SAND2022-13222C

National Nuclear Security Administration

United States
Department of Energy
National Nuclear Security Administration
International Nuclear Security

Nuclear Safety and Nuclear Security Interface Workshop

Vienna, Austria, October 2022

Riyaz Natha
Sandia National Laboratories

SAND2021-0176 TR

INS
International Nuclear Security
Reducing Risk of Nuclear Terrorism

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.

Relationship Between Plans

Security Plan

Primary documentation describing physical protection system and intended to meet the requirements specified by the competent authority

– NSS No.27-G

Contingency Plan

Predefined sets of actions for response to unauthorized acts indicative of attempted unauthorized removal or sabotage, including threats thereof, designed to effectively counter such acts

– NSS No.13

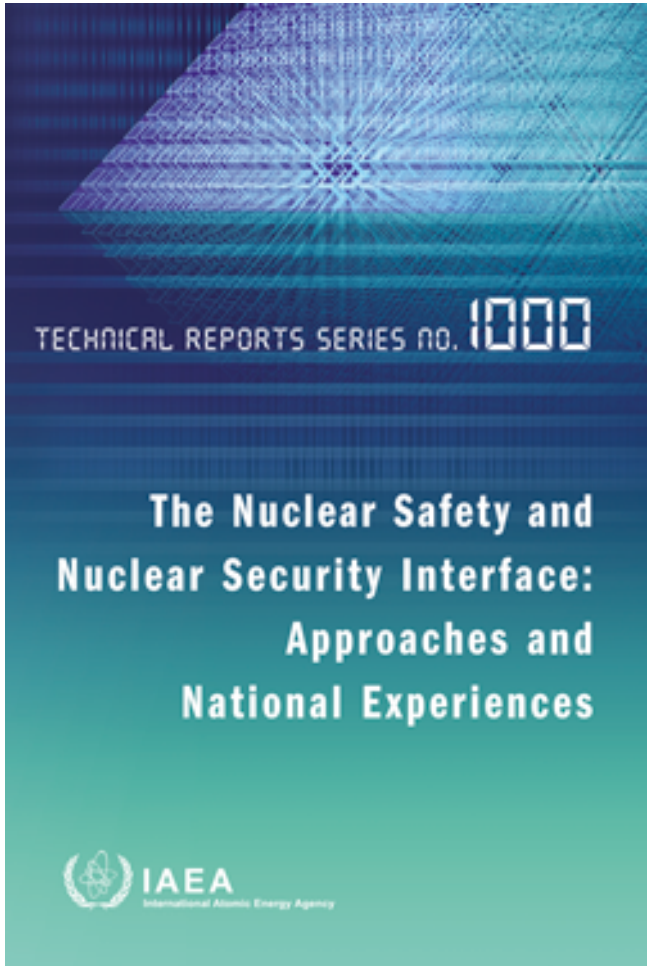
Emergency Plan

Describes preparedness and response to a nuclear or radiological emergency

– IAEA General Safety Requirements Part 7

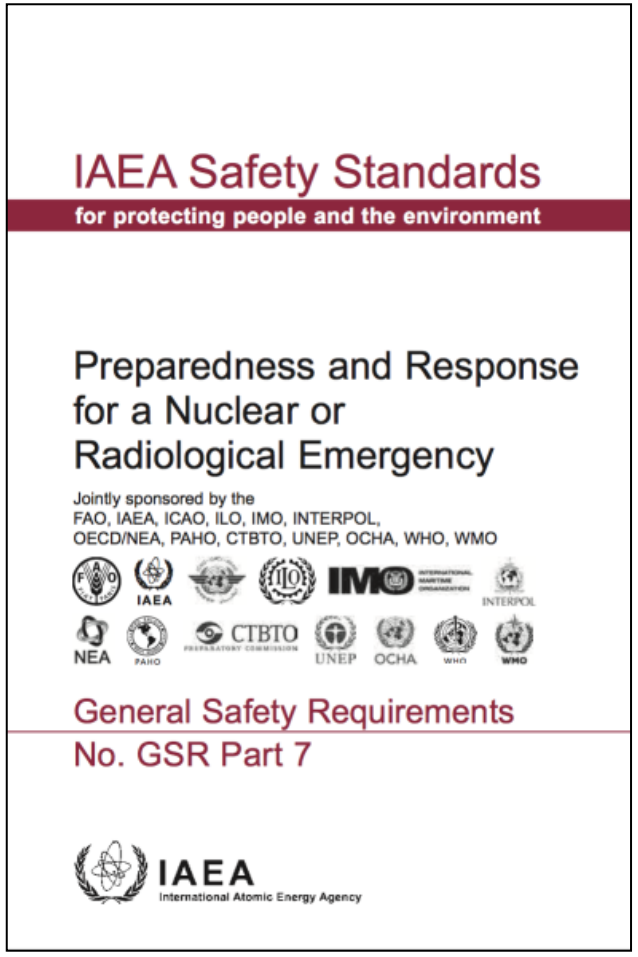
IAEA Guidance

- The Nuclear Safety and Nuclear Security Interface: Approaches and National Experiences
  - 2021, Technical Report Series No. 1000
- This publication “aims to provide a better understanding of the important elements of the interface between nuclear safety and nuclear security for facilities and activities and to highlight the challenges, opportunities and good practices for its effective management when planning and implementing different programmes and activities.”



Goals of Emergency Response (GSR Part 7)

- The government shall ensure that plans and procedures necessary for effective response to a nuclear or radiological emergency are established
- Regain control of the situation and mitigate consequences
- Avoid or minimize severe deterministic effects
- Render first aid, provide critical medical treatment, manage treatment of radiation injuries
- Reduce risk of stochastic effects (e.g., carcinogenesis)
- Keep public informed and maintain public trust
- To the extent practicable:
  - Mitigate non-radiological consequences
  - Protect property and the environment
  - Prepare for the resumption of normal social and economic activity



Contingency and Emergency Planning

Unauthorized Acts (Contingency Plan)	Safety / Emergency Events (Emergency Plan)
• Loss of nuclear material • Potential sabotage attempts, human-caused accidents • Discovery of insider threats • Unauthorized intrusions • External threats (e.g., bomb warning) • Stand-off attacks • Airborne, waterborne attacks • Cyberattacks • Compromise of sensitive information	• Natural disasters: earthquakes, flooding, hurricanes • Human-caused accidents • Critical equipment malfunction or failures • Medical emergencies

Security-Safety Interface

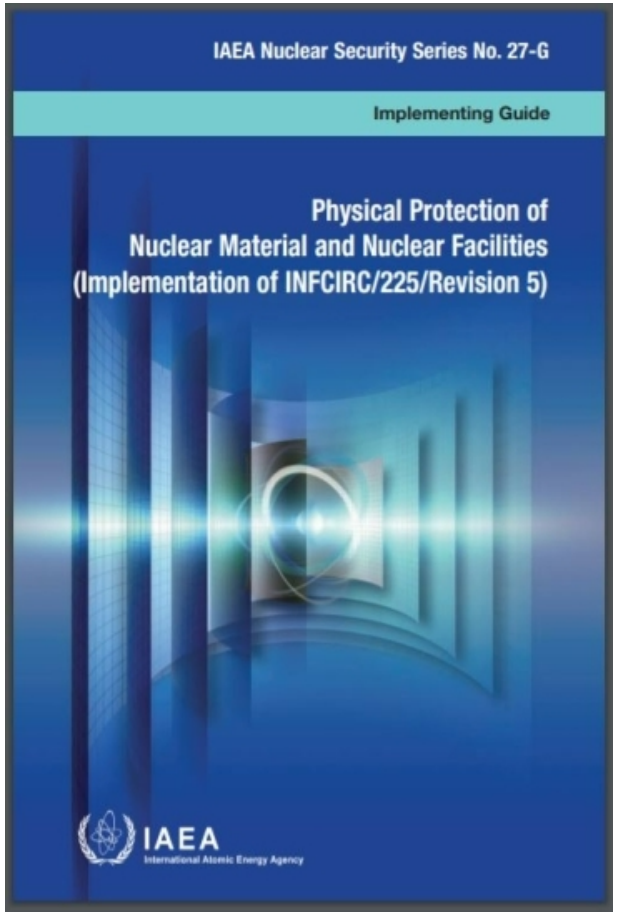
- Although nuclear security and safety share a common objective, some measures in each area might be points of potential conflict:

Security	Safety
Minimize access points	Allow for emergency egress
Maintain confidentiality of security information	Disseminate safety requirements for transparency

- Designers and Operators should be careful to ensure that security measures do not compromise safety and that safety measures do not compromise security
- Safety and security plans should be mutually supportive

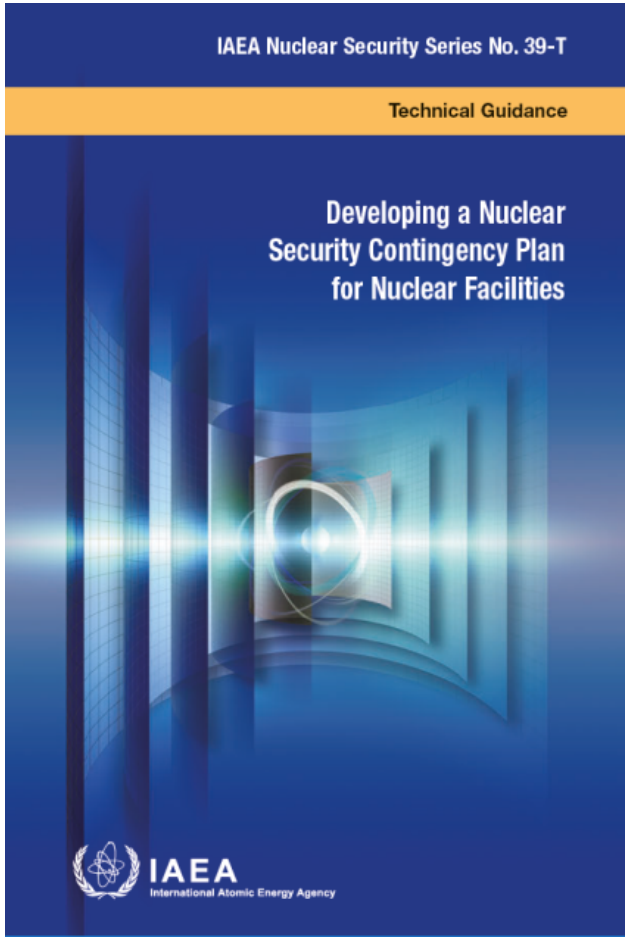
Security Plan

- Important throughout the lifecycle of a nuclear facility
- The Operator should prepare a security plan as part of the application to obtain a license
  - Should be based on the DBT
- The Competent Authority reviews and approves it as part of licensing conditions
- The Operator should implement the approved security plan
- Reviewed and updated periodically
  - Changes should be approved by the Competent Authority
- The Competent Authority should verify the Operator's compliance with the security plan
- Contains sensitive information



Contingency Plan

- Part of the Security Plan
- The objective is to guide a systematic, coordinated, and effective response to security incidents
  - Prevent attempted unauthorized removal or sabotage of nuclear material or facilities
  - Locate and recover missing nuclear material
  - Mitigate or minimize the effects of sabotage
    - Regain control of the facility
    - Secure the facility during mitigation and recovery operations, protect emergency equipment and personnel
    - Prevent further damage



Contingency Plan

- Two levels of contingency plan should be established:
  - State's contingency plan
  - Operator's contingency plan
  - These plans should complement each other
- The State should ensure that:
  - Operators and appropriate State response organizations conduct exercises to assess and validate the contingency plans
  - Various stakeholders are trained in how to react in such situations (NSS No.13)

Other Plans, Documents

The following could be appendices, separate documents, or incorporated into other plans:

- Insider threat
- Tactical plans
- Compensatory measures
- Safeguards agreements
- Memoranda of understanding (MOU)
- Evacuation plans
- Protests, labor strikes – contingency plans
- Others?

Safety-Security Interface Scenario #1

- There is a report of a building on fire
  - How do we know if this is a safety or security issue?
  - How do we respond during the emergency call?
  - Safety and security personnel on the call?
  - Who responds to the site?
  - How do you respond to multiple fires?
  - Is this possibly a diversion scenario?
  - How do you prioritize fire alarms and security alarms in the CAS or SAS?
  - What compensatory measures are noted and activated?

Safety-Security Interface Scenario #2

- Ambulance or fire truck entering the site or part of the facility
  - During these emergencies, time is critical
  - Are these vehicles onsite or offsite?
  - How many emergency vehicles do we expect to respond?
  - Are there plans in place for this scenario?
  - Do we know that this is a first responder or an adversary?
  - Have we considered communication before they arrive?
  - Can we have an escort vehicle enter and follow them?
  - What compensatory measures are noted and activated?

Safety-Security Interface Scenario #3

- A fire alarm is triggered
  - Which emergency doors are activated?
  - Are cameras and sensors recording information for future review?
  - Where do people muster?
  - Do we consider safety weather patterns in the security response?
  - How do we ensure that material and documents are accounted for?
  - Are potential adversaries being considered during the response?
  - Is there an insider/outsider collusion scenario?
  - When is it safe to re-enter facility?

Safety-Security Interface Considerations

- There can be numerous scenarios in which these interfaces could occur
- Communication between safety and security personnel is critical, especially in facilities where these organizations are in different departments
- Integrating experts from NMAC provides additional information on response actions
- Tabletop exercises and performance testing are critical
- Understanding the threat and respective DBT is a key component of adversaries' capabilities
- Joint testing of contingency, emergency, and security plans with all site personnel and any offsite personnel who might respond to potential events
- Licensee/Competent Authority cooperation on document review and testing