Interface between Safety and Security for Research Reactors

A. M. Shokr

RRSS/NSNI/IAEA

Outlines

- Introduction
- Similarities, differences, and potential conflicts:
  - *Management of nuclear safety and security*
    - Legislative and regulatory framework
    - Responsibilities
    - Management system
  - *Maximization of synergy between safety and security*
    - Design concepts and criteria
    - Operating principles
    - Emergency response
    - Use of a graded approach
- Safety-security interface challenges
- Concluding remarks

Introduction

- **Nuclear Safety:** “The achievement of proper operating conditions, prevention of accidents or mitigation of accident consequences, resulting in protection of workers, the public and the environment from undue radiation hazards”

- **Nuclear Security**: “The prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear materials, other radioactive substances, or their associated facilities”

Introduction

- Nuclear Safety: Main concerns are radiological risk to human and environment, whatever the cause. For research reactors causes could be human errors, equipment failure, internal events (fire, pipe break, etc.) and external events (earthquakes, flooding, etc.).

- Nuclear Security: Main concerns are theft of nuclear and other radioactive material and radiological sabotage of a nuclear facility or nuclear material. For research reactors high risk targets are HEU fuel (theft) and sabotage of large inventories of fission and activation products.

Introduction

- Nuclear safety and nuclear security share the same over all objective: To protect people and environment form radiological hazards.

- The acceptable risk should be the same whether the initiating event of a radiological release is due to human and equipment failures, internal and external events or an event of malicious origin.

Introduction: Why interfacing?

The workers, public, and environment are subjected to threats arising from both safety and security related hazards.

A more effective protection of people and the environment can be achieved through a proper interface of both nuclear safety and nuclear security.

Introduction – Why interfacing?

Nuclear safety is necessary, but cannot protect on its own, nuclear or other radioactive material from un-authorised access, theft, diversion, sabotage, or other malicious acts.

Similarly, nuclear security is necessary, but not sufficient on its own to protect people or environment from an accident.

Introduction: Why interfacing?

Some nuclear safety issues have no security implications (e.g. reactor pool tank operating conditions).

Some security issues have no safety implications (e.g. theft of intellectual property).

But, most issues are not mutually exclusive.

An effective safety and security interface approach reduces risk.

Introduction: Why interfacing?

Safety and security: Reinforcement of one another:

In most situations ➔ elements or actions in one area also enhances the other area.

Confinement building serves to prevent a significant release of radioactive material to the environment in accident conditions (safety), it also provides a robust structure that protects the reactor from a terrorist attack (security).

OPAL Research Reactor building (ANSTO-Australia)

Interface between safety and security: Similarities, differences and potential conflicts

Management of nuclear safety and security

Legislative and regulatory framework

- Legislative and regulatory framework: To ensure oversight of installations and activities of potential radiological risk and require security provisions. The regulatory body should be effectively independent and should be able to:
  - *Authorize facilities and activities;*
  - *Perform review and assessment of safety and security submittals;*
  - *Establish and implement regulatory inspection programmes;*
  - *Enforce the regulations.*
- The regulatory body may be the same but nuclear safety and nuclear security are subjected to different regulations.
- Coordination is required for safety and security inspections. If there two or more organizations regulating safety and security, more coordination efforts are likely required.

Prime responsibility on safety and security

- The prime responsibility for nuclear safety rests with the operator. This responsibility can not be delegated. Operating organizations are also responsible for security.
- The involvement of the State is more broader and larger in security than safety:
  - *The operator usually can't ensure alone the protection of the site and installation;*
  - *Direct involvement of the State in the assessment of threats. The threats are evolving, and the State and operator should ensure that the security measures are adequate to the threat level;*
  - *Management of crisis associated with a security event requires involvement of more State bodies compared to safety.*

Integrated management system

- A single and coherent system in which all the parts of an organization are integrated to enable achieving its objectives.
  - The system should bring safety and security at the same level.
  - Functional categories (management responsibility, resources management, process implementation and improvements) are the same. However, the processes are specific.

Integrated management system

- The management system should be aimed at establishing strong safety culture and strong security culture, which are of similar attributes and subjected to similar requirements:
  - *Safety Culture: Transparency and openness, and sharing information are essential;*
  - *Security Culture: Confidentiality (information communicated only with authorized personnel);*
  - *Both cultures should not oppose each other and should mutually reinforce one another.*
  - *Both cultures should not be merged in a single one.*

Maximizing the synergy between safety and security

Interfacing of safety and security should be considered in all stages of the research reactor lifetime

- Design: Design concepts and criteria
- Operation: Operating principles
- Emergency planning: Emergency repose
- Use of a graded approach

Design concepts and criteria

- *Defence-in-Depth (DID) concept applies for both nuclear safety and nuclear security.*

- *Application of the DID is slightly different for security than safety: Barriers are established to prevent risk of accident or delay malicious act.*

- *Design Basis Accident (DBA) for safety - Design of safety systems;*

- *Design Basis Threat (DBT) for security – Design of physical protection system.*

Design concepts and criteria

– *Design for safety of research reactors reinforces the efficiency of protection against malicious acts.*

  - Single failure criterion;
  - Redundancy and diversity;
  - Physical separation;
  - Fail-safe criterion.

– *Application of these criteria means that aggressors must compromise several targets in order to cause radiological release.*

Design concepts and criteria

Safety design	Security advantage
Use of passive systems	Makes it more difficult for potential adversaries to tamper with safety systems
Introduction of robustness against human errors	Serves to increase protection against an insider threat
Doors or barriers for radiation protection purposes	Serves a security function by delaying or preventing unauthorized access
Safety specialists have knowledge of the potential consequences of the failures of equipment important to safety and control	Useful in helping security specialists to identify sensitive targets

Operating principles

- *Maintenance and periodic testing of equipment important to safety and security: Coordination is necessary so that compensatory measures do not undermine the necessary balance between safety and security (e.g. compromising security surveillance systems during maintenance operations should be avoided);*

- *Operating feedback experience: Much more limited in the security field.*

- *Periodic reviews: Ageing of facilities is a concern for nuclear safety and nuclear security. Examination of the status of the facility on periodical basis, which may results in the need for modernization or refurbishment, updating of procedures and documents, and revision of the safety analysis (including DBA) or the design basis threat.*

Operating principles

– *Operating procedures and access control: Should take into consideration the requirements for both safety and security:*

- Facilitated access is needed for emergency teams while it may be controlled for security purposes;
- Some areas within the rector facility may be subjected to special physical protection system while it should be possible to be accessed for evacuation of personnel in case of emergency;
- Experimenters at research reactors Vs access control for security purposes;
- Safety procedures in some cases may slowdown transport of materials, while the duration of transport should be minimized for security purposes.

Operating principles

Coordination is needed in developing the operating procedures. When conflicts are unavoidable, the matter should be resolved based on the philosophy of minimizing the risk to the operators and public.

Emergency response

- *The radiological emergency plan should address those events related to the facility and due to malicious acts;*

- *Contingency plan is upstream radiological emergency plan. It is designed to secure the site before any mitigation action is taken. For security, emergency response refers to those actions aimed at "reversing" the immediate consequences of unauthorized access or actions. Response to the radiological consequences that might occur is part of the radiological emergency plan;*

- *The two plans should be complementary and coherent, which should be tested during general (coordinated) emergency exercises.*

Use of a graded approach

- *Application of the safety requirements and security recommendations should commensurate with the potential hazard of the facility.*

- *It is applied to the nuclear safety requirements for siting, design, operation, utilization, modification, training and qualification, emergency preparedness, and regulatory supervision; and for security recommendations related to protection against sabotage and definition of the DBT.*

- *Parameters that are used in grading the application of requirements include power and source term, fuel design and handling, amount and enrichment of fissile materials, existence of high pressure or high energy piping, quality of means of confinement, siting and proximity to population*

Safety-Security Interface Challenges

- Inadequate regulatory guidance;
- Cultural differences;
- Traditional organizational separation;
- Lack of integration in the design process;
- Lack of adequate coordination during facility operation.

Concluding remarks

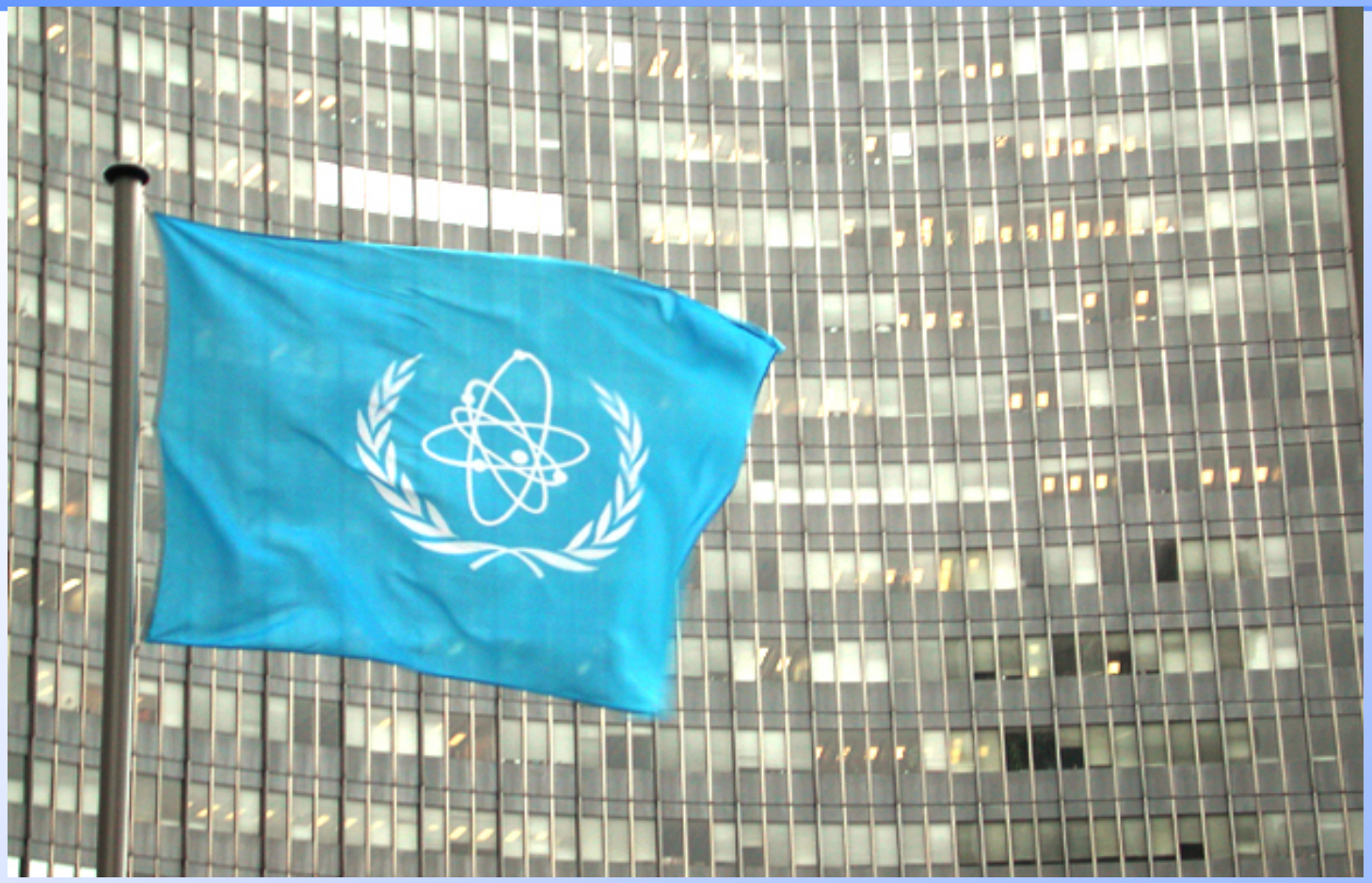
- There are more similarities than differences in the management of nuclear safety and nuclear security, including regulatory supervision, organizational aspects, design concepts and methods, operating principles, emergency prepardness, and use of a graded approach.

- Appropriate application of the design concepts and criteria for nuclear safety, and good operational safety practices will enhance the protection against sabotage.

Concluding remarks

- Safety culture and security culture should not be merged in one; and should not oppose each other and mutually reinforce one another.

- Specific attributes in some areas related to nuclear safety and nuclear security may lead to conflicts in the implementation of the relevant activities. This conflict should be managed by proper coordination of the methods and approaches, and operating practices through the research reactor lifetime.



…Thank you for your attention