Regulatory approach to cyber security in Finland

International Regulators Conference on Nuclear Security

Washington, December 4-6, 2012

Dr. Lasse Reiman

Director, STUK

Paula Karhu

Senior Inspector, STUK

Security Strategy for Society in Finland

- **Government Resolution, December 2010**
  - The main sections of the strategy are
    - Securing the vital functions
    - Crisis management
    - Implementation of the strategy
  - The strategy presents the threat scenarios against society's vital functions
    - Includes cyber threats, major accidents and terrorism
    - Includes also serious disturbances in the power supply
  - The strategy present basic principles concerning safeguarding the critical functions in society which depend on ICT systems and communications in crisis situations

- **National Counter Terrorism Strategy** established, National Cyber Strategy under development

Managing cyber threats in Finland

- The Finnish Communications Regulatory Authority (FICORA) is responsible for handling information security incidents in Finland, the computer security incident response unit is called CERT-FI
- The CERT-FI maintains the national information security situation awareness system
- The CERT-FI monitores the global situation and vulnerabilities that may be of relevance to Finnish interests
- The CERT-FI provides technical vulnerability notes, advisories and warnings as necessary (including I&C systems)

Regulatory approach to cyber threats at nuclear facilities

- **The Government Decree on Nuclear Security** (734/2008) requires that a DBT is established. In addition, the Decree stipulates the following
  - Advanced information security principles shall be utilised in the planning of the nuclear facility and its information, communication and automation systems.
  - Unauthorised access to the protection and control systems shall be prevented
- STUK Regulatory Guide **YVL A.11 Security of nuclear facilities** (Final Draft) presents general requirements on information security
  - Information security associated threats shall be systematically analysed and protection measures chosen based on the analysis
  - Documents and data pertaining to a nuclear facility and its automation and telecommunication systems shall be safeguarded
  - If it is necessary to hand over classified information to third parties, the information shall be protected
  - The Guide includes classified appendixes

Regulatory approach to cyber threats at nuclear facilities

- STUK Regulatory Guide **YVL B.1 Safety design of nuclear power plants** (Final Draft) has the following requirements on I&C:
  - Security countermeasures shall be planned based on risk assessments
  - Unauthorised access to the software of I&C systems and computers shall be prevented through adequate physical, technical and administrative security arrangements. The installation of unauthorised components including software shall be reliably prevented. Any modifications made to the software shall be detectable and traceable.
  - The interface of the I&C architecture to administrative computer systems shall be implemented by making the transmission of data unidirectional in such a way that any transmission of data towards the I&C architecture is prevented through separation at the physical level.

Regulatory approach to cyber threats at nuclear facilities

- **STUK Regulatory Guide YVL A.12 Information security of a nuclear facility** (in preparation) will present the detailed requirements on information security including cyber security
  - Guide presents general requirements concerning information management systems and detailed requirements concerning protection objectives and protective mechanisms of safety and security significant ICT systems
  - The bases of requirements are IAEA NSS 17 Computer Security at Nuclear Facilities, ISO/IEC standards and Finnish National Security Auditing Criteria (KATAKRI)
  - Additional requirements based on the significance of the system

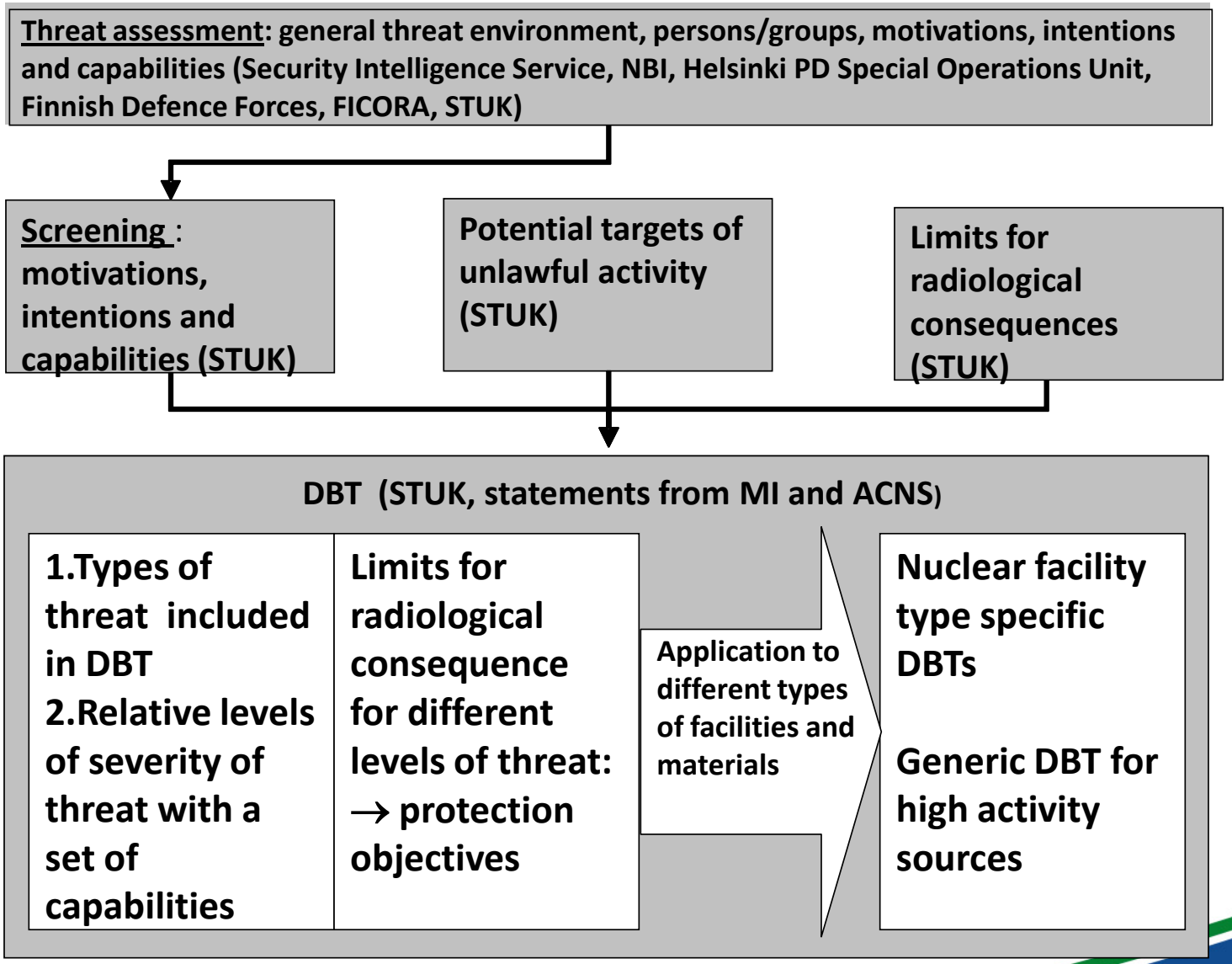
Finnish regulatory approach to cyber security

- Cyber security shall be be considered in the design of I&C
- Protection and control systems shall be isolated from the Internet
- The I&C design features contribute essentially to cyber security
  - DiD, physical separaration, functional isolation, hardwired systems
- Defence-in-Depth protective strategies and effective security controls for CDA need to be implemented
  - Technical controls
  - Operational controls
- Special emphasis on
  - the use of mobile devices
  - maintenance and configuration management practices
  - awareness of employees
- DBT including cyber threats

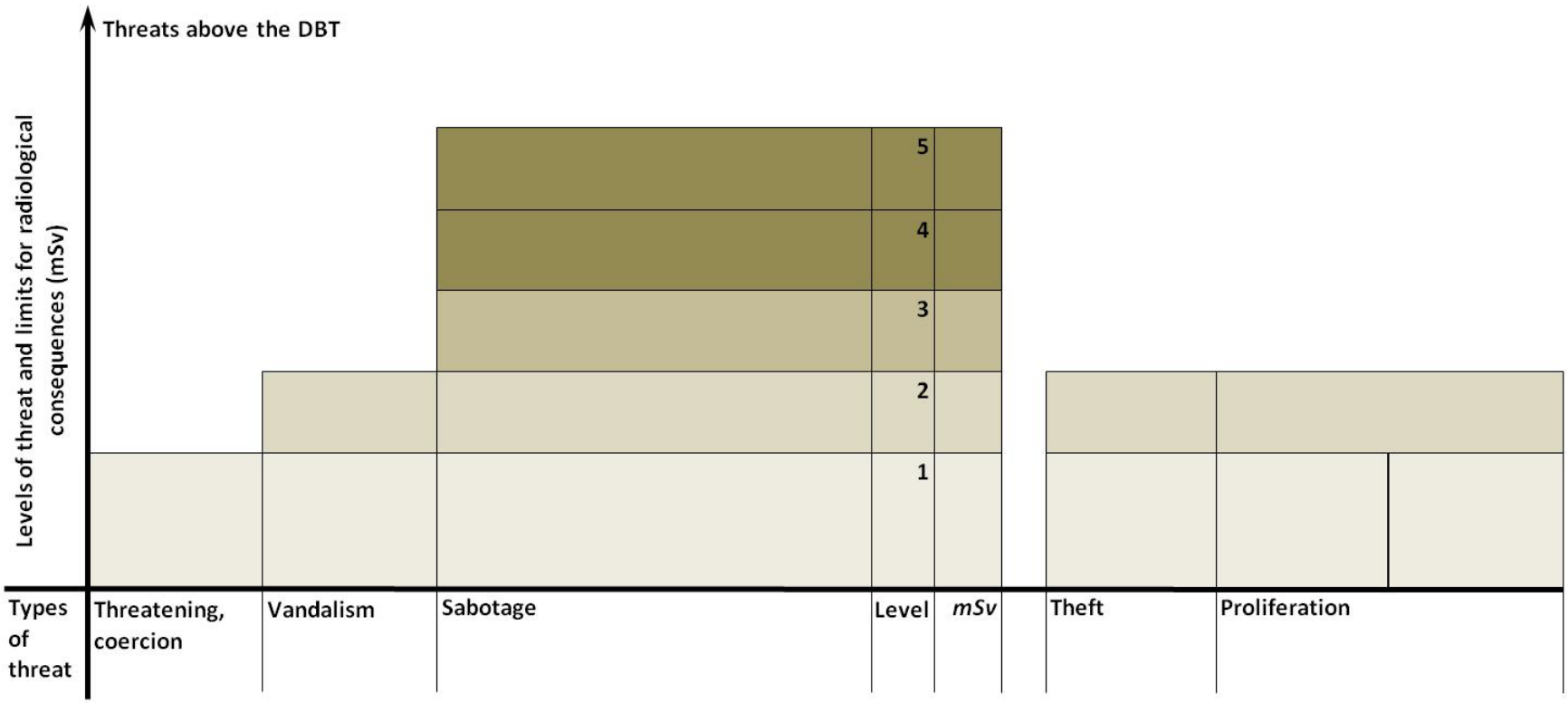
Oversight of cyber security

- Review of overall security plans and system specific security plans
  - Close co-operation with I&C experts in design review
- The licensee is required to organize an independent expert review of cyber security in the design phase
  - NRC RG 5.71 was used as a basis in one review
- In the construction and operation phases STUK carries out yearly inspections of information security practices including cyber security
- STUK has carried out information security audits to some foreign organizations using KATAKRI
- The licensee is required to organize an extensive independent assessment of their information security at no less than three years intervals
  - Possible changes of threat shall be considered

Process of preparing the DBT



DBT structure



mSv: annual dose limit for a member of the public (exception: level 5 with a short-term dose limit).

Each "box" has a set of defined adversary capabilities.

Each level has a limit for radiological consequences & protection objectives.

Threat assessment and DBT

Organisations involved in TA:

-Finnish Security Intelligence Service (SUPO, leading role)

-National Bureau of Investigations (NBI)

-Helsinki Police Department Special Operations Unit

-Finnish Defence Forces' technical research centre

-Finnish Communications Regulatory Authority (FICORA)

-STUK

Also utilized in TA:

-assessment based on past events (report by Interpol, IAEA ITDB, domestic events) and discussions with nuclear operators

Cyber threats are included in the DBT

-includes all life-cycle phases (design, manufacture, installation, operation including modifications and maintenance)

-includes different ways to influence CDA especially locally on-site

The Finnish regulatory approach to (cyber) security: A combination of performance based and descriptive requirements

In the DBT

- characterisation of (cyber) security threats
- insider considerations
- assumption of good knowledge
- protection objectives for each level in the DBT threat level scheme

In STUK Regulatory Guides (YVL Guides)

- a set of descriptive requirements for (cyber) security derived from the DBT
- oversight process

Active participation in international activities (NSS, IAEA, ISO 27K, IEC) to further develop international standards and national guidance