SAND2021-9200PE

Security Considerations for SMRs and Advanced Reactors

FIRST Capacity-Building Webinar Series

Session 4: Nuclear Security for SMRs

Doug Osborn Ph.D.
Sandia National Laboratories

Pratap Sadasivan Ph.D.
Senior Technical Advisor, NNSA Office of International Nuclear Security

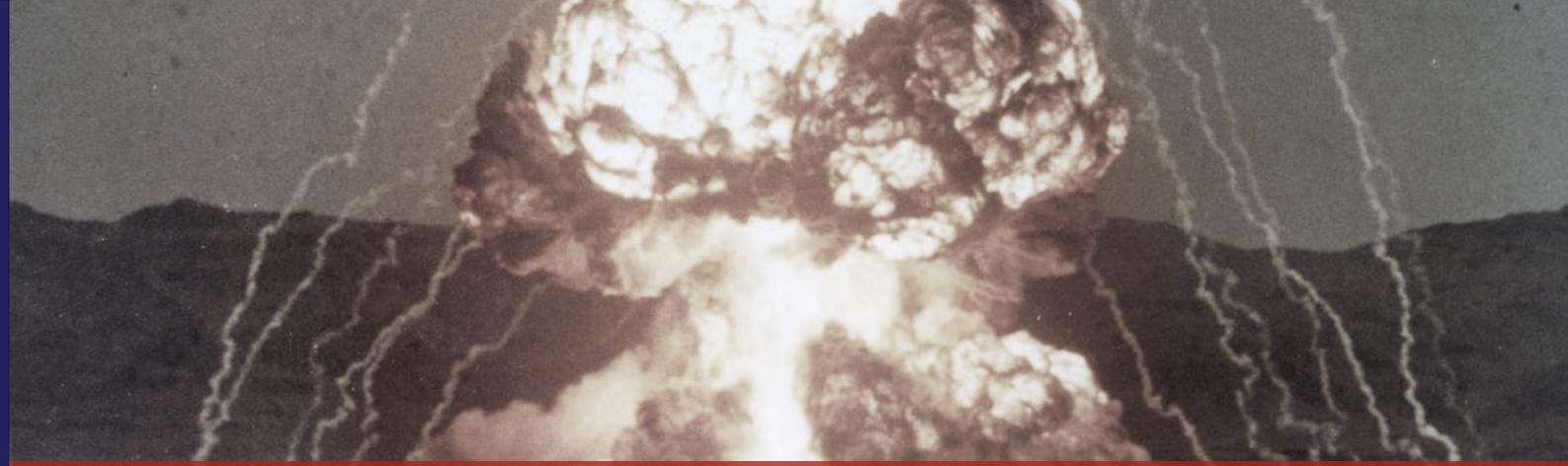
August 18, 2021

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2021-XXXX-PE

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

What is nuclear security?

"prevention and detection of, and response to, theft, sabotage…or other malicious acts involving nuclear material…or their associated facilities" [IAEA]



Theft followed by construction and use of a threat device can create catastrophic loss

Sabotage can lead to loss of life, deep economic damage, and societal disruption

Direct Sabotage – direct damage to the reactor or spent fuel
Indirect Sabotage – attacks on non-reactor elements of the system to cause a reactor incident

Used by permission from TEPCO; Kenji Tetawa

INS International Nuclear Security
Reducing Risk of Nuclear Terrorism

Sabotage threat is real

An employee planted four bombs at the Koeberg nuclear power plant (1982) during construction resulting in significant delays in opening of the plant

(2014) Turbine sabotage took Doel 4 reactor offline for months – insider suspected

(2016) Suspected terrorists in the Brussels airports and metro attacks may have considered attacking nuclear plant

Suspected Al Qaeda operative (2010) had worked at multiple U.S. nuclear plants

Sabotage at any facility can have local and global consequences

Types of consequences

- **Radiological**
- **Environmental**
- **Economic**
- **Sociopolitical**

Any scenario internationally resulting in a radiological release is likely to affect public and government confidence

While radiological and environmental consequences may be limited in area, economic and socio-political consequences are global in nature – including erosion of confidence in nuclear energy

INS Sabotage Mitigation Objectives

Per Amendment to the Convention on the Physical Protection of Nuclear Material and supported by IAEA's NSS No. 13

- Protect against unauthorized removal of nuclear material in use, storage, and transport
- Ensure implementation of rapid and comprehensive measures to locate and recover lost or stolen material
- Protect nuclear material and facilities against sabotage
- Mitigate or minimize the radiological consequences of sabotage

Sabotage Targets

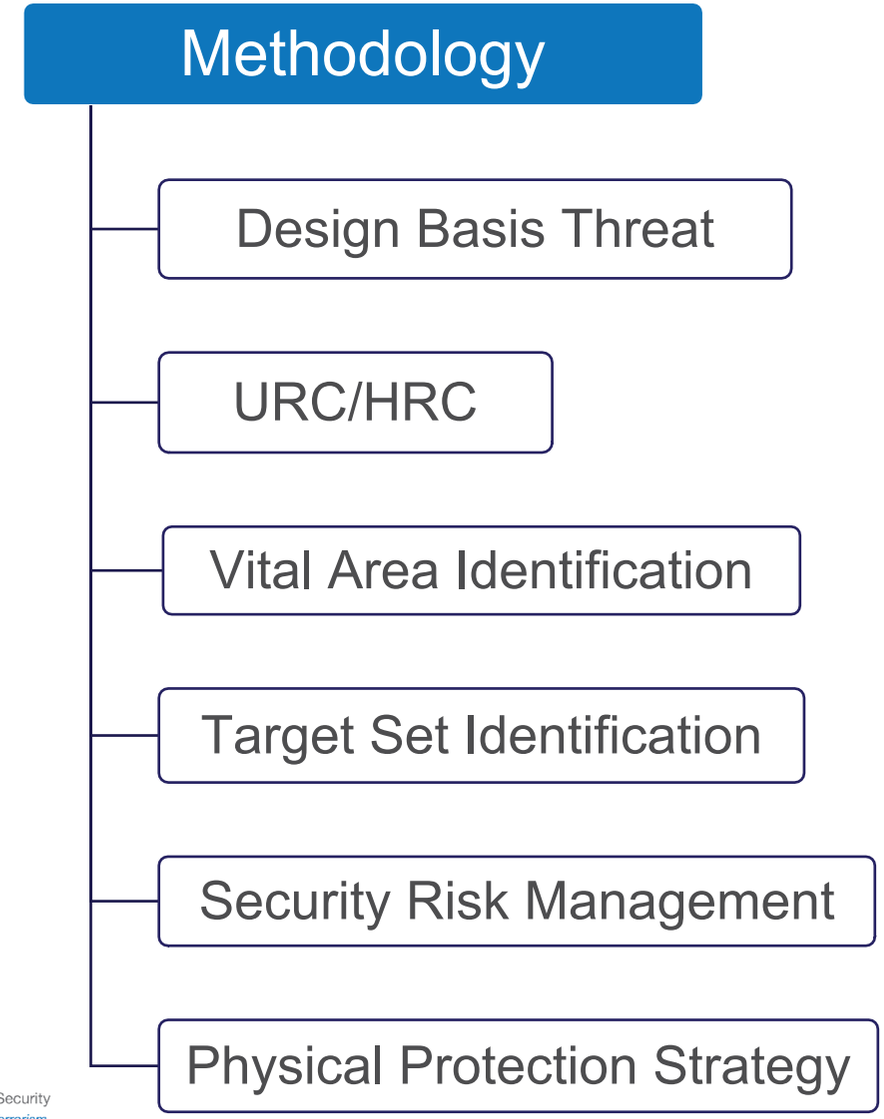
- Nuclear or other radioactive materials
- Process or support equipment needed to prevent unacceptable radiological consequences

NSS No. 13 specifies Physical Protection Strategy (PPS) should protect against unacceptable radiological consequences (URC) and high radiological consequences (HRC)

- State is responsible for identifying what constitutes URC and HRC

PPS should protect against any sabotage scenarios that exceed URC thresholds (*graded approach*)

INS Sabotage Mitigation Capabilities



Variances in SMR facility types requires a dynamic suite of methods, tools, and subject matter experts

International partnerships can focus on;

- Training and Workshops,
- Tool and Methodology Development,
- R&D and Capacity Building

Advancements in SMR design require new suite of tools and methods

- Dynamic PSA for Vital Area Identification

System Design Aspects – Examples for SMRs
Have an impact on Vital Areas and Target Sets for Sabotage

Fuel
Coolant
Decay heat removal
Size
Power Conversion
Reactivity Control
Lifetime/Refueling cycle
Cooling System Location

Cooling Water
Siting (Grade, Remote)
Redundant safety equipment
Passive Safety
Factory Fabrication
Autonomous/ remote operations

Security Implications of SMR Design Aspects (1/4)

Aspect	Security Considerations - Examples
Fuel	• Changes in likelihood of theft attempt, impacts protection strategy • New NMAC approaches may need to be developed • Possibility for protracted diversion at a bulk facility.
Coolant	**Additional (potentially new or unanticipated) sabotage, theft, or diversion pathways**
Decay heat removal	Additional (potentially new or unanticipated) sabotage pathways
Size	Increased numbers of ARs → Increased accessibility → more opportunities for unauthorized access → higher likelihood of sabotage/theft*
Power Conversion	Potentially new or unanticipated sabotage pathways
Reactivity Control	(potentially new or unanticipated) sabotage pathways Including sabotage of secondary

Security Implications of SMR Design Aspects (2/4)

Aspect	Security Considerations - Examples
Lifetime/ Refueling Cycle	• **More difficult access → reduces likelihood of sabotage or theft attempt** • **Fresh fuel storage on-site?** • **Less frequent refuels → fewer opportunities to access nuclear material.**
Cooling System Location	More difficult access → reduces likelihood of sabotage or theft attempt
Cooling Water	Increasingly remote use locations → increasing challenges to detection & response capabilities

Security Implications of SMR Design Aspects (3/4)

Aspect	Security Considerations - Examples
Siting - Below Grade	• Generally makes the reactor more secure against intruders but may impede security response in a barricading scenario. • Easier to protect against plane impacts and stand-off weapons, but this advantage is reduced to the extent that vital safety equipment is located above the aircraft/missile shield. • Provides an extra barrier to the dispersion of radioactive material in the event of a successful sabotage attack
Siting - Remote Location	• Complicates access to the site. • Security force may have more time to respond/recover.

Security Implications of SMR Design Aspects (4/4)

Aspect	Security Considerations - Examples
Redundant safety equipment/ separation	• Would complicate planning of an attack and likely lower the probability of success. • Fewer areas need protection because most of the vital safety equipment is within the reactor vessel with minimal penetrations.
Passive Safety	**Greater use of passive safety features, including natural circulation, may offer advantages in specific sabotage scenarios. However, this must be evaluated on a case-by-case basis.**
Factory Fabrication	• Added security-by-design passive delay features and ‘kill zones’
Autonomous/ remote operations	The use of autonomous systems will have implications for cyber security and new pathways to sabotage.

Addressing Security Implications – SMR Examples (1/2)

Aspect	Implications for Security	Example Security Analysis/Assessments
Fuel	• Changes in likelihood of theft attempt, impacts protection strategy • New NMAC approaches may need to be developed • Possibility for protracted diversion at a bulk facility.	Fresh/Core/SNF asset characterization Attractiveness Potential release fraction from sabotage
Coolant	**Additional (potentially new or unanticipated) sabotage, theft, or diversion pathways**	**Vital Areas and Sabotage Targets** **Adversary Path Analysis** **Protection Strategy and Economics**
Decay heat removal	**Additional (potentially new or unanticipated) sabotage pathways**	
Size	**Increased numbers of ARs → Increased accessibility → more opportunities for unauthorized access → higher likelihood of sabotage/theft***	

Addressing Security Implications – SMR Examples (2/2)

Aspect	Implications for Security	Example Security Analysis/Assessments
Power Conversion	Potentially new or unanticipated sabotage pathways	Non-radiological consequences
Reactivity Control	**(potentially new or unanticipated) sabotage pathways Including sabotage of secondary**	**Adversary path analysis** **Potential release fraction from sabotage**
Factory Fabrication	• Added security-by-design passive delay features and 'kill zones'	Transport Security Assessment
Autonomous/ remote operations	The use of autonomous systems will have implications for cyber security and new pathways to sabotage.	Cyber-security assessment

Security-By-Design

Includes protection-related thinking earlier into the design process

- If applicable, address security during design of the reactor system
- When procuring from suppliers;
  - Address security during procurement process to ensure security is appropriately built into the design
  - *Address security during design of the facility*
    - Local factors drive many security aspects
    - For example, local economic factors drive security technology costs and personnel and response force costs

Potential Collaboration Areas

- Sabotage Analysis Approaches and Tools
- Threat Assessment/Design Basis Threat
- Security By Design of Facilities
- Design of Physical Protection Systems – approaches and tools
- Security Economic Evaluations

National Nuclear Security Administration

Questions

INS International Nuclear Security
Reducing Risk of Nuclear Terrorism