

Small Modular Reactors and Advanced Reactor Security: Regulatory Perspectives on Integrating Physical and Cyber Security by Design to protect against malicious acts and evolving threats

How can future nuclear technologies and Small Modular Reactors (SMRs) deter and prevent organized crime groups, terrorists and malicious actors from attempting to steal or sabotage nuclear materials and facilities. This paper present the benefits of integrating Security By Design (SeBD) in regulatory frameworks to allow more flexible and effective design of physical protection systems for new SMRs. Under its effort to modernise the Nuclear Security Regulations, the Canadian Nuclear Safety Commission (CNSC) regulatory approach plays a key role in recognising the importance of SeBD in moving toward a performance based approach with less prescriptive requirements. CNSC also recognises the need for a graded approach using a risk informed criteria for nuclear security. As part of SMR Vendor Design Review process, CNSC reviews SeBD and interfaces with safety (robustness), safeguards (Nuclear Material Accounting and Control), operation and sustainability. CNSC also recognize the need to share relevant nuclear sensitive information from the national Design Basis Threat (DBT) with SMR designers so they can consider credible and future threats in their design. Finally, the interfaces between nuclear security and system engineer specialists within the VDR process allows to look at both physical and cyber security systems in a more holistic approach. This allows the regulator to look at how SMR developers intends to optimize nuclear safety to mitigate against potential acts of sabotage.

SeBD offers opportunities to reduce costs for new nuclear facilities. However, it is not a “silver bullet”. SeBD needs to be integrated as part of an overall security strategy taking into consideration the security policies, the facility characteristics, the material used and the national threat/DBT. In addition, there are outstanding security challenges to address such as: remote facilities without effective and timely off-site response capabilities, the intent of building unmanned facilities, the increase cyber security risks with the over reliance on digital technologies, the use of lethal force by autonomous and remotely operated security systems or protecting floating SMRs. These SMR designs are for future use, but now is the time to address some of theses ethical questions that may shape the reality of future generations.

Gender

Male

State

Canada

Primary author: Mr DUGUAY, Raphael (CNSC)

Presenter: Mr DUGUAY, Raphael (CNSC)

Track Classification: PP: Nuclear security of new nuclear technologies (e.g., small modular reactors)