SMR REGULATORS' FORUM

Working Group on Design and Safety Analysis

Phase 4 Report

Safety, Security and Safeguards in Remote Locations

November 2026



The content produced by the Forum is protected by copyright. Where external parties seek to reproduce the Forum's outputs, in part or in their entirety, for their own purposes, the Forum requires the parties to seek authorization from the Scientific Secretary at: SMR-RF-Contact-Point.Team@iaea.org detailing the extent and purposes of any reproduction. Once such authorization is granted, the Forum requests any reproduction of its material in other publications to be duly credited/attributed.

TABLE OF CONTENTS

EXECUTIVE SUMMARY 1

1. INTRODUCTION 6

1.1. SMR REGULATORS' FORUM'S WORK IN THE AREA OF DESIGN AND SAFETY ANALYSIS 6
1.2. THE IAEA CONTEXT 7
1.3. SCOPE 8

2. BACKGROUND 9

2.1. SITING CONSIDERATIONS IN REMOTE LOCATIONS 9
2.2. 3S INTEGRATION 10

3. COMMON POSITIONSS 11

3.1. LOGISTICS 11
3.2. TRANSPORTATION OF NUCLEAR MATERIAL 11
3.3. CONSIDERATIONS FOR NOVEL SMR CONSTRUCTION AND DEPLOYMENT CONFIGURATIONS 12
3.4. HARSH EXTERNAL CONDITIONS 12
3.5. THEFT PREVENTION 13
3.6. RESPONSE CAPABILITIES IN REMOTE LOCATIONS 13
3.7. RISKS RELATED TO PERSONNEL 14
3.8. PHYSICAL PROTECTION 14
3.9. ENSURING COMMUNICATION 15
3.10. ADDRESSING CYBERSECURITY CHALLENGES 15
3.11. MAINTENANCE, TESTING, INSPECTION, AND REPAIR 17
3.12. SELF-SUFFICIENCY OBJECTIVES 18
3.13. CHALLENGES AND MITIGATIONS RELATED TO SAFEGUARDS IN REMOTE LOCATIONS 18
3.13.1. FACTORY ASSEMBLY AND FUELLING 19
3.13.2. REMOTE DATA TRANSMISSION 20
3.14. TEMPORARY DEPLOYMENT 20

REFERENCES 21

ABBREVIATIONS 23

CONTRIBUTORS TO DRAFTING AND REVIEW 24

EXECUTIVE SUMMARY

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

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

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

This report has been produced by the Design and Safety Analysis (DSA) Working Group (WG) of the SMR RF during its Phase 4 of work (2024 to 2026). It explores the safety, security, and safeguards (3S) challenges of deploying SMRs in remote locations. It distinguishes remote location (siting) from remote operation (off-site monitoring and control). While remote SMR deployment offers benefits such as energy accessibility, decentralization, and flexibility, it also presents unique challenges: equipment availability, self-sufficiency, physical/cyber sabotage vulnerabilities, safeguards implementation, and emergency preparedness.

This report was developed based on information, insights, and experience gained from the regulatory activities of the SMR RF Members. While it is generally aligned with existing IAEA documents, deviations may occur in some cases. This report aims to provide useful information to regulatory bodies and industry involved in the development, deployment and oversight of SMRs.

The text presents 'common positions', that is, statements relevant to the topic under discussion that are unanimously agreed upon by the Forum Members. It is important to note that these common positions reflect the views of the Forum's experts and do not represent a formal consensus of all IAEA Member States.

The common positions developed by the DSA WG are outlined below and include recommendations for potential updates to the IAEA Safety Standards.

COMMON POSITIONS FOR THIS REPORT

Common Position 1

Careful consideration should be given to ensuring that supply chains, various modes of transportation (e.g. land, water, air), the timely delivery of spare parts, and security measures used to facilitate site operations and maintenance are included in logistics plans.

Common Position 2

Vendors/Licensees should implement security measures during transportation and mitigate theft risks effectively, considering the increased vulnerability associated with remote locations. Appropriate safety measures should always be ensured during the transport of the SMR's nuclear material, and safeguards measures, as applied by the IAEA, should be accommodated. It is paramount to maintain subcriticality during the transport of nuclear fuel and fuelled SMRs, especially freshly-fuelled SMRs.

Common Position 3

Vendors/Licensees should implement monitoring, detection and response systems and procedures for mitigating hazards and security threats at SMRs located in remote locations, taking into account the specific characteristics and vulnerabilities associated with their construction and deployment configurations.

Common Position 4

Vendors/Licensees of remotely located SMRs should consider extreme weather conditions in the design, operation and emergency response.

Common Position 5

The Vendors/Licensees should consider the effects of climate change in the design and operation of remotely located SMRs, as the impact of climate change may be more challenging in remote locations than in other locations.

Common Position 6

Where a limited onsite staff presence exists, the theft risk may be increased. Vendors/Licensees should reduce and mitigate theft risks by assessing the appeal of targeted materials, conducting thorough security risk assessments and implementing measures as appropriate.

Common Position 7

Capabilities of onsite and offsite response relied upon during an emergency should be considered in planning from the outset and coordinated. This should cover all 3S considerations.

Common Position 8

Vendors/Licensees should consider increasing the robustness of the insider threat mitigation measures when siting in remote locations.

Common Position 9

Special attention should be given to proper maintenance of the safety and security culture(s) in remote locations.

Common Position 10

The appropriate number of personnel working at an SMR in a remote location should be considered and maintained in all operational states and under a range of conditions (including harsh conditions) to facilitate the 3S.

Common Position 11

Licensees should pay particular attention to staff trustworthiness considering specific conditions (for example, harsh weather and isolation) associated with remote locations.

Common Position 12

The unique challenges posed by remote siting should be considered in the design of preventive and protective measures. Vendors/Licensees are recommended to use Security by Design (SeBD) to maximize the threat delay. It is recommended to use risk analyses to assess the impact of this inherent delay time in the design of an overall 3S response strategy.

Common Position 13

Due to the potential remote operations, monitoring and need for external control in accident management, communication systems in SMRs should be designed to be resilient against failures and sabotage. Vendors/Licensees should ensure that there is sufficient redundancy, segregation, independence and diversity of communication means commensurate with their 3S significance. The algorithms of the digital Instrumentation and Control (I&C) systems important to safety should perform conservative responses in the event of communication malfunctions and failures (e.g. data errors, loss of communication).

Common Position 14

SMR Vendors/Licensees should assess the vulnerability of autonomous systems to cybersecurity threats. Vendors should provide sufficient cybersecurity protection, commensurate with the 3S significance of the consequences.

Common Position 15

SMR Vendors/Licensees should address the potential vulnerabilities resulting from the Artificial Intelligence (AI)/Machine Learning (ML) implementation in digital I&C systems. Addressing these vulnerabilities requires a comprehensive approach to

cybersecurity, including, but not limited to, rigorous testing, robust security policies, employee training, and continuous monitoring and updating of systems.

Common Position 16

Careful planning should be performed for 3S Maintenance, Testing, Inspection, and Repair (MTIR) activities in remote locations given the challenges associated with potential scarcity of qualified professionals. Availability of supplies for MTIR needs to be ensured and appropriate compensatory measures need to be identified.

Common Position 17

Due to challenges presented by remoteness and a potential for a delayed response, SMRs situated in remote locations may need to be more resilient to accidents and hazards (for example, have longer coping times). More emphasis should be placed on the design features and/or measures to reduce reliance on offsite emergency response.

Common Position 18

To meet site specific needs, proper measures and contingency plans should be developed and put in place to maintain fundamental safety functions in remote locations until the offsite support can be provided.

Common Position 19

The IAEA safeguards by design (SBD) process (see Refs [1, 2, 3]) can play a crucial role in addressing challenges related to remote locations and operations. Therefore, Member States representing vendors should engage with the IAEA early in the design phase to facilitate the effective implementation of safeguards when facilities are constructed.

Common Position 20

Design information verification is a key aspect of effective safeguards implementation. If the supplier State is not under a comprehensive IAEA Safeguards Agreement, the reactor design may still need to be verified and sealed by the IAEA prior to transportation to remote locations.

Common Position 21

Where possible, the Vendors/Licensees and Member State should facilitate Remote Data Transmission (RDT) in remote locations to increase the effectiveness and efficiency of the IAEA safeguards measures with benefits to all stakeholders. There are synergies with safety and security that can possibly be leveraged. Information security must be ensured.

Common Position 22

Regardless of whether the deployment is long-term or temporary, the 3S considerations outlined in this report, as well as in the previous DSA WG report on 3S [4], should remain applicable where appropriate.

Recommendations for the IAEA

The IAEA is recommended to develop guidance on temporary deployment and thereby assist regulatory bodies in their efforts to develop their requirements and guidance.

1. INTRODUCTION

Small Modular Reactors (SMRs) are increasingly being considered by various countries as a viable option for providing nuclear power in remote locations. The integrated implementation of safety, security, and safeguards (the 3S approach) is a crucial aspect of deploying SMRs, even more so in such areas [4, 5].

For the purpose of this report, a remote location is one that is situated far from either established urban centres or regions with significant infrastructure development. Remote locations are often characterized by limited access to electricity grids, transportation networks, and essential services. These areas could include off-grid communities, industrial facilities in isolated regions, mining sites, military installations, or regions with challenging climate and/or geographical terrain. Floating SMRs may also fall within the definition of a remote location, where appropriate.

This is distinct from the concept of remote operation; remote operations refer to the management, control, oversight of systems, processes, or activities from a location that is physically distant from the site where the operations are taking place. In the context of SMRs or other industrial facilities, remote operations typically involve monitoring and controlling various aspects of the facility's operation, such as reactor operational parameters, safety systems, security and safeguards measures, from an off-site location.

Deploying SMRs in remote locations may offer several compelling benefits, such as energy accessibility and security, decentralization, flexibility and scalability, environmental benefits and support for critical infrastructure. However, there are several challenges that may be unique or enhanced due to deployment of SMRs in remote locations; these include but are not limited to: availability of equipment; self-sufficiency; vulnerabilities to physical and cyber sabotage; ensuring safeguards; and challenges associated with the preparedness and response to a nuclear emergency.

The purpose of this document is to highlight potential challenges for 3S aspects throughout the lifecycle of a SMR deployed in a remote location, and to form common positions from the contributing regulatory bodies.

1.1. SMR REGULATORS' FORUM'S WORK IN THE AREA OF DESIGN AND SAFETY ANALYSIS

The SMR RF began with a Pilot phase (2015 to 2017), during which important topics in relation to the design and safety analysis were covered [6], including:

- Use of a Graded Approach;
- The implications of SMR characteristics on Defence in Depth;
- Documenting considerations in implementing flexible Emergency Planning Zones.

In Phase 2 (starting in 2018), a Design and Safety Analysis Working Group (DSA WG) was established, and it has continued until Phase 4 (2024 to 2026), examining several critical topics:

- Multi-unit aspects [7, 8]
- Uncertainties arising from the use of passive systems in SMR [7]
- Design Extension Conditions (DEC), previously known as beyond design basis accidents (BDBAs) [7]
- Containment systems [9]

In the preceding phase of the Forum, the DSA WG examined numerous 3S considerations pertaining to the operation of SMRs, as outlined in its report titled 'Safety, Security, and Safeguards from a Regulatory Perspective: An Integrated Approach' [4]. This comprehensive review served as the foundation for understanding the intricate interplay between safety, security, and safeguards implementation within the context of SMR operations. Building upon the insights garnered from the previous deliberations, this report endeavours to delve deeper into the nuances associated with 3S aspects of SMRs intended to be deployed in remote locations throughout its lifecycle.

1.2. THE IAEA CONTEXT

Requirement 8 (Interfaces of safety with security and safeguards) of IAEA SSR-2/1 [10] states:

> "Safety measures, nuclear security measures and arrangements for the State system of accounting for, and control of, nuclear material for a nuclear power plant shall be designed and implemented in an integrated manner so that they do not compromise one another."

However, IAEA Safety Report No. 123 [5] identified that there was limited guidance on applying an integrated 3S approach to SMRs, particularly in managing the interfaces between these areas. One of the key areas identified for requiring further work included the consideration of remote locations.

Several IAEA Nuclear Security Series (NSS) publications are applicable to the consideration of remote locations, such as NSS No. 20 [11], NSS No. 13 [12], NSS No. 25-G [13], NSS No. 42-G [14], NSS No. 17-T [15], NSS No. 33-T [16], NSS No. 35-G [17], NSS No. 40-T [18], NSS No. 49-T [19]; however, they do not address the specific implementation to SMRs intended for remote locations and the interfaces with safety and safeguards.

IAEA safeguards will be applied to SMRs located in remote areas in accordance with the applicable safeguards agreements. Implementing the necessary measures and activities early in the design process will ensure a more effective and efficient application of safeguards upon construction. Existing IAEA guidance on safeguards by design for reactors can be found in IAEA Nuclear Energy Series No. NP-T-2.8 [1] and No. NP-T-2.9 [2].

1.3. SCOPE

This report focuses on the 3S challenges throughout the lifecycle of an SMR intended for deployment in remote locations. For the purposes of this report, the term SMR includes microreactors, which are considered a subset of SMRs. Whilst the scope of this report is based on SMRs, the general principles may be applicable to any nuclear reactor intended for deployment in remote locations.

This report was developed based on information, insights, and experience gained from the regulatory activities of the SMR RF experts, supported by the IAEA safety, security and safeguards experts, and it reflects the main common positions agreed. It is largely consistent with existing IAEA standards and guidance and aims to highlight potential areas of interest to regulatory bodies and industry in the development, deployment and oversight of SMRs intended for remote siting.

2. BACKGROUND

Remote locations and operations pose unique challenges and opportunities for the deployment and operation of SMRs, including consideration of any associated waste management and disposal facilities, and how these interconnected facilities may also be affected. In these areas, characterized by geographical isolation, sparse infrastructure, and limited access to centralized energy grids, the siting and operation of SMRs would require careful consideration of various factors, including 3S. Additionally, the remote operation of SMRs presents its own set of challenges, such as logistical constraints, reduced access to technical expertise, and reliance on remote monitoring and control systems.

This report introduces the complexities of siting SMRs in remote areas and addresses the key considerations for ensuring the successful deployment and operation of these innovative nuclear technologies in such challenging environments.

2.1. SITING CONSIDERATIONS IN REMOTE LOCATIONS

When siting SMRs in remote locations, several factors related to 3S may be unique or enhanced relative to non-remote locations. The DSA WG considers that the following aspects may pose unique or enhanced challenges:

1. Characteristics of the Site, such as weather (including extreme weather conditions), climate, geology, seismology, and hydrology.
2. Infrastructure Availability: remote locations may lack essential infrastructure, such as transportation networks, electricity grids, and communication systems.
3. Emergency Response: remotely located SMRs may require less onerous offsite countermeasures; however, offsite response times may be longer, requiring longer self-resilience.
4. Safe Operation: remote locations may pose unique safety challenges due to their isolation and limited access. In particular, remote siting poses challenges for MTIR.
5. Security Considerations: remote locations may pose unique physical security challenges due to their isolation and limited access. Remote locations also pose challenges to deployment of competent resources in case of cyber incidents involving digital I&C systems that are essential for SMR operations and safety. This is especially true for SMRs that may be operated autonomously.
6. Supply Chain and Transport: remote locations may lead to enhanced challenges related to supply chain and transport of items that directly or indirectly impact nuclear safety, security and safeguards.
7. Communication: siting in remote locations and/or remote operations may present unique or increased communication challenges for 3S. Data transfer, operability and emergency response may require more robust communication links to prevent loss of control with respect to 3S.
8. Safeguards Considerations: monitoring and verification activities in remote locations will likely become more challenging, requiring unique solutions.
9. 3S Integration: the expected reduction of SMR's on-site staff compared to conventional reactor facilities, which would increase the use of autonomous

systems, may demand a higher level of integration between safety, security and safeguards systems. This is explored further below.

By emphasising these considerations, stakeholders can identify suitable locations for SMRs in remote areas to optimize 3S and meet the SMR purpose effectively.

2.2. 3S INTEGRATION

Due to the unique challenges associated with remote locations, the results of the risk assessment and the balance among the risk management measures may differ from those for the same design located elsewhere. An integrated 3S approach can enable mitigation of vulnerabilities and reduction of potential risks during the facility design, construction, operation and decommissioning [4].

Traditionally, safety, security, and safeguards have been treated as separate entities in existing nuclear power plants, with security and safeguards often retrofitted later without optimization [20, 21, 22]. This has led to inefficiencies, increased costs, and additional operational burdens. The move towards smaller, more operationally agile SMRs underscores the need to reassess this traditional approach. By considering security and safeguards alongside safety from the outset of design, an integrated 3S approach seeks to reduce resource demands throughout the facility's lifecycle.

To ensure integration, consideration of the 3S interface should occur at all decision points. In some cases, measures designed for one discipline, such as safety, may also benefit security and safeguards. However, conflicts can arise when one discipline's requirements differ from another's. These conflicts are often driven by the different purposes of each discipline: safety measures are designed to address unintentional events, while security and safeguards are focused on actors who may adapt their tactics based on knowledge of the defences.

Managing these interfaces systematically allows for the recognition of decision points, optimization of synergies, and resolution of conflicts, ultimately ensuring the shared objective of protecting people and the environment from the harmful effects of ionising radiation. In almost all areas highlighted in the previous section, an interface exists between the different domains of 3S. For example, improvements in communications of plant data for remote monitoring or operations may increase vulnerabilities to cyber-attacks.

Integrated 3S evaluations may be more consistent than separate evaluations of the individual domains. Explicitly identifying and considering cross-domain interactions helps mitigate risks associated with siloed approaches in the design phase of a remote reactor. Inspection procedures can also be developed around design objectives that align with the categories of 3S interactions, leveraging technical information generated from the 3S evaluations. Furthermore, early adoption of 3S enables enhanced risk analyses, supporting the optimization of facility performance during operation. For more information on the integration of 3S, see Ref. [4].

3. COMMON POSITIONSS

The DSA WG has explored several themes related to remote locations. Whilst many aspects of nuclear safety, security and safeguards were explored during the production of this report, common positions were reached only in areas that present unique or potentially enhanced challenges associated with remote locations. These positions are presented in the following sections.

3.1. LOGISTICS

Remote locations often lack transportation infrastructure and may have limited access to essential resources, equipment, and spare parts required for SMR maintenance and repairs. Developing comprehensive logistics plans and establishing supply chains that also account for necessary security measures is essential to ensure the safe, secure, and timely delivery of necessary materials and support services to the SMR site. Security measures should be sufficient to address the verification of personnel and material accessing the site, including measures for identifying authorized personnel and means to check or search authorized personnel, vehicles, and equipment for contraband prior to entry.

Common Position 1

> Careful consideration should be given to ensuring that supply chains, various modes of transportation (e.g. land, water, air), the timely delivery of spare parts, and security measures used to facilitate site operations and maintenance are included in logistics plans.

3.2. TRANSPORTATION OF NUCLEAR MATERIAL

During transportation of nuclear material, special attention should be given to transportation security and response arrangements, considering longer or unconventional routes that may heighten vulnerabilities. Appropriate safety measures should also be considered to address the hazards associated with the transport of nuclear material, taking into account the potentially longer distances, unconventional routes and limited emergency response capabilities that may be associated with remote locations.

Common Position 2

> Vendors/Licensees should implement security measures during transportation and mitigate theft risks effectively, considering the increased vulnerability associated with remote locations. Appropriate safety measures should always be ensured during the transport of the SMR's nuclear material, and safeguards measures, as applied by the IAEA, should be accommodated. It is paramount to maintain subcriticality during the transport of nuclear fuel and fuelled SMRs, especially freshly-fuelled SMRs.

3.3. CONSIDERATIONS FOR NOVEL SMR CONSTRUCTION AND DEPLOYMENT CONFIGURATIONS

Novel construction and deployment configurations may provide benefits for protection and resilience but can also introduce unique vulnerabilities and challenges for the response to hazards and security threats throughout the lifecycle of a remotely located facility. For example, underground construction could be beneficial as a defensive measure against theft and sabotage but could potentially introduce challenges for response and other considerations during the lifecycle of the remotely located facility. Irrespective of their location, underground constructions can potentially be more vulnerable to some external hazards such as flooding, and more resilient against other hazards, such as seismic events and wind loads. Similarly, remotely located floating SMR plants may provide resilience against certain land-based hazards, but may introduce vulnerabilities associated with marine hazards, weather conditions, access, emergency response, security, and logistical support. It is recognized that, in remote locations, it can be potentially more challenging to implement effective response to internal hazards such as fires, as further described in section 3.6. Facilities will need to be designed and operated with the unique set of hazards in mind, recognizing that these hazards may further be aggravated by the effects of climate change. This may include monitoring and detection systems beyond what would be typically expected.

Common Position 3

> Vendors/Licensees should implement monitoring, detection and response systems and procedures for mitigating hazards and security threats at SMRs located in remote locations, taking into account the specific characteristics and vulnerabilities associated with their construction and deployment configurations.

3.4. HARSH EXTERNAL CONDITIONS

Some remote locations experience harsh weather conditions. This may impact design, operability and emergency response. Specifically, this may impact transport, site access (including for various inspections), deliveries, normal operation, emergency response, data transfer, emergent maintenance, as well as the design and performance of heating, ventilation and air-conditioning systems and structures, and of systems and components (SSCs) that provide protection against external hazards.

Common Position 4

> Vendors/Licensees of remotely located SMRs should consider extreme weather conditions in the design, operation and emergency response.

Common Position 5

> The Vendors/Licensees should consider the effects of climate change in the design and operation of remotely located SMRs, as the impact of climate change may be more challenging in remote locations than in other locations.

3.5. THEFT PREVENTION

SMRs in remote locations with no or limited staff may be vulnerable to theft of nuclear material, critical equipment to support nuclear safety, or, depending on the design and deployment configuration, the reactor itself.

Common Position 6

> Where a limited onsite staff presence exists, the theft risk may be increased. Vendors/Licensees should reduce and mitigate theft risks by assessing the appeal of targeted materials, conducting thorough security risk assessments and implementing measures as appropriate.

3.6. RESPONSE CAPABILITIES IN REMOTE LOCATIONS

Situating an SMR in a remote location may impact emergency response effectiveness and timeliness. Remotely located SMRs are likely to have design features and security plans in place to mitigate or prevent a significant radiological release offsite and to extend the time available for response. The safety and security design aspects of the facility should be considered in the performance objectives for response capabilities onsite and for those offsite resources that may be called upon in an emergency in remote locations.

In the previous DSA WG report on 3S [4], it has been recognized that:

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

This Common Position remains applicable herein.

It is expected that for SMRs sited in remote locations, there should be less reliance on the prompt onsite and offsite emergency response (see common positions in section 3.12). However, when needed, there should be coordination with local authorities and emergency services for effectively managing emergency situations in remote areas, although this may be challenging.

Common Position 7

> Capabilities of onsite and offsite response relied upon during an emergency should be considered in planning from the outset and coordinated. This should cover all 3S considerations.

3.7. RISKS RELATED TO PERSONNEL

Maintaining the reliability (trustworthiness) of personnel, as well as the adherence to safety and security culture, is paramount. This may be particularly challenging for remote locations or contracted-out operations due to a small staff compliment and limited oversight. Due to oversight limitations, it is important to supplement the administrative insider threat mitigation measures with robust technical measures.

Common Position 8

> Vendors/Licensees should consider increasing the robustness of the insider threat mitigation measures when siting in remote locations.

Common Position 9

> Special attention should be given to proper maintenance of the safety and security culture(s) in remote locations.

Balancing the workforce size and security risks in remote locations may pose unique challenges that demand careful management. Particular attention should be paid to the appropriate number of staff needed to conduct licensed activities at an SMR in remote locations. Reduced staffing levels should not compromise the implementation of appropriate human performance measures, including independent verification and, where appropriate, two-person or dual-control arrangements for safety- and security-significant activities. Where such arrangements are affected by remote operation or limited staffing, alternative measures should be considered to maintain an appropriate level of protection against human error and insider threats.

Common Position 10

> The appropriate number of personnel working at an SMR in a remote location should be considered and maintained in all operational states and under a range of conditions (including harsh conditions) to facilitate the 3S.

In remote locations, harsh weather conditions and/or social isolation may pose difficulties for staff wellbeing and may have implications to both safety and security.

Common Position 11

> Licensees should pay particular attention to staff trustworthiness considering specific conditions (for example, harsh weather and isolation) associated with remote locations.

3.8. PHYSICAL PROTECTION

Nuclear security plans typically rely on security personnel, early detection, delay measures, onsite response with a certain period of autonomy, and offsite response as elements of security protection, all of which place dependencies on humans. Therefore, remote

locations with only a few people on site may pose unique challenges to a demonstration of a robust nuclear security plan and resilience of the plant up to the point at which off-site support can be provided. The security response, or lack thereof, may have important implications for the facility design, and therefore is of particular importance for remote siting.

Early adoption of SeBD is recognized as an effective means to reduce the risk posed by a security-initiated event [4, 5]. SeBD can increase delay time and mitigate the potential consequences of a security-initiated event due to the inherent capabilities of SSCs. SeBD coupled with a proper risk assessment allows for the optimization of armed response. A proper risk assessment will consider both onsite and offsite response capabilities.

Common Position 12

> The unique challenges posed by remote siting should be considered in the design of preventive and protective measures. Vendors/Licensees are recommended to use SeBD to maximize the threat delay. It is recommended to use risk analyses to assess the impact of this inherent delay time in the design of an overall 3S response strategy.

3.9. ENSURING COMMUNICATION

Operation in remote locations may rely on advanced and secured communication technologies, automation systems, and remote monitoring tools to enable real-time data transmission, decision-making, and operational intervention, even when personnel are not physically present at the site. As such, remote operation of SMRs requires careful planning and robust communication systems protected using a risk-informed approach against all types of hazards and threats, particularly those with cyber capabilities, and relies on remote monitoring and control technologies to ensure safe and efficient operation.

The above considerations are also important for communication with authorities for oversight and for the purposes of emergency preparedness.

Common Position 13

> Due to the potential remote operations, monitoring and need for external control in accident management, communication systems in SMRs should be designed to be resilient against failures and sabotage. Vendors/Licensees should ensure that there is sufficient redundancy, segregation, independence and diversity of communication means commensurate with their 3S significance. The algorithms of the digital I&C systems important to safety should perform conservative responses in the event of communication malfunctions and failures (e.g. data errors, loss of communication).

3.10. ADDRESSING CYBERSECURITY CHALLENGES

The increasing digitization of SMR operations requires a proactive and layered cybersecurity strategy to protect against evolving cyber threats. Cybersecurity must be treated as a core

component of the 3S framework because a successful cyber-attack on digital systems can compromise safety, security, and safeguards simultaneously. This is particularly critical for SMRs in remote locations, where continuous operational data may need to be transmitted to and from off-site support centres, and where autonomous systems may play a significant role in plant operation.

Security, reliability and functionality of remote operations and monitoring should be continuously ensured, and the availability, integrity and confidentiality of all transmitted and processed information should be always maintained. Remote data transmission technologies, such as broadband, satellite, radio frequency, and frame relay links, introduce specific vulnerabilities that adversaries can exploit. To mitigate these risks, all data relevant to critical facility functions in transit and at rest should be encrypted using strong cryptographic protocols. Access to SMR systems should follow zero-trust principles, where no user or device is inherently trusted, and every access request is authenticated, authorized, and continuously validated. Strong and multi-factor authentication should be mandatory for all remote operators, and network segmentation should isolate critical systems from external interfaces.

Modern cybersecurity monitoring and capabilities should be implemented to provide comprehensive coverage of all critical digital assets within the facility. These capabilities should include advanced capabilities designed to continuously identify, detect, and respond to anomalies and malicious activity across all communication channels and critical networks and systems, enabling timely and effective mitigation of emerging threats. Vendors and Licensees should adopt internationally recognized standards or best practices to ensure consistency, robustness, and regulatory alignment, and they should establish an information and computer security management model that is comprehensive and impactful.

Supply chain security is equally important: all hardware and software components should be verified for security before deployment, suppliers should be required to comply with cybersecurity requirements, and Vendors/Licensees should actively monitor and assess the performance and cybersecurity capabilities of their supply chain to ensure ongoing compliance and resilience. Certification and accreditation programmes should be put in place to identify and remediate vulnerabilities.

Modern technologies like Artificial Intelligence and Machine Learning (AI/ML) and autonomous systems introduce additional cybersecurity challenges. The level of autonomy and the tasks performed by these systems must be carefully assessed to ensure resilience against cyber threats. Systems should incorporate fail-safe modes that default to conservative operational states in case of anomalies or loss of communication. AI/ML technologies used in SMR control systems require robust measures to prevent cyber risks like data poisoning, adversarial attacks, and model corruption. Measures should include the use of verified and sanitized training datasets, integrity checks and monitoring for AI models and agents, AI Application Programming Interfaces (APIs) security and deployment of explainable AI techniques to maintain transparency and trustworthiness. Continuous monitoring for anomalies in AI-driven operations is essential to reduce the cyber incidents. Vendors/Licensees should develop and maintain a preparedness and cyber incident response plan tailored for remote SMR operations and locations. This plan should include

procedures, secure communication channels, and pre-arranged agreements with cybersecurity experts for remote support. Incident response capabilities should be designed and maintained to provide timely and effective support to remote location, ensuring that cyber incidents can be addressed without delay regardless of geographical remoteness. Regular trainings simulating cyber-attack scenarios should be conducted to validate incident response readiness. Cyber resilience ensures continuity of critical safety and security functions even during a cyber event. Furthermore, thorough advance preparations should be carried out to anticipate and mitigate potential cybersecurity incidents, ensuring that all necessary resources, procedures, and measures are in place before an event occurs (see Common Position 7).

Common Position 14

SMR Vendors/Licensees should assess the vulnerability of autonomous systems to cyber security threats. Vendors should provide sufficient cyber security protection, commensurate with the 3S significance of the consequences.

Common Position 15

SMR Vendors/Licensees should address the potential vulnerabilities resulting from the AI/ML implementation in digital I&C systems. Addressing these vulnerabilities requires a comprehensive approach to cybersecurity, including, but not limited to, rigorous testing, robust security policies, employee training, and continuous monitoring and updating of systems.

3.11. MAINTENANCE, TESTING, INSPECTION, AND REPAIR

Remote locations may pose challenges for conducting essential maintenance, testing, inspection, and repair activities due to the scarcity of supplies and qualified professionals. In the absence of on-site expertise, there is a potential for leaving the plant in a vulnerable state if failures were to occur or if MTIR could not be performed on time. This may necessitate the storage of supplies, including but not limited to spare parts, in the proximity of a remotely located SMR.

Similarly to safety, for circumstances where security equipment or components become inoperable, security compensatory measures should be identified in advance and included in security plans. The timing for repair should be based on the significance of the security function that the equipment or component provides (e.g. failed cameras or alarm sensors). Ideally, the security system should be designed with built-in redundancy and separation so that the degradation to any one component has little to no adverse impact for performing its intended function.

Common Position 16

Careful planning should be performed for 3S MTIR activities in remote locations given the challenges associated with potential scarcity of qualified professionals.

Availability of supplies for MTIR needs to be ensured and appropriate compensatory measures need to be identified.

3.12. SELF-SUFFICIENCY OBJECTIVES

Self-sufficiency becomes critical for both the design and operation of SMRs situated in remote locations. Given challenges associated with the emergency response, the coping time of remotely situated SMRs may have to be longer than if such SMRs were to be situated elsewhere. This would impact their design for remotely located sites. Similarly, the challenges associated with weather conditions or hazards may also necessitate design optimization for remotely situated SMRs.

In accident conditions, SMRs in remote locations may depend on essential supplies and services to maintain fundamental safety functions and ultimately achieve and maintain a safe state until the offsite services can be deployed. They should be designed to meet appropriate self-sufficiency objectives and criteria. The supplies to meet the self-sufficiency objectives and criteria may include back-up power, water, lubricating oil and fuel oil. For example, reliable power sources are crucial for SMR operations, safety, security, safeguards, and emergency responses, especially in remote areas where grid connections might not be available. Some SMR designs propose natural circulation for cooling without relying on alternative power sources. Access to alternative power can be more difficult in remote locations, necessitating thorough planning.

Common Position 17

Due to challenges presented by remoteness and a potential for a delayed response, SMRs situated in remote locations may need to be more resilient to accidents and hazards (for example, have longer coping times). More emphasis should be placed on the design features and/or measures to reduce reliance on offsite emergency response.

Common Position 18

To meet site specific needs, proper measures and contingency plans should be developed and put in place to maintain fundamental safety functions in remote locations until the offsite support can be provided.

3.13. CHALLENGES AND MITIGATIONS RELATED TO SAFEGUARDS IN REMOTE LOCATIONS

Remote locations may pose challenges for safeguards implementation. Limited infrastructure (internet connections, roads, rail, accommodations) and harsh weather conditions may significantly affect IAEA inspector access to the site. For example, the absence of nearby accommodations or basic amenities could make multi-day inspections particularly difficult. The challenges associated with remote locations may preclude the implementation of certain technical safeguards measures, such as unannounced

inspections, which then forces an increased reliance upon a more limited selection of measures.

For SMRs with long operation cycles, where access to the core or spent fuel may not be possible for years at a time, the IAEA will likely need to apply seals to the core, then periodically verify seal integrity and installed surveillance systems. The seals would need to be applied in such a way that they can be verified without posing health hazards to the inspectors, and without being exposed to excessively high radiation levels. At the same time, this sealed core scheme may present challenges for operators requiring access to the core for MTIR. Resulting solutions will need to account for both IAEA verification objectives and operator needs, including through the use of unattended monitoring systems (UMS) for containment and surveillance, such as remotely verified electronic seals and laser curtain systems.

Common Position 19

> The IAEA SBD process (see Refs [1, 2, 3]) can play a crucial role in addressing challenges related to remote locations and operations. Therefore, Member States representing vendors should engage with the IAEA early in the design phase to facilitate the effective implementation of safeguards when facilities are constructed.

3.13.1. FACTORY ASSEMBLY AND FUELLING

There may be situations when fuel or a fully fuelled reactor core is produced in one country (supplier) and shipped to another (host). In such cases, the safeguards measures will be applied in each location and during transport in accordance with the legal safeguards agreements of the States involved.

During factory assembly and fuelling processes, the IAEA would typically perform design information verification (DIV) at the manufacturing site in the supplier State in accordance with their Safeguards Agreement. Following design verification, an IAEA seal may have to be applied at the factory before the shipment to the host country. If the fuel is shipped separately from the assembled core, safeguards will be applied in the host State just as they are for stationary, terrestrial reactor facilities.

Whether the core is refuelled in the host State at the deployment location or is returned to the supplier for refuelling, safeguards will be applied in accordance with the relevant legal agreements. DIVs are expected to be repeated throughout the lifetime of the reactor, regardless of where the reactor is located. If the core fuel is discharged in the host State and then returned to the supplier State, the IAEA's verification of spent fuel may need to take place in both the host and the supplier States, depending upon safeguards legal agreements.

Common Position 20

> Design information verification is a key aspect of effective safeguards implementation. If the supplier State is not under a comprehensive IAEA Safeguards

Agreement, the reactor design may still need to be verified and sealed by the IAEA prior to transportation to remote locations.

3.13.2. REMOTE DATA TRANSMISSION

The IAEA generally promotes the use of RDT for safeguards monitoring, ranging from basic state-of-health assessments to more complex process monitoring that demands high reliability and bandwidth. The adoption of RDT is driven by several factors, including improved efficiency and a reduced financial burden for both the IAEA and the operator. However, RDT requires digital connectivity, which may not be consistently available, particularly in remote locations where SMRs may be sited. Given the wide range of potential applications, the absence of reliable connectivity may necessitate alternative methods, such as more frequent on-site inspections, which can increase costs and logistical complexity. To address this, Vendors/Licensees, and Member States should facilitate RDT implementation in remote areas whenever possible.

Common Position 21

Where possible, the Vendors/Licensees and Member State should facilitate RDT in remote locations to increase the effectiveness and efficiency of the IAEA safeguards measures with benefits to all stakeholders. There are synergies with safety and security that can possibly be leveraged. Information security must be ensured.

3.14. TEMPORARY DEPLOYMENT

In certain regions, especially those with remote locations, SMRs might be temporarily deployed to provide power to infrastructure or to provide backup or emergency power. For example, floating reactors may be deployed in remote locations to meet electricity demands.

Common Position 22

Regardless of whether the deployment is long-term or temporary, the 3S considerations outlined in this report, as well as in the previous DSA WG report on 3S [4], should remain applicable where appropriate.

Currently, there is a lack of regulatory guidance on considerations relating to temporary deployment.

Recommendation for the IAEA

The IAEA is recommended to develop guidance on temporary deployment and thereby assist regulatory bodies in their efforts to develop their requirements and guidance.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, International Safeguards in Nuclear Facility Design and Construction, IAEA Nuclear Energy Series No. NP-T-2.8, IAEA, Vienna (2013).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, International Safeguards in the Design of Nuclear Reactors, IAEA Nuclear Energy Series No. NP-T-2.9, IAEA, Vienna (2014).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Assistance for States on Implementation of IAEA Safeguards, IAEA, Vienna. Available at: https://www.iaea.org/topics/assistance-for-states

[4] SMALL MODULAR REACTOR REGULATORS' FORUM, Safety, Security and Safeguards from a Regulatory Perspective: An Integrated Approach, Working Group on Design and Safety Analysis, Phase 3 Report (2023).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Applicability of IAEA Safety Standards to Non-Water Cooled Reactors and Small Modular Reactors, Safety Reports Series No. 123, IAEA, Vienna (2023).

[6] SMALL MODULAR REACTOR REGULATORS' FORUM, Considering the Application of a Graded Approach, Defence-in-Depth and Emergency Planning Zone Size for Small Modular Reactors, Pilot Project Report (2018).

[7] SMALL MODULAR REACTOR REGULATORS' FORUM, Multi-unit/Multi-module Aspects Specific to SMRs, Working Group on Design and Safety Analysis, Interim Report (2019).

[8] SMALL MODULAR REACTOR REGULATORS' FORUM, Design and Safety Analysis Issues Specific to Multi-unit/Module SMR Facilities and Use of Passive and Inherent Safety Features, Working Group on Design and Safety Analysis, Phase 2 Report (2021).

[9] SMALL MODULAR REACTOR REGULATORS' FORUM, Containment Systems, Working Group on Design and Safety Analysis, Phase 3 Report (2023).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), IAEA, Vienna (2016).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013), https://doi.org/10.61092/iaea.ajrj-ymul

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear

Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011), https://doi.org/10.61092/iaea.ko2c-dc4q

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities, IAEA Nuclear Security Series No. 25-G, IAEA, Vienna (2015).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security for Nuclear Security, IAEA Nuclear Security Series No. 42-G, IAEA, Vienna (2021).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Techniques for Nuclear Facilities, IAEA Nuclear Security Series No. 17-T (Rev. 1), IAEA, Vienna (2021).

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T, IAEA, Vienna (2018).

[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Security During the Lifetime of a Nuclear Facility, IAEA Nuclear Security Series No. 35-G, IAEA, Vienna (2019).

[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Handbook on the Design of Physical Protection Systems for Nuclear Material and Nuclear Facilities, IAEA Nuclear Security Series No. 40-T, IAEA, Vienna (2021).

[19] INTERNATIONAL ATOMIC ENERGY AGENCY, Evaluation of Physical Protection Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 49-T, IAEA, Vienna (2025), https://doi.org/10.61092/iaea.pckz-it39

[20] INTERNATIONAL ATOMIC ENERGY AGENCY, Safeguards by Design, IAEA, Vienna. Available at: https://www.iaea.org/topics/assistance-for-states/safeguards-by-design

[21] INTERNATIONAL ATOMIC ENERGY AGENCY, The Nuclear Safety and Nuclear Security Interface: Approaches and National Experiences, Technical Reports Series No. 1000, IAEA, Vienna (2021).

[22] INTERNATIONAL ATOMIC ENERGY AGENCY, Management of the Interface between Nuclear Safety and Security for Research Reactors, IAEA-TECDOC - 1801, IAEA, Vienna (2016).

ABBREVIATIONS

3S	Safety, Security and Safeguards
AI	Artificial Intelligence
DSA	Design and Safety Analysis
I&C	Instrumentation and Control
ML	Machine Learning
MTIR	Maintenance Testing, Inspection, and Repair
NSS	Nuclear Security Series
RDT	Remote Data Transmission
SBD	Safeguards by Design
SeBD	Security by Design
SMR	Small Modular Reactor
SMR RF	Small Modular Reactor Regulators' Forum
SSCs	Structures, Systems, and Components
WG	Working Group

CONTRIBUTORS TO DRAFTING AND REVIEW

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

Acevedo Zapata, A.	International Atomic Energy Agency (IAEA)
Alves Tavares, R.L.	International Atomic Energy Agency (IAEA)
Barley, D.	Office for Nuclear Regulation (ONR), United Kingdom
Blackmore, P.	Canadian Nuclear Safety Commission (CNSC), Canada
Botelho, I.J.	International Atomic Energy Agency (IAEA)
Bowers, A.	U.S. Nuclear Regulatory Commission (U.S. NRC), United States of America
Broeders, M.	Canadian Nuclear Safety Commission (CNSC), Canada
Calle Vives, P.	International Atomic Energy Agency (IAEA)
Christian, D.	Authority for Nuclear Safety and Radiation Protection (ANVS), Kingdom of the Netherlands
Crawford, E.	Office for Nuclear Regulation (ONR), United Kingdom
Drummond, M.	Office for Nuclear Regulation (ONR), United Kingdom
Gerceker, N.	International Atomic Energy Agency (IAEA)
Halhead, S.	Office for Nuclear Regulation (ONR), United Kingdom
Hiittenkivi, E.	Radiation and Nuclear Safety Authority (STUK), Finland
Hlobystov, V.	Scientific and Engineering Centre for Nuclear and Radiation Safety (SEC NRS), Russian Federation
Honkamaa, T.	Radiation and Nuclear Safety Authority (STUK), Finland
Huhtakangas, T.	Radiation and Nuclear Safety Authority (STUK), Finland
Iida, T.	Nuclear Regulation Authority (NRA), Japan
Israel, S.	Nuclear Safety and Radiation Protection Authority (ASNR), France
Jansen, R.	Authority for Nuclear Safety and Radiation Protection (ANVS), Kingdom of the Netherlands
Jin, C.Y.	Korea Institute of Nuclear Safety (KINS), Republic of Korea
Joffel, E.	Radiation and Nuclear Safety Authority (STUK), Finland
Joubert, J.	National Nuclear Regulator (NNR), South Africa
Karhu, P.	Radiation and Nuclear Safety Authority (STUK), Finland

Kent, M.	Canadian Nuclear Safety Commission (CNSC), Canada
Kim, D.Y.	Korea Institute of Nuclear Safety (KINS), Republic of Korea
Kim, G.W.	Korea Institute of Nuclear Safety (KINS), Republic of Korea
Kojo, R.	Nuclear Regulation Authority (NRA), Japan
Kwon, K.	Korea Institute of Nuclear Nonproliferation and Control (KINAC), Republic of Korea
Lee, S.	U.S. Nuclear Regulatory Commission (U.S. NRC), United States of America
Lei, L.	Nuclear and Radiation Safety Center (NSC), People's Republic of China
Li, D.	International Atomic Energy Agency (IAEA)
McDowall, B.	Office for Nuclear Regulation (ONR), United Kingdom
Minakawa, T.	Nuclear Regulation Authority (NRA), Japan
Naidoo, K.	National Nuclear Regulator (NNR), South Africa
Ono, H.	Nuclear Regulation Authority (NRA), Japan
Piotukh, V.	International Atomic Energy Agency (IAEA)
Plummer, D.	Office for Nuclear Regulation (ONR), United Kingdom
Prasad, S.	Office for Nuclear Regulation (ONR), United Kingdom
Romanello, V.	National Radiation Protection Institute (SURO), Czech Republic
Romano, M.	Office for Nuclear Regulation (ONR), United Kingdom
Sakurai, A.	Nuclear Regulation Authority (NRA), Japan
Sastre Fuente, E.	U.S. Nuclear Regulatory Commission (U.S. NRC), United States of America
Sato, S.	Nuclear Regulation Authority (NRA), Japan
Sato, T.	Nuclear Regulation Authority (NRA), Japan
Shi, J.	International Atomic Energy Agency (IAEA)
Simic, S. (Chair)	Canadian Nuclear Safety Commission (CNSC), Canada
Song, C.	Korea Institute of Nuclear Safety (KINS), Republic of Korea
Syblík, J.	National Radiation Protection Institute (SURO), Czech Republic
Trahan, A.C.	International Atomic Energy Agency (IAEA)