World Institute for Nuclear Security

SECURITY OF SMALL MODULAR REACTORS (SMRs)

WORKSHOP REPORT

VIENNA, AUSTRIA, 5–6 MARCH 2019

BACKGROUND

The emergence of small modular reactors (SMRs) has the potential to provide energy in numerous countries around the world. These reactors are inherently safer than commercial nuclear power plants currently in operation; they could also be located closer to densely populated areas and provide energy where the needs are. Moreover, due to their flexibility, SMRs could play a key role in the emerging decentralised power supply energy market, providing clean, safe, competitive and reliable energy while protecting the environment. Potential reductions in cost and maintenance, as well as ease of operation, provide additional incentives to use SMRs in a wide range of environments and geographical locations.

One key requirement for the sustainable operation of SMRs is to reduce the cost of nuclear security without compromising either safety or security. Another issue is how SMR design and technological choices will impact the risk picture and how the regulatory approach might need to evolve in response. These and similar issues require that security implications be considered early in the design stage (when safety considerations are also being designed in). Doing so will help to support the acceptance and successful implementation of this new technology.

WORKSHOP STRUCTURE

This workshop was divided into five main sessions, which enabled a wide variety of speakers to provide their perspectives on SMR security.

OPENING SESSION

The opening session, which was led by WINS Executive Director, Dr Roger Howsley, provided an overview of the topic, of WINS' vision regarding SMR security, and WINS' commitment to address nuclear security in the new emerging reactor technologies. Dr Howsley explained that the main objective of the workshop was to review and discuss security matters related to the design, commissioning and operation of SMRs. These included:

- SMR technologies and the implications for security
- Implementing security by design and converging nuclear safety and security
- Impact of SMRs on the security of the fuel cycle
- Impact of SMRs on the regulatory framework

Dr Howsley also shared the results of the pre-workshop survey:

- A little over 80% of workshop participants think that SMRs based on light-water reactor (LWR) technology are less intrinsically secure than other technologies.
- Seventy percent think that potential SMR customers view security as one of the key issues.
- A little over 50% believe that the cost of nuclear security will be lower for SMRs than for conventional NPPs.
- Fifty percent are not sure whether SMRs will be resilient to cyberattacks.
- Seventy percent believe that SMRs represent an opportunity to increase harmonisation of international security regulation.

PARTICIPANT INTRODUCTIONS AND EXPECTATIONS

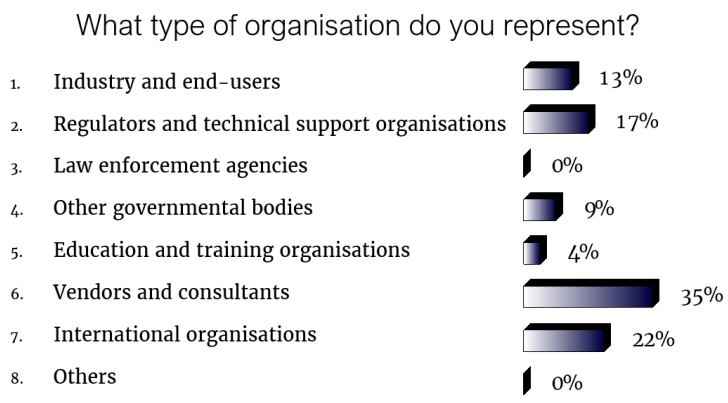
The workshop facilitator, **Ms Diana Danziger**, continued the opening session by asking participants to introduce themselves and share their expectations for the workshop. Examples of participants' expectations included to:

- Obtain an overview of security issues and challenges specific for SMRs
- Learn about the proposed security considerations, including cybersecurity measures
- Learn from the perspective of designers and operators of SMRs
- Inform stakeholders in nuclear security and help break down the barriers that currently exist
- Network, share experiences, benchmark and update knowledge
- Participate in interesting, expert-level discussions
- Be inspired

The participants also mentioned some major security challenges with SMRs:

- Siting of SMRs near urban areas
- Lack of communication among different stakeholders
- Creating a robust and sustainable manufacturing process using a professionally competent workforce
- Cybersecurity resilience
- Fuel cycle implications in terms of nuclear security and non-proliferation
- Regulation and compliance

In an e-vote, participants were asked to indicate what kind of organisation they work for. Their answers indicated a wide variety of backgrounds:



KEYNOTE PRESENTATION

In the keynote presentation, **Mr Riyaz Natha,** Sandia National Laboratories (USA), addressed security considerations for SMRs. He highlighted the important role that the IAEA and nuclear regulators play in SMR deployment and said that SMRs have the potential to grow in the following years. This is why it is so crucial to consider their security implications now.

Mr Riyaz also raised several important questions (many of which were discussed and analysed during the workshop) for participants to consider:

- Will States need to create additional regulations to address the new technologies?
- Should current nuclear security guides be revised to address SMR deployment, or should new guides be created?
- For government/private consortiums, who would be responsible for nuclear security implementation?
- Would construction of security components still require the same rigor as for traditional nuclear power plants?
- What legal considerations need to be addressed for SMR ownership?
- What would taking a graded approach toward SMR security look like, especially as scalability increases for modular energy?
- How would local and national DBTs or threat assessments (NSS-10) apply to these facilities?
- Should sabotage analysis for unacceptable (URC) or high radiological consequences (HRC) be based on State regulations or on NSS-13?
- Will it be necessary to store fresh fuel onsite per NSS-13?
- What are the security considerations for underground, above-ground, underwater, and portable units?
- If SMR units are being transported as turn-key systems, how will security be implemented during transport?
- How will nuclear material and accounting control measures be implemented?
- What compensatory measures will be necessary for loading and unloading fresh and spent fuel?
- Do the IAEA, WINS or other international organisations currently provide documents and guidelines that specifically address SMR security?

Participant Discussion

During the discussions that followed the keynote speech, some participants stated that nuclear safety could address 75% of the nuclear sabotage issues, which may be be one of the reasons that SMR developers are not paying a lot of attention to security. Participants also mentioned that the SMRs that will be built in the coming years will likely be placed next to or inside current nuclear facilities. Consequently, they will use the already existing physical protection systems. This is the case, for example, of the CAREM project in Argentina and the NuScale reactor at the Idaho National Laboratory.

SESSION 1: SMR TECHNOLOGIES AND THEIR IMPACT ON SECURITY

The objective of this session was to provide an overview of different SMR technologies that are currently under development. This not only includes the LWR, but also such technologies as the molten salt reactor (MSR) and the fast neutron reactor (FNR). The session addressed how various technologies will impact on the security requirements, the criteria to use to assess nuclear security arrangements for different technologies, and the influence of SMR locations on security requirements.

First Presentation

Mr Frederik Reitsma, Team Leader on SMR Technology Development at the IAEA, delivered the first presentation, which was titled *The status of Different SMR Technologies and the Role of the IAEA to Support Its Member States in SMR Technology Development*. He explained that many SMRs are under development and that a wide variety of technologies are being considered. Many IAEA member States—including new-comer countries planning to deploy NPPs for the first time—are interested in the development and deployment of SMR technology, but only three are currently under construction, and only a few more have specific development plans.

Mr Reitsma explained that the IAEA has categorized SMRs into six main types and published a document describing the main features of 56 SMR designs. He also said that SMRs have an important role to play in climate change and future energy solutions around the world. For example, they could be integrated with renewable energy sources to co-generate electricity. Some advantages of cogeneration would include:

- Increasing the flexibility of the electric network to match energy demand.
- Improving the economics of nuclear power plants (NPPs) due to better use of fuel and/or shared infrastructure
- Improving NPP efficiency
- Sustaining a clean environment free of CO_2

When it comes to security, Mr Reitsma said that it is important to consider the following SMR design characteristics:

- Simplification by modularisation and system integration
- Multi-module plant layout configuration
- Underground construction for enhanced seismic and physical security
- Enhanced safety performance though a passive system

Participant Discussion

In discussions following the presentation, participants emphasised that stakeholders not only need to consider the economic and financial aspects, but also public and political opinion.

Second Presentation

In the second presentation of Session 1, **Mr Adrian Prior**, Frazer-Nash Consultancy (UK), discussed the Nuclear Innovation Programme (NIP) in the UK. Funded by the UK Government, NIP's objective is to encourage research, innovation, new technical

approaches, and the development of skills and capability in a range of cutting-edge areas, including the safety and security of SMRs.

Mr Prior explained that the main objective in reactor design is to develop the digital tools and fundamental scientific understanding necessary to design and build future generations of reactors in an accelerated and cost effective way that continually increases safety. Together with Rolls-Royce and other nuclear stakeholders, Frazer-Nash Consultancy is working on security projects like security by design, cost/benefits analysis, an as low as reasonably practicable (ALARP) approach for safety and security, security assessment principles and many others. He also discussed the benefits of using security modelling and simulation assessment for security in the nuclear industry.

Expert Panel Discussion

After Mr Prior's presentation, participants had the opportunity to listen to a panel of experts, including:

- Troels Schönfeldt, CEO of Seaborg Technologies APS (Denmark)
- Janne Wallenius, Founder of Leadcold (Sweden)
- Eddie Marrett, Head of Security Consultancy, Civil Nuclear at Rolls-Royce (UK)
- Andrew Knight, Nuclear Safety Engineer at Rolls-Royce (UK)

The panel discussed the main requirements for SMR security, whether developers consider security in the conceptual phase or through design implementation, if any features in reactor design enhance security system effectiveness against physical threats and/or radiological sabotage, and some of the main advantages that SMRs have over current operating plants for improving security efficiency.

Some of the panel's major conclusions were:

- Nuclear security stakeholders need to have a full understanding of the threat. They need to understand what the evolving threat could be like in coming years and how to adapt to it.
- The first requirement is cost-benefit.
- SMR technology is a great opportunity for the nuclear industry and could lead to a nuclear renaissance. It also provides an opportunity to change people's views on the nuclear sector.
- No clear guidelines exist regarding SMR security. Developers are not sure where the boundaries are or how much protection is necessary for their designs.
- It is very important to take the design basis threat (DBT) into account, but doing so is not the answer for everything.
- It is still unclear who is going to insure SMRs facilities, which means there is a business opportunity for private insurance companies.
- Some vendors think security staff need to be eliminated so the SMR can be cost-effective.
- The price of MWh for SMRs could be more expensive than for large conventional NPPs.

Participant Discussion

In table discussions following the panel presentation, participants identified the need for regional and international agreements amongst vendors, customers and host countries on security requirements. They also pointed out that security discussions among different stakeholders are not currently taking place and that a forum for discussion would be extremely useful.

Third Presentation

In the final presentation of Session 1, **Ms Liliana Garrigó,** National Atomic Energy Comission CNEA (Argentina), explained that CNEA is developing its first SMR, which is totally designed in Argentina. The prototype, called CAREM 25, will be located next to the Atucha I and Atucha II NPPs, a few kilometres away from Lima, Province of Buenos Aires. Ms Garrigó explained that the construction of CAREM, which will generate in the order of 25 MWe, respects the highest requirements of safety and security. For example, it will include an advanced control room with minimum human interaction. Due to the reactor design, the risk of a radiological release or an accident involving loss of coolants is extremely low. Furthermore, CAREM is safer due to natural circulation and the existence of passive systems.

Ms Garrigó also explained that the physical protection system and legal framework reference the following publications:

- Nuclear Regulatory Authority of Argentina (ARN): AR 10.13.1. Rev. 1 Standard of physical protection of nuclear materials and facilities
- IAEA-TECDOC-1276: *Handbook on the Physical Protection of Nuclear Materials and Facilities*
- INFCIRC/225/Rev.5: *The Physical Protection of Nuclear Material and Nuclear Facilities*

Participant Discussion

In the discussions that followed Ms Garrigó's presentation, participants focused on what should be addressed in a mission statement for SMR security. Some observations included:

- Security should be proportionate, based upon outcomes, and specific to the reactor design.
- The manufacturing process of SMRs opens a new threat through the supply chain.
- The perception of nuclear security should be given more importance.
- Safety and security must work together from the very beginning.
- SMRs should be designed to tolerate cyberattack.
- Nuclear security stakeholders should pay more attention to nuclear material accounting.
- Physical attacks might face longer delay times.
- SMR reactors should be designed to tolerate zero cybersecurity risk.

SESSION 2: IMPLEMENTING SECURITY BY DESIGN AND CONVERGING NUCLEAR SAFETY AND SECURITY

This session explored the design requirements for nuclear security and the extent to which the security DBT has already been taken into account. It also addressed how security by design could be implemented during the various lifetime phases of a nuclear facility and to what extent safety methodologies can be used to calculate and justify security arrangements.

At the beginning of Session 2, participants briefly discussed possible SMR security costs per unit and per MWe in comparison to conventional NPPS. Most said they think security costs will be lower for SMRs and that the most important factor is security staffing, which is a significant factor in the total cost of operations and maintenance. They also thought the strategic development and deployment of SMRs will help to shrink costs, especially if security by design takes place and safety and security are integrated early in the process of reactor design. In addition, the development of pragmatic and performance-based security arrangements will help to minimize security workforce expenses.

First Presentation

In the first presentation of Session 2, **Mr Eddie Marrett,** Rolls-Royce (UK), talked about the challenges of SMR security and of finding a balance between commercial and regulatory pressures. He also said that achieving the main principles of security by design means adopting an integrated approach that ensures an inherently secure design, passive security and an evolving response. Some important considerations in this regard include:

- Understanding the evolving threat
- Knowing what to protect against
- Understanding when enough is enough, what the limits are of investing in security
- Convincing other stakeholders

Moreover, Mr Marrett emphasized how SMRs provide an opportunity for establishing common plant requirements, optimising the process and using metrics to quantify system performance. Security by design and the coalescence of safety with security will enable the nuclear industry to use a common language for processes, tools and functional requirements. He concluded by emphasising that the need to meet beyond design basis threats does not necessarily mean an increase in physical security measures.

Participant Discussion

In the discussion that followed, participants addressed how lessons learned from protecting current nuclear facilities can be applied to SMR security. They also discussed how to implement a defence-in-depth approach for SMRs and how to promote security through design and installation. Some of their major points include:

- In the absence of a detailed threat assessment from the regulator, SMR developers have to use their best efforts to anticipate the likely threats as part of an all risks approach to SMR safety and security.

- Implementing security by design may allow organisations to cut the security budget, but only if doing so is in line with the national threat.
- When developing SMR technology, it is important to include all nuclear security stakeholders at an early stage. Just one of the benefits of doing so is that it would encourage robust cooperation and communication among them.
- Effectively coalescing nuclear safety and security requires a cultural shift in the industry, which could take years. When recruiting for security positions, hiring applicants with mixed nuclear backgrounds or backgrounds in safety might help rather than just hiring people with professional military backgrounds.
- The use of remotely operated defence systems should be considered.
- Except for high-temperature gas-cooled reactor (HTGR) SMR technology, having as much containment as possible will benefit security.
- Minimizing vehicles, deliveries and the number of staff in SMR facilities may reduce insider threat.
- When it comes to defence-in-depth, it is important to carefully evaluate the lifecycle and vetting regime. Furthermore, multiple layers and strong barriers should be implemented, especially for independent systems, and no single point of failure should be allowed.
- Some ideas for promoting security by design included: designing reactors with a whole-life core that does not require onsite refuelling; building the nuclear island below ground; improving nuclear security culture and infrastructure; ensuring online refuelling; and creating delay by creative thinking.

Second Presentation

Mr Andrew Knight, Rolls-Royce (UK), addressed *Safety and Security Integration* in the last presentation of the day. He explained that applying safety analysis and methodology—such as Probabilistic Safety Assessment (PSA)—to physical protection systems could help the nuclear security industry figure out when enough is enough in regard to securing assets and optimising investments in security measures. To achieve this, nuclear security needs to find the right model based on the following principles:

- Define acceptable risk. (Use ALARP principles.)
- Measure the risk.
- Understand the threat.
- Stabilise predictive systems.
- Calculate the effectiveness of security measures for neutralising a threat.
- Find an accurate risk model.
- Design a robust, reliable framework for nuclear security in conjunction with the framework for nuclear safety.

Participant Discussion

In the discussion that followed, some participants pointed out that frequency calculations and security measures based on probabilities are very difficult to identify for nuclear security. For example, modelling human security performance is a very challenging task. In nuclear safety, there are independent probabilities; however, in security, most probabilities are dependent. Furthermore, the probability that an event will be initiated makes decision trees and numerical analysis much more complex.

Participants then identified some good practices for integrating safety and security:

- Use a specific geographical location for building SMR facilities to increase the delay of a physical attack.
- Consider scenarios in detail so there is a clear understanding of feasible response actions. If SMRs require an offsite response, it is essential to consider exactly what is expected of the police or response organisation.
- Ensure that multidisciplinary safety and security teams share a common language when addressing SMR security.
- Consider the risk appetite of security and safety and ensure they are aligned.
- Consider exclusion zones during the siting phase.
- Integrate security into operational procedures. Give one person the responsibility to ensure that the procedures have been implemented. (This would encourage a more engaged team.)
- Simplify operations and harmonise safety and security.
- During the decommissioning stage, carry out tabletop exercises to ensure a common understanding of the key phases; also be sure to reassess risks.

Dr Roger Howsley concluded Day 1 by pointing out that SMR technology can help to encourage the regulatory body to move from prescriptive regulation to outcome-focused regulation. He also advised participants to push back on regulators in terms of design basics and emphasized the importance of having a mission statement for SMR security that focuses on what the security systems are trying to do rather than on the consequences of not having such systems in place.

He added that stakeholder engagement for SMRs is absolutely essential; organisations and States need to understand this and engage with stakeholder groups. Fundamentally, he said, communication is an essential issue for public acceptance of SMRs. In addition, looking at other sectors with similar security challenges could help the nuclear sector design SMR security more efficiently.

SESSION 3: CYBERSECURITY FROM AN INSIDER PERSPECTIVE

Session 3 focused on the potential threats to SMRs from cyberattack. It also addressed the cybersecurity challenges from an insider perspective and whether cyberattacks on SMRs are more of a concern than on conventional LWRs.

First Presentation

In a presentation titled *Addressing Cyber Threats*, **Mr Christoper Cope,** National Nuclear Laboratory NNL (UK), explained what operational technology is, what its security concerns are, and specific insider threat issues surrounding SMRs. For example, traditional reactors are built onsite, whereas SMRs are built elsewhere and then assembled onsite. This makes supply chain security a major consideration. Another issue is that remote monitoring in SMR connectivity will play a key role and that new regulations for this need to be created.

In addition, Mr Cope said that although SMRs are smaller, their security requirements do not necessarily decrease. He also said that the human factor plays a critical role in security when it comes to insider threat. Authorized people could act deliberately to carry

out a malicious act; they might also contribute to a malicious act by accident or be duped or coerced. This is one reason that the industry needs to address social engineering, take steps to reduce the risk from the workforce, and encourage the design of robotic systems.

Participant Discussion

In the following discussion, some participants said they thought that employing fewer staff in an SMR could lower the probability of accidental risk (e.g. of making a mistake). As a consequence, this would minimise the probabilities of creating or enhancing security vulnerabilities unconsciously. They also said that no direct correlation exists between fewer staff and a lower potential for insider threat but that it would be easier to identify and target an insider who causes major harm.

Participants also agreed that one of the greatest risks when fewer staff are present is that each employee has considerable knowledge about—and responsibility for—a wide range of areas. Should they become an insider, such knowledge makes them particularly dangerous. This is why vetting requirements should be stricter when there are fewer staff.

Another concern of participants was that reducing the cost of an SMR could lead to more and more automated systems and even fewer security staff, which could actually increase cyber risk. With a traditional LWR, one control room monitors each reactor. However, with a cluster of SMRs, one control room would likely be responsible for monitoring multiple SMRs, making the risk exponentially higher. Participants agreed that special cybersecurity controls need to be developed to manage such risk. An additional possibility would be to create a special remote surveillance control room to monitor conditions in the main control room, especially in regard to cyberattacks on the system.

Participants also mentioned that robotic networks and bots could represent a major threat since they can become autonomous and smarter while attacking. Still another issue is that hardware and software need to be as secure as possible as early in the process as possible. The challenge is how to ensure that no company involved in the design, development and deployment of an SMR (from conception to operation) introduces a threat. Procedures need to be developed that minimise the risk that someone could build backdoors into hardware components that would enable a major security breach. To achieve this, individuals involved in cybersecurity should work closely together with their counterparts in safety, security and employee vetting.

Clearly, all evolving threats need to be considered, and excellent communication and coordination between the main control room and SMRs, as well as among all inside and outside stakeholders, is critical.

SESSION 4: IMPACT OF SMRS ON THE FUEL CYCLE

The purpose of this session was to explore the potential impact of SMRs on fuel cycle processes and practices and their security implications. The session also addressed new transport needs and security challenges resulting from SMR technology. In addition, the session addressed international transport issues and the need for States to form agreements with each other regarding SMR transport.

First Presentation

Dr Bhaskar Sur, Canadian Nuclear Laboratories CNL (Canada), began the session with a presentation titled *CNL's Strategic Initiative on SMR and Nuclear Security Issues Anticipated from Development and Operation of New Fuel Cycle Technologies.* He explained that the Canadian nuclear regulator is mostly outcome-focused, which motivates SMR vendors to apply for a pre-licencing vendor design review. He also said that potential end users of SMRs in Canada are mainly in small northern communities, remote mining establishments and military facilities and dedicated facility power. Dr Sur pointed out that nuclear fuel cycle activities will clearly impact on the security of SMR development and operations.

Because the nuclear fuel cycle interlinks safety, security and safeguards, SMR fuel characteristics will be affected due to the existence of passive safety systems, the absence of (or minimal amounts of) refuelling, and the implementation of remote and autonomous operations. Moreover, some SMR designs do not consider traditional nuclear fuel but liquid fuel. All of these new technology features plus other considerations (i.e. long-life reactor core) will require new approaches from many different disciplines of the fuel cycle, including inspections, nuclear security offsite and onsite response, safeguards by design (to be considered at an early stage along with security by design), nuclear material accountancy, transport, etc.

Second Presentation

In the second presentation of Session 4, **Mr Simon Chaplin,** World Nuclear Transport Security (WNTI) (UK), talked about *Transport Considerations for Fuel Cycle Materials*. He said that WNTI foresees several SMR transport challenges, such as:

- If the SMR (e.g. floating NPP) is transported, what regulations would it have to comply with?
- Some SMRs may use MOX fuel, which is subject to extremely high security requirements (Category 1) during transport.
- What regulations need to apply when transporting spent fuel from the SMR or when transporting a decommissioned SMR module with spent fuel inside?
- What kind of transport regulations are necessary if the floating NPP needs to be towed back 'home' every 12 years for refit/overhaul (like ROSATOM's)?

Mr Chaplin also said that one of the biggest challenges for SMR security during transport is going to occur when long distances are involved and different jurisdictions overlap. If an SMR is transported by sea, the shipper may need to transit the territorial waters of a third-party nation. How should this be handled?

Participant Discussion

In the discussion that followed, many participants agreed that the introduction of SMRs will have the greatest impact on the power generation and burn-up phase (out of all phases in the fuel cycle). They also said that public perception of coastal transport and protection of information needs to be addressed. In addition, participants said they were unsure what the costs would be for shipping SMRs and that the cost of a Category 1 SMR could be double that of Category 2 or 3. Because security requirements for SMRs loaded

with fresh fuel will depend on the level of enrichment and categorization, the real differentiator will be design. This means that each design will ultimately have a different impact.

SESSION 5: IMPACT OF SMRs ON THE REGULATORY FRAMEWORK

Session 5 explored how SMRs will impact the existing regulatory framework, including the status of regulations for SMRs in construction, considerations for new regulations, and whether the most effective approach is prescriptive or outcome-focused. The session also discussed regulations on emergency planning zones (EPZ), the assessment of loss of large areas (LOLA), and integrated response planning (IRP) for SMRs.

Panel Discussion

The session began with a panel conversation between Cristina Domínguez, Nuclear Regulatory Authority ARN (Argentina), and Paul McGreavy, Office from Nuclear Regulation ONR (UK). Ms Domínguez shared her experiences on the regulation of the CAREM project in Argentina, pointing out that the regulator was very involved in the project from the beginning. The Argentinian regulator began by establishing an ad hoc licensing scheme applicable to CAREM 25. Since the reactor is a prototype of innovative design, this forward scheme, which was developed for licensing in successive stages, is applicable to the construction (including the design stage), commissioning and testing phases.

The purpose of the ad hoc licensing process is to allow more flexibility in the development of the project. This implies a much closer regulatory oversight whose purpose is to achieve the required safety performance according to Argentinean Regulatory Standards.

The panelists explained the Generic Design Assessment (GDA) methodology that has been developed in the UK for SMRs. They added, however, that the overarching regulatory framework will not change as the result of the development and deployment of SMRs. They also said that regulators are holding discussions about the need to sign regulatory agreements so vendors do not have to go through the full process for every country. This approach would be cost-effective for both regulators and vendors.

Participant Discussion

One of the main inputs from participants who are vendors was that the licensing process for SMRs in Canada is particularly attractive. The Canadian regulatory body has a very proactive attitude, and its approach to inspection has become much more outcome-based over time. Canada currently has ten designs under regulatory review, and vendors who go through the process have learned a great deal as a result.

Another participant said that investing in a nuclear power project implies financial, legal, regulatory and social aspects. A robust understanding of the scope of this analysis is critical for project developers, host governments and prospective financers.

When it comes to newcomer countries, governments are required to create a suitable environment for investment, including professional and independent regulatory regimes; policies on peaceful uses of nuclear energy; involvement with international non-

proliferation measures; and implementation of a liability regime and legal framework for security.

Most participants agreed that there must be an international agreement to operate SMRs in one country. Therefore, SMRs represent an opportunity to increase the harmonisation of international nuclear security regulation. Regulators should be flexible in the licensing process to encourage innovations in reactor design.

Third Presentation

In the final presentation of the workshop, **Mr Dr Lap-Yan Cheng,** Brookhaven National Laboratory BNL (USA), spoke about *Rulemaking for Emergency Planning and Physical Security for SMRs*. He explained the background for SMR rulemaking regarding emergency preparedness and physical security. He also described a scalable method for determining the size of emergency planning zones (EPZ) rather than the fixed 10-mile and 50-mile scale used for large LWRs. In other words, the size of EPZ will be reduced for SMRs. Such rulemaking is technology-neutral and outcome-focused.

Mr Cheng also discussed current research on physical security from a regulatory perspective. Some major points included:

- Address security issues early in the design stage.
- Resolve security issues through facility design and engineered security features, as well as through the formulation of mitigation measures. Reduce reliance on human actions.
- The current framework is adequate for SMRs and non-LWRs.
- Give applicants the ability to propose alternative methods and approaches that are equivalent in performance and that meet the intended functions and requirements.
- Existing security requirements impose an unnecessary regulatory burden on licensees.
- Compliance with existing requirements will diminish cost competitiveness.
- Evaluate an alternative to the prescribed minimum number of armed responders.
- Evaluate prescriptive requirements for onsite secondary alarm stations.

Participant Discussion

Before the closing session, some participants said they would like to discuss the following question: From a security cost perspective, what would be cheaper: a facility with 6 SMRs of 50 MWe or 1 conventional NPP? There was no a general agreement on this question. Some participants thought the SMRs would be cheaper due to the existence of passive systems and a lack of consideration of some design basis accidents (DBAs). Others said the regulator could treat 6 SMRs as 6 vital areas instead of one. The main conclusion was that the SMR industry needs to conduct tests, learn from the outcomes, and report on the results.

CONCLUSION AND WAY FORWARD

The purpose of the final discussion was to identify and discuss tangible and realistic next steps, as well as to review the roles that operators, regulators, industry, and international organisations should play. In addition, participants were asked to review which workshop

topics were most relevant to them, which ones were directly applicable, and which ones were not. Participants were also encouraged to identify some key points for the WINS Special Report on the security of SMRs. Below are some of the results:

- The definition of an SMR is not clear. Technology matters.
- SMRs cover a wide range of technology. Security needs to be proportionate and specific to the circumstances (technology, location, etc.).
- Case studies could be added.
- Make it clear that unless security is carefully considered in design and takes safety characteristics into account, it will cost the same per site (or more).
- The international industry and a regulator forum should drive a common approach to SMR regulation, including potential new regulations.
- Participants strongly endorse an outcome-based approach to security as best practice (technology, size, location neutral).
- There should be more readily available information on international DBTs (i.e. baseline/representative DBTs).
- Apply integrated security and safety cost-benefit analysis to ensure affordability.
- Clarify the basis on which SMRs might have fewer nuclear security needs.
- Integrate safety and security. They should be addressed early and together.
- Calculate the true cost of security and provide examples.
- Calculate lifecycle security costs.
- Collaborate to develop cyber design threats.
- Regulations need to be flexible and commensurate to the design.
- Ensure vendors and designers have the information they need to implement security by design.