radiation detection systems for both radiation safety and security purposes (e.g. alarms indicating elevated radiation backgrounds that also serve to detect attempted unauthorized removal of material).

Construction Stage

The construction stage may have some design work by an Operator to meet licensed commitments and design parameters for the facility as structures, systems, and components (SSCs) are built and installed, and operational physical protection systems are developed and finalized. During this phase, construction site security measures need also to be implemented to prevent the introduction of prohibited items or malicious acts that could compromise the future integrity of the facility (i.e., sabotage). There are opportunities here for operators to employ Security by Design methods within this phase:

- Modifications to security SSCs or physical protection systems and measures need to be evaluated to verify security system effectiveness and efficiency.
- Modifications to the facility design (to include vital equipment) need to be evaluated for impact to the security system design.
- Safety and security organizations need to design operational programmes and procedures to address safety and security needs in concert.
- The security organization needs to design procedures to address security needs by design, through security element SSCs or personnel.

- Limited scope performance testing needs to support final security plan submission to the competent authority.

Commissioning Stage

The commissioning stage ensures that all elements of the physical protection system are installed as designed and operate as intended. Before facility operation, the operator needs to verify all aspects of the physical protection system, and address shortcomings with a by-design approach that can best serve the operational lifetime needs of the facility. Full performance testing of the physical protection system will prepare the operator for competent authority inspections and oversight to confirm the effectiveness of the nuclear security measures, including implemented design decisions for the nuclear security system.

5. Conclusion

The NHSI Nuclear Security Working Group considers Security by Design for SMRs as a means for industry and for regulatory bodies to directly influence the security performance and long-term operational cost efficiency of designs. Security by Design can also support harmonization of regulatory practices by encouraging early consideration of key international nuclear security recommendations, regardless of specific technology or application. This paper provides some examples of Security by Design considerations during the life cycle of the design process, as well as key IAEA nuclear security guidance that can assist designers, vendors, and operators in pursuing more robust nuclear security solutions early in the design process. Early inclusion of Security by Design ensures the greatest potential for a robust and resilient design that can be compatible with operations, while potentially introducing cost savings through avoidance of retrofits later in the design process or during construction, commissioning, or operation of a facility. Additional analyses will support the cost-benefit of Security by Design approaches for the initial construction and operational costs associated with a security system. In this way, the benefits of Security by Design reinforce the vision and goal of NHSI, including the long-term aspiration of the Regulatory Track to develop harmonized approaches that support resource efficiency, accelerate deployment, and maintain national responsibilities for nuclear security.