Civil Nuclear Power - The Cyber Security Perspective

Guido Gluschke

g.gluschke@uniss.org

Institute for Security and Safety (ISS)
at the Brandenburg University of Applied Sciences, Germany

Deutsche Physikalische Gesellschaft
AKE 11: Nuclear Energy and Security

Münster, 29 March 2017

Fachhochschule Brandenburg
University of Applied Sciences
Institute for Security and Safety

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 UN, OSCE, EU and NATO

Member of the Energy Expert Cyber Security Platform - Expert Group of the European Commission DG-ENERGY

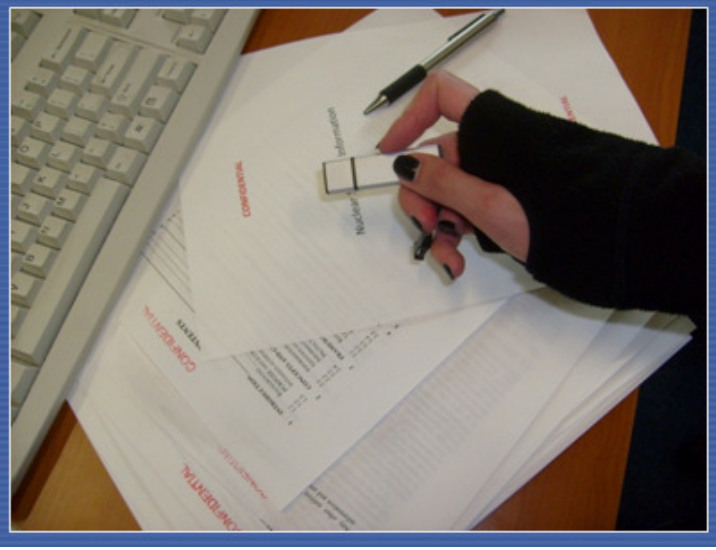
Past Chair of IAEA International Nuclear Security Education Network (INSEN)

Fachhochschule Brandenburg
University of Applied Sciences
Institute for Security and Safety

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:

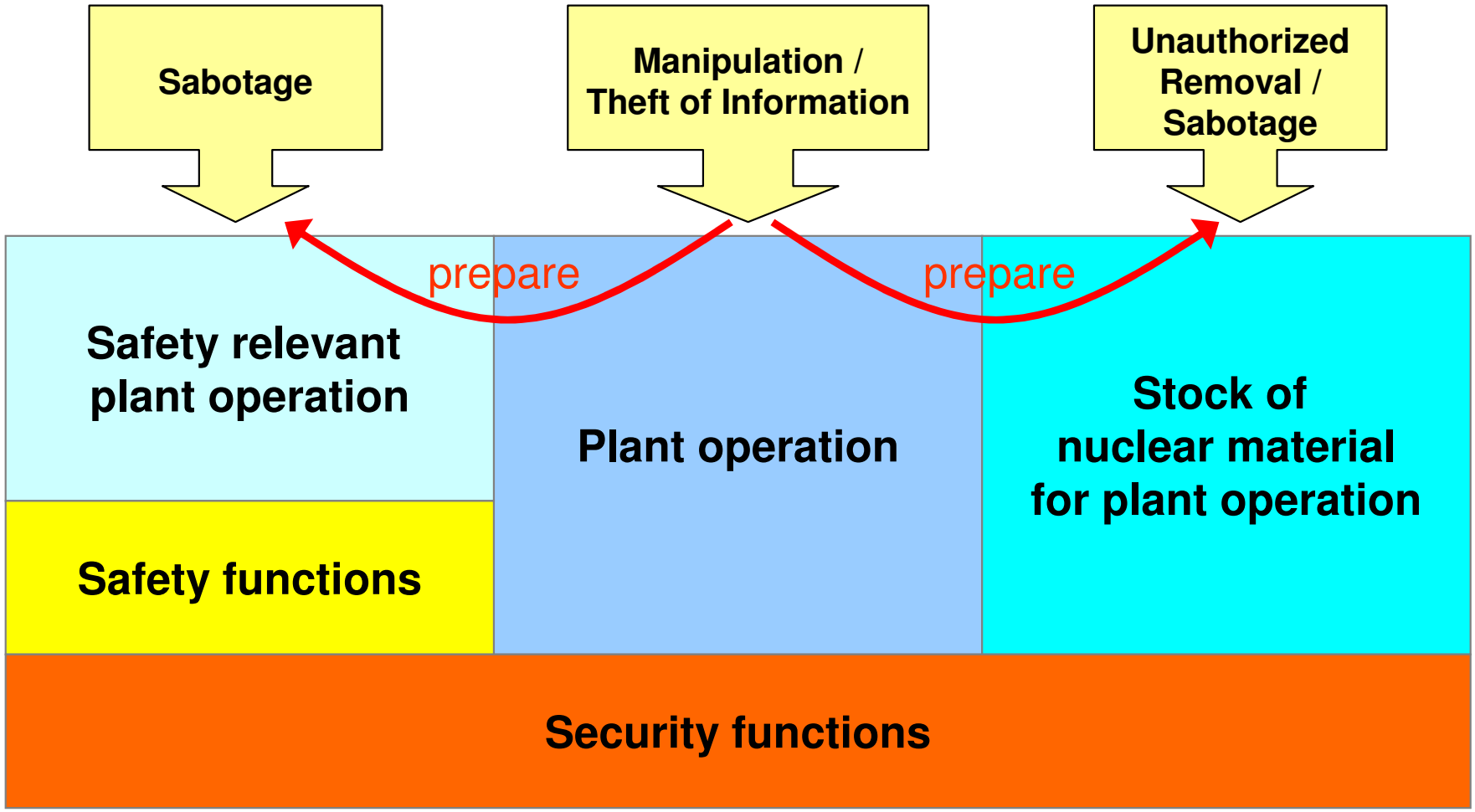
- ***unauthorized removal*** of nuclear/other radioactive material
- ***sabotage*** against nuclear material or nuclear facilities
- ***theft*** of nuclear sensitive information



IAEA

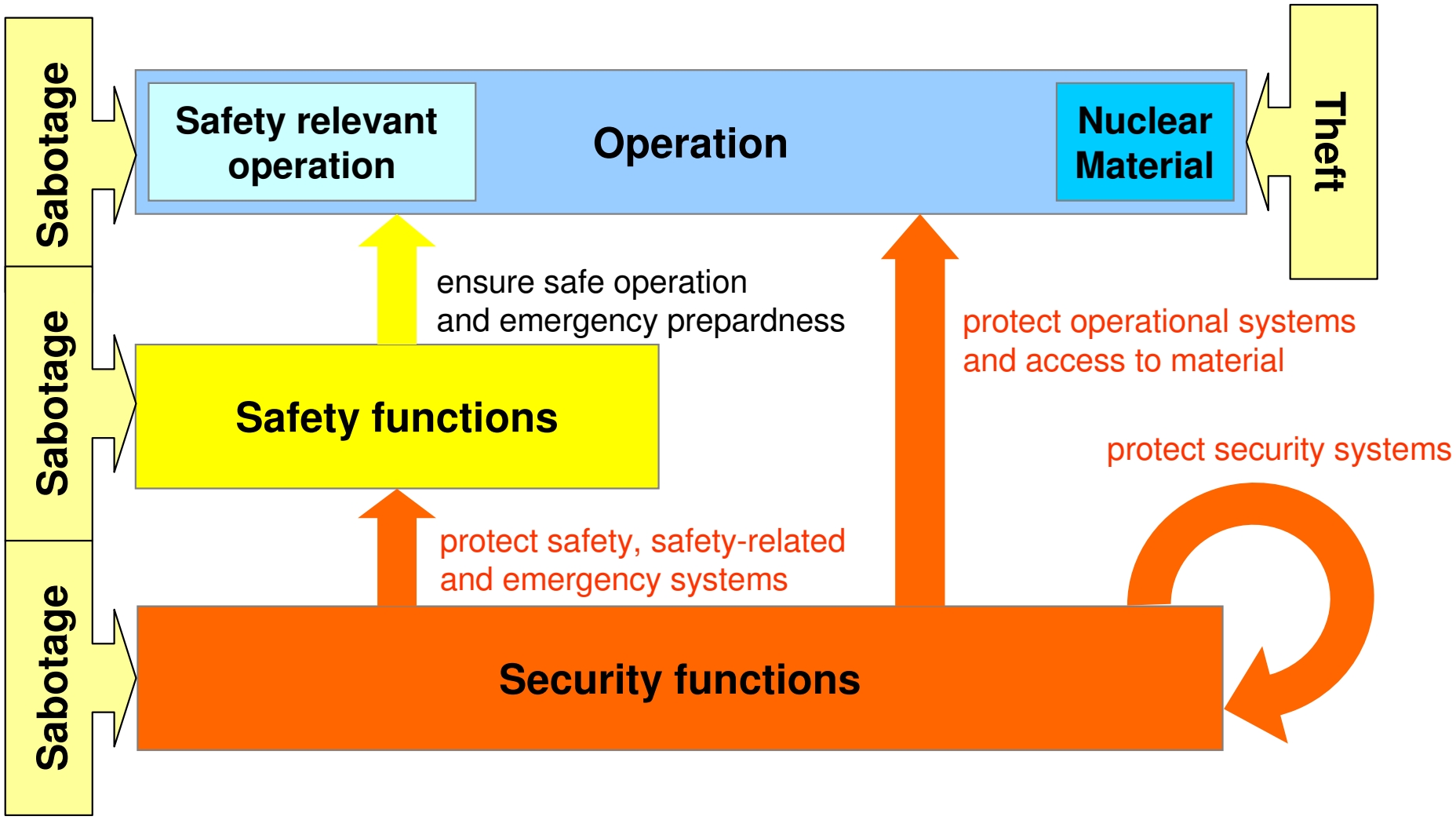
Fachhochschule
Brandenburg
University of
Applied Sciences
Institute for
Security and Safety

Protection Of A Nuclear Facility (NPP)



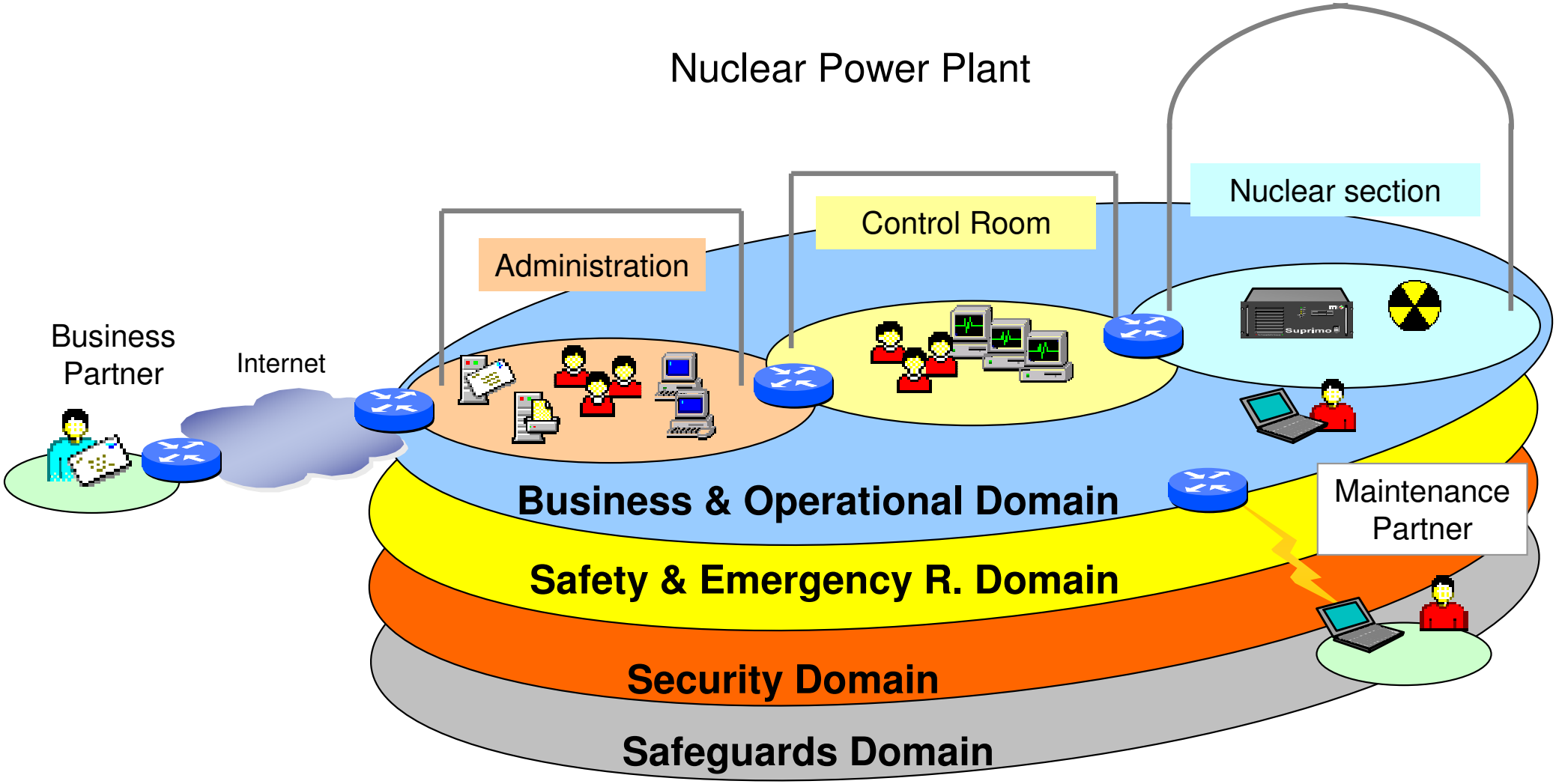
Fachhochschule
Brandenburg
University of
Applied Sciences
Institute for
Security and Safety

Protection of a Nuclear Facility



Fachhochschule Brandenburg
University of Applied Sciences
Institute for Security and Safety

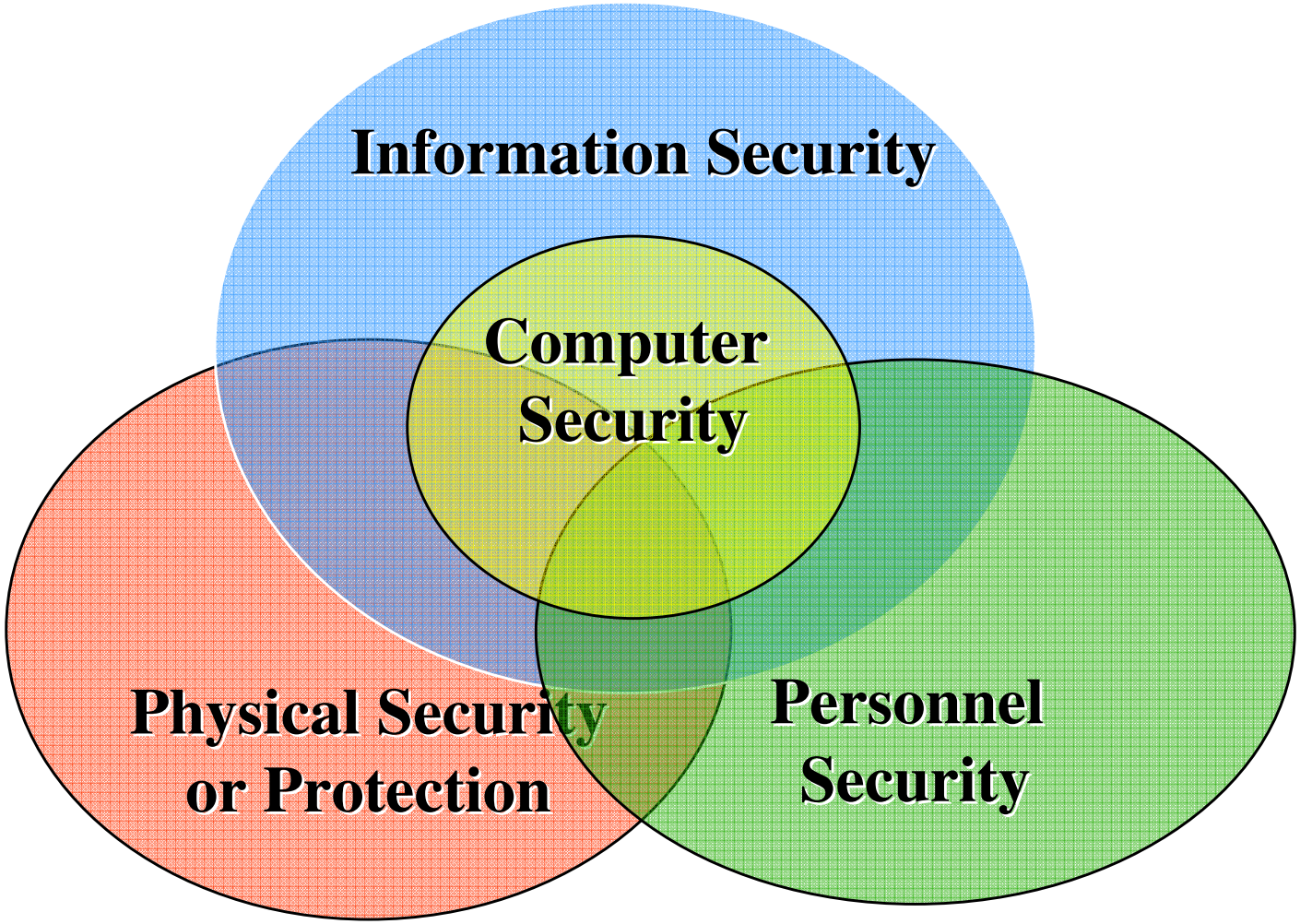
Computer Systems Supporting Nuclear Plant Domains



Fachhochschule Brandenburg
University of Applied Sciences
Institute for Security and Safety

Relationship Between Security Subdomains

Information and Computer Security are not isolated subdomains, but are interlinked with the other aspects of the security domain.



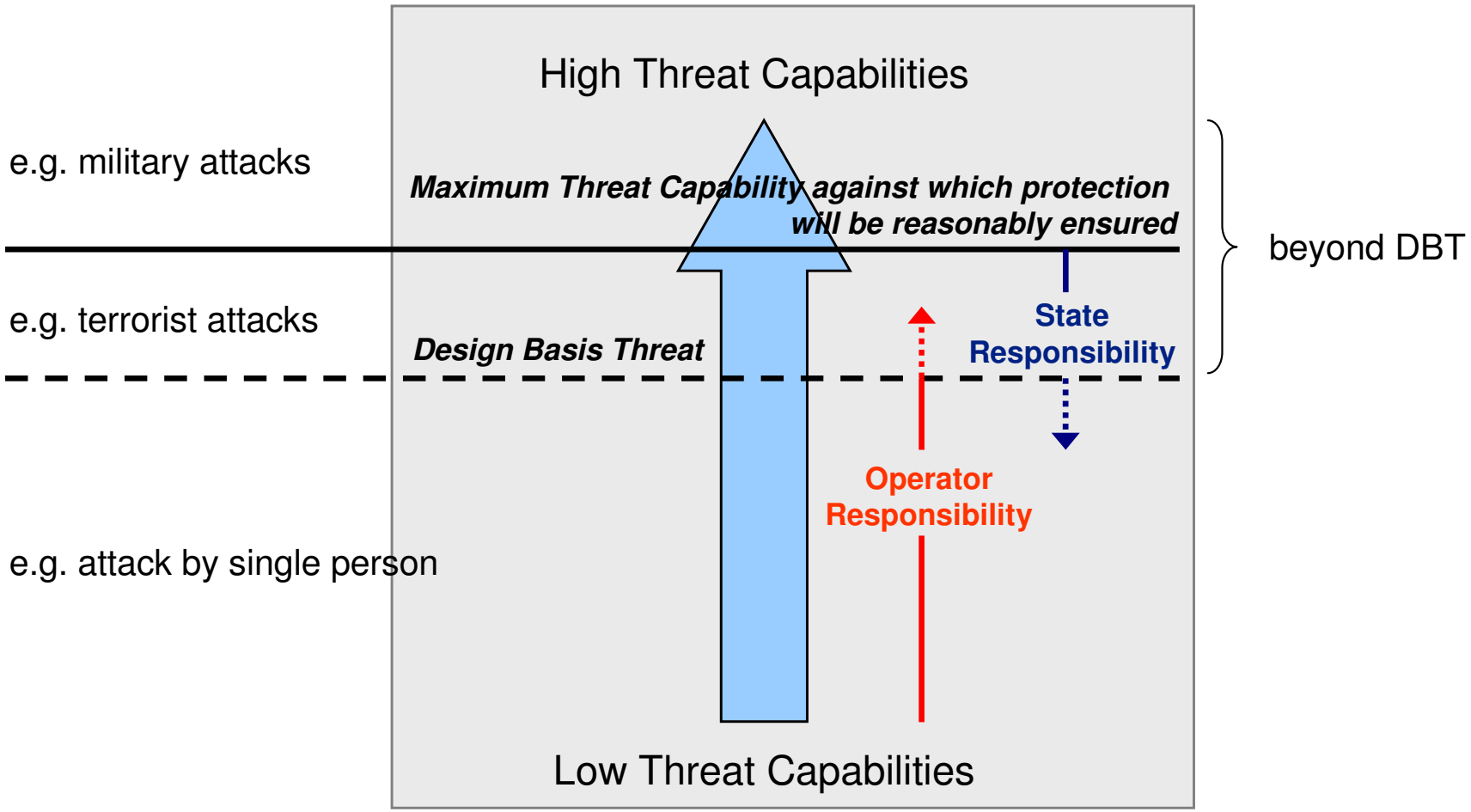
Fachhochschule
Brandenburg
University of
Applied Sciences
Institute for
Security and Safety

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

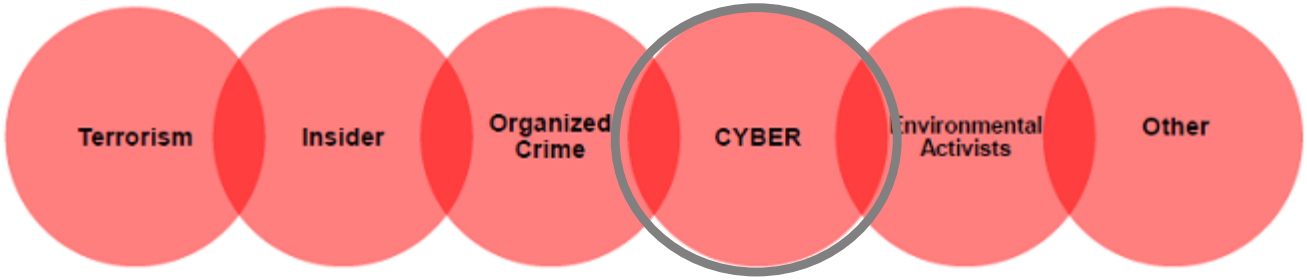
Fachhochschule Brandenburg
University of Applied Sciences
Institute for Security and Safety

IAEA Design Basis Threat (DBT) Model For Responsibilities

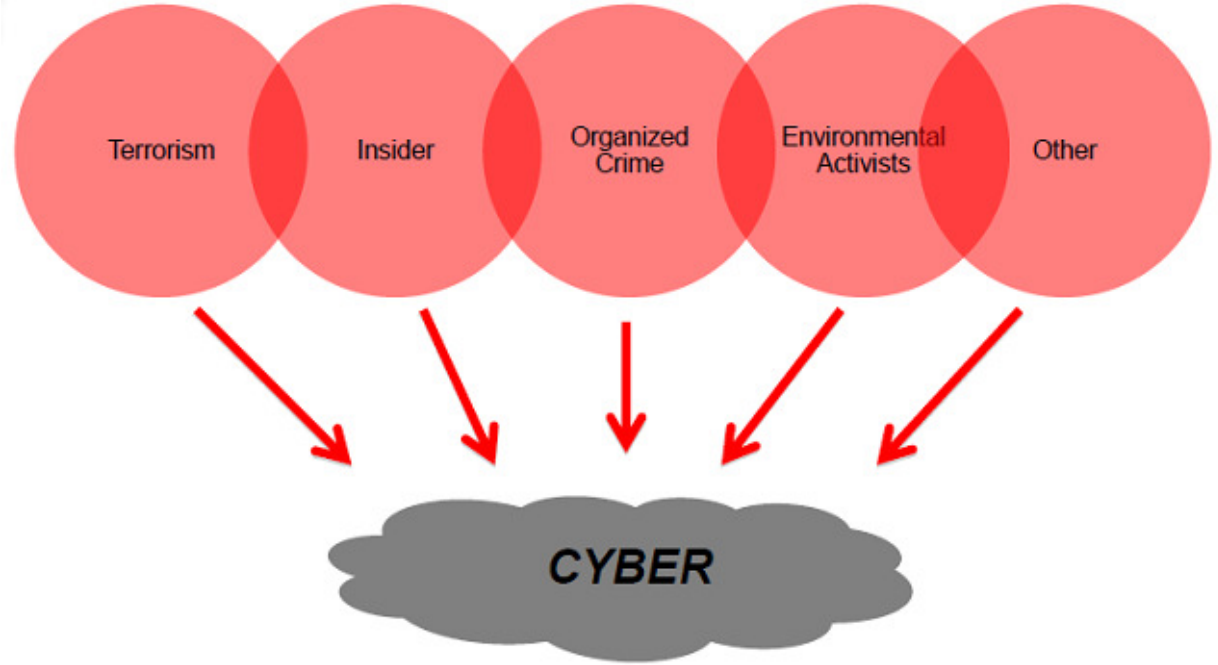


Fachhochschule Brandenburg
University of Applied Sciences
Institute for Security and Safety

How to handle cyber in DBT?



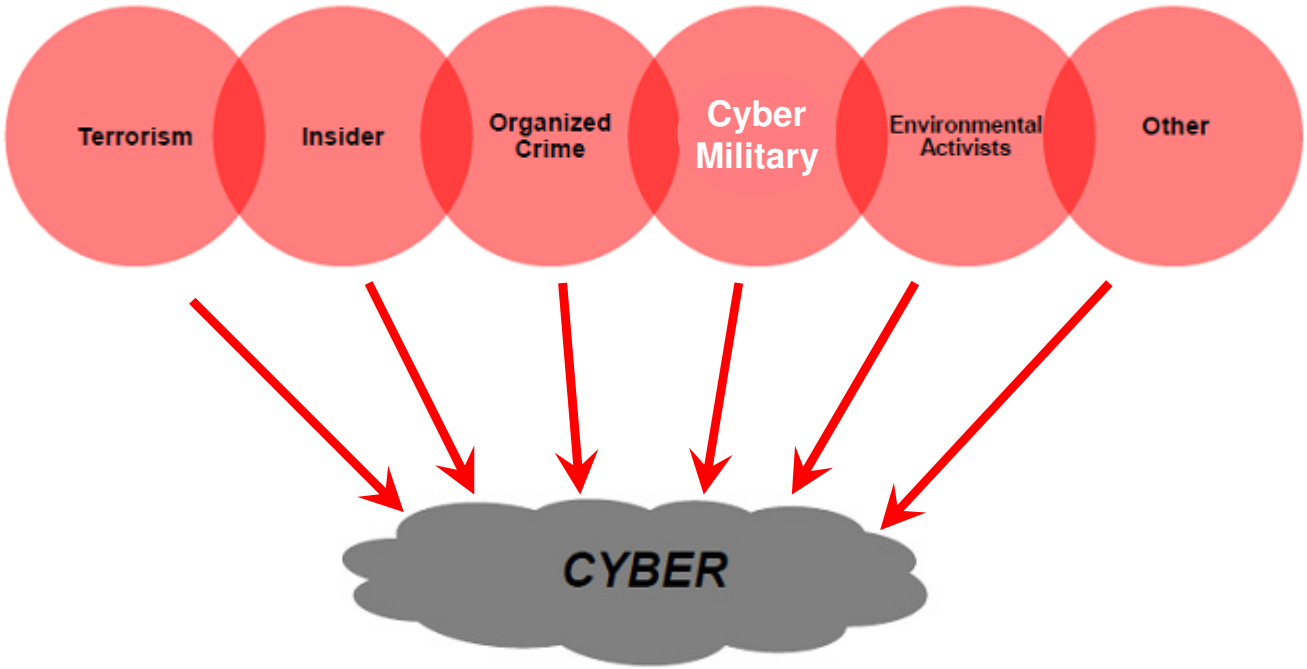
OR



Source: Michael Beaudette, WINS workshop Toronto March 2012

Fachhochschule Brandenburg
University of Applied Sciences
Institute for Security and Safety

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



Fachhochschule Brandenburg
University of Applied Sciences
Institute for Security and Safety

Military Threat Groups
The Nation State's Dilemma

In the western hemisphere military attacks against nuclear installations are typically beyond DBT

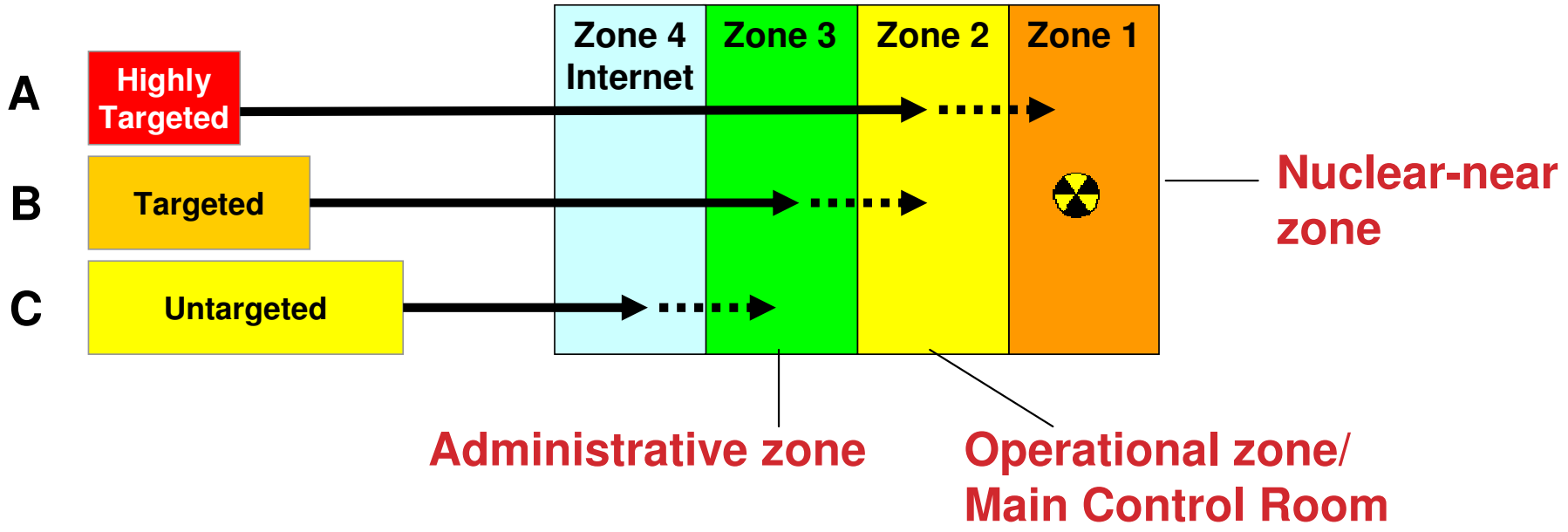
They are assigned to the nation state; in any case the licencee is not responsible for protecting his plant against this threats

This view can be argued by the following paradigms:

- Military weapons are controlled by nation-state
- Theft, as well as illigal movement, illigal import, or illigal use of military weapons should be detected/tracked by nation-state intelligence services
- In case of use, military activities has to be fended off by nation-states forces

Fachhochschule Brandenburg
University of Applied Sciences
Institute for Security and Safety

Simple Attack Model



A Highly targeted: Targeted against particular component/system[1]

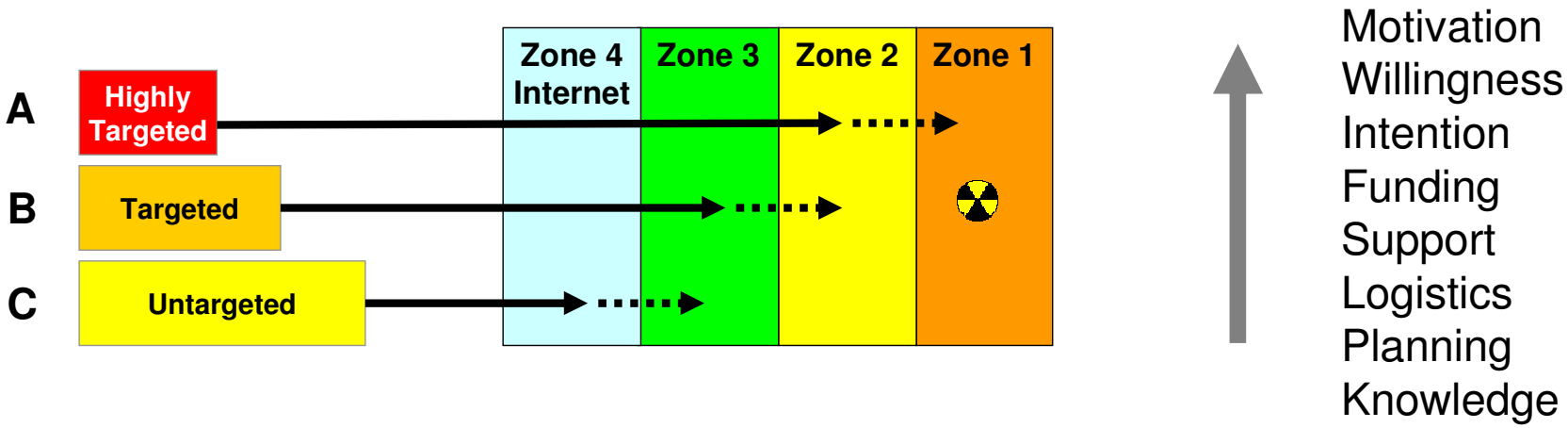
B Targeted: Targeted against particular organization/facility[2]

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

[1] e.g. The Stuxnet incident: see http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet
[2] e.g. The Monju incident: see https://www.contextis.com//resources/blog/context-threat-intelligence-monju-incident/

Fachhochschule Brandenburg
University of Applied Sciences
Institute for Security and Safety

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)

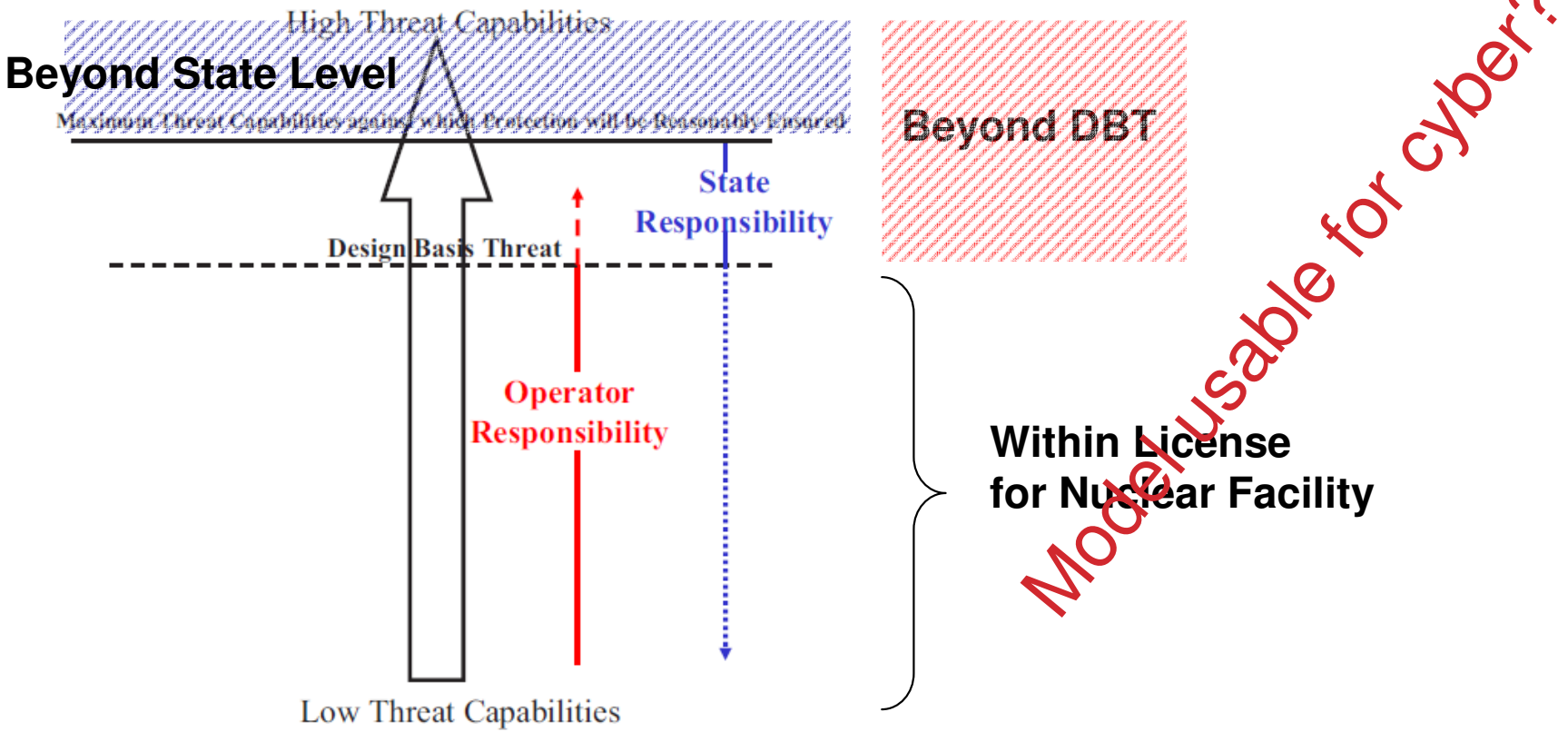
A Highly targeted*: no prevention, advanced detection and response
B Targeted: extended prevention, advanced detection and response**
C Untargeted: standard prevention, detection and response

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

Fachhochschule Brandenburg
University of Applied Sciences
Institute for Security and Safety

IAEA Model
Beyond DBT/Beyond State Level

- In the physical world 'physical threat bounderies' exists
  - There is always something more
- In general, understanding/definition of this limit is necessary, otherwise facilities have to shut down



Fachhochschule Brandenburg
University of Applied Sciences
Institute for Security and Safety

Limitations Everywhere In Cyber

We are as secure as possible from our perspective, considering our means and our knowledge.

- Limits of informatics, mathematics, physics
- Limits of human imagination and knowledge
    - Single point of failure, Common cause failure
- Limits of vendors and supply chain
    - quality limitation in implementation of hardware and software
    - trusted supply chain
- Limits of verification and testing
    - no error free software
- Limits of detection and response
    - limited technics for detection
    - limited capabilities, knowledge and experience

Fachhochschule Brandenburg
University of Applied Sciences
Institute for Security and Safety

Past Initiatives on Nuclear Cyber Security where ISS was involved in

IAEA Nuclear Security Series No. 17, Computer Security at Nuclear Facilities, IAEA Vienna, Mar 2011

NS 22 Computer Security for Nuclear Security Professionals, INSEN, Oct 2013

Cyber Security at Nuclear Facilities: National Approaches, Institute for Security and Safety, Potsdam, Jun 2015

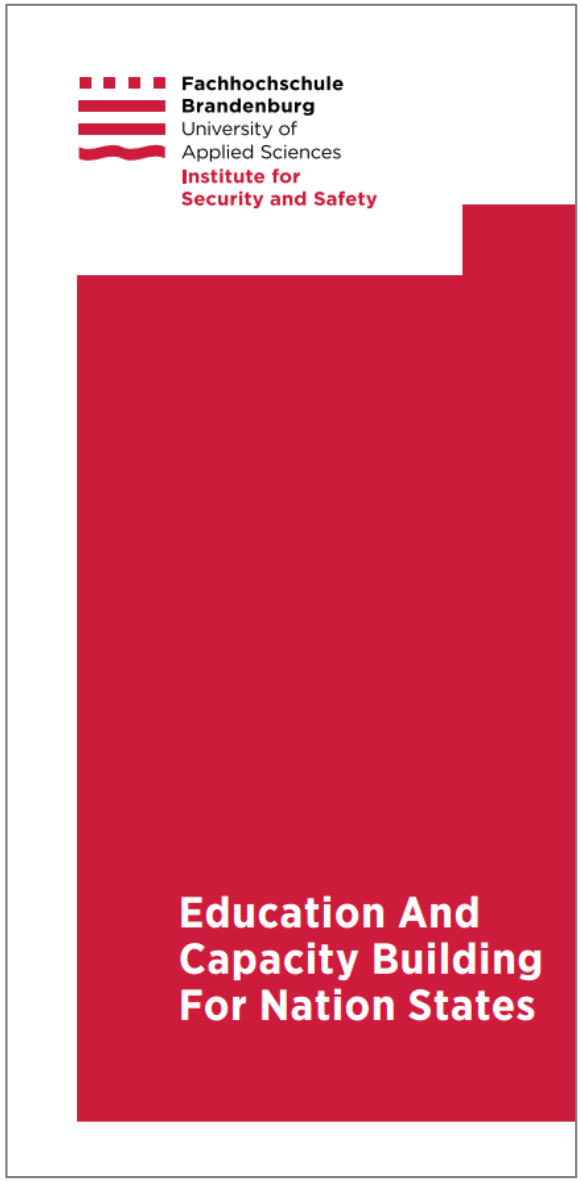
Cyber Security at Civil Nuclear Facilities: Understanding the Risks, Chatham House, London, Oct 2015

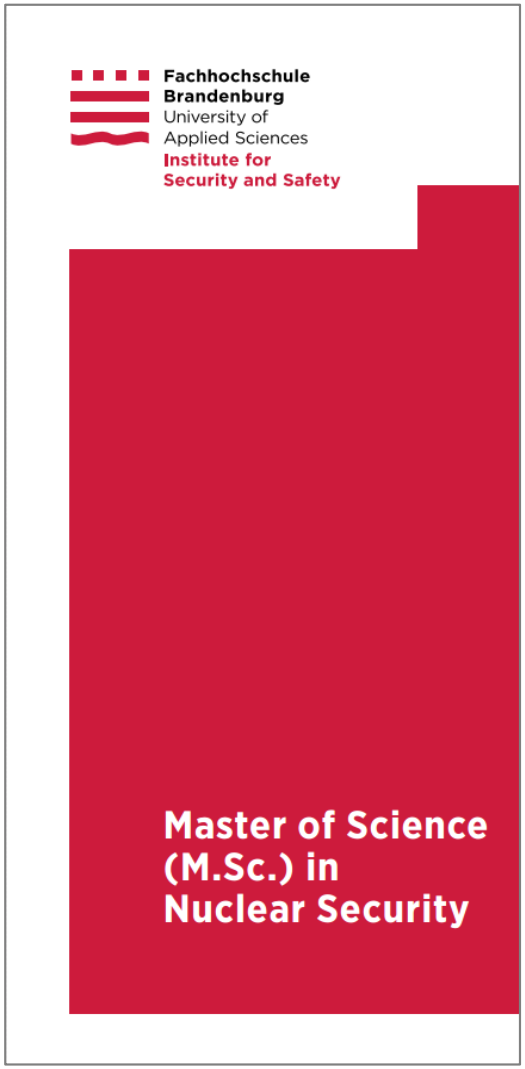
Outpacing Cyber Threats: Priorities for Cybersecurity at Nuclear Facilities, Nuclear Threat Initiative, Washington, Dec 2016

Cyber Security in the Energy Sector - Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector, European Commission, Brussels, Feb 2017

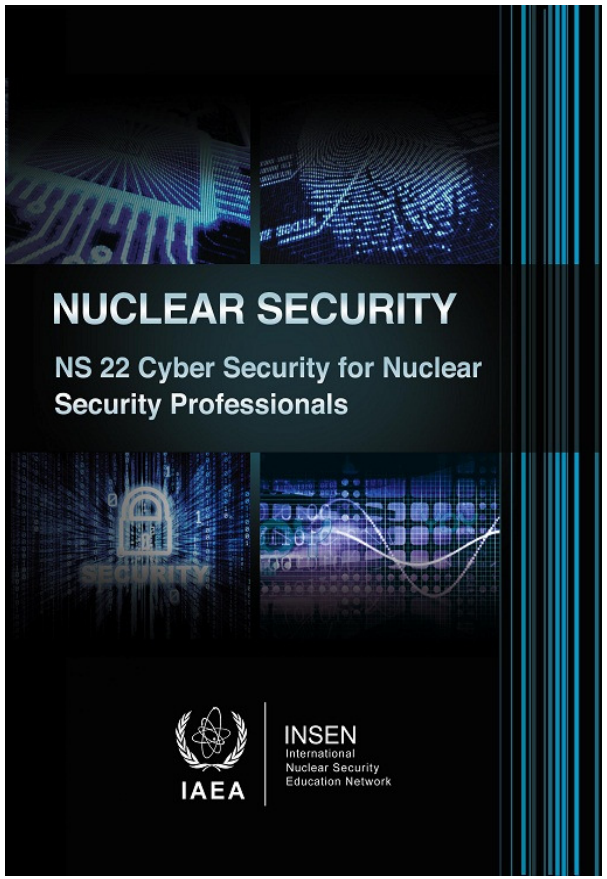
Fachhochschule Brandenburg
University of Applied Sciences
Institute for Security and Safety

Capacitity Building On Cyber And Nuclear Security





www.mins.study



Developed by
Institute for Security and Safety
at the Brandenburg University
of Applied Sciences
together with the IAEA.

Fachhochschule Brandenburg
University of Applied Sciences
Institute for Security and Safety

New ISS Development: 3D-Models For Security Education

Thank you for your attention!

Guido Gluschke

g.gluschke@uniss.org

Institute for Security and Safety

www.uniss.org