THE SECURITY OF ADVANCED REACTORS

Álvaro Acevedo
Programme Manager at the World Institute for Nuclear Security

ABSTRACT

The development of advanced reactor (AR) [1] designs to generate carbon-free power for a variety of commercial applications, beyond electricity supply, is attracting growing interest. The deployment of these AR designs is intended to address longer-term challenges associated with nuclear technology including the cost of deployment; their competitiveness with existing technologies; the concern surrounding potential proliferation issues; the management of long-lived radioactive waste; their safety; and the security issues associated with AR designs. The future deployment of these reactors is dependent on designers and developers addressing important issues related to the security of these reactors and associated facilities, including proposed fuel types. In 2020, the World Institute for Nuclear Security (WINS) conducted a broad and in-depth study of ARs that focused on developers of ARs. The purpose of the study was to extend their understanding of nuclear security issues. WINS interviewed more than 20 subject matter experts and identified five actionable recommendations that will need to be addressed by the main stakeholders for the successful deployment of ARs. This WINS study presents a high-level perspective of the main international instruments, standards and guidance that should influence the development of national laws and regulations that will govern the deployment of ARs in different countries. The main theme of the study was to encourage developers and designers to incorporate security as early as possible into the different designs. WINS analysed the specific security considerations and challenges of the various reactor designs in meeting different countries' existing regulatory requirements and introduced an overview of security by design methodologies that could be adopted by AR developers. This paper will present the highlights of the study and its importance for designers and developers as well as operators and regulatory bodies in all countries where this technology will be deployed.

INTRODUCTION

In recent years, there has been growing interest around advanced reactor (AR) designs in developing nuclear energy as an alternative to fossil fuel. This new generation of reactors will deliver carbon-free power for a range of commercial applications that extend beyond simply supplying electricity. ARs also have the potential to address longer-term challenges of nuclear technology, including cost and competitiveness, potential proliferation issues, as well as the management of long-lived radioactive waste, safety and security. The last issue lies at the centre of this paper.

To benefit from these emerging technologies, the World Institute for Nuclear Security (WINS) believes that developing confidence is vital for stakeholders, particularly the public who will expect these new reactors and facilities to be secure. To this end, WINS conducted in-depth research and published a Special Report that focuses on the security of ARs. The preparation of

[1] There is no general consensus on what exactly falls into the category of AR. For example, the IAEA includes light water small modular and large Generation III+ reactors in the AR category, together with Generation IV and other non-light water reactors. On the other hand, the Global Nexus Initiate (GNI) report (2019) on *Advancing nuclear innovation: Responding to climate change and strengthening global security* only included reactors that use molten salt as a fuel, have TRISO-based fuel or a fast neutron spectrum. For simplicity, the WINS Special Report on *Security of Advanced Reactors* and this paper examine the same reactor designs as those contained in the GNI report.

this report included more than 20 interviews with various developers, regulators and subject matter experts.

As a result of this research, the WINS Special Report provides an overview of the international environment in the deployment of ARs, examines specific security considerations and challenges of various reactor designs, and further recommends security by design methodologies.

INTERNATIONAL PERSPECTIVE AND REGULATORY ISSUES

The involvement of the international community is crucial to ensuring this new generation of reactors is secure. In this regard, the WINS Special Report offers a high-level perspective of the available international instruments, standards and guidance that shape national regulations and laws surrounding ARs.

To begin with, WINS recognises that the International Atomic Energy Agency (IAEA) is the primary international organisation that provides guidance relevant to developers and has two key documents in this area. The first is the IAEA Nuclear Security Series (NSS) 13 document, which provides general guidance on physical protection and interfaces with safety and nuclear material accountancy and control activities. The IAEA also provides comprehensive guidance in its NSS 35G entitled *Security During the Lifetime of a Nuclear Facility* and suggests incorporating nuclear security in the early design stage and integrating security with safety, safeguards, operational and other measures.

In addition to these two guidance documents, two international working groups exist to evaluate the viability of ARs in a number of areas, including physical protection. The first is the International Project on Innovative Nuclear Reactors and Fuel Cycles (INPRO), and the second is the Proliferation Resistance and Physical Protection Working Group.

Because of the need to have an effective licensing process to successfully develop and deploy these new and diverse technologies, WINS interviewed officials from three regulatory bodies to understand common challenges in how they are developing regulations for and the approach to licensing these ARs. Regulators interviewed by WINS are examining a performance-based approach with fewer prescriptions or requirements, which recognises that ARs may require a more flexible and technology-neutral approach in order to address significant variations between the different reactor designs. There is also recognition that emerging technologies and threat capabilities will be particularly relevant to ARs, particularly cybersecurity, which poses a new and evolving threat that will necessitate an update of the regulatory framework.

SECURITY CONSIDERATIONS FOR ADVANCED REACTOR DESIGNS

One of the main objectives of the WINS Special Report is to encourage AR developers to incorporate security as early as possible into different designs. This concept is referred to as *security by design*, the methodologies of which are laid out in further detail in the next section. In order to accomplish this, developers first need to understand the security considerations for AR designs.

Building Physical Protection Systems

The variables that underpin traditional physical protection systems stem from three pillars in managing risk: threat reduction, improvement of the effectiveness of the systems and reduction

of the potential consequences of malicious acts. Similarly, a wide variety of variables also drive the physical protection of ARs.

As part of WINS' research, we found that the risk of theft or sabotage depends on the quantity of material used and frequency of refuelling, which varies depending on the specific technical characteristics (size, type of fuel required, operating cycle, etc) of each reactor. All these considerations will impact security. Some designs will make reactors less susceptible to overheating and core damage as they will make use of passive safety features and be less reliant on external power as a result. For example, some developers propose an underground siting to defend against potential sabotage scenarios such an aircraft crash. Some AR designers are incorporating engineered physical protection systems into their designs. However, challenges arise when attempting to factor in several variables in the early stages of design.

Threat reduction can be challenging in light of new AR designs. It can be difficult to determine the potential impact of variables in certain cases, such as threat reduction during the transportation of fuel. Most AR systems are likely to be dependent on offsite fuel fabrication facilities in receiving fresh fuel supply. For example, fuel that is fabricated offsite in a factory could be transported with the full core inside, preventing the theft of fuel elements during refuelling onsite. This feature hinders theft of nuclear material and facilitates its protection. However, offsite-refuelling/onsite-refuelling has an interface with safety, since transporting nuclear material that has a significant total decay of heat is not as safe as transporting smaller quantities. This is worth mentioning considering that the full core of some reactor designs contains more than 10 kg of uranium-235, with enrichment higher than 10%. This results in additional requirements for security measures compared with transporting fuel for a traditional pressurised water reactor (PWR). This is because it would be easier to produce a nuclear explosive device from a PWR's fuel. The threat is greater in consequence. This constraint is reflected in the IAEA's categorisation of nuclear material based on its attractiveness for fabricating a nuclear explosive. The mass of uranium-235, uranium-233, polyurethane, and the enrichment level drive nuclear material from non-categorised for natural uranium to categories III, II and I.

Following from this, the attractiveness of nuclear material for theft depends on the mass of the fissile material - polyurethane, uranium-233 or uranium-235 - and the level of enrichment. The mass of the fissile material in a reactor core is somewhat related to the balance between enrichment and burnup at the end of life and the power of the reactor. For this reason, larger reactors - which produce more decay heat - need more stringent security measures. On the other hand, irradiated material tends to deter adversaries from theft. In consequence, spent fuel could be reduced down by one category level. However, irreversible health effects will not stop some attackers from committing a malicious act, such as suicide terrorists. The type of the fuel is also relevant for determining the magnitude of the risk based on the complexity to separate fissile materials. In TRISO fuel, this is due to its physical robustness and high melting temperature. In molten salt fuel, this is caused by the chemical bonds that make harder to separate uranium. These characteristics could be leveraged to reduce other security requirements in TRISO and molten salt reactors.

Enhancing the effectiveness of a physical protection system for ARs is also critical in reducing risk. This pillar also includes a wider array of variables, which are harder to quantify simply due to their interplay and their relations with the variables affecting the first and third pillars. Furthermore, certain measures meant to advance effectiveness can lead to an increased risk. For instance, longer fuel cycles - where refuelling happens every several years (or never) -

would improve the effectiveness of the physical protection system by narrowing the window in which the fuel is the most susceptible to theft. However, at the same time, this refuelling scheme entails concentrating a larger amount of fissile material in the core, which makes it more attractive to saboteurs. The radiological consequences of successful sabotage in a reactor with a larger amount of fissile material are potentially more harmful. The effectiveness of the physical protection system can be greatly increased by adopting the defence in depth security measures and the instilment of security culture in every stakeholder from an early stage.

Early adoption of defence in depth strategies in security is crucial in avoiding a divergence between safety and security on a particular feature. The siting strategy also has a remarkable impact on the second pillar. This includes the location but also integration with the site, i.e. embedded (below grade) or above grade. Embedding the reactor building offers a set of advantages for safety and security. Improved sightlines for security forces can result in the need of less staff for surveillance of a site. Embedment generally helps in protecting against human-made threats, such as airplane crashes, missiles, sabotage or internal explosions. Likewise, embedment is generally an asset from a safety standpoint, reducing the hazards from accidental explosions, tornadoes or earthquakes. However, embedment can also hinder safety and/or security. It limits entries and exits on the reactor hub, which can facilitate attackers locking themselves in and impede security forces from accessing the hub. Furthermore, gas reactor design that relies on conduction through the reactor room and out to the outside atmosphere to evacuate decay heat will increase its thermal resistance if the reactor is embedded.

Also critical in advancing the effectiveness of an AR physical protection system is the usage of pebbles – which are hexagonal graphite fuel blocks in which the TRISO fuel particles are dispersed – and are advantageous from an operational and fuel optimisation point of view. This is because pebbles permit online refuelling. The low amount of nuclear material in one pebble allows for a reduced category during transportation. However, their small size makes them easy to steal and hide. For this reason, it is important to have nuclear material accounting and control measures in place to track fuel inventory. In addition, remote monitoring of the core in pebble bed reactors is somewhat challenging, since it is difficult to know the exact locations of the pebbles at every moment - and there are thousands of them. Along these lines, it is not possible to use effectively cameras to remotely surveil all types of ARs (except for gas reactors) due to the opacity of the coolant. The position of hexagonal blocks, their size and the transparency of the coolant sets graphite block gas reactors apart from the others in this regard.

On the other hand, the large negative temperature coefficients of sodium reactors and gas reactors, result in an intrinsically robust physical protection system, making it nearly impossible for an adversary to cause severe core damage.

Mitigating the outcome of malicious attacks is the third pillar in physical protection. There is another aspect where safety and security may diverge when it comes to ARs. The use of a digital twin – which is a real time model of the reactor's operational state – provides a great advantage in previewing the outcome of every possible decision in real time. However, overreliance on digital twins can pose a security challenge if extra computing power from the clusters web connected is needed. In this case, a cyberattack could shut down the digital twin or make it return an unwanted outcome. The degree to which a plant can be isolated from the web is a physical protection feature.

Similarly, the main control mechanism (industrial control systems), such as control rods or safety rods, might be designed such that there is a divergence between safety and security

criteria. Gravity is usually the driving mechanism to scram the reactor if the control rod activation mechanism is deenergised. In some AR designs, gravity does not drive control rods. In this case, a normally closed sprang system is added so that if the control rod is deenergised, it closes. Normally closed control mechanisms present safety features, but if these systems can be tweaked to retain activation, thanks to a redundancy in its activation system (such as additional electric trains connected to diesel groups or batteries coupled to the electromagnets that energise them), they can pose a vulnerability from a physical protection standpoint. From a hardware standpoint, small plants (such as molten salt reactors) will be in general easier to protect, in that there will be fewer systems, structures and components that need surveillance and fewer vulnerabilities.

The IAEA proposes a consequence-based protection approach against sabotage, referred to as a *graded approach*. The current graded approach to sabotage protection and requirements can be adapted for ARs, reflecting their strengths and vulnerabilities. The best security asset of many ARs is that their inherently safe characteristics overlap with security, which in turn reduces the consequences of a sabotage. Sodium, lead and lead-bismuth fast reactors, and molten salt reactors lack pressurisation and water in their primary system, and the thermal margin to core meltdown in the case of liquid metals or fuel boiling, in the case of molten salt, is rather high. These features nearly eliminate the possibility of a hydrogen explosion or an overpressure explosion on the primary system, making the spread of radionuclides far from the installation rather unlikely, even if a sabotage is successful.

For instance, TRISO particles can keep structural integrity and remain leakproof at temperatures above 1800 °C. Moreover, there is no water in the primary system. These two features make reactors fuelled with TRISO particles less hazardous than LWRs in case of sabotage. Even if sabotage is successful, TRISO particles are unlikely to melt. Even if there is an explosion in the primary system, as long as the fuel remains inside the TRISO particles, there will be still three barriers between it and the outside, reducing the radiological consequences to humans and the environment.

Cost of Acquiring a Licence

In addition to devising physical protection systems, AR developers perceive the cost of being granted a licence as primary concern, according to WINS' research. This means that developers need decide carefully when proposing ways to optimise security arrangements without compromising either safety or security. This is made even more challenging as incorporating security features similar to those required by traditional nuclear power plants into the reactor design is not economic, primarily in terms of operation and maintenance costs. According to developers interviewed by WINS, the enhanced safety characteristics of ARs should form the basis for demonstrating risk-informed security requirements.

Automation

Furthermore, as far as AR developers are concerned, automation is a significant design goal. The automation in safety and security for structures, systems and components will make reactor operations more economical. Automation may reduce human error significantly and the potential for insider threats. Likewise, the inclusion of robotics technologies like drones can drive down security costs by reducing the number of security staff employees. Furthermore, advanced technologies could be deployed to improve the detection of threats.

During its research, WINS was able to map out the following various security challenges:

- **High-Assay Low-Enriched Uranium (HALEU) and the supply chain**. HALEU is fuel enriched between 5% and 20%. Some of the developers interviewed by WINS are concerned about the differentiation between LEU and HALEU. The description of HALEU has introduced confusion about its categorisation for the purposes of physical protection requirements.
- **Remote siting**. A significant number of the advanced reactor designs such as the heat pipe reactors are initially intended to be used at remote locations including offshore. However, difficult access to these remote sites can present security advantages and disadvantages. One of the issues with the remote siting is cyber or the ability to have effective response teams.
- **Transport**. There are some uncertainties about whether some reactor designs will transport fuel or whether the fuel will be transported separately, which will depend on the size and configuration of the core of the reactor. It is important for the designer to consider transport during the fuel cycle including during decommissioning.
- **Cybersecurity**. The approach taken to address cybersecurity is no different from the existing one for traditional LWRs while some new challenges may emerge due to the evolving threat. In essence, there is nothing particularly unique about ARs from a cyber perspective beyond the potential for remote siting. So, just like traditional LWR, designers will need to identify cybersecurity considerations from inception to decommissioning.

SECURITY BY DESIGN FOR ADVANCED REACTORS

As mentioned earlier, *security by design* is based on the concept that security should play an integral role in the design process from the onset. It is a risk-informed approach that requires a clear security strategy and a commitment to make security a primary design consideration on par with nuclear safety. It also requires a coordinated approach by all parties including operators, project managers and regulators.

Some of the key principles of security include deter, deny, detect and delay. We can further add design to these principles. When these principles are incorporated into the design of a nuclear facility, they can reduce the risk of a major security incident. Although initial design costs may be higher, security by design will help to reduce the costs of preventing a nuclear security incident, and the savings will accumulate over the life of the advanced reactor. Developing a comprehensive approach to security by design requires implementation of the following steps:

- **Set Up Your Organisation**: Security by design can only work if your organisation is set up to deliver it. This means all stakeholders—from the chief executive down—must view security as an integral part of the organisation.
- **Understand the Threats and Consequences**: Security by design requires that you understand the postulated threats your advanced reactor facility could face, including both unauthorised removal of material and sabotage.
- **Establish Your Design Objectives**: Your security design should be based on the possible threats against your facility and the resources you have to manage them.
- **Develop Your Protection Model**: Many different design solutions are available to meet your security objectives. The ones you choose will depend on what you are protecting, their status, the nature of the threat and the resources that are available.

The WINS Special Report recommends three comprehensive methodologies and provides detailed security by design guidance to developers. While WINS recognises other methodologies exist, the following three are a starting point:

1.) The Security by Design Handbook by Sandia National Laboratories *(SNL)*

This handbook describes an approach to 'security by design,' beginning with a strategy to achieve it, and then showing how that strategy can be implemented. Although the handbook is mainly aimed at decision makers, advisors, and senior managers working in a country interested in developing nuclear power, it is also useful for operator organisations so that they can better grasp their part to play in support 'security by design.'

2.) *Secure by Design* guidance document developed by Adrian Prior and Robert Barnes in the UK

This provides guidance for security practitioners in the UK civil nuclear sector to apply the secure by design principles. According to this guidance document, a successful approach should encourage efforts to reduce security risk at source before taking into consideration the effect of a security protection system; adopt a system-level approach to designing nuclear security systems; engineer security functionality features into the design of a facility, plant or process; encompass the facility's entire lifecycle.

3.) Evaluation Methodology developed by the Gen IV Proliferation Resistance and Physical Protection Working Group

This methodology identifies a set of challenges, analyses a system response to these challenges, and assesses outcomes for a proposed design. The challenges are the threats that potential actors (proliferant States or sub-state adversaries) pose. The characteristics of advanced reactor systems (both technical and institutional) are used to evaluate the system's response and further determine its resistance against threats of proliferation and robustness against sabotage and terrorism threats.

CONCLUSIONS

To conclude, the emergence of ARs has noteworthy potential to provide energy in numerous countries. The reduction in costs, maintenance and ease of operations are strong incentives to use ARs in a wide range of environments and geographical locations. ARs are inherently safer than commercial nuclear power plants in operation, could be located closer to densely populated areas, and effectively provide energy where needs are. Moreover, due to their flexibility, ARs could play a key role in the emerging decentralised power supply energy market by providing clean, safe, competitive and reliable energy while protecting the environment.

The purpose of the WINS Special Report on the *Security of Advanced Reactors* is to outline security implications associated with these new technologies. Security implications need to be identified and addressed as early as possible, as design and technological choices will impact the risk picture and might require evolution in the regulatory approach. Taking nuclear security into consideration from an early stage of the design process will support the acceptance and successful implementation of this new technology.

ACKNOWLEDGEMENTS

WINS acknowledges the generous sponsorship of the Nuclear Threat Initiative (NTI) for the preparation of the Special Report on *Security of Advanced Reactors* and its promotion. WINS is grateful to all subject matter experts who participated at the international workshops in Vienna (March 2019) and Ottawa (2020). These events formed the foundation of the Special Report. WINS acknowledges all the distinguished experts and organisations, including advanced reactor developers, who contributed to the development of the Special Report through workshops, technical meetings, interviews and peer review. Please note that the views and opinions expressed in the Special Report and this paper are those of WINS and do not necessarily reflect the views and opinions of those experts and organisations who were consulted during the writing of the Special Report and this paper.

REFERENCES

American National Standards Institute. 2020. N290.7-14 - *Cyber Security for Nuclear Power Plants and Small Reactor Facilities*. Retrieved from https://webstore.ansi.org/standards/csa/csan2902014

Bari, B., Whitlock, J., Therios, I., Peterson, P. 2012. *Proliferation Resistance and Physical Protection Working Group: Methodology and applications*.

Barnes, Robert A. 2020. *Secure by design – Guidance document principles and methods*. Rolls Royce Civil Nuclear UK.

Buongiorno, J., Shirvan, K., Baglietto, E. , Forsberg, C., Driscoll, M., Einstein, H., Macdonald, I., Stewart, W. R., Velez-Lopez, E., Johnston, K., Hashimoto, G. 31 March 2020. *Japan's Next Nuclear Energy System (JNext): Final Report*. Center for Advanced Nuclear Energy Systems (CANES).

Congressional Research Service. 2019. *Advanced nuclear reactors: Technology overview and current issues*.

Dhal, F. 2020. *Director General Grossi outlines plans to 'recalibrate' IAEA*. IAEA Office of Public Information and Communication.

Generation IV International Forum:

- (2011). *Evaluation methodology for proliferation resistance and physical protection of Generation IV nuclear energy systems*, Revision 6.
- (2011). *Proliferation resistance and physical protection of the six Generation IV nuclear energy systems*.
- (2009). *PR&PP evaluation: ESFR full system case study final report*.

Global Nexus Initiative. 2019. *Advancing nuclear innovation: Responding to climate change and strengthening global security*.

Grant Buster, Michael Laufer and Per Peterson. 2015. *Fracture Analysis of Reduced Diameter Spherical Graphite Fuel Elements under Diametrical Loading Conditions*.

International Atomic Energy Agency:

- INFCIRC/274/Rev.1/Mod.1: Amendment to the Convention on the Physical Protection of Nuclear Material
- *INPRO manual: Physical protection*. International Project on Innovative Nuclear

- NSS No. 13. (2011). *Nuclear security recommendations on physical protection of nuclear material and nuclear facilities*.
- NSS No. 27G. (2018). *Physical protection of nuclear material and nuclear facilities*.

OECD Nuclear Energy Agency. 2017. *The strategic plan of the Nuclear Energy Agency 2017-2022*. Organisation for Economic Co-operation and Development.

OECD Nuclear Energy Agency. 2004. *Stakeholder involvement techniques: A short guide and annotated bibliography*. Organisation for Economic Co-operation and Development.

Prior, A. and Barnes, R. 15-19 March 2020. *Nuclear security and safety – Secure by design*. Proceedings of ICAPP.

Sandia National Laboratories. 2013. *Security-by-design handbook*.

Sambuu, Odmaa & Obara, Toru. 2014. *Comparative study on HTGR design for passive decay heat removal*. Progress in Nuclear Energy. 82. 10.1016/j.pnucene.2014.07.013.

Office of Nuclear Energy. 2018. *What is a nuclear microreactor*? US Department of Energy. Retrieved from: www.energy.gov/ne/articles/what-nuclear-microreactor

US Nuclear Regulatory Commission:

- (2020). *Aurora – Oklo application*. www.nrc.gov/reactors/new-reactors/col/aurora-oklo.html
- (2020). *Emergency preparedness for small modular reactors and other new technologies*.
- NRC-2017-0227 (2019). *Rulemaking for physical security for advanced reactors.*
- (2 April 2020). *Advanced reactor stakeholder public meeting.*
- SRM-SECY-18-0076. (2018). *Options and recommendation for physical security for advanced reactors - Rulemaking plan*.

World Institute for Nuclear Security. 2014. BPG 4.1 *Implementing security by design at nuclear facilities*. Version 2.1.

World Institute for Nuclear Security. 20-21 November 2019. *Workshop report: Security of small modular reactors*.