NUCLEAR INDUSTRY VIEWS ON THE SECURITY OF SMALL MODULAR REACTORS
Results of a pilot survey

R. CAVELLEC
World Nuclear Association
London, United Kingdom of Great Britain and Northern Ireland

N. PATERSON
World Nuclear Association
London, United Kingdom of Great Britain and Northern Ireland

R. PEEL
King's College London
London, United Kingdom of Great Britain and Northern Ireland
Email: ross.peel@kcl.ac.uk

Abstract

Modular Reactors (MR) present a range of novel characteristics which have the potential to create security considerations. These characteristics can be categorized according to five areas: (1) Power Capacity and Modular Manufacture and Construction, (2) Reduced Capital and Operating Costs, (3) Increasing Automation and Remote Operations, (4) Advanced Reactors and Fuels, and (5) Deployment and Siting Options. Prior work in this field has identified a range of security considerations unique to novel advanced reactors and MRs. In order to build upon this, during March and April 2024, the World Nuclear Association's 65-member Nuclear Security Working Group was surveyed to collect views on nuclear security considerations for SMR and other advanced nuclear power plant designs. The Working Group's members are distributed globally, with a wide range of experiences and expertise in nuclear security. The paper will present and discuss the results of this survey. Several novel security considerations were identified by the Working Group members, and these are explored, with potential mitigation approaches presented.

1. INTRODUCTION

Modular reactors (MR) present a wide range of features that make them different from the large conventional nuclear power plants (LCNPP) operating worldwide today [1]. Many of these features are expected to create novel considerations in nuclear security, both positive and negative, which will need to be addressed by designers, builders and operators of MRs. These were explored by one of the authors previously [2], and have also been explored by others [3-7]. These prior works have largely been prepared by nuclear energy and/or security experts within think tanks and educational institutions and have not taken into account the views and expertise of practitioners within the nuclear industry, despite it being incumbent upon industry to design and deliver MRs. Thus, to better understand the security considerations for MR, a project has been initiated to collect views from nuclear security and MR experts on the security considerations unique to MRs and how these might be mitigated. These views are being collected through a combination of surveys and interviews with experts within the World Nuclear Association's Security Working Group. In the first phase of this project, a pilot survey was created and distributed to industry experts within and connected to members of the working group, to request their views on how a range of novel MR features might impact on nuclear security for these plants. This paper reports the results of this pilot survey and discusses the findings. These will be used beyond the paper to improve the survey itself before it is then disseminated to a wider group of experts in order to solicit a more extensive set of responses.

This paper adopts a broad definition for the term modular reactors (MR), incorporating both miniaturized versions of today's operating nuclear power plants (often called small modular reactors (SMR)) and advanced NPP technology types including so-called Generation IV reactors. It is also applicable to emerging NPP designs with power ratings in excess of the 300 MWe proposed by the International Atomic Energy Agency (IAEA) [8].

The remainder of the paper proceeds as follows. First, this introduction explains in broad terms the novel features and characteristics of MRs that may create nuclear security considerations. In the second section, the paper will detail the methods used, explaining the survey, how it was distributed, and the responses collected. The

third section explores and discusses the results of the survey. The fourth section concludes the paper and defines the next steps to take in expanding the survey and supplementing it with data collected through interviews.

1.1. Novel Features of Small Modular Reactors with the Potential to Create Security Considerations

There are currently almost 80 MR designs described within the IAEA's Advanced Reactor Information Service (ARIS) database [1]. Furthermore, the authors are aware of a number of other conceptual designs which are not listed within ARIS. Each design has its own peculiarities, which will multiply when considering the deployment of an MR to a real site, meaning that the security considerations for each deployed plant will be unique and must be assessed on a case-by-case basis. However, many of the considerations will be common across numerous MRs, and it is these that are addressed here. The common features of MR that have the potential to create or enhance security considerations have previously been categorized in six groups, although these are not fully independent and features may be relevant to more than one group [2].

Firstly, MRs are expected to be smaller than LCNPP, generally with a capacity of up to 300 MWe, whereas most LCNPPs have capacities in excess of 1000 MWe. This enables MRs to be largely manufactured in a factory and then transported to a site for installation, reducing at-site construction works whilst leading to greater uniformity across all units of a given type. This will enhance the need for security in the supply chain whilst creating new considerations for transport security.

Secondly, MR designers are highly conscious of capital and operating costs due to the current pressures on nuclear energy, as well as competition in the market, and are seeking to minimise these, often through reduced staff numbers. This may create pressures to reduce security staff numbers and/or share security resources between multiple units, meaning that security requirements will need to be reduced through design and/or met through other means. Recent analyses have shown MRs to be underperforming economically compared to initial suggestions, and whilst costs are predicted to drop as the first of a kind of each MR design, these promises are yet to be proven [9].

Thirdly, MR designers are making greater use of digital instrumentation and control than today's LCNPPs and are often seeking to stretch this further to allow for the use of automation in plant systems and/or the operation of plants under the control of a relatively small number of off-site operators and other personnel. The use of more digital systems has the potential to increase the risk from cyber-attacks, whilst changing the way nuclear facilities are staffed will create considerations with regards to insider threat mitigation.[1]

Fourthly, many MR designers are seeking to broaden the range of reactor and fuel types beyond what is seen today in LCNPPs, to include higher enrichments of uranium or the use of non-uranium fuel materials, molten salt or graphite coated (TRISO) fuel forms, high-temperature, or fast reactors, and many more Generation IV-type technologies. These design choices affect the potential consequences of nuclear security incidents and may create novel vulnerabilities.

Fifthly, designers are preparing MRs for a wider range of deployment scenarios, in part enabled by the use of novel technologies, including siting in populated areas such as cities and industrial parks, transportable NPPs, deployment of self-managing "nuclear batteries" to isolated areas and more. Each of these novel deployment types changes the context in which nuclear security must be applied, potentially creating new vulnerabilities for threat actors to exploit whilst modifying the potential consequences of a nuclear accident.

Finally, many MR stakeholders are considering novel business models that have only rarely, if ever, been applied to NPPs. These stakeholders include a number of newly created nuclear technology developer organisations, without established organisational cultures and possibly a lack of experience in nuclear security. These challenges were addressed in previous work but were not included in the survey as the respondents were expected to include MR stakeholder organisations, who may intentionally or unintentionally give biased responses to questions about the security considerations created under this group.

These groups should not be viewed as the only potential creators of novel security considerations. Whilst the groups above have sought to be exhaustive in their coverage, specific MRs and/or deployments may present additional considerations which are not captured here. MR stakeholders are encouraged to use the information in

---

[1] In nuclear security, an 'insider' is defined as "One or more individuals with authorized access to nuclear facilities or nuclear material in transport who could attempt unauthorized removal or sabotage, or who could aid an external adversary to do so." [10] INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5), IAEA, Vienna, (2018).

this paper as part of their MR security activities, but the list of challenges should only be treated as partial, and not complete.

2. METHODS

The results presented in this paper were collected through a survey distributed online by the World Nuclear Association (WNA). The WNA is an international organisation that supports its member organisations by promoting their collective interests and providing them with a range of support functions. It seeks to connects nuclear stakeholders, represent industry interests, inform audiences on nuclear energy issues, and influence decisionmakers, organisations and the media to promote nuclear energy [11]. One activity of the WNA is to convene 12 working groups and six advisory groups on a range of topics in nuclear energy, including nuclear security.

The pilot survey was created and distributed online using the Qualtrics platform and consisted of seven sections. The first section asked a series of questions to determine the background of the respondent, asking their nuclear sector stakeholder type (e.g., government, regulator, operator, designer), the number of staff within their organisation, and their country or continent. This was in order to allow disaggregation of results along these dimensions. The survey was anonymous, and no information was collected that would allow the identification of participants by default, although participants could choose optionally to leave their name and email address in order to indicate consent to participate in a follow-up interview. Participants were also asked to self-rate their expertise in nuclear security and in small modular reactors. In the second section, they were asked several general questions about MR security, regarding whether current approaches in and international guidance for nuclear security will be adequate for MRs, and whether MR developers are giving enough attention to safety, non-proliferation and security (with security broken down into physical protection, computer security and insider threat mitigation). The five remaining sections each related to one of the five groups of novel MR features outlined above, and were delivered in a random order, such that if participants were to exit the survey before completing it, there would be an even distribution of answers across the five groups. Almost all survey items were multiple choice questions asking participants to rate their agreement with a statement or views on a scenario along a Likert scale, followed by a free text box where participants could optionally provide further information to explain their choice, react to the premise of the question, or provide further thoughts. Beyond the initial requirement to confirm that participants had read the information about the survey and provided their consent to the necessary data processing, no question was mandatory, meaning that participants could answer as many or few questions as they wished.

The pilot survey was distributed by WNA staff by direct email to selected experts within the WNA Security working group, with the request that they both complete the survey and provide feedback on the survey itself. Potential participants were provided with a hyperlink to the survey, to be completed through the Qualtrics platform. No reward or compensation was offered to participants. Participants were invited to share the survey hyperlink with their colleagues, should they be willing to do so, in order to broaden the range of responses beyond the immediate working group membership.

Sixteen responses were received to the survey, of which five were purely feedback on the survey itself. The remaining eleven responses did answer at least some of the survey questions, and it is their responses that will be discussed in the results section below. The respondents were from a range of sectors and based primarily in Europe or North America, although a small proportion of respondents were also based in Africa and East Asia.

3. RESULTS

The results of the survey are discussed below, broken down by the sections of the survey as defined above. Given the relatively low number of responses to the survey these results should not be inferred to be representative of the views of the nuclear security or MR expert communities, nor the WNA or its Security Working Group. No statistical analysis has been performed on the results for this pilot phase of the study. As such, these results should be analysed simply as a set of views from a group of partially self-identified experts in nuclear security and MRs on the topic.

3.1. General views on MR security

Participants were generally undecided on the question of whether current approaches in nuclear security will be adequate for MRs. Several participants noted concerns in relation to novel or disruptive technologies, such as remote or autonomous operation, which have the potential to create poorly understood risks. One participant suggested that current security approaches focussed on physical protection will need to broaden to better manage cyber-capable threats, and that security-by-design[2] approaches should be the focus of developers to manage risks in an integrated way. There was also disagreement about whether existing guidance in security will be adequate, with one participant commenting that these new technologies may require this guidance to be updated.

Participants were also asked whether the attention given by designers to safety, security, and non-proliferation and safeguards is adequate. The results of this are shown in Figure 1. All participants said that safety is receiving at least "somewhat adequate" attention from developers, and most said the attention on safety was sufficient. However, for security, and non-proliferation and safeguards, participants were more divided. Most participants did feel that the attention given to these aspects was somewhat adequate, but some also felt that the attention given was "somewhat inadequate". Regarding security in particular, participants gave more positive responses regarding computer security than physical protection or insider threat risks. In a comment on this question, one participant noted that the responses here are generalised across all developers, whereas they believe that the attention given to each area is likely to vary notably from one developer to another.

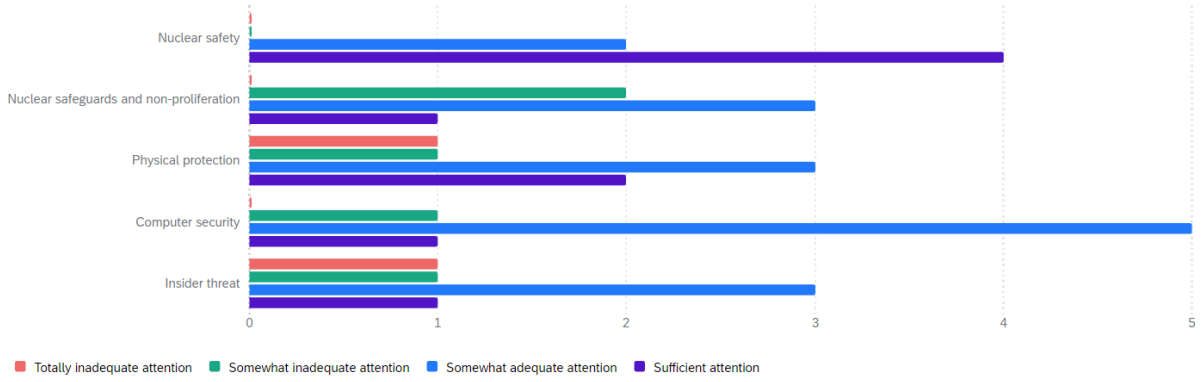

FIG. 1. Results from the question: "In general, are emerging reactor technology developers giving sufficient attention to the following issue areas?" Seven responses were received to this question.

3.2. Modular construction of smaller power plants

Participants were first asked about the security implications of modular manufacturing in a factory environment. Responses were split on whether this would present a net benefit or challenge to security, noting that this would depend on the controls applied within and in support of the manufacturing environment to manage risks from insiders, and to prevent the introduction of counterfeit, fraudulent or suspect items (CFSI) into the supply chain. One participant said that they would only deem this acceptable if the same security processes were to be applied to fabrication facilities as are employed at NPP construction sites, and felt that the costs of doing so should be acceptable if spread over multiple units manufactured in such facilities.

Modules produced in such facilities would need to be transported to the eventual site of installation, and participants were asked if these modules might present highly attractive targets to threat actors. Five out of eight respondents felt they would, but it was noted that this would depend if these modules contained nuclear material, with the perceived value to threat actors being greater if this were the case. The risk for modules without nuclear

---

[2] The security-by-design approach has been defined as, "'The design of the nuclear operation, from the start, to meet nuclear security objectives with equal priority to nuclear safety.' This means designing out Vital Areas (VAs) and reducing the potential for unauthorised removal of nuclear material, thereby minimising the need for a [physical protection system, rather than simply incorporating the physical protection system into the design of the facility]." [12]
WORLD INSTITUTE FOR NUCLEAR SECURITY, 4.1 Implementing Security by Design at Nuclear Facilities, World Institute for Nuclear Security, Vienna, 2019.

materials was not seen to be significantly greater than the transport of large components for current NPPs. A specific question was then asked about cassette cores—complete reactor cores of fuel which are transported, installed and irradiated as a single component—and whether these are more challenging from a security perspective than cores composed of a number of smaller fuel assemblies or bundles. Participants answers tended slightly towards cassette cores being more problematic, but no comments were provided as to why.

3.3. Economics of MR and security

Participants were first asked what proportion of an MRs annual operating budget should be spent on nuclear security, divided between physical protection, computer security and insider threat mitigation. Five participants provided answers to this question, with four giving a combined security budget of 10-20% of total operating budgets, and the fifth being 61%. This is compared to a reported 15-25% of total operating budgets being spent on security staff costs today [3]. Breaking down these budgets by security type, each participant allocated 20% ± 3% to insider threat mitigation. For the remaining 80%, most had a higher budget for computer security than for physical protection. However, one participant commented that this breakdown will be highly dependent on the MR technology and deployment site.

Several questions sought to address how developers might reduce security costs, which is primarily thought to be achievable through the reduction in security staff numbers and instead by designing security into the plant itself, for instance by making the plant resistant to design basis security threats for long enough to allow the neutralisation of the threat by an offsite response force. Asked first if plants could be designed to deliver security performance with no on-site human security presence, participants were divided but most did agree this would be possible. One agreed only subject to there being no security risk from doing so. One participant noted, however, that on-site human security also supports public acceptance of nuclear power, and even if the technical and regulatory approvals were to be achieved, public acceptance may be a higher barrier to overcome. As a variation on the previous question, participants were then asked about whether they believed it would be possible to design MRs to be fully self-protecting against physical threats for extended durations, e.g., several hours, without the intervention of human guards or response forces." Six of the eight responding participants agreed that this would be possible.

The factory manufacture of MRs suggests that all units of the same type will be identical. Given that the threat landscape faced by nuclear facilities varies both between and within countries, participants were asked if they believed that a single design could be delivered for any given MR that would suit all siting scenarios globally. Five out of eight participants strongly disagreed with this suggestion, though three thought it would be possible. To manage this potential need to adapt to differing security threat environments, participants suggested that the security-by-design approach be used to minimise the consequences and vulnerabilities associated with MR designs, e.g., by reducing nuclear materials inventories, making nuclear material inherently self-protecting, and ensuring high standards of computer security.

3.4. Greater use of digital systems, automation, and remote operations

To control operating costs, reduce human error, and achieve other potential benefits, many plants are seeking to make greater use of digital systems in security, including automated systems potentially supported by artificial intelligence. In this section of the survey, participants were first asked how well they believed automated systems might be able to deliver the detection, delay, response and deterrence functions of nuclear security within the coming ten years.

With regards to detection, this was broken down by identifying potential threats, assessing identified threats, and deciding what action to take based on the results of threat assessment. It should be noted that this is across the full range of threats, including physical, cyber and insider. Most participants felt that threat identification could be automated "very well" within this period, that assessment would be automated "moderately well", and that decision making would only be automated "slightly well", suggesting the opinion amongst participants that humans will likely remain critical in at least threat assessment and decision making for some time to come. However, even if only threat identification can be automated, this will allow the transition of humans into an oversight role, potentially allowing a reduction in staff numbers.

Participants were split evenly as to whether delay could be delivered be automated systems. One participant noted that this depends on the type of threat, and that passive security features such as concrete walls could be

considered to be ‘automated’. When asked a similar question about deterrence of threats through the projection of an image of impregnable security, participants generally felt that automated systems may be less able to deliver this than visible human guards. Several suggestions were provided as to how deterrence might be provided by automated systems, such as constructing the facility below ground level, minimising the number of access points, and deploying automated aerial surveillance drones.

Participants felt that physical and automated elements of security systems will be able work together to respond to security events, with human response forces being supported by automated systems. It was further suggested that if response forces were located far from the site, a non-human first responder may be required, even if this were to be only as a delaying tactic to allow time for the human response forces to arrive and deploy.

Participants were then asked about the impact of reducing security headcount, and on average believed that there would be an increase in cyber-attack risk, but were more split on deterrence of physical and insider threat action. They noted that reducing personnel numbers may embolden less careful attackers and thus increase risk, and that greater use of automation risks worsening security by extending the attack surface for cyber-attacks. They also noted that humans are versatile and able to fulfil multiple roles at need, whereas automated systems are usually composed of a set of dedicated elements, and so additional redundancy may be required to offer the same level of resilience.

Participants also suggested that digital twin technologies (highly accurate digital representations of complex real world systems, such as nuclear power plants) will likely be able to enhance surveillance capabilities, and advocated for technology developer organizations to internalize the security-by-design philosophy such that digital security will be embedded in the design of the MR itself, especially for remote operation or when using automated systems. They said that only through embedding security at the design stage can the greatest security benefits be achieved at the lowest cost, as this will allow the remainder of the plant, and its processes and procedures, to be designed in a way that respects the security objectives of the MR.

Participants were also asked about the remote operation of MRs by staff working from offsite, and half of them believed this would be possible, but many noted that this would be heavily dependent on the individual reactor technology, site, and other factors, and a general answer without this context would not make sense. One noted that this may be more achievable if the MR has highly effective containment, is secured in position, and it has been demonstrated that there will be no environmental impacts resulting from any accident. They nevertheless said that response forces may still be required.

When asked about response forces, and whether local law enforcement officers might fulfil this capability without specialised nuclear-specific training, participants said officers may deliver response, but they must have training on nuclear issues. One participant suggested that they could, in responding, coordinate closely with the facility’s operating staff in their tactical decision making, although the speed at which security incidents evolve, and the introduction of complexity into the response force chain of command, may make this ineffective.

When asked about the potential for staff to work remotely from their own homes, it was strongly agreed by participants that this would be acceptable for staff unable to directly influence nuclear operations. For staff who do have such influence, participants were split in their responses. A participant noted that remote operation will necessarily create a need for highly secure communications networks, and these must be built in at the design stage. When asked to rank a series of roles based on their ability to work remotely, security personnel were amongst the least able to do so, being viewed as required on-site to deliver their roles.

Instead of working from home, participants were asked whether centralising staff in an office-type location away from the nuclear site would bring security benefits relative to individual home working. Some participants believed so, but most were unsure. It was noted that this proposal would limit the risks of insider threat from unmonitored lone workers, as well as protecting workers from external attack at a secured office location.

3.5. Advanced reactor and fuel technologies

Many developers are seeking to implement passive safety systems in their designs, and it was asked whether these will have a positive or negative impact on security. Most participants reported a positive impact, saying that removing the need for active systems removes potential security event initiators, and that plants which are safe by design reduce the need for security, at least in terms of sabotage, if not unauthorised removal of nuclear materials.

Developers are often also seeking to move towards MRs with lower inventories of nuclear material compared to LCNPPs, but often the nuclear materials are of a higher security category. They were split on whether there would be a net benefit or worsening of nuclear security as a result of these factors occurring in parallel. It was noted that this would depend on the specific quantities and materials involved, but as many deployments of MR will likely feature multiple units operating on a single site, the overall quantity of nuclear material on the average site may not be much lower than it would have been had a LCNPP been installed, resulting in an overall worsened level of radiological consequence in case of a safety or security incident. However, as part of a well-designed and -implemented security system, the resulting risk may be managed successfully. One participant noted that some MRs using enriched uranium are seeking to remain below the 10% ^{235}U threshold, allowing their fuel to be at the same security category as the low enriched uranium used in most LCNPPs. Participants felt that novel fuel forms, such as TRISO and molten salt fuels under consideration for some MRs, did present additional challenges, but that these were largely technical challenges that would be overcome by the relevant developers.

Regarding the deployment of multiple units to a single site, participants were generally accepting of proposals to have security features being used in common across several MRs and/or nuclear materials storage areas, noting that it is easier to protect a single area rather than several areas, but also noting the risks of common causes of failure, whereby defeating a security measure for one unit would mean that this measure would be defeated for all units on the site.

3.6. Wider range of siting and deployment scenarios

Participants were mostly of the opinion that the wider range of siting and deployment scenarios proposed for MRs would create novel security challenges. They noted the risks in particular of urban siting and the potential harm to public confidence in case of a security incident, but also suggested that a rethinking of security approaches could be possible for MRs, taking a graded approach to security based on the anticipated radiological consequences of incidents, rather than focusing on protecting facilities themselves. This would result in, e.g., minimised security measures for MRs where the radiological consequences are demonstrably low in all cases.

Following up on the urban example and other siting scenarios with small footprints, MRs may have a site boundary that is physically very close to vital areas. For such cases, participants were split on whether security objectives could still be achieved without this physical separation. One participant noted difficulty in accepting the idea of having a compact MR site located adjacent to, e.g., an urban residential area, but another noted that physical separation is only one way to achieve the required security functions of timely detection and delay such that attacks can be neutralised, and that barriers and other measures can also enable this. Participants were overall split on whether the loss of distance would make timely detection more challenging.

Moving instead to isolated sites, participants generally anticipated an increase in security costs relative to more traditional siting scenarios, but noted that the radiological consequences might be lower for such sites, allowing for a reduction in security measures. When considering response arrangements, participants were asked about the requirements for response forces, and most commonly accepted were dedicated response forces operating from a centralised hub with a responsibility for several nuclear facilities spread over an area, and local response forces not specifically assigned to nuclear facilities but with training in nuclear security issues operating from a location close to the site. Of course, these two types of responders are distinct and both may be employed as required to fulfil the response function – specially trained local law enforcement officers as first responders, with follow-on capacity provided by dedicated nuclear incident responders from a centralised hub.

From the answers given, it appears that participants value security personnel with specific training in nuclear issues rather than those with no nuclear-specific training, such as the UK's Civil Nuclear Constabulary, a specialised police force dedicated to the protection of civil nuclear facilities and materials [13]. They were also less accepting of response forces being "far" from the site rather than close by. Given the nature of "isolated" sites, which might be spread over vast distances, it may well be that the centralised hub would naturally end up being "far" from at least some of the units for which is provides coverage. Designers will need to consider the trade-off between the achievable self-protection period (i.e., delay) for a given level of security risk driven by the plant design, the nuclear materials inventory, and ultimately the unacceptable radiological consequences, versus the time for response forces to mount an effective operation from their location. Designing for a longer period of self-protection will have capital costs during design and construction, but every minute of delay time allows response forces to be sited further away, potentially in a non-isolated location where it will be easier/cheaper to

maintain their capability, and/or in a location that covers a greater number of units and reduces the response force budget per unit. For the first unit(s), on- or near-site response is likely to be required, but should additional units be constructed then the response function provision might transfer later to a central hub covering them all, lowering operating costs for each unit.

Participants also raised the "coal repowering" scenario proposed by some developers, where former coal-fired power plant infrastructure is used to support an MR. They noted that it will be necessary to consider and likely implement a range of new security measures that were not previously required, ranging from physical protection measures to secure computer infrastructure, supported by new security and safety culture and training programs.

4. DISCUSSION AND CONCLUSION

The results of the pilot survey reported in this paper demonstrate that the respondents have a wide range of views on the novel security considerations for MRs, suggesting that there remains a lack of consensus on many of these issues. The respondents suggested a range of challenges and mitigation measures that developers would do well to consider as they design their MR concepts. Several points were noted repeatedly throughout the results, and these are summarized below.

Respondents noted several times in the survey that each MR design is unique and will have its own specific novel features creating security considerations, in addition to safety considerations, proliferation resistance considerations, and more. They said that it is difficult to answer questions about MR security in broad terms without considering a specific MR design and/or site. Whether the participants would consider a given situation to be acceptable from a security perspective is impacted by numerous factors, as a result of the wide variety of SMR technologies currently in development and the lack of experience in delivering security using the types of approaches suggested here. Security solutions will, of course, need to be developed on a case-by-case basis, ideally using a security-by-design approach which seeks to reduce and ideally eliminate the potential consequences of any security incident. Despite this, considering broad questions of what might be acceptable is a useful exercise for the nuclear security community, as well as for MR developer organisations, as they seek to understand the range of the possible, particularly as they seek to engage with nuclear regulatory bodies and/or national competent authorities,

Respondents also called on developers to apply the security-by-design approach. Suggestions included focusing on reducing the inventories of nuclear materials and their security category under INFCIRC/225, and maximising time for response forces to neutralise threats through early detection and maximised delay on attackers. If the radiological consequences of security incidents can be minimised or even eliminated during design then the delivery of security during the MR's operational life will become simpler and less costly. Developers must give proper attention to all three security domains, and pay particular attention to computer security given the greater use of digital systems, automation, remote operation, and other features with the potential to increase the attack surface for attackers with cyber capabilities.

Furthermore, there will be interfaces and interactions between security and other considerations, and none of these areas can be effectively managed in isolation. The effective mitigation of nuclear risk requires a holistic approach to both mitigate mutually reinforcing risks and to maximise the benefits of synergies between different areas of nuclear design.

One participant's comment summarises much of the above: "I think it is less about using automated security response systems. It is mostly about making the reactor design robust enough such that no matter how, when, who, [or] with what it is attacked, the consequences will be very low (lower or at least [the] same as the safety consequences of a postulated design [basis] accident). Thus, security-by-design of MRs and advanced reactors is of high importance and some vendor may realize it, some may not. I also hope regulators would realize it and embrace it."

This project has taken onboard a range of comments made by participants on the survey design, which will be used in the improvement of the survey itself. The revised survey will be distributed in due course to a wider range of potential respondents, and supported by interviews with those who volunteer from amongst these respondents. It is intended that a fuller set of results, from a larger number of participants, will be published in due course.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Advances in Small Modular Reactor Technology Developments, IAEA, Vienna, Austria, (2022).

[2] PEEL, R., FOSTER, G., and AGHARA, S., Nuclear Security and Safeguards Considerations for Novel Advanced Reactors, King's College London, London, (2022).

[3] LYMAN, E., Small Isn't Always Beautiful - Safety, Security, and Cost Concerns about Small Modular Reactors, Union of Concerned Scientists, Cambridge, MA, 2013.

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

[5] GLOBAL NEXUS INITIATIVE, Advancing Nuclear Innovation - Responding to Climate Change and Strengthening Global Security, Global Nexus Initiative, 2019.

[6] WORLD INSTITUTE FOR NUCLEAR SECURITY, Security of Advanced Reactors, World Institute for Nuclear Security, 2020.

[7] SQUASSONI, S., New Nuclear Energy: Assessing the National Security Risks, George Washington University, 2024.

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Technology Roadmap for Small Modular Reactor Development, IAEA, Vienna, 2021.

[9] SCHLISSEL, D. and WAMSTED, D., Small Modular Reactors: Still Too Expensive, Too Slow and Too Risky, Institute for Energy Economics and Financial Analysis, Lakewood, OH, 2024.

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5), IAEA, Vienna, (2018).

[11] At Work 2024, World Nuclear Association, 2024.

[12] WORLD INSTITUTE FOR NUCLEAR SECURITY, 4.1 Implementing Security by Design at Nuclear Facilities, World Institute for Nuclear Security, Vienna, 2019.

[13] About Us - Civil Nuclear Constabulary https://www.gov.uk/government/organisations/civil-nuclear-constabulary/about