CENTRE FOR SCIENCE & SECURITY STUDIES

KING'S College LONDON

Nuclear Security and Safeguards Considerations for Novel Advanced Reactors

Dr Ross Peel (King's College London), George Foster (Amport Risk Ltd)
and Professor Sukesh Aghara (University of Massachusetts Lowell)

2022

Contents

Executive Summary **4**

1. Introduction **6**
1.1. Background 6
1.2. Purpose and Objectives 6
1.3. Methodology 7
1.4. Scope and Intended Audience 7
1.5. Previous Work on this Topic 7
1.6. Structure of this Report 8

2. Security and Safeguards: Key Elements and Approaches **9**
2.1. Aims of Nuclear Security and Safeguards 9
2.2. Nuclear Security Risk Assessment 9
2.3. Safeguarding of Nuclear Materials 11

3. Differences between Novel Advanced Reactors and Large Conventional Nuclear Power Plants **13**
3.1. Power Capacity and Modular Manufacture and Construction 13
3.2. Reduced Capital and Operating Costs 13
3.3. Increasing Automation and Remote Operations 13
3.4. Advanced Reactors and Fuels 14
3.5. Deployment and Siting Options 15
3.6. Developer Business Models and Marketing Approaches 16

4. Nuclear Security and Safeguards Considerations for NARs **17**
4.1. Power Capacity and Modular Manufacture and Construction – Considerations 17
4.2. Reduced Capital and Operating Costs – Considerations 17
4.3. Increasing Automation and Remote Operations – Considerations 18
4.4. Advanced Reactors and Fuels – Considerations 20
4.5. Deployment and Siting Options – Considerations 22
4.6. Developer Business Models and Marketing Approaches – Considerations 25

5. Recommendations **27**
5.1. Recommendations for Research Organisations 27
5.2. Recommendations for Technology Developers 27
5.3. Recommendations for Operators 28
5.4. Recommendations for Regulators and SSAC Organisations 29
5.5. Recommendations for National Policymakers 29
5.6. Recommendations for the International Atomic Energy Agency 30

6. Conclusions **31**

References **32**

Annex **36**

Nuclear Security and Safeguards Considerations for Novel Advanced Reactors

An overview of how the unique features of small and advanced modular reactors create opportunities to deliver optimised nuclear security and safeguards while reducing lifetime operating costs.

About the Centre for Science & Security Studies

The Centre for Science & Security Studies (CSSS) contributes knowledge and understanding to policy and scholarly debates at the intersection of science and security. The Centre was created in 2003, with the support of a capacity building grant from the John D. and Catherine C. MacArthur Foundation. Staff in the Centre take a collaborative approach to research and teaching to bring in different disciplinary perspectives. Initially, the Centre had a strong nuclear focus, although this has expanded in recent years to include chemical weapons, biosecurity, and emerging technologies.

Acknowledgements

The authors are grateful to the UK Department for Business, Energy and Industrial Strategy (BEIS) for sponsoring the production of this report. This work was funded under the Nuclear Security Culture Programme, an academic-industry partnership that works around the world to strengthen nuclear security practice, forming a key part of the UK's Global Nuclear Security Programme (GNSP).

We are also grateful to those who gave their time to be interviewed and provide their expertise to the report.

Compiled by Dr Ross Peel (King's College London), Mr George Foster (Amport Risk Ltd), and Professor Sukesh Aghara (University of Massachusetts Lowell). Reviewed by Professor Christopher Hobbs (King's College London). Copyediting and proofreading by Amelie Stoetzel and Karl Dewey.

Published by King's College London in the Centre for Science & Security Studies.

Centre for Science & Security Studies
Department of War Studies
King's College London
Strand
London WC2R 2LS
United Kingdom

kcl.ac.uk/csss
@KCL_CSSS

Executive Summary

Interest is growing globally in a transition from Large Conventional Nuclear Power Plants (LCNPP) to Novel Advanced Reactors (NAR), comprising small modular and advanced modular reactors. Dozens of NAR designs are being developed with planned construction and operation over the next 10-20 years. NAR developers are putting significant work into safety and operational aspects of their designs, but security and safeguards are often secondary considerations, despite these aspects being strongly interconnected. This risks creating a situation where the dependencies, synergies and challenges associated with the relationship between the safety, security and safeguards are not addressed optimally to achieve design-, operational- and cost-efficiency.

This report reviews specific nuclear security and safeguards issues that are specific to NARs and less or not relevant to LCNPPs. It does not examine individual NAR technologies, instead presenting issues that are common across multiple designs. Starting from a discussion of the differences between NARs and LCNPPs, more than 20 security and safeguards considerations are elucidated, leading to several recommendations for NAR stakeholders. Overall, these issues demonstrate that security and safeguards should be considered early in the process, alongside safety.

The smaller power capacities of NARs mean that operational budgets will be relatively constrained. To ensure appropriate levels of safety, security and safeguards new approaches may be required to deliver these functions. To this end, developers should build security and safeguards into their design. New technological security solutions to detect threat actors as early as possible, coupled with a range of layered delay features, can slow adversaries until an adequate response can be mounted by off-site personnel, allowing a reduction in on-site personnel numbers.

Developers will also need to consider the security and safeguards implications of novel NAR deployment choices, such as smaller site footprints, their siting (for example, in highly isolated locations or in locations close proximity to non-nuclear facilities), and the mobilisation of NARs on sea or land vehicles. NAR concepts are intended to operate with fewer staff than LCNPPs, with many intending to use significantly more automated systems to support operations. Such systems may be operated remotely by off-site staff. This increased use of digital systems underscores the importance of strong cybersecurity protections and creates a need for secure and reliable communications between the site and remote operators where relevant. There may be security advantages to reducing on-site personnel numbers, as this directly reduces the physical insider threat risk. Conversely, it increases the importance of cybersecurity.

A range of advanced NAR technologies are under development using novel nuclear fuel materials. Many of these will potentially present a higher proliferation risk. Some fuels will not be fixed within the NAR, creating unique difficulties for nuclear materials accountancy and control, and safeguarding. Furthermore, many NAR designs are planned to operate on a single fuel load for many years, or even decades, creating challenges for continuity of knowledge in safeguarding.

The above considerations represent just a small number of key issues that NAR developers, potential operators, regulators, national governments, and the International Atomic Energy Agency (IAEA) must address. These stakeholders must work together in a spirit of open communication and collaboration to effectively address these issues whilst there is still time to integrate solutions into developing NAR designs, helping the benefits of NARs to be realised internationally.

List of Abbreviations

AMR	Advanced Modular Reactor
AP	Additional Protocol
ARIS	Advanced Reactor Information System (a database maintained by the IAEA of advanced nuclear power reactor designs)
CapEx	Capital Expenditure
CSSS	Centre for Science and Security Studies
CoK	Continuity of Knowledge
HALEU	High Assay Low Enriched Uranium (uranium with an enrichment of 5-20% ^{235}U)
HTGR	High-Temperature Gas-Cooled Reactor
IAEA	International Atomic Energy Agency
IEMO	Initiating Event of Malicious Origin
LCNPP	Large Conventional Nuclear Power Plant
LEU	Low Enriched Uranium (used here to refer to uranium with <5% ^{235}U).
LWR	Light Water Reactor
MBA	Material Balance Area
MOX	Mixed OXide nuclear fuel
MSR	Molten Salt Reactor
NAR	Novel Advanced Reactor (a blanket term combining SMR and AMR)
NMAC	Nuclear Materials Accountancy and Control, sometimes also termed MC&A
NPP	Nuclear Power Plant
NRC	US Nuclear Regulatory Commission
PHWR	Pressurised Heavy Water Reactor
PRIS	Power Reactor Information System (a database maintained by the IAEA of all nuclear power reactors which have at least started construction)
SeBD	Security by Design
SgBD	Safeguards by Design
SMR	Small Modular Reactor
SQ	Significant Quantity
SSAC	State System of Accounting for and Control of nuclear materials
TNPP	Transportable Nuclear Power Plant
TRISO	TRIstructural ISOtropic (a fuel form consisting of <1 mm fissile material kernels surrounded by layers of graphite and silicon carbide, within bulk solid graphite)
UNF	Used Nuclear Fuel (sometimes known as Spent Nuclear Fuel: SNF)
URC	Unacceptable Radiological Consequences

1. Introduction

1.1. Background

Over the last decade, a growing number of new and established nuclear technology vendors have been developing design concepts for Novel Advanced Reactors (NAR). These designs distinguish themselves from the Large Conventional Nuclear Power Plants (LCNPP) operating or under construction globally by nature of their reduced power output and/or multifunctional use through advanced design features. NAR are divisible into two broad groups: Small Modular Reactors (SMR), which use evolutionary technology based on current LCNPP designs, and Advanced Modular Reactors (AMR), which have fundamentally different designs, and use advanced materials and controls. It is anticipated that it will be at least 20 years before AMRs are deployed at grid scale [1]. Dozens of NAR designs are in rapid development globally, with a small number of prototype SMR models either under construction or recently put into operation [2]. It is expected that the deployment of SMRs will accelerate within the next 10 years.

The international market for nuclear power plants is increasingly driving towards the use of NARs, either alongside or in place of LCNPPs. There are numerous potential benefits to NARs which have been explored in detail elsewhere [1]. However, the main drivers for NAR development stem from a need to transition towards cost-effective, low carbon and reliable energy generation, which current solutions cannot provide. Within nuclear, LCNPPs have now become so expensive as to place them beyond the reach of all but the richest nations working hand-in-hand with large state-backed engineering firms [3]. NARs have the potential to act as reliable, low carbon generating assets which, whilst still highly expensive, are within the financial capacity of a much wider range of states.

1.2. Purpose and Objectives

Thus far, most NAR developers have placed significant emphasis on nuclear safety, in many cases building this into their concepts as a core driver. However, nuclear security[1] and safeguards[2] considerations have received comparatively less attention. Developers generally approach security with an underlying assumption that the safety features of their designs render nuclear material less accessible from NARs when compared to LCNPPs. Proliferation resistance is also often one of the reactor design attributes highlighted by the technology developers. However, developing and meeting safeguards commitments are the responsibility of the state and the facility operator. Hence, safeguards are often neglected as a consideration during NAR design [6]. In addition, many NAR developers hire staff into safety-focussed roles much earlier in their design process than security-focussed roles.

This paper seeks to provide a comprehensive overview of the nuclear security and safeguards issues which are specific to NARs and differentiate them from LCNPPs. As there is a wide variation between NARs, some of these issues are technology specific. However, many of the design and risk management processes that determine nuclear security and safeguards requirements are the same, enabling a common approach in how these may be addressed for each NAR design. As such, this paper does not seek to provide NAR stakeholders with solutions for specific reactor types. Instead, the reader is encouraged to use this paper as a guide as they seek to elucidate the requirements for differing NAR designs and identify opportunities to implement improved security and safeguards mechanisms, both within their own national context and beyond.

1 "Nuclear security is defined as the prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities" [4].

2 Nuclear safeguards are "a set of technical measures… to independently verify a State's legal commitment not to divert nuclear material from peaceful nuclear activities to nuclear weapons or other nuclear explosive devices." Safeguardability is a property of a nuclear facility, defined as how easily and effectively it can be subject to safeguards [5].

Many NARs are still in design, presenting an opportunity to embed into them recognised best practices of Security by Design (SeBD) [7]– where security is built into a Nuclear Power Plant (NPP) during its design phase, as opposed to being retrospectively bolted on to an already finalised design, the common approach for LCNPPs. This can also apply to nuclear proliferation resistance, in the form of proliferation resistant design and Safeguards by Design (SgBD) [8]. Both SeBD and SgBD have the potential to enhance nuclear security and proliferation resistance whilst reducing NPP design and operating costs, increasing the international appeal of these low carbon energy sources.

1.3. Methodology

This report draws on an extensive literature review and interviews with a range of international industry subject matter experts. Eight experts were consulted, all of whom have considerable experience in the security and safeguarding of nuclear energy systems, and either actively work, or have worked, on the development of NARs.

1.4. Scope and Intended Audience

This report presents nuclear security and safeguards considerations for NARs throughout their lifetime, from the design and site selection stage through operation to eventual decommissioning and site remediation. It also covers facilities for the manufacture of NARs and their associated modules, and relevant nuclear materials, from assembly to on-site interim storage as Used Nuclear Fuel (UNF). This report does not specifically examine nuclear fuel cycle facilities, although many of the considerations and recommendations listed here will apply at such facilities.

The considerations presented here will be relevant both to those who design and implement security and safeguards systems – reactor designers, prospective technology buyers, and NAR operators, and those who control the frameworks within which nuclear energy systems operate – regulators, national policy makers and international governance bodies. There is a need for clear, consistent, and frequent communication between these stakeholder groups as NARs progress from conceptual to final design and implementation, to ensure that security and proliferation resistance are built into the design holistically alongside nuclear safety and operational considerations.

1.5. Previous Work on this Topic

Whilst some previous work has been done on this topic by others, a single comprehensive overview of security and safeguards considerations for NARs is missing and will add value to the field at this critical moment as NAR technologies, and particularly SMRs, move towards increasingly firm designs and opportunities to reap the benefits of SeBD and SgBD are likely to be lost.

Nuclear security and safeguarding of NARs are relatively immature fields of research when compared with nuclear safety. Security has often been only described as part of a combined presentation of “safety and security” issues, although there have been some efforts to address security and safeguards issues, which are briefly reviewed below. There also exists an array of more narrowly focussed work in the scientific literature, on issues related to specific reactor or fuel designs, or technology categories. Guidance in this area from official sources, such as the International Atomic Energy Agency (IAEA), is still in development, with the Agency holding several recent events to explore these topics [9, 10]. In addition, the Design and Safety Analysis Working Group of the International SMR Regulators Forum had planned in 2021 to focus its work on security for the period until 2023 [11].

Several independent organisations have also prepared reports which touch on security and safeguards aspects of NARs, which may be of interest to the reader. For example, the Union of Concerned Scientists reported on the safety, security, and economics of SMRs in September 2013 [12], and AMRs in March 2021 [13]. The Global Nexus Initiative published a report on the next steps required to advance towards AMRs in June 2019, including a brief assessment of both security and safeguards [14]. The World Institute for Nuclear Security, with support from Nuclear Threat Initiative, published a report on the security of AMRs in August 2020 [15].

The Proliferation Resistance and Physical Protection working group of the Generation IV International Forum has produced a range of detailed technical work of relevance to AMRs [16]. Finally, technical work on advanced reactor security and safeguards is being delivered through the Gateway for Accelerated Innovation in Nuclear programme, with a particular focus on novel reactor technologies [17]. The aforementioned reports focus primarily on specific advanced reactor types or fuels, differing from this paper which seeks to present a broad overview of security and safeguards considerations.

1.6. Structure of this Report

The remainder of this report leads off with a presentation of nuclear security and safeguards principles in Section 2, including security risk assessment and management methods. This is followed by an examination of NARs and how they differ from LCNPPs in Section 3. Section 4 will explore the security, safeguards and proliferation resistance considerations created by these differences. The report ends with recommendations on how the considerations raised could be effectively approached in Section 5, and conclusions in Section 6.

2. Security and Safeguards: Key Elements and Approaches

2.1. Aims of Nuclear Security and Safeguards

Nuclear safety and security have the common goal of protecting the public and the environment from the harmful effects of radiation from uncontrolled radiological releases, be they from an accident or sabotage at a nuclear facility. In addition, nuclear security and safeguards aim to prevent the theft or diversion of sensitive nuclear materials and technology, reducing the risk of further nuclear weapons proliferation to state and non-state actors.

Broadly, nuclear security seeks to mitigate the risks posed by external adversaries – individuals or groups seeking to steal nuclear materials or carry out acts of sabotage – and "insiders" who misuse their authorised access to nuclear facilities to achieve the same objectives. Insiders may act alone or in concert with external adversaries. Their methods evolve over time and with the availability of new technologies. For example, there is now an increasing emphasis on the risks posed by cyberattacks and how these can be used to enable theft or sabotage [18].

Nuclear safeguards aim to prevent the diversion of nuclear materials and technology from civil purposes into military applications through the timely detection of the diversion of significant quantities of nuclear materials from peaceful activities. The other aspect of safeguards is the prevention and detection of misuse of nuclear facilities. The IAEA also seeks to detect undeclared activities and materials in member states to strengthen the international safeguards regime [19].

2.2. Nuclear Security Risk Assessment

In designing nuclear security systems, risk assessments are carried out examining both the likelihood of and consequences stemming from nuclear facility sabotage and/or theft of nuclear materials. Such consequences might include, for instance, uncontrolled radiological release, or the acquisition of weaponisable nuclear material by terrorist organisations [20].

For the purposes of this discussion, we will focus on uncontrolled radiological releases. When the severity of such a release surpasses tolerability, it is said to have "Unacceptable Radiological Consequences" (URC). Nuclear security seeks to mitigate the likelihood and potential consequences of URC through the application of measures to reduce the risk. The logic behind security risk should be governed by a range of reasonable and conceivable worst-case scenarios for theft and sabotage, leading to the implementation of sufficient and proportionate security measures. Where uncertainties exist, conservative estimations are made to account for this. These scenarios are used to assess the probability of URC resulting from an incident. Ideally, security approaches should be proportionate to the risk and the associated consequences. However, this is not always the case and layers of conservatism can be built up in security approaches, either through directed activity or regulatory guidance. For example, a highly impactful conservative assumption is that an Initiating Event of Malicious Origin (IEMO) is certain to occur – its deterministic probability is one. Excessive conservatism can lead to an overengineered security system and elevated security response with minimal additional benefit, as shown in Figure 2-1. This is often seen with modern LCNPPs, where improved safety and security approaches have often been added alongside existing systems, rather than replacing them [3].

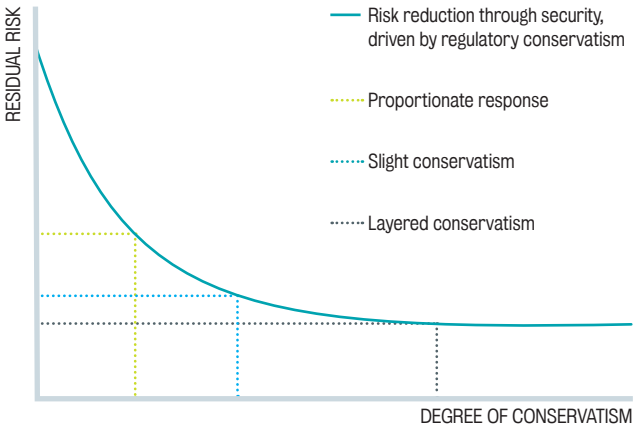

Figure 2-1: Reasonable conservatism in the face of risk uncertainty is sensible. However, when layers of conservatism build up this can drive the overengineering of security systems, resulting in increased system complexity, scale and cost with little additional security benefit. Please note that this figure is simply an indication of the relationship between conservatism, which drives the implementation of security measures, and residual risk. No mathematical relationship between these two factors should be inferred.

Risk is created by the interplay of three factors when related to a critical asset:

1. The security threats to the integrity of nuclear material – sabotage, theft or diversion;

2. The categorisation of the Nuclear Material in relation to potential consequences, e.g., a URC originating from the uncontrolled compromise of the material;

3. The vulnerabilities of the nuclear facility and access to nuclear material that might allow the consequences to be realised.

The application of risk management can allow for mitigation of the threat through deterrence and a reduction in consequences and vulnerabilities, as shown in Figure 2-2.

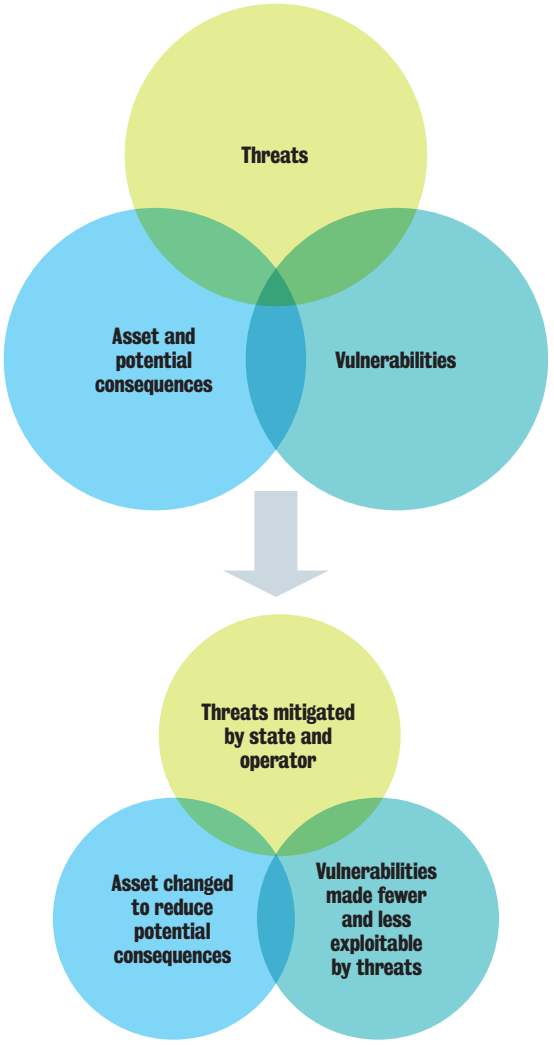

Figure 2-2: Top: Interplay of threats, assets (consequences) and vulnerabilities in the creation of nuclear security risk – the central area in which all three overlap. Bottom: Application of nuclear security and proliferation risk assessments to mitigate the threat and reduce consequences and vulnerabilities, shrinking the central area of overlap and thus reducing risk.

The key factors which drive consequences are the quantity and types of nuclear materials at the facility. The IAEA categorises nuclear materials for security purposes into three groups, with Category III requiring the lowest level of protection and Category I the highest [21]. Consequences can thus be lowered by reducing the quantities of nuclear material at the site, especially higher Category materials. Alternatively, materials may be made more resistant to attackers or the efforts of thieves or proliferators. For instance, storing separated plutonium as a toughened bulk material, rather than as a fine powder, will reduce the ability of saboteurs to disseminate the material in the air by setting off an explosive device nearby. Likewise, diluting a quantity of nuclear material within a large volume of inert solid matter will make it harder for a proliferator to acquire a significant quantity of material for a nuclear weapon.

Overall, vulnerabilities are driven by specific design choices or an absence of their consideration. These might include, as examples, access points to sensitive areas, nuclear fuel loading/unloading areas, critical safety equipment, and any other location or process where nuclear materials are potentially accessible or where acts of sabotage could lead to URC. As such, there is no single approach towards vulnerability reduction, and this is something that must be considered for each individual technology. However, two key approaches to vulnerability reduction lie in creating sufficient protective measures to negate the probability of success, and in imparting sufficient ability to detect and delay adversaries to enabling an effective response to neutralise the threat. This is best achieved through the integration of security into NAR design at the earliest opportunity, integrated alongside safety and other considerations. It is in vulnerability reduction that SeBD approaches will be most effective.

According to the IAEA there are four basic elements to nuclear security — deterrence, detection, delay, and response. Useful and complete definitions of these can be found in IAEA publications and online, but a brief explanation is provided here for the convenience of the reader [22, 23]. Effective security systems consider all four elements as part of a holistic approach to security.

Table 2-1: Four key elements of effective nuclear security.

Element	Description
Deterrence	Dissuading threat actors from taking action against the nuclear site.
Detection	Detecting the planning for, or execution of, malicious activity against a site.
Delay	Slowing adversaries, thereby maximising the time available to respond.
Response	Timely interruption and neutralisation of the adversary to prevent their success.

2.3. Safeguarding of Nuclear Materials

Nuclear safeguards systems provide an essential means for preventing the theft or diversion of weapons useable fissile materials from nuclear facilities. The goal of nuclear safeguards is the timely detection of the diversion of significant quantities of nuclear materials from peaceful activities. *Timely* is defined by how readily the diverted material could be converted into a weaponisable form, while a *Significant Quantity (SQ)* is defined based on the quantity required to fabricate a rudimentary nuclear weapon, which can be as little as 8 kg [24].

The area of international safeguards, implemented by the IAEA, characterises one of the only major mechanisms of international cooperation to reduce the risk of nuclear weapons proliferation and promote peaceful use of nuclear energy. Safeguards include all activities undertaken by the state and the IAEA to ensure accurate accounting for and control of nuclear materials from civilian nuclear facilities. Measures taken by individual states are known collectively as State Systems of Accountancy and Control (SSAC). Hence, nuclear safeguards are applied to the entire nuclear fuel cycle and are not only limited to nuclear reactors.

The international safeguards framework was developed following the coming into force of the Treaty on the Non-proliferation of Nuclear Weapons in 1970 [25]. The IAEA safeguards approach continues to evolve to maintain credible safeguards to meet the new verification demands from IAEA Member States. The most recent addition to the set of IAEA safeguards agreements is referred to as the Additional Protocol (AP). Two significant additions in the AP agreements are the ability for the inspectors to deploy environmental sampling and the ability to use remote monitoring techniques (for example, satellite imagery) to detect illicit activities. By the end of 2021, there were 184 states with safeguards agreements in force with the IAEA, of which 136 had AP in force [26].

Existing nuclear safeguards systems are robust and mature. The use of fuel enriched to less than 5% in U-235, known as Low Enriched Uranium (LEU), in LCNPPs make the fuel material effectively unusable in weapons. However, the amount of enrichment effort necessary to achieve 5% enriched uranium represents about 80% of the total effort to get to 80% enriched uranium, which is much more useable in weapons applications. The material at the enrichment facility is in bulk form and hence requires different safeguards measures for accounting and control. Unlike fuel assemblies at the nuclear reactors, which are handled as discrete units, the material flows at enrichment facilities provide the opportunity for continuous diversion scenarios.

Similarly, the safeguards measures put in place for Light Water Reactors (LWR) using scheduled refuelling cycles have mature safeguards measures in place for materials accounting, surveillance, and control. IAEA safeguards inspections are planned accordingly, limiting requirements for the on-site presence of safeguards personnel to relatively small windows of time. For reactors with online refuelling, such as Pressurised Heavy Water Reactors (PHWR), different solutions are necessary. Several intrinsic and extrinsic proliferation barriers, combined with higher frequency inspections protocols, have been implemented to meet IAEA international safeguards goals. Compared to LWR, the safeguards systems necessary for PHWR reactors require greater coordination between facility operators, state authorities, regional and IAEA safeguards personnel [27].

Overall, for LCNPPs operating in an open fuel cycle (without reprocessing), the risks of diversion of material and misuse of facilities are well characterised. However, as we look towards NARs, the domestic and international safeguards community will face new challenges and opportunities to build on the success of the past by designing reactor systems that reduce diversion pathways through the entire nuclear fuel cycle, including the reactor. Hence, whilst safeguards may not be a critical step to licensing from the perspective of NAR developers, an understanding of the current safeguards systems will inform design activities so that safeguards verification requirements can be easily met during operation. Reducing safeguards burden in this way could give NAR designs a competitive advantage.

The elements of the safeguards regime for materials control include material balance and reporting, measurements of material flow and inventory verification, containment, surveillance, and remote monitoring. Safeguards measures are carried out in part by IAEA member states, which make declarations to the IAEA covering their nuclear activities. The IAEA then independently verifies the correctness and completeness of each state's declarations [27]. Nuclear Materials Accountancy and Control (NMAC) processes are used by states to account for their inventories and prepare their IAEA declarations [28].

NMAC is relevant to safety, operations, security and safeguards. The use of measurements, analyses, records, and reports to maintain precise knowledge of the inventories of special nuclear material in defined Material Balance Areas (MBA) of the facility are the elements of NMAC for nuclear safeguards. The objectives of the accounting system are to provide:

1. Knowledge of exact amounts of nuclear materials,
2. Timely detection of a material loss, and
3. An estimate of amounts lost and their location.

Based on this knowledge, in order to follow the best practice design principle of SgBD, a reactor designer could incorporate proper controls to detect the diversion or eliminate availability of material with lower conversion time at any stage of the material life cycle in the reactor. This would extend the timeline for detection of material loss, thus reducing inspection frequency and limiting the requirements for high fidelity measurements.

3. Differences between Novel Advanced Reactors and Large Conventional Nuclear Power Plants

The international market for nuclear power plants is increasingly driving towards the use of NAR, either alongside or in place of LCNPPs. There are numerous benefits to NAR which have been explored in detail by other authors [1]. However, some of these potential benefits have a bearing on security and safeguards, even for the most conventional SMR designs. These benefits and differences are explored below, with the security and safeguards considerations they create discussed later in the corresponding sub-sections under Section 4. These are further summarised in an Annex at the end of this document.

3.1. Power Capacity and Modular Manufacture and Construction

NARs generally have smaller power capacities than LCNPPs – typically up to 300 MWe, although there are some NAR designs which exceed this [2]. The reduced size allows for major equipment, including complete nuclear steam supply systems, to be mass manufactured on a production line and transported as a series of prefabricated modules for installation at a site. Nuclear fuel can also potentially be installed at the point of manufacture, with the NAR then being transported in a fuelled state. This creates efficiencies in plant production, lowers risk in NPP construction and reduces work required at the site, while also allowing for greater experience sharing between standardised NPPs. This stands in contrast to LCNPPs, which are constructed generally as huge, so-called megaprojects, where much of the plant construction occurs at the site, each NPP is somewhat unique, and construction delays and budget overruns are commonplace.

3.2. Reduced Capital and Operating Costs

The greatly reduced size and ability to manufacture NARs on a production line basis is expected to drive reductions in capital cost compared to LCNPPs. As mentioned in Section 1.1, the reduced capital cost and associated financing costs place NARs within the reach of more states and potential operators than modern LCNPPs. Some developers have claimed that the installed cost per megawatt of capacity will also be lower than LCNPPs, and whilst this claim is debated [29, 30], it is highly likely that NAR capital costs will be an order of magnitude below those of LCNPPs [31].

The reduced size of NARs means that they will produce less energy than LCNPP, assuming equal capacity factors. Without a compensating increase in energy price, NAR revenues will be lower than LCNPPs, meaning that they will need to reduce their operating costs to be economically viable as commercial power producers. Many designers are taking a range of measures to reduce operating costs, such as reducing personnel numbers, including in security functions.

3.3. Increasing Automation and Remote Operations

To allow for reduced personnel numbers, NAR developers are designing out the need for human operators and instead adding in a much greater degree of automation than LCNPPs have hitherto used. This also opens the door to remote operation by off-site staff, and even fleet operation of numerous NAR units from a centralised off-site location. It should be noted that there is no specific impediment to LCNPPs also seeking to automate, and future designs may do so, although until now they have limited themselves to the introduction of digital instrumentation and control systems as an aid to human decision making, rather than autonomous plant operation.

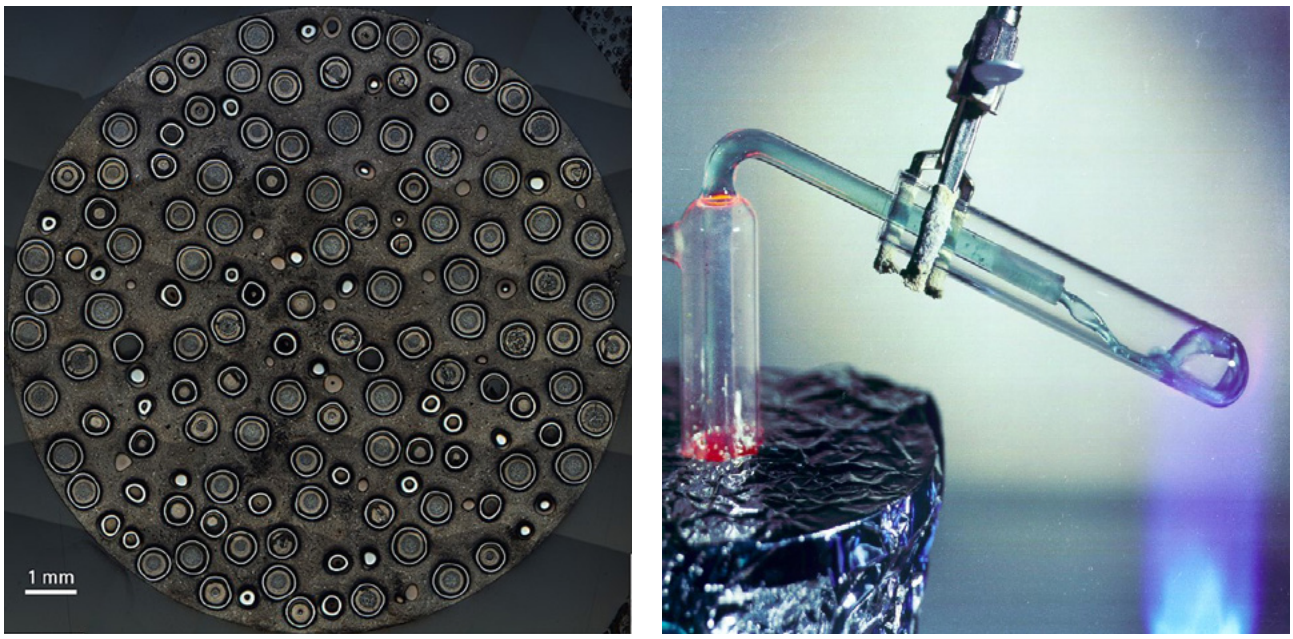

Figure 3-1: Images of novel nuclear fuel physical forms. Left – cross section of TRISO fuel, showing <1 mm kernels fissile material surrounded by layers of graphite and silicon carbide, dispersed within a graphite matrix [34]. Right – molten lithium beryllium salt of the type under consideration for use in many Molten Salt Reactor (MSR) designs [35].

The increased use of autonomous digital agents in nuclear energy systems represents a major change in how NPPs will operate, taking humans increasingly out of direct operations into a monitoring and decision-making role. This can also allow for a proportion of operational activities to be carried out remotely; for some small NAR concepts, the design goal is the complete automation of the entire plant, where the human role is completely removed. This will also allow for fleet operation or monitoring of a distributed network of plants by a centralised team.

3.4. Advanced Reactors and Fuels

Many NARs developers are planning to use advanced reactor and fuel technologies to deliver a range of operational and safety advantages compared to LCNPPs, although the wide variation across the range of NARs means there are few ubiquitous features between them. Almost all are designed to make use of passive safety features, meaning that in any accident scenario the reactor will remain safe, even in the absence of operator input or access to external power or cooling water [33]. Being of a lower power rating than LCNPPs, NARs generally also require lower nuclear materials inventories.

Many of the NAR designs will use fuels that are significantly different than the current fleet of LCNPP. These fuels will improve safety and sustainability aspects of NARs as they would mitigate issues such as fuel meltdown and provide much higher burnup of the fuel extending the time in between refuelling and, in some cases, completely removing the need for refuelling. Details of a range of proposed technologies can be found in the IAEA's Advanced Reactor Information System (ARIS) database [2]. Some examples of novel security and safeguards challenges are worthy of broader discussion. For example, several designs aim to operate for extended periods without refuelling – some as many as 30 years. Several proposed NAR designs operate in the fast neutron spectrum. This enables these reactors to use fuel materials which are currently designated as liabilities, such as civilian plutonium stockpiles and transuranic elements. Two technologies of specific note are Molten Salt Reactors (MSR) and pebble bed High Temperature Gas-cooled Reactors (HTGR) using TRISO fuel. Images of fuel samples for these reactors are shown in Figure 3-1. In both cases, the fuel is not static but rather flows through the reactor, similarly to the continuous online refuelling of PHWRs.

However, in case of HTGR using TRISO pebbles the fuel is continuously mixing and hence may have to be treated as bulk material when in the core rather than discrete fuel bundles. MSRs with liquid fuels present additional challenges of a continuous material stream, on-line refuelling, and reprocessing. Finally, several designs also have the flexibility of being able to use thorium.

Generally, NARs will use a much broader range of novel fuel materials, stepping away from Low Enriched Uranium (LEU) oxide with less than 5% ^{235}U as used in most LCNPPs. Some of these include uranium of enrichment up to 20%, known as High Assay Low Enriched Uranium (HALEU), uranium-plutonium Mixed OXide fuels (MOX) and thorium fuels. Some developers intend that fuel cores will be assembled as a module separate from the reactor, and that rather than refuelling the reactor that whole cores will be installed, irradiated, and then removed and exchanged. In such NARs, refuelling at the site will use 'plug-and-play' cores, in contrast to LCNPPs where fuel is often either removed from the core, partially replaced, shuffled, and reintroduced, or cores are refuelled continually on a channel-by-channel basis. This brief review of the new fuel types and forms that are being proposed for use in NAR show that significant work still remains to be done and operational experience to be gained before these become available for large scale deployment.

3.5. Deployment and Siting Options

The smaller size of NARs, coupled with the implementation of advanced passive safety features to reduce or eliminate their demand for off-site power and cooling water supplies, allows for greater flexibility in deployment. LCNPPs are currently constructed within very large site footprints, with a site boundary perimeter fence far from the protected asset. NARs on the other hand are looking at a wider range of deployment scenarios, driving an intention to shrink plant footprints, reducing the distance between the site boundary and the protected asset. Many technology developers are also seeking to reduce emergency planning zones, allowing for NARs to be sited much closer to non-nuclear facilities. This could allow, in theory, the deployment of a network of NARs within an urban area.

Furthermore, NARs are scalable – a single unit might be used to supply heat and power to support a remote community isolated from large, reliable electrical distribution grids. Two or three such units, or a single larger unit, might supply power to an energy-intensive collocated industrial application, such as steel making or water desalination. Alternatively, a larger number of units might be sited together to replace an LCNPP or fossil fuel power plant, giving greater operational flexibility or eliminating carbon emissions.

Scalability also brings operational benefits to sites with many NAR units. As the number of units increases, the impact of shutting down a single unit for refuelling has a reduced impact on the total capacity of the site. For instance, for a site with 12 reactors, each one could be shut down for one month per year for refuelling and maintenance, and the capacity factor of the whole site will be stable at above 90%. In contrast, when an LCNPP reactor shuts down, a large amount of electrical generating capacity is removed from the grid, and such shutdowns must be planned in consultation with other generating assets on the grid to prevent power outages for users.

The smallest NARs can be mounted on and operated from mobile platforms. For example, the *Akademik Lomonosov* floating nuclear power plant already supplies electricity in Siberia (see Figure 3-2) [36], and plans for road mobile nuclear energy systems are being considered, at least in the military domain [37]. These Transportable Nuclear Power Plants (TNPP) offer potential benefits in terms of being able to supply nuclear energy much more rapidly to areas in need, having applications in disaster relief or providing energy to locations without the necessary infrastructure to accept a fixed land based NPP.

Figure 3-2: The *Akademik Lomonosov* floating nuclear power plant at Murmansk port in Russia, before sailing to Siberia. [38].

3.6. Developer Business Models and Marketing Approaches

Within this paper, the terms "NAR developer" and "technology developer" are used to refer to any organisation carrying out NAR design activities. However, there are a range of business models amongst the NAR developer community, within which individual NAR technologies may fit. At one end of the scale are science and engineering research organisations and academia, who are usually developing NAR technologies or elements thereof with the intention of then selling or licensing their intellectual property to another organisation. The rapid expansion of several start-ups funded through private equities and angel investors is new for nuclear energy sector. This has fuelled innovation similar to the technology revolution of the 1990s.

At the next level are organisations following the formerly common business model of LCNPP development companies – they seek to deliver a complete NAR plant design which will then be sold or licenced to a prospective operator and/or construction firm. One step further, developers are planning to adopt the modern LCNPP business model through the formation of consortia with construction, operation and potentially financing organisations. Finally, some developers intend to also construct and/or operate their own NAR designs, rather than working with a separate operator.

What is common across all technology developers is a desire to distance their technology from the publicly perceived challenges of nuclear energy – danger of radioactive releases, concerns around waste management, and more recently excessive costs and overruns in construction time and budget. The management of any residual security or safeguards hazards is likely to be significantly impacted by this commercial intent. Thus, a key marketing objective for NAR developers is to present their designs as completely distinct from LCNPPs. Developers are working hard to realise the promise of NARs to be a source of clean energy generation, which is safe, secure, and free from proliferation risk, and has improved nuclear waste management and a lower cost and risk profile.

4. Nuclear Security and Safeguards Considerations for NARs

In this section, the security and safeguards considerations stemming from the differences in Section 3 are presented. Sub-section numbers correspond between the two sections, with differences in Section 3.1 leading to the considerations in Section 4.1 and so on. Again, these are summarised in table format in the Annex to this paper.

4.1. Power Capacity and Modular Manufacture and Construction – Considerations

4.1.1. Construction Approaches for NAR

Whilst the prefabrication of modules on a production line creates numerous advantages for NAR construction, it also introduces potential vulnerabilities. Complete nuclear reactors will be produced and stored at centralised production facilities, meaning these facilities must thus be appropriately secured, especially if the reactor will also be fuelled at the facility. There are also safeguards considerations for these facilities if handing nuclear material, as complete reactors or plug-and-play cores will contain significant quantities of nuclear material which will then be transported to a site for installation, potentially requiring export of the core to other states which may not have IAEA safeguards agreements. One potential approach to safeguarding would be to treat these cores as single items and applying IAEA-monitored active seals to them at the point of manufacture, only removing these when the core is to be installed at its destination [39].

4.1.2. Transportation Considerations for NAR

Off-site prefabrication of modules for later installation at the nuclear site means that NARs will be transported in a much more complete state than LCNPPs, increasing their attractiveness as targets to threat actors. Nuclear materials and equipment in transit are exposed to additional vulnerabilities compared to when they are at secure sites [6].

Road and rail vehicles move along predictable paths and may be less accessible to response forces if they are not embedded in the movement convoy. The additional risk can be mitigated, however, through the same principles of detection and delay. The NAR or modules, if designed according to SeBD principles, may offer a degree of delay to sabotage or theft attempts. This will be enhanced by an integrated design process for the transportation package, incorporating sufficient security and safeguards measures. Continuous remote monitoring of the cargo under transportation could also allow for the early detection of activity by threat actors, as well as tracking of stolen equipment and materials for recovery, for instance, by using autonomous drones.

4.2. Reduced Capital and Operating Costs – Considerations

4.2.1. Reduced Operating Budgets for NARs compared to LCNPPs

NARs need to reduce operating costs compared to LCNPP without compromising safety, security, or safeguards. Lyman estimates that costs associated with security staff represent 15-25% of large LWR operations and maintenance costs in the US [12], whilst in the UK security costs can make up approximately 8-10% of total annual operating costs [31]. Furthermore, the greatest proportion of security costs are direct costs for personnel [6]. NARs may not be able to operate economically if they are required to deliver security in the same way as LCNPPs [6, 15, 40]. As such, new approaches will be required to deliver the same or improved standards, and it is through technological innovation that many developers intend to do this.

"If SMRs, AMRs or Advanced Nuclear Technologies are going to achieve everything that everybody is hoping, then we need to start innovating now. We need to stop thinking that we can pick up an existing physical security system and just essentially drop it and resize it for an SMR. The question should instead be 'how do we achieve the outcome? What are the technologies we may need, now or more likely in the future, to deliver that outcome?' [31].

Innovation from developers, flexibility from regulators and integration of security with other functions will be required to allow NARs to compete in the energy marketplace. Technology can provide some of the key elements of security listed in Table 2-1 more readily than others – detection and delay can be built into NAR designs, buying additional time for an effective response. However, as yet there are no sufficiently mature technological solutions to deliver response, and human responders remain the best option. If the NAR design itself is self-protecting against all credible threats for, e.g., two hours, this means that the need for a dedicated on-site response capability could potentially be eliminated if an off-site response force can arrive and effectively neutralise the threat within this time window. This also opens up the possibility of using non-dedicated responders drawn at-need from law enforcement or the military. Whilst design costs and capital expenditure for NARs may be increased as a result, these increases will be minimal compared to the lifetime costs of dedicated security personnel. One expert cited an example of a Category I nuclear materials storage facility, for which the implementation of SeBD led to a total capital cost increase of less than 3%, far less than the total cost of paying additional security personnel costs over the facility's lifetime would have been [41].

4.2.2. Reduced Capital Cost of NAR Compared to LCNPP

The lower capital expenditure requirements to construct an NAR compared to an LCNPP will make these technologies available to new states for which nuclear energy had previously been unaffordable. The potential benefits of NARs can be highly attractive to policymakers, but they must develop suitable legal and regulatory systems to ensure the 3Ss of safety, security and safeguards are delivered in line with international standards and not seek to implement NARs prematurely.

Technology developers should consider the differing regulatory regimes, threats and levels of organisational maturity within potential customer countries, allowing for SeBD and SgBD to alleviate the burden for operators. According to one interviewee, "The U.S. government is trying to work with [NAR] vendors. They understand what the implications are for security and safety in other countries to allow them to be more marketable...But given that a lot of these vendors are not even thinking about security right now, it is hard to get them to think about more than one country's security regulations" [6]. Developers thus need to ensure security and safeguards are considered as part of their design for all markets, both foreign and domestic. This could allow developers to develop a small number of variations around their core design to meet specific needs, as this may be economically advantageous. For instance, some security options, such as measures capable of delivering lethal force, may be less acceptable in some markets than others. As such, different variants could be designed – with and without certain features.

4.3. Increasing Automation and Remote Operations – Considerations

4.3.1. Reducing the Human Role in Plant Operations

Many NAR developers are planning to use automated systems to replace human personnel. Technological solutions are developing rapidly, and developers can look ahead to anticipate the security possibilities which may be available at the point of NAR deployment.

This might be achieved through the use of directional, multi-sensor surveillance masts and/or autonomous drones capable of patrolling sites to detect potential threats, allowing for a much smaller team of human monitors than would have been required to conduct foot patrols of the facility. However, a full consideration of such changes is required, for example, the normalisation of drone flight around the facility may create new vulnerabilities by allowing adversary drones to go unnoticed.

The use of reliable and well-integrated autonomous systems can free up human operators from mundane monitoring tasks to take on higher-level oversight and critical decision-making roles. However, the proper development and assurance of such systems will be critical if they are to be sufficiently trustworthy for nuclear use.

NAR developers will need to consider how they can both build in and demonstrate the required levels of performance to allow plant monitoring and decision making to pass from humans, as delivered in LCNPPs, to digital systems. If this can be achieved in nuclear security, the human role in threat detection can be greatly reduced, and this can be extended beyond detection if the system can take independent decisions on the deployment of active delay features and/or act as the decision-maker for response force deployment. Developers will need to apply systems thinking approaches to consider how humans and digital agents will interact to ensure optimised security at lowest cost. Such approaches may also be applicable in nuclear safeguards, allowing for autonomous monitoring of safeguards-relevant information and making immediate notifications to the IAEA in case of concerning behaviour.

Beyond security and safeguards, digital and automated systems are planned for introduction throughout plants. As they gain greater control over NAR operations, it must be borne in mind that such systems are potentially vulnerable to cyber threats. Best practices of cyber security design must be followed in any nuclear facility to secure digital systems, both against today's threats and also potential future adversary capabilities – such future proofing reduces the risk that additional work will be required in future to re-secure the facility [42].

4.3.2. Remote and Fleet Operation of NARs

Remote operation of NARs will mean that a large quantity of critical data will constantly be exchanged between the NPP site and off-site personnel, increasing the potential consequences of cyber-attacks, and thus driving the importance of cyber security in remote operations. The Stuxnet cyber-attack showed that a virus can interfere with nuclear industrial systems whilst sending false signals to control room operators [43]. Operators must have confidence in the integrity of the data received from plant instrumentation and that the plant is accurately responding to their commands. Remote operation of secure facilities and critical infrastructure can be done securely. For example, London City Airport's air traffic control functions are delivered remotely. However, this was only made possible by using government-level or near-military level cybersecurity software and systems, which will not be exportable as a component of NARs.

To enable this, national governance bodies may need to be involved in supporting the development and assurance of commercial, exportable cybersecurity products which can offer suitable protections for NARs.

To ensure security and integrity of communication between remotely operated NARs and central control points, multiple independent communications methods must be ensured, which might include dedicated hardwired connections, satellite communications, internet-based systems and other methods. Where infrastructure for such methods does not exist, it will need to be developed. Communications must be designed such that no credible scenario can compromise all methods of exchanging data with the NAR, with automated systems of mutual authentication and communications monitoring to guard against falsification. Any deviation between communication lines could indicate a cyber-attack in progress and be responded to appropriately, with the plant automatically taking appropriate actions to place itself into a safe and secure state until communication can be restored.

Operation of security at a remote site will be determined by the effectiveness of autonomous detection and delay systems with an associated requirement to achieve a high confidence in effectiveness through design and pre-installation performance evaluation and integrated design efforts. The purpose of this must be to provide the highest probability of detection, analysis, and assessment of potential threats to the NAR site. This is necessary to ensure that any activation of a remote response capability occurs with the strongest possible validation. This will create design, installation and operational dependencies which should be determined, analysed, and assessed prior to design lockdown.

Secure network communications and cyber resiliency of industrial digital controls systems are thus part of the critical path to fleet operation of NARs. The development of cyber-physical testbeds, digital twins and cyber intrusion detection systems have gained considerable attention, as new requirements and regulations need to be developed for safe and secure operations of these systems.

Development of the necessary instrumentation and control systems for use with NARs is an important technical area of research and development that would benefit the design, operation, and maintenance of several NAR designs, enabling remote monitoring and eventually autonomous operation capabilities.

4.3.3. Insider Threat Considerations

Significantly reducing staff numbers brings potential advantages in terms of insider threat by reducing the density of the 'threat surface'. The number of individuals who may be compromised by threat actors through improper influence is greatly reduced, allowing the introduction of focussed human reliability programmes which in large installations might be considered unaffordable and unsustainable. This would represent an overall benefit in increasing the trustworthiness of the workforce. NAR developers can further reduce insider threat risk by limiting access throughout the plant. The greater degree of automation, along with operational features of certain NAR types, allow for personnel access to sensitive areas to be more tightly restricted in terms of numbers requiring access. Knowledge amongst on-site personnel may also be reduced by automation owing to an assumption that fewer personnel will require detailed whole-system knowledge of safety-critical features and operational technology.

"We have to create a digital environment that creates trust" [3].

The greatest reduction in physical insider threat can be achieved through complete removal of all personnel from the site. However, even if the NAR is remotely operated by human staff, this will still reduce physical insider threat compared to having those same staff working at the NAR site. All interaction with the plant will be carried out through digital systems with multiple safety fail-safe measures and reportable diagnostics to protect against sabotage along with normal data logging of all user actions. This will both act as a deterrent to malicious activity and provide an evidence trail should such activity occur. Whilst complete removal of all staff from the plant may not be fully achievable, it should still be a design goal, as any progress towards this will greatly reduce insider threat. However, the risk of cyber insider threat remains, and appropriate measures must be taken to guard against cyber efforts by personnel in remote control stations.

4.3.4. Deterrence Reduction

Throughout this paper, it is argued that NAR operators will find it necessary to reduce major costs associated with security, and to facilitate this NAR developers must use SeBD approaches to allow for reductions in the number of security personnel, instead using a combination of early detection and delay features to allow for off-site responders to attend the site and interdict threat actors in a timely manner. This illustrates the greater emphasis necessary to place on the relationship between time and distance when viewing their impact on the operational functions of delay and response. However, the removal of visible personnel from sites may be challenging in an environment where there is a need to provide public assurance of security, and this may create pressure to retain security personnel on site even if not required to deliver the nuclear security function due to the use of SeBD features, which will provide 'inherent security'. This pressure may emerge due to layers of conservative security analysis potentially resulting in an overengineered, costly security system or from policymakers directing that security personnel be deployed to NAR sites even when not required. An alternative approach would be to conduct public outreach to demonstrate that designed security measures contribute to a safety profile which maintains the requirement to minimise possible sabotage or threat through malicious activity.

4.4. Advanced Reactors and Fuels – Considerations

4.4.1. Passive Safety Benefits to Security

As stated in Section 1.2, many developers believe that passive safety and proliferation resistance characteristics of their reactors also convey security benefits, and this is correct – the use of passive safety systems in NARs also benefits nuclear security. Eliminating the need for operator action, off-site power and cooling water removes many vulnerabilities in associated systems, structures and components that can be exploited by saboteurs and reduces the potential consequences of a radiological release. For this reason, security and safety design should be performed holistically and in parallel, to ensure mutual optimisation. Indeed, the US NRC suggests that developers should aim for "Concurrent resolution of safety and security requirements, resulting in an overall security system that requires fewer human actions" [44].

4.4.2. Novel Fuel Materials

This wide range of NAR fuels creates several security and safeguards considerations, and these cannot be comprehensively addressed here. Detailed examinations at the level of the individual NAR design are beyond the scope of this paper, but technology developers must give thorough considerations of the safety, security and safeguards impacts of their specific reactor and fuel cycle choices. Some general considerations are presented below, but the reader is encouraged to engage with work by others on this topic, as discussed in Section 1.5.

Firstly, as stated in Section 3.1, NARs will generally have lower fissile materials inventories than LCNPPs, reducing the potential consequences of security incidents. However, the use of non-LEU fuels means this must be offset against the potentially higher theft categorisation of the fuel [21]. Almost all LCNPPs are Category III facilities, but HALEU fuel will require Category II protections, whilst plutonium or thorium will lead to Category I, with consequently greater attraction for threat actors. The use of thorium adds the need to secure, monitor and account for uranium-233, an isotope which there is no experience of handling in the civilian nuclear fuel cycle. As such, technology developers should not assume that the security requirements of LCNPPs will translate to their concepts and must instead take steps to understand the specific requirements that will apply to them.

Some fuel forms present novel challenges for NMAC, and thus for safeguards. Traditional NMAC and safeguarding approaches at the reactor are designed for fixed fuels, and facility operators lack experience of applying security and safeguards to liquid fuels and fuels with variable residency time inside and outside the reactor core. For both pebble bed HTGRs and MSRs, determination of the quantity of material within the core, the batches from which it came, and its composition are as-yet unresolved technical challenges. Stakeholders working with these technologies will need to consider how they will perform NMAC for security purposes and how they will provide data to the IAEA that satisfies safeguarding, and this is likely to require the development of new inspection and modelling tools. These fuels will be challenging to account for on an items basis, and as such are likely to be handled as a bulk material.

Whilst NMAC may be performed on a mass basis for quantities of these fuels, engagement with the IAEA will be required to ensure planned safeguards approaches are aligned – reprocessing facility approaches are unlikely to be directly applicable, as these are material throughput facilities, whereas MSRs will not operate in this way [39].

A specific security consideration for these bulk fuels is protracted clandestine theft. With a diameter of ~6 cm and a mass of ~250 g, TRISO spheres are small and light enough to be carried in a pocket, and thus could conceivably be smuggled out of a nuclear facility over time to accumulate a significant quantity of nuclear material. However, the number of pebbles necessary to secure sufficient material make them less attractive from a diversion perspective. Additionally, the design of the TRISO particles makes the recovery of the fissile material very difficult. This can be further addressed through proper facility design to eliminate points where small quantities of fresh fuel are accessible, use of surveillance within fuel loading areas, and storing spheres within large, sealed containers. Similar approaches are recommended for MSRs.

4.4.3. Extended Fuel Cycle Length

NARs are targeting a much wider range of refuelling intervals than LCNPPs. The IAEA's ARIS database lists three designs with 30-year fuel cycles, with 15 in the 2- to 10-year range. There are safeguards considerations associated with these long fuel cycle lengths. The necessity of using higher enrichment fuel has been discussed elsewhere, particularly with regards to HALEU fuel. Significant effort is underway to provide reliable fuel supply and adequate operational experience with these fuels in current reactors and near-term SMR designs. The risks of diversion reside elsewhere in the nuclear fuel cycle with some limited challenges at the reactor site mainly from inventory taking and inspections.

Current IAEA safeguards approach and inspections for LCNPPs are designed for 12-24 months refuelling cycles. The safeguards protocols are well developed for materials accounting, monitoring and surveillance of fresh fuel, fuel inside the reactor core, spent fuel storage in pools and eventually in dry casks. Cost efficient safeguarding of such facilities may be achieved, at least in part, through active seals on the reactor and other remote monitoring and surveillance solutions coupled with IAEA inspections.

These much longer fuel cycles will challenge the IAEA's current equipment, requiring changes to the technology that is used, the inspection activities, the inventory recording and reporting requirements. Assuring Continuity of Knowledge (CoK) under such circumstances currently would require periodic revisits by IAEA personnel to service or replace equipment, which may require the reactor to be shutdown, leading to lost revenue for operators. However, new technology and novel approaches to data sharing may allow safeguarding to be carried out using alternative schemes – technology developers are encouraged to explore how they can ensure safeguardability of their reactor in the long-term with support from IAEA specialists engaged through their national authorities.

Longer time intervals between refuelling also reduces the frequency of fuel movements to reactor locations. This is conventionally a period of increased vulnerability owing to the material being removed from local static control with established security measures into a 'mobile' environment.

However, the potentially significantly extended period between refuelling should drive a design intent to minimise or negate the need for episodic protection, over refuelling cycles, by designing transfer systems that have security built into 'closed' and automated processes.

4.4.4. Nuclear Waste Materials

The wide range of initial nuclear fuels will lead to an equally broad range of Used Nuclear Fuel (UNF) types. Outside of the reactor, the security of these materials will not be vastly different from LCNPP UNF security. However, there are considerations for NMAC and safeguarding. It is important for proper safeguards that the composition of UNF can be calculated accurately, such that the quantities of diversion-relevant materials can be determined. For LCNPPs, computational methods have been developed to calculate this composition based on the known power history of the reactor, the position of the fuel within it, and so on. For most novel fuels, these models may still be broadly applicable, but may require adjustments and revalidation. However, for TRISO and molten salt fuels these models will not be suitable due to the complex way the fuel moves through the core.

As such, new computational approaches and measurement tools will be needed to determine UNF composition for safeguards purposes. Technology developers will need to consider how they will develop these models and tools and validate them.

4.5. Deployment and Siting Options – Considerations

4.5.1. Reduced Site Footprint and Collocation with Non-nuclear Facilities

"Security is 'time from detection' to 'time to interdiction and defeat'. The earlier you detect, the more time you buy yourself to respond, and the less delay you have got to put in the way. If you do not have the luxury of space and you do not have the site configuration that allows for a fence, then how are you doing that detection? You are going to need some very significant delaying engineering if your first point of detection is the building perimeter". [31]

Large site footprints, with detection systems at their outer boundary, create delay, due in part to the travel time between the point of detection and the protected asset. Smaller NAR site footprints, where the point of detection is closer to the protected asset, thus lead to reduced delay. As NARs need to create greater delay than LCNPPs due to their reduced or eliminated guard forces, new approaches will be required to create this delay. One such approach is to extend detection beyond the site boundary. NAR operators could sponsor intelligence gathering activities on the potential threats to their sites, while advanced technological approaches may enable detection of threat actors at greater distance.

When looking to detect beyond the site boundary, it is critical to first consider what is 'normal' in the area. For example, close to the Pantex nuclear weapons assembly and disassembly facility in the United States, armed hunters and crop spraying aircraft are normal sights, but threat actors could use these activities to mask their approach [6]. Sites co-located with industrial facilities or in remote communities may be able to manage this using automated facial recognition cameras operating beyond their boundaries, able to alert security personnel should an individual begin to the approach the site who does not work at the industrial facility or live in the community.

If early detection alone cannot give adequate time for a response to neutralise threats, technology developers might consider introducing additional delay features in accordance with the defence in depth principle. One expert indicated that delay features have been successfully incorporated into at least one NAR concept design already: "[Babcock & Wilcox] got the security people from naval reactors to actually help them design features into [the mPower reactor] which would give them the delay they needed – the avoidance of people getting to critical areas in the plant and things like that – and the security for that reactor would have been wonderful" [6]. When it comes to designing in delay features, technology developers should think creatively, starting from first principles considerations of what the adversary will need to do to accomplish their goals, conducting adversary sequence modelling, and identifying how simple, reliable and robust delay features can be introduced at each stage.

Measures might include cutting power to areas of the plant where the adversary is operating, activating disabling agents into secure areas, removing oxygen, or raising bollards within hallways to prevent the movement of wheeled vehicles [6]. The above examples are all active delay features, requiring activation to function and rendering it difficult to operate within the plant once activated. Developers should also consider the use of passive delay features, such as walls and moats, as these can continue to fulfil their function in the absence of an activation signal.

When designing-in delay features, it is critical that these be introduced into the design early and integrated well alongside safety and operational elements to ensure the greatest benefit at least cost. It is equally important then to ensure that these delay features are preserved as the design matures and not removed or substantially compromised at a later stage.

4.5.2. Isolated and Remote Sites

Remote and isolated NAR sites will be exposed to elevated security costs compared to NARs in more accessible locations. Guard force costs will be increased by the need to provide local accommodation at remote sites and the travel costs associated with work rotation and training certification, although investment in family accommodation and local training facilities may offset the latter of these.

However, these costs will remain large. Unless sufficient security can be built-in during the design process, around-the-clock annual provision of guard forces will be necessary, and developers are thus recommended to invest in SeBD to mitigate through-life operational costs. The above said, NARs operating in isolated environments may benefit from increased energy prices due to lack of economical alternative generating options, allowing them to offset elevated operating costs [31].

The extended travel times required to respond to isolated and remote sites will require developers to maximise the amount of delay imparted by the NAR and strive for the earliest possible detection of threat actors. Responders might be specially trained personnel drawn from a central hub [31], or law enforcement or military personnel, as appropriate [6]. How this response is delivered will be largely dependent on the location of site and how responders would travel to it.

Reliance on law enforcement or military personnel as a response force, rather than dedicated personnel with nuclear-relevant knowledge, is likely to enable cost efficiencies, but non-dedicated responders will require appropriate situational awareness of the site, need to understand the importance of protecting it, and be equipped and trained to respond effectively. An alternative option that has been suggested would be to use autonomous systems to provide a degree of response capability [41]. However, robotic systems of this nature still require much research and development work before they could be effective, and there will also be a range of ethical, legal and regulatory hurdles to overcome before they could be deployed.

NAR developers and operators should also consider environmental factors. People and equipment are affected by environmental factors such as terrain, weather, temperature, and humidity, and will not perform as well for as long under challenging conditions. Equipment capital costs will likely be greater due to the need for winterisation or other special protections and may suffer from a shortened service life. Personnel numbers will also be greater, with guard forces being able to spend less time outdoors. Staff work rotations may be shorter, increasing transportation costs.

These factors will drive elevated operational security costs, further underlining the importance of following a SeBD approach.

4.5.3. Combined Security at Multi-unit Sites

As described in Section 3.5, one NAR deployment option is the replacement of LCNPPs and large fossil-fuelled power plants. Replacing an LCNPP with perhaps twelve NARs means that the nuclear material will be divided between a greater number of smaller units, reducing the potential consequences of adversary actions. To achieve similar radiological consequences to an attack on an LCNPP, multiple units would have to be breached, creating additional burden on the adversary. However, if nuclear materials are aggregated, allowing adversaries to access more material in a single act, these benefits may be negated. Some multi-unit NAR concepts place all reactors into a shared zone with security measures around it, meaning that if attackers breach the space, all NAR units will be accessible.

This is represented graphically in Figure 4-1. Security cost efficiencies and operational advantages may be available when security measures are shared between units, but technology developers must balance these against the greater potential consequences of a radiological release or theft of nuclear material.

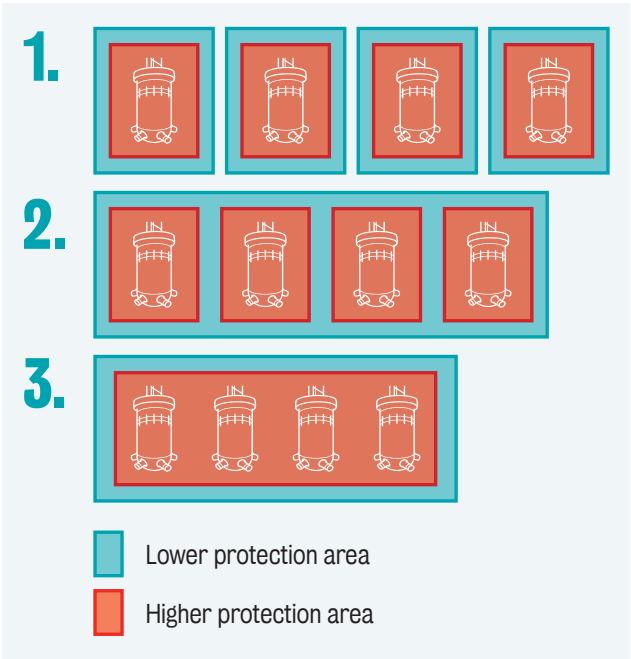

Figure 4-1: Concepts for separation between NAR units. 1) All NAR units on a site are secured as if they are single units, with no shared security features. 2) NAR units on the same site share some security features for less sensitive areas but features for more sensitive areas are independent. 3) All security features are shared between the NAR units on the site. Note: This simplified diagram shows two layers of security in all cases. However, developers should also consider whether they can use additional layers of security to achieve similar outcomes.

In Section 3.5, the benefits of having a larger number of small units were discussed; specifically, how shutting down a single unit at a time has a smaller impact on the overall power output of the site. This does, however, complicate site safeguarding. Verification of materials inventory becomes more challenging as there is no point at which a major proportion of material exists outside of operating reactor cores, meaning the verifiable proportion of material is reduced compared to LCNPP sites. New approaches to transparent nuclear materials accountancy may be required to provide full visibility to the IAEA.

4.5.4. Transportable Nuclear Power Plants

TNPPs have a range of novel security and safeguards considerations, encompassing considerations related to siting, transportation and reduced footprints whilst also being potentially open to novel attack vectors. Furthermore, debate on a range of legal, regulatory and safeguards aspects of TNPPs is ongoing in the international community [45]. This paper does not attempt to cover all potential security and safeguards considerations for TNPPs, but some of the most significant are presented below. Mobility brings both advantages and disadvantages in terms of security and safeguards.

Firstly, threat actors could attempt to hijack complete TNPPs. Considerations pertaining to theft, pirating and loss of control for mobile platform reactors clearly necessitate further development of technology solutions and legal frameworks of ownerships and liabilities. This risk might be negated by immobilising the plant once it reaches its destination, such as by removing wheels or digging vehicles into the ground. Floating NPPs might be moved into a drydock or secured firmly to the seabed. Each of these measures will introduce a degree of delay to adversaries attempting to steal the mobile NAR. However, these measures would also counteract one of the security advantages, namely that TNPPs can be quickly removed from dangerous areas when under increased threat, help reduce the risk of sabotage, theft, or diversion. Unlike fixed NARs, this ability to retreat from danger allows TNPPs to operate in more challenging circumstances, such as disaster relief or politically unstable states.

TNPPs will likely have very small site footprints, even compared to other NARs; it may be that the outer edge of the vehicle is also the first opportunity for threat detection. Whilst operators may choose to define a larger site within which the TNPP can be protected, technology developers cannot rely on operators doing so, and must build in sufficient measures to adequately secure the reactor and nuclear material. Floating NPPs in particular are open to a range of novel attack vectors to which other NPPs are largely immune, such as divers, submersible vehicles or torpedoes, such attack vectors must be considered. Should a floating NPP be sunk, this must not be permitted to compromise security – threat actors must still face sufficient delay in nuclear materials recovery to allow for a response force to arrive and protect the site until nuclear materials can be recovered.

4.5.5. Nuclear Materials Ownership Ambiguity

The novel business models and ownership structures outlined in Section 3.6 and novel deployment scenarios described in Section 4.5.1 create potential NMAC and safeguards consideration. Firstly, sealed, autonomous nuclear power units may not have an operator in the way that is commonly understood today. Without this role, it is not immediately obvious who should be responsible for the nuclear materials in the plant, carry out NMAC and hold the material as part of their safeguards liability – should it be the organisation which initially installed the plant, the provider of the fuel, or the state whose territory it operates from? Although the ultimate responsibility for safeguards compliance resides with the state, the complexity of having several small remotely deployed NARs will require development of new safeguards approaches. These issues must be clarified prior to the construction of such an NAR, especially when built in newcomer states.

As discussed in Section 3.2, some NAR designs reduce the barrier to high cost for deployment whilst presenting the opportunity for more than one state to share a fleet of reactors to meet their energy needs. These present a need for new legal instruments that clarify ownership and liabilities of all involved parties. There are a few examples of shared reactors between two states – for example, Croatia and Slovenia where the two nations share the Krško reactor which is physically located in Slovenia. Issues with fuel management have continued to challenge international laws. Similar considerations are associated with TNPPs.

As the NAR moves between a range of states with differing safeguards arrangements, there are outstanding questions regarding ownership and liability. A major question regarding TNPPs is: can they operate in a foreign state without becoming the safeguards responsibility of that state? To do so, it would be necessary for the TNPP to act as an extension of its owner's state, at least for the purposes of safeguards. For floating NPPs, this may be feasible, given that a vessel at sea acts as an extension of the territory under which it is flagged. This could allow TNPPs to operate in states without the usually required safeguards commitments, instead operating under the safeguards agreements of their home state. To do so would likely require that the TNPP be sealed by IAEA personnel prior to travelling to the foreign state and remain so until it returned to its home state. This novel concept may be attractive to states wishing to benefit from nuclear power which currently lack comprehensive safeguards agreements with the IAEA. New international safeguards instruments and the development of regional agreements are anticipated, led or facilitated by major technology developers.

4.6. Developer Business Models and Marketing Approaches – Considerations

4.6.1. Business Models and Security and Safeguards by Design

As stated in Section 4.2.2, whilst many reactor vendors are working on the economic assumption of reduced security personnel numbers, few are developing security plans to enable this. In fact, some developers do not see security design as part of their role, instead passing this responsibility to the operator after the design has been finalised and the opportunity to integrate SeBD into the NAR has been missed. This may limit the attractiveness of the design to potential buyers, as greater costs will be incurred to implement effective security [6]. Developers are likely to increase their engagement with security and safeguards as they become more invested in the success of the NAR design and the operator. Developers under the first business model presented in Section 3.6 are thus at greater risk of failing to incorporate security and safeguards considerations into their designs, as they will not have to concern themselves with the delivery of these aspects. However, developers should be cautious of such thinking, as it can lead to plant designs which are not economically operable and will not be purchased or licensed by potential operators.

The expansion in the number of start-ups developing nuclear technologies brings up the importance of information security and knowledge management. Individual technologies and patents by themselves may seem benign and to present no significant security risks. However, risks from capable technology integrator organisations should not be ignored. The insertion of vulnerabilities in the technology and its supply chain, which could be exploited for future security breaches, are also higher as many NAR designs will rely on a global, widely distributed supply chain.

4.6.2. Marketing and Reputational Risk

The new image of nuclear power projected by NAR stakeholders is fragile, and there is a risk that should a security incident occur, the resulting negative publicity will be felt by all developers as the public and media draw parallels to previous legacy issues, e.g., prior nuclear accidents, concerns about nuclear waste disposal, fear of nuclear terrorism, etc.

As such, it is vital that the NAR sector and associated stakeholders do their utmost to ensure security and safeguards standards are maintained. Even an attack which is caught in time and prevented is liable to cause reputational damage, so deterrence is highly preferable to a successfully managed incident. Reputational risk management can thus be partly addressed through security, of which deterrence is a key security function, as described in Section 4.3.4. However, whilst there may be common management approaches for both nuclear and reputational risk, developers should ensure to distinguish between these two functions. The elements of nuclear security that are effective for sabotage and theft prevention may not contribute to management of reputational risk and protection of commercial interests, and vice versa. NAR developers should consider carefully how both elements can be successfully managed, seeking efficiencies where possible but without compromising on nuclear security performance.

5. Recommendations

The past decade has been an exciting time for the nuclear sector, as it seeks to continue to provide cost effective, secure, reliable, and clean energy for the coming century. The explosion of start-ups in pursuit of NARs has invigorated the industry and infused new capital that fuels innovation and development of several exciting new technologies that are not just evolutionary but revolutionary in design, build and operation. The security and safeguards considerations presented in this paper are intended to aid the discussion and generate a dialogue among the various communities, focused not only on safety but also security and safeguards in preparation for many of these reactors coming to fruition in next 10-20 years. Several recommendations are summarised below. Whilst these are organised by stakeholder, readers are encouraged to review all recommendations as many of these are interrelated and cannot be addressed by organisations working alone. Regular communication across all stakeholders will be necessary to ensure the robust delivery of security and safeguards for NARs in a cost-effective manner.

Whilst this report argues that retrofitting of security into firm designs is more costly than implementing these features early in the process, retrofitting of new technologies can be beneficial. Organisations currently operating LCNPPs should also be paying attention to developments in NAR security and safeguards, as technologies and approaches developed for NARs may also be relevant for LCNPPs, allowing for improvements and potential cost savings.

5.1. Recommendations for Research Organisations

There are a range of outstanding questions regarding the security and safeguarding of NARs which will require resolution. Currently, many of these are addressed through the application of informed judgements, however, this cannot continue indefinitely, and there is an increasing need for detailed research and citable evidence. Research organisations should engage with industry stakeholders to address topics in the NAR security and safeguarding spaces.

Some potential topics are listed below, but these are only a sub-set of the full range of potential topics:

1. Examination of specific NAR concepts and technology groups to determine their particular security and safeguards considerations and address these.

2. Analysis of the application of graded approaches to NAR security and the economic impacts of this to determine how it can enable cost-effective security.

3. Quantification of nuclear security risk on a probabilistic basis to enable reductions in layered conservatism in regulatory approaches.

4. Development of tools and models to determine burnup and composition for novel irradiated fuels, particularly TRISO and molten salt fuels.

5.2. Recommendations for Technology Developers

Technology developers are currently at various stages of the design process, but almost all are still malleable. Developers are encouraged to bring security and safeguards into their design activities alongside safety and operational considerations as soon as possible and do so holistically to embed security and safeguards thinking into engineering design processes, following SeBD and SgBD best practices. The coordinated use of safety systems with physical protection systems, cyber security and NMAC can provide a complementary framework of defence in depth architecture for early detection, passive safety and deterrence to misuse, significantly improving cost and operational efficiencies. These considerations will also apply to facilities manufacturing NAR systems and modules. Whilst developers are often working with limited funds and there will be costs in devoting time to security and safeguards considerations, a failure to make the most of the opportunity now will only lead to greater costs in future.

Furthermore, it will likely result in an NAR which is not cost-optimised for delivery of effective security and safeguards, potentially resulting in an uneconomical design. In addition to technology development, the developers should consider early engagement with key stakeholders such as state authorities, regional safeguards organisations and the IAEA, particularly because the acceptability of many solutions may be dependent on multiple and overlapping treaties and legal frameworks. Such engagement might be done on an individual basis, or collectively through nuclear industry groups.

The detailed knowledge of material flows and inventories necessary for NMAC provides opportunities for synergies between security and safeguards. SgBD will support CoK of the isotopic concentrations, material form and its location, enhancing safety, reinforcing security, and reducing the burden of nuclear safeguards inspections. By learning from sixty years of experience in safeguarding systems and incorporating changes to the reactor core and fuel design, NAR developers can significantly reduce costs to achieve high safeguards and security performance standards.

Developers should consider not only the current threats and regulatory environment of their domestic market, but also consider how adversary capabilities will differ internationally and over time. Should the threat change to the point where security measures are no longer sufficient, this may require supplementary security measures in the form of additional personnel deployments, with deleterious results for plant economics. However, if these other threats can be mitigated at the design stage it is much more likely that the plant will be economical over its full lifecycle. Likewise, an understanding of international regulatory environments and appropriate adaptations during design will make the final plant much more exportable to international markets.

Developers should engage with other stakeholders throughout the design process. Large utilities and facility operators can provide insight into how the NAR design can be best adapted to their needs, making it more attractive for adoptions in established and newcomer countries alike.

Regulatory authorities in target markets can provide feedback into whether a design can be approved and what will be required, as well as allowing designers to feedback their own challenges with regulatory approaches. Engagement with the IAEA, through appropriate national authorities, will allow developers to determine how they can best demonstrate safeguards compliance to minimise the potential safeguards burden. Finally, engagement with other developers through nuclear industry groups will facilitate sharing of best practices and exploration of novel ways in which nuclear safety, security and safeguards can be effectively delivered by NARs. Developers and potential operators are encouraged to engage meaningfully with such groups – in working collectively, they will be able to better engage with regulators and government to request regulatory and legal reform where appropriate, creating a sufficiently permissive environment for NAR designs to be realised.

5.3. Recommendations for Operators

As argued above, NAR developers can seek to transfer liability for security and safeguards to operators, creating costs and responsibilities which the operator will very likely wish to avoid, particularly in states without existing experience of delivering nuclear security or safeguards. As has been argued above, by following SeBD and SgBD approaches, developers can instead build these into the NAR itself, and whilst this may lead to a modest increase in capital costs, these will be significantly lower than the lifetime operational costs of delivering security and safeguards using LCNPP-type approaches.

In the coming years, operators will engage with technology developers to select NAR designs for construction, based on a range of decision-making criteria, including risk-adjusted full-life operating profit-and-loss calculations. Potential NAR operators are thus already in a relatively strong position to influence NAR design processes and can use this position to encourage developers to design out unnecessary operational costs and instead follow SeBD and SgBD approaches. Operators would thus do well to engage with developers early and encourage decisions which will drive security into the fabric of the NAR design rather than accepting liability for planning and delivery of security and safeguards as the operator.

5.4. Recommendations for Regulators and SSAC Organisations

Many current regulatory frameworks are not well adapted for first-of-a-kind NAR designs and operating models, and are often a step behind accepting the solutions that technology developers are working towards [3]. NAR developers have expressed concern at the high costs and long timescales for design assessment and licencing. Regulators can support NAR developers through greater streamlining of review processes and should avoid the view that there is no fundamental difference between NAR and LCNPP. The advent of NARs presents a valuable opportunity for a comprehensive review of regulatory processes to minimise unnecessary burdens on technology developers.

To better facilitate the realisation of the benefits offered by NAR, regulators are recommended to engage with industry groups and research organisations to explore new and revised approaches in delivering their role. Many developers are also planning to use novel technological approaches in their designs, and regulators and SSAC organisations must develop the necessary capacity and culture to consider these novel approaches. These novel approaches must be considered in terms of their ability to address the threat. If NARs are forced to use overengineered and oversized security arrangements this will drive up costs, and regulators should thus consider carefully whether their existing approaches are well adapted to the threat or excessively conservative. If the latter, work will be required to examine how this conservatism can be brought under control, such that costs can be reduced without compromising on security performance.

Regulators should, however, take care not to overcorrect in attempting to reduce conservatism. Pressure from technology developers or policymakers eager to implement NARs may place regulators in a difficult position where they are overly permissive. A careful balance must be struck between being overly conservative and overly permissive, but a step in the right direction might be to use probabilistic risk assessment approaches when assessing IEMO. Regulators must ensure to be flexible and open to new concepts, whilst demanding the same high standards of license applicants.

This could be achieved by permitting the use of suitably qualified off-the-shelf components in nuclear applications and using goals-based regulatory approaches in states where these are not already used. The US NRC has already taken steps in this direction, as its directed approach was adequate for large LWRs, but acted as a hindrance to NAR development and licencing [15].

5.5. Recommendations for National Policymakers

"That regulation needs to change is only one side of the argument. I have no doubt that the whole environment, law and regulation, will change".[3]

Regulation is not the only governance structure on nuclear energy – national legal frameworks and international policy guidance from the IAEA also have major enabling or constraining effects on NAR development and deployment. National governments seeking to achieve benefits in their country from NARs can take several actions. Firstly, they should seek to create a supportive legal and regulatory environment for these novel energy systems, both to facilitate development of NAR technologies within their territory and to welcome the introduction of technologies from abroad. Changes are already being implemented in many countries to encourage regulators to change their approach to be more permissive to NARs [6]. One approach to this will be to facilitate communications between developers and the IAEA, allowing for discussions on safeguards implementation during design, which has the potential to reduce NMAC and safeguards burdens on all stakeholders for the completed NAR. For nuclear newcomer countries, the IAEA also offers support in creating the necessary structures and organisations to accept and manage nuclear power through its Milestones Approach [46]. Additional support may be available from other national governments with more established programmes.

Given the widespread intention of NAR developers to export their designs globally, governments of states hosting NAR developers may wish to engage with these developers proactively regarding export controls, sanctions, and related considerations.

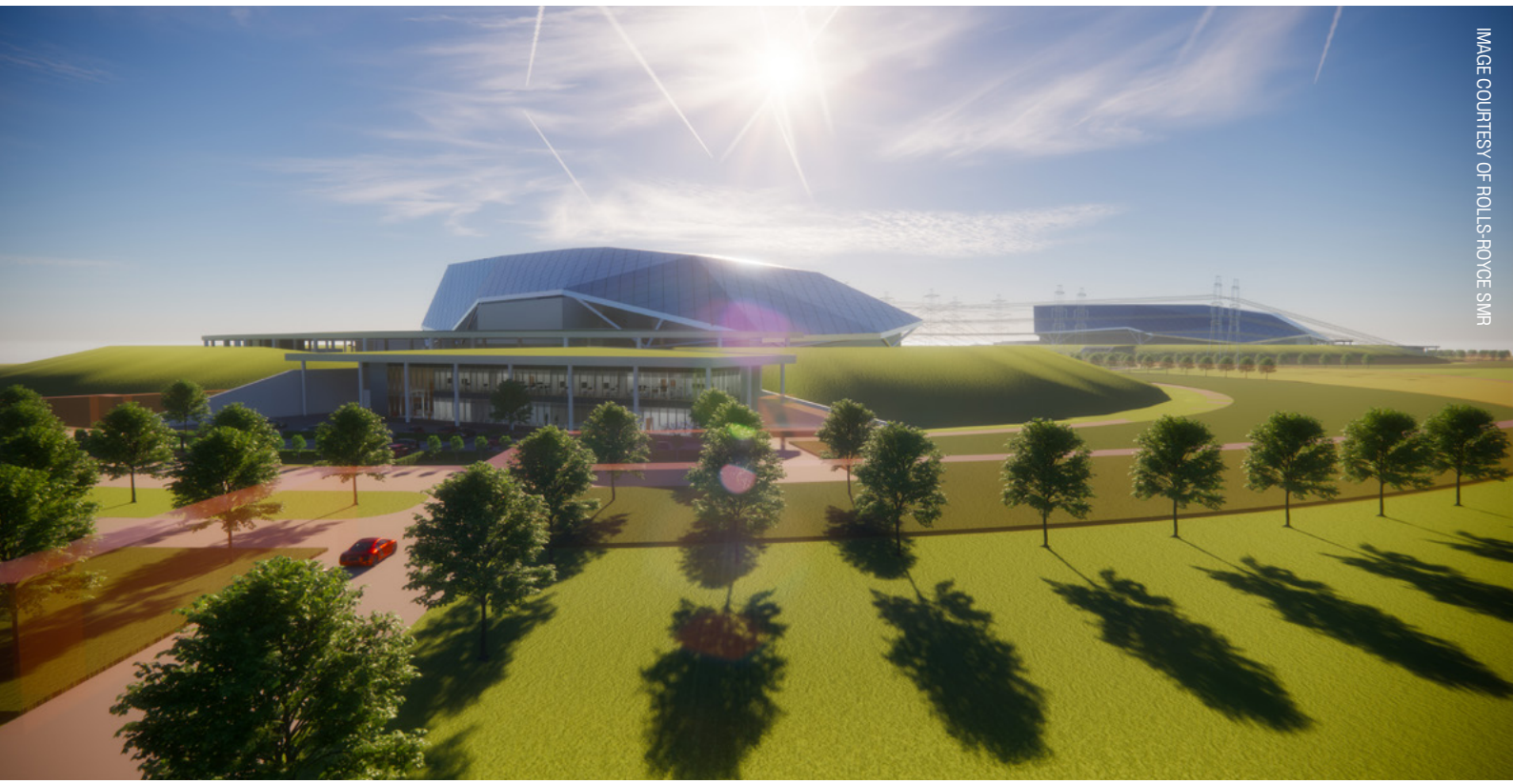

IMAGE COURTESY OF ROLLS-ROYCE SMR

NARs are advanced technologies which can be misused by proliferators and will also transfer knowledge of dual-use technology which may be adapted for malign ends. Early consultation with developers on these issues can steer them away from potential problems later.

5.6. Recommendations for the International Atomic Energy Agency

As there will potentially be a much greater number and geographical distribution of NARs compared to LCNPPs, it is unlikely that current IAEA nuclear safeguards approaches will be adequate to meet the increased demand without significant increases in safeguards budgets, especially for the development of new safeguards concepts. Innovative approaches will be required to ensure CoK over nuclear materials and verify that nuclear materials and facilities are being used solely for peaceful purposes. A particular question to address is the delivery of safeguarding on fully autonomous or remote sites – unannounced safeguards inspections at such facilities may require additional consideration.

The IAEA is already hosting a range of fora and events for NAR stakeholders, and these should continue and be further developed. One area of activity would be an NAR safeguards forum, where developers can exchange ideas and engage with IAEA personnel as they develop their design. The influx of a younger workforce in the design and development of NARs is not yet reflected within the nuclear safeguards community. The benefit of fresh prospective and innovation is evident in many of the design concepts including the business models, financing instruments and advanced manufacturing. The convening power of the Agency to bring together experts will allow for production of advice and technical guidance which will be of great use to developers, operators, and regulators. The IAEA should explore means of engaging a younger workforce by promoting career opportunities and highlighting the broader impact that international safeguards play in continued expansion of peaceful use of nuclear energy among its Member States. This said, such guidance should take care to avoid becoming overly prescriptive in terms of security and safeguards approaches. The developer community is currently in a position to explore innovative safeguards solutions, and the safeguards community should refrain from overly prescriptive guidance and requirements based heavily on past experiences as this could stifle innovation.

6. Conclusions

This report has explored how the differences between LCNPPs and NARs create novel considerations, as well as some re-interpretation of existing considerations, in nuclear security and safeguarding, and presented recommendations on how these might be addressed. The term "novel advanced reactor" covers a huge range of reactor technologies, fuels, deployment options and operating strategies. As such, this report does not claim to have addressed all such considerations – instead, NAR stakeholders can use it to inform their thinking as they address security and safeguards for their specific NAR(s).

Overall, the smaller size of NARs means that whilst they are more flexible in deployment than LCNPPs, they will need to find ways to reduce their operating budgets, including security budgets. Many developers are working on an assumption of requiring few or no on-site security personnel, but detailed plans for how this can be achieved are often lacking. To achieve this, developers need to consider how they can integrate technological and other solutions into their NAR design to deter threat actors, detect attempted sabotage, theft or diversion at the earliest possible opportunity, and delay adversaries for long enough to allow for a response provided by off-site security forces, be they either dedicated nuclear response forces or drawn from law enforcement or the military at need. The full range of threats must be considered, including physical, cyber and insiders.

Nuclear safeguards also present specific considerations for NARs. The number and distribution of NARs globally could stretch IAEA safeguarding resources beyond their breaking point, and new approaches will be required to deliver safeguards without huge increases in cost. Furthermore, many NARs will have significantly longer fuel cycles than LCNPP, meaning that the IAEA and NAR developers must consider how safeguards can be implemented to guarantee continuity of knowledge at such facilities.

Security by design and safeguards by design (SeBD and SgBD) should be implemented or encouraged by five major stakeholder groups – NAR developers, NAR operators, regulatory bodies, national governments, and the IAEA. Engagement between these groups at the national and international levels will be crucial to ensure that opportunities are not missed to integrate nuclear security and safeguards considerations holistically into NARs at the earliest possible stage alongside other design considerations such as nuclear safety and operations. This will drive reductions in nuclear power plant operating costs and whilst simultaneously supporting improvements in nuclear security, safeguards, and safety.

References

1. International Atomic Energy Agency, *Technology Roadmap for Small Modular Reactor Development*, in *IAEA Nuclear Energy Series*. 2021, International Atomic Energy Agency: Vienna.

2. International Atomic Energy Agency. *Advanced Reactors Information System (ARIS)*. [cited 06 March 2022]; Available from: https://aris.iaea.org/sites/SMR.html

3. Expert 1, *Nuclear Security Considerations of SMR and AMR Interview*, by R. Peel and G. Foster. 2022.

4. International Atomic Energy Agency. *Security aspects of nuclear facilities*. [cited 23 January 2022]; Available from: https://www.iaea.org/topics/security-aspects

5. International Atomic Energy Agency. *IAEA Safeguards - Delivering Effective Nuclear Verification for World Peace*. 2016 [cited 5 February 2022]; Available from: https://www.iaea.org/sites/default/files/16/08/iaea_safeguards_introductory_leaflet.pdf

6. Expert 2, *Nuclear Security Considerations of SMR and AMR Interview*, by R. Peel and G. Foster. 2022.

7. World Institute for Nuclear Security, *4.1 Implementing Security by Design at Nuclear Facilities*. 2019, World Institute for Nuclear Security.

8. International Atomic Energy Agency, *International Safeguards in Nuclear Facility Design and Construction*. Nuclear Energy Series. 2013, Vienna: International Atomic Energy Agency.

9. Kovacic, D., et al. in *Webinar on Safety, Security and Safeguards Interfaces and Challenges for Novel Advanced Reactors*. 3 February 2022. Vienna: International Atomic Energy Agency.

10. Watson, N. and L. Peguero. *IAEA Presents New Platform on Small Modular Reactors and Their Applications*. [cited 5 February 2022]; Available from: https://www.iaea.org/newscenter/news/iaea-presents-new-platform-on-small-modular-reactors-and-their-applications

11. SMR Regulators' Forum, *Phase 2 Summary Report: Covering Activities from November 2017 to December 2020*. 2021.

12. Lyman, E., *Small Isn't Always Beautiful - Safety, Security, and Cost Concerns about Small Modular Reactors*. 2013, Union of Concerned Scientists: Cambridge, MA.

13. Lyman, E., *"Advanced" Isn't Always Better - Assessing the Safety, Security, and Environmental Impacts of Non-Light-Water Nuclear Reactors*. 2021, Union of Concerned Scientists.

14. Global Nexus Initiative, *Advancing Nuclear Innovation - Responding to Climate Change and Strengthening Global Security*. 2019, Global Nexus Initiative.

15. World Institute for Nuclear Security, *Security of Advanced Reactors*. 2020. [cited 6 March 2022]; Available from: https://www.wins.org/document/security-of-advanced-reactors/

16. The Proliferation Resistance and Physical Protection Evaluation Methodology Working Group and System Steering Committeesof the Generation IV International Forum, *Proliferation Resistance and Physical Protection of the Six Generation IV Nuclear Energy Systems*. 2011, Generation IV International Forum.

17. *Advanced Reactor Safeguards program area*. 2022 [cited 25 February 2022]; Available from: https://gain.inl.gov/SitePages/ARS.aspx

18. International Atomic Energy Agency, *Objective and Essential Elements of a State's Nuclear Security Regime*. Nuclear Security Series. 2013, Vienna: International Atomic Energy Agency.

19. World Nuclear Association. *Safeguards to Prevent Nuclear Proliferation*. 2021 April [cited 3 March 2022]; Available from: https://world-nuclear.org/information-library/safety-and-security/non-proliferation/safeguards-to-prevent-nuclear-proliferation.aspx

20. *Risk Informed Approach for Nuclear Security Measures for Nuclear and Other Radioactive Material out of Regulatory Control*. Nuclear Security Series. Vol. 24-G. 2015, Vienna: International Atomic Energy Agency.

21. International Atomic Energy Agency, *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities*. Nuclear Security Series. 2011, Vienna: International Atomic Energy Agency.

22. International Atomic Energy Agency, *Nuclear security recommendations on radioactive material and associated facilities*. IAEA Nuclear Security Series. 2011, Vienna: International Atomic Energy Agency.

23. Centre for the Protection of National Infrastructure. *Asset*. 18 March 2021 [cited 20 February 2022]; Available from: https://www.cpni.gov.uk/asset-0

24. International Atomic Energy Agency, *IAEA Safeguards Glossary*. International Nuclear Verification Series. 2003.

25. United Nations Office for Disarmament Affairs. *Treaty on the Non-Proliferation of Nuclear Weapons*. [cited 6 March 2022]; Status of the Treaty. Available from: http://disarmament.un.org/treaties/t/npt

26. International Atomic Energy Agency. *Status List - Conclusion of Safeguards Agreements, Additional Protocols and Small Quantities Protocols*. 31 December 2021 [cited 06 March 2022]; Available from: https://www.iaea.org/sites/default/files/20/01/sg-agreements-comprehensive-status.pdf

27. International Atomic Energy Agency, *Safeguards Implementation Practices Guide On Establishing And Maintaining State Safeguards Infrastructure*. IAEA Services Series. 2018, Vienna: International Atomic Energy Agency.

28. International Atomic Energy Agency, *Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities*. IAEA Nuclear Security Series. 2015, Vienna: International Atomic Energy Agency.

29. Mignacca, B. and G. Locatelli, *Economics and finance of Small Modular Reactors: A systematic review and research agenda.* Renewable and Sustainable Energy Reviews, 2020. **118**: p. 109519.

30. Mignacca, B., G. Locatelli, and T. Sainati, *Deeds not words: Barriers and remedies for Small Modular nuclear Reactors.* Energy, 2020. **206**: p. 118137.

31. Expert 3, *Nuclear Security Considerations of SMR and AMR Interview*, by R. Peel and G. Foster. 2022.

32. International Atomic Energy Agency. *Glossary of Terms in PRIS Reports*. 2022 [cited 20 February 2022]; Available from: https://pris.iaea.org/PRIS/Glossary.aspx

33. Olatubosun, S.A. and C. Smidts, *Reliability analysis of passive systems: An overview, status and research expectations.* Progress in Nuclear Energy, 2022. **143**: p. 104057.

34. *Cross-section of a fuel pellet containing TRISO particles at 10mm scale*, Cross-section_of_TRISO_fuel_pellet.jpg, Editor. 2014, US Department of Energy.

35. *Picture of molten FLiBe salt*, FLiBe.png, Editor. 2011, Oak Ridge National Laboratory.

36. International Atomic Energy Agency. *AKADEMIK LOMONOSOV-1*. Power Reactor Information System 2022 [cited 17 February 2022]; Available from: https://pris.iaea.org/PRIS/CountryStatistics/ReactorDetails.aspx?current=895

37. US Department of Defense. *Prototype Mobile Microreactor Environmental Impact Statement consultation website*. [cited 17 February 2022]; Available from: https://www.mobilemicroreactoreis.com/index.aspx

38. Dider, E., *The first Russian floating nuclear power station being transported from Murmansk*, Спуск_ПАТЭС_на_воду_20190823.jpg. 2019, This file is licensed under the Creative Commons Attribution-Share Alike 4.0 International license.

39. Expert 4, *Nuclear Security Considerations of SMR and AMR Interview*, by R. Peel and S. Aghara. 2022.

40. Expert 5, *Nuclear Security Considerations of SMR and AMR Interview*, by R. Peel and G. Foster. 2022.

41. Expert 6, *Nuclear Security Considerations of SMR and AMR Interview*, by R. Peel. 2022.

42. International Atomic Energy Agency, *Computer Security Techniques for Nuclear Facilities*. IAEA Nuclear Security Series. Vol. 17-T (rev 1). 2021, Vienna: International Atomic Energy Agency.

43. Cárdenas, A.A. and R. Safavi-Naini, *Chapter 25 - Security and Privacy in the Smart Grid*, in *Handbook on Securing Cyber-Physical Critical Infrastructure*, S.K. Das, K. Kant, and N. Zhang, Editors. 2012, Morgan Kaufmann: Boston. p. 637-654.

44. World Nuclear Association. *Advanced Nuclear Power Reactors*. Information Library 2021 [cited 23 January 2022]; Available from: http://www.world-nuclear.org/information-library/nuclear-fuel-cycle/nuclear-power-reactors/advanced-nuclear-power-reactors.aspx

45. International Atomic Energy Agency, *Legal and Institutional Issues of Transportable Nuclear Power Plants: A Preliminary Study*. IAEA Nuclear Energy Series. 2013, Vienna: International Atomic Energy Agency.

46. International Atomic Energy Agency, *Milestones in the Development of a National Infrastructure for Nuclear Power*. Nuclear Energy Series. 2015, Vienna: International Atomic Energy Agency.

Annex: Differences between LCNPP and NAR and resultant security and safeguards considerations

Characteristic	Large conventional nuclear power plants	Novel advanced reactors (SMR and AMR)	Impact of difference	Security/safeguards considerations	Recommendations
Power capacity and construction approach	Large reactor must be constructed as megaproject with significant on-site fabrication.	Smaller reactor allowing for off-site factory fabrication, with modules transported to site.	Complete nuclear reactors being constructed off-site in specialised facilities, potentially being fuelled at same location.	Manufacturing facilities are additional points of vulnerability which must be protected. Nuclear safeguards must be applied at facilities.	Developers and regulators must apply appropriate security solutions and make provision for safeguarding of manufacturing facilities.
			Equipment and materials transported in a much more complete state, making them more attractive to adversaries.	Equipment must be more effectively protected during transport. Usual safeguarding requirements apply.	Developers must consider how to apply security in transport through detection and delay features, and remote monitoring.
Amount of energy produced	Large revenue due to large power production, thus able to support larger operating budget	Smaller revenues due to reduced power production, creating a need for efficiencies in operational expenditure	Security is a major expenditure for LCNPPs. NARs will need to deliver at least the same security and safeguards performance on a lower budget.	Security and safeguards risk management standards must be upheld. NAR developers will need to use cost-effective security- and safeguards-by-design approaches to meet this imperative.	Developers should design to build early detection and maximum delay into their NAR, reducing/eliminating the need for dedicated, on-site security staff.
Timescale to return on investment	Very high upfront capital expenditure (CapEx) before first power produced, leading to front-loaded risk.	Lower CapEx, spread over more, smaller units. This allows for power generation to start earlier, prior to installation of subsequent units. Revenues are generated sooner, lowering risk.	Much wider range of potential states able to accept foreign nuclear technology. Some customer states may lack sufficient expertise, legal statute, organisational maturity, etc. to regulate plants	Developers will need to adapt to a range of customer requirements. Independent, credible and honest regulatory bodies and relevant national legal frameworks must be developed prior to NAR deployment.	Developers should engage with customer states early to build these considerations into their design. Governments should engage with IAEA for support.
Human role in plant operations	Direct human control and management of all functions with computer assistance in information provision.	Greater degree of automation in plant functions – human role reduced to oversight and response in case of issues.	NAR operations will be managed by computers to a larger degree. Some plants may be completely autonomous. Automation will also include security and safeguards functions.	Potential for greater impact of successful cyber-attacks and need for appropriate, proven and trustworthy cyber security measures in response.	Develop integrated security approaches which maximise the benefit of both human and technological elements.
Staff location	All operations-relevant staff work from plant site.	A proportion of staff may operate from off-site, delivering their role remotely.	Critical data will flow across the plant boundary though communications networks - information leaving the site and instructions returning.	Data must be secured against interference. Need for multiple, secure and reliable communication networks for remote staff. Appropriate cyber and physical security provisions required for each method.	Developers and operators must ensure the availability of several communication channels, with automated self-diagnosis and verification.
Staff numbers	Many hundreds of personnel working at the site.	Few staff required – a few tens or less, working on-site, off-site, or a combination of the two.	Fewer total staff at NARs, delivering critical roles which cannot be automated. Reduced plant knowledge amongst operations personnel.	Reduced number of potential insider threat actors, allowing more focussed and cost-effective human reliability programmes. Remote staff actions will be readily logged by digital control systems.	Developers should aim to reduce staff numbers as much as possible and consider transferring staff off-site. Implement human reliability activities.
Security personnel role	Strong presence of security personnel guarding entrances, patrolling site and so on.	Few security personnel, likely in monitoring roles and not visible from off-site.	Security presence is less visible.	Reduced deterrence due to less visible security.	Developers should seek alternative approaches to achieve deterrence, such as public outreach activities.
Safety systems approach	Primarily active measures, requiring access to off-site resources (water and power) to maintain safety.	Passive safety-by-design approaches	Passive safety systems make plants more able to cope in case of damage to systems or danger to personnel.	Plants are less vulnerable to both safety and security incidents, and are thus less vulnerable to attempted sabotage, giving security benefits through safety design.	Developers should integrate security and safety planning functions, considering these two factors holistically.

Characteristic	Large conventional nuclear power plants	Novel advanced reactors (SMR and AMR)	Impact of difference	Security/safeguards considerations	Recommendations
Fuel composition	Narrow field, primarily uranium of less than 5% enrichment. Solid uranium oxide pellets in large fuel bundles or assemblies.	Wide field of possibilities under consideration, including higher category materials, bulk solids, and liquid fuels.	Fuel materials may be more attractive to threat actors (higher categorisation under INFCIRC/225). Some fuels are not fixed and move within the reactor. Bulk fuels present NMAC challenges and may be more easily stolen.	Security measures must be appropriate to fuel risks. New approaches will be required to perform NMAC and safeguards verification on TRISO and molten salt fuels and ensure that these fuels are not stolen over time.	Research should be conducted into new safeguards approaches where required. Developers should build in measures against protracted theft.
Fuel cycle length	Commonly 12-18 months, though may be shorter.	Variable, but potentially multiple years or decades	Greater refuelling interval. Fuel composition may be outside of previous experience and models.	Challenging to maintain CoK. Accurate determination of irradiated fuel composition may require new methods.	Researchers, developers and the IAEA should work together to reduce safeguards burdens at long fuel cycle NARs.
Waste types	Well understood used nuclear fuel. Some countries also hold separated materials from reprocessing.	Wider range of used nuclear fuel materials envisaged, very likely with lower quantities per NAR unit.	Nuclear waste materials may be more attractive to threat actors, especially if separated on site, e.g., from an MSR. Composition of waste may not be readily determinable using current methods.	Security measures must be well adapted to the risks of the specific waste materials on site. New methods and models may be required to determine composition of used fuel.	Research organisations and developers should work together to develop new models for used fuel composition.
Site footprint	Large land area around protected asset due to large site footprint.	Small footprint, with outermost borders of the site much closer to the protected asset.	Distances from point of first detection to point where adversaries can commit sabotage/theft are much smaller.	Threat actors may be able to approach sensitive areas more readily and rapidly before being detected, giving them a greater chance of success.	Developers must design in approaches for early detection of threat actors, including beyond site boundaries. Protected areas must deliver sufficient delay to allow for response.
Plant application and site location	Large-scale electricity generation to a major grid. Site located away from population centres, usually with access to large supplies of cooling water (river, sea, etc).	Wider applications, including electricity generation for large and small grids, and combined heat and power. Flexible siting without the need for external cooling. Allows for collocation with non-nuclear facilities, or siting in remote areas.	NARs could be located adjacent to non-nuclear facilities in urban areas, or in very isolated locations disconnected from major grids, transport links, communication lines, and so on. Plants may be providing heat directly to nearby users. Potential sites include extreme environments, such as Arctic conditions.	Surrounding buildings may provide cover for approaching adversaries, reducing ability to detect them. Isolated sites may be unable to bring in follow-on responders in a timely manner. Sabotage to process heat users may have knock-on impacts on NAR operations. Sites may suffer extreme temperatures, degrading equipment performance. Elevated staffing costs for isolated sites.	As above. Additionally, developers and operators need to work together to ensure NAR is appropriate to a given application and location and make provision for potential threats in local environment.
IAEA safeguards burden	Relatively few, large sites. Isolated but easily reached.	Relatively many sites, of varying size and accessibility.	IAEA safeguards teams may find their resources stretched even further in trying to apply safeguards to all facilities.	Without budgetary increases, innovative verification measures will be needed to allow for safeguards with fewer on-site inspection days.	Developers and operators must work with the IAEA to develop innovative remote and automated safeguards tools, especially for facilities without on-site staffing during normal operations.
Scalability	Limited range of options for total installed capacity at a site due to large per unit power	Smaller individual reactors allowing for wider range of installed capacity per site.	Installed capacity at a site could range from less than 10 MWe to several gigawatts.	A graded approach to security will be required based on risk. Units may be secured separately or as a collective.	Research required into graded approaches for NARs. Developers should consider how to balance security and operational benefits of graded security approaches at multi-unit sites.

Characteristic	Large conventional nuclear power plants	Novel advanced reactors (SMR and AMR)	Impact of difference	Security/safeguards considerations	Recommendations
Materials storage	On-site storage of large quantities of fresh and used fuel outside for few reactors.	Lower on-site quantities of stored fuel. Materials stored serve a potentially large number of units.	Reducing quantities of nuclear material on site reduces the attractiveness to threat actors and potential consequences of radiological release.	Security requirements for fresh fuel storage may be lower, assuming that the fuel material itself does not increase the risk. However, if nuclear materials from several reactors are aggregated into a smaller number of storage facilities, threat actors will be able to sabotage or steal more material in a single act.	Developers and operators should avoid aggregating large quantities of nuclear material, but will need to balance this against operational considerations. Total nuclear materials inventory on sites should be kept to a minimum at all times.
Mobility	No mobility – plant location is fixed	Smallest plants can be mobile on land or water	Plant is mobile and likely to be designed for rapid delivery and set up. May be travelling within and between territories with their own legal and regulatory frameworks.	A range of both opportunities and challenges. Unique attack vectors become feasible and must be considered. NAR may be removeable in case of evolving threat.	The IAEA, national governments and regulators should continue developing ongoing dialogue on mobile NAR issues, of which there are many. States should avoid mobile NARs until these are resolved.
Materials ownership	Nuclear materials are responsibility of their owner, usually the operator.	Some sealed, autonomous units do not have an operator, leaving materials without an obvious owner.	Potential for nuclear material to be outside the full and proper control of a responsible owner.	Nuclear materials must always be adequately secured and safeguarded. Ownership and responsibility should be clear and unambiguous at all times.	Customers interested in autonomous sealed NARs should ensure that nuclear materials ownership and responsibility are clearly delineated in all agreements.
Developer business model	Developers sell design to an operator/ constructor, or form a consortium.	Wider array of business models, also including developing and selling incomplete designs, or acting as both developer and operator.	Many concepts and ideas developing rapidly in a number of organisations, of which a significant proportion are inexperienced and/ or funded by very limited investment.	Immature developer organisations may inadvertently share their technologies with proliferators, which might integrate these technologies to produce weapons of mass destruction. Small/ lean developers without appropriate staff may fail to integrate security and safeguards into designs.	Developers should engage with national governments prior to sharing technologies to avoid breach of export control regulations and/ or international sanctions. Developers should strongly consider bringing security and safeguards thinking into design activities as early as possible.
Marketing and Reputational risk	Promotion of high standards of safety to eliminate risk of previous accidents recurring. Burdened with poor reputation.	Developers seeking to promote NARs as completely different to LCNPP, and separate them from these legacy issues.	NAR developers rely on separation from LCNPPs to maintain positive public perception and business prospects.	A single security or safeguards incident has the potential to damage this fragile marketing strategy. Security must not just protect the asset and nuclear materials, but also be shown to be effective.	Developers must consider how security can also be deployed against reputational risk. Reputational risk to one NAR site or design will likely impact all NARs globally.

Centre for Science & Security Studies
Department of War Studies
King's College London
Strand
London WC2R 2LS
United Kingdom

kcl.ac.uk/csss
@KCL_CSSS