

Protection of Nuclear Facilities against Sabotage

IAEA Security Series No. 4

Special Session – 14 August 2007
SMiRT Toronto

Aybars Gürpınar, IAEA Consultant



IAEA

Atoms for Peace: The First Half Century
1957–2007

Contents

Introduction of the Document:

- IAEA Security Series - Technical Guidelines on the engineering safety aspects of the protection of NPPs against sabotage (2007)
 - Preparation Process
 - Scope
 - Contents
- Concluding Remarks

IAEA Assessment Guidelines Preparation Process

- Development initiated 2002
- Participants in development from US, Canada, UK, Germany, Switzerland, France, South Korea, Russia
- Workshops presented
 - Russia (2), China (2), South Korea, The Netherlands (JRC of the EU), Brazil, Romania, Bulgaria, Kazakhstan, Japan, Germany, Pakistan, India, Iran, Turkey, Armenia, Spain, Canada
- Other presentations (EU – Brussels, Ispra JRC, UK, US NRC (2), USC, RAMCAP (Vienna, 2005), NEI (2007))

Scope - Critical Facilities

- Facilities comprised of complex processes and systems
- Failure of facility perceived to have catastrophic consequences
 - Health and safety of workers and the public
 - Environmental consequences
 - Business interruption
 - Public confidence in security

Scope - Critical Facilities

- Nuclear facilities
- Oil and gas
 - Up-stream (off-shore, on-shore, distribution)
 - Down-stream (processing, storage, distribution)
- Chemical
 - Production plants, end users, storage, distribution)
- LNG

Scope - Nuclear Facilities

- Nuclear Power Plants
 - Core damage, containment failure, radioactive release
 - Spent fuel storage (spent fuel pool, dry fuel storage)
 - Fresh fuel storage
- Research Reactors
- Fuel Cycle Facilities
- Transportation

Presentation Focuses on Nuclear Reactors

Scope - Multi-Disciplinary Problem

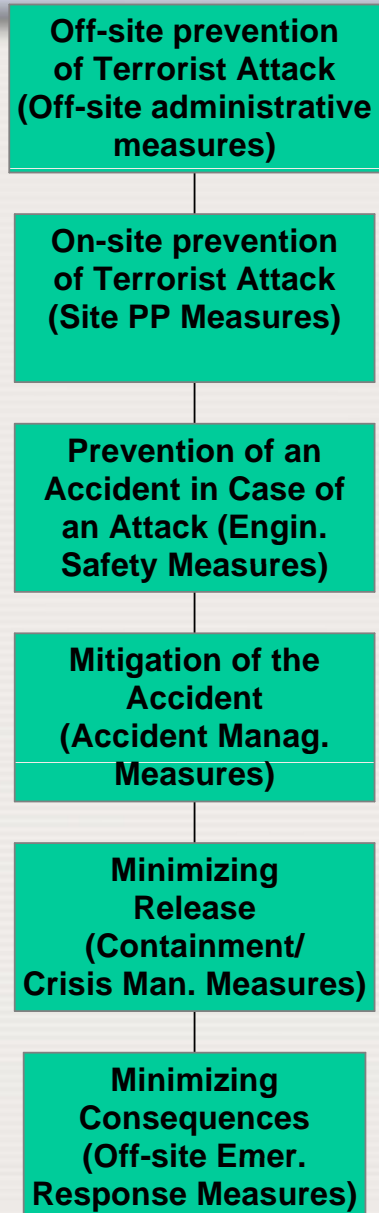
- Malevolent Attack Experience
- Consequence Evaluation
- Safety
- Systems
- Security
- Operations
- Engineering
- Emergency Response

Definition of Sabotage

(from INFCIRC 225/Rev 4)

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 and the environment by exposure to radiation or release of radioactive substances.

Defense in Depth for Safety/Security of Nuclear Power Plants



Background

- **September 11, 2001 changed the threat perception**
 - **Sophistication of planning**
 - **Suicidal nature of the act**
- **Regulators required immediate security upgrades**
- **Regulators also asked for robustness reviews**
- **IAEA TECDOC process started for a systematic approach to verify survivability**

Contents - Key Elements Drive the Evaluation Process

- Terrorist Attack Scenario Development (Based on DBT or BDBT)
 - What?
 - Where?
 - When? (Full power, refueling outage, ...)
- Plant Functional Requirements
 - Safe Shutdown (highly redundant?)
- Future Status
 - Restart or decommissioning?

Contents - Terrorist Attack Scenario Development: Perpetrators

- Knowledgeable, information-rich, resourceful
- Suicidal
- Outsiders (strike forces,)
- Insiders
- Insiders/outsideers

Contents - Plant Functional Requirements

- Plant Operational State
 - Full power
 - Refueling outage
 - Other maintenance activities
- Desired End State
 - Safe Shutdown (one train, highly redundant?)
- Future Plan
 - Restart
 - Decommissioning

Contents - Approaches to Terrorist Attack Risk Assessment: Existing and New Facilities

- Events enveloped by design conditions
- Probabilistic Safety Assessment (PSA) - based
- Sabotage Margin Assessment (SMA)
- Bunker System: Facility modification

All approaches benefit from a structured systematic process, e.g., PSA

Deja vu all over again -- external events 1980's and beyond

Contents - Assessment is a Multi-Phase Program

- Phase 1 Threat Evaluation
- Phase 2 Beyond Design Basis Threat Specification
- Phase 3 Physical Protection Design and Evaluation
 - Systems/operations -- Safe Shutdown Path(s)
 - In-plant evaluation (walkdown)
 - Analytical and testing evaluations
- Phase 4 Risk Acceptance Criteria

Threat Assessment

- Comprehensive and well organized threat identification program
- State and local organizations
 - Intelligence
 - Military
 - Law enforcement
- End Product
 - Threat Assessment Document
 - Document all realistic and credible threats
 - Strictly confidential

Insider threat protection

Tampering with safety related systems or components should be detected as soon as possible. An independent reactor protection systems is needed to be designed in such a way that fundamental safety functions are fulfilled for a specified limited time without human actions. The robustness against human error contributes significantly to insider threat protection and vice versa.

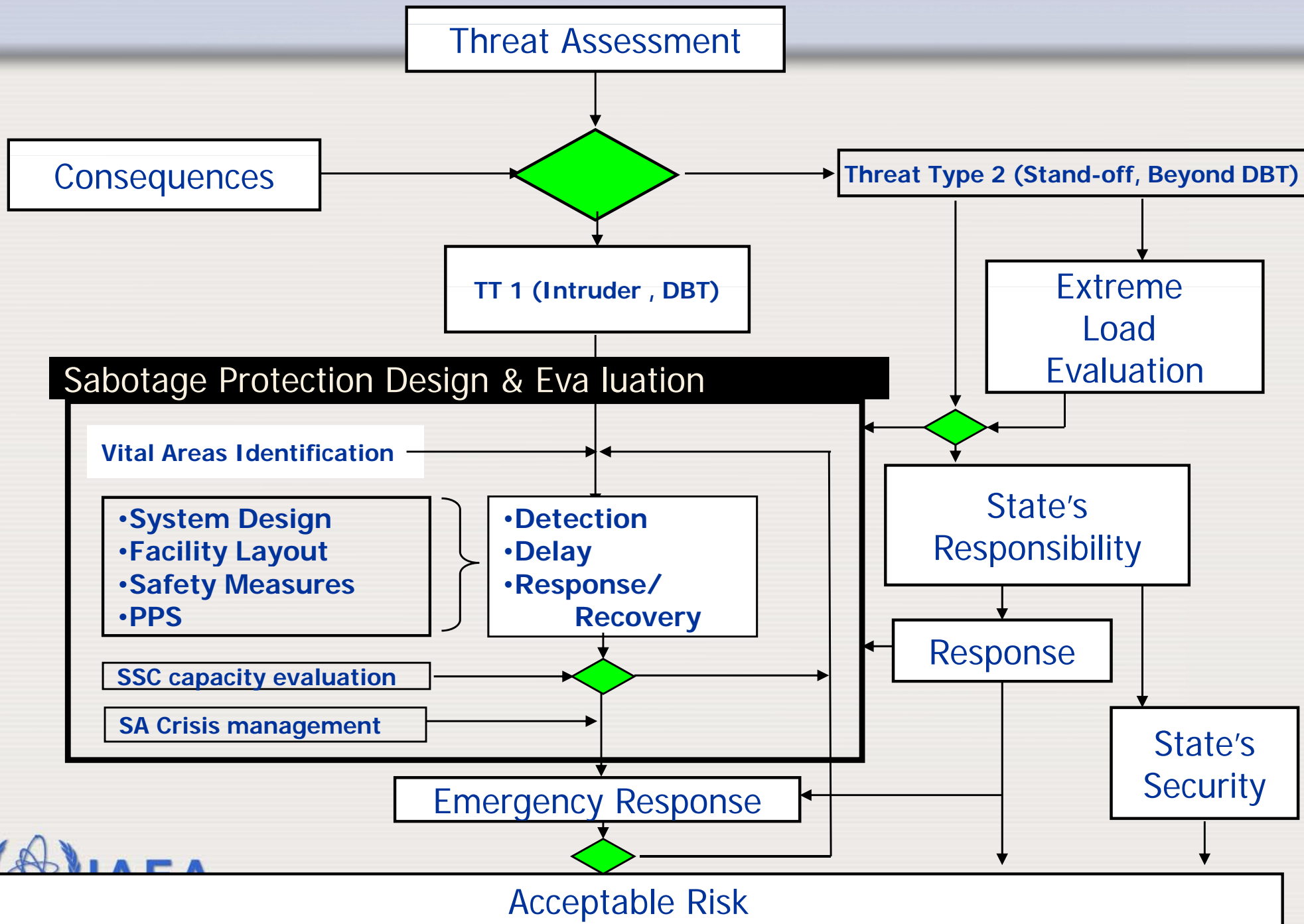
Objectives of the Guidelines

- Provide a methodology that results in a systematic study to verify survivability of the basic reactivity control, cooling and containment functions of nuclear installations.
- Utilize existing techniques of safety margin assessment
- Demonstrate that at least one safe shutdown or success path for selected threat scenarios

Scope

- **Applies to complex nuclear facilities: power plants, research reactors, fuel fabrication, etc.**
- **Events considered:**
 - intrusion into the site
 - initiated outside the site area: aircraft, missile, etc.
 - malevolent vehicle
 - multiple modes
- **Out of scope:**
 - theft , economic loss, public concern

Protection of Nuclear Facilities Against Sabotage



Criteria for BDBT (example)

- **Show sufficient robustness to prevent immediate, uncontrolled release (i.e. no catastrophic failure)**
- **Essential safety systems function**
 - available or can be started & run
 - operation possible in extreme environment
 - capable of repair
- **Radiological dose minimized**
- **Acceptance criteria on realistic (i.e., not conservative) assumptions**

Extreme Environment Matrix: the start of a family of “load” tables

TABLE 3-1 EXTREME ENVIRONMENT MATRIX									
Threat Scenario No.	Threat Scenario Description	Impact	PHYSICAL LOADING CONDITIONS					Flooding	Other
			Blast	Heat/fire	Hazardous Materials Release	Smothering			
1	<i>Boeing 767 fully fueled crash into NPP site</i>	<i>1,2</i>	<i>None</i>	<i>1</i>	<i>None</i>	<i>None</i>	<i>None</i>	<i>None</i>	
2									
3									
N									

Safe Shutdown Path (Cont'd.)

Basic Philosophy:

- **Define one or more safe shutdown paths to:**
 - Shutdown the facility & maintain safe shutdown
 - Provide for heat sinks
 - Contain radioactive materials
 - Provide monitoring & control functions
- **Selection criteria:**
 - Able to demonstrate margin or capacity
 - Include physical protection systems
 - Minimize number of vital areas
 - One safe shutdown path required, but redundant paths beneficial

CONCLUDING REMARKS

- A defense-in-depth based approach was developed that combines safety/security, on-site/off-site and intrinsic/extrinsic measures
- Extension to other criteria (business interruption, etc) and other facilities (oil, gas)
- Interaction of concepts of robustness, resilience and regulation