12-17-2020

Small Modular Reactors and Advanced Reactor Security: Regulatory Perspectives on Integrating Physical and Cyber Security by Design to Protect Against Malicious Acts and Evolving Threats

Raphael Duguay
Canadian Nuclear Safety Commission

Follow this and additional works at: <https://trace.tennessee.edu/ijns>

Part of the [Architectural Engineering Commons](#), [Criminology Commons](#), [Nuclear Engineering Commons](#), and the [Risk Analysis Commons](#)

Recommended Citation

Duguay, Raphael (2020) "Small Modular Reactors and Advanced Reactor Security: Regulatory Perspectives on Integrating Physical and Cyber Security by Design to Protect Against Malicious Acts and Evolving Threats," *International Journal of Nuclear Security*. Vol. 7: No. 1, Article 2.

<https://doi.org/10.7290/ijns070102>

Available at: <https://trace.tennessee.edu/ijns/vol7/iss1/2>

This article is brought to you freely and openly by Volunteer, Open-access, Library-hosted Journals (VOL Journals), published in partnership with The University of Tennessee (UT) University Libraries. This article has been accepted for inclusion in International Journal of Nuclear Security by an authorized editor. For more information, please visit <https://trace.tennessee.edu/ijns>.

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

Cover Page Footnote

The author wishes to acknowledge and thank Walter Dorn, John O'Dacre, Patrick Adams, Jessica Fahey, Sean Belyea, Kevin Lei, and Felicity Harrison for their valuable support and constructive comments to this paper.

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

Raphael Duguay

Canadian Nuclear Safety Commission

International Conference on Nuclear Security: Sustaining and Strengthening Efforts, 10–14 February 2020, Vienna, Austria

Abstract

How can future nuclear technologies and Small Modular Reactors (SMRs) deter and prevent organized crime groups, terrorists, and malicious actors from attempting to steal or sabotage nuclear materials and facilities? This paper presents the benefits of integrating Security by Design (SeBD) into a regulatory framework to allow more a flexible and effective design of physical protection systems for SMRs. During its effort to modernize the *Nuclear Security Regulations*, the Canadian Nuclear Safety Commission (CNSC) licensing application process provides for the option of SeBD in moving toward a performance-based approach with less prescriptive requirements. CNSC also recognizes the need for a graded approach using risk-informed criteria for nuclear security. As part of the SMR Vendor Design Review

doi:10.7290/ijns070102

(VDR) process, CNSC reviews SeBD proposals as well as interfaces with safety (robustness), safeguards (Nuclear Material Accounting and Control), operations, and sustainability. The CNSC also recognizes the need to share relevant, nuclear, sensitive information from the National Design Basis Threat (DBT) with SMR designers so they can consider credible and evolving threats in their proposed SeBD. Finally, the interfaces between nuclear security and system engineering specialists within the VDR process allow one to look at both physical and cyber security systems in a more holistic approach. This allows the regulator to look at how SMR developers propose to optimize nuclear safety to mitigate or protect against potential acts of sabotage and radiological release.

SeBD offers opportunities to reduce costs for new nuclear facilities. However, it is not a “silver bullet.” SeBD needs to be integrated as part of an overall security strategy taking into consideration essential security policies, facility characteristics, the materials used, and the national threat/DBT. In addition, there are other relevant security challenges to address, such as remote facilities without readily available off-site response capabilities, the concept of building unmanned/remotely operated nuclear facilities, ever evolving cyber security threats, over-reliance on digital technologies, the use of lethal force by autonomous and remotely operated security systems, or protecting floating (e.g., offshore) or transportable SMRs. Some of these SMR designs being considered are for future use, but now is the time to address some complex issues and legal/ethical questions that may shape the reality of future generations.

Key words: Small Modular Reactors, Security by Design, Nuclear Security, Physical Protection, Nuclear Security Regulations

Acknowledgements: The author wishes to acknowledge and thank Walter Dorn, John O’Dacre, Patrick Adams, Jessica Fahey, Sean Belyea, Kevin Lei, and Felicity Harrison for their valuable support and constructive comments to this paper.

ABSTRACT.....	1
I. SECURITY BY DESIGN FOR SMRS AND ADVANCED REACTORS.....	5
A. CONTEXT.....	5
B. SECURITY BY DESIGN FOR NUCLEAR SECURITY: WHAT DOES IT MEAN?	7
C. OVERVIEW OF SECURITY IN THE DESIGN PHASE.....	10
D. SEBD FOR SMRS AND NUCLEAR FACILITIES	11
E. OVERVIEW OF SECURITY BY DESIGN PRINCIPLES	12
1. Including The Design Basis Threat And/Or Threat Statement In The Design.....	13
2. Security Of The Nuclear Supply Chain.....	13
3. Defence In Depth And Balanced Protection.....	14
4. Nuclear Plant Security Zones	14
5. Reliability And Redundancy.....	15
6. Contingency Plans And Business Continuity Plans.....	15
II. INTERNATIONAL PERSPECTIVE OF SEBD FOR NEW NUCLEAR FACILITIES AND SMRS	16
F. INTERNATIONAL ATOMIC ENERGY AGENCY (IAEA) GUIDANCE	16
G. THE INTEGRATION OF SECURITY BY DESIGN (SEBD) IN THE REGULATORY FRAMEWORK	17
1. Uk Office For Nuclear Regulation (Onr).....	17
2. Usa Nuclear Regulatory Commission (Nrc).....	20
3. Canadian Nuclear Safety Commission (Cnsc).....	21
A) Cnsc Smr Vendor Design Review	23
B) Giving Access To Nuclear Security Information In The Dbt For Smr Developers	24
C) Cnsc Graded Approach For The Security Of Smrs	25
H. 2.3 SAFEGUARDS AND SECURITY BY DESIGN (SSBD) OPPORTUNITIES.....	25
1. The Longer View, Challenges, And Additional Thoughts.....	28
I. Q1: HOW MUCH ENGINEERED SECURITY IS ENOUGH TO AVOID THE RELIANCE ON ARMED ONSITE NUCLEAR RESPONSE PERSONNEL TO INTERDICT OR NEUTRALIZE THE THREATS?	29
J. Q2: WHAT IS THE APPROPRIATE NUMBER OF SECURITY PERSONNEL FOR SMRS?.....	38

K.	Q3: WHAT ARE THE SECURITY CONSIDERATIONS FOR FLOATING (OFF-SHORE, REMOTE SMRS AND TRANSPORTABLE SMRS?	40
L.	Q4: WILL SMRS BE USED FOR PEACEFUL PURPOSE ONLY?	42
M.	Q5: WILL SMRS BE SAFE FROM HACKERS?	43
N.	Q6: OTHER CHALLENGES FOR LICENSING SMRS?	44
III.	CONCLUSION AND RECOMMENDATIONS	46
IV.	ANNEX 1: IAEA NSS 35-G NUCLEAR SECURITY DESIGN ACTIONS FOR COMPETENT AUTHORITY AND OPERATORS [23]	48
V.	WORKS CITED	50

I. Security by Design for SMRs and Advanced Reactors

This first section introduces the current context and provides an outline of Security by Design (SeBD) for nuclear facilities, in particular SMR designers. It also provides an overview of SeBD principles and practices to better understand their use for new nuclear technologies and advanced reactors.

A. Context

According to the International Atomic Energy Agency (IAEA) [1] and Nuclear Energy Institute [2], a Small Modular Reactor (SMR) is defined as “a nuclear reactor, generally 300 MWe equivalent or less, designed with modular technology using module factory fabrication, pursuing economies of series production and short construction times.”

According to the IAEA, “Global interest in small and medium sized or modular reactors has been increasing due to their ability to meet the need for flexible power generation for a wider range of users and applications and replace ageing fossil fuel-fired power plants. They also display an enhanced safety performance through inherent and passive safety features, offer better upfront capital cost affordability and are suitable for cogeneration and non-electric applications. In addition, they offer options for remote regions with less developed infrastructures and the possibility for synergetic hybrid energy systems that combine nuclear and alternate energy sources, including renewables” [1].

Safety, security, and safeguards must be considered in the design of these new technologies to address international commitments, recommendations, good practices, and national regulations. It is important for designers, vendors, and nuclear regulators to include nuclear security throughout the entire lifecycle and emphasize its importance at the design phase and in the national regulatory framework.

In the recent Global Nexus Initiative (GNI) [3] report on *Advancing Nuclear Innovation: Responding to Climate Change and Strengthening Global Security*, the authors’ categorize three types of advanced reactor technology: Molten Salt, Triso-Based, and Fast Neutron Spectrum. In this study, they assess the application of international nuclear safeguards and nuclear security provisions for these three major types of reactors. Their preliminary results conclude that:

- Advanced reactors can play an important role in reducing carbon emission.
- The application of nuclear non-proliferation and security regimes need to be further developed.
- Many concepts can be safeguarded to prevent nuclear proliferation, but there are questions on how it can be implemented and at what cost.
- Advanced reactors consider nuclear security and measures to prevent radiological release. However, concerns remain on the security applications for remote locations, remote monitoring, and effective and timely response in case of a security event in a remote location.
- Safety and security should be thoroughly assessed for these advanced reactors as the nuclear governance structure evolves.

- There must be political and public confidence and adequate international assistance to effectively contribute to the upcoming climate and security challenges.

For nuclear security and advanced reactors, GNI presented in 2018 four key challenges: 1) Physical Protection, 2) Facility Sabotage and Nuclear Terrorism, 3) Cyber and Emerging Technologies, and 4) Reactor Siting [4]. In this preliminary security assessment, GNI experts found that:

- Molten Salt appears to have low vulnerability to theft of nuclear material and dispersal of radioactivity.
- TRISO-Based appears to have low vulnerability to theft of nuclear material and dispersal of radioactivity.
- Fast Spectrum presents a Category 1 risk with plutonium in fresh fuel or, if separated, from spent fuel.
- Below ground placement may lower security risks.
- Remote location challenges need more analysis.
- Emerging technologies like Artificial Intelligence and block chain may play a role in addressing some security concerns.
- For sabotage, further information is required to assess the vulnerabilities against an act of sabotage and how developers demonstrate how they can mitigate, reduce, or eliminate potential radiological consequences.
- Nuclear newcomers need to be better prepared.

Compared to current Nuclear Power Plants (NPPs), SMRs may rely on coolants other than water, such as gases or molten metals or salts. Some designs are not susceptible to overheating and core damage. According to the GNI report, “there is less reliance on external power, and passive safety features can reduce potential radiological release risk. SMR designers are incorporating engineered physical security systems, hardware, and controls on digital assets to reduce or eliminate the reliance on human security personnel and to reduce cost” [4]. The economics of getting a licence, building, and sustaining operations of SMRs is considered to be a major challenge for industry representatives. Well-considered decisions will have to be made when proposing ways to reduce the cost of security without compromising either safety or security. SMRs may be perceived as high-value targets and be considered as a critical infrastructure if they produce a reliable source of electricity. They are designed to be produced in factories and may be proposed for use in remote areas. Therefore, they must be designed to withstand terrorist attacks and other malicious acts. Security is an essential requirement for its commercialization. Some SMR designs already consider measures to mitigate seismic effects, natural hazards like tornadoes or hurricanes, and airborne terrorist attacks. But how much security will be needed?

The first part of this paper explains SeBD concepts, its benefits, and provides an overview of security principles in the design phase that can help reduce costs and mitigate risks. The second section presents how SeBD can be incorporated into a regulatory framework to optimize the benefits for all relevant

stakeholders. The last section discusses future challenges and questions that should be addressed by the international community and the IAEA.

B. Security by Design for Nuclear Security: What Does it Mean?

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 [5], 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
- Increases efficacy of Protective Force (e.g., on-site security guards) in the event of an attack

In 2014, Mark Snell and Calvin Jaeger conducted research on SeBD for both planned and operational nuclear facilities on the behalf of the Sandia National Laboratories [6]. According to the authors, Security-by-Design (SeBD) is an approach whereby security is fully integrated into the design process of a nuclear facility from the very beginning. For nuclear facilities, the authors defend that when SeBD is adequately implemented, the physical protection system is more robust to future changes in requirement over the lifecycle of the facility and more effective against malicious acts. An interesting point is the need to anticipate future changes in the Design Basis Threat(s) (DBT) and Threat Assessments, as well as the potential changes in requirements that may occur during the lifecycle of a nuclear facility. The following Table 1 provides examples of how SMR design could integrate this new threat information in countermeasures.

Table 1: How SMR designs could integrate threat information in countermeasures

Topic	Possible Countermeasures
Hypothetical changes in capabilities to any threat attempting to commit	
<ul style="list-style-type: none"> 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.
<ul style="list-style-type: none"> Theft 	Reduce the number and inventory of Inner Areas with Category I material, and locate them so that they are easier to protect.
Hypothetical changes to External Threats	
<ul style="list-style-type: none"> Better attack vehicles 	Room for more standoff and improved and possibly more vehicle barriers; early detection capabilities against unauthorized vehicles
<ul style="list-style-type: none"> 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
<ul style="list-style-type: none"> 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
<ul style="list-style-type: none"> More adversaries and/or better tactics 	Allow for a larger protective force and/or better tactical training
<ul style="list-style-type: none"> 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
<ul style="list-style-type: none"> Cyber-attack capabilities 	Better cyber protection, both for control systems and critical security systems
Hypothetical Changes to Internal Threats	
<ul style="list-style-type: none"> 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.
<ul style="list-style-type: none"> Cyber-attack capabilities 	Better cyber protection, both for control systems and critical security systems

Source: Sandia National Laboratories, 2013 *Security by Design Handbook* [7], *Threat Capabilities That Might Change over Time and Possible Countermeasures*

Snell and Jaeger also present the assumptions, observations, and conclusions from The *Security-by-Design Handbook* [7] developed by the USA Department of Energy - 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

doi:10.7290/ijns070102

2. Using a risk-informed design methodology
3. Integrating facility design during the operations 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 [7].

According to World Institute of Nuclear Security (WINS) 2019 Best Practice Guide on SeBD [8], 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.

SeBD is very similar to the Crime Prevention Through Environmental Design (CPTED) in its approach to reduce risks [9]. CPTED encourages the proper design and effective use of the surrounding environment to reduce crime opportunities. To provide maximum control, an environment may be divided in smaller, clearly defined areas or zones to create *defensible space* [10, 11]. CPTED approach focuses on:

doi:10.7290/ijns070102

- Manipulating the physical environment to change human behaviors
- Redesigning space or using techniques to encourage desirable behaviors and discourage illegitimate activities
- Reducing the “no man lands” and ensuring proper ownership of the space used

CPTED strategies can help prevent crime and terrorism by using creative architectural designs with inherent security features. The first generation CPTED models used several practices, such as increasing natural surveillance, implementing effective access control designs, increasing territorial markers and reinforcement (such as warning signs), and keeping a well-maintained space or facility to deter crime opportunities for offenders. Similar to the concept of SeBD, CPTED aims to increase the effort, time, and resources needed to defeat physical protection systems to gain access to the protected facility or compromise the asset (e.g., target).

C. Overview of Security in the Design Phase

SeBD can be considered as the output of an integrated security system design process. This process is well established within the Design and Evaluation Process Outline (DEPO) methodology for physical protection systems described by Mary Lynn Garcia [12]. This process was later refined by Sandia National Laboratories [13] and outlined in Figure 2.

Figure 2: Figure 2: The Design and Evaluation Process Outline (DEPO)

Source: Sandia National Laboratories, Introduction to the International Training Course on the Physical Protection of Nuclear Facilities and Nuclear Materials [13]

To determine which security measures and physical protection systems are needed, designers must understand the characteristics and size of the facility. This includes the type and amounts of nuclear material needed and identifying the vital areas and critical targets to establish priorities. Following this first step, there is a need to conduct a security risk assessment to understand the credible threats to protect against, the national threat, and/or the Design Basis Threat (DBT). This is imperative to understand the capabilities, motives, and intentions of potential adversaries. This assessment should include a vulnerability assessment in order to integrate mitigating controls in the design of physical protection systems [14].

In WINS SeBD Best Practice Guide [8], it is also considered crucial that designers understand the security requirements and DBT. Threat information should be shared with an approved designer so that mitigating measures are effectively implemented at the design phase. If they are kept in the dark for confidentiality reasons, the proposed SeBD measures may not reduce the threats and consequences effectively.

Cooperation between system engineers and security professionals is needed to fully mitigate defined threats [7, 8]. For example, the designer must first understand the objective of the Physical Protection Systems (PPS), required capabilities, and what it must protect against. Next, the system design or review is completed to mitigate, reduce, or eliminate the risks. This is where the preliminary system design starts.

According to Norman [15], an integrated security system design provides the following benefits:

- Uniform application of security policies
- Integrated multiple systems into one for operational simplicity
- Can integrate systems from multiple buildings and multiple sites
- Can integrate the services for multiple business units for consistency

D. SeBD for SMRs and Nuclear Facilities

SeBD for nuclear facilities may include designs against the threat(s) and/or design to mitigate potential consequence resulting from a threat.

The following SeBD example is specific to mitigate the consequence of a malicious act:

- Vital areas located underground to mitigate air-plane crash or stand-off attacks, also reducing potential radiological consequence in case of sabotage.

The following SeBD examples are to prevent and respond against the threat(s):

- Strategically located security post and armed security personnel that can respond rapidly and effectively to multiple targets/vital areas
- Design specially reinforced positions near vital areas that can resist ballistic and explosives attacks, strategically placed to neutralize adversarial threats
- Multi-purpose Central Alarm Stations (CAS) with safety, security, and Nuclear Material Accounting and Control (NMAC) surveillance and monitoring functions and capabilities. The CAS can be used to monitor daily operations, security, and emergency responses.
- Holistic IT Security Management System for the proper use, classification, handling, and management of sensitive/classified information

According to Bolton, C.J., “SeBD can reduce the intrinsic vulnerability of nuclear facilities while minimizing costs and disruption to operations. The fundamental processes of a nuclear facility should be designed from the start to give the same priority to nuclear security objectives as to nuclear safety. Vital areas should be designed out, minimizing the need for protective security and reducing the risk from insiders. This requires a proactive approach, involving engineers, security managers, safety specialists, and operators to optimize the benefits from the intrinsic features of the processes, materials, and structures. A robust, threat-tolerant design is required. In some areas, measures included in the design to improve nuclear safety will also assist security. In others, a design solution needs to be sought that will minimize conflicting requirements. As a result, SeBD requires appropriate organizational commitment and culture to enable full integration of the design for operations, security, safety, and safeguards” [16].

Bolton’s explanation underlines the importance of security by design for the protection of vital areas in NPPs. To effectively protect vital areas, multiple stakeholders should be consulted including engineers, safety, and operational and security specialists. This approach also prevents conflict between safety and security during the design phase. SeBD should also incorporate measures to mitigate insider threats. To facilitate the implementation and endorsement of security by design, it needs to be supported by the site management team and integrated in operations at all stages: design, construction, operation, licensing, and decommissioning. Bolton also emphasizes the importance of integrating nuclear safety and security, and safeguards. This good practice is also reflected in the SeBD Handbook [7] and the WINS Best Practice Guide [8] for the use for integrated and multi-disciplinary design teams.

E. Overview of Security by Design Principles

The intent of this section is to identify key security design principles that are applicable for SMRs. In E. Marrent’s presentation [17] at a WINS workshop on Security by Design for SMRs [18], Marrent proposed the following interpretation:

1. Integrated approach: working with engineering and safety specialists to achieve integrated security systems; for example: integrating physical and cyber security specialists in the design process
2. Inherently secure: design plants, facilities, buildings, and systems with security in mind at the beginning of the process
3. Passive security: reduce reliance on active security and human measures to counter a security event
4. Evolving response: the ability to provide a flexible response to changing threat levels, and security systems to meet the unknown future threats

The last element of this definition is essential. It reflects the importance of using flexible security measures and systems to address evolving threats.

1. Including the Design Basis Threat and/or Threat Statement in the Design

In nuclear security, the national threat assessment and/or DBT must be considered in the design of nuclear security measures. The operator should take into consideration the attributes and characteristics of both external and internal threats who might attempt to steal or sabotage the nuclear or radioactive material; for example, blended attacks with adversaries physically attacking the site while simultaneously launching a cyber-attack on security surveillance systems. This is derived from IAEA Nuclear Security Recommendations Nuclear Security series # 13 (NSS.13) [19] and guidance in NSS 19 [20]. As a result, SMRs will have to take into consideration the DBT when possible. Therefore, it's important to consider how both national and foreign SMR vendors and designers are able to be security-vetted in order to have access to classified information (e.g., DBT) when designing a reactor.

The DBT evolves over time to reflect the changes in threats. The design concept is usually fixed once the facility is built. Because it is difficult to predict evolving threats and future actions of criminals or terrorists, the DBT should be treated as a "surrogate" so it stands in place for unknown threats [8]. For example, an SMR should be built out of range of a ballistic threat as defined in the applicable DBT. The design could propose increased stand-off distance to minimize the effects of certain ballistic threats (e.g., shoulder fired missile) and reduce potential upgrade costs as the DBT changes to reflect more capable weapons. Another possibility is to acquire additional land around a nuclear facility to increase the buffer zone and stand-off distance for credible DBT type threats. WINS notes that a well-engineered solution to one hazard may also provide good resistance to others.

2. Security of the Nuclear Supply Chain

Another important aspect of security by design is to consider the security of the nuclear supply chain to ensure that the personnel and organizations involved during the different stages (design, construction, operations, and decommissioning) are trustworthy and reliable. This also includes the management and procurement arrangements (ex: contracts) to integrate quality controls and security, including cybersecurity. This entails using reliable suppliers and implementing effective provisions to protect confidentiality, integrity, and availability of the information and assets, as well as to prevent backdoor

intrusions and denial of service (DOS). The construction of SMR security components will need to go through this rigorous process.

Another important consideration is the need to protect design documents that are considered sensitive and/or classified. When technical requirements of physical protection systems are integrated in design criteria, the design document must be adequately protected against espionage and theft. Contractors and third parties can be used by adversaries to gain access to this information. Protecting security design documents against cyber-attack should be integrated in the supply chain arrangements. The value of nuclear reactor design documents is very high, and the threat of corporate espionage and cyber-attacks should not be underestimated.

3. *Defense in Depth and Balanced Protection*

In practice, SeBD includes the use of multiple security layers and measures that an adversary must defeat to access nuclear or other radioactive materials. It can include physical security zones and administrative controls applying a defense in depth approach (see Figures 3 and 4). The security layers must be designed to ensure that all pathways to the targets are adequately protected. This is commonly referred to as balanced protection to avoid any weak points. This approach should also consider the tactics and techniques used by insiders.

Figure 3: Defense in Depth example of Egypt Buhen fortress (around 1860 BC), multiple walls and optimizing topography.

Photo source: Wikipedia

Figure 4: Defense in Depth example at a Nuclear Power Plant with multiple layers of fences and a vehicle denial barrier to create delay.

Photograph taken at Gentilly 2.

4. *Nuclear Plant Security Zones*

For nuclear power plants, there are three security zones with increased levels of physical security measures. The controlled area or limited access area is the zone surrounding the plant and used to control access to the site. The protected area is closer to the reactor and is equipped with multiple

physical barriers and perimeter intrusion detection systems that prevent and detect intrusion attempts. Access to the protected area is restricted and involves personnel security screening, escorts for authorized visitors, and checkpoints to search people and vehicles entering and exiting the site for weapons, explosives, or contraband items. Specialized detection equipment is also installed to detect nuclear material going out of the facility. The vital area(s) are located inside the protected area. They are also equipped with stand-alone physical barriers, intrusion detection systems, and other administrative controls to protect the nuclear materials. Vital areas contain equipment, systems, or devices which could directly or indirectly lead to high radiological consequences if they were successfully sabotaged (see Figures 5 and 6). Finally, sites that store and/or use high-risk or Category I nuclear material will have an inner area equipped with additional stand-alone protection, access control measures, and enhanced personnel security screening [19, 20].

Figure 5: Citadel of Besancon, France. Site using multiple defensive layers to harden the site by using 360-degree protection around the critical buildings and optimizing high grounds, Fortifications by Vauban

Photo Source: Wikipedia

Figure 6: Example of the security zones and site layout for nuclear power plants using a defense in depth design.

Photo Source: NEI

5. Reliability and Redundancy

SeBD must consider reliability and redundancy of equipment and measures to ensure continuous operations. This can include, for example, multiple and complementary detection sensors and cameras; back-up power supply for critical intrusion detection and assessment systems/devices; Central Alarm Station (CAS) and Secondary Alarm Stations (SAS) located in different facilities or outside the plant area; or multiple response forces located in well-protected, strategic locations to facilitate timely and effective interventions. There are important cyber security design protection measures that must be considered to protect the CAS and SAS functions, as well as any server rooms and other critical digital assets.

6. Contingency Plans and Business Continuity Plans

Finally, SeBD should include contingency plans. Contingency plans and/or business continuity plans are essential. In the case of multiple attacks from an adversary, the capacity of the response forces can be

overwhelmed. Therefore, there is a need to consider on-site multi-organization support as well as off-site response forces to ensure well-coordinated and effective tactical support.

In summary, all the elements mentioned above incorporate factors for the sustainability of nuclear security measures. SeBD is a conceptual approach that promotes the integration of security at the earliest stage to mitigate malicious acts, but it should also be part of the entire facility lifecycle. It should be part of a holistic approach, integrated with operations, safety, and nuclear material accounting and control, so they are mutually supportive and avoid conflicts. There are other nuclear security principles that are applicable for SMRs, such as nuclear security culture, which will be discussed in section 2.

Overall, the competent authority should identify and define key security principles to assist operators and designers in understanding the requirements and expectations for SeBD. The next section provides examples on how SeBD principles can be integrated into national regulatory approaches to increase its benefits for all relevant stakeholders.

II. International Perspective of SeBD for New Nuclear Facilities and SMRs

This next section will focus on the integration of SeBD in regulatory approaches and requirements for the design of new nuclear facilities and SMRs. It will highlight its benefits and explain how it can help mitigate evolving threats.

F. International Atomic Energy Agency (IAEA) Guidance

Security design requirements for SMRs and advanced reactors are not clearly set in one universal standard. As shown in Figure 1, the *Convention of Physical Protection of Nuclear Material* (CPPNM) [21] and its amendment [22], including the IAEA Nuclear Security Series, set recommendations for the fundamental security principles for a nuclear security regime. The IAEA also provides technical guidance in NSS 35-G *Security during the Lifetime of a Nuclear Facility* [23]. In this guide, the IAEA promotes the inclusion of nuclear security in the early design stage and the integration of security with safety, safeguards, operation, and other requirements. In particular, nuclear security and safety measures should be designed and implemented in an integrated manner so that security measures do not compromise safety, and safety measures do not compromise security. For example, the design team should include security personnel to ensure that conflicts between nuclear safety, nuclear security, and safeguards are identified and resolved appropriately. The IAEA NSS 35-G provides recommended “design actions” for the competent authority and the operators, which are fully applicable to SMRs (see annex 1).

According to the IAEA guide [23], considering security requirements early in new designs, partial redesigns, or modifications will result in a nuclear security regime that is more efficient and effective. This document recognizes that the design phase is an iterative process that goes from the conceptual

design through final design in a repeated cycle of activities. In other cases, the design may be developed and approved prior to siting the facility, or it can result in a request for approval to construct a nuclear facility. The guide identifies key actions to follow for the state and the operators during each stage of the nuclear facility lifecycle. During the design stage, the guide promotes the minimization of conflicts between security and other design requirements, for example, by eliminating potential vulnerabilities with suitable engineering solutions.

In the 2015 IAEA Glossary [24], the terms “designers” and “vendors” for SMRs do not exist. There is a distinction between operators (e.g., licensees) and designers/vendors. An operator is a person or organization that is licensed or authorized by a competent authority. The SMR designer or vendor is not an authorized entity recognized by the IAEA. Therefore, they are not subject to contract or licence agreements and can operate outside the legal and regulatory framework in some countries. This can be considered as an important obstacle for sharing classified information because of the risk for designers or vendors benefiting from using this information and selling it to another country. As a result, there is a need for contractual legal agreements to protect classified information and new guidance at the international level to address nuclear security for SMR.

For State-sponsored SMRs, this is not a challenge. For companies in the private sector, these arrangements need to be considered with the competent authorities to ensure that nuclear security information is appropriately handled, managed, and transmitted with third-party companies located in foreign countries. Some national restrictions may apply due to the confidentiality and the state information protection regulations.

The next section provides examples on how the security guidance and principles during the design phase can be integrated into a regulatory framework to ensure a clear, transparent and consistent approach.

G. The Integration of Security by Design (SeBD) in the Regulatory Framework

1. UK Office for Nuclear Regulation (ONR)

In 2017, ONR published a set of security assessment principles (SyAPs) [25] with supporting Technical Assessments Guides (TAGs). SyAPs provide licensees with defined security outcomes that must be demonstrated to be compliant. The SyAP states that “the licensees are responsible for leadership, design, implementation, operation and maintenance of security programs to protect the public from risks arising from a radiological event caused by the theft or sabotage...”

The flexibility provided within the SyAPs enable licensees to innovate and implement alternative approaches to security, so long as the defined outcome is met.

According to ONR definitions, “‘security by design’ is an approach that seeks to reduce vulnerabilities rather than attempting to secure or mitigate them post design. It mitigates specific threats by using an approach, design or arrangement tailored to address malicious acts.”

For example, the threat of a vehicle-borne, improvised explosive device can be mitigated during the design phase by making the building impervious to such an attack or through installing hostile vehicle mitigation measures that prevent any vehicular access within a requisite standoff distance. Inherent security is not the same as “passive security.” Inherent security can be improved by:

1. Reducing the inventory of nuclear or other radioactive materials to the minimum necessary
2. Controlling the physical state of the material by removing/minimizing their potential effects if compromised (e.g., vitrification of high-level radioactive waste, encryption of stored data)
3. Application of engineering, administrative, or technical security measures

Security Hierarchy of Controls

Figure 7: Diagram on the Security by Design Hierarchy of Controls. Source: Office for Nuclear Regulation [25]

The above ONR diagram provides examples of controls that could reduce the need for, and reliance on, protective security systems. It also displays the continuum between the effectiveness and costs associated with the controls. The publication of these key security principles and definitions set the

foundation of the outcome-based approach. The recognition of these security fundamental principles described in the regulatory framework is considered a best practice.

Table 2: ONR Fundamental Security Principles and Key Security Plan Principles

Fundamental Security Principles	Key Security Plan Principles
1 - Leadership and Management for Security	KSYP 1 Security by Design
2 - Organisational Culture	KSYP 2 The Threat
3 - Competence Management	KSYP 3 The Graded Approach
4 - Nuclear Supply Chain Management	KSYP 4 Defense in Depth
5 - Reliability, Resilience and Sustainability	KSYP 5 Security Functional Categorization and Classification
6 - Physical Protection Systems	KSYP 6 Codes and Standards
7 - Cyber Security and Information Assurance	
8 - Workforce Trustworthiness	
9 - Policing and Guarding	
10 - Emergency Preparedness and Response	

Source: Office for Nuclear Regulation

For regulatory assessment, ONR developed a Generic Design Assessment (GDA) process to assess the new nuclear power station designs [26]. The GDAs allow ONR to evaluate safety, security, and environmental implications of new reactor designs separately from applications to build them at specific sites. The GDA process is an essential step to get a Design Acceptance Confirmation (DAC) and a Statement of Design Acceptability (SoDA) in the UK.

According to the ONR website (as of April 2019), security forms a major part of the GDA process and requires the design company to submit Conceptual Security Arrangements providing sufficient information to enable ONR to make an informed judgement of the adequacy of the security aspects of the generic design. The Conceptual Security Arrangements will ultimately form the basis of a Nuclear Site Security Plan for any licensed site using the design. ONR security inspectors work as part of the wider ONR regulatory team to ensure the design company incorporates security by design across the full spectrum of protective security measures, including physical protection, cyber and information, and personnel security.

2. USA Nuclear Regulatory Commission (NRC)

The US Nuclear Regulatory Commission (NRC) is engaged in several pre-application activities with SMR designers. In 2012, Nuclear Energy Institute (NEI) published a position paper [27] on the *Physical Security of Small Modular Reactors* to raise the issues related to nuclear security and cyber security for SMRs with the current NRC security regulations. In 2016, the NEI submitted a white paper on a "Proposed Consequence-Based Physical Security Framework for Small Modular Reactors and Other New Technologies" [28] to describe the complexity of this issue and propose an alternative approach. In this document, industry proposed that advanced reactor designers can incorporate engineered physical security systems, hardware, and features into their facilities to reduce or eliminate the reliance on an onsite armed response force to prevent radiological sabotage. The document also proposed that the NRC adopt new physical security requirements following a performance-based approach commensurate with the risk. From the industry perspective, SMRs and new reactors designs have lower risk profiles, and there is a need for more flexible regulations and security requirements to avoid unnecessary regulatory burden on applicants and licensees.

In 2017, the NRC issued a preliminary draft guidance for *Non-Light Water Reactor Security Design Considerations* [29]. This document provides a set of SeBD considerations that designers can integrate early in the design process. The intent of this document is to assist both NRC staff and future applicants and identify opportunities for resolving security issues through the facility design, engineered security features, formulation of mitigation measures, and reduced reliance on human actions. NRC design considerations highlight the importance of protecting against the DBT external assaults and for cyber security. The document contains 10 security design considerations: seven for physical security and three for cyber security. In a 2017 presentation [30], NRC staff provided good examples of Security by Design approaches and recommendations, as shown in Table 3.

Table 3: NRC Examples of Security by Design Approaches

Plant Layout – Layered Security Boundaries	Building Configuration	Physical Security Systems
Owner Controlled Area (OCA) <ul style="list-style-type: none"> Enclosed by fence (signage, lighting, etc.) Security Controlled Area (SCA) <ul style="list-style-type: none"> Inside OCA Vehicle and personnel barrier systems Alarms/assessment, standoff from PA 	<ul style="list-style-type: none"> Enhance line of sight – eliminate blind spots Harden access – walls, doors, windows, openings Limit number of entry and exit access Harden entry and exit points Separate vital equipment Compartment building areas Limit access pathways between areas 	<ul style="list-style-type: none"> Active delay barriers Automated access authorization verification Remotely control physical access Remotely operated weapon systems Deployable interdiction or neutralization system

doi:10.7290/ijns070102

<p>Protected Area (PA) Inside SCA</p> <ul style="list-style-type: none"> • Multiple delay barriers, perimeter intrusion detection and assessment system, isolation zones, engagement space • Interdict/neutralize • PA encloses the nuclear reactor building • Arrange PA, nuclear reactor building, and physical barriers to efficiently achieve security functions <p>Vital Area (VA) -Inside PA</p> <ul style="list-style-type: none"> • Limit access to VA to only those needed 		
--	--	--

Source: US Nuclear Regulatory Commission

Following the comments provided by NEI, NRC prepared ECY-18-0076, "Options for Physical Security for Light-Water Small Modular Reactors and Non-Light-Water Reactors" [31], which was sent to the Commission on August 1, 2018. On November 19, 2018, the Commission directed the staff to initiate a limited-scope revision of regulations and guidance related to physical security for advanced reactors and approved, subject to edits, a related rulemaking plan. This proposed rulemaking permits future applicants to demonstrate their safety case and technical basis. The new security requirements would be more commensurate with the risk posed by advanced reactors. The most likely focus of this revision would be to evaluate an alternative to the prescribed minimum number of armed responders (e.g., minimum of 10 armed responders) and the prescriptive requirement to have onsite secondary alarm stations. In July 2019, the NRC proposed several regulatory options for the physical security of advanced reactors [32] for public consultation with a cost benefits analysis for each alternative proposed. At the time of this article, the NRC was still considering options for the new proposed rule.

3. Canadian Nuclear Safety Commission (CNSC)

In the regulatory document *REGDOC-2.5.2 Design of Reactor Facilities: Nuclear Power Plants* [33], CNSC highlights the importance of interfaces of safety, security, and safeguards for NPP designs. Safety measures, nuclear security measures, and arrangements for the system of accounting for, and control of, nuclear material for an NPP must be designed and implemented in an integrated manner so that they do not compromise one another. *REGDOC-2.5.2* also ensures that physical protection systems and cyber security programs are considered in NPP design management and documentation. Specific security

requirements are established and ensure that designs take into account the interfaces between the safety, security, and safeguards and other aspects of the facility layout.

Under the existing *Nuclear Security Regulations* [34], CNSC considers the use of SeBD and the graded approach based on risk-informed considerations. Under its effort to modernize the *Nuclear Security Regulations* and to address evolving threats, CNSC staff intends to move toward a performance-based approach with less prescriptive requirements. This more flexible approach will allow adaptation to an evolving security environment, such as the fastest and evolving threats of cyber-attacks. The intent is to develop a flexible regulatory approach that consider radiological consequences and health impacts to the public in case of a release and to establish security levels following a graded approach.

In 2016 and 2017, the CNSC organized three workshops with multiple stakeholders [35]. One of these workshops was dedicated to SMR vendors, designers, and licensees interested in the construction and deployment of small modular reactors and the proposed changes to the *Nuclear Security Regulations (NSR)*. The industry representatives identified some key elements, such as:

- The regulations should be more performance-based, where it makes sense to do so
- The need to use a threat and risk assessment methodology as well as the design-basis threat analysis (DBTA) process as the baseline for performance-based regulation
- The need to emphasise "security by design" in the *NSR*
- The need for additional guidance or information specific to small modular reactors in remote locations related to detection, delay, and response options
- The need to consider unique features of small modular reactors, such as underground placement of an integrated reactor, a limited number of above-ground access points, inherent passive "safety features," and robust safety barriers to protect against external threats, such as aircraft crash, all of which enhance both safety and security
- The need for the regulations to provide for alternative approaches to that of an onsite security response force
- The option to propose an alternative approach based on fully engineered security and safety features in conjunction with an offsite response force, which provides a proven methodology to counter any design-basis threat (DBT)
- The need to enable or provide for the "Security by Design" approach for the security monitoring room, including whether it can be located onsite or offsite – the security monitoring room location should be based on a TRA
- The need for guidance to facilitate the identification, handling, transmitting, and storage of nuclear security-sensitive information
- The need to provide for flexibility to be able to use a graded risk-based approach for security monitoring room requirements – this would be helpful for building in the flexibility to allow for the use of advanced, proven security technology

Many of these considerations have been integrated in the new *NSRs* [34]. This project is still ongoing. CNSC is engaged in discussion with industry representatives to be able to find risk-informed criteria for nuclear security that can assist in applying a graded approach for SMRs.

a) CNSC SMR Vendor Design Review

The CNSC developed a Pre-Licensing Vendor Design Review (VDR) as an optional service for SMR developers. A VDR is a mechanism that enables CNSC staff to provide feedback early in the design process based on a vendor's reactor technology. NPP designs can include SMR concepts, advanced reactor concepts, or more traditional designs. The assessment is separated into three phases and is completed by the CNSC at the request of the vendor.

Table 4: NRC Examples of Security by Design Approaches

CNSC Vendor Design Review Phases for the Focus Area 15 B on Nuclear Security			
	Phase 1	Phase 2	Phase 3
Security elements that SMR developers should demonstrate	Facility characterization Identification and classification of nuclear materials Vital areas identification and identification of requirements Obtain national threat/DBT information relevant to the design Identify and demonstrate understanding of security requirements, regulations, codes, and standards	Description of the proposed PPS system design, concepts, roles, and responsibilities of security personnel Full evaluation of DBT/BDBT, including threat and vulnerability assessment Security of the facility (SeBD) Security of the Vital area (SeBD) Design of Central Alarm Station, Security Posts, etc. (SeBD) Preliminary Facility Security Plan Preliminary Cyber Security Plan	Demonstrate adequate integration of security system designs Programs and procedures developments Security planning and contingency plans for response forces and off-site response forces Formalized Facility Security Plan Formalized Cyber Security Plan
General security	<ul style="list-style-type: none"> Establish a program to protect sensitive and/or nuclear security information Personnel security screening, vetting process, background checks for staff and contractors 		

provisions to consider	<ul style="list-style-type: none"> • Computer security measures, protection of sensitive digital assets and electronic equipment's (ex: USB, laptops, hard drive) • Security elements of the supply chain
------------------------	---

As part of the SMR VDR process, CNSC staff review a SeBD and the interfaces with safety, in particular the robustness of structures, systems, and containment as well as safeguards for nuclear material accounting and control. During the VDR review, the interfaces between nuclear security and system engineering specialists allow for assessment of both physical and cyber security systems in a more holistic approach. 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 blended attacks.

b) Giving Access to Nuclear Security Information in the DBT for SMR Developers

CNSC also recognizes the need to share relevant nuclear sensitive information from the national Design Basis Threat (DBT) with SMR designers so they can consider credible and future threats in their design and therefore enable innovation. Providing access to the Canadian DBT (classified Secret), including aircraft impact loads and scenarios, may be beneficial for SMR developers at the preliminary design stage so they can fully realize the potential benefits of integrating design, security, and preparedness. This is important information that should be used in the early stages of the design process to optimize SeBD effectively. CNSC is also planning to develop a non-classified DBT similar to the US NRC practice to facilitate the sharing of information.

There are challenges for sharing classified information with SMR vendors, especially designers from other countries (foreign nationals), because of the requirement to possess a valid security clearance. In addition, challenges may rise for industries that support the SMR industry, as some of these support organizations or agencies are not located in Canada. Also, there is a risk that designers or vendors could benefit from using this information by selling it to a different country, or they could publish it in an open forum.

Access to nuclear security information in the early stages of the design process is one way that threat information can be considered in the design process. In the absence of threat assessment or DBT information, vendors and designers can use open-source information, past nuclear security events, recent terrorists' attacks to identify patterns and techniques, and study adversary profiles including the types of weapons and explosives and delivery mechanisms. There are other sources of information available that demonstrate the evolving threat environment, which provides insight on what to protect against (e.g.: hiring consultants with police, military, or security engineering experience). SMR developers and the operator must anticipate likely threats, and therefore, is important to share threat information to determine how much physical protection is adequate and how much security is needed.

The use of an integrated threat assessment that include both physical and cyber threats is a good practice. The RCMP Harmonized Threat and Risk Assessment (HTRA) model is an example of such a tool that could be used after the design phase [36]. This threat assessment can later be used to develop the preliminary security plan of the proposed facility.

c) CNSC Graded Approach for the Security of SMRs

To support a performance-based regulatory approach for SMRs and advanced reactors, CNSC developed and implemented technology-neutral requirements and a risk-informed graded approach. Specific security requirements are established for all stages of the lifecycle of the nuclear facility, and in particular during the conceptual design phase, to optimize the benefits of security, integrate safety and security interfaces, and reduce retrofit-cost. Because the risk profile for SMRs may be different, the CNSC regulations set out security requirements based on objectives to be met.

Following the IAEA recommendation and guidance set in IAEA NSS 13 [19] and NSS 27-G [37], CNSC is considering a graded approach based on the category of the nuclear material and potential radiological consequences in case of sabotage. In applying the graded approach, security objectives and/or requirements would be established for protecting each category of nuclear material and for preventing each level of potential radiological consequences at nuclear facilities. SMR proponents would have to demonstrate how they propose preventing acts of sabotage, how they protect vital areas, and how they propose using SeBD to mitigate the radiological consequence in case of sabotage. According to Suzuki and Kazuyuki, “to reduce vulnerabilities in the design of NPP, it is very important to introduce security by design approach in the initial stage of the NPP construction while considering interface between safety and security” [38]. For example, it is possible to reduce sabotage risk using the vital area identification methodology. Vital area identification for nuclear facilities is described in IAEA NSS 16 [39].

According to the WINS Best Practice Guide on SeBD [8]: “the key to effective – but not burdensome – regulation is dialogue between the regulator and the industry to ensure that there are no surprises.” One of the important benefits of defining the fundamental principles, in security and architecture, is that they stand the test of time [40]. The regulatory body should consider defining a set of nuclear security principles that include security by design to ensure that future applicants and current operating nuclear reactors can integrate them in their programs. A good practice for designers is to have a high-level mission or policy statement to reflect their commitment to safety, nuclear security, peaceful use, and non-proliferation.

H. 2.3 Safeguards and Security by Design (SSBD) Opportunities

As part of the regulatory framework, there are opportunities for integrating safeguards and security by design (SSBD) considerations. In this area, the protection of nuclear security information is a good example that covers both safeguards and security. Nuclear Material Accounting and Control (NMAC) requires an effective interface between security, safeguards, and the nuclear material accounting area to ensure electronic sharing of information is well protected. Some strategies can also benefit both

safeguards and security, such as minimization of nuclear material inventories, implementing intrinsic security measures, reducing the need for refueling, and using multiple barriers for NMAC. Therefore, there are important safeguards and security functions that can be addressed during the conceptual design, and opportunities for synergies. According to Hedbitch et al., “SSBD can improve timely, efficient, and cost-effective integration at each stage of the nuclear facility lifecycle, and they must be effective during the conceptual design as well as in later phases” [41].

In 2014, S. Demuth and F. Badwan [42] shared the results of their focused study on developing a methodology for integrating safety, security, and safeguards (3S). This study was based on lessons learned from the U.S. NRC safety/security interface requirements for NPPs. This three-step process consists of:

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 independently with the security design and the safeguards design
3. Integrated safety/security and safety/safeguards designs are combined into a fully integrated safety, security, and safeguards design. At each step, there is a sub-process to ensure that safety or security requirements do not compromise the proposed design solution and vice-versa

Figure 8: Three Step Process for Integrating Safety, Security, and Safeguards during Design

Source: S. Demuth and F. Badwan [42]

In 2015, Badwan et al. [43] published a discussion paper on the work completed by the U.S and Russia to develop a common approach for SSBD/3S for consistent application to SMRs located anywhere in the world. This approach is intended to lead to better proliferation resistance and physical security design features for SMRs. The authors provided examples of SMR Design Considerations for Security and MC & A/Safeguards (see Table 6). However, we could not find any published research or guidance document linked to this bilateral initiative.

Table 5: SMR Design Considerations for Security and MC&A/Safeguards Developed by USA and Russia

SMR Design Considerations for Security	SMR Design Considerations for MC&A/Safeguards
<ul style="list-style-type: none"> • An underground or a shallow buried hardened structure may provide excellent protection against large explosive and aircraft impact. • Simplified active and passive safety system design results in a limited number of vital areas. • Passive safety features can increase delay times, when analyzing effects on nuclear systems from sabotage events. • Smaller fission product inventory implies smaller radiological releases. • Long refueling period results in less frequent opening of reactor core, hence, less opportunity for sabotage and material diversion events. • Replacing the entire reactor core and pressure vessel with a factory-manufactured integral unit minimizes onsite handling of core fuels. 	<ul style="list-style-type: none"> • A well-established MC&A methodology for pebble-bed fuel, which is being considered for certain advanced SMR designs, does not currently exist. Consequently, pebble fuel will likely require greater safeguards design effort upfront than conventional ceramic pellets. • The frequency of reloading fuel, the amount and time duration during storage of fresh fuel prior to reloading, its fissionable content and fissionable species will all impact MC&A requirements. <ul style="list-style-type: none"> ○ The frequency of loading will impact how often fresh fuel will be present on-site. ○ The amount of fresh fuel required for reload and its fissionable content will affect how much SNM material is at risk. ○ The length of time fresh fuel is stored will determine how long the fissionable material is at risk. • High burn-up fuel, while desirable for economic reasons, will produce higher Pu content in the used fuel. This higher Pu content may make the used fuel more attractive for theft. On the other hand, higher burn-up implies a greater concentration of fission products which can make the fuel less attractive for theft. • Some SMR designs (Hyperion is one example) do not need onsite re-fueling. Instead, the entire core is removed at the end of fuel life, which may significantly reduce the MC&A requirements.

Source: Badwan et al.(2015) [43]

In 2013, [Méndez](#) and [Middleton](#) from Sandia National Laboratories published a handbook on Integrating Safety, Operations, Security, and Safeguards (ISOSS) into the design of Small Modular Reactors [44]. This handbook compares the traditional design process for nuclear facilities with the traditional engineering design process. ISOSS is a framework that assists in integrating and harmonizing safety, operations, security, and safeguards into the design process. The goal of this approach is to decrease the integrated lifetime cost of building and operating advanced SMR facilities. The role of integrating the 3S can be performed between the preliminary design and the final design. To be able to follow this approach, it would be beneficial to have one single nuclear regulator at the national level that is capable of integrating the “3S” in their framework and operations.

In a “3S” risk analysis for SMRs, Sandia National Laboratories *System Studies for Global Nuclear Assurance & Security* [45], experts studied the interdependencies between safety, safeguard, and security. Using a hypothetical SMR facility and generic DBT, the experts used the DEPO methodology (Figure 2) to analyze the result comparing low, medium, and high security budgets. In the SMR security analysis, they found that treating the nuclear reactor as any other commercial facility, with a low economic investment into physical security and relying on off-site response is not viable to protect against an act of sabotage. They also identified the need for an onsite armed response force, as well as adequate delay measures to interrupt the adversary and initiate a denial response strategy. SMRs in remote locations should consider investing in large delay elements and robust communication with response forces because of the unpredictable delay time for external response forces. In their conclusions, the experts challenge the efficacy of “inherent” or “passive” safety systems because of the interdependencies within the unique SMR facility designs. This research also demonstrates the need for onsite armed response forces to protect against acts of sabotage. The number and capabilities of onsite armed response forces may vary from one site to another based on the complexity of the site, its security measures to detect and delay adversaries, and other facility specific considerations (ex: remote location, time for off-site response forces to intervene, site specific threat and vulnerability assessment).

In conclusion, there are many benefits for both regulators and future applicants in integrating SeBD and SSBD in the regulatory framework. There are also opportunities for safety, security, and safeguards being integrated during the preliminary design and the final design phases. The final part of this paper will discuss remaining challenges for the security of SMRs and ethical questions that need to be considered by the international community.

1. *The Longer View, Challenges, and Additional Thoughts*

The following section explores some outstanding challenges and ethical questions of nuclear security for SMRs. Some SMRs are still in the early stages of their designs. Industry is lobbying for more flexible requirements to provide alternatives to reduce the regulatory burden and costs. Some designers propose new technologies that allow remotely operated nuclear facilities with the objectives of saving cost and reducing the reliance on people by reducing staffing. Some countries, like Russia and China, are building floating (offshore) SMRs to provide electricity in remote areas. The same technologies can be

used by any Member State to power remote military bases, submarines, and military ships. This might inadvertently increase global militarization and potential “nuclear” militarization. The industry would prefer that “security by design features” such as engineered barriers, underground location of critical operational components, and inherent passive safety barriers be recognized as alternatives to an onsite armed nuclear response force. Can the next generation SeBD strategies and technologies compensate for the need of an armed security response force? Will these new designs meet international nuclear security conventions? Can SMRs be safe from hackers? Will remotely operated and automated security systems, drones, or robots be effective for timely response? Let’s open the debate and share some thoughts.

I. Q1: How much engineered security is enough to avoid the reliance on armed onsite nuclear response personnel to interdict or neutralize the threats?

Context: Facilities can build-in active and passive security systems that allow one to neutralize, delay, and incapacitate human threats without any human security presence. There is no need to “reinvent the wheel.” Designers in ancient Egypt used mazes, fake tunnels, and secret chambers as anti-theft countermeasures¹. They tried to camouflage the assets (i.e., target) locations and obstacles to deter thieves and tomb raiders. These sites were located in remote locations with limited or no presence of security guards. Unfortunately, most Egyptian tombs have been broken into and their contents stolen. Many security techniques used in prisons, military bases, banks, and other critical infrastructures can be adjusted for use in SMRs. For example, traditional SeBD techniques mentioned in section 1 can be integrated in SMR design such as:

- Improving line of sight and eliminating blind spots around the facility
- Hardening the target (e.g., doors, windows, large openings, underground pathways)
- Limiting the number of egress points ways to create checkpoints or security choke points²
- Hardening entry and exits points, removing potential breaching equipment and/or vehicles, compartmentalizing the building areas to create security zones
- Limiting the number of pathways between areas, minimizing the number of targets, relocating targets underground

Some SMR designs will use a smaller reactor core size to generate lower power density. They will have inherent passive safety features that also benefit nuclear security. They will be located below grade or use in-ground construction to mitigate potential radiological consequences from aircraft crash or

¹ The use of deadly booby traps in pyramids is a myth, however in warfare studies, booby traps were used as guerilla strategies. These measures could not be used in a SMR or NPP environment because of the safety hazards for workers and potential maintenance issues.

² The use of chokepoints is a strategy to force the adversary toward a specific pathway that will expose them to line of fire by the security response force.

terrorist attacks. Therefore, they will be built to slow potential emergency situations or accidents and have a smaller footprint.

Future, innovative SeBD practices can include the following: A) security man traps, B) active and passive dispensable barriers, C) unmanned aerial vehicles (a.k.a. drones), and D) remotely operated weapons systems (ROWS). Using effective defensive tactics and strategies will also support the SMR security program that would rely on a limited number of armed responders, for example, hardening fighting positions such as bunkers, safe rooms, strategically located ballistics shields, or firing platforms. The next section will briefly describe these new innovative technologies and approaches that could be leveraged by SMR designers and operators.

A) Engineered Personnel and Vehicle Interlocks (a.k.a. Security Man Traps)

Person traps are used in physical security to separate one area from another to prevent unauthorized access. They are generally used to verify credentials and prevent tailgating and piggybacking. They are implemented in prisons, banks, jewellery stores, airports, or other facilities. Person traps can be designed as interlocking doors, so that when one door is unlocked, the other is automatically secured [46]. When the access control design is well integrated with the facility layout and physical environment (e.g., topology), it can increase the design's effectiveness.

With security person traps, designers can integrate lockdown systems or automated mechanisms to secure the facility during an attack (see Figures 9, 10 and 11). They may also incorporate rapid entry systems to enable off-site emergency responders to enter the facility when no one is available to provide access. These systems must be carefully evaluated to ensure they cannot be exploited by adversaries or insiders. In both applications, these systems must be integrated with safety and other emergency requirements. Another example is automated lock down systems at egress points that are activated upon detection of nuclear materials by radiation monitors. This design detects and prevents unauthorized removal of nuclear materials.

Figure 9: Hardened turnstiles installed in between two areas to form a personnel portal. Entry authorization uses biometric hand geometry and individual code. Radiation portal monitors at the exit point automatically lock down to present egress if they detect radiation.

Photograph from CNSC

Figure 10: Security screening area designed to prevent unauthorized access without proper search for weapons, explosive and contraband.

Photograph from Darlington, Ontario Power Generation site.

Figure 11: Security vehicle search area designed to prevent forced entry penetration of vehicle without being searched.

Photographs courtesy of Chalk River National Laboratories.

B) Active and Passive Dispensable Barriers

Active dispensable barriers can, once activated, stop, incapacitate, or delay an adversary from accomplishing their task [12]. They are used as vehicle barriers or to slow down an attack. New technologies such as mobile vehicle barriers are becoming more reliable and easily deployable.

Figure 12: Castle drawbridge.

Source: Wikipedia

Figure 13: Active barriers designed to prevent forced vehicle entry using defense in depth approach. The system is located far from entry points for safe stand-off distance.

Photograph from Ontario Power Generation Facility in Pickering.

A good SeBD technique was used in the 16th century with a drawbridge at the entrance of medieval castles (See Figure 12). The drawbridge would be raised to form an additional barrier in case of an attack. It would be backed by one or more portcullises and gates to form a person trap. Access to the bridge would be designed to be resistant against attacks and there would be arrow slits (e.g., murder holes) in flanking towers and/or holes in the ceiling where rocks, tar, or boiling oil could be dropped on the attackers. Medieval castles were built with multiple SeBD techniques, such as narrow gateways with sharp turns to slow the attackers and other defence in depth techniques. The same principles can apply for SMRs, for example, using hardened guard posts (e.g., bullet and explosive protection) at entry and exit points, hardening tactical locations inside the protected area, using security person traps for both personnel and vehicles, and using innovative non-lethal force to interdict or neutralize adversaries.

SMR physical security systems can integrate active delay barriers with an automated access authorization verification system [46]. To reduce the cost, there is the potential of implementing remotely operated access control systems integrated with surveillance cameras to manage physical access to the site (see Figure 13). There is also the potential to use remotely operated lethal and less than lethal weapons systems. These devices can be deployed to interdict or neutralize adversaries if they attempt an intrusion within the restricted facility. These remotely operated systems are usually connected to the onsite Central Alarm Station. However, we could not find any publicly available studies on the use of non-lethal remotely operated systems.

Other dispensable barriers can have the effect of isolating the adversary visually, acoustically, or both (e.g.: smoke or fog, sirens, blinding strobe lights). These barriers can be activated by a member of the security force remotely or by a sensor and are designed to slow down the adversary. Therefore, it is

doi:10.7290/ijns070102

essential to have an effective response force to respond to the event in a shorter time than the dispensable barrier(s) delay the threat [12]. As mentioned in draft IAEA NST 55, “dispensable material is normally stored in a compact form, and through a chemical or physical reaction, is expanded to fill the opening or space during an attack” [47]. The properties of compact storage and rapid expansion make dispensable barriers systems attractive in certain applications.

C) Unmanned aerial vehicles (UAVs) or unmanned aerial system (UAS)

Emerging technologies may have an impact on future SeBD applications. The use of automated security systems, advanced robotics, artificial intelligence, facial recognition, Unmanned Aerial Vehicles (UAVs), and/or remotely operated systems may be used to replace or augment traditional security personnel to detect, assess, and respond to alarms or intrusion.

New drones can be equipped with cameras, radiation sensors, or heat sensors and can be assigned to perimeter monitoring, radiation detection, and emergency response. Drones can also be used to detect and take down other drones before they enter the restricted air space over the nuclear reactor [48].

Source: IFSecglobal

The evolution of surveillance cameras in the past decade is a good example of systems that are now remotely accessible from anywhere in the world if there is an internet connection. New video monitoring systems are rapidly changing to integrate artificial intelligence and UAVs. UAVs can supplement existing fixed video technologies used to monitor protected and/or restricted areas. They can also be used for tracking and monitoring intruders [48].

The use of drone detection and defense systems is promising. They allow better and more flexible assessment capabilities and can cover a wide range of areas difficult to access by humans. They also limit the exposure of security officers to possible adversary attacks [48]. However, according to a Chatham House report [49], the technology is still in an early phase of development and needs to overcome the challenges related to battery power drainage, agility, speed, and real-time image processing. Also, there are safety concerns with the use of drones flying over nuclear plants. In addition, UAV/UAS need to be tested in different weather conditions. Their legal use must also follow the limitations set up in state regulations [47].

Remote video monitoring is starting to occur using robotics and drones in areas that lack fixed cameras because they are not feasible due to the location or power availability. Improved analytics and automation in camera technologies allows real-time alerts when an activity is taking place and requires

doi:10.7290/ijns070102

action. However, there is still an essential element that integrates a human decision in the monitoring, assessment, and communication operations. Unmonitored or partially monitored camera surveillance systems are ineffective if not properly integrated with the human element. For SMRs, the UAS will have to be operated by a pilot in the CAS or in the field. In some countries they have to be operated under a line-of-sight rule. Also, the use of surveillance technologies and the protection of privacy must be carefully balanced. The implementation of a UAV program to enhance nuclear security operations should be transparent and used in accordance with applicable laws and regulations.

D) Remotely Operated Weapons Systems (ROWS)

ROWS are widely used by the military in conflict zones. If properly installed and integrated within the design, it may be an option to consider for remote SMRs applications. These security systems must be well integrated in a comprehensive security program. There is also a need for effective performance testing, human factors/user validation, and assessment to ensure the system cannot be compromised against both physical and cyber-attacks. If drones are used for nuclear security applications in Canada, they will need to be tested in the field and evaluated for human factors to demonstrate to CNSC (the regulator) that they can be operated effectively, safely, and securely for their intended purpose.

An example of such a design is the patented prototype RoboGuard [50] that can be deployed rapidly around a security perimeter fence to assess the cause for an alarm. This unmanned robot can be integrated with drone technologies for video surveillance and assessment to follow intruders inside the restricted area using analytics (see Figure 14). The technology is still in its early stage of development and testing needs to be conducted under extreme cold and snowy Canadian winter conditions.

Figure 14: Senstart robot for unmanned perimeter surveillance. RoboGuard travels on a monorail for patrols that could be integrated with drones for video surveillance applications along with security perimeter.

Source: Senstart [50]

E) SeBD of Central Alarm Stations

For SMRs, the role of the Central Alarm Station (CAS) will be critical and multipurpose. The surveillance system must be adequately integrated with the access control and intrusion detection systems to facilitate the immediate assessment of alarms. The CAS team is usually responsible for preventing emergencies, detecting threats, and dispatching response forces to events, so they can support normal daily operations. The CAS design must consider human factors and follow industry codes and national standards and requirements. Video monitoring and assessment should be a team effort and this critical function will continue to rely on humans to make critical decisions. Technological solutions and advanced analytics will continue to facilitate the human decision-making process and task performance. Because of its role and multi-functions, a CAS and secondary alarm stations will be necessary for advanced nuclear reactors. The primary CAS must be within a protected area. The secondary stations should not be located in the same building, so the site can maintain critical functions if the first CAS building is compromised. For the CAS, the team and the human element is the most critical component for its effective application. Additional guidance and design requirements for CAS can be found in the IAEA NST 55 [47]. Security personnel protecting nuclear power plants have a need to maintain situational awareness on threats; as such, technology and information can assist in collecting, validating, and analysing information from a wide variety of sources to augment security intelligence and support planning, operations, and decision making. SMR will need communication and internet access to facilitate the daily operations and maintenance activities. Also, tamper-resistant tracking technology should be installed on all nuclear security personnel radios and vehicles to allow CAS operator to have real-time situational awareness.

F) SeBD of Vital Areas

In remote locations, vital areas that are located underground inside a reactor building and its containment are designed to provide an additional layer of security to prevent malicious acts and sabotage of the SMR. Another example of layered design is having a containment structure built over the small nuclear plant. In these specific circumstances, the security requirement for the protection of vital area(s) can follow a risk-informed decision-making process to recognize these alternative practices and to follow a graded approach. As mentioned by WINS, “automatic safety measures can also help to minimize consequences of sabotage, but only if they cannot be disabled or subjected to tampering by adversaries” [8].

Designers or vendor should assess how technology can be leveraged to support the SMR operations, enabling the communication of information and the security of the site, including the protection of nuclear materials and workers.

Discussion: Remotely Operated Weapons System (ROWS) are used in military applications. They can be equipped on ground combat vehicles or other combat platforms to engage targets without leaving the protection of their vehicle, watch towers, or reinforced security post. They offer significant force multiplication, increase response efficiency, and allow improvements in delay and response [45]. According to the Sandia National Laboratories website, one operator can use multiple weapons, and the systems can reduce operator inaccuracy and fatigue making it more efficient and effective in neutralizing adversaries [51].

There are serious concerns raised on the use of lethal autonomous weapons systems referred to as Lethal Autonomous Robots (aka LARs or Killer robots) [52]. Mr. Walter Dorn, a professor at the Royal Military College & Canadian Forces College, has urged limits to ensure there is always an element of human decision-making in carrying out lethal force [53]. In a speech delivered in 2015 on the next generation of drone warfare, Professor Dorn identified five “A” reasons why LARs are dangerous and should never be developed or deployed: Accident, Accountability, Access, Availability, and Acceptability. No matter how advanced the technology, there is always the potential for glitches and malfunctions with technology that could harm soldiers or civilians [53, 54].

According to a panel of expert on technology and innovation in peacekeeping missions [55], the deployment of such technologies will present a serious threat to human liberties and human rights. The same issues will arise with the increasing use of surveillance technologies and UAVs and the invasion of privacy. A robot cannot be put in jail, and there will be difficulties in punishing them and making them accountable for their actions. Cyber security, hacking of the machines, also represents a serious potential vulnerability. If the technology is made commercially available, there will be a proliferation of

its use and increased fear of its availability on illegal markets, including to organized crime and terrorist groups.

In Canada, there are legal requirements to demonstrate that the proper use of force continuum is applied. The current CNSC regulations require an element of human decision-making in carrying out the use of lethal force. Armed Nuclear Response Force (NRF) members have to go through rigorous training, qualification, and testing for use of firearms and non-lethal weapons. They also have to pass psychological, medical, and physical exams and enhanced security vetting. Through the conduct of mandatory security exercises and drills, the performances of nuclear response teams are tested against DBT adversaries regularly.

There are future technical discussions needed concerning the potential implementation of this technology, and performance tests are required to verify the effectiveness of remotely operated systems and interfaces with off-site response forces.

There is an important dilemma that blurs the lines of what is right and what is wrong.

In 2016, the police used a robot to kill an active shooter in Dallas [56]. According to several press articles, this police bomb disposal robot used deadly force against the suspect after five police officers were murdered and seven other wounded. There is a very great temptation to use any tool necessary to save the lives of police officers and civilians.

Figure 15: Top: Police robot used to kill an active shooter. Martin Godwin for the Guardian [56]. Below: Modular Advanced Armed Robotic System

Currently, there is no legal framework on the use of force by robots, and there are no regulations or international conventions. Similar robots have been used by military forces to deliver explosives. These new technologies can be used for SWAT situations, Hazmat calls, or bomb threats. There is always a military or law enforcement officer controlling the robot's action (Figure 15). Will these systems be fully autonomous, and are we ready for them to make their own decisions?

Source: PRNewsFoto/Foster-Miller Inc.

Will Canada accept the use of robots or an automated security system that can kill, wound, or incapacitate adversaries? This is doubtful but not irrelevant. Currently the United Nations does not have a treaty to ban the development or use of fully autonomous lethal weapons.

That being said, other countries may be willing to use some degree of human control over lethal autonomous weapons. In remote locations, the time of response for off-site agencies will be much greater, SMR designers will have to consider additional delay measures to increase the delay time. Security systems that can incapacitate or distract the adversaries may be considered to slow down the attack. There will be a need for creative delay systems ahead and a need to demonstrate the effectiveness of these defensive measures.

Engagement with industry stakeholders will be an important element in addressing these security challenges and the proper use of this technology. As mentioned by WINS [8], design choices should provide a security margin proportionate to the risk without excessive disruption of business and, in these cases, without comprising nuclear safety and/or security.

Finally, there is an inherent need to have onsite armed nuclear response personnel to interdict and/or neutralize threats from the DBT. A robust and flexible operational security response will be required no matter what intrinsic safety measures are added to the reactor design. But how many nuclear armed response force personnel are needed?

J. Q2: What is the appropriate number of security personnel for SMRs?

Context: Reducing the number of security personnel is one way to reduce cost, which is considered vital for the economic deployment of SMRs. SMRs developers argue that inherent safety and security characteristics of SMRs and the integration of SeBD can form the basis for reducing the size of the required security response force.

In 2013, the Union of Concerned Scientists published a paper titled “Small Isn’t Always Beautiful: safety, security and cost concerns about SMRs” [57]. In this report, Edwin Lyman forecasted the issue of SMRs vendors convincing the NRC to have some relief in safety and security areas. SMR vendors are vigorously seeking regulatory relief to allow them to meet weaker safety and security standards. The document also states that reducing the security force at a nuclear reactor would appear to be “penny-wise but pound-foolish.” According to Lyman, security labor cost may be significant, from 15 to 25 percent of total operations and maintenance (O&M) cost for an operating nuclear reactor. However, they are not the dominant contributor to the overall O&M costs. In comparison to total plant staffing, the security force is approximately 20 to 30 percent of the total workforce. Their mission is to protect the entire plant, personnel, and surrounding region.

Discussion: This report raises the following, legitimate concerns about reducing the minimum number of armed nuclear security forces:

- If the nuclear reactor protective response team numbers are less than the number of armed attackers identified in the national DBT, the probability of a successful neutralization is significantly reduced and may compromise the nuclear facility security. In practice, the minimum number of armed nuclear response force should be equal to or greater than the number of adversaries identified in the national DBT. This does not include the other unarmed nuclear security personnel responsible for searching people and/or vehicles entering the site and manning the CAS 24/7.
- It is a fundamental mistake and danger to underestimate an opponent (Lao Tzu). Given that the armed attacking force is assumed to use multiple groups and diversion tactics, it would be very difficult to defend the facility protected area with fewer armed security personnel, and even harder if it contained multiple SMR plants (e.g., multiple targets) within the protected site.
- Underground siting may enhance protection against some attack scenarios, but not all. A well-planned attack could cause a loss of coolant event. Other important systems such as turbines, electrical switchyards, generators, or cooling towers, will remain above ground, where they are still potentially vulnerable (Lyman, 2013) [58]. If the SMR uses remote central alarm stations, this will also make it an attractive target for adversaries. These targets may not be considered vital areas, but they can compromise the safety and security of workers and the nuclear plant if they are destroyed.

With future SMRs, there will be a need to identify the minimum staff complement, which will include the minimum number of armed and unarmed security personnel. This will depend on the facility application, size, access points, number of vital areas and SMRs, and the number of staff working at the nuclear plant to support operations and maintenance activities. All of these factors will need to be taken into consideration.

SeBD should consider options to increase the effectiveness of the Protective Force in the event of an attack and *should not* be used to reduce the reliance on the Protective Force. SeBD should augment the rate of survivability of the Protective Force. For example, using reinforced hardened guard posts, ballistics resistant windows, armored response vehicles with turrets, and mobile shields located in strategic locations. Safe rooms should also be considered to protect staff during lock downs. SeBD should provide options that would increase the rate of survivability in case of an attack.

The number of armed security response personnel needs to be well researched and analyzed in accordance with the DBT to enable an effective and timely intervention. The use of probabilistic risk analysis tools, simulators or computer models such as EASI (Estimate of Adversary Sequence Interruption) should be used to support the analysis. The SMR designers and operators should also conduct detailed job/task analysis to determine the skills and knowledge required by employees and how many people will be needed. In remote areas, the on-site nuclear security response force needs to

be autonomous and self-sufficient because of the longer response time for off-site forces. The number and size of the security force should be carefully assessed, evaluated, and tested with on-site security drills and exercises. But how will this methodology apply for floating (offshore) SMRs and/or SMRs in remote areas?

K. Q3: What are the security considerations for floating (off-shore, remote SMRs and transportable SMRs?

Context: In the traditional approach, a nuclear facility must be able to counter the number of adversaries and their techniques described in the national DBT. In general, the DBT applies to facilities that use, store, and transport category I and II nuclear materials but it can also be used for operators handling Category III nuclear material. Based on past terrorist attacks and security incidents, the adversaries' training, weapons availability (including breaching tools), vehicles, explosives, and cyber capabilities must be considered. The size and the remoteness of the SMR is one factor that can increase or lower the risk profile. However, what criteria can be used to decrease the risk profile and security requirements to follow a graded approach? If the site is small, in a remote area where the threats are very low and the radiological consequences are less harmful for the population, can this be considered a criterion to reduce regulatory burden or security requirements? In Canada, communities in the far north that will rely on SMR for power would be more vulnerable in case of a denial-of-service attack in the middle of winter. If the SMR is shut down remotely it would have more devastating impact to the population who are dependent on it for their electrical power supply.

The first Russian floating nuclear power station being transported from Murmansk (source: Elena Dider, Wikimedia commons)

Westinghouse's, eVinci micro reactor and Westinghouse

For floating (offshore) and remote SMRs, the geolocation of the site and the difficulty of getting physical access can present both security benefits and disadvantages. It also makes it more difficult to transport nuclear material to the location and divert it. The likelihood of the threat may be different and significantly lower. There are also concerns related to the vulnerabilities of external communications link and cyber-security. It will be harder for adversaries to get access to the site, but it will also be difficult for the off-site security response forces. For a theft scenario, adversaries will also have challenges escaping without being caught. For a sabotage scenario, the impact and consequences may be lower

doi:10.7290/ijns070102

because of design mitigations strategies. Will radiological consequences in the case of sabotage be acceptable? Where is the line between manageable radiological consequences and unacceptable radiological consequences? From a regulatory perspective, there should be no compromise for safety, security, and the environment. There is also a greater need to ensure that SMR cannot be shut down, be made vulnerable to cyber-attacks, or succumb to denial-of-service attacks.

Source: Illustration from NuScale Power

Discussion: In practice, the security risk assessment should consider the threat from insiders and the potential for blended attacks (e.g., simultaneous physical and cyber-attacks). It should also consider the size and location of the SMR in its analysis. The security risk assessment includes an adversary path analysis and a vulnerability assessment to support risk-informed designs and decisions. Security measures should also be tailored to the specific threat and risk related to the site and application. The regulatory system applies the same requirements and approach to all nuclear facilities based on the quantity and enrichment levels of the nuclear material. If the approach for security is tailored and assessed on a case-by-case basis, it would go against having a consistent and harmonized system. Some experts also believe that it would create weakness in the nuclear security regime because the sites would not be treated the same way, creating weaker sites that could be targeted because the security measures are lower than for the larger, current nuclear plants.

For floating (offshore) or remote SMRs, will limited bandwidth and the lack of interoperability be a significant challenge for nuclear security? Currently, there are concerns with 5G technology, and there are potential issues with SMR modules built in foreign countries who own and maintain the technology associated with them especially in security and safety systems. How does the licensee know that a 5G or other potentially risky technology has not been installed?

There are also potential cyber security threats existing with satellite use. Dealing with various kinds of security threats could introduce additional tasks for an operator, on top of the operational tasks, unless a dedicated individual is assigned to security matters. For very small, remote facilities this may not be done. Such an issue needs to be considered in the staffing analysis and in the Integrated System Validation (ISV) exercise done for the control room. Security issues are not currently considered during ISV. For remote operations or reduced operator staffing this could be an issue that warrants further thought.

In order to build in security by design, there might have to be much more analysis work done at the conceptual and preliminary design stages than is currently done. There are bound to be human factor issues of concern, yet vendors have not discussed this to any degree.

There are remaining challenges for mitigating insider and cyber threats. With the current trends in technology, the evolution of Artificial Intelligence, robotics, and more autonomous systems, there is also an increase in cyber risks to be considered. It is not a choice but a trade-off to replacing humans with technologies. Reducing human involvement may reduce some cost, but it will also reduce human benefits and adaptability. The increased use of technologies will transfer the risk(s), and these decisions will need to be carefully reviewed since it does not mitigate the threats.

There is a need to conduct comprehensive threat and risk assessments and site vulnerability assessments for nuclear power plants. There is also a need to establish risk-informed criteria to apply to a graded approach for the security of SMRs. However, the nuclear power plant (SMR) will need to meet the established regulatory requirements, including the DBT.

Another challenge will be the reliance on off-site monitoring stations. Current regulation prescribes the existence of a Central Alarm Station inside the Protected Area. In some countries, the secondary alarm stations can be located inside or outside the protected area. This raises cyber security concerns and could also be viewed as a vulnerability in the design since the CAS or SAS can be attacked.

Finally, transportable SMRs or transporting “key-in hand” SMR modules or reactor core may pose a challenge but putting nuclear reactors on ships is not new. In this area, we can learn from the Russian experience “Akademic Lomonosov” with nuclear-powered icebreakers. This Russian icebreaker has two reactor units, MDT-40 capacity of 35 MW and will provide reliable power to Chukotka. It uses a nuclear reactor that has been tested over several years. This floating NPP has been designed to be used in cold and harsh weather conditions for the North region. To avoid legal conflicts with other States, the fueling operations are conducted in close proximity to the location where it is used [59]. In addition, to avoid any legal or juridical issues when crossing neighbouring waters/territory, the transport of the reactor is carried out without the nuclear fuel on board to meet the wishes of neighbouring countries. This is a good example that removes the existing legal conflict by acting from the principle of good relations with regional countries and partners. The manufacturer manages the disposal of the nuclear waste, and maintenance is provided by the Russian nuclear industry. In fact, nuclear reactors have been placed on ships and submarines for more than 50 years.

L. Q4: Will SMRs be used for peaceful purpose only?

Context: A report written by Robitaille. G from United States Army War College, titled *Small Modular Reactors: The Army’s Secure Source of Energy?* [57] explores the use of SMRs for critical military facilities

and their potential as viable sources of secure energy in the future. In this research, the author explains that military facilities are dependent on electricity from the grid which could be subject to compromise because of the age of the infrastructure, damage from natural disaster, and the potential for cyber-attacks. These installations use diesel-powered generators as temporary backup. These critical facilities have a need for a secure and reliable source of energy.

Discussion: The concept of SMRs is not new for the US Department of Defense (DOD). US military engineers built a nuclear reactor for a secret underground city project in Greenland back in the 1950's which was later abandoned in the mid 60's [60]. The reactor was up and running for 33 months before being deactivated and removed. According to Robitaille, the US army built eight nuclear power plants from 1954 to 1977. This program was shut down because of the cost. Many of the nuclear power plant designs were based on US Naval reactors. The recommendation from Robitaille is that DOD needs to consider SMRs as a safe and secure alternative source of electricity. The same conclusion can be used by any Member State who wishes to provide a reliable and secure source of electricity to remote military bases.

This study raises the concern for non-proliferation and the rise of SMRs for military applications. This is outside the scope of this research but will remain a challenge for international security and could be a political issue for countries embarking on nuclear programs. SMRs can support future transport or space applications. Once they are built and deployed, they will eventually be available to the global market and sold to international buyers. So, the answer to the question is no. Once commercially available, SMRs can be used for both peaceful and military applications. Therefore, there is a need for the international community and the IAEA to discuss non-proliferation and peaceful use of SMRs. In particular, because many SMRs will rely on HEU.

M. Q5: Will SMRs be safe from hackers?

Context: In 2015, a Chatham House report on *Cyber Security at Civil Nuclear facilities: Understanding the Risks* [49] exposed the growing risk of a cyber-attack on civil nuclear facilities because of the increased reliance on digital systems and the growing use of "off-the-shelf" software. The report breaks the myth that nuclear facilities are "air gapped" (isolated from the public internet). Nuclear facilities such as SMRs may use internet connectivity such as Virtual Private Network (VPN) connections. These VPN connections, if they are not secured, can be exploited by hackers. There is also a risk of malicious access through portable devices such as flash drives within the secured or isolated network. Therefore, insider threat mitigation strategies and mitigation controls need to be considered in the design of the cyber security program. The human element plays a critical role in security to minimize insider threat.

Because SMRs may be built in factories and assembled remotely, there will be cyber vulnerabilities in the supply chain which may increase risk of safety or security equipment being compromised or tampered with. Traditional nuclear plants are built on site. New SMRs protocols may benefit from being constructed in a restricted or protected area that is subject to national laws and regulations. Since these

new modular designs can be transported to other locations, the protection of critical SMR equipment will be important to maintain the integrity of the products throughout the supply chain.

There are other cyber security risks if the SMR uses remote monitoring systems. For example, if the Secondary Alarm Station (SAS) is located outside the nuclear plant and if the operator can remotely access surveillance cameras feeds or other electronic systems, it creates potential cyber pathways for adversaries. Therefore, there will be challenges in designing remote communications for unmanned facilities and designing plant control network air gaps to the internet.

Discussion: In Canada, the Canadian Standard Association (CSA) standard on cyber security, N290.7 [61], applies to nuclear power plants and SMRs. However, there is a growing need to provide additional guidance and requirements to supplement this standard to ensure that reliable and effective cyber security measures are implemented. Is this standard adequate for SMRs? Can SMRs be designed like airplanes to be safe from hackers? Will SMR designers integrate technologies for monitoring, detecting, and mitigating cyber-intrusion and cyber-physical security events in their systems and networks? Will cyber security requirements be adequate for remotely operated systems? If an SMR is part a national critical infrastructure network, it may also be subject to enhanced cyber resilience and redundancy measures for protecting against power grid cyber-attacks. There will be a need to further explore and test a facility's cyber security capabilities to assess and evaluate its effectiveness.

N. Q6: Other challenges for licensing SMRs?

Context: C.Reirsen and A.Gomez-Cobo from ONR identified several challenges for licensing SMRs [62]:

- Regulatory oversight of off-site modular construction
- Potential for resource sharing between companies
- Potential to license separate construction and operating companies
- Prospect of separate ownership of modules on a single site
- Potential for multi-module operation by small number of operators from a centralized facility

As a result, ONR established a strategy and provided answers to each of these questions. Without summarizing the full report, there is a desire to have clear regulatory authority for overseas locations. There is also a need to implement clear “red-lines” when a licensee model involves resource sharing from different companies, especially in the capability needed to take safety decisions. ONR reaffirms the importance of human factors analysis. This also includes security staffing. Other challenges also exist for design assessment of SMRs in relation to the limited availability of evidence-based information to support regulatory decisions.

In 2015 the World Nuclear Association published and reported on *Facilitating International Licensing of Small Modular Reactors* [63]. This report identified the main issues for licensing SMRs and potential

approaches on how to facilitate a more efficient way forward. Some associated issues included the following:

- Issues of fabrication at a factory in one country for installation in another country
- Issues of several factory locations in a country for installation in another country

Discussion: The report is silent on nuclear security challenges and issues. The report proposed an in-factory certification process which would be recognized at the international level by national safety authorities, similar to the certification process currently used by the aircraft industry. From a nuclear security perspective, this in-factory certification process would reduce potential cyber security risk and the potential for tampering with critical safety equipment.

Another challenge will be the increased insider and cyber security risks with remotely operated systems by third party companies and in the supply chain.

Ostendorff, W. and Cubbage, A. [64] from Stanford University exposed other SMR policy issues. Industry has proposed some alternative licensing strategies to reduce the control room staffing and the emergency planning zones. Since that time, NRC has been working with NEI, prospective applicants, and other stakeholders to provide additional clarity to these issues. The following Table describes the minimum staffing complement that is less than currently required by NRC regulations based on the number of units that can be controlled from one common control room. In SECY-11-0098, NRC concluded that evaluating an applicant operator staffing exemption request is the best short-term response.

Table 6: Minimum requirement per shift for n-site staffing of nuclear power plant units by licensed operator and senior operators

Number of nuclear power units operating	Position	One unit	Two units		Three units	
		One control room	One control room	Two control rooms	Two control rooms	Three control rooms
None	Senior operator	1	1	1	1	1
	Operator	1	2	2	3	3
One	Senior operator	2	2	2	2	2
	Operator	2	3	3	4	4
Two	Senior operator		2	3	3	3
	Operator		3	4	5	5
Three	Senior operator				3	4
	Operator				5	6

Source: US NRC 10 CFR 10.50.54

For security requirements for SMRs, Ostendorff and Cubbage mention that security strategies will be reviewed on a plant-specific basis using the existing regulatory requirements and guidance. However, since 2015, the NEI and NRC have been working together to find alternative solutions for nuclear security. This is being done to recognize security during the design process, to increase reliance on engineered systems, and to reduce reliance on operational requirements and staff. By optimising the site layout for security, reducing the number of vital areas, and incorporating safety systems underground and within containment, there may be room for prospective applicants to reduce the number of on-site nuclear security personnel with the future rule making proposed by NRC in 2019 [32].

Reducing the number of operational staff can also increase insider risks. The operator will rely on few individuals with more roles, responsibilities, including authority, and multi-function job positions. These individuals could become “super insiders.” When the human element is the weakest link in the security chain, it becomes a more attractive source of information for adversaries. Understanding and monitoring the insider threat challenge will therefore remain an important element of the SMR physical and cyber security program(s).

III. Conclusion and Recommendations

SeBD is a conceptual approach that provides for the integration of security at the earliest stages to mitigate malicious acts, and it should also be part of the facility lifecycle. It is a holistic approach that

doi:10.7290/ijns070102

should be integrated with operations, safety, and nuclear material accounting and control, so they are mutually supportive and avoid conflicts. Security for SMRs includes both physical and cyber security measures. It also includes operational security practices, personnel security screening, and programs to protect nuclear/sensitive security information.

The principles and requirements for SeBD should be set out in the nuclear regulatory framework and regulations. The threat assessment or DBT and relevant nuclear security requirements should be provided to the operator/designer or vendor for the development of a comprehensive set of nuclear security requirements for use during the design of the facility. Because of the sensitive nature and confidentiality of the DBT, competent authorities must take adequate provisions to protect the information.

The ONR, US NRC, and CNSC have developed specific guidance for the security of SMRs and advanced reactors recognizing the benefits of integrating security by design and key fundamental security principles early in the process. The economics to build and sustain operations of SMRs is considered to be a major challenge for industry representatives. This includes security cost. For example, some SMR designers consider security early in the design phase such that they can design and build vital areas underground to minimize security risk. This strategy can provide good protection against large explosives and aircraft impact. However, further studies are needed to assess its effectiveness against sabotage attacks.

This paper discussed some challenges and security dilemmas with SMRs. The traditional industry may be assuming that designers and vendors are working in such a way as to present a design that meets the current highly stringent requirements and regulations for security. However, designers and vendors are not operators and may not bound to an operating licence. Designers and vendors are able to design and build part of the equipment in one country then sell to another country. They may be bound on a contract established to produce the design for an operating organization. This creates quality control issues, export complexity, competition, and opportunities for corporate espionage and sabotage.

Anticipating emerging threats is essential to improve situational awareness for security personnel and decision makers. The United Nations 2014 report on peacekeeping missions and the use of technology and innovation [55] highlights the importance of leveraging current technologies to enhance situational awareness, understand the operating context, help inform personnel, and protect assets and installations. There are support tools that exist and provide real-time situational awareness, data visualization, and analysis, including basic tools to collect, process, use, and disseminate information effectively. This is essential to create an intelligence-led decision-making model to support operations. Nuclear Power Plants or SMRs equipped with UAVs as mobile intelligence, surveillance, and reconnaissance (ISR) can patrol restricted areas along the protected boundaries and enhance overall security. Modern surveillance and reconnaissance devices can be powerful tools to enhance security and collect information. Technology should not supplement the need for human presence and decision

making to protect assets but should be used to support security operations and functions and enhance nuclear security forces capabilities to detect, delay, and respond to intruders.

We anticipate that a number of these recommendations will generate discussion. It is the author's intent to provide a transparent, solutions-oriented discussion on technology as a critical enabler of SMRs.

Recommendation 1: There is a need for the IAEA to create a forum of discussion to provide clear recommendations and guidance for the security of new nuclear technologies to ensure peaceful use of SMRs.

As identified by Global Nexus Initiative (2018), there is a need to discuss security measures between designers, IAEA, and other experts on potential physical and cyber security vulnerabilities, share updated and technical information, and incorporate security in the reactor design and construction phases.

Recommendation 2: There is a need for global consensus on the application of the CPPNM and its amendment for SMRs and advanced reactors to ensure a harmonized approach on Nuclear Security. Creating a forum of discussion on technology and innovation that have a nexus to nuclear security is needed. This will develop a collaborative framework that can assist member states to make the appropriate decision in the implementation of new technology and manage effective transition to innovative technologies and/or practices to set a solid foundation for the successful implementation for new nuclear plants.

IV. ANNEX 1: IAEA NSS 35-G Nuclear Security Design Actions for Competent Authority and Operators [23]

The IAEA guide encourages the following design actions for the competent authority:

“Action 3-2: Ensure that a design basis threat or representative threat statement and relevant regulatory requirements for nuclear security are provided to the operator for development of nuclear security input for use during the design of the facility, if required.

Action 3-3: Ensure that any design modifications remain in compliance with applicable regulatory requirements for nuclear security and safety.

Action 3-4: Conduct a technical assessment of the final design of a facility to ensure that it meets applicable requirements for nuclear security and safety before licensing activities or granting authorization.

Action 3-5: Ensure that trustworthiness checks are implemented for personnel with access to sensitive information.”

The guide includes actions for operators to ensure that:

“Action 3-6: Determine the nuclear security measures based on the number and type of security areas included in the design.

Action 3-7: Implement an information security programme for sensitive information used or generated during the nuclear facility design stage.

Action 3-8: identify the category of nuclear material to be protected against unauthorized removal as well as the possible radiological consequences of sabotage in order to ensure that nuclear security design requirements are met.

Action 3-9: ensure that all organizations with nuclear security responsibilities relating to the facility should participate in facility design activities.

Action 3-10: coordinate nuclear security measures to be incorporated in the design with measures to be incorporated for other disciplines (e.g., safety, safeguards and operations) in order to compare relevant regulatory requirements, identify synergies and resolve potential conflicts.

Action 3-11: identify technologies and components (e.g., barriers, sensors and assessment systems) best suited to meet applicable regulatory requirements for nuclear security. This information should be used to develop detailed design requirements for nuclear security measures.

Action 3-12: Review all aspects of the design to ensure the appropriate inclusion of nuclear security measures.

Action 3-13: Assess the final design to ensure that it meets applicable regulatory requirements for nuclear security, as well as assess any proposed subsequent facility design changes that would affect nuclear security.

Action 3-14: Provide the final design of the systems and components that contribute to nuclear security (e.g., physical protection equipment, security related sensitive digital assets, computer hardware, and network and power equipment) to the competent authority for assessment and approval.

Action 3-15: Provide the competent authority with any subsequent design changes affecting the systems that contribute to nuclear security, as required, incorporating the concept of configuration management

Action 3-16: Account for applicable regulatory requirements for nuclear security during the design stage, including for computer security, sustainability, contingency planning, emergency preparedness, incident reporting, trustworthiness, quality assurance, nuclear security culture and nuclear materials accounting and control, as applicable.”

V. Works Cited

1. International Atomic Energy Agency, Small Modular Reactors. *Int. At. Energy Agency* (2016), (available at <https://www.iaea.org/topics/small-modular-reactors>).
2. Nuclear Energy Institute (NEI), Small Modular Reactors. *Nucl. Energy Inst.*, (available at <https://www.nei.org/advocacy/build-new-reactors/small-modular-reactors>).
3. Global Nexus Initiative (GNI), Advancing Nuclear Innovation: Responding to Climate Change and Strengthening Global Security. *Glob. Nexus Initiat.* (2019), (available at <http://globalnexusinitiative.org/results/reports/advancing-nuclear-innovation-responding-to-climate-change-and-strengthening-global-security/>).
4. A. Nilsson, C. Jorant, E. Redmond, K. Luongo, GNI Advanced Reactors Security Analysis & Findings (2018), (available at <http://globalnexusinitiative.org/wp-content/uploads/2018/12/GNI-Security-Nov.-15-FINAL-11.13.18.pptx>).
5. Bureau of International Security and Non-proliferation, Security by Design in the United States. *US Dep. State* (2012), (available at <http://2009-2017.state.gov/t/isn/rls/fs/186672.htm>).
6. M. K. Snell, C. D. Jaeger, "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>).
7. M. Snell, C. Jaeger, C. Scharmer, S. Jordan, K. Tanuma, K. Ochiai, T. Iida, "Security-by-Design Handbook" (SAND2013-0038, 1088049, Sandia National Lab. (SNL-NM), Albuquerque, NM (United States), 2013), doi:10.2172/1088049.
8. World Institute for Nuclear Security, "Implementing Security by Design at Nuclear Facilities," *WINS International Best Practice Guide* (World Institute for Nuclear Security, Vienna, 2019).
9. R. V. G. Clarke, "Situational" Crime Prevention: Theory and Practice. *Br. J. Criminol.* **20**, 136–147 (1980), doi:10.1093/oxfordjournals.bjc.a047153.
10. O. Newman, *Creating Defensible Space* (DIANE Publishing, 1996).
11. J. D. Freilich, G. R. Newman, in *Oxford Research Encyclopedia of Criminology and Criminal Justice* (Oxford University Press, 2017; <https://oxfordre.com/criminology/view/10.1093/acrefore/9780190264079.001.0001/acrefore-9780190264079-e-3>), doi:10.1093/acrefore/9780190264079.013.3.
12. M. L. Garcia, *The Design and Evaluation of Physical Protection Systems* (Elsevier/Butterworth-Heinemann, Amsterdam; Boston, 2nd ed., 2008).
13. Sandia National Laboratories, "International Training Course on the Physical Protection of Nuclear Facilities and Materials," *The Twenty-Seventh International Training Course* (Sandia

- National Lab. (SNL-NM), Albuquerque, NM (United States), 2018), (available at https://share-ng.sandia.gov/itc/assets/01_introduction-to-the-international-training-course.pdf).
14. M. Khairallah, *Physical Security Systems Handbook: The Design and Implementation of Electronic Security Systems* (Elsevier: Butterworth-Heinemann, Amsterdam, 2006; <http://site.ebrary.com/id/10185983>).
 15. T. Norman, *Integrated Security Systems Design: Concepts, Specifications, and Implementation* (Elsevier Butterworth-Heinemann, Amsterdam; Boston, 2007).
 16. C. J. Bolton, *Security by Design* (International Atomic Energy Agency, 2014; http://inis.iaea.org/Search/search.aspx?orig_q=RN:45045510), *International Conference on Nuclear Security*.
 17. E. Marrent, Presentation to WINS Workshop on Security by Design (2019).
 18. World Institute for Nuclear Security, "Security of Small Modular Reactors (SMRs)" (World Institute for Nuclear Security (WINS), Vienna Austria, 2019), (available at <https://wins.org/wp-content/uploads/2018/11/2019-20-3-REPORT-WS-on-Security-of-SMRs-1-1.pdf>).
 19. International Atomic Energy Agency, *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)* (International Atomic Energy Agency, Vienna, 2011; https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf), *IAEA Nuclear Security Series*.
 20. International Atomic Energy Agency, *Establishing the Nuclear Security Infrastructure for a Nuclear Power Programme: Implementing Guide* (International Atomic Energy Agency, Vienna, 2013; http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1591_web.pdf), *IAEA Nuclear Security Series*.
 21. International Atomic Energy Agency, "Text of the Convention on the Physical Protection of Nuclear Material" (INFCIRC/274, International Atomic Energy Agency, Vienna, 1979), (available at <https://media.nti.org/documents/cppnm.pdf>).
 22. International Atomic Energy Agency, "Amendment to the Convention on the Physical Protection of Nuclear Material" (INFCIRC/274/Rev.1/Mod.1, International Atomic Energy Agency, Vienna, 2016).
 23. International Atomic Energy Agency, *Security During the Lifetime of a Nuclear Facility: Implementing Guide* (International Atomic Energy Agency, Vienna, 2019; <https://www.iaea.org/publications/12363/security-during-the-lifetime-of-a-nuclear-facility>), *Nuclear Security Series*.
 24. International Atomic Energy Agency, "Nuclear Security Series Glossary Version 1.3," *Nuclear Security Series* (International Atomic Energy Agency, Vienna, 2015), (available at <https://www.iaea.org/sites/default/files/18/08/nuclear-security-series-glossary-v1-3.pdf>).

25. Office for Nuclear Regulations, “Security Assessment Principles for the Civil Nuclear Industry,” *Security Assessment Principles (SyAPs)* (Version 0, Office for Nuclear Regulation (UK), 2017), (available at <http://www.onr.org.uk/syaps/index.htm>).
26. Office for Nuclear Regulations, Generic Design Assessment (GDA) of New Nuclear Power Stations. *Off. Nucl. Regul.* (2020), (available at <http://www.onr.org.uk/new-reactors/index.htm>).
27. NEI Small Modular Reactor Licensing Task Force, “Physical Security for Small Modular Reactors” (Position Paper, Nuclear Energy Institute, Washington, DC, USA, 2012), (available at <https://www.nrc.gov/docs/ML1222/ML12221A197.pdf>).
28. NEI Small Modular Reactor Working Group, “Proposed Consequence-Based Physical Security Framework for Small Modular Reactors and Other New Technologies” (White Paper, Nuclear Energy Institute, Washington, DC, USA, 2015), (available at <https://www.nrc.gov/docs/ML1534/ML15349A067.pdf>).
29. Nuclear Regulatory Commission, Non-Light Water Reactor Security Design Considerations. *Fed. Regist.* (2017), (available at <https://www.federalregister.gov/documents/2017/03/13/2017-04873/non-light-water-reactor-security-design-considerations>).
30. P. Lee, K. Lawson-Jenkins, Security by Design - Physical and Cyber Security Design Considerations (2017), (available at <https://www.nrc.gov/docs/ML1709/ML17093A583.pdf>).
31. M. M. Doane, “Options and Recommendation for Physical Security for Advanced Reactors” (Policy Issue (Notation Vote) SECY-18-0076, U.S. Nuclear Regulatory Commission, Washington, DC, USA, 2018), (available at <https://www.nrc.gov/docs/ML1805/ML18052B032.pdf>).
32. Nuclear Regulatory Commission, “Rulemaking for Physical Security for Advanced Reactors” (Regulatory Basis for Public Comment NRC-2017-0227, U.S. Nuclear Regulatory Commission, Washington, DC, USA, 2019), (available at <https://www.nrc.gov/docs/ML1909/ML19099A017.pdf>).
33. Canadian Nuclear Safety Commission, REGDOC-2.5.2, Design of Reactor Facilities: Nuclear Power Plants. *Can. Nucl. Saf. Comm.* (2014), (available at <http://nuclearsafety.gc.ca/eng/acts-and-regulations/regulatory-documents/published/html/regdoc2-5-2/index.cfm>).
34. Canadian Nuclear Safety Commission, Nuclear Security Regulations (SOR/2000-209). *Can. Nucl. Saf. Comm.* (2015), (available at <https://laws-lois.justice.gc.ca/eng/regulations/SOR-2000-209/index.html>).
35. Canadian Nuclear Safety Commission, Stakeholder Workshop Report: Periodic Review of the Nuclear Security Regulations. *Can. Nucl. Saf. Comm.* (2017), (available at <http://www.nuclearsafety.gc.ca/eng/acts-and-regulations/consultation/history-regs/stakeholder-workshop-report-periodic.cfm>).

36. G. Beauchemin, G. Dansereau, "Harmonized Threat and Risk Assessment (TRA) Methodology" (TRA-1, Communications Security Establishment and Royal Canadian Mounted Police, 2007), (available at <https://cyber.gc.ca/sites/default/files/publications/tra-emr-1-e.pdf>).
37. International Atomic Energy Agency, *Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5)* (International Atomic Energy Agency, Vienna, 2018; <https://www.iaea.org/publications/11092/physical-protection-of-nuclear-material-and-nuclear-facilities-implementation-of-infcirc/225/revision-5>), *Nuclear Security Series*.
38. S. Mitsutoshi, K. Demachi, Security by Facility Design for Sabotage Protection. *J. Nucl. Sci. Technol.* **55**, 559–567 (2018), doi:10.1080/00223131.2017.1417170.
39. International Atomic Energy Agency, *Identification of Vital Areas at Nuclear Facilities: Technical Guidance Reference Material* (International Atomic Energy Agency, Vienna, 2013; <https://www.iaea.org/publications/8592/identification-of-vital-areas-at-nuclear-facilities>), *Nuclear Security Series*.
40. T. Anderson, Editor's Note: Fundamentals. *Secur. Manag. Publ. ASIS Int.* (2019), (available at http://www.asisonline.org/security-management-magazine/articles/2019/04/editors-note-fundamentals/?_t_id=8yEa3b8FuoYiSDOGiKOD8A%3d%3d&_t_uuid=JKJXFIJGSEi8wSnqWSmRuw&_t_q=fundamentals&_t_tags=language%3aen%2csiteid%3ab1140b07-9e31-4808-809a-878911c7f3f1%2candquerymatch&_t_hit.id=ASIS_Models_Pages_SMArticleDetailPage/_f073ed64-aba1-4fb2-8fcd-1cf78fe9393f_en&_t_hit.pos=1).
41. D. Hebditch, S. J. Third, J. P. Martin, M. Wise, (Phoenix, AZ, USA, 2010).
42. S. DeMuth, F. Badwan, (Marseille, France, 2014; https://www.researchgate.net/publication/283292551_Integrating_Safety_Security_and_Safeguards_for_Used_Fuel_Storage).
43. F. M. Badwan, S. F. DeMuth, M. C. Miller, G. Pshakin, (U.S. Department of Energy, Office of Scientific and Technical Information, United States, 2015; <https://www.osti.gov/servlets/purl/1170624>).
44. C. Méndez, B. Middleton, "Integrating Safety, Operations, Security, and Safeguards into the Design of Small Modular Reactors: A Handbook" (SAND2013-9429, Sandia National Laboratories, United States, 2013), (available at https://www.researchgate.net/profile/Carmen_Mendez6), doi:10.2172/1121986.
45. A. D. Williams *et al.*, "System Studies for Global Nuclear Assurance & Security: 3S Risk Analysis for Small Modular Reactors (Volume I)? Technical Evaluation of Safety Safeguards & Security." (SAND2018-12447, 1489621, 2018), pp. SAND2018-12447, 1489621.
46. American Society of Industrial Security (ASIS), *Facilities Physical Security Measures Guideline* (ASIS International, Alexandria, VA, 2009).

47. International Atomic Energy Agency, "Handbook on the Design of Physical Protection Systems for Nuclear Material and Nuclear Facilities: Draft Technical Guidance," *Nuclear Security Series* (Draft Technical Guidance NST055, International Atomic Energy Agency, Vienna, 2017), (available at <https://www-ns.iaea.org/downloads/security/security-series-drafts/tech-guidance/nst055.pdf>).
48. C. Baylon, Leveraging Drones to Improve Nuclear Facility Security and Safety. *Chatham House* (2015), (available at <https://www.chathamhouse.org/expert/comment/leveraging-drones-improve-nuclear-facility-security-and-safety>).
49. D. Livingstone, C. Baylon, R. Brunt, Cyber Security at Civil Nuclear Facilities: Understanding the Risks. *Chatham House R. Inst. Int. Aff.* (2015) (available at <https://www.chathamhouse.org/publication/cyber-security-civil-nuclear-facilities-understanding-risks>).
50. APSM, Senstar Announces Revolutionary Award-Winning Robot for Perimeter Surveillance. *DRASTIC NEWS - Drones Robot. Autom. Secur. Technol. Inf. Commun.* (2014), (available at <https://drasticnews.com/senstar-announces-revolutionary-award-winning-robot-for-perimeter-surveillance/>).
51. Sandia National Laboratories, Remotely Operated Weapon Systems. *Sandia Natl. Lab.*, (available at https://sandia.gov/research/robotics/high_consequence_automation/rows.html).
52. K. Harris, "Killer Robots" Pose Risks and Advantages for Military Use. *Can. Broadcast. Corp. CBC* (2015), (available at <https://www.cbc.ca/news/politics/killer-robots-pose-risks-and-advantages-for-military-use-1.3026963>).
53. *Drones and Killer Robots: Canada's Policy* (Science for Peace, 2016; <https://www.youtube.com/watch?v=uP2zLWWnTWI>).
54. A. W. Dorn, *Keeping Watch: Monitoring, Technology and Innovation in UN Peace Operations* (United Nations University Press, Tokyo; New York, 2011).
55. United Nations (UN), "Performance Peacekeeping: Final Report of the Expert Panel on Technology and Innovation in UN Peacekeeping" (United Nations (UN), 2014), (available at https://peacekeeping.un.org/sites/default/files/performance-peacekeeping_expert-panel-on-technology-and-innovation_report_2015.pdf).
56. S. Thielman, Use of Police Robot to Kill Dallas Shooting Suspect Believed to be First in US History. *The Guardian* (2016), (available at <http://www.theguardian.com/technology/2016/jul/08/police-bomb-robot-explosive-killed-suspect-dallas>).
57. G. E. Robitaille, "Small Modular Reactors: The Army's Secure Source of Energy?" (Strategy Research Project, U.S. Army War College, Pennsylvania, USA, 2012), (available at <https://apps.dtic.mil/dtic/tr/fulltext/u2/a561802.pdf>), doi:10.21236/ada561802.

58. E. Lyman, "Small Isn't Always Beautiful: Safety, Security, and Cost Concerns about Small Modular Reactors" (Union of Concerned Scientists, 2013), (available at <http://www.jstor.org/stable/resrep00070>).
59. T. Nilsen, "After pressure from Norway, Rosatom says floating nuclear plant will be fueled in Murmansk." *Barents Obs.* (2017), (available at <https://thebarentsobserver.com/en/industry-and-energy/2017/07/after-pressure-norway-rosatom-says-floating-nuclear-plant-will-be-fueled>).
60. U.S. Army, *US Army's Top Secret - Camp Century Restored - Declassified Film* (<https://www.youtube.com/watch?v=TTPCXB6Oc1E&feature=youtu.be>).
61. Canadian Standard Association, "Cyber Security for Nuclear Power Plants and Small Reactor Facilities," *CSA N-Series of Standards* (CSA N290.7-2014, Canadian Standard Association, 2014), (available at <https://webstore.ansi.org/Standards/CSA/CSAN2902014>).
62. C. Reiersen, A. Gomez-Cobo, ONR perspectives on design assessment and licensing of SMRs (2016), (available at https://www.nuclearinst.com/write/MediaUploads/Events/SMR2016/Session%203/Craig_Anna_ONR_presentation-_June_2016-final.pdf).
63. Cooperation in Reactor Design Evaluation and Licensing (CORDEL) Working Group, Small Modular Reactors Ad-hoc Group, "Facilitating International Licensing of Small Modular Reactors" (2015/004, World Nuclear Association, 2015), (available at https://world-nuclear.org/uploadedFiles/org/WNA/Publications/Working_Group_Reports/REPORT_Facilitating_Intl_Licensing_of_SMRs.pdf).
64. W. C. Ostendorff, A. E. Cubbage, "Licensing Small Modular Reactors: An Overview of Regulatory and Policy Issues," *Shultz-Stephenson Task Force on Energy Policy Reinventing Nuclear Power Essay Series* (Hoover Institution Press, Stanford University, Stanford, California, 2015), (available at https://www.hoover.org/sites/default/files/research/docs/ostendorff_licensingmrs_2rs_reduced_4_0.pdf).