IAEA Guidance on Physical Protection and Security of SMR Facilities

Presentation to INPRO Dialogue Forum on SMR Nuclear Power Reactors

12 October 2011
### Physical Protection regime: Issues and Milestones

<table>
<thead>
<tr>
<th>Issues</th>
<th>Milestone 1</th>
<th>Milestone 2</th>
<th>Milestone 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>State Responsibility</td>
<td>Conditions</td>
<td>Conditions</td>
<td>Conditions</td>
</tr>
<tr>
<td>International Transport</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assignment of Physical Protection Responsibilities</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legislative and Regulatory Framework</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>International Cooperation and Assistance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identification and Assessment of Threat</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Based Physical Protection System and Measures</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sustaining the Physical Protection Regime</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Planning and Preparedness for Response to Nuclear Security Events</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SMR vs. large NPP Reactors: common and specific features

Commonalities for security consideration

- Large inventories of radionuclides (source term)
- Unacceptable radiological consequences of sabotage
- LEU or MOX fuel (potential theft targets)

Specific features for security consideration

- Sabotage target/ vital area locations
- SMRs without on-site refueling
- Longer refueling periods (several years)
- SMRs without spent fuel storages
- SMRs with fresh fuel of category 2 (LEU 10… 20%)
Specific features vs. security risks

Theft of nuclear material (NM)

- Lower risk because of longer refueling periods
- Very low risk for SMRs without on-site refueling
- More attractive NM in case of LEU above 10% (transportation of fresh fuel)

Radiological sabotage on-site

- Less number of areas for protection against sabotage
- Less vital areas (high consequences)
- Lower risk of spent fuel sabotage
- More opportunities for integration of safety and security
By definition: sabotage is

“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”

- IAEA recommendations for security measures against sabotage are made on the basis of the potential radiological consequences

- Consideration of the range of radiological consequences that can be associated with a n NPP and grading them defining limits for unacceptable radiological consequences (URC)
Sabotage consequence evaluation

Define the consequences of interest to determine the events to be considered

- Safety of nuclear facility staff, the public and the environment
  - Release of radioactive substances
  - Radioactive contamination
  - Radiation exposure and its levels
  - Identification of areas, related to URC
Graded Approach to Sabotage Protection Requirements

- **High Radiological Consequences**
  - Identify vital areas and protect as specified in INFCIRC/225.
  - Graded protection requirements based on level of potential consequences

- **Unacceptable Radiological Consequences**
  - No specific requirements for physical protection
  - Secure and control access to safety-related equipment

Consequences
Security Management Process

1. Setting up Facility Security Policy
2. Threat Evaluation
3. Vulnerability Assessment
4. Consequence Analysis
5. Acceptable Risk Level?
6. Preparing Security Plan
7. Periodic Review and QA
8. System modification and upgrading S/W,H/W, Procedures
Specific features of SMR nuclear facilities may reduce security risks, related to NM theft

Protection measures for SMR facilities against radiological sabotage: more opportunities for safety-security integration

For protection of NPP and the associated materials against radiological sabotage the IAEA recommends:

- Use design basis threat as a basis for security system design
- Evaluate and grade potential radiological consequences
- Define credible sabotage scenarios