Safety analysis in design and assessment of the physical protection of the OKG NPP

okg
- a company in the E.ON-group

Background

okg
- a company in the E.ON-group

OKG in a nutshell…

~ 10 % of the electric power production in Sweden

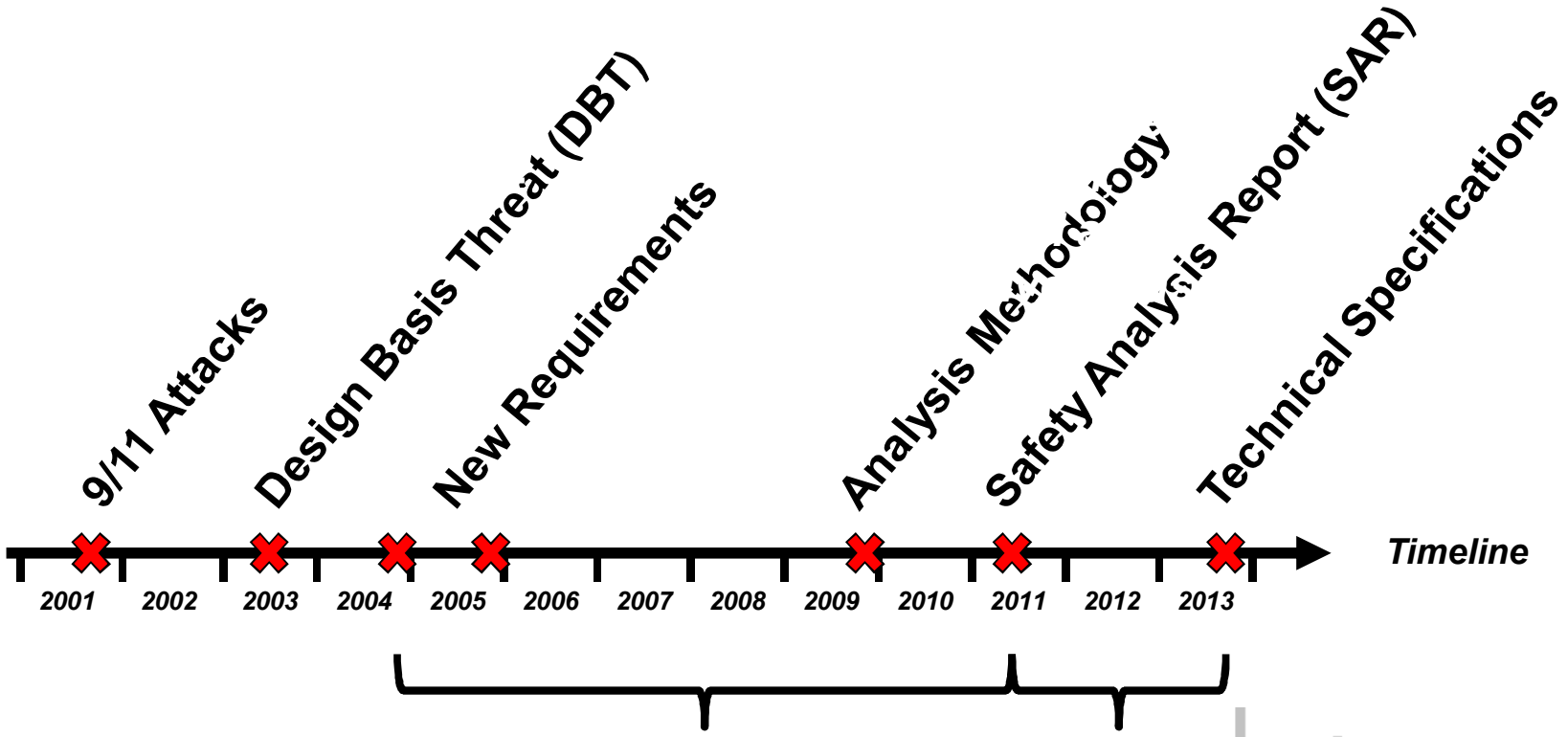
O1 (1972)
492 MW

O2 (1974)
586 MW

O3 (1985)
1450 MW

okg
- a company in the E.ON-group

History – Security upgrade

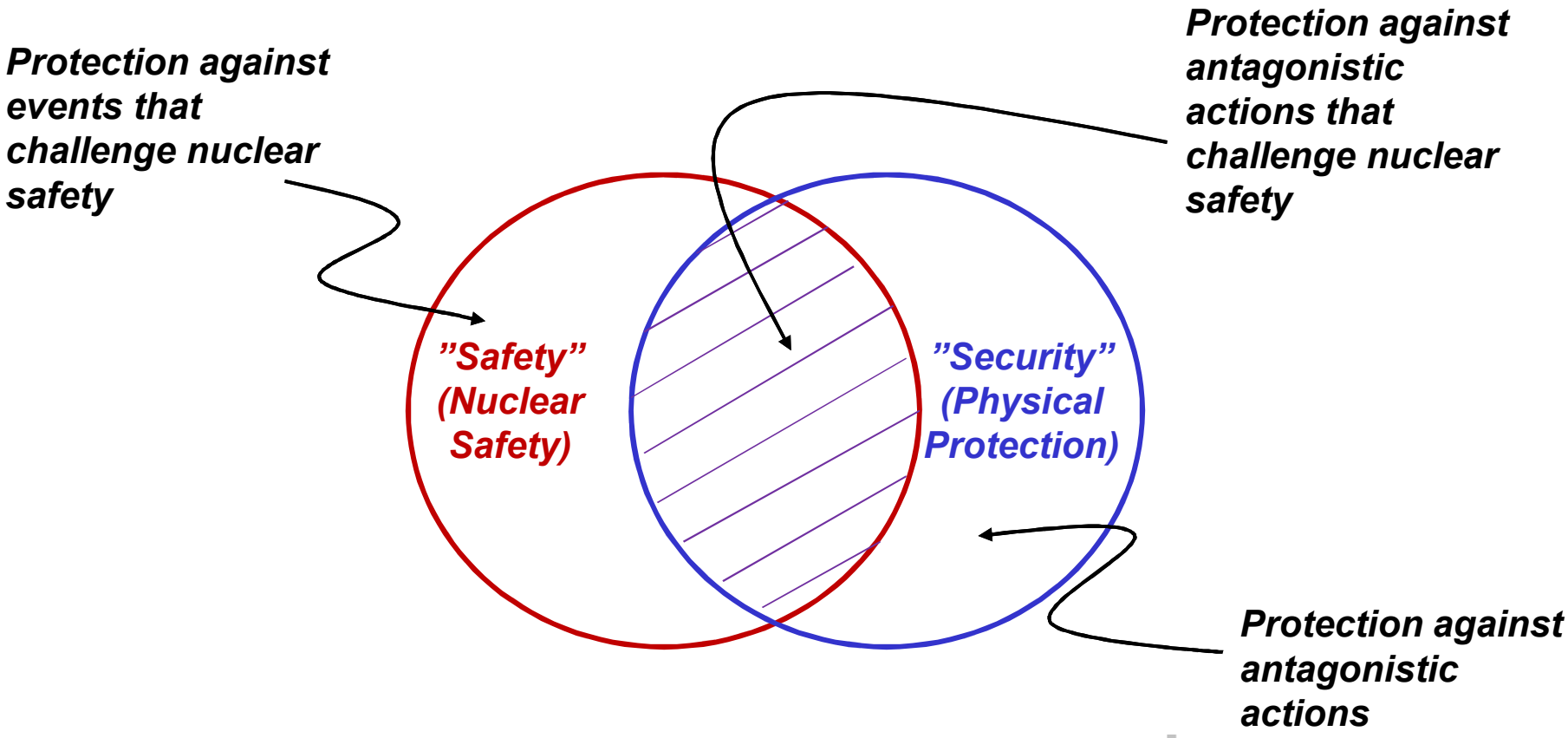


okg
- a company in the E.ON-group

The integrated approach

okg
- a company in the E.ON-group

The relationship between Safety and Security



okg
- a company in the E.ON-group

Deterministic Safety Analysis (DSA)

Conventional DSA

- Identify initiating events and associated event classes
- Identify event specific boundary conditions
  - Mode of operation
  - Deterministic requirements
  - Event specific degradation
- Identify event specific acceptance criteria

DBT-based DSA

- Identify DBT-based scenarios
- Identify scenario specific boundary conditions
  - Mode of operation
  - "Pessimistic postulates"
  - Scenario specific degradation
- Select scenario specific acceptance criteria

okg
- a company in the E.ON-group

Probabilistic Safety Analysis (PSA)

Conventional PSA

- Identify initiating events and associated event frequencies
- Identify event specific boundary conditions
- Select probabilistic safety goals

DBT-based PSA

- Identify DBT-based scenarios
- Identify scenario specific boundary conditions
- Select relevant acceptance criteria

okg
- a company in the E.ON-group

Finding an analysis ”Template”

Internal (area) events

- Potentially degrading barriers and safety functions
- Spatial dependences may be important
- PSA informed DSA may be useful

Antagonistic actions

- Potentially degrading barriers and safety functions
- Spatial dependences may be important
- PSA informed DSA may be useful

⇒ **Arrange DBT-based analysis according to the structure for “internal events” analysis.**

okg
- a company in the E.ON-group

Application 1 - *Design*

okg
- a company in the E.ON-group

A fictive DBT

- **Antagonist 1 –** ***A non-violent group of activists seeking public attention to convey an anti-nuclear message***
- **Antagonist 2 –** ***A terrorist cell seeking to create public fear, by causing a nuclear accident***

okg
- a company in the E.ON-group

Scenario 1 - *Specification*

- **Motif/Objective:** ***A non-violent group of activists seek public attention through a demonstration at the site. Attempts to penetrate protective barriers may occur.***
- **Abilities:** ***The activists have access to publically available information. If they try to penetrate protective barriers, they will only use "burglary type" tools.***
- **Pessimistic postulates:** ***Assume that the activists will try to penetrate protective barriers.***
- **Acceptance criteria:** ***Consequences must not exceed the limits defined for the event class "normal operation". (It must be possible to continue operation within the limits of the technical specifications.)***

okg
- a company in the E.ON-group

Scenario 1 - *Analysis*

- **Vulnerability analysis:** ***Acceptance criteria are violated if the activists are able to provoke a reactor shut down. This will occur if the activists threaten safety relevant equipment.***
- **Protective measures:** ***Place safety relevant equipment in the restricted (protected) area. Install security alarm capability, to detect unauthorized access.***
- **Conclusion:** ***Given that the physical protection of the restricted area will resist "burglary type" tools, normal operation may continue as long as there is no security alarm. Thus, given that the protective measures are implemented, the acceptance criteria for scenario 1 are met.***

okg
- a company in the E.ON-group

Scenario 2 - *Specification*

- **Motif/Objective:** ***A terrorist cell seek to create public fear, by causing a nuclear accident through the detonation of a bomb.***
- **Abilities:** ***The terrorists have access to publically available information and to insider information regarding routines for normal operation. They will use explosives to force protective barriers, and to damage safety relevant equipment. Offsite power may or may not be taken out in the attack.***
- **Pessimistic postulates:** ***Assume that offsite power is non-available.***
- **Acceptance criteria:** ***Consequences must not exceed the limits defined for the event class "unanticipated events. (Safe shut down must be achieved. Some outage time is accepted for repairs.)***

okg
- a company in the E.ON-group

Scenario 2 – *Analysis (1/3)*

- **Vulnerability analysis:** ***The acceptance criteria will be violated if the terrorists are able to detonate a bomb in an area where it is likely to cause core damage or damage to spent fuel. The PSA models for the power plant may be used to identify such areas. If any "weak spots" are found, they may need additional protection if the terrorists are likely to be able to identify them as targets.***

okg
- a company in the E.ON-group

Scenario 2 – *Analysis (2/3)*

- **Protective measures:** ***Exclude sensitive information regarding dependencies from all documents describing routines for normal operation, to prevent terrorists from identifying targets for the bomb. Still, some "weak spots", e.g. the main control room, may be identified based on publically available information. By placing safety relevant equipment in the restricted (protected) area, installing security alarm capability to detect unauthorized access, and implementing sufficient obstructing and delaying measures, it is possible to delay the detonation until the attack may be interrupted by arriving security forces.***

okg
- a company in the E.ON-group

Scenario 2 – *Analysis (3/3)*

- **Conclusion:** ***By implementing administrative routines to protect sensitive information, by implementing an adequate physical protection of safety relevant equipment, and by making arrangements for security alarms and action plans in case of an attack, the security arrangement as a whole will be sufficient to enable safe shut down and prevent core damage. Thus, given that the protective measures are implemented, the acceptance criteria for scenario 2 are met.***

okg
- a company in the E.ON-group

Design of the physical protection – Summary

- The DBT is transformed into a set of scenarios that define the design requirements.
- The scenarios provide guidance on how to select relevant protective measures.
- The DBT-based analysis (evaluation of all scenarios considering the selected protective measures) verify that the physical protection as a whole is sufficient.

okg
- a company in the E.ON-group

Application 2 – *Management support*

okg
- a company in the E.ON-group

Safety evaluation (1/2)

- **A structured method for categorizing safety concerns*: Safety significance depend on the degree of influence on the "defense in depth".**
  - **"Negligible" (no actions necessary)**
  - **"Low" (permanent corrective measures may be considered if practicable)**
  - **"Medium" (risk reducing measures necessary, plant operation acceptable for some limited time until corrective measures have been implemented)**
  - **"High" (immediate risk reducing measures or plant shut down should be considered)**

***IAEA Safety Reports Series No. 12, Vienna (1998)**

okg
- a company in the E.ON-group

Safety evaluation (2/2)

- **Safety significance is determined by reevaluating affected DSA.**
- **Introducing DBT-based DSA ⇒ The method for safety evaluation may be applied to security concerns.**
- **Safety/Security integration ⇒ Prioritization between risk reducing measures is facilitated.**

okg
- a company in the E.ON-group

Application 3 – *Operational support*

okg
- a company in the E.ON-group

Requirements in the Technical Specifications (1/2)

- DBT-based analysis results
- FMEA

} ⇒

- Minimal requirements for credited security measures (functional level)

okg - a company in the E.ON-group

Requirements in the Technical Specifications (2/2)

- Minimal requirements
- Compensating measures

⇒

- New section in the technical specifications

okg
- a company in the E.ON-group

Concluding remarks

- **Safety/Security integration advantages**
  - **Common language ⇒ Interdisciplinary acceptance**
  - **Extended nuclear safety applications (design & assessment)**
  - **More informed requirements in the technical specifications**
- **Disadvantages**
  - **Initial “threshold” in communication with stakeholders. Requires attention and resources.**

okg
- a company in the E.ON-group

Thank you!

Pär Lindahl

par.lindahl@okg.eon.se

okg
- a company in the E.ON-group