NEW NP

IAEA International Atomic Energy Agency

International Conference on Physical Protection of Nuclear Material and Nuclear Facilities

13-17 November 2017, Vienna

Deterring, Protective, Delaying And Detective Application Security Controls For Nuclear Facilities

Ms. Deeksha Gupta

AREVA GmbH, Erlangen, PhD Candidate

Ms. Xinxin Lou

Bielefeld University, PhD Candidate

Mr. Mathias Lange

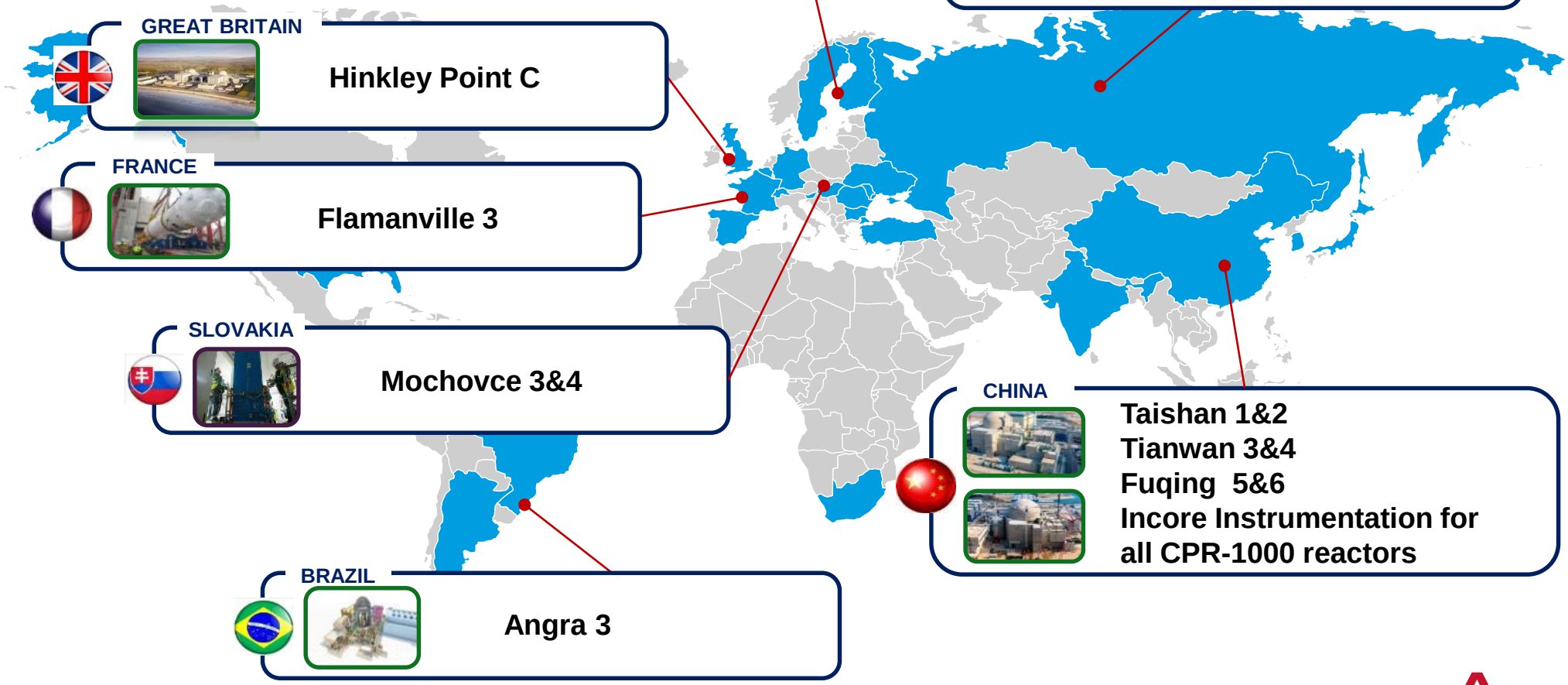
Magdeburg-Stendal University of Applied Sciences, Institute of Electrical Engineering, Magdeburg

Dr. Karl Waedt

AREVA GmbH, Erlangen

AREVA

Our Main Projects..



FINLAND

Olkiluoto 3

RUSSIA

Novovoronesh II 1&2
Leningrad II 1&2

GREAT BRITAIN

Hinkley Point C

FRANCE

Flamanville 3

SLOVAKIA

Mochovce 3&4

CHINA

Taishan 1&2
Tianwan 3&4
Fuqing 5&6
Incore Instrumentation for all CPR-1000 reactors

BRAZIL

Angra 3

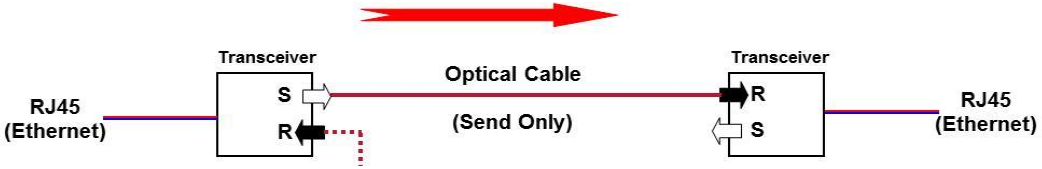
AREVA

Our Portfolio in Security..

… Monitoring Equipment, e.g. SIPLUG with newest Industry 4.0 **Interoperability**

➔ **OPC Unified Architecture**

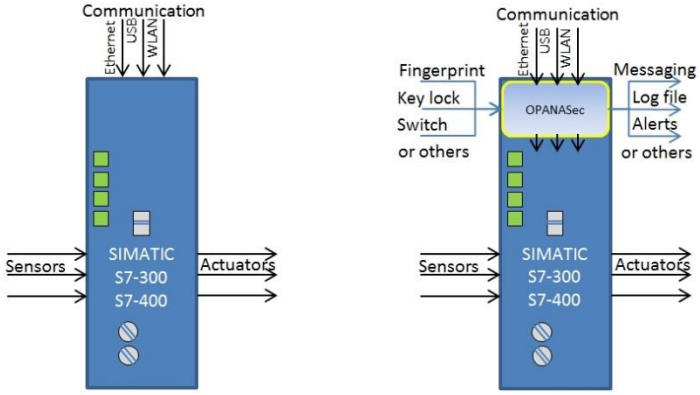
… Optical **Data Diodes**



… Customized Nuclear & **Industrial Security** Offers

Consulting	Products & Solutions	Services
ISMS: ISO/IEC 27000	Automation Security	Threat Analysis
Security Simulations	Application Normative Frameworks	Implementation of Countermeasures
Audit Support	Physical Protection	System Hardening
Awareness Trainings	Forensic Readiness	Surveillance & Tests
…	…	…

… **OPANASec** protection for **SCADA**



… Cybersecurity R&D

…

AREVA NP

AREVA

Outline

AREVA

IAEA International Atomic Energy Agency

Introduction

Outline

1. Introduction
2. Security Controls
3. Security Controls Model
4. 3D Modeling of Physical Components
5. Summary

AREVA

Introduction
Types of Security Controls

- **Security controls are applied:**
  - **To meet the main focus of security: availability and integrity**
  - **To minimize the risk of physical and cyberattack to the facility**

- **Main types of security controls:**
  - **Administrative**
    - e.g., risk management, personnel security, and training
  - **Technical**
    - hardware or software components
  - **Physical**
    - fencing, lightning, doors, locks and security guards etc.

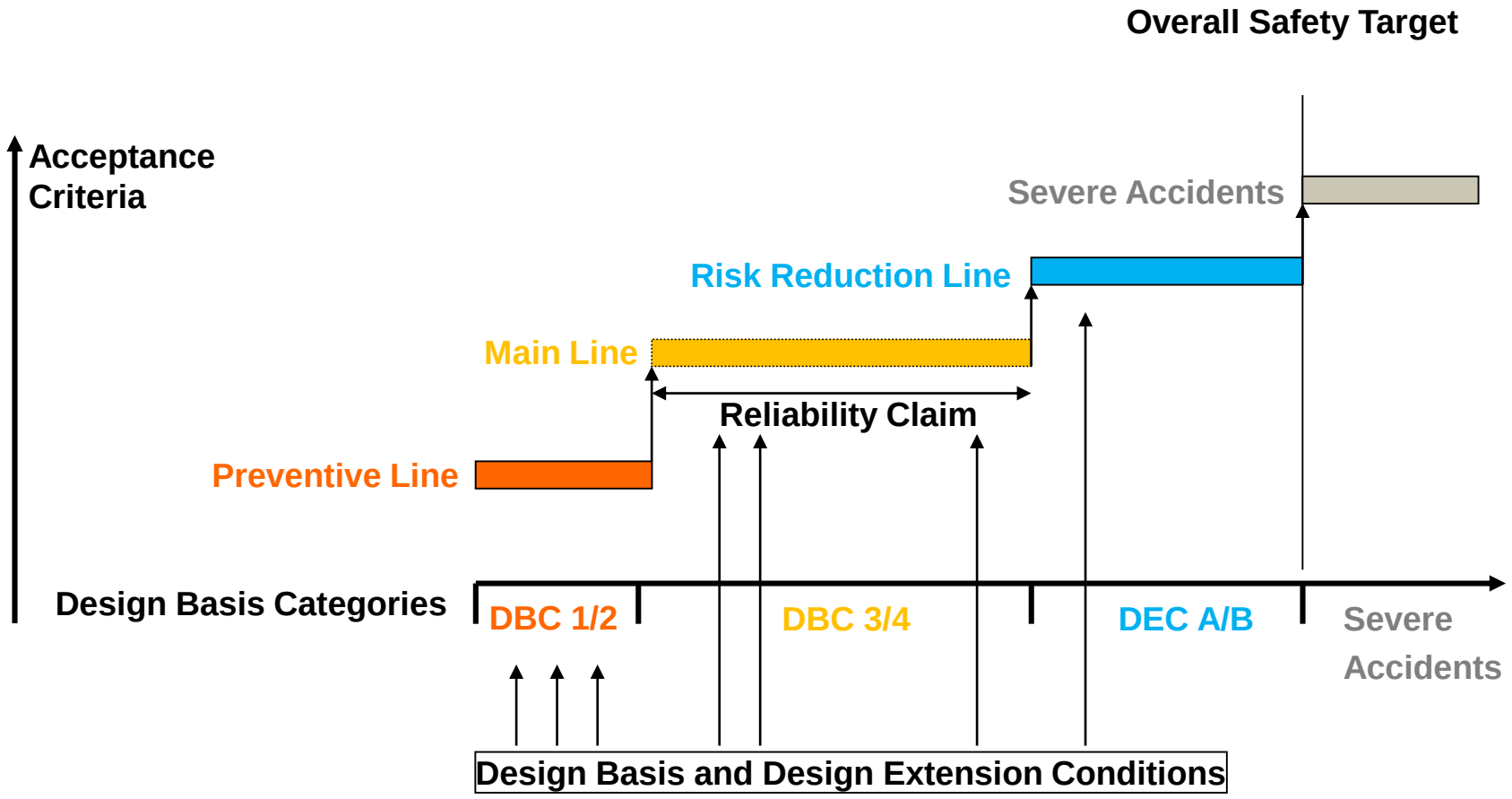
Introduction
Scope of Security Controls

- **Preventive Controls** can be subdivided into:
  - **Deterring**
    - harder for attacker to come close to the target
  - **Protective**
    - strong protection,
    - e.g., unidirectional security gateway (data diode)
  - **Delaying**
    - login protected with a password
    - delay in second attempt of password
- **Detective Controls**
- **Corrective Controls**

Safety Defense-in-Depth (Safety DiD) and Security Defense-in-Depth (Security DiD)

- **Safety DiD**
  - Derived from Nuclear Safety Objectives
  - Traditionally considered in line with the Safety Culture
- **Security DiD**
  - Derived from Physical Security and Cybersecurity Objectives
  - Basis for the Security Zone Model and Grading of Security Controls

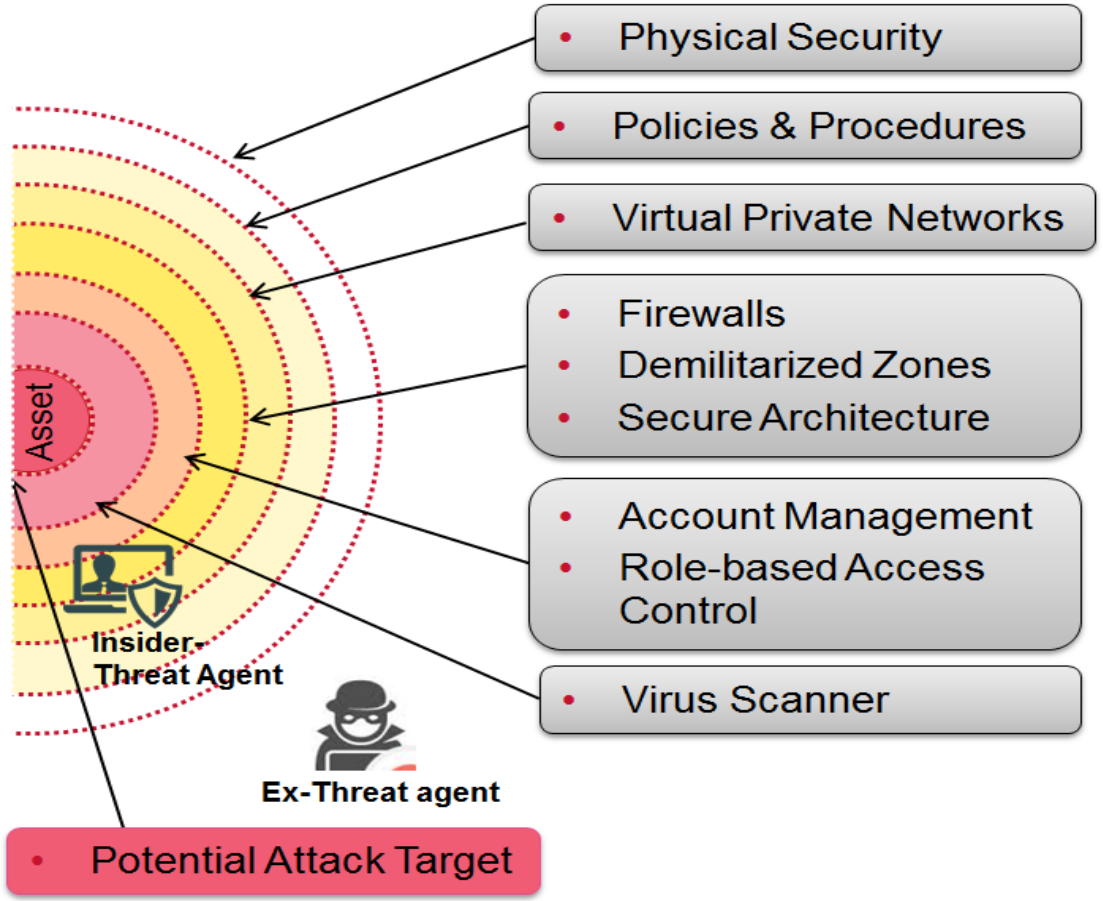
Safety Defense-in-Depth



Security Defense-in-Depth

- **Security controls should be placed to provide a security defense-in-depth**

→coordinated use of multiple security controls in a layered approach



Security defense-in-depth
Domain Based Security (DBSy) Grading

Defend (L3)

Detect & Resist (L2)

Deter (L1)

Be aware

AREVA

Security Defense-in-Depth

Preventive

- **Protective:** to assure the protection of an asset from an assumed specific security threat
- **Deterrence and delay:** to avoid the attack or at least delay that for long enough to counter act

Detective

- **Detection of attacks:** initially those that were not deterred, but may include attempts at attacks
- **Assessment of attacks:** to find out the nature and severity of the attack. For e.g., the number of false passwords entry

Corrective

- **Communication and notification:** to make aware responsible authorities and/or computer systems from the attack in a timely manner
  - **Network and system management play an important role in this work**
- **Response to attacks**: involves the actions by responsible authorities and computer systems to minimize the effect of an attack in a timely manner

IAEA International Atomic Energy Agency

Security Controls

Outline

1. Introduction
2. Security Controls
3. Security Controls Model
4. 3D Modeling of Physical Components
5. Summary

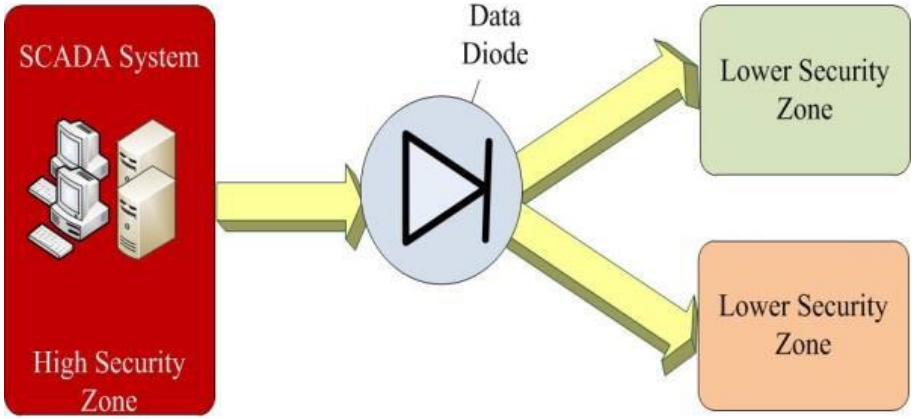
AREVA

Preventive Controls

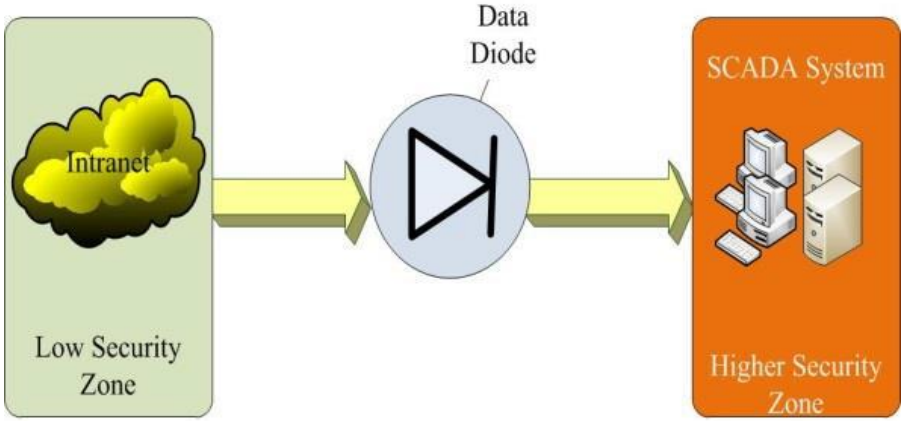
- **To block an intruder from successful penetration of a physical security control of the facility**
- **Example:**

  security guard, security awareness training, video surveillance, firewall, Biometric access control, antivirus software, etc.

  - **Example of protective Control:**



(a) Data Diode (High Security to Low Security Zone)



(b) Data Diode (Low Security to Higher Security Zone)

AREVA

Detective Controls

- To increase the protection from any malicious act by monitoring the activities
- Do not stop any malicious act to happen
- Detective Controls identify and log them
- Early detection of a malicious act enables a quick response
- Effectiveness of the security controls defined by probability of detection
- Examples:
  - Logging, e.g. card reader indication,
  - video surveillance (assuming appropriate lighting), alarms,
  - intrusion detection systems identifications, etc.

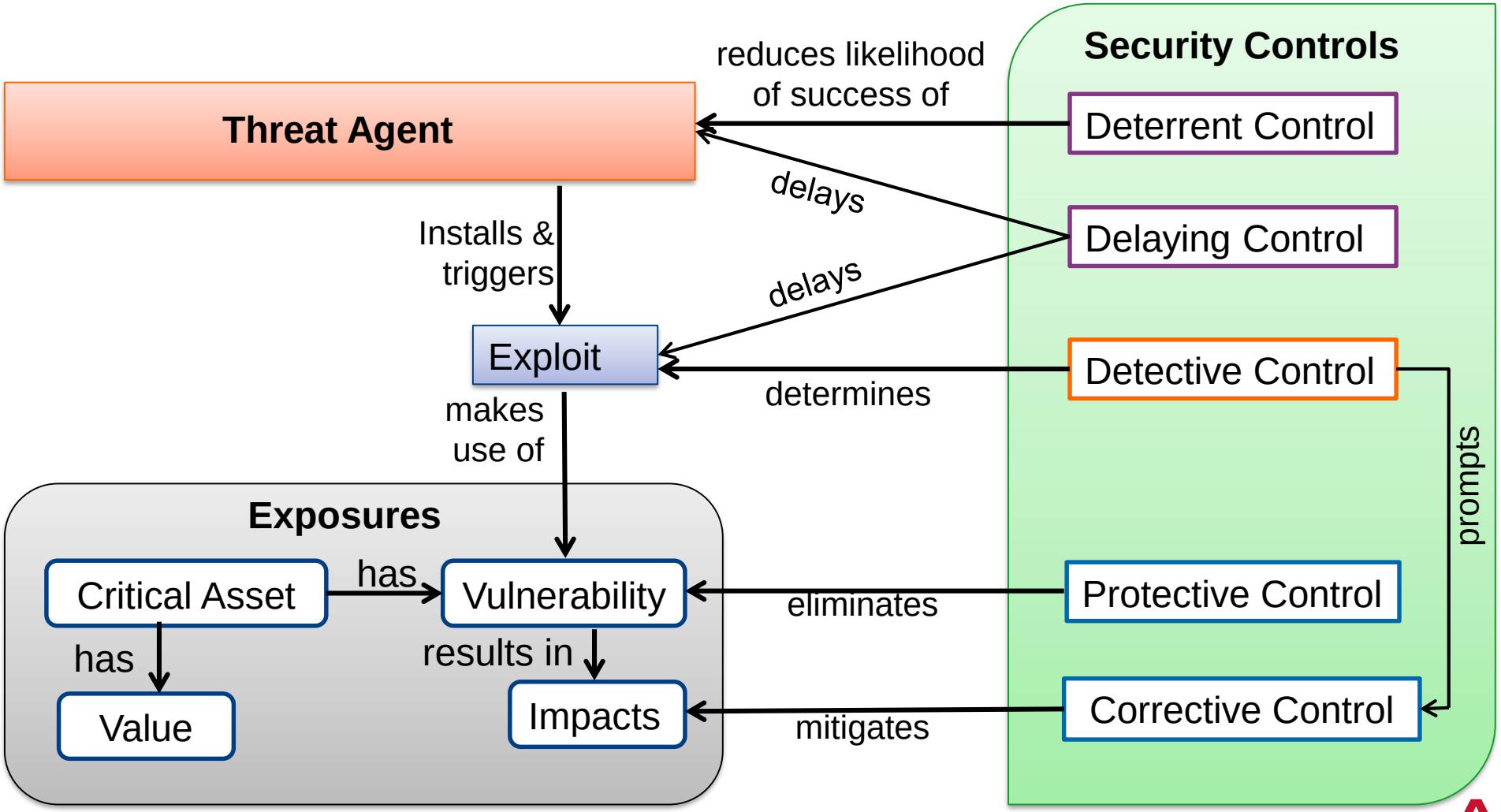
IAEA International Atomic Energy Agency

Security Controls Model

Outline

AREVA

Security Controls Model



IAEA International Atomic Energy Agency

3D Modeling of Physical Components

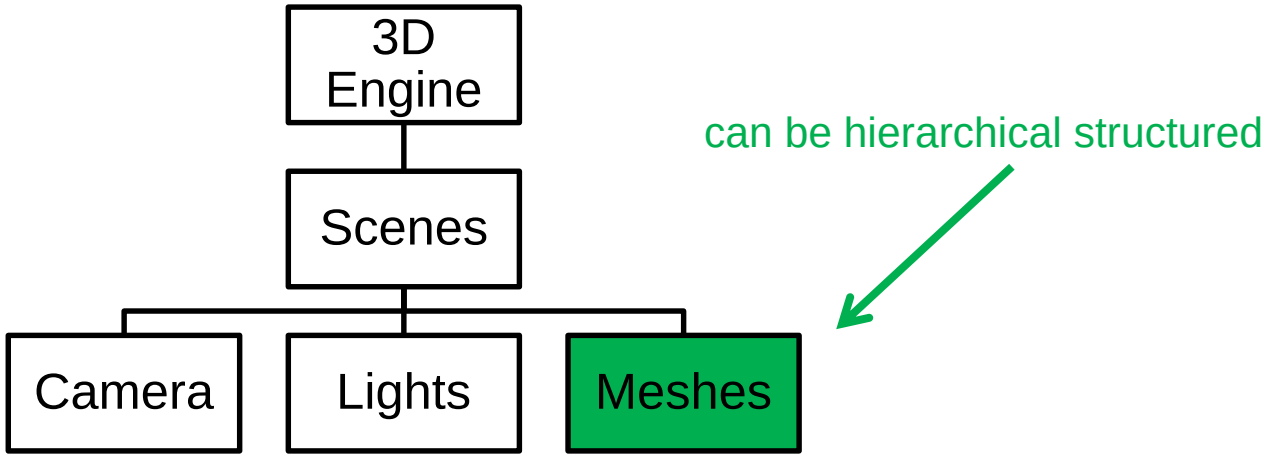
Outline

1. Introduction
2. Security Controls
3. Security Controls Model
4. 3D Modeling of Physical Components
5. Summary

AREVA

Principle of 3D Modeling

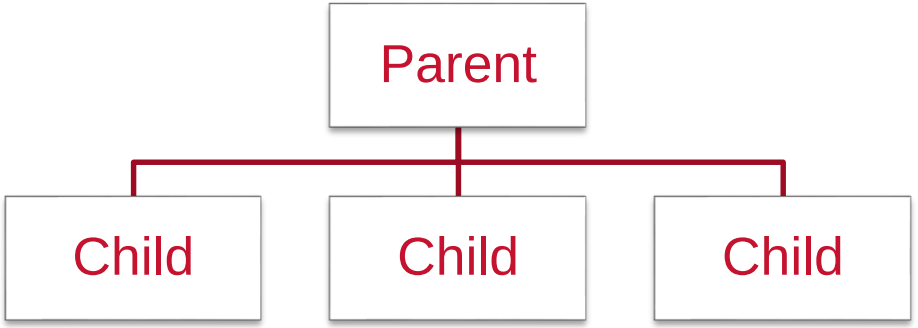
- 3D models represent virtual images with a internal hierarchical structure
- To develop a 3D model, a modeling tool with a 3D engine is required
- The 3D engine can manage multiple scenes
- A scene consists of one camera, a certain number of lights and several meshes
- The meshes represent a 3D model



Principle of 3D Modeling

- **The hierarchical structure helps to organize the 3D objects/ meshes**
- **And should base on a graph with parent-child relationships:**

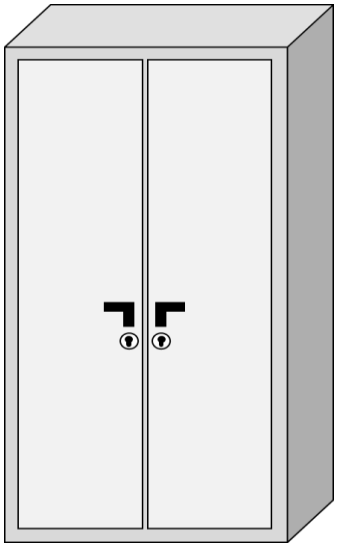
- Each node has:
  - one parent
  - array of children

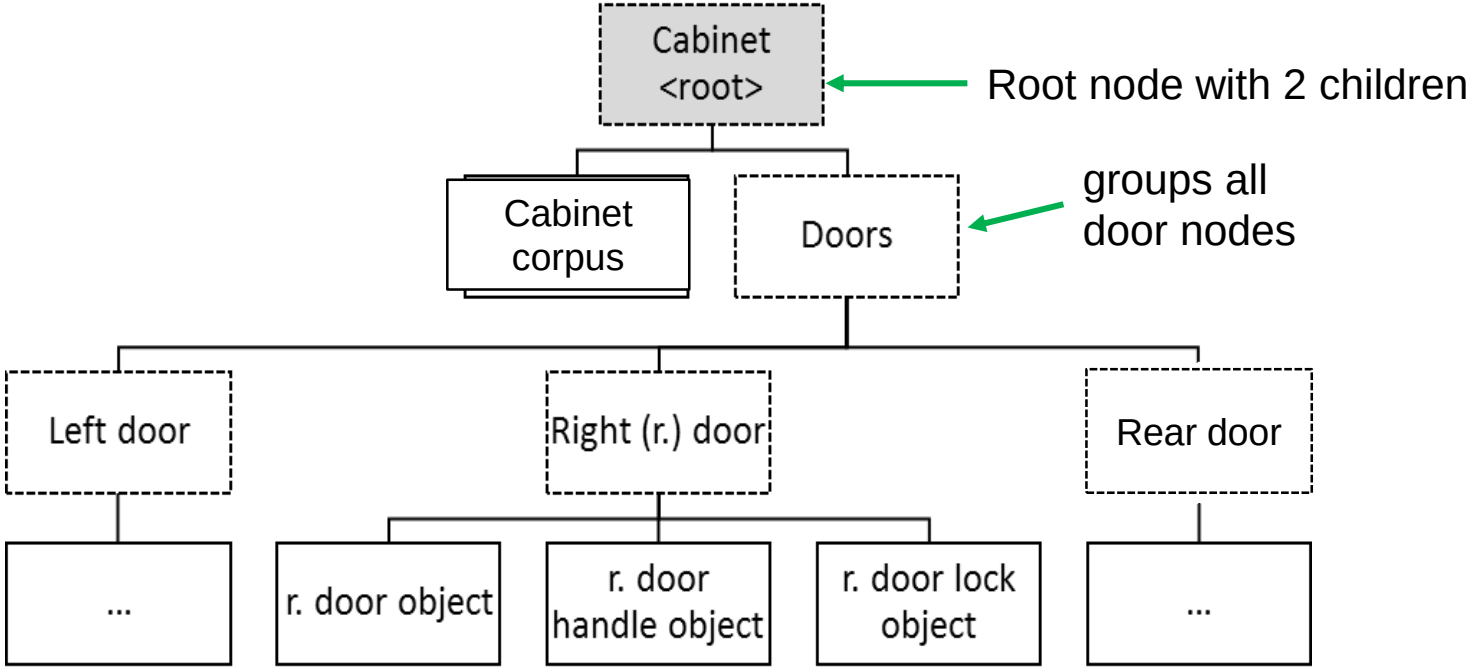


- Each child can be:
  - a single 3D Object
  - another node

=> This structure is going to help us to identify security zones and to place the security controls. *(Later more)*

1. Physical asset modeling: Cabinet example





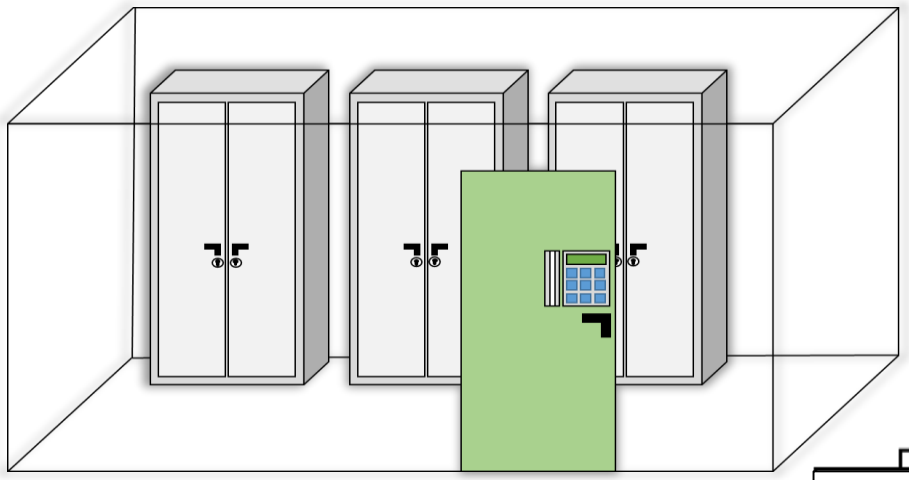
Legend:

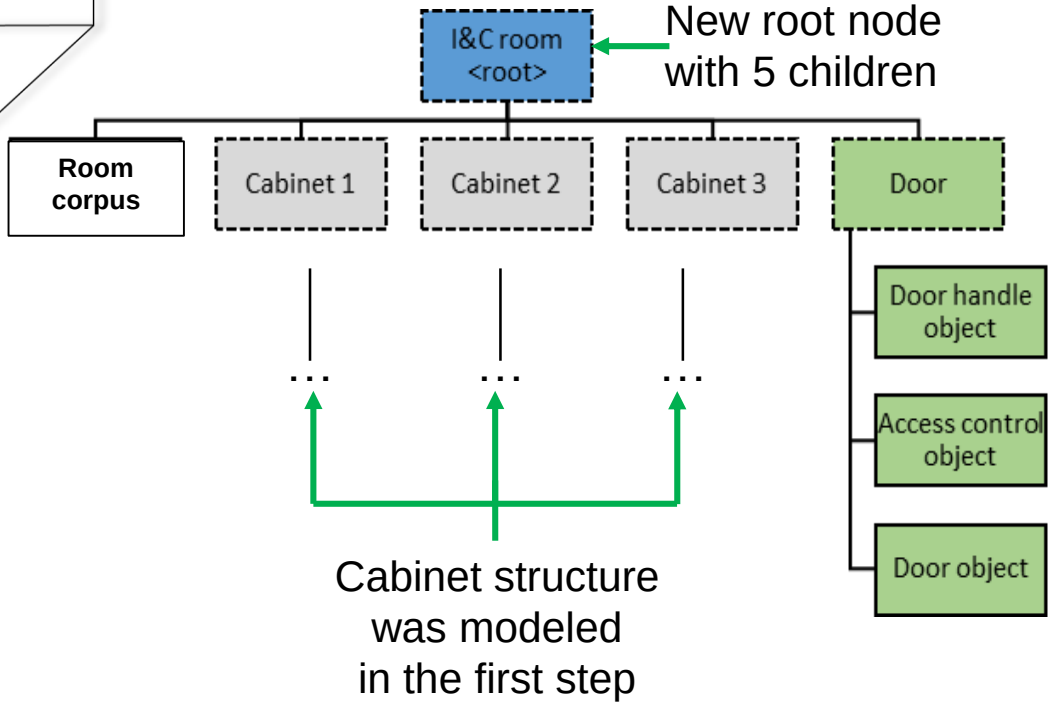
Node

3D Object

AREVA

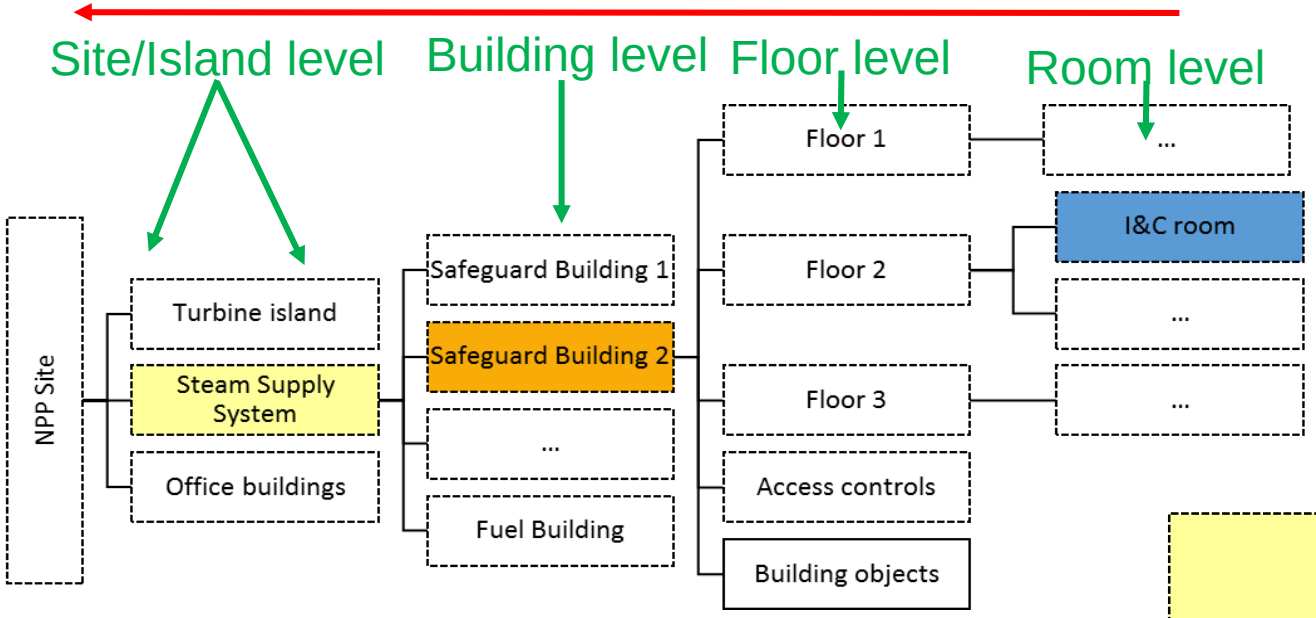
2. Room modeling: I&C room example

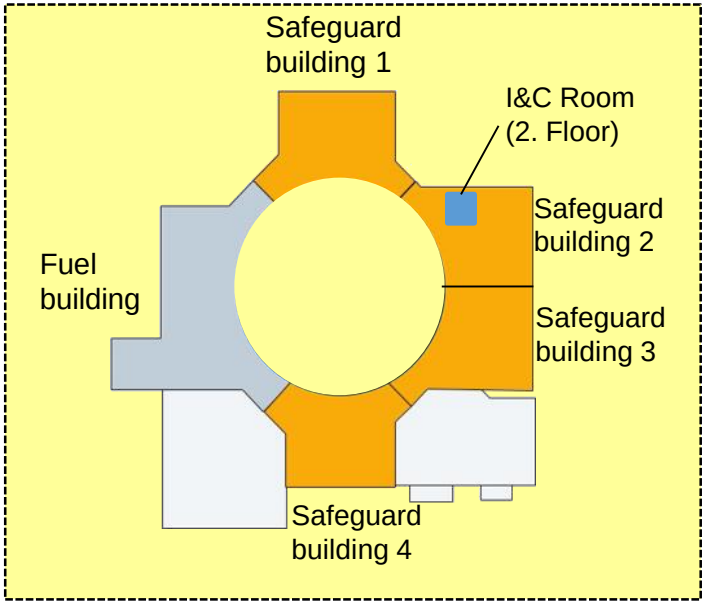




AREVA

3. Floor -> 4. Building -> 5. Site/Island Modeling





AREVA

AutomationML

- **The 3D Model with the hierarchical structure must also be stored persistently**
- **AutomationML (IEC 62714-x) is a exchange format for plant engineering information and allows to store:**

	Data Format	Standard
Geometry/ 3D data	COLLADA	*coming soon*
Kinematic data	COLLADA	*coming soon*
Logic data	PLCopen	IEC 61131-x
Topology/ Hierarchical structure	CAEX	IEC 62424

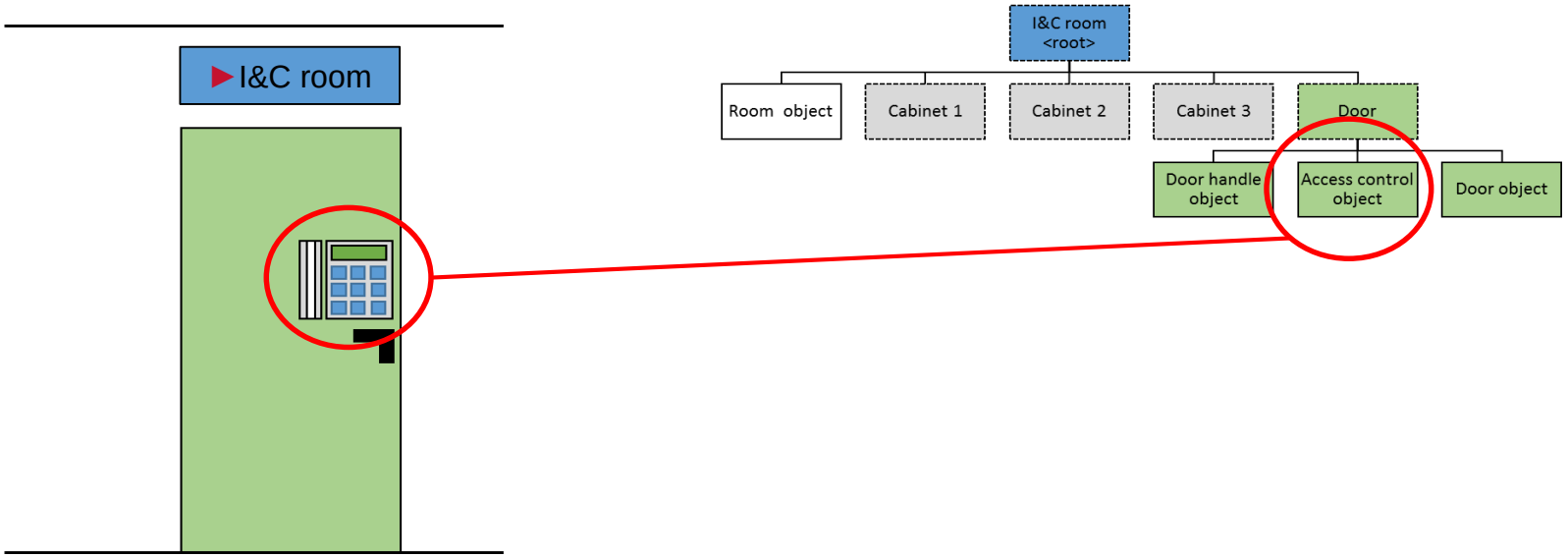
of single components or of a complete site.

- **AutomationML supports the combination of physical models with logical models**

(For example: To combine the physical zones with the logical zones)

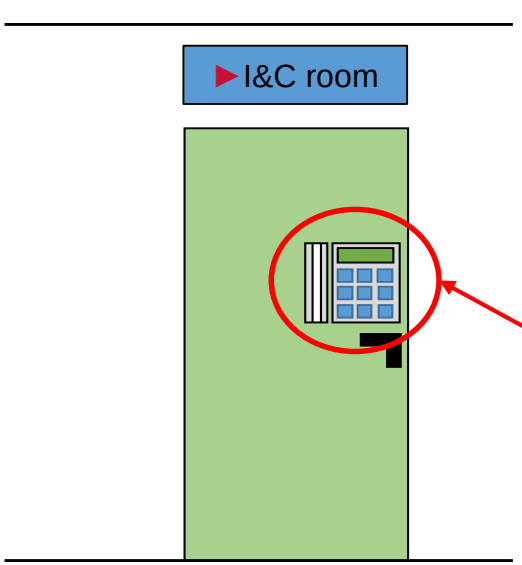
Linking Security Controls

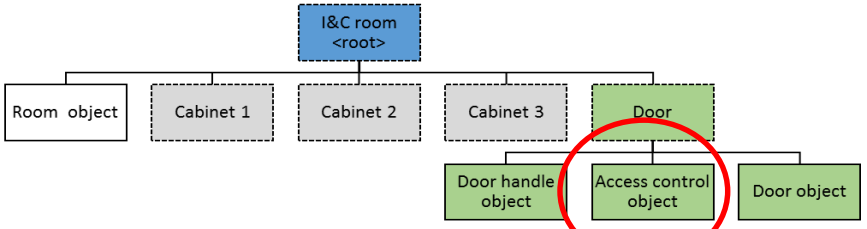
- The security relevant assets should be protected by security controls
- By developing a 3D Model with a hierarchical structure, the security controls can be placed at their effective position



Linking Security Controls

- The security relevant assets should be protected by security controls
- By developing a 3D Model with a hierarchical structure, the security controls can be placed at their effective position
- To assure the correct implementation, the security controls are linked to the description and implementation guidance from IEC 62443-x-x and ISO/IEC 27002:2013





ISO/IEC 27002:2013

11.1.2 Physical Entry Controls

b) Access to areas where confidential information is processed or stored should be restricted to authorized individuals only by implementing appropriate access controls, e.g. by implementing a two-factor authentication mechanism such as an access card and secret PIN.

Linking Security Controls

- **Implementation of the persistent linking:**
  - **The general security standards like ISO/IEC 27002:2013 are hierarchically structured**

The Standards can be modeled as XML elements or JSON objects.

- **Each section of the standard should get a unique ID for the linking**

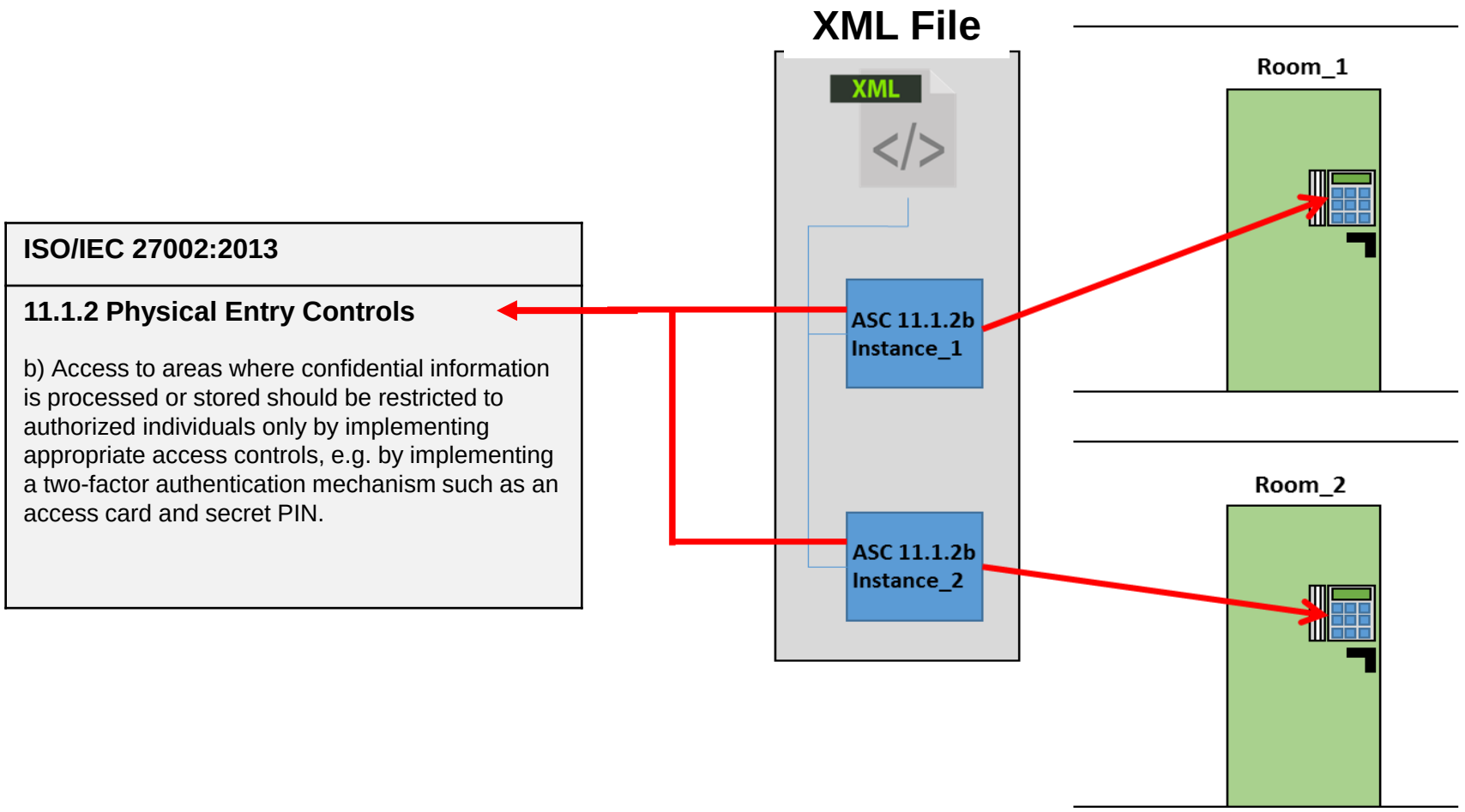
Implementation of persistent linking

- **The 3D Model is also hierarchically structured by the modeling procedure**

The file format for the 3D models is typically also based on XML

- **By modeling the 3D models with a graph, each 3D object should also get a unique ID for the identification**

Implementation of persistent linking



Summary

Outline

Summary

- Deterring, protective and delaying controls are comprised as preventive security controls [New IEC 63096]
- Strong preventive security controls is very important in the nuclear domain
- Strong protective controls, e.g., data diodes, effectively prohibit an attack
- Where strong protective security controls cannot be applied:
  - Deterring and delaying controls will add an additional layer of Security DiD
  - and reduce the WOP for threat agents
- Development of a 3D model:
  - Great potential to support the practical implementation for the physical security parts of the security standards
  - 3D Model are useful to place physical security controls at the effective positions

Acknowledgement

Some of the modelling-analyses are being elaborated as part of AREVA's participation in the "SMARTEST" Cybersecurity Testing R&D with three German University partners, partially funded by German Ministry BMWi.

NEW NP

IAEA International Atomic Energy Agency

International Conference on Physical Protection of Nuclear Material and Nuclear Facilities

13-17 November 2017, Vienna

Deterring, Protective, Delaying And Detective Application Security Controls For Nuclear Facilities

Ms. Deeksha Gupta

AREVA GmbH, Erlangen, PhD Candidate

Ms. Xinxin Lou

Bielefeld University, PhD Candidate

Mr. Mathias Lange

Magdeburg-Stendal University of Applied Sciences, Institute of Electrical Engineering, Magdeburg

Dr. Karl Waedt

AREVA GmbH, Erlangen

Thank you for your attention!

Thanks to the organizers!

AREVA