Technische Hochschule
Brandenburg
University of
Applied Sciences
Institute for Security
and Safety

Nuclear power aspects

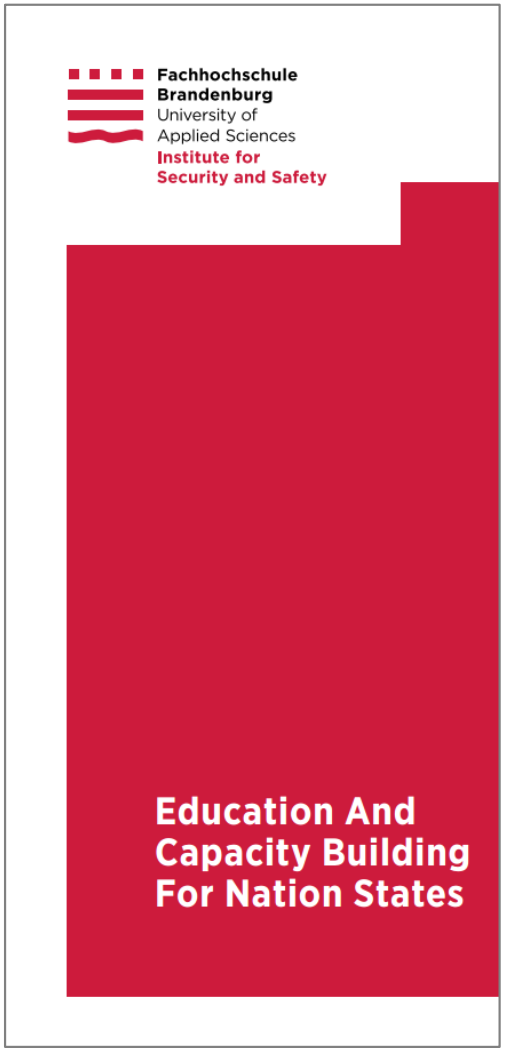
ITU/ENISA Regional Conference on Cybersecurity, Sofia

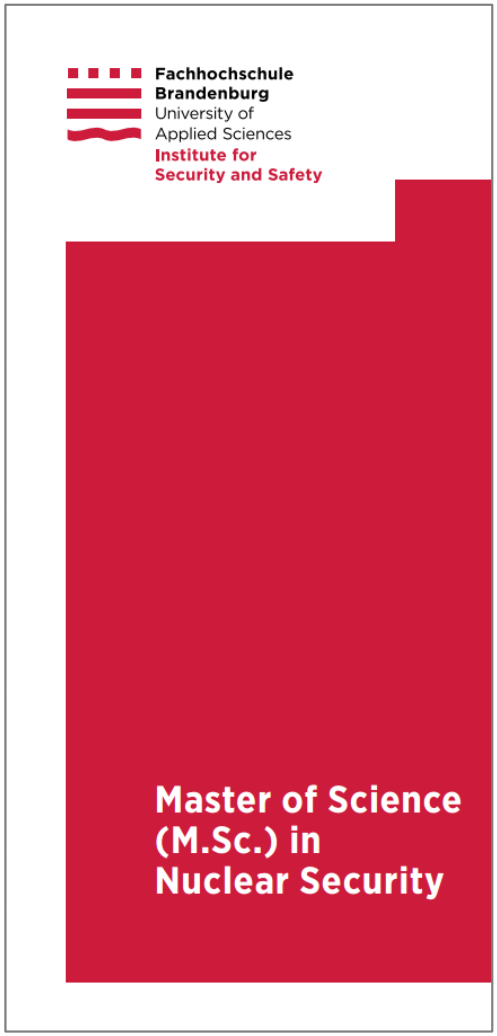
Guido Gluschke – November 30, 2016

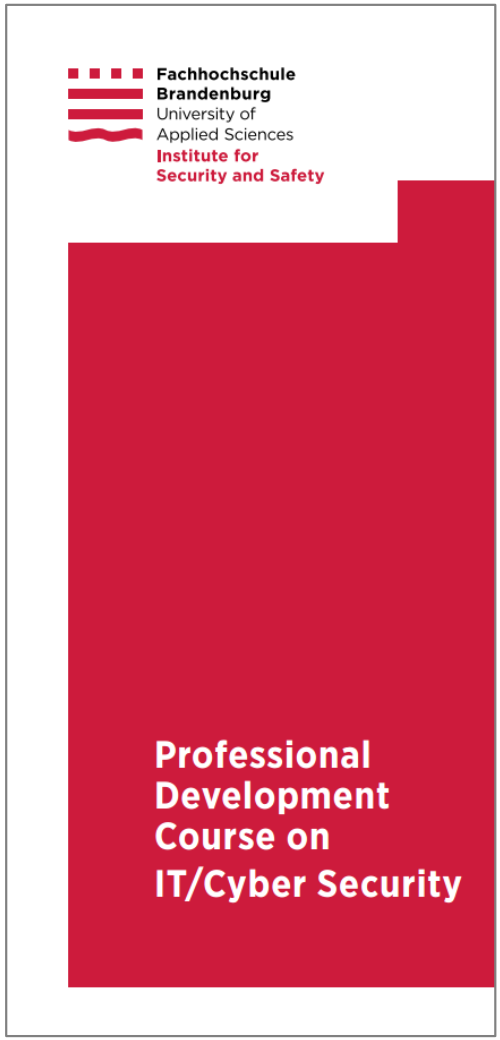
Introduction

- Guido Gluschke
- Co-Director Institute for Security and Safety at the Brandenburg University of Applied Sciences
- Background:
  - Computer Science / Cyber Security
  - Security Management / Nuclear Security
  - Critical Infrastructure Protection / Energy Sector
- Program manager for joint activities with international organisations such as UN, IAEA, OSCE, EU and NATO
- Member of the Energy Expert Cyber Security Platform - Expert Group of the European Commission DG-ENERGY
- Member of the NTI Cyber Security Expert Group
- Past IAEA INSEN Chairman

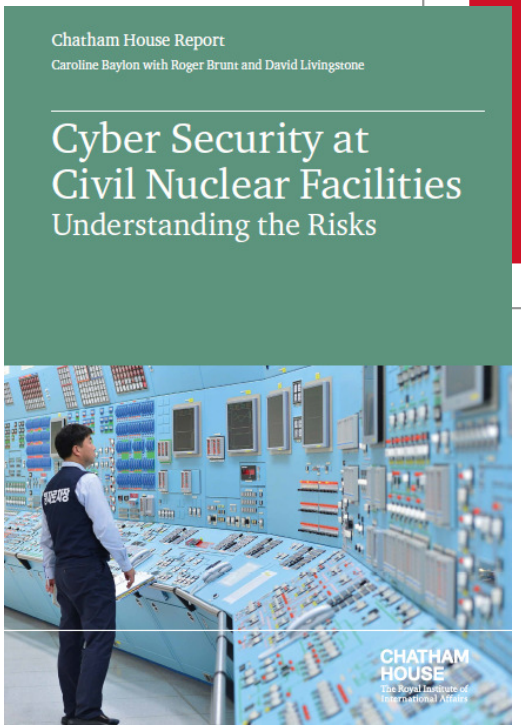
Our Focus:
Capacitity Building On Cyber And Nuclear Security

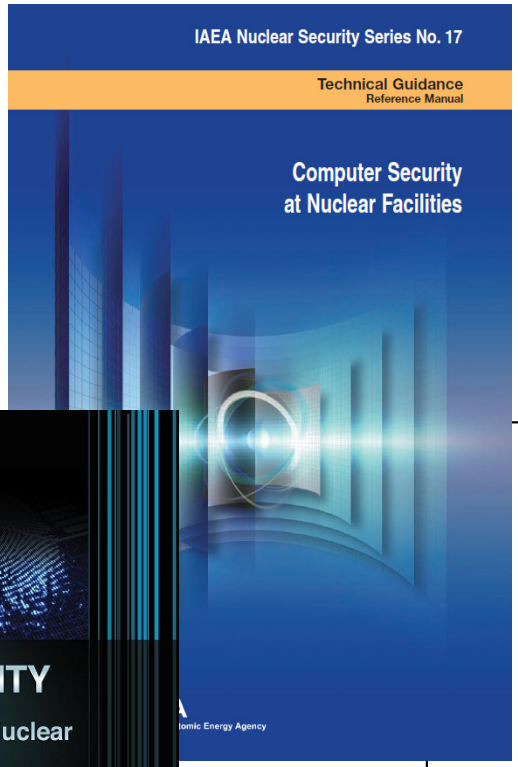


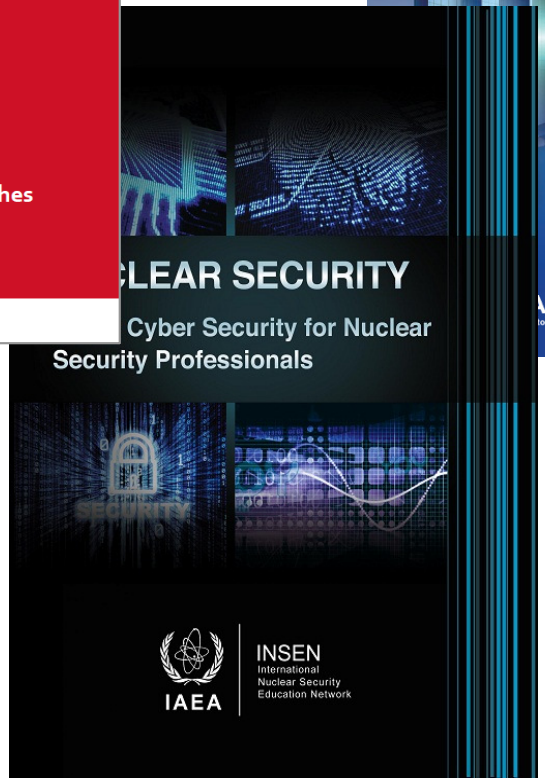




International Initiatives On Cyber Security At Civil Nuclear Facilities







NTI
BUILDING A SAFER WORLD

Report will be launched in December 2016 in Vienna

IAEA's Nuclear Computer Security Goals

The Computer and Information Security programme is focused on preventing computer acts that could directly or indirectly lead to:

- ***unauthorized removal*** of nuclear/other radioactive material
- ***sabotage*** against nuclear material or nuclear facilities
- ***theft*** of nuclear sensitive information

IAEA

IAEA NSS Documents On Nuclear Computer Security

Published

Planned

NSS Nuclear Security Fundamentals

NSS 20
Objective and Essential Elements of a State's Nuclear Security Regime Objectives, Concepts, Principles

NSS Nuclear Security Recommenations on

NSS 13
Nuclear Material and Nuclear Facilities

NSS 14
Radioactive Material and Associated Facilities

NSS 15
Nuclear and Other Radioactive Material out of Regulatory Control

NSS Computer Security Implementation Guides

NST045
Computer Security for Nuclear Security

NSS 23-G
Security of Nuclear Information

NSS Computer Security Technical Guides

NSS 17
Computer Security at Nuclear Facilities

NST047
Computer Security Methods for Nuclear Facilities

NST036
Computer Security Methods for I&C systems at Nuclear Facilities

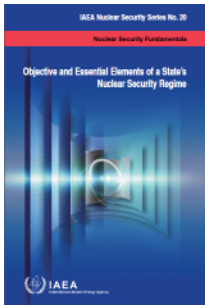
Documents outside of NSS Guidance

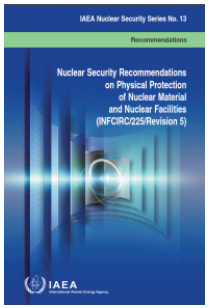
NST031
Security Management for Research Reactors

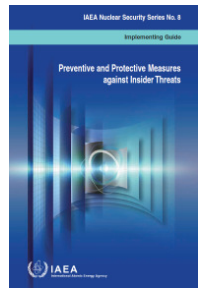
NST038
Incident Response Planning for Computer Security Events

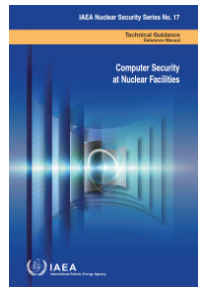
NST037
Conducting Computer Security Assessments

IAEA









CPPNM 2005 Amendment - The 12 Nuclear Security Principles

- FUNDAMENTAL PRINCIPLE A: Responsibility of the State
- FUNDAMENTAL PRINCIPLE C: Legislative and Regulatory Framework
- FUNDAMENTAL PRINCIPLE D: Competent Authority

Nation State

- FUNDAMENTAL PRINCIPLE E: Responsibility of the License Holders
- FUNDAMENTAL PRINCIPLE F: Security Culture
- FUNDAMENTAL PRINCIPLE H: Graded Approach
- FUNDAMENTAL PRINCIPLE I: Defence in Depth
- FUNDAMENTAL PRINCIPLE J: Quality Assurance
- FUNDAMENTAL PRINCIPLE K: Contingency Plans

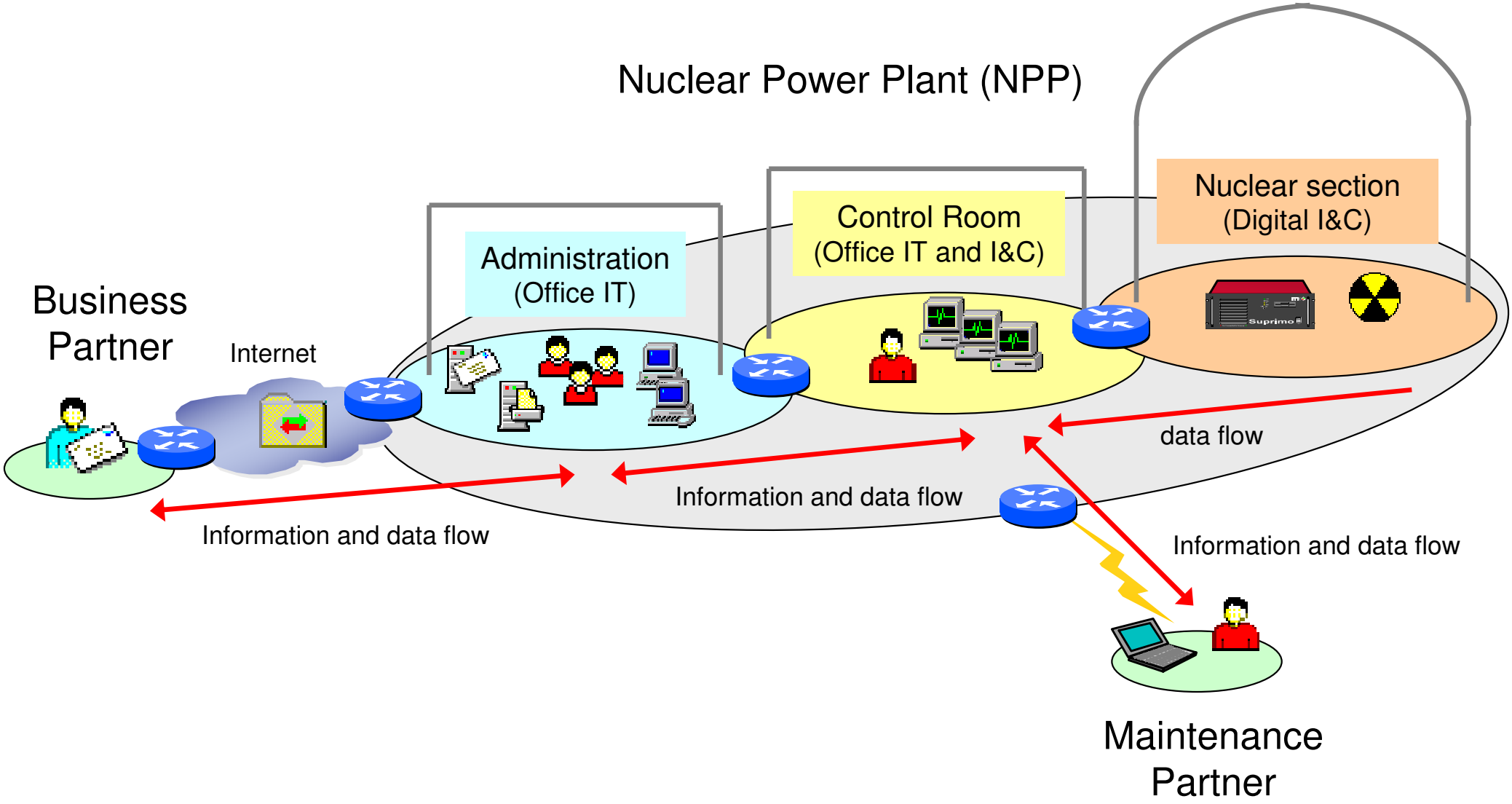
Operator

- FUNDAMENTAL PRINCIPLE B: Responsibilities During Int'l Transport
- FUNDAMENTAL PRINCIPLE G: Threat
- FUNDAMENTAL PRINCIPLE L: Confidentiality

Both

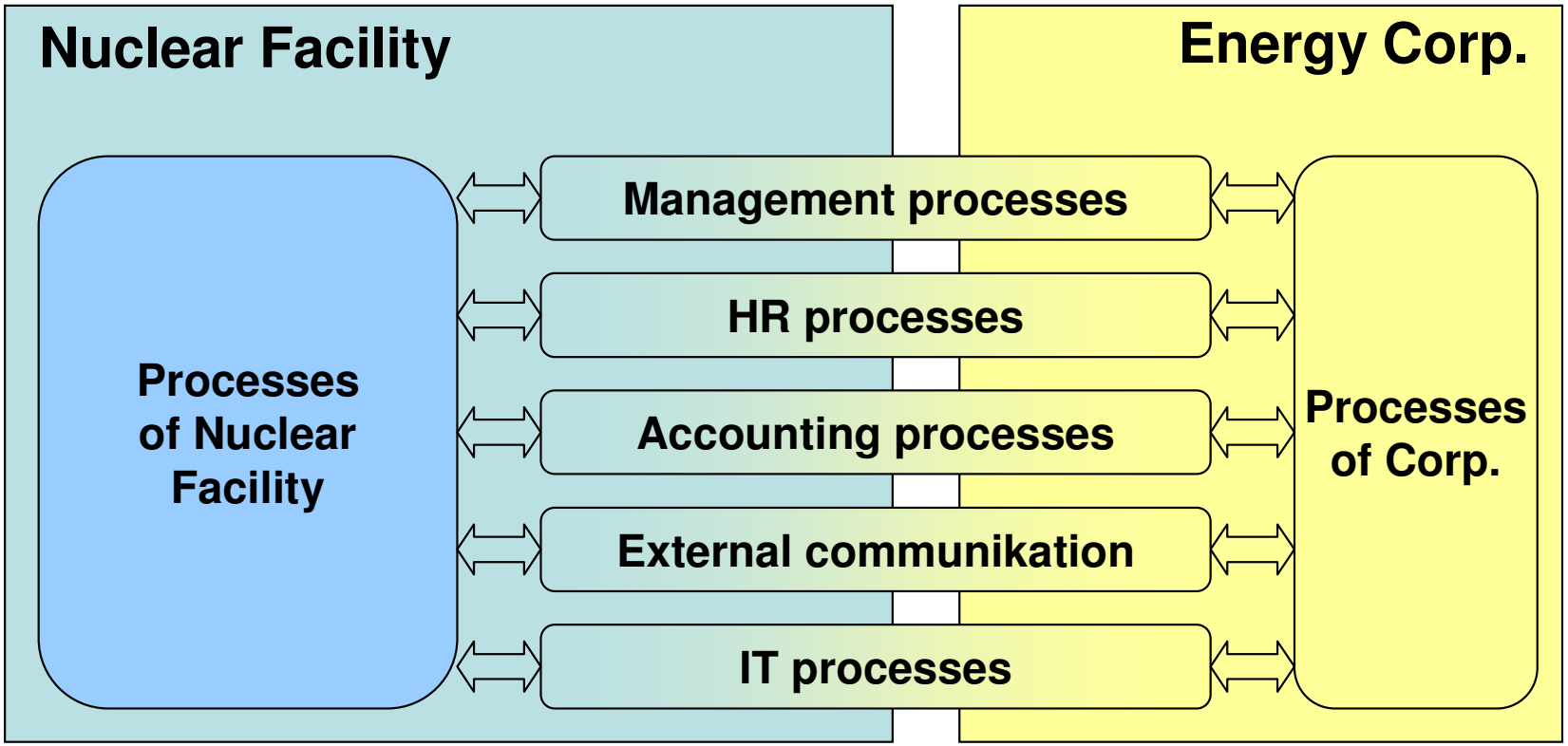
Entered into force on 8 May 2016!

Information Security Domains at an NPP



Typical information flow between Corporation and Nuclear Branch

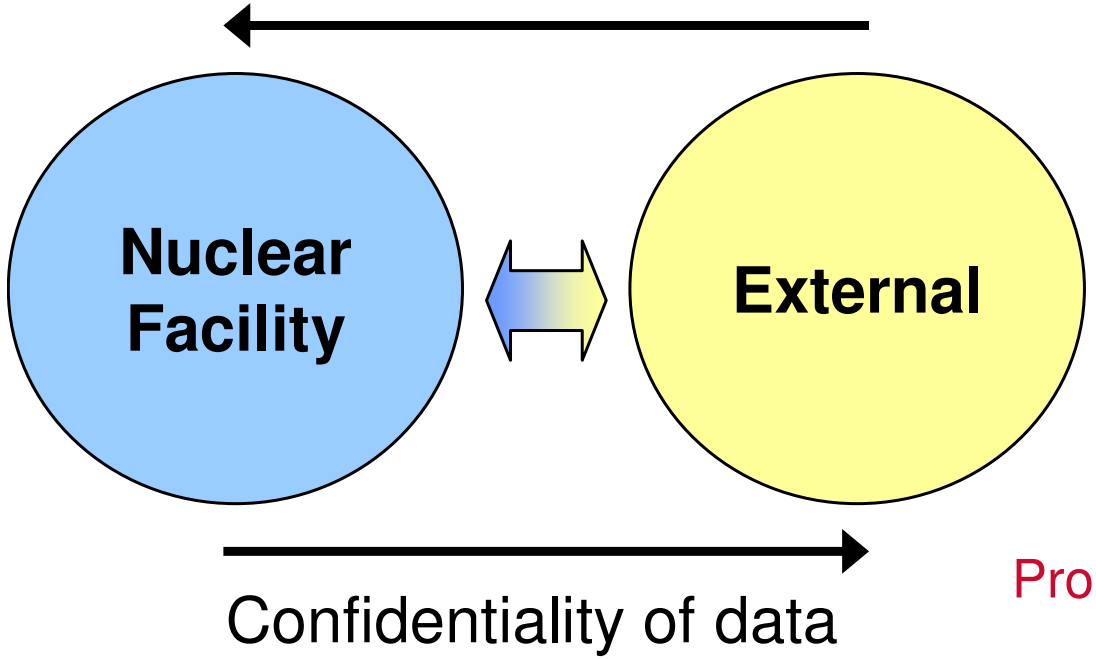
- If the nuclear facility belongs to an energy company some mutual business processes are typically found in which information has to be exchanged.



Main Security Goals On External Data Flow

Problem of disruption

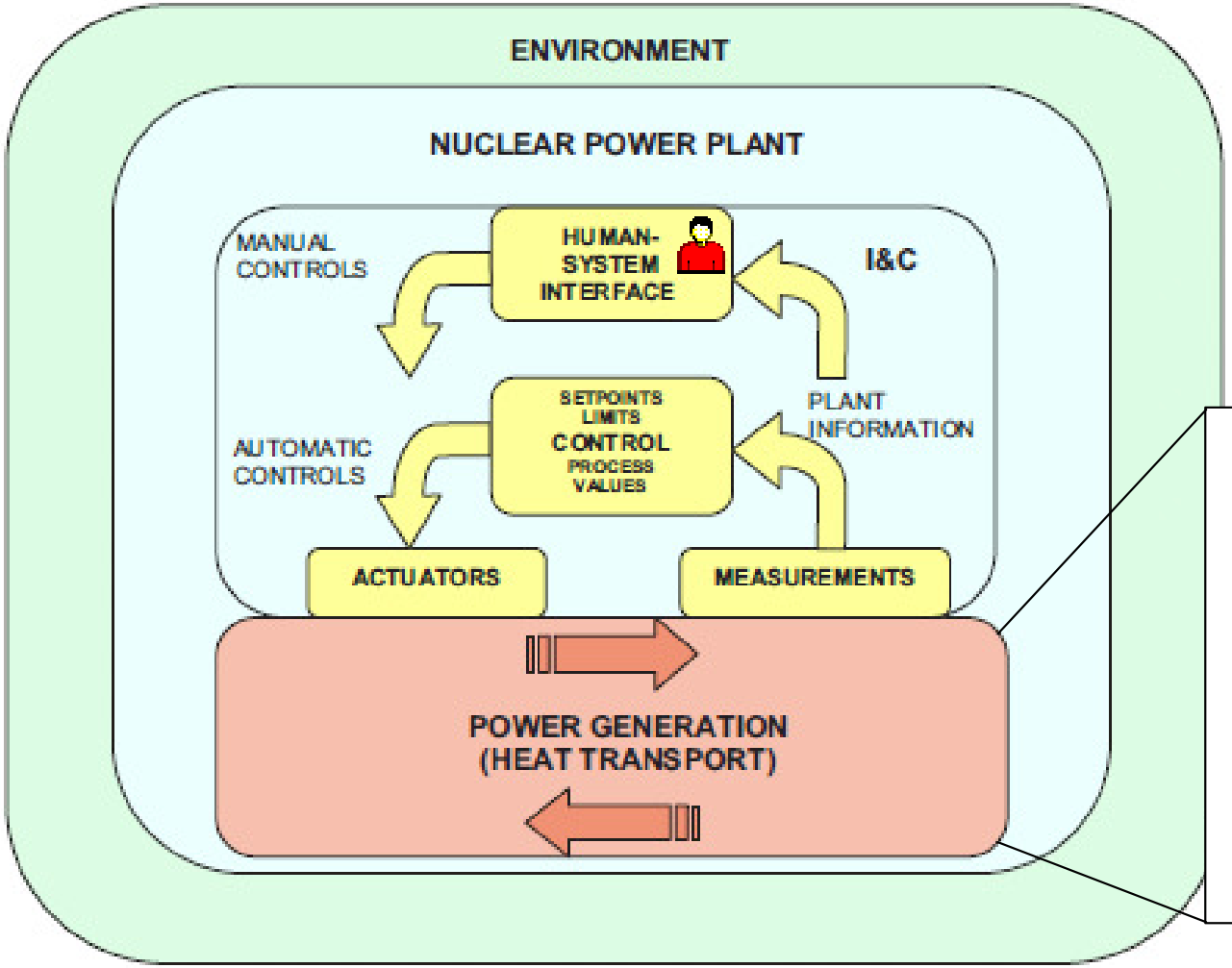
Data integrity and freedom of interference from data



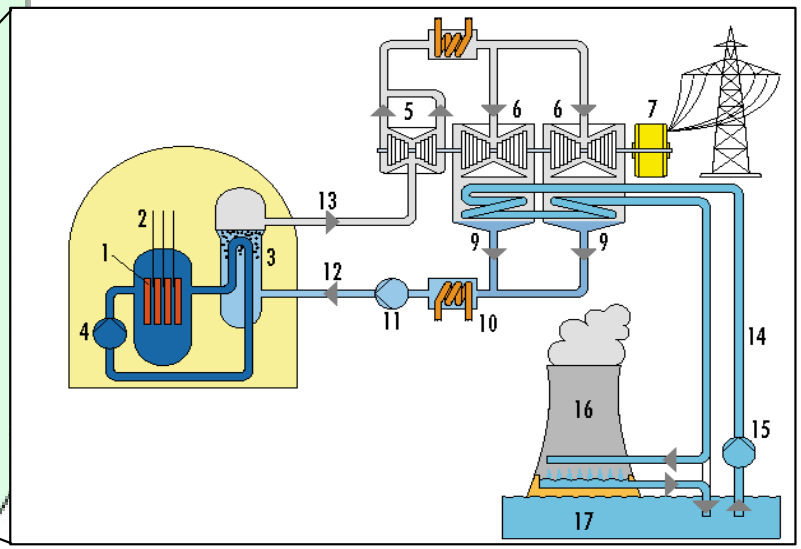
Confidentiality of data

Problem of disclosure

Understanding Nuclear I&C Assets



Energy production process



Source: IAEA Nuclear Energy Series NP-T-3.12

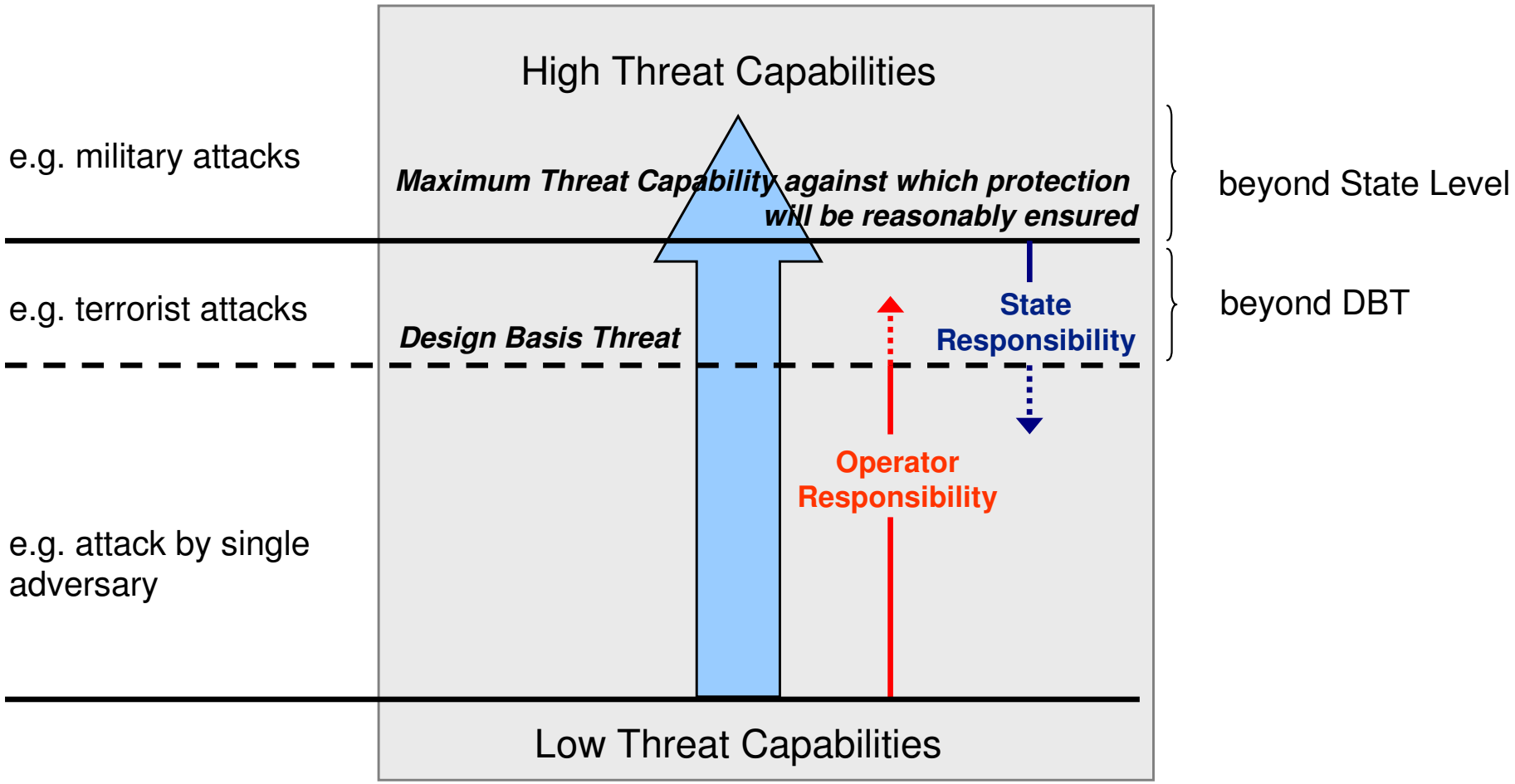
I&C Systems Trends

- In the past, control systems (including those associated with nuclear facilities) existed as unique islands, but that has changed.
- Today's trends:
  - Hybrid systems, not longer poorly I&C
  - The migration toward digital technologies and more uniform systems
  - Business considerations and technology improvements have resulted in greater connectivity between systems
  - Cost and efficiency considerations have resulted in remote access
  - The complexity of control systems is significant and increasing (Impossible to evaluate all potential environments of use)

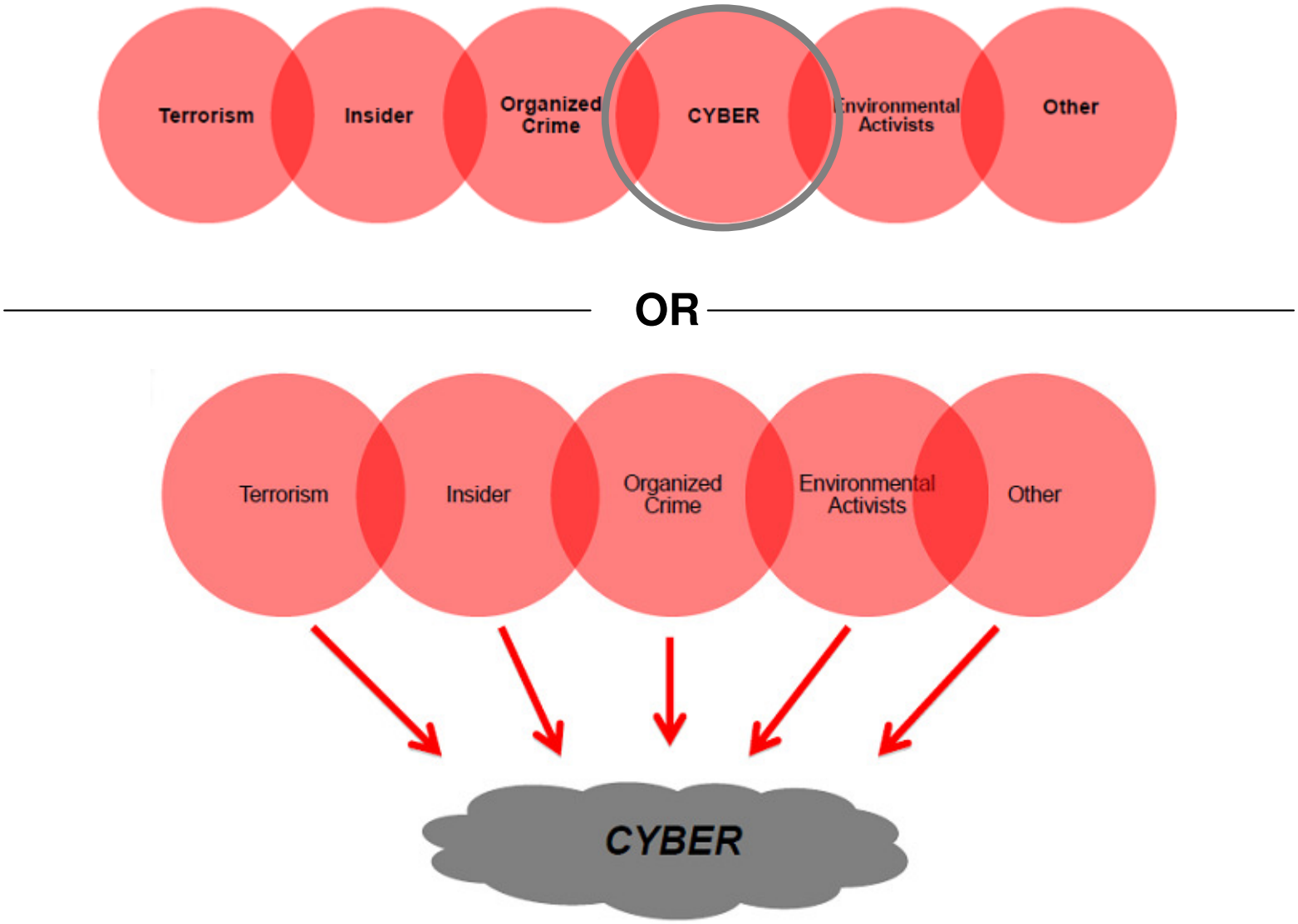
Civil Nuclear Power Plants In The Digital Age

- Complex System (NPP >20.000 digital devices)
- More and more digitalized parts, in particular ICS
- Increased internet connectivity
- Cyber as a new domain of military actions
- Industrial Control Systems (ICS) as new targets
- Cyber attacks rapidly changing, very professional
- Sufficient cyber security knowledge often not available at the facility (e.g. for incident response)
- Responsibilities for different levels of cyber defence unclear in most nation states, categorisation and attribution of attacks difficult

Nuclear Methodology: Design Basis Threat (DBT) Responsibilities

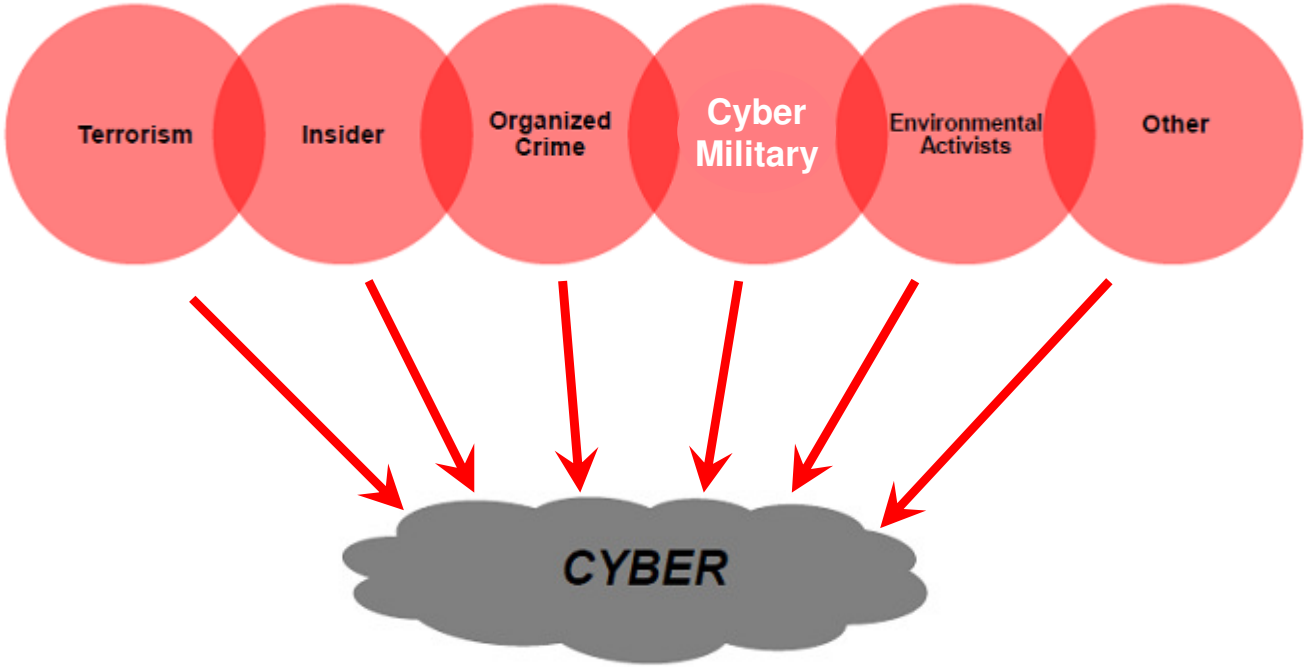


How To Handle Cyber In The DBT?

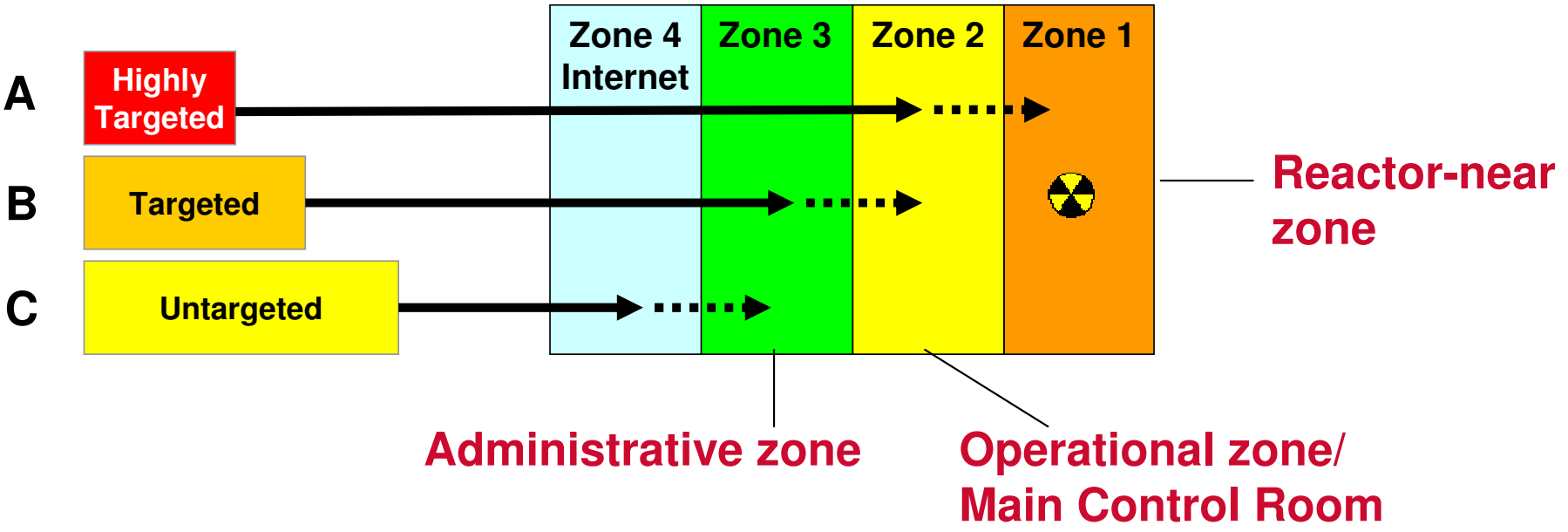


Source: Michael Beaudette, WINS workshop Toronto March 2012

Two Dimensions For Threats Against Civil Nuclear Facilities: Cyber As A Tool / Cyber As A Military Option



Simple Attack Model

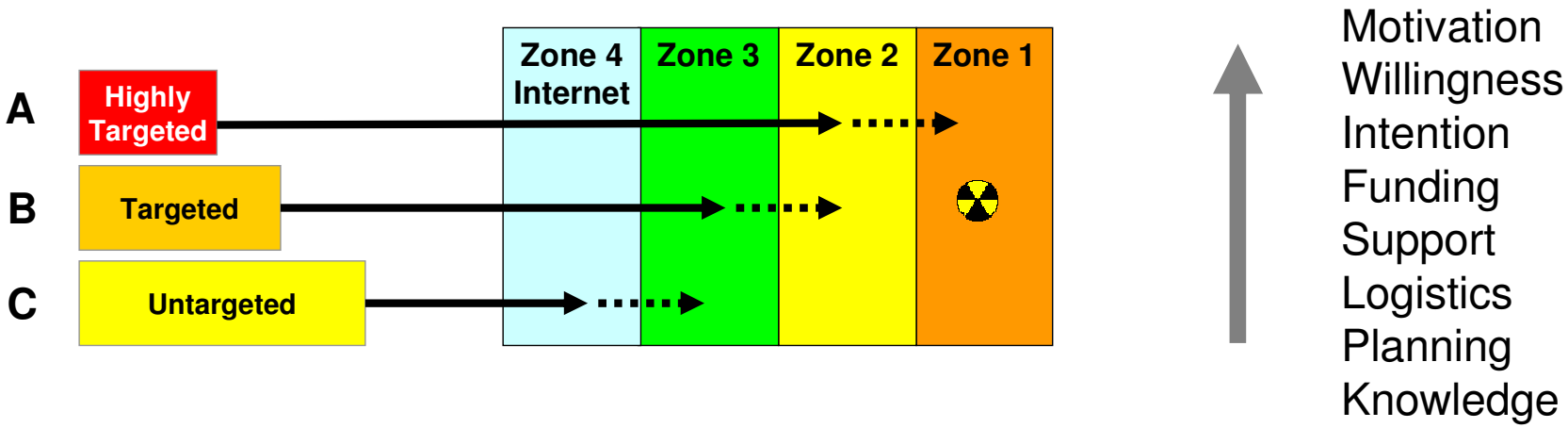


A Highly targeted: Targeted against particular component/system

B Targeted: Targeted against particular organization/facility

C Untargeted: Not targeted against particular organization/facility (Random target/Target of opportunity)

Attack Characteristics

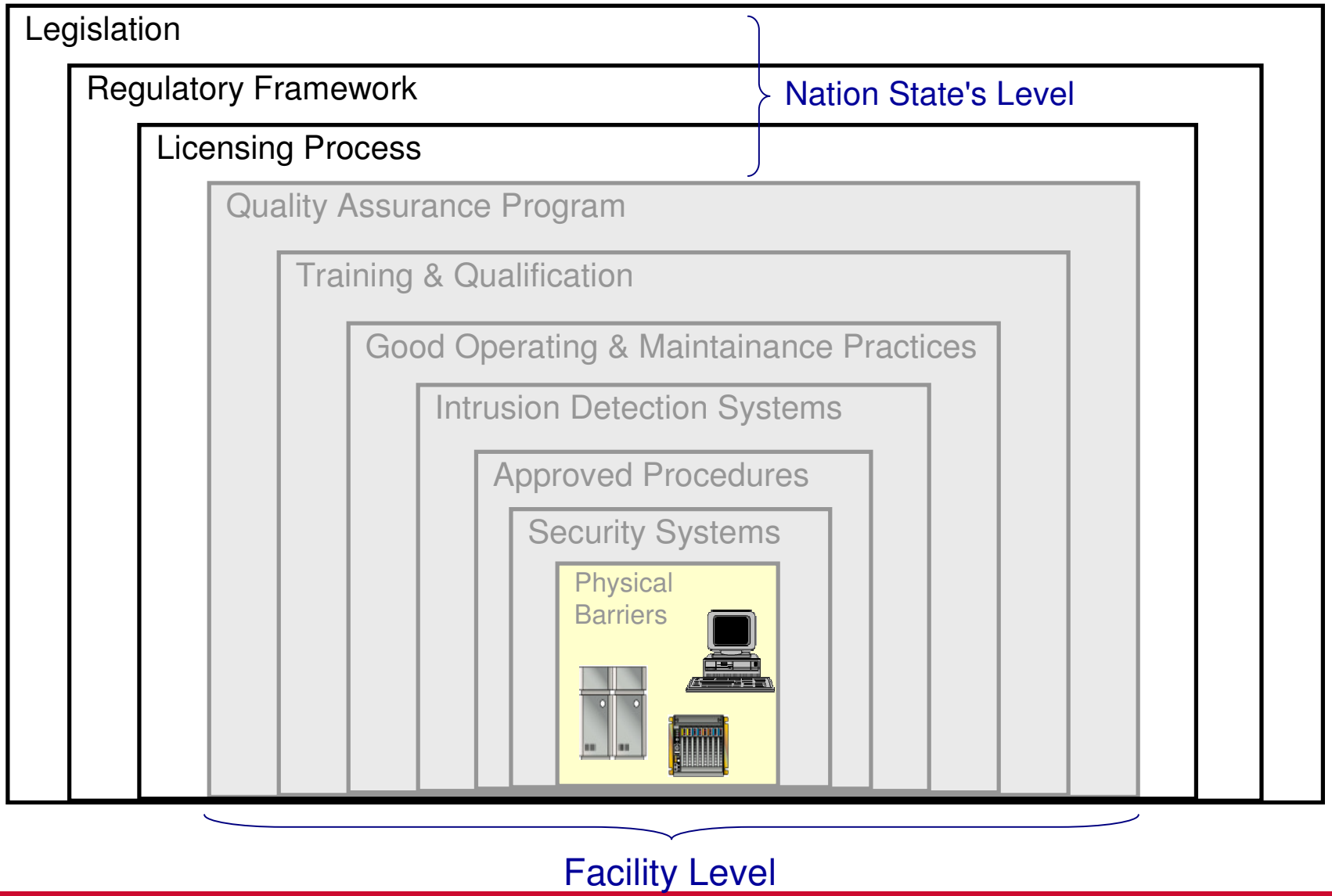


A Highly targeted: Military-style adversary (Threat is not understood)
B Targeted: Traditional adversary groups (Threat is basically understood)
C Untargeted: Everyone else (Threat is well understood)

A Highly targeted*: no prevention, advanced detection and response
B Targeted: extended prevention, advanced detection and resp.**
C Untargeted: standard prevention, detection and response

***State-of-the-art is definitely not be enough**
****State-of-the-art is most likely not be enough**

Nuclear Sector
Various Layers Of Defense And Protection



Technische Hochschule
Brandenburg
University of
Applied Sciences
Institute for Security
and Safety

Thank you for your attention!

g.gluschke@uniss.org
www.uniss.org