IAEA 60 Years
Atoms for Peace and Development

Nuclear Security of Nuclear Facilities

INPRO Dialogue Forum
18-21 October 2016
Vienna

Muhammad Khaliq,
Section Head
Division of Nuclear Security
Department of Nuclear Safety and Security

Presentation Outline

- Risks and protection objectives
- Physical Protection Regime and its elements
- Security by Design
- Way forward

Associated Risks

- Risk of unauthorised removal with the intent to construct a nuclear explosive device
- Risk of unauthorised removal which could lead to subsequent dispersal
- Risk of Sabotage

Objectives of PP Regime

- To protect against unauthorized removal
- To locate and recover missing nuclear material
- To protect against sabotage
- To mitigate or minimize effects of sabotage

Physical Protection Regime

- The legislative and regulatory framework governing the physical protection of nuclear material and nuclear facilities
- The institutions and organizations within the State responsible for ensuring implementation of the legislative and regulatory framework
- Facility and transport physical protection systems

Elements of a PP Regime

A: State responsibility
B: Responsibilities during transport

C: Legislative / regulatory framework
D: Competent authority

E: Responsibility of license holder
F: Security culture

G: Consideration of threat
H: Graded approach

I: Defense in depth
J: Quality assurance

K: Contingency plans
L: Confidentiality

Security by Design

- Integrate design of PPS into overall design
- Identify all potential targets for unauthorized removal and sabotage
- Prior to construction, identify how physical protection will be implemented during all construction phases

Sabotage

INFCIRC/225/Rev. 5

Sabotage - “Any deliberate act directed against a nuclear facility or nuclear material in use, storage or transport which could directly or indirectly endanger the health and safety of personnel, the public or the environment by exposure to radiation or release of radioactive substances.”

Protecting Against Sabotage

IAEA 60 Years Atoms for Peace and Development

INFCIRC/225/Rev. 5, Sections 5.9 – 5.19

- PPS design should be based on the design basis threat or threat assessment
- Operator in cooperation with the competent authority should define credible sabotage scenarios for sabotage of the facility
- Sabotage scenarios should consider external and insider threats
- Stand-off attacks should be assessed if within the capability of the threat
- PPS design should take into account the robustness of engineered safety and operational features of the facility
- PPS design should take into account and be integrated with the measures for protection against theft
- Protection should be provided against attacks on computer based systems

Threat Assessment or DBT

- ***Threat Assessment:*** **An evaluation of the threats - based on available intelligence, law enforcement, and open source information - that describes the motivations, intentions, and capabilities of these threats**
- ***Design Basis Threat (DBT): the attributes and characteristics of potential insider and/or external adversaries, who might attempt unauthorized removal of nuclear material or sabotage, against which a physical protection system is designed and evaluated*.**
- **A DBT is "…*developed from an evaluation by the State of the threat of unauthorized removal and of sabotage.*"**
- **A DBT is a policy document used to establish performance criteria for a PPS. It is based on the results of threat assessments as well as other policy considerations**

Scenario Development

- **Purpose: To provide basis for confident evaluation of PPS performance**
- **Scenarios should be:**
  - **Credible**
  - **Internally consistent**
  - **Intellectually honest**
  - **Conservative**
  - **Transparent**
  - **Well documented, and**
  - **Useful (i.e. provide useful results)**
- **Develop details of realistic adversary attempt**
  - **Single adversary path, tasks and timeline**
  - **Performance of PPS against attack**

- **IMPORTANT: *Overall physical protection system effectiveness is represented by physical protection effectiveness for few specific scenarios***

Insider

- ***Insider:*** **Any individual with authorized access to *nuclear facilities* or *transport* who might attempt unauthorized removal or sabotage, or who could aid *outsiders* to do so**
- **Insiders might include, but are not limited to:**
  - **Management**
  - **Regular employees**
  - **Security personnel**
  - **Service providers**
  - **Visitors**
  - **Inspectors**
- **Insider Attributes**
  - **Authorized access to *nuclear facilities* or *transport* (from definition)**
  - **Authority**
  - **Knowledge**

Stand-off Attack

- **Stand-off Attack:** An attack, executed at a distance from the target nuclear facility or transport, which does not require adversary hands-on access to the target, or require the adversary to overcome the physical protection system
- **Should be considered if threat has a capability to perform a stand-off attack**

Computer Based Attacks

- Computer technology is used extensively in nuclear facilities for safety, operational and security functions
- Attacks on computer systems may compromise any of these functions
- Security requirements for computer systems are essential to protection against sabotage

Computer Security Threats

- Unauthorized access to information
- Interception and change of information, software, or hardware
- Blocking of data transmission or system shutdown
- Inserting false data in data communication or computer systems

How much safe is SAFE

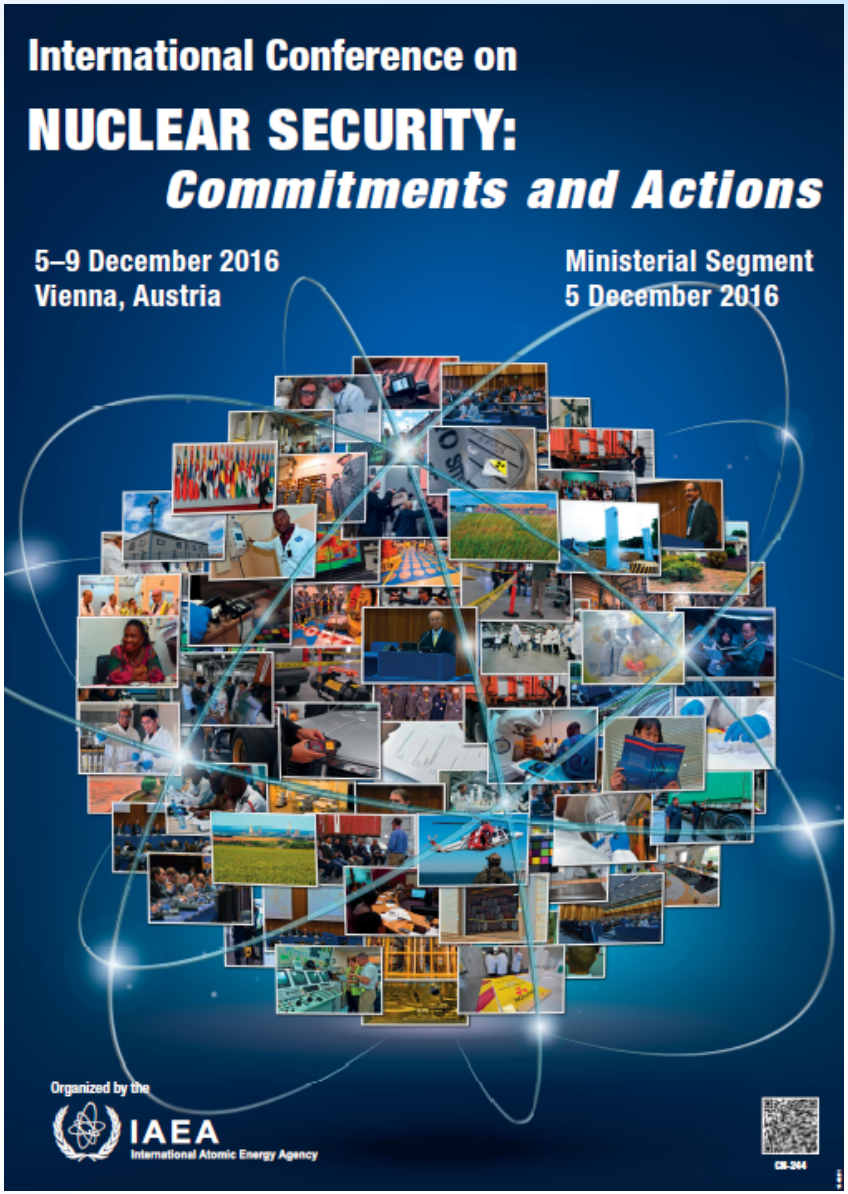
- Term “SAFE” may have different meaning when we discuss malicious acts instead of equipment failure, natural disaster, human error, and other common initiating events
- What is the value we must protect?
- To sustain this value, what assets must be protected? Why must they be protected? What happens if they're not protected?
- What potential adverse conditions and consequences must be prevented and managed? At what cost?
- How do we integrate our answers to these questions into an effective, implementable, enforceable security strategy and plan?

Conclusions

- Global deployment of SMR is a security challenge
- The protection against sabotage concept would be mostly affected
- The “security share” in overall construction and operational cost might be higher than for conventional NPPs
- Transport of SMR (either “fresh” and “used”) may also be challenging from security point of view

2016 International Nuclear Security Conference

- Will address all areas of nuclear security
- Ministerial Segment on 5 December
- High level sessions to look at policy issues
- >25 technical sessions on nuclear security topics



IAEA 60 Years
Atoms for Peace and Development

Thank you!