Working Group on Design and Safety Analysis

Phase 3 Report

Safety, Security and Safeguards from a Regulatory Perspective: An Integrated Approach

December 2023

TABLE OF CONTENTS

EXECUTIVE SUMMARY

There continues to be sustained global interest in small modular reactors (SMRs), which have the potential to play an important role in globally sustainable energy development as part of an optimal energy mix. In particular, SMRs may enhance energy availability and security of supply in countries expanding their nuclear energy programs and those embarking on a nuclear energy program for the first time.

As the interest in SMRs continues to grow, so does the importance of international collaboration. Given that its main purpose is to bring together experienced regulators to identify and address key SMR-related challenges, the SMR Regulators' Forum has an increasingly important role to play in making such collaboration possible.

The SMR Regulators' Forum was formed in 2014 as a regulator-to-regulator entity to consider key issues that could emerge in future SMR regulatory discussions and propose common positions regarding the way in which these could be addressed. The Forum's work is expected to help enhance safety as well as efficiency in SMR regulation, including licensing, and to enable regulators to inform changes, if necessary, to their requirements and regulatory practices. Since then, the Forum has had three phases of work. For more details about the Forum, please visit: https://www.iaea.org/topics/small-modular-reactors/smr-regulators-forum.

This report has been produced by the Design and Safety Analysis (DSA) Working Group (WG) of the SMR Regulators' Forum during its Phase 3 (2021 to 2023). It analyses the integrated approach, by considering security and safeguards alongside safety during the early design development of the facility, with the aim of decreasing demand on resources for the implementation and operation of security and safeguards measures throughout the facility's life cycle. The text presents "common positions", i.e. agreements reached within the WG, on various issues relevant to the Safety, Security and Safeguards, known as 3S, integration.

This report was developed based on information, insights, and experience gained from the regulatory activities of the SMR Regulators' Forum members. It is generally consistent with existing IAEA documents but may deviate in some cases. This report is intended to provide useful information to regulators and industry in the development, deployment, and oversight of SMRs.

Common Positions for this report

Common Position 1

Claims made by developers that passive safety measures would reduce security risks need to be justified through the security risk assessment.

Common Position 2

Licensees are recommended to use insights from safety assessment to inform nuclear security. Probabilistic techniques can draw on Probabilistic safety assessment (PSA) and be useful for Vital Area Identification (VAI), sabotage target identification, vulnerability assessments etc.

Common Position 3

Potential conflicts between safety and security measures should be identified and minimized during the design stage. Potential synergies should be leveraged.

Common Position 4

When developing operating principles and procedures, licensees should account for both safety and security risks. Licensees should ensure that potential adverse and beneficial effects from implementation of changes (such as refurbishments, safety and security analyses changes, changes of operating principles and procedures) are considered for both safety and security measures to ensure these are addressed prior to their implementation. In other words, the facility change evaluation process should consider both safety and security measures to eliminate potential conflicts.

Common Position 5

Licensees are recommended to coordinate safety and security procedures, emergency response plans and security response plans, as part of emergency preparedness and response to security events. For SMRs, this may be especially challenging due to potential remote operation, siting and other aspects. Potential conflicts between safety and security measures should be identified and minimized when developing emergency preparedness procedures.

Common Position 6

When assessing risks and preparing for emergencies and malicious acts, licensees/developers should factor in 3S interfaces and combined risks where applicable and reasonable. This is especially important for novel applications such as cogeneration.

Common Position 7

SMR design process should reconcile measures in place to meet both, the IAEA safeguards arrangements, and the safety of the plant to ensure that they do not have adverse impacts on each other.

Common Position 8

SMR design may be compact, or complex compared to existing nuclear power plants (NPPs). Therefore, it is important that designers facilitate other means to accomplish safeguards activities if areas of the facility will be inaccessible to IAEA personnel during operation because of safety concerns. The exception to this is for temporary issues. For any kind of temporary issue, the licensee should proactively engage with the IAEA, or their regulator, as appropriate.

Common Position 9

Licensees/developers should approach the IAEA in the early stages of the SMR development to ensure that IAEA safeguards can properly be implemented. Existing IAEA safeguards measures may be applicable to SMRs. If not, new IAEA safeguards approaches, measures and techniques need to be developed by the IAEA.

Licensees/developers should be aware of the importance of physical facility layout and its potential constraints. Retrofitting to accommodate safeguards should be avoided so as to prevent negative impacts on safety and/or security.

Common Position 10

The novelty associated with SMR fuel designs may introduce new types of containers for transport. SMR safety designs should accommodate IAEA safeguards measures for containers and transport.

Common Position 11

SMR design should accommodate material accounting in the event of failed fuel and any retrieval of failed fuel.

Common Position 12

For Molten Salt Reactors (MSRs) where there is plating of radioactive material, the operator will need to account for nuclear material by tracking the movement of the material under all normal and off-normal operating conditions and the IAEA will have to verify the operator's information. This includes maintenance activities. The operator's instrumentation for tracking fuel movement should not have a negative impact on the same type of instrumentation used for safeguards purposes, and vice versa. If during regular operation and/or transients, molten salt including fuel needs to be drained, the designer and licensee should accommodate the IAEA's requirements for verification in all structures, systems and components (SSCs). The possibility to leverage synergies in this area should also be explored.

Common Position 13

The design should aim to allow the IAEA to maintain its safeguards systems even during off-normal events (for example - transients).

Common Position 14

With the nature of SMR fuel types, considering the potential for increased enrichment compared to the existing NPPs, the design process needs to ensure criticality safety. The configuration of nuclear material storage and movement outside the SMR needs to consider a safety aspect of criticality control and accommodate IAEA safeguards verification.

Common Position 15

If during regular operation and/or transients, fissile material needs to be drained (e.g., MSR), the design and licensee should accommodate the IAEA's requirements for verification.

Common Position 16

When applicable, SMR design process should strive to achieve in-vessel retention, which benefits both safety and safeguards, under severe accidents.

Common Position 17

The Nuclear Material Accounting and Control (NMAC) system for SMRs should be designed to meet all legal obligations associated with a safeguards agreement, as well as the nuclear security objectives. The possibility to leverage synergies in this area should also be explored.

Common Position 18

SMR design may be more compact and/or complex compared to existing NPPs, leading to additional security considerations. Therefore, it is important that the SMR designs facilitate IAEA access or other means for independent safeguards verification activities in their security plans.

Common Position 19

Given recent technology changes and increased cyber security risks and awareness, SMR designs can address cyber security issues in the design. Remote data transmission for safeguards should not compromise the cyber security and should meet standards prescribed by the IAEA. The possibility to leverage synergies in this area should also be explored.

Common Position 20

There should be no interference between surveillance systems designed for security and for the IAEA safeguards.

Common Position 21

Given the novelties of the SMR technology, there may be insufficient reliable data to inform Risk-Informed and Performance-Based Integrated Decision-Making (RIPB-DM) process. It is therefore recommended that, for the implementation of the integrated 3S approach, these limitations should be recognized.

Common Position 22

The use of a systems engineering process should aim to ensure that the areas of potential conflict between safety, security and safeguards are identified and resolved. Such a process provides a structured approach for identification of: (a) trade-offs in areas of potential conflict among the 3S, and (b) synergies between the 3S, i.e., complementary design approaches that optimize safety, security and safeguards.

Common Position 23

Significant 3S synergies are found in the design of structures, where the same structural design may provide safety protection against external and internal hazards, security protection against threats, and safeguard protection against unauthorized removal. In the plant layout, the 3S integration challenges generally relate to the preservation of human life via issues such as the effect of barriers and access control measures on the length of exit paths and number of emergency exits. Compact plant layouts influence the accommodation for reactor SSCs, including safety, security and safeguards systems and therefore, early consideration of the potential implications of a more compact plant

is recommended while also emphasizing the need to provide sufficient space to accommodate 3S SSC. Although a compact plant layout may be advantageous from a security response perspective, it may also be advantageous to an adversary as there may be fewer barriers to vital area access. This should be considered by developers.

Common Position 24

SMR designs need to consider and address any issues with the reliability, quality, and information security (confidentiality, integrity and availability) for any planned remote data transmission for the 3Ss and other purposes including operation. The possibility to leverage synergies among the 3Ss in this area should also be explored.

Common Position 25

SMR developers should include security and safeguards personnel as part of the design team to ensure that conflicts among the 3S are identified and resolved appropriately (3S approach).

Common Position 26

Regulators should be prepared to interface with all 3S stakeholders by having sufficient capacity and facilitating information sharing among the 3S disciplines.

Common Position 27

While it would not be realistic or necessary to change safety, security and safeguards assessment principles, the regulator should review higher-level guidance to regulation so to enable 3S approach. This internal regulator policy could in turn inform related training and other activities to build capability and capacity to regulate the SMR designs. International collaboration and lesson learning would also add value.

Common Position 28

Digital Instrumentation and Control (I&C) systems in SMRs should be designed to be resilient against the various cyber security threats. I&C systems and related digital components should be designed and operated in accordance with the concept of defence-in-depth against compromise. If digital twins were to include protection against compromise (cyber-attacks) in their design, they could improve both safety and security.

1. INTRODUCTION

There is sustained global interest in SMRs, which have the potential to enhance energy availability and security of supply by complementing other energy sources employed by IAEA Member States. SMRs usually have an electrical output up to 300 MW(e) and are factory-built as modules so to as minimize on-site construction and allow them to be shipped to utilities for installation as demand arises.

While the expansion of nuclear power will benefit energy security and the combating of global warming, the increase in the number of reactors could increase risks in terms of safety, security and safeguards and makes it imperative that regulatory requirements are met in all circumstances [1].

Various SMR designs encompassing advanced and novel technology are currently being developed and many are still in the design stage. This presents an opportunity for developers and regulators alike:

(a) to proactively reduce risks, by not only designing for safety but also for security (security-by-design, SeBD) and safeguards (safeguards-by-design, SBD), and

(b) to pursue a holistic approach to assessing risk to safety, security, and safeguards (known as 3S).

The "3S-by-design" should allow safety, security, safeguards, and their interactions to be considered from the earliest stages of the design development rather than, as previously, separately address security and safeguards after the conceptual design had been finalized.

The following stakeholders are important for the implementation of 3S:

- National governments with their own laws and regulations.
- National regulators with their own regulatory philosophies and approaches.
- Developers [1]of SMRs.
- Potential operators of SMRs.
- Existing or potential licensees of SMRs.
- The IAEA which provides standards that Member States adopt and use.

[1] The term "developers" is sometimes used interchangeably for designers and vendors, or, as here, as an umbrella term for both

2. KEY ASPECTS OF SMALL MODULAR REACTORS FOR 3S

Considerations of safety, security and safeguards are essential in the design, construction, commissioning, operation and decommissioning stages of NPPs. The considerations should be done in a coordinated, risk-informed, balanced manner, to take advantage of synergies[2] and to resolve potential conflicts. This is called 3S interface management.

The IAEA Nuclear Safety and Security Glossary [2] defines safety as "the protection of people and the environment against radiation risks, and the safety of facilities and activities that give rise to radiation risk". Regarding safety, there have been concerns about radioactive releases due to SSC failure or human error since the early days of the nuclear industry. As a result, the nuclear industry has benefited from a comprehensive and sophisticated safety regime, supported by the IAEA through its creation of safety standards and its provision of safety services such as Operational Safety Reviews (OSRs).

Unlike safety, nuclear security and safeguards have long been considered to be issues that were best addressed towards the end of the design process with details not being finalized until the facility was near complete. In part, this arises because installation of the final security arrangements is one of the last construction activities to be performed with safeguards and management of nuclear material only being needed once nuclear fuel has been brought onto site. For nuclear safeguards measures, further factors are their high level of standardization and their implementation being the responsibility of a third international party (the IAEA).

This approach is no longer adequate. In the case of nuclear security[3], rising concern, throughout the world, over terrorist and criminal elements (i.e., non-State actors) has highlighted the need to enhance security measures in nuclear facilities against malicious acts. For new facilities, this is best done by considering security in the early design stages so as to allow engineered security features and mitigation measures to be formulated to reduce reliance on human actions.

Safeguards[4], i.e. independent IAEA verification of non-proliferation, provides assurance to the international community that States are fulfilling their commitments concerning the peaceful use of nuclear energy and deters States, through the risk of early detection, from acquiring or using nuclear material, facilities and/or other items for proscribed purposes. While it is not possible to provide absolute assurances, the IAEA seeks to provide credible assurances to the international community that States are abiding by their safeguards obligations. These assurances are provided in the safeguards conclusions, which are reported annually in the Safeguards Implementation Report. The IAEA's safeguards approach for a facility is based on nuclear material accountancy as a safeguards measure of fundamental importance, complemented by containment and surveillance measures and monitoring. Under the safeguards agreements, each State is required to establish and maintain a State system of accounting for nuclear material (SSAC) under the agreement. The IAEA Safeguards Glossary

[2] Synergy means an interaction between two or more entities that produces a combined effect greater than the sum of their separate effects. That is not what happens in this case – a measure might, for example, improve both safety and security but the combined effect is not greater than the sum of the separate parts. A better word might be complementarities, but "synergy" is now in general use and we will retain it here.

[3] Defined by Ref. [2] as "the prevention and detection of, and response to, criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities or associated activities".

[4] Defined by Ref. [3] as "the technical means by which the IAEA verifies States' undertakings under their safeguards agreements and protocols thereto".

[3] defines SSAC as "a national system established under which the State authority responsible for safeguards implementation accounts for and controls nuclear material".

Safety, security and safeguards share the ultimate objective of protecting people, society, the environment and future generations from the harmful effects of ionizing radiation. Safety and security share the objective of avoiding radiological releases, whether accidental (safety) or caused by malicious actors (security). Security and safeguards share the objective of avoiding nuclear proliferation, either from State (safeguards) or non-State actors (security). The international regulatory community (as represented by the SMR Regulators' Forum) recognizes that the application of a process to enhance the integration of safety, security and safeguards into the design of SMRs as well as of other new commercial nuclear facilities has the potential to ensure that the ultimate objective is achieved. 3S interface management also has the potential to reduce the overall costs and better manage commercial risks associated with meeting regulatory requirements, while also reducing proliferation risks as the use of nuclear energy expands worldwide.

2.1. SAFETY BY DESIGN

IAEA recommendations relating to safety by design are presented in SSR-2/1 [4] and many supporting design safety guides.

As with any new reactor type, SMRs have the potential to achieve improvements in safety over existing NPPs[5] through simplicity of design and the incorporation of various inherent and passive safety characteristics which may complement or sometimes replace the active safety components used in other reactors. SMR designs bring forward opportunities to enhance, at the design stage, the robustness and independence of the Defence-in-Depth levels as well as resilience to different types of hazards. The objectives of safety by design of SMRs is to inherently eliminate or minimize potential accident initiators, and to mitigate/counteract the remaining initiators within the design limits, by simplified and reliable passive systems. Compared to previous power reactors, SMR features which may affect safety include, but are not limited to:

- Low nuclear material inventory, which depending on other aspects of the design, may lead to low residual heat and, in terms of releases of radioactivity, a smaller source term.
- Low core power capacity, which reduces overall cooling requirements and allows for a wide selection of sites, through a suitable optimization of the number of modules per site.
- Larger surface to volume ratio which facilitates easier decay heat removal particularly in single phase flow.
- The inherently compact design of SMRs which reduces the risk originating from certain external hazards. For example, the compact design is advantageous because of:
    - an increased resistance to earthquakes, and
    - a smaller cross-section which reduces the target size in a missile strike.

[5] Existing NPPs include GEN II & III

- The ability to use natural circulation for decay heat removal.
- The reduction and simplification of SSCs which reduces the number of common mode events.
- Depending on the design and the location, SMRs will often have smaller safety zones, exclusion zones, and emergency planning zones.
- The possibility, aided by flexibility in siting, of SMRs being used for purposes other than electricity generation alone. These could be production of industrial heat, district heating, desalination, energy storage, hydrogen generation etc. either as single products or combined with electricity production (cogeneration).
- Some SMRs are designed to be built partially or completely underground to enhance nuclear safety and security against external events and malevolent acts.
- In certain SMR designs, a large margin between the temperature of the coolant in all plant states and its boiling temperature results in system simplification and exclusion by design of all accidents caused by high pressure. In such designs, the selection of coolants with higher heat capacity along with higher boiling points leads to low fluid pumping requirements and energy transport at near constant temperature which enables designs with compact coolant and heat transport loops (small pipes, pumps, heat exchangers).
- In light water SMRs, In-Vessel Retention (IVR) of a molten core has a higher probability of success considering the lower decay heat and source term.
- In light water SMRs, the option of core control without soluble boron eliminates Reactivity Initiated Accidents (RIA) caused by dilution error.
- Gas-cooled SMRs using tristructural isotropic (TRISO) particles are claimed to fully retain fission products under all operating and accident conditions.
- SMRs using molten salt fuel are claimed to have inherent temperature stability because increases in temperature reduce reactivity by expelling liquid fuel from the core.
- Most SMRs have an average fuel campaign of 24 months, which is similar to that of advanced large reactor types. However, some types of SMRs allow for longer intervals between fuel changes. These include a sodium-cooled fast reactor design that has a core life of up to 30 years without refuelling. This results in a substantial reduction in the amount of spent fuel stored on site and the frequency and quantity of fresh fuel deliveries. In addition, some SMRs are designed to refuel by replacing the entire reactor vessel and the fuel within, which is different from large reactors that replace individual fuel assemblies. Such approaches may reduce the potential for accidents during fuel transfer/refuelling at the site and thereby reduce the risk of accidental releases of radioactivity to the environment. Reduced transportation of nuclear fuel may also reduce the risk of proliferation.

The above SMR safety features can be illustrated through the example of a water-cooled integral pressurized water reactor (i-PWR). In recent years, significant efforts were made

toward development of iPWR-type SMRs with the intention of realizing a number of key safety benefits:

- The placement, within the RPV, of all or most major primary circuit components eliminates the possibility of many large break, loss-of-coolant accidents and can reduce the potential for primary coolant levels falling below the top of the core (so-called "core uncovery"),
- Lower core thermal power,
- Large primary coolant inventory per MW(th) to provide a heat sink and promote natural circulation,
- Large secondary coolant inventory to facilitate passive decay heat removal and containment cooling,
- Taller RPV to facilitate decay heat removal via natural circulation, i.e., higher elevation difference between heat source and sink and increased coolant inventory,
- Internal control rod drive mechanisms to eliminate rod ejection accidents and reduce the number of RPV penetrations,
- Pipe penetrations that are small and generally positioned high on the RPV leading to an increased amount of water in the core after a hypothetical pipe break,
- Safety system can be powered purely by gravity and does not rely on pumps or motors,
- Control room location underground and in close proximity to the reactor building,
- Elimination of active containment post-accident systems (i.e., spray and fan coolers),
- Greater reliance on passive safety systems, and
- Smaller containment volume.

With these inherent and/or passive safety systems, the core damage frequency (CDF) for SMRs is claimed to be 100 times smaller than for large reactors.

2.2. SECURITY BY DESIGN

Security by design (SeBD) is an approach to the design of a nuclear facility in which nuclear security principles and provisions are brought into the design process as early as possible. IAEA recommendations related to SeBD are presented in IAEA Security Standards NSS-13 [5] and NSS 35-G [6], among other documents.

The principles and requirements for SeBD should be set out in the nuclear regulatory framework and regulations. The threat assessment or design basis threat (DBT[6]) and relevant nuclear security requirements should be provided to the SMR developer. Because of the sensitive nature and confidentiality of the DBT, competent authorities must take adequate provisions to protect the information. The SMR developer should then aim to remove or

[6] Defined in Ref. [2] as "the attributes and characteristics of potential insider and/or external adversaries, who might attempt unauthorized removal or sabotage".

mitigate the DBT and meet all applicable regulatory requirements for nuclear security during the design stage.

2.2.1. The Security by Design concept[7]

SeBD is a concept that incorporates security into all phases of facility design, construction, operations, and decommissioning. According to the Bureau of International Security and Non-proliferation [7], successful "security by design" results in a more robust physical security infrastructure that:

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

In 2014, Snell and Jaeger conducted research on SeBD for both planned and operational nuclear facilities on the behalf of the Sandia National Laboratories [8]. For nuclear facilities, the authors contend that, when SeBD is adequately implemented, the physical protection system is more robust to future changes in requirements over the lifecycle of the facility and more effective against malicious acts. An interesting point is the need to anticipate future changes in the DBTs and Threat Assessments, as well as potential changes in requirements that may occur during the lifecycle of a nuclear facility. Table 1 provides examples of how SMR design could anticipate heightened or new threats with appropriate countermeasures.

[7] SeBD concept has been described comprehensively by Duguay in [9] and is reproduced in this section

Table 1: How SMR designs could integrate threat information in countermeasures (Source: Threat Capabilities That Might Change over Time and Possible Countermeasures [10])

Topic	Possible Countermeasures
Hypothetical changes in capabilities to any threat attempting to commit	
• Sabotage	Reduce number of vital areas subject to sabotage, build on safety concepts such as inherently safe designs, and locate them so that they are easier to protect.
• Theft	Reduce the number and inventory of Inner Areas with Category I material, and locate them to so that they are easier to protect.
Hypothetical changes to External Threats	
• Better attack vehicles	Room for more standoff and improved and possibly more vehicle barriers; early detection capabilities against unauthorized vehicles
• Lighter and/or more capable tools and more capable explosive attacks	Provide thicker walls, allow room for more doors and/or activated delays, and design "nested" security layers, with no common walls across multiple layers
• Better weapons and/or weapons training	More capable weapons and training as well as use of fighting positions with overlapping fields of fire, hardened facility post and hardened response vehicles for more survivability
• More adversaries and/or better tactics	Allow for a larger protective force and/or better tactical training
• Increased frequency of or capability of unarmed antinuclear activists	Improved site features and security plans, as well as regulatory changes, to make it easier for guards to prevent the entry of and to arrest such activists
• Cyber-attack capabilities	Better cyber protection, both for control systems and critical security systems
Hypothetical Changes to Internal Threats	
• More active and or violent insider adversaries; or multiple insiders	Compartmentalize layout and limit those with access, authority, and knowledge of security systems and targets. Track human and material movement.
• Cyber-attack capabilities	Better cyber protection, both for control systems and critical security systems

Snell and Jaeger also present the assumptions, observations, and conclusions from the *Security-by-Design Handbook* [10] developed by the USA National Nuclear Security Administration (NNSA) and the Japan Atomic Energy Agency. This manual identifies SeBD best practices and principles. The Handbook also describes three effective strategies, including:

1. Using integrated design teams with experience in safety, safeguards, operations, and sustainability/reliability,
2. Using a risk-informed design methodology, and
3. Considering the complete facility lifecycle.

Based on their literature review, the authors argue that there is no need to "reinvent the wheel" for SeBD applications for operational nuclear facilities or planned future SMRs. The SeBD handbook highlights the key security principles that designers and regulators can integrate in their programs. Figure 1 summarizes some of the key factors and how they relate to the concept of SeBD.

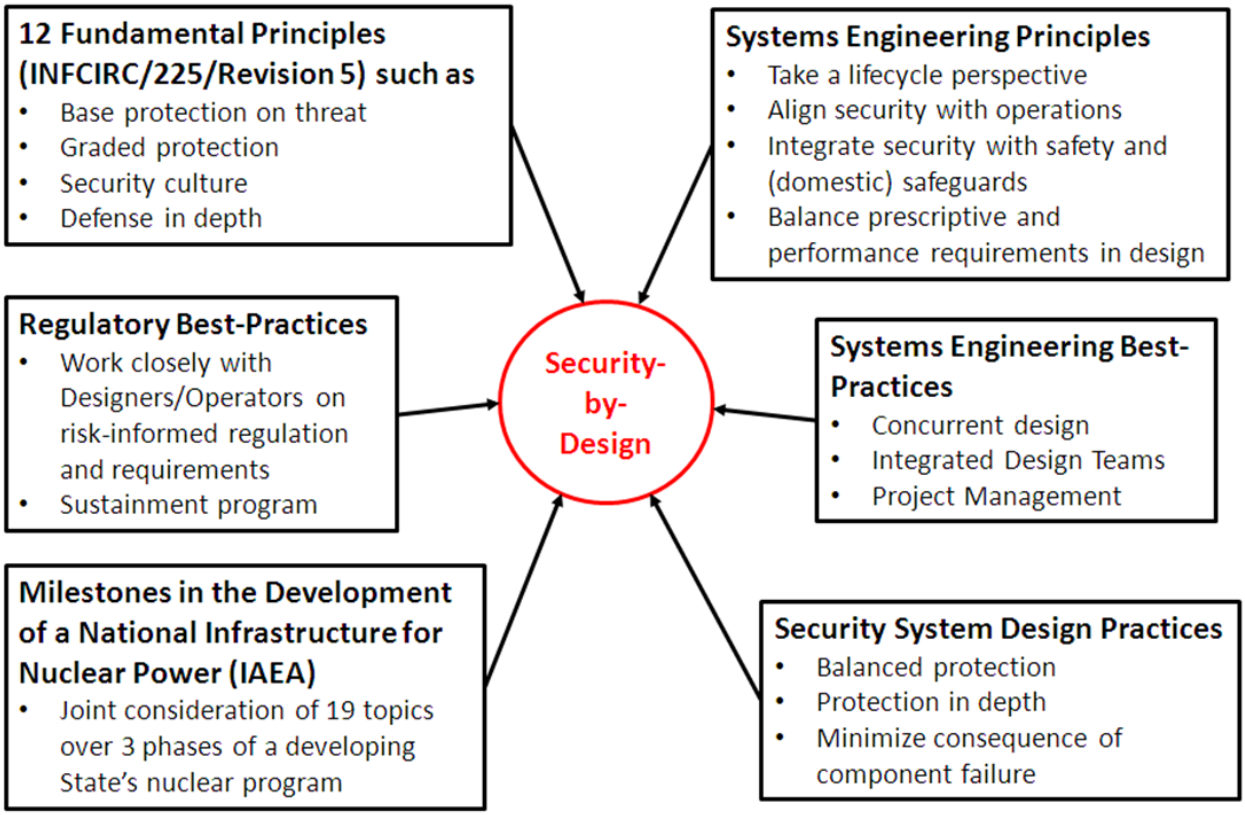


Figure 1:Key factors and how they relate to the concept of SeBD (Source: Contributing Factors from the Sandia National Laboratories SeBD Handbook [10])

According to World Institute of Nuclear Security (WINS) 2019 Best Practice Guide on SeBD [11], SeBD is also a risk-informed approach that requires multi-disciplinary teamwork and a clear security strategy. SeBD is a concept that is sometime referred to as "intrinsic security", meaning that it is permanent, inseparable, or built in. Implementing SeBD can reduce the risk of major security incident and associated costs.

2.2.2. SeBD application to SMRs

Compared to large nuclear reactors, SMRs have many novel aspects which may have security implications as well as safety implications and may necessitate changes to the approach to nuclear security. Foremost, the regulator and operator/developer need to understand the risks inherent in the design – regardless of the design maturity – and think in terms of an SeBD approach. With potentially new developers entering into the civil nuclear market, they may seek innovative ways to think and manage risk. They may also wish to exploit the safety benefits of new reactors claiming security advantages and hence seek commercial gain. This

will need to be justified to regulators and argued with evidence. SeBD as an approach, seeks to understand the risks inherent in design and reduce them by changes to that design or address residual risks by designing in a security regime. For SMRs, security begins to reflect the approach taken in safety risk management. Aspects of SMR designs that affect security risk and may present opportunities to rethink a security regime, include:

- Potentially different security risks because of the nature of new fuels (accessibility and size of the nuclear inventory, fuel elements, and the core) and frequency of re-fueling,
- Potentially lower security risks due to intrinsic safety which could prevent a significant offsite release,
- Potentially different insider risks and cyber risks due to autonomous operation and remote monitoring,
- Potentially different security risks with the increased dependency on off-site response forces,
- Potentially different security risks because of the SMRs' compact designs. If all targets and safety features are gathered in a small area and can be destroyed at the same time, the added value of nuclear security for safety features will be significantly reduced,
- Structural design may or may not lower security risks as compared to the traditional one, depending on the technology,
- Underground construction will reduce certain risks (e.g., from aircraft crash) but may create others (e.g., flooding),
- Multiple unit sites increase the nuclear inventory and thereby the security risk, but shared services may have positive implications for both safety and security,
- Remote sites and mobile units may present challenges for adequate and timely off-site response, and
- Supply chain risks may be increased (insider threat vectors).

As previously mentioned, developers may argue that for their SMRs, lower security risks would lead to fewer protective security measures. Such claims should be justified to regulators by demonstrating that security objectives are met, by assessing the security risk quantitatively or qualitatively. Regulators should expect licensees/developers to:

1. identify security requirements (i.e. facility characterization, target identification, threats, regulatory requirements) and quantify risks (e.g., unacceptable radiological consequences from sabotage or unauthorized removal),
2. see what risks might be designed out or reduced by the unique design and operation (e.g., below grade construction, fuel material, passive design, etc.) and design security system including detection, delay and response measures, and
3. evaluate security system (i.e., performance testing, path analysis, scenario analysis) and identify and quantify any residual risks and how these risks will be mitigated.

For example, as conceptualized in bullet 2 above, identification of sabotage targets and vital areas during the design stage of a nuclear facility provides the opportunity to reduce the number of sabotage targets and the size of vital areas, and allows the implementation of a more cost-effective nuclear security system. By locating non-critical SSCs out of vital areas, the SMR developer can reduce the number of personnel access points to vital areas. In addition, safety measures can be designed to make it more difficult for an adversary to defeat their mitigation capabilities (for example, by placing redundant safety critical SSCs in different vital areas).

IAEA guidance on security contained in NSS 20 on Nuclear Security Fundamentals [12], NSS 13 on Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities [4], NSS 27-G on Physical Protection of Nuclear Material and Nuclear Facilities [13], NSS 35-G on Security during Lifetime of a nuclear facility [6], NSS 42-G on Computer Security for Nuclear Security [14] and the methodologies offered in these guides, are applicable to SMRs. Hence, using these methodologies for assessing risks to inform a new design or design modification remains relevant good practice.

It is essential to design nuclear security systems holistically, by integrating physical security and information security, including cyber security, into an effective system. As cyber threats evolve rapidly, and the use of programmable digital systems increases, integrated design of physical and information security, including cyber security, is important to achieve robustness of the nuclear security system.

2.3. SAFEGUARDS BY DESIGN

2.3.1. Early engagement

Safeguards by design (SBD) is the integration of safeguards considerations into the design process for new or existing facilities from initial planning through the design, construction, operation, waste management and decommissioning phases. Waiting to consider safeguards measures until the design is finalized and then retrofitting can increase costs and extend schedules. Stakeholders should therefore discuss an optimal combination of safeguards measures early in the design process in order to reduce the need for inspections and to facilitate either the installation of IAEA equipment or the joint-use of operator equipment. Engagement between stakeholders on SBD is typically an iterative process, whereby the facility's structures, systems and components, and the proposed safeguards measures are considered and adapted as the design matures. While the developer is responsible for the design, the IAEA is responsible for the development of an appropriate safeguards approach. The goal is to meet the State's legal safeguards obligations (prescribed in its safeguards agreement with the IAEA), and to configure those measures so that they acknowledge the constraints of the design.

While the SBD concept is not new, some SMR developers are not familiar with detailed safeguards requirements, with their focus on safety and to a lesser extent, security. Often the application of safeguards has been seen as a requirement on the operator and IAEA, not the developer. Ultimately, however, the safeguards measures have to be integrated with both the facility operation and its design. This lack of general awareness can also create further design conflicts when developers export technology to a State with a different set of safeguards requirements (for example from a State with a Voluntary Offer Agreement in force versus one with a Comprehensive Safeguards Agreement).

An additional benefit to SBD is the promotion of optional early engagement between the developer and the operator, the operator and the State, and the State and the IAEA on safeguards requirements and expectations for the proposed design. Early engagement between stakeholders on safeguards requirements and expectations can help facilitate their effective and efficient implementation, and prevent issues from arising later in the facility's lifecycle, as pointed out in "Safeguards by design (SBD) for Small Modular Reactors" [15]. Throughout the process, clear communication and awareness amongst the stakeholders plays a critical role in establishing a common understanding of the elements required to meet the State's international legal obligations. Further, the introduction of new types of facilities and the associated research and development that supports them may have State-level impacts in that the application of safeguards at other facilities may need to be changed.

The application of SBD is a voluntary undertaking by the State. The concept does not introduce any new requirements or obligations on the State. For new facilities in States with a comprehensive safeguards agreement (CSA) with the IAEA based on INFCIRC/153 (Corrected) [16], the Subsidiary Arrangements only require the "provision of preliminary design information for new facilities as soon as the decision to construct or to authorize construction has been taken whichever is earlier". For States with an Additional Protocol based on INFCIRC/540 (Corrected) [17] to their CSA in force, the State is further required to submit an annual declaration of the "general plans for the succeeding ten-year period relevant to the development of the nuclear fuel cycle (including planned nuclear fuel cycle-related research and development activities) when approved by the appropriate authorities…". This may increase the IAEA's awareness of proposed facilities and new technologies, but it does not require engagement on the application of safeguards.

During the period of development of a new facility design – prior to the CSA-required submission of preliminary design information to the IAEA – a State may voluntarily discuss the safeguards implications of its design information with the IAEA. While not legally required, SBD can be regarded as a best practice, and as a means of improving the effectiveness and efficiency of safeguards. Benefits to stakeholders include improvements in the ability of developers and operators to understand safeguards requirements and expectations from the IAEA and the State.

2.3.2. Safeguard challenges

Many of the advanced and novel SMR designs being proposed by developers raise safeguards challenges, including those related to new fuel types, reactor designs, supply arrangements, spent-fuel management, operational roles and deployment options. While existing safeguards approaches, techniques, equipment and measures may be available to address some of these challenges, the combination of multiple challenges in a single design may present new and complex safeguards issues. In cases where there is no existing experience to draw from, stakeholders will require time to collaboratively develop a solution. Early engagement to identify appropriate stakeholders, develop communication channels, and establish clear requirements and expectations will help enable the development of an effective and efficient safeguards approach for the novel technology.

SMRs can be expected to have the following characteristics that could affect the implementation of safeguards, as outlined in Section 5.1 "Modular reactors" of NP-T-2.9 [18]:

- Low thermal signature – challenging to use satellite or other forms of remote sensing to verify operation,
- Coolant – use of coolants other than water such as lead-bismuth or sodium does not allow for traditional optical viewing of the fuel in the core or in the spent fuel storage,
- Number of units per site – the larger the number of units, the greater the need for refuelling and number of discharges per calendar year,
- Long-life reactor core (sealed vessel) – misuse of the facility and diversion of spent fuel becomes more difficult to detect,
- Advanced fuel cycle – significant analysis will be required to understand the most effective and efficient safeguards approach for the Gas-cooled Fast Reactor (GFR), Lead-cooled Fast Reactor (LFR), MSR, Supercritical Water-cooled Reactor (SCWR), Sodium-cooled Fast Reactor (SFR) and Very High Temperature Reactor (VHTR),
- Enrichment – if a design requires uranium fuel enriched to close to 20% (HALEU), this will involve modified safeguards measures from those customarily applied to LEU-fuelled reactors; above 20%, direct-use nuclear material is involved which will require increased safeguards activities,
- Surplus reactivity – a core with surplus reactivity might tolerate target irradiation without affecting those key operational parameters that can be monitored,
- Fuel-element size – small size tends to facilitate item concealment, and
- Spent-fuel storage geometry – smaller fuel elements would possibly need to be stored vertically for cooling purposes, with a strong economic incentive to stack fuel and reduce the storage footprint. This could present a challenge to current safeguards inspection activities owing to lack of direct-line visibility of fuel elements from above.

In addition to the above characteristics, some SMR designs (e.g., molten salt/molten fuel SMRs) may incorporate the on-site chemical separation of fuel as part of the reactor operations. This adds safeguards considerations for the material streams from this process (fuel returned to the reactor and the mixed waste). Also, manufacture and fuelling of an SMR in one country for operation in another country may pose safeguards implementation challenges if the two countries are under different types of safeguards agreements with IAEA (for example from a State with a Voluntary Offer Agreement in force versus one with a Comprehensive Safeguards Agreement).

As the international organization responsible for the verification of a State's obligations on the peaceful uses of nuclear energy, the IAEA provides various resources to promote the implementation of the concept of SBD. Through its Member State Support Programme (MSSP), the IAEA has undertaken a task on "Safeguards-by-design for SMRs" with several Member States. The task aims to identify the key technical challenges for safeguards implementation involving SMRs, and the steps that can be taken to support incorporating SBD principles into the designs. Further, the IAEA supports the efforts of the SMR Regulators' Forum and raises awareness of various safeguards concepts, including SBD, with stakeholders at various international and regional fora.

3. COMMON POSITIONS: INTERFACES AMONG SAFETY, SECURITY, SAFEGUARDS

In addressing its allocated topic, the DSA WG came to agreements on various issues relevant to 3S integration and the introduction of SMRs. Where these differ from well-known existing approaches, they are highlighted here as "common positions".

Standard practice with existing NPPs has been to consider safety, security and safeguards as separate entities. The move toward smaller and more operationally agile SMRs highlights a need to re-evaluate this traditional approach. Historically, many security and safeguards features for nuclear facilities have been retrofitted. Such practice, often performed without attention to optimization, has led to inefficiencies, cost overruns and an increased burden on operations staff. An integrated 3S approach, by considering security and safeguards alongside safety during the early design development of the facility, is intended to decrease demand on resources for the implementation and operation of security and safeguards measures throughout the facility's life cycle.

A 3S interface is any decision point where nuclear safety, security and safeguards need to be considered. Often a measure implemented on behalf of one discipline (e.g., safety) may complement one or both of the other disciplines so that, for example a thick-walled containment building may benefit both safety and security. Sometimes, however, there may be conflicts as when, say, security requires critical safety equipment to be protected from tampering but that makes urgent operator action more difficult. Conceptually, conflicts may occur because of different "opponents" in that safety measures are designed against unintentional events, while security and safeguards measures are designed to deal with active adversaries, who may adapt their actions based on their knowledge of the defences. This is particularly acute when one considers insider security threats or the fact that, for safeguards, the adversary is the operator and State. Interface management is a systematic way to recognise the decision points, to take advantage of the synergies and to resolve the conflicts to achieve the joint fundamental objective of protecting people and the environment from the harmful effects of ionizing radiation [19].

Several SMR characteristics may result in enhanced interfaces between safety, security and safeguards, and require extra consideration from the point of view of each of the individual S's as well as the 3S. Table 2 presents such characteristics, where NAR stands for novel advanced reactor, but the characteristics are applicable to SMRs as well. Many of them are discussed in subsequent sections.

Table 2: Matters to be considered in the context of 3S for SMRs [19]

NAR and nuclear security	NAR and nuclear safeguards	NAR and nuclear safety
Security measures are risk-informed, based on potential consequences and threat assessment: What are the potential consequences? How are the classified requirements managed in design and evaluation?	Design information, safeguards by design	Application of defence in depth principle (DiD)
New types of facilities, fuels, transports: Definition of assets and protection objectives	Identifying technical objectives focused on enabling the IAEA to detect any diversion of declared nuclear material, and undeclared production or processing of such material	New applications (process heat, district heating, hydrogen production…)
New types of operators: Assignment of responsibilities	Designing NAR to be more proliferation resistant or more safeguardable	New operating concepts (decreasing role of personnel in facilities with high degree of passive systems and automated operations, remote operation, long grace-times, walk-away safety…)
New types of locations (remote, urban, marine, mobile): Remote operations, regular oversight	Effective use of technical inspection methodology R&D needs? Joint use of technology	New kind of locations (remote, urban, marine, mobile...)
Response: Coordination and planning with relevant authorities, role of operators	New types of locations, numerous facilities: Reducing inspection effort per facility is a must	Size of emergency planning zone (EPZ)
	Remote monitoring, remote inspections: Inspection rights	New kind of business models, emergence of operators and vendors with less experience than the traditional ones have
	Additional Protocol importance (legal framework)	Difficulties in performing inspections in integrated concepts after assembly

3.1. SAFETY AND SECURITY INTERFACES

According to Gandhi and Kang [20], design concepts traditionally applied to nuclear safety such as defence-in-depth, single failure criteria, redundancy and diversity, fail safe criteria, and passive systems are also applicable to nuclear security design as well. These safety designs and systems can potentially reinforce protection against malicious acts. Application of these concepts to nuclear security means that would-be perpetrators of nuclear sabotage must compromise several layers of protection in order to cause radiological release.

3.1.1. Passive/inherent safety

Developers claim that passive safety will prevent significant offsite releases resulting from nuclear security events.

Common Position 1

> Claims made by developers that passive safety measures would reduce security risks need to be justified through the security risk assessment.

3.1.2. Use of the insights from safety analysis to inform security

Safety analysis has a direct influence on security in that the identification of potential sabotage targets that need protection are informed by the safety analysis and the nuclear safety case ([21], [22]). Facility operators should identify SSCs, associated operator actions or nuclear or other radioactive material, which, if sabotaged, could directly or indirectly lead to unacceptable radiological consequences (URC). These SSCs, associated operator actions and nuclear material should then be identified as potential sabotage targets and protected accordingly. The URC is a level of radiological consequences, established by the State, above which the implementation of nuclear security measures is warranted.

In the process of identification of potential sabotage targets and vital areas, security looks at Initiating Events of Malicious Origin (IEMOs). An IEMO is defined as an initiating event that is deliberately caused by an adversary in an attempt to sabotage a facility. A review of Postulated Initiating Events (PIEs), accident scenarios and event sequencies, developed for the safety analysis, is examined to identify potential IEMOs, but they are not the only source for potential IEMOs. Identification of these other sources requires consideration of the capability of the adversary to perform sabotage acts. In some cases, due to classification of documents and secrecy surrounding DBTs, this analysis may be carried out using a more generic threat capability which then allows wider participation in workshops etc. without compromising national security.

Informed by the safety analysis, the SSCs that prevent the potential IEMOs from developing into an accident sequence leading to the loss of a fundamental safety function (to control, cool, contain) are then identified. Similarly, the SSCs that mitigate the consequences following the loss of the fundamental safety function are also identified. The potential IEMO, and the associated protective and mitigating SSCs, create a potential Sabotage Event Scenario (SES). This is because, should the adversary successfully initiate the IEMO and compromise the related protective and mitigating SSCs, then the IEMO will develop into an accident sequence potentially leading to URC and high radiological consequence (HRC).

The SSCs associated with the potential SESs become the sabotage targets that would be candidates for protection in vital areas which are defined as “area[s] inside a protected area containing equipment, systems or devices, or nuclear material, the sabotage of which could directly or indirectly lead to high radiological consequence” in the IAEA Safety and Security Glossary [2].

The process for identification of potential sabotage targets and vital areas provides an early opportunity for SeBD. To be valuable, this integrated work needs to be carried out early in the design development.

3.1.3. Safety Assessment

Safety assessment provides necessary inputs to the design of NPP (and SMR) security systems. Specifically, it is used to identify the SSCs that come into play in postulated accident scenarios and thereby helps in the identification of vital areas and targets by determining the vulnerabilities of the reactor and its systems and its robustness against DBTs.

PSA is a category of safety assessment that is widely used in the nuclear industry to estimate frequencies of undesirable consequences (such as core damage states and radioactive release categories) and to obtain risk profiles of nuclear facilities for further risk-informed decision making. The classical PSA approach is to estimate the frequency of accidents and analyze the accident sequence using event trees and fault trees. This information could be directly utilized for VAI. A parallel probabilistic approach has been used for developing guidelines for protection of nuclear power plants against sabotage. Because of the difficulty of estimating the frequency of a terrorist attack, however, the probability of such an event is set at unity. This approach is then used to evaluate the consequences of the attack (i.e., potential development of the accident scenarios as a results of the attack) based on the PSA models (e.g., event trees) and by calculating the conditional risk metrics (e.g., conditional core damage probability in case of the postulated malicious act). This application allows one to obtain the entire spectrum of potential accident scenarios triggered by the malicious act, rank them based on the risk, and use this information for the decision making to strengthen nuclear security measures.

Common Position 2

> Licensees are recommended to use insights from safety assessment to inform nuclear security. Probabilistic techniques can draw on PSA and be useful for VAI, sabotage target identification, vulnerability assessments etc.

3.1.4. Operating principles

Zakariya and Kahn [23] identified operating principles as an area in which synergy between safety and security could be maximized: “Coordination is needed in developing operating procedures, especially when conflicts are unavoidable; the matter should be resolved based on the philosophy of minimizing the overall risk to the public [24]. Coordination is necessary so that compensatory measures do not undermine the necessary balance between safety and security (e.g., compromising security surveillance systems during maintenance operation should be avoided). However, verifying the status of the facility on periodical basis is necessary, which may either result in the need for modernization or refurbishment, updating of procedures and documents, and revision of the safety and security analysis. Similarly, in access control measures for sensitive areas in the facility, consideration should be given for the requirements for safety and security. While facilitated access is needed for emergency teams, it may be controlled for security purposes. Some areas within the reactor facility may be subjected to special security systems and it should be possible to be accessed for evacuation of personnel in case of emergency. Likewise, safety procedures in some cases may slow down transport of materials, while the duration of transport should be minimized for security purposes”.

Common Position 3

Potential conflicts between safety and security measures should be identified and minimized during the design stage. Potential synergies should be leveraged.

Common Position 4

When developing operating principles and procedures, licensees should account for both safety and security risks. Licensees should ensure that potential adverse and beneficial effects from implementation of changes (such as refurbishments, safety and security analyses changes, changes of operating principles and procedures) are considered for both safety and security measures to ensure these are addressed prior to their implementation. In other words, the facility change evaluation process should consider both safety and security measures to eliminate potential conflicts.

3.1.5. Emergency preparedness

One of the areas where there may be different approaches between nuclear safety and nuclear security is in command and control in response to emergencies. This is an area that needs extensive coordination, particularly for considerations such as who makes the decisions and how the responsibilities are allocated.

Common Position 5

Licensees are recommended to coordinate safety and security procedures, emergency response plans and security response plans, as part of emergency preparedness and response to security events. For SMRs, this may be especially challenging due to potential remote operation, siting and other aspects. Potential conflicts between safety and security measures should be identified and minimized when developing emergency preparedness procedures.

3.1.6. Cogeneration

The idea behind cogeneration is to use SMRs to generate electrical energy and another valuable product. For example, SMR thermal power could be converted into electricity and delivered to the grid during the high load/high price hours (usually daytime), while during hours of low demand/low price (usually night-time), thermal energy might be used to produce hydrogen. Cogeneration introduces risks from the nearby industrial process that could impact the SMR, if there was a fire or explosion for example. Further, the presence of an associated industrial facility presents another target for malefactors. It follows that the safety analysis, security arrangements and emergency preparedness need to factor in the risks arising from cogeneration.

Common Position 6

When assessing risks and preparing for emergencies and malicious acts, licensees/developers should factor in 3S interfaces and combined risks where applicable and reasonable. This is especially important for novel applications such as cogeneration.

3.2.SAFETY AND SAFEGUARDS INTERFACES

Safety-safeguards interfaces have recently been discussed by Kovacic and Renda [25] as follows: "Many safety and safeguards interfaces occur during the operation of nuclear facilities. These normally involve access controls to areas of the facility and equipment due to high radiation fields or other safety and occupational hazards. During the design phase, the main drivers for designers are the economic and safe operation of the AR and so the challenge for them is to understand how the application of the IAEA safeguards should be considered during this early phase."

3.2.1. Failure of safeguards and safety components

Failure of safeguards and safety components is identified in Ref. [25] as one of the safety-safeguards interfaces: "Designs that accommodate IAEA equipment should ensure that the failure of a safeguards component will not impact the safety of the plant. One such example is the design provisions for the placement of an IAEA safeguards equipment cabinet that may have a structural failure during a seismic event and impinge on a safety-related component."

Common Position 7

> SMR design process should reconcile measures in place to meet both, the IAEA safeguards arrangements, and the safety of the plant to ensure that they do not have adverse impacts on each other.

3.2.2. Physical facility layout

As Kovacic and Renda explained in Ref. [25]: "Facility design should ensure that IAEA inspectors have access to equipment and material to perform independent on-site verification/inspection activities. If areas of the facility will be off-limits or otherwise inaccessible to personnel during operation because of safety concerns, design considerations should be implemented that would allow the IAEA to use other means to accomplish its goals."

Common Position 8

> SMR design may be compact, or complex compared to existing NPPs. Therefore, it is important that designers facilitate other means to accomplish safeguards activities if areas of the facility will be inaccessible to IAEA personnel during operation because of safety concerns. The exception to this is for temporary issues. For any kind of temporary issue, the licensee should proactively engage with the IAEA, or their regulator, as appropriate.

Common Position 9

> Licensees/developers should approach the IAEA in the early stages of the SMR development to ensure that IAEA safeguards can properly be implemented. Existing IAEA safeguards measures may be applicable to SMRs. If not, new IAEA safeguards approaches, measures and techniques need to be developed by the IAEA. Licensees/developers should be aware of the importance of physical facility layout and its potential constraints. Retrofitting to accommodate safeguards should be avoided so as to prevent negative impacts on safety and/or security.

3.2.3. Containerization

Designs for placing nuclear material into containers for safe handling and transport should always consider whether the containers will be accessible to the IAEA for safeguards verification and the ease with which IAEA seals can be applied.

Common Position 10

> The novelty associated with SMR fuel designs may introduce new types of containers for transport. SMR safety designs should accommodate IAEA safeguards measures for containers and transport.

3.2.4. Failed fuel

Failed fuel is a significant operational and safety concern and should be kept to a minimum. Safety designs should consider how the IAEA would be able to independently verify the amount of material lost from failed fuel and the resulting material balance. Dose rates should be minimized in the areas that need to be accessed by the IAEA and the operating personnel.

Common Position 11

> SMR design should accommodate material accounting in the event of failed fuel and any retrieval of failed fuel.

3.2.5. Fissionable material tracking in SMRs

In various SMR technologies, the design should accommodate for the movement of fissionable material which may not feature in standard large LWR designs. For example, in MSR, the interaction of fuel salt with the plant SSCs can result in the plating of nuclear material to the internal structures of the reactor.

Common Position 12

> For MSRs where there is plating of radioactive material, the operator will need to account for nuclear material by tracking the movement of the material under all normal and off-normal operating conditions and the IAEA will have to verify the operator's information. This includes maintenance activities. The operator's instrumentation for tracking fuel movement should not have a negative impact on the same type of instrumentation used for safeguards purposes, and vice versa. If during regular operation and/or transients, molten salt including fuel needs to be drained, the designer and licensee should accommodate the IAEA's requirements for verification in all SSCs. The possibility to leverage synergies in this area should also be explored.

3.2.6. Off-normal events

Kovacic and Renda explained the safety-safeguards interface during off-normal events in [25]: "The IAEA must be able to perform its independent verification activities under all operational circumstances, up to and including the design basis accident. Therefore, design considerations that would allow the IAEA to maintain its safeguards systems even during off-normal events would be beneficial".

Common Position 13

The design should aim to allow the IAEA to maintain its safeguards systems even during off-normal events (for example - transients).

3.2.7. Criticality control

As explained in Ref. [25]: "The quantity and configuration of nuclear material outside of the reactor system as fresh or used fuel may be limited by criticality concerns. Designs should consider that any containers and other configurations and amounts must always be under IAEA safeguards. This requirement also has a direct interface with nuclear material accounting, where the quantity of nuclear materials should be known at specific area in the facility at all times."

Common Position 14

With the nature of SMR fuel types, considering the potential for increased enrichment compared to the existing NPPs, the design process needs to ensure criticality safety. The configuration of nuclear material storage and movement outside the SMR needs to consider a safety aspect of criticality control and accommodate IAEA safeguards verification.

Common Position 15

If during regular operation and/or transients, fissile material needs to be drained (e.g., MSR), the design and licensee should accommodate the IAEA's requirements for verification.

3.2.8. In-Vessel Retention (IVR)

In SMRs, the feasibility of the IVR of the molten core may have a higher probability of success than in large water reactors considering the lower decay heat and source term.

Common Position 16

When applicable, SMR design process should strive to achieve in-vessel retention, which benefits both safety and safeguards, under severe accidents.

3.3.SECURITY AND SAFEGUARDS INTERFACES

Security and safeguards share certain functions at the facility level. The following interfaces previously identified by Kovacic and Renda [25] should be considered:

3.3.1. Nuclear Material Accounting and Control (NMAC)

The IAEA Safety and Security Glossary [2] defines the system for NMAC as: "an integrated set of measures designed to provide information on, control of and assurance of the presence of nuclear material, including those systems necessary to establish and track nuclear material inventories, control access to and detect loss or diversion of nuclear material, and ensure the integrity of those systems and measures". The NMAC system helps to deter and detect

unauthorized removal of nuclear material by maintaining an inventory of all nuclear material, including information related to its location. Domestically, the NMAC system is required for licensing, operations, and security and is developed in accordance with requirements established by the State authority. A graded approach may be taken in designing the NMAC system for application to nuclear security to ensure that the selected measures are proportionate to the potential consequences of unauthorized removal of nuclear material. The performance of the NMAC system should address situations where nuclear material is both stolen in a single event (abrupt theft) and situations where nuclear material is acquired in small amounts during several events (protracted theft).

NMAC is shared between national nuclear security and international safeguards. Although this interface mostly affects facility operations, certain design features could influence how effectively or efficiently the IAEA can perform independent verification of nuclear material quantities at the facility.

Common Position 17

> The NMAC system for SMRs should be designed to meet all legal obligations associated with a safeguards agreement, as well as the nuclear security objectives. The possibility to leverage synergies in this area should also be explored.

3.3.2. Access controls

The physical layout and access controls for a facility affect both safeguards and security. Designs should consider not only the need to control access for reasons of security, but also the need for access to allow IAEA safeguards verification. For example, some areas of the facility, equipment, and material that are protected for security reasons and not normally accessed, may need to be made available to IAEA inspectors; alternatively, some other means of verification will need to be provided so that safeguards activities can be performed. Another example is access controls during potential nuclear security events. If there are any security design features that would limit access for IAEA safeguards verification, provisions should be made for independent verification by other means.

Common Position 18

> SMR design may be more compact and/or complex compared to existing NPPs, leading to additional security considerations. Therefore, it is important that the SMR designs facilitate IAEA access or other means for independent safeguards verification activities in their security plans.

3.3.3. Remote data transmission

Any design features or provisions that prevent the transmission of data from the facility should be reconciled with the potential need for the IAEA to receive such data remotely.

Common Position 19

> Given recent technology changes and increased cyber security risks and awareness, SMR designs can address cyber security issues in the design. Remote data transmission for safeguards should not compromise the cyber security and should meet standards

prescribed by the IAEA. The possibility to leverage synergies in this area should also be explored.

3.3.4. Surveillance systems

Surveillance systems that are designed for domestic security will not be used for IAEA safeguards. Therefore, consideration should be given by the designer for locations in the facility that could support both domestic and (independent) international surveillance systems and that ensure the two do not interfere with each other.

Common Position 20

There should be no interference between surveillance systems designed for security and for the IAEA safeguards.

3.4. SAFETY, SECURITY AND SAFEGUARDS INTERFACES

Identification of safety, security and safeguards interfaces is essential for the implementation of the 3S concept. Such interfaces can be synergistic, neutral, and potentially conflicting. Safety, security, and safeguards measures which contribute to all three regimes and complement one another are considered to be synergistic. In Figure 2 below, the synergetic interfaces are shown in bold, blue font. As explained in previous sections, there is also potential for neutral measures and conflicting measures, shown in Figure 2 in normal black and italic red fonts, respectively. One goal of managing the 3S interfaces is to take advantage of the synergies and resolve the possible conflicts.

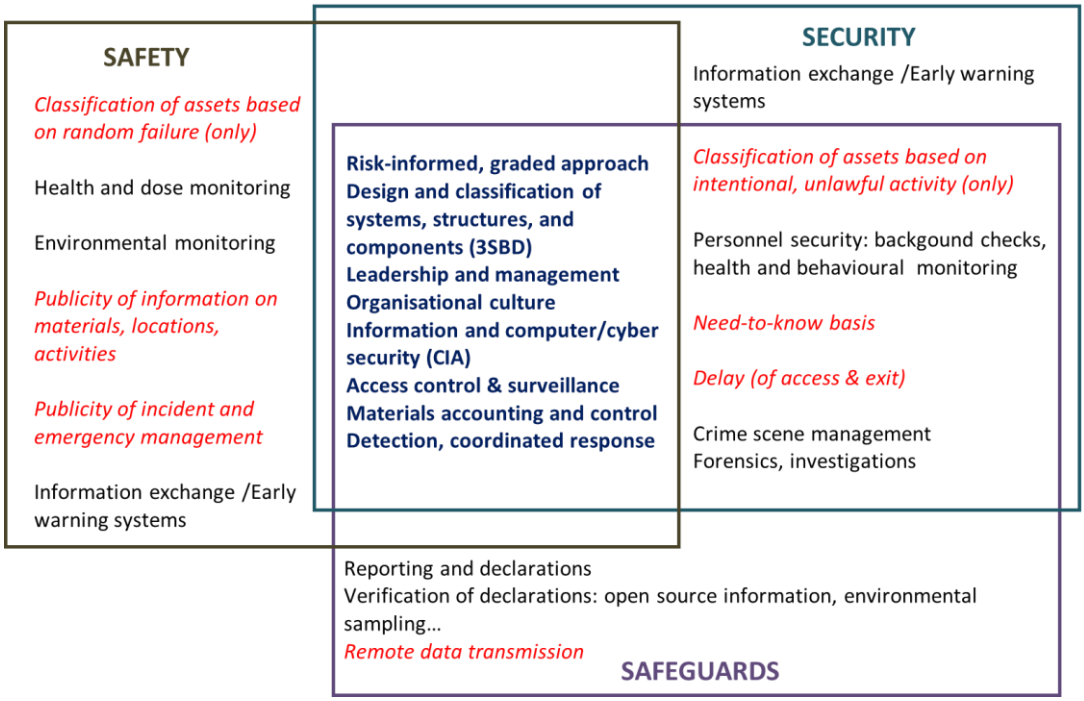


Figure 2: Examples of synergistic (blue, bold font), neutral (normal font) and potentially conflicting (red, italic font) measures in nuclear safety, security, and safeguards (3S) [19]

3.4.1. Risk-Informed and Performance-Based Integrated Decision-Making process (RIPB-DM)

RIPB-DM is defined by the US NRC as:

An approach in which risk insights, engineering analysis and judgment including the principle of defense-in-depth and the incorporation of safety margins, and performance history are used, to (1) focus attention on the most important activities, (2) establish objective criteria for evaluating performance, (3) develop measurable or calculable parameters for monitoring system and licensee performance, (4) provide flexibility to determine how to meet the established performance criteria in a way that will encourage and reward improved outcomes, and (5) focus on the results as the primary basis for safety decision-making.

RIPB-DM may be used by regulators and developers/ operators as a structured, repeatable process by which decisions are made on significant nuclear safety matters, including consideration of deterministic and probabilistic inputs. RIPB-DM plays a role in mitigating safety risks and provides a basis for informing security risk analysis, with implications to safeguards.

Common Position 21

> Given the novelties of the SMR technology, there may be insufficient reliable data to inform RIPB-DM. It is therefore recommended that, for the implementation of the integrated 3S approach, these limitations should be recognized.

3.4.2. Systems engineering process

The inherent reactor characteristics for the design are determined by the early fundamental design decisions to meet safety objectives, learning from operating experience, studies of technology maturity, etc. Systems engineering brings together these disparate aspects to develop, at an early stage, a comprehensive set of plant-level and system-level functional objectives. Examples of plant-level objectives include those for passive and active fulfillment of functions, man-machine interfacing, plant cost, plant availability, plant protection, construction schedule, load following versus base load, barrier protections against external events, etc. This step includes the identification of SSCs and their functions, and an identification of hazards associated with these SSCs. An integrated 3S approach would consider the needs for safety, security and safeguards and their interactions.

Common Position 22

> The use of a systems engineering process should aim to ensure that the areas of potential conflict between safety, security and safeguards are identified and resolved. Such a process provides a structured approach for identification of: (a) trade-offs in areas of potential conflict among the 3S, and (b) synergies between the 3S, i.e., complementary design approaches that optimize safety, security and safeguards.

3.4.3. Design of structures and plant layout

Structures generally provide one or more of the functions of pressure retention, shielding and confinement, and support to systems and components. Structures are designed for their credible

accident loads which can be from missile impacts (internally or externally generated), earthquakes, flooding, etc.

Nuclear reactor structures have historically been designed to protect the public by preventing the release of radioactive materials. These structures also provide a security barrier that prevents malefactors from taking control of nuclear material. Furthermore, the nuclear reactor structures provide substantial physical protection against impact loads such as aircraft crash. Nuclear reactor structures are also an important part of IAEA safeguards, helping to ensure that nuclear material is not removed without detection.

Common Position 23

> Significant 3S synergies are found in the design of structures, where the same structural design may provide safety protection against external and internal hazards, security protection against threats, and safeguard protection against unauthorized removal. In the plant layout, the 3S integration challenges generally relate to the preservation of human life via issues such as the effect of barriers and access control measures on the length of exit paths and number of emergency exits. Compact plant layouts influence the accommodation for reactor SSCs, including safety, security and safeguards systems and therefore, early consideration of the potential implications of a more compact plant is recommended while also emphasizing the need to provide sufficient space to accommodate 3S SSC. Although a compact plant layout may be advantageous from a security response perspective, it may also be advantageous to an adversary as there may be fewer barriers to vital area access. This should be considered by developers.

3.4.4. Remote data transmission

SMRs may be located and operated remotely and could be situated in areas lacking reliable internet connections. For the duration of the operating life, SMRs have a potential to rely on data transmission rather than on-site personnel to cover many of the 3S activities, compared to existing NPPs.

Common Position 24

> SMR designs need to consider and address any issues with the reliability, quality, and information security (confidentiality, integrity and availability) for any planned remote data transmission for the 3Ss and other purposes including operation. The possibility to leverage synergies among the 3Ss in this area should also be explored.

3.4.5. Project communication

Early and open communication of security and safeguards requirements is expected to help the safety experts and designers identify areas of potential conflict earlier in the project planning and design process when they can be resolved at lower cost and schedule impact.

Common Position 25

> SMR developers should include security and safeguards personnel as part of the design team to ensure that conflicts among the 3S are identified and resolved appropriately (3S approach).

3.4.6. Regulatory organizational culture and structure

It is anticipated that the future nuclear landscape will attract new developers and designers exploiting novel designs and choosing new ways to manage risks. SMRs may also have wider use beyond electricity generation. Regulators need to understand the evolving nuclear landscape and be equipped to respond to the changes. The potential benefit of a 3S approach and one that is 'by design' is to identify, understand and manage risks from whatever discipline they arise. This will require regulators to be proactive in exploring the potential benefits of a 3S approach. Regulators would generally accept that there are benefits in terms of efficiency and effectiveness from coordination, collaboration and integration across the 3S. However, such changes might be driven by industry rather than regulatory organizations. For example, new developers may be innovative, take a systems engineering approach, alongside 3S risk management in an integrated way and seek commercial advantage while expecting a more flexible approach from the regulator in terms of meeting the latter's expectations. Therefore, based on international and shared experience and understanding of future trends, regulators would want to adopt this more holistic approach albeit with caution given that there would likely be resource implications and a need for different skills, organizational arrangements, ways of working etc.

As Barley and Halhead have recognized in Ref. [26]: "To best deliver this cross-purpose working (a pragmatic mix of cooperation, collaboration, and some integration across and specialisms) requires a related organizational mindset, culture and structures that facilitate and inform joint working."

Common Position 26

> Regulators should be prepared to interface with all 3S stakeholders by having sufficient capacity and facilitating information sharing among the 3S disciplines.

As expressed by Ref. [26], a regulator could establish a "strategy that sets the conditions for such joint working to deliver a holistic regulatory approach". Further, as a means to mature, the regulatory organization might require the "idea of the 3S holistic approach (as opposed to a safety-based holistic case) to be examined, understood and defined so to set the conditions for any framework to develop this regulatory philosophy into something more tangible. By nature of regulation, this development journey would need to be evolutionary and achieved through dedicated research so that organizational development is shaped by a regulatory thinking that is aligned with future trends."

Common Position 27

> While it would not be realistic or necessary to change safety, security and safeguards assessment principles, the regulator should review higher-level guidance to regulation so to enable 3S approach. This internal regulator policy could in turn inform related training and other activities to build capability and capacity to regulate the SMR designs. International collaboration and lesson learning would also add value.

3.4.7. Cyber security for digital I&C

I&C systems, including the NMAC system, play a critical role in ensuring safety and security and the non-proliferation commitments of nuclear facilities. As digital technologies continue to evolve and become more capable, they are increasingly being incorporated into and

integrated with I&C systems. New nuclear facilities and modern nuclear facility designs use highly integrated digital I&C systems to handle and store vast quantities of process and inventory data. Digital technologies are also often introduced into I&C systems during the modernization of existing NPPs. Digital I&C can enhance the efficiency of SMR operations and maintenance because of the advanced real-time monitoring and prognostics. For example, the plant performance metrics and the off-normal condition detection and response can be provided to operations, and the component health status – to maintenance staff. While digitalization has many advantages, its application within I&C systems has made these systems vulnerable to cyber-attacks.

A cyber-attack is defined in IAEA "Computer Security of Instrumentation and Control Systems at Nuclear Facilities" [27] as "*a malicious act carried out by individuals or organizations that targets sensitive information or sensitive information assets with the intent of stealing, altering, preventing access to or destroying a specified target through unauthorized access to (or actions within) a susceptible system*". Sensitive information assets include control systems, networks, information systems and any other electronic or physical media.

Physical protection of computer-based systems (including digital I&C systems) is recommended in Ref. [12], paragraph 4.10, which states that "*computer based systems used for physical protection, nuclear safety and nuclear material accountancy and control should be protected against compromise (e.g. cyber-attack, manipulation or falsification) consistent with the threat assessment or design basis threat*". This same requirement is often used as a basis for national computer security regulation for NPPs.

Cyber security is an important interface among the 3S because a cyber-attack on I&C systems may jeopardize the integrity of all 3S. The effects of cyber-attacks on I&C systems related to safety may result in a wide range of consequences, such as a temporary loss of process control or unacceptable radiological consequences. Although most digital I&C systems in nuclear facilities are isolated from publicly available networks, some connection nodes connected to an open network can be added for maintaining, restoring, monitoring or testing of digital I&C systems. The security of these connection nodes is critical. To reduce the cyber-attacks risks, one-way communication may be required between security zones of the physical SMR facility.

Cyber security is a major consideration for remote SMR operations where operational data may need to be supplied continuously to off-site remote support centers. The confidentiality, availability and integrity of that information must be ensured. Remote information exchange may introduce pathways that can be exploited by adversaries, therefore requiring robust security considerations to be applied to the communication infrastructure. Some SMR designs propose autonomous plant operation which relies on software-based systems with access to sensitive plant process networks. Autonomous systems will be susceptible to code injection during the development process, during delivery and during software installation.

Common Position 28

> Digital I&C systems in SMRs should be designed to be resilient against the various cyber security threats. I&C systems and related digital components should be designed and operated in accordance with the concept of defence-in-depth against compromise. If digital twins were to include protection against compromise (cyber-attacks) in their design, they could improve both safety and security. There are some useful international standards e.g. Refs. [27], [28] and [29].

4. POSSIBLE METHODOLOGIES FOR INTEGRATION OF SAFETY, SECURITY AND SAFEGUARDS

4.1.INTRODUCTION

At a high level a 'by design' approach to the three disciplines provides the overarching philosophy for the development of a fully integrated 3S approach. Guidance is comprehensive for the specific disciplines although generally lacking with respect to integration. While 'by-design' may not address integration directly, however, it encourages it through integrated team working, the development of safety-informed security experts, security-informed safety experts, the adoption of a holistic systems engineering approach and a joint modifications process from early concept design to detailed design and construction. This would seem to be a sensible and realistic position from which to move on to a more fully integrated 3S approach; it also resonates with Generation IV challenges.

As to the mechanics of 3S integration, this section introduces some possible methodologies that could facilitate progress and allow, perhaps, the Common Positions to be addressed in SMR design. Three methodologies are described in Sections 4.3 to 4.5 and, although these are primarily conceptual and offer only partial integration, they do offer some insights and, in particular, make clear that achieving full integration will be both complex and challenging. But, first, we look at current IAEA guidance.

4.2. CURRENT IAEA GUIDANCE

NSS 27-G [13] and 40-T [30] offer a template for design and evaluation of a physical protective system (that could now include cyber protection). It specifies a systems engineering approach that identifies the physical protection needs of the specific facility, designs a physical protection system to meet these needs and then evaluates its effectiveness. By its very nature this approach demands integrated design teams. While this is helpful, there is no emphasis on the value of adopting a SeBD methodology nor on a more integrated 3S approach. Nevertheless, this description in a key NSS guide provides the basis to develop 3S-thinking and, for now, meets most security planners and regulators needs.

4.3. BOW TIE

The 'bow tie' approach is used for risk management across a number of high-risk infrastructure industries including civil nuclear. While originally used for security risk management in nuclear, it can be developed to include security and safety risks (see US NRC's approach shown in Figure 3). This model may also be helpful to regulators as it aids understanding of the level of risk inherent in a design but does not inform design development.

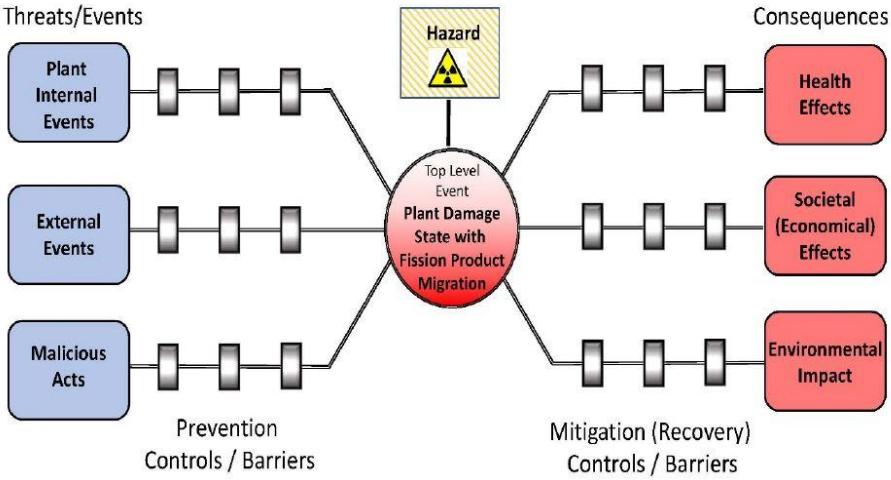


Figure 3: US NRC's proposed integrated approach to threats and events

Bowtie-type methodology is based on international risk management good practise. It takes 'threats' and considers proactive/preventive measures; then differentiates with reactive/mitigating measures and then resultant consequence. Developers' 3S experts (assuming they work as an integrated team) would determine what claims they could make based on evidence of the efficacy of both preventive/mitigation measures and robustness of the design. This provides a more complete picture of all risks to the NPP (hence a more comprehensive methodology) for developers to propose risk-based security (or a different non-traditional regime) and equally for regulators to see things more completely and organize accordingly (integrated teams) for their assessments and judgements.

4.4.DEMUTH AND BADWAN METHODOLOGY

DeMuth and Badwan [31] have proposed a methodology that is focused on Used Fuel Storage. Here, integrating the 3S's could be considered a three-step process where:

(1) the domestic material control and accountancy (MC&A) design is combined with the international (IAEA) safeguards design to create an integrated "safeguards" design,

(2) safety is integrated separately with the security design and the safeguards design, and then finally, and

(3) integrated safety/security and safety/safeguards designs are combined into a fully integrated safety, security, and safeguards design.

Safety is chosen as the central set of performance objectives for the recommended full integration because of its more complex system requirements than security or safeguards. At each of the three steps an iterative process is used, where for instance a safety design solution is proposed to satisfy a particular safety requirement and its impact upon the functioning of the existing security design is checked. Should functioning of the existing security design be compromised then the proposed safety design solution must be modified and its impact upon security rechecked.

In order to execute the three-step process of Figure 4, a complex set of the relevant requirements must first be identified and their interrelationship understood, which underscores the importance of Section 3 on Interfaces.

The role of integrating the 3S's within the overall facility design effort is shown in Figure 5 and represented as the "Response Analysis". According to DeMuth and Badwan [31], the response analysis is "an activity performed between the preliminary design and the final design". It is referred to as Response Analysis because it is the response (or impact) of one of the 3S disciplines to a change in the design of another discipline that is of interest. Design is finalized once the response analysis satisfies all of the performance objectives and the design has been optimized to minimize risks and costs.

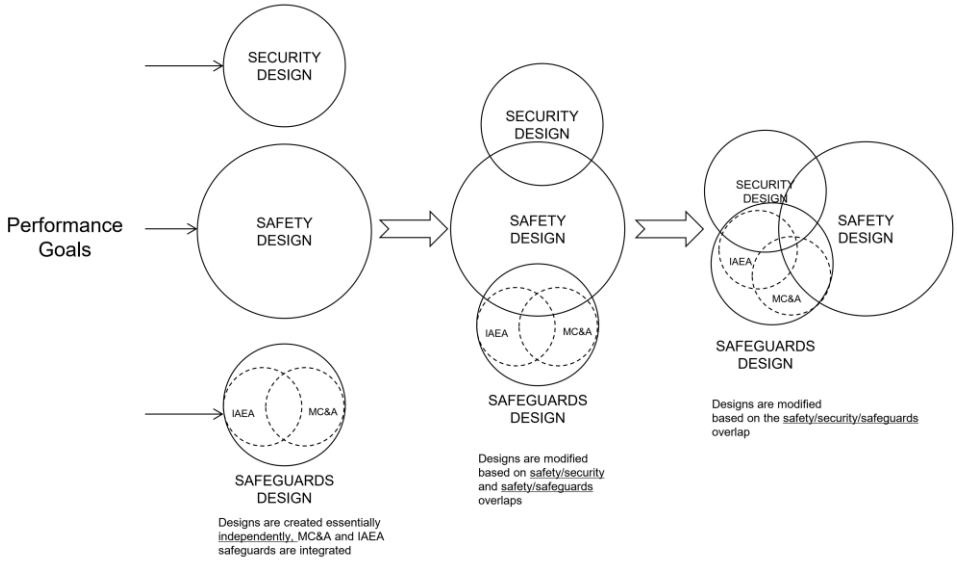


Figure 4: Three-step process for integrating safety, security, and safeguards [31]

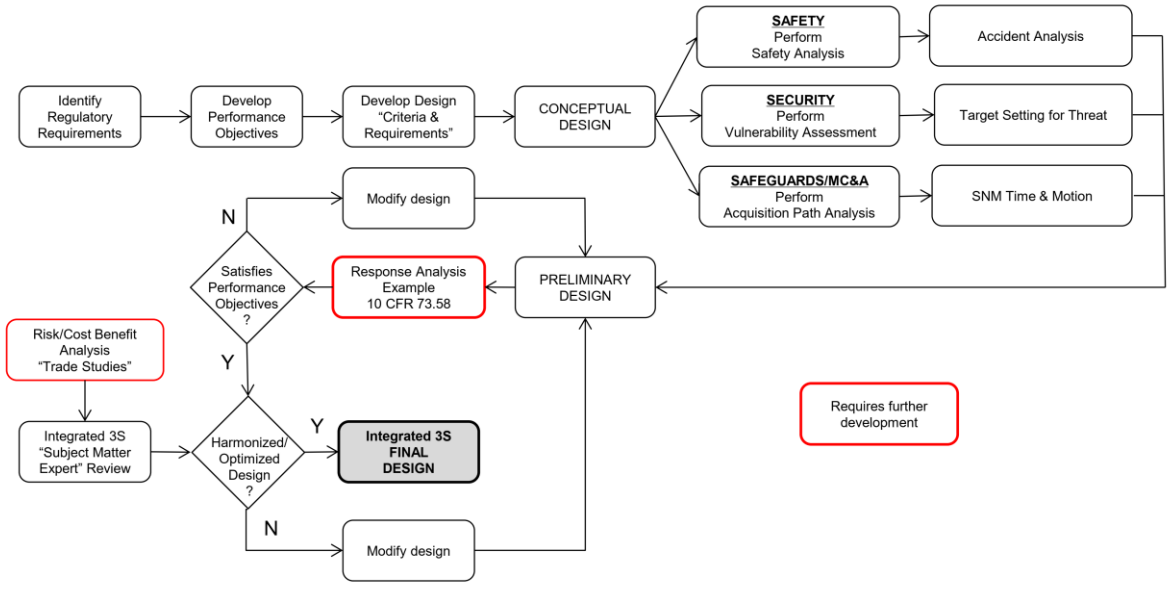


Figure 5: Overall design effort for a nuclear facility [31]

4.5.OBJECTIVE PROVISION TREE METHODOLOGY

The 'Objective Provision Tree' (OPT) model is part of the Integrated Safety Assessment Methodology developed by the Risk and Safety Working Group of the Generation IV (Gen IV) International Forum [32]. It follows on from earlier IAEA safety documents (e.g., Safety Reports Series No. 46 [33]) and, by incorporating security, now provides a way to analyse safety and security risks through the examination of lines of protection for prevention, control or mitigation of risks to plant operation. Its use in application to Generation IV designs has the IAEA's support for safety assessment although not for security considerations. The idea behind this approach is to 'design in' early rather than 'bolt on' later, and this is consistent with a broader 'by design' approach to 3S. As a methodology it is, compared to other methods, applicable to all design phases. It is also compatible with an outcome or objective regulatory regime as it does not dictate design requirements. While Ref. [32] uses it to address only the safety-security interface, it can be extended to cover all three disciplines.

The OPT method provides a top-down method which, for each level of DiD and for each safety objective/function (control of reactivity, removal of heat from the fuel, and confinement of radioactive materials), identifies:

- the possible challenges to the safety functions,
- the plausible mechanisms which can materialize these challenges, and
- the provided provision(s) to prevent, control or mitigate the consequences of the challenges/mechanisms.

All this is expressed through a hierarchical structure of relationships in the form of a tree. Figure 6 provides a standard structure for an OPT.

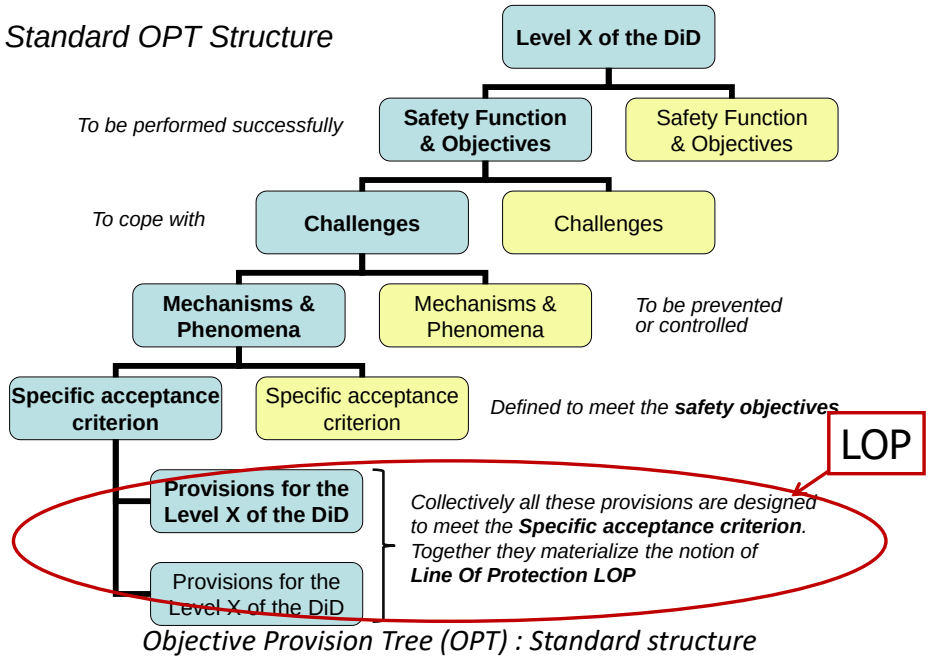


Figure 6: Objective Provision Tree ([32])

As explained by in [32]: "The logic sketched by the Major Stages of Pathway Analysis for Physical Protection can so be translated and adapted to the OPT logic. In the logic of the OPT one must replace the notion of safety function with that of security function. Notions as "challenge / threat", "mechanisms" and "provision" remain fully applicable."

Figure 7 provides, on its left side, the OPT logic for safety, and on its right side, practical insights for the construction of the OPT for protection against sabotage.

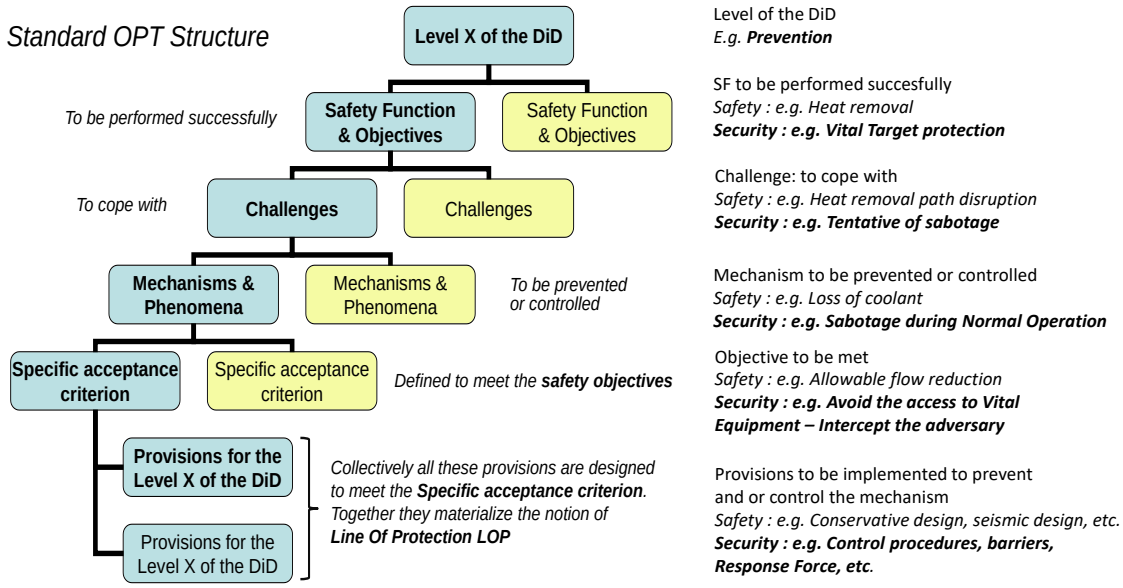
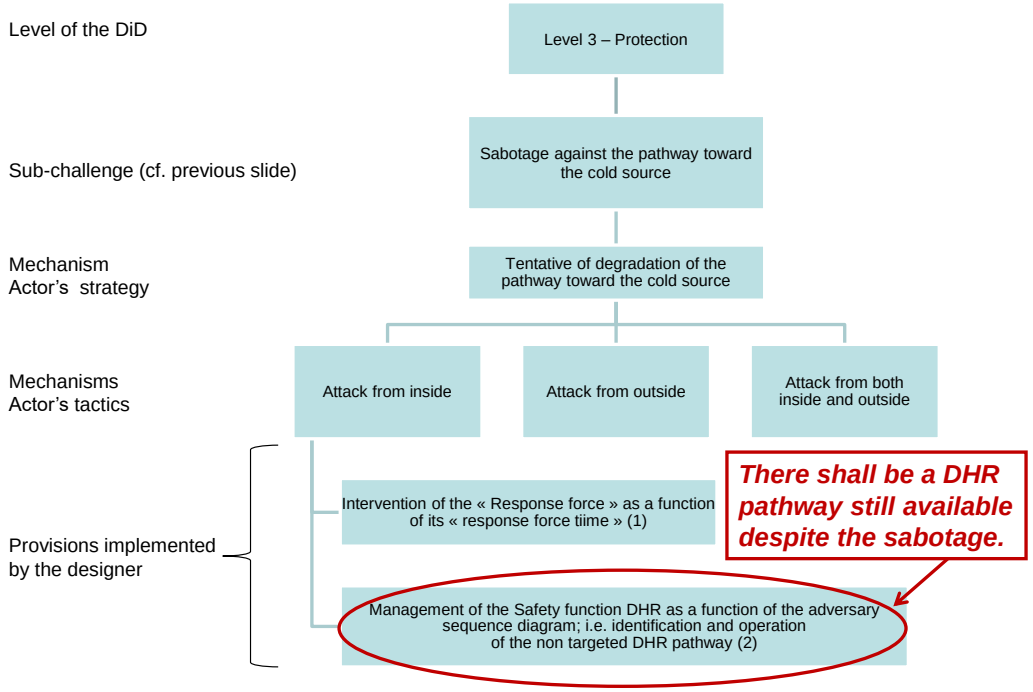


Figure 7: Objective Provision Tree – OPT for prevention against sabotage [32]

For practical application of the methodology, Ammirabile and Fiorini [32] show an example (Figure 8) of a simplified OPT to present the security architecture that should be implemented to protect the shutdown cooling system (SCS/DHR) against potential sabotage at the Levels 3 and 4 of DiD. Figure 8 shows that, in order to maintain shutdown cooling in case of a successful attack from inside, it is necessary to have other decay heat removal (DHR) pathways. The availability of independent and functionally redundant DHR pathways is a link between this particular OPT for security and related OPTs for safety, which although not shown herein for the sake of brevity, would point to an alternative DHR pathway. If it had been the case that an alternative pathway was unavailable, there would be a need for complementary DHR pathways, and for a re-design.



(1) – With a total delay that will be function of the early / late detection and of the « Response Force Time »
(2) - This suppose tha availability of several independent & functionally redundant DHR pathways

Figure 8: Simplified OPT for preventing against sabotage [32]

5. REGULATORY ROLE IN 3S

When considering SMR designs, regulators will likely develop their own relevant practices to indicate how new designs will be assessed. This is usually undertaken before any licensing process is initiated. Advanced technology and the introduction of new developers, some of whom may not be familiar with regulation, will influence this process. While some of the technological developments are specific to the civil nuclear industry, such as new fuel types and advances in passive safety, others like digital technology and artificial intelligence have wider applications. Technology alone, however, has not driven recent regulatory development but, rather, a shift towards a more goal-setting regime where the regulator sets the objectives leaving the developer or vendor to make choices in terms of how these goals are met. The outcome is that the vendor takes primary ownership of and responsibility for the design. This approach not only enables innovation but ensures risks – both commercial and physical - are for the vendor to assess, evaluate and to address. By owning the risks, and their management, it gives the vendor freedom to choose the means of mitigation rather than being confined by more prescriptive requirements. It also tends to ensure better understanding of those risks requiring enhanced levels of competence and a more mature regulatory organisational culture. In this way there are mutual benefits as regulatory expectations are met and more commercial objectives for the vendor are acknowledged. Therefore, there is a clear incentive for seeking greater 3S integration driven by the future nuclear landscape, but also in concert with developing regulatory ideas.

Regulators will need to explore a shift to a more ambitious integration across its own purposes. How far this regulatory shift in thinking might progress is not fully recognized but it is a necessary step towards embracing a 3S approach.

In previous chapters, the report has examined the SMR characteristics and the resulting drivers for regulatory organisations to engage with a 3S approach. This chapter provides regulatory experiences of early engagement with developers or would-be vendors, specifically, the Canadian Nuclear Safety Commission's (CNSC) Vendor Design Review (VDR) and the UK Office for Nuclear Regulation's (ONR) Generic Design Assessment (GDA), in the expectation that they would inform future regulatory thinking with respect to 3S integration.

5.1. CNSC SMR VENDOR DESIGN REVIEW

The CNSC developed a pre-licensing VDR as an optional service for SMR developers. A VDR is a mechanism that enables CNSC staff to provide feedback on a vendor's reactor technology early in the design process. Based on Ref. [34], the assessment is separated into three phases and is completed by the CNSC at the request of the vendor

Phase 1 review – Intent to comply with regulatory requirements: CNSC staff assess the information submitted in support of the vendor's design and determine if, at a general level, the vendor design and design processes are demonstrating implementation of CNSC design requirements, and related regulatory requirements.

Phase 2 review – Pre-licensing assessment: This phase goes into further detail, with a focus on identifying any fundamental barriers to licensing the design whether they exist currently or could emerge in future.

Phase 3 review – Pre-construction follow-up: In this phase, the vendor can choose to follow up on one or more focus areas covered in phases 1 and 2 against CNSC requirements pertaining

to a licence to construct. For those areas, the vendor's anticipated goal is to avoid a detailed revisit by the CNSC during the review of the construction licence application.

Phase 1 and 2 reviews have 19 review Focus Areas, which represent key areas of importance for a future construction licence application, while the Phase 3 review is tailored on a case-by-case basis.

CNSC staff review SeBD and how security interfaces and integrates with safety and safeguards as part of the VDR process. For example, the objectives of Focus Area 15 "Robustness, safeguards and security" are to "confirm that the vendor understands CNSC expectations and regulatory requirements as they pertain to the provision of robustness, security and safeguards in the design" and to "confirm that the design, as it is evolving, is meeting CNSC expectations for the provision of robustness, security and safeguards in the design" [34]. These objectives necessitate:

(a) reviews of safety information pertaining to containment and/or other buildings (for example, their design requirements and expectations), security information (for example, robustness against external events or threats including control of personnel access to SSCs) and safeguards information (for example, design requirements and expectations for nuclear material accounting and control),

(b) identification of interfaces between and among safety, security and safeguards, through multidisciplinary team collaboration, and

(c) identification of opportunities, if any, for 3S integration, which are then communicated to the vendor.

It should be noted that while there is already good collaboration within CNSC in (a) and (b) above, further efforts will have to be put in towards integration, (c), which by necessity will be an evolutionary process.

Another example of multidisciplinary team collaboration is during the review of the Focus Area 5 "Control system and facilities: a) main control systems, b) instrumentation and control, c) control facilities, d) emergency power system(s)". Focus Area 5 requires collaboration between nuclear security and nuclear safety (system engineering) specialists, to assess the effects of potential physical and cyber-attacks on control systems and facilities. This allows the regulator to evaluate how SMR developers intend to optimize nuclear security to mitigate against potential acts of sabotage, and how to consider physical and cyber defensive measures to counter separate or blended attacks.

5.2. ONR GENERIC DESIGN ASSESSMENT REVIEW

GDA offers an opportunity for ONR to work in a more holistic way as it represents a process for the safety and security (and now safeguards) assessment of new nuclear power plants. GDA is explained in [35] and various ONR guides (e.g. Ref. [36]) that describe regulatory expectations and offer organizational structures that enable cross-specialism work. GDA process will be applied where ONR is asked to assess a proposed design in advance, or in parallel to an application for a nuclear site licence. As explained by Barley and Halhead [26]: "The objective for GDA is to provide confidence that the proposed design is capable of being constructed, operated and decommissioned in accordance with the standards of safety, security, safeguards and environmental protection required in Great Britain. For the Requesting Party,

this offers a reduction in uncertainty and project risk regarding the design, safety, security, safeguards and environmental protection cases so as to be an enabler to future licensing, permitting, construction and related regulatory activities."

Recent technological developments and developments within the UK's regulatory regime, have created the conditions for considering greater interaction between the 3S's. One of the drivers for such change is regulatory learning, as explained in Ref. [26]: "Before discussing how the nuclear security purpose of ONR has developed and specifically during the recent GDA, experience has also shaped internal thinking. The expansion of the safeguards purpose has raised its profile and status within the organisation. The rapid development in cyber security thinking, capacity and relationship with safety has forced not only greater collaboration between the 3S's but also been a catalyst for change. Specifically, this is in terms of digitised control and instrumentation systems, and more advanced technology. Recent experience in GDA has brought together cyber security experts and safety-based control and instrumentation specialists. This has led to joint meetings, more holistic assessments of risk and acceptance that each specialism may require to use its own specific terminology but often draw from similar risk assessment methodology. When looking more broadly at the sabotage threat, VAI studies have drawn from the safety case and design details, although this may not be truly a holistic assessment of risk. While these observations are drivers towards a more holistic approach, there will be a need to conduct regulatory research and development outside GDA drawing on wider thinking from other regulators internationally."

In early 2022, ONR and the Environment Agency completed the GDA of the UKHPR 1000 reactor design. For the security assessment of that design, ONR applied their new regulatory approach based on their Security Assessment Principles so to better align security with safety. Although this initiative is only the beginning of seeking closer integration between security, safety and safeguards functions, it set the conditions for a more integrated approach to assessing risks inherent in a design and how these might be addressed adequately by a vendor or Requesting Party.

REFERENCES

[1] ENDO, T., Countries Planning to Introduce Nuclear Power Generation and the 3Ss-Making the 3S's an International Standard, ICNND, Barton, Australia (2009).
[2] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Nuclear Safety and Security Glossary, Non-serial Publications, IAEA, Vienna (2022).
[3] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safeguards Glossary, International Nuclear Verification Series No. 3 (Rev. 1), IAEA, Vienna (2022).
[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, Specific Safety Requirements No. SSR-2/1 (Rev. 1), IAEA, Vienna (2016).
[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).
[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Security During the Lifetime of a Nuclear Facility, IAEA Nuclear Security Series No. 35-G, IAEA, Vienna (2019).
[7] BUREAU OF INTERNATIONAL SECURITY AND NON-PROLIFERATION, Security by Design in the United States. US Dep. State (2012) (available at https://2009-2017.state.gov/t/isn/rls/fs/186672.htm).
[8] SNELL, M.K., JAEGER, C.D., Incorporating Security-by-Design in both Planned and Operational Nuclear Facilities, SAND2014-15268C, Sandia National Lab. (SNL-NM), Albuquerque, NM (United States), 2014 (available at https://www.osti.gov/biblio/1315235).
[9] DUGUAY, R., 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, Volume 7 (2020).
[10] SNELL, M., et al., Security-by-Design Handbook, SAND2013-0038, 1088049, Sandia National Lab. (SNL-NM), Albuquerque, NM (United States), doi:10.2172/1088049 (2013).
[11] WORLD INSTITUTE FOR NUCLEAR SECURITY, Implementing Security by Design at Nuclear Facilities, WINS International Best Practice Guide, Vienna (2019).
[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013).
[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 27-G, IAEA, Vienna (2018).
[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security for Nuclear Security, IAEA Nuclear Security Series No. 42-G, IAEA, Vienna (2021).
[15] LEE J.-S., et al., Safeguards by design (SBD) for Small Modular Reactors (SMRs), Symposium on International Safeguards 2022, 31 October – 4 November 2022, Vienna, Austria.
[16] The Structure and Content of Agreements Between the Agency and States Required in Connection with the Treaty on the Non-Proliferation of Nuclear Weapons, INFCIRC/153(Corrected), IAEA, Vienna (1972).
[17] Model Protocol Additional to the Agreement(s) between State(s) and the IAEA for the Application of Safeguards, INFCIRC/540(Corrected), April 1999.
[18] INTERNATIONAL ATOMIC ENERGY AGENCY, International Safeguards in the Design of Nuclear Reactors, IAEA Nuclear Energy Series No. NP-T-2.9, IAEA, Vienna (2014).
[19] KARHU, P., et al., Management of nuclear security-safety interface: what, why and how, Proceeding of the International Conference on Nuclear Security: Sustaining and Strengthening Efforts, IAEA, Vienna, Austria (2020).

[20] GANDHI, S., KANG, J., Nuclear safety and nuclear security synergy, Annals of Nuclear Energy, Volume 60, October 2013.
[21] INTERNATIONAL ATOMIC ENERGY AGENCY, Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage, IAEA Nuclear Security Series No. 4, IAEA, Vienna (2007).
[22] INTERNATIONAL ATOMIC ENERGY AGENCY, Identification of Vital Areas at Nuclear Facilities, IAEA Nuclear Security Series No. 16, IAEA, Vienna (2013).
[23] ZAKARIYA, N.I., KAHN, M.T.E., Review: Safety, security and safeguard, Annals of Nuclear Energy, Volume 75, Pages 292-302, January 2015.
[24] SHOKR A.M., Synergy between Nuclear Safety and Security for Research Reactors, Operating Principles, p. 14-16, IAEA, Vienna, Austria.
[25] KOVACIC, D.N., RENDA, G., Considering International Safeguards during the design of advanced reactors and interfaces with safety and security, Conference on Topical Issues in Nuclear Installation Safety: Strengthening Safety of Evolutionary and Innovative Reactor Designs, 18–21 October 2022, Vienna, Austria.
[26] BARLEY, D.A., HALHEAD, S., Safety, security and safeguards working together in a modernised Generic Design Assessment, Conference on Topical Issues in Nuclear Installation Safety: Strengthening Safety of Evolutionary and Innovative Reactor Designs, 18–21 October 2022, Vienna, Austria.
[27] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T, IAEA, Vienna (2018).
[28] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear power plants - Instrumentation, control and electrical power systems - Cybersecurity requirements, IEC standard 62645, 31 July 2020.
[29] ISO standard/IEC 27001, Information security management systems, 2022.
[30] INTERNATIONAL ATOMIC ENERGY AGENCY, Handbook on the Design of Physical Protection Systems for Nuclear Material and Nuclear Facilities, IAEA Nuclear Security Series No. 40-T, IAEA, Vienna (2021).
[31] DEMUTH, S., BADWAN, F., Integrating Safety, Security, and Safeguards for Used Fuel Storage, European Nuclear Conference, 12-14 May 2014, Marseille, France.
[32] AMMIRABILE, L., FIORINI, G.I., Application of the objective provision tree tool for the safety-security interface assessment, Conference on Topical Issues in Nuclear Installation Safety: Strengthening Safety of Evolutionary and Innovative Reactor Designs, 18–21 October 2022, Vienna, Austria.
[33] INTERNATIONAL ATOMIC ENERGY AGENCY, Assessment of Defence in Depth for Nuclear Power Plants, Safety Reports Series No. 46, IAEA, Vienna (2005).
[34] CANADIAN NUCLEAR SAFETY COMMISSION, Pre-Licensing Review of a Vendor's Reactor Design (available at https://www.nuclearsafety.gc.ca/pubs_catalogue/uploads/REGDOC-3-5-4-Pre-Licensing-Review-eng.pdf).
[35] UK's OFFICE OF NUCLEAR REGULATION, New Nuclear Power Plants: Generic Design Assessment Technical Guidance (available at https://www.onr.org.uk/new-reactors/reports/onr-gda-007.pdf).
[36] UK's OFFICE OF NUCLEAR REGULATION, New Nuclear Power Plants: Generic Design Assessment, Guide to Requesting Parties, Revision 0 (2019).

LIST OF ACRONYMS AND ABBREVIATIONS

3S	safety, security and safeguards
CDF	core damage frequency
CNSC	Canadian Nuclear Safety Commission
CSA	comprehensive safeguards agreement
DBT	design basis threat
DHR	decay heat removal
DiD	Defence-in-Depth
DSA	Design and Safety Analysis
EPZ	emergency planning zone
GDA	Generic Design Assessment
GFR	Gas-cooled Fast Reactor
HALEU	High-assay low enriched uranium
HRC	high radiological consequence
I&C	Instrumentation and Control
IEMU	Initiating Events of Malicious Origin
i-PWR	integral pressurized water reactor
IVR	In-Vessel Retention
LEU	Low enriched uranium
LFR	Lead-cooled Fast Reactor
LWR	light water-cooled reactor
MC&A	material control and accountancy
MSR	Molten Salt Reactor
MSSP	Member State Support Programme
NAR	novel advanced reactor
NMAC	Nuclear Material Accounting and Control
NNSA	National Nuclear Security Administration
NPP	nuclear power plant
NSS	Nuclear Security Series

ONR	UK Office for Nuclear Regulation
OPT	Objective Provision Tree
OSR	Operational Safety Reviews
PIE	Postulated Initiating Events
PSA	Probabilistic safety assessment
R&D	research and development
RIA	Reactivity Initiated Accidents
RIPB-DM	Risk-Informed and Performance-Based Integrated Decision-Making
RPV	Reactor pressure vessel
SBD	safeguards-by-design
SCS	shutdown cooling system
SCWR	Supercritical Water-cooled Reactor
SeBD	security-by-design
SES	Sabotage Event Scenario
SFR	Sodium-cooled Fast Reactor
SMR	Small Modular Reactor
SSAC	State system of accounting for and control of nuclear material
SSC	structures, systems and components
TRISO	tristructural isotropic
URC	unacceptable radiological consequences
USNRC	U.S. Nuclear Regulatory Commission (USNRC)
WG	working group
WINS	World Institute of Nuclear Security
VAI	Vital Area Identification
VDR	Vendor Design Review
VHTR	Very High Temperature Reactor

LIST OF CONTRIBUTORS

This report was produced and/or reviewed by the following volunteer representatives from the IAEA Member States who are also members of the DSA WG of the SMR Regulators' Forum and was subsequently approved by the Steering Committee:

Contributor	Country	Institution
Sanja Simic (Chair)	Canada	Canadian Nuclear Safety Commission (CNSC)
Paul Blackmore	Canada	Canadian Nuclear Safety Commission (CNSC)
Raphaël Duguay	Canada	Canadian Nuclear Safety Commission (CNSC)
Michael Kent	Canada	Canadian Nuclear Safety Commission (CNSC)
Lei Lei	China	National Nuclear Safety Administration (NNSA)
Marek Ruscak	Czech Republic	National Radiation Protection Institute (SURO)
Nina Lahtinen	Finland	Radiation and Nuclear Safety Authority (STUK)
Paula Karhu	Finland	Radiation and Nuclear Safety Authority (STUK)
Toni Huhtakangas	Finland	Radiation and Nuclear Safety Authority (STUK)
Tapani Honkamaa	Finland	Radiation and Nuclear Safety Authority (STUK)
Redouane El Ghalbzouri	France	Autorité de Sûreté Nucléaire (ASN)
Régine Gaucher	France	Department of the High Official for Defense and Security / Department of Nuclear Security (SG/SHFDS/DSN)
Sebastien Israel	France	Institut de Radioprotection et de Sûreté Nucléaire (IRSN)
Marielle Fayol	France	Ministère de L'Écologie, de Développement Durable et de L'Énergie
Hiroshi Ono	Japan	Nuclear Regulatory Authority Japan (NRAJ)
Takefumi Minakawa	Japan	Nuclear Regulatory Authority Japan (NRAJ)
Kazuko Goto	Japan	Nuclear Regulatory Authority Japan (NRAJ)
Shigeaki Sato	Japan	Nuclear Regulatory Authority Japan (NRAJ)
Azusa Sakurai	Japan	Nuclear Regulatory Authority Japan (NRAJ)

Contributor	Country	Institution
Akane Kawasue	Japan	Nuclear Regulatory Authority Japan (NRAJ)
Dong-Yeol Kim	Republic of Korea	Korea Institute of Nuclear Safety (KINS)
Kookheui Kwon	Republic of Korea	Korea Institute of nuclear Non-proliferation and Control (KINAC)
Hyun-Chul Kim	Republic of Korea	Korea Institute of nuclear Non-proliferation and Control (KINAC)
Sergey Sinegribov	Russian Federation	Scientific and Engineering Centre for Nuclear and Radiation Safety (SEC NRS)
Jean Joubert	South Afrika	National Nuclear Regulator (NNR)
Kameshni Naidoo	South Afrika	National Nuclear Regulator (NNR)
Duncan Barley	United Kingdom	Office for Nuclear Regulation (ONR)
Sarah Halhead	United Kingdom	Office for Nuclear Regulation (ONR)
Beth McDowall	United Kingdom	Office for Nuclear Regulation (ONR)
Anthony Bowers	United States of America	U.S. Nuclear Regulatory Commission (USNRC)
Stacy Prasad	United States of America	U.S. Nuclear Regulatory Commission (USNRC)
Eduardo Sastre-Fuente	United States of America	U.S. Nuclear Regulatory Commission (USNRC)
Steven Vitto	United States of America	U.S. Nuclear Regulatory Commission (USNRC)
Paula Calle Vives	IAEA	International Atomic Energy Agency (IAEA)
Volha Piotukh	IAEA	International Atomic Energy Agency (IAEA)
Jeremy Whitlock	IAEA	International Atomic Energy Agency (IAEA)
Shahen Poghosyan	IAEA	International Atomic Energy Agency (IAEA)
Tarek Majeed	IAEA	International Atomic Energy Agency (IAEA)
Mario Alves dos Santos	IAEA	International Atomic Energy Agency (IAEA)
Izaias Jose Botelho	IAEA	International Atomic Energy Agency (IAEA)