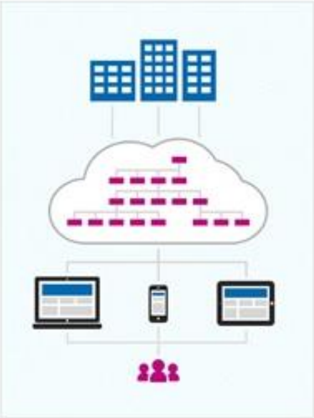
Context of the Course and Lasaris lab at FI MU

Barbora Buhnova, PV260 Software Quality, 2020

Lab of Software Architectures and Information Systems

The lab is dedicated to research, development and teaching of topics related to various theoretical and practical problems related to the development of large software systems and employment of modern information technologies in practice. We address the issues and challenges related to the design and development of information systems, including process and data modeling, management of system development, and various technologies, incl. mobile technology. We are involved in research and development projects in the field of corporate and public information systems, complex event processing, and design of large-scale IT infrastructures, such as the smart energy networks (smart grids).



The lab was founded in September 2008 as a part of the Faculty of Informatics, Masaryk University in Brno. The core team of the Lab consists of regular faculty staff members and students of doctoral, master and bachelor study programmes. The lab cooperates with industrial partners and with the Institute of Computer Technology, Technology Transfer Office, associations and clusters of companies and non-university institutions supporting innovative business. The partners of the Lab include a number of foreign universities and research institutions, e.g. University of Vienna.

Czech CyberCrime Centre of Excellence C4e

– A multidisciplinary center that brings together expert academic departments to address complex cyberspace problems

MUNI

MUNI ICS

MUNI FI

MUNI LAW

NÚKIB

CONCORDIA

Cyber Security for Europe

National Cybersecurity R&D Laboratory

EUROPEAN UNION
European Structural and Investment Funds
Operational Programme Research, Development and Education

MŠMT
MINISTRY OF EDUCATION, YOUTH AND SPORTS

Cybersecurity Innovation Hub

Coordinated by National Cyber Security Competence Centre (NC3)

- Key initiatives
  - Computer Security Incident Response Team (CSIRT) of MU https://csirt.muni.cz
  - Lab of Software Architectures and Information Systems https://www.lasaris.cz
  - Institute of Law and Technology at MU https://cyber.law.muni.cz
  - CyberRange (Kybernetický polygon, KYPO) https://www.kypo.cz
- Collaboration on
  - Cybersecurity Education (National CyberCzech Technical Exercise, Cybersecurity Qualification Framework)
  - Policy and Legislation in Cybersecurity (Cyber Security Act, Methodology)
- Partners
  - Masaryk University, Brno University of Technology
  - Czech National Cybersecurity Agency, Network Security Monitoring Cluster
  - Regional Chamber of Commerce, Industry Cluster 4.0

Cybersecurity Innovation Hub

National Cybersecurity Competence Centre

DIGITALIZATION ADVANCEMENT

The Dual-Use Dilemma

Technology facilitates and speeds up activities around us

- Can be used for the good, as well as to cause harm
- E.g. it helps people to organize for the good, as well as for the bad

If we want to boost the good, **opening up to its enormous potential**, we need to simultaneously **boost the protection against the bad**

Context-related Challenges

- **Hyperconnected world** and business landscape, problem cascading, unpredictable impacts
- Uncertainty about the **trustability of connected devices**
- **Highly distributed environment**, entry points to secure, data inconsistency, unreliable sensors, partial failures
- Securing against **threats that are not existing yet**

Engineering for the Unknown

It is no longer enough to engineer systems for **problem avoidance**

- We need to anticipate **intentional & unintentional** problems on all levels

Prebuilt mechanisms for:

- recognizing an attack/fault,
- stopping it from propagating,
- ensuring safety under attack/fault,
- recovering from an attack/failure,
- forensics after the attack/failure

CRITICAL INFRASTRUCTURE

Critical Infrastructure

- The concept of critical infrastructure and key resources includes all assets that are so vital for any country that their destruction or degradation would have a debilitating effect on the essential functions of government, national security, national economy or public health.
- Disruption of a single sector of critical infrastructure, due to **terrorist attacks**, **natural disasters** or man-made damage, is likely to have cascading effects on other sectors.

Critical Infrastructure Examples

1. **Energy** - e.g. Smart Grids, Power plants
2. **Information and Communication Technologies** - e.g. Datacentre/Cloud services
3. **Water** - e.g. Water distribution
4. **Food** - e.g. Agriculture/Food production
5. **Healthcare** - e.g. Hospital care, Emergency healthcare
6. **Financial services** - e.g. Banking, Payment transactions
7. **Public order and safety** - e.g. Maintenance of public order, Judiciary systems

Critical Infrastructure Examples (continued)

8. **Transport** - e.g. Traffic management, Public transport, Railroads, Aviation
9. **Industry** - e.g. Industrial control systems
10. **Civil administration** - e.g. Government functions
11. **Space** - e.g. Protection of space-based systems
12. **Civil protection** - e.g. Emergency and rescue services
13. **Environment** - e.g. Air pollution monitoring
14. **Defence** - e.g. Military installation, National defence

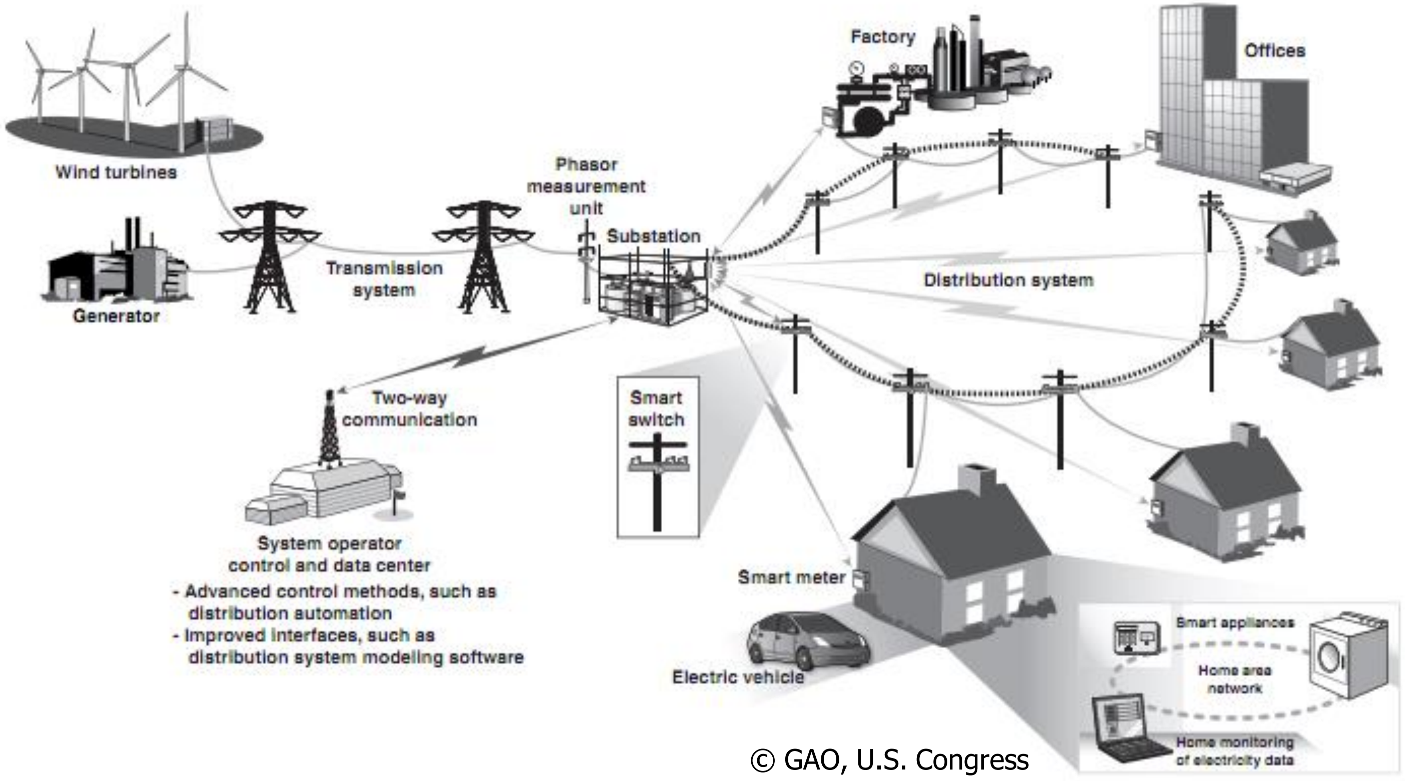
Critical Infrastructure – Traffic elaborated

- Aviation
- Air navigation services
- Airports operation
- Road transport
- Bus/Tram services
- Maintenance of the road network
- Train transport
- Management of public railway
- Rail transport services
- Maritime transport
- Monitoring and management of shipping traffic
- Ice-breaking operations
- Postal/Shipping

Yet, They Have a Lot in Common

What makes these infrastructures critical?

- The cyber and physical space merged into one
- If we stayed all digital, not much would be in danger, but we go into remote control of everything

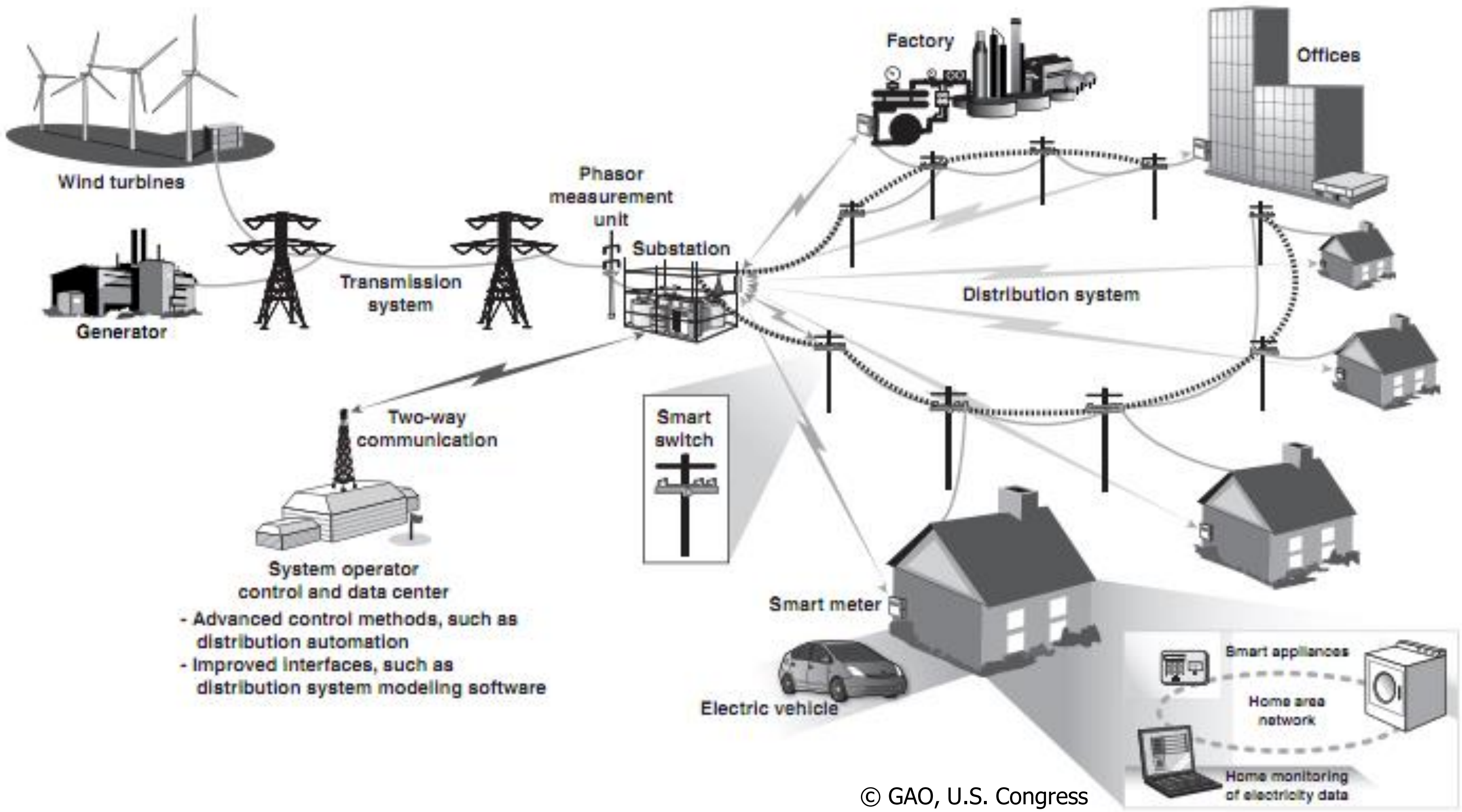


© GAO, U.S. Congress

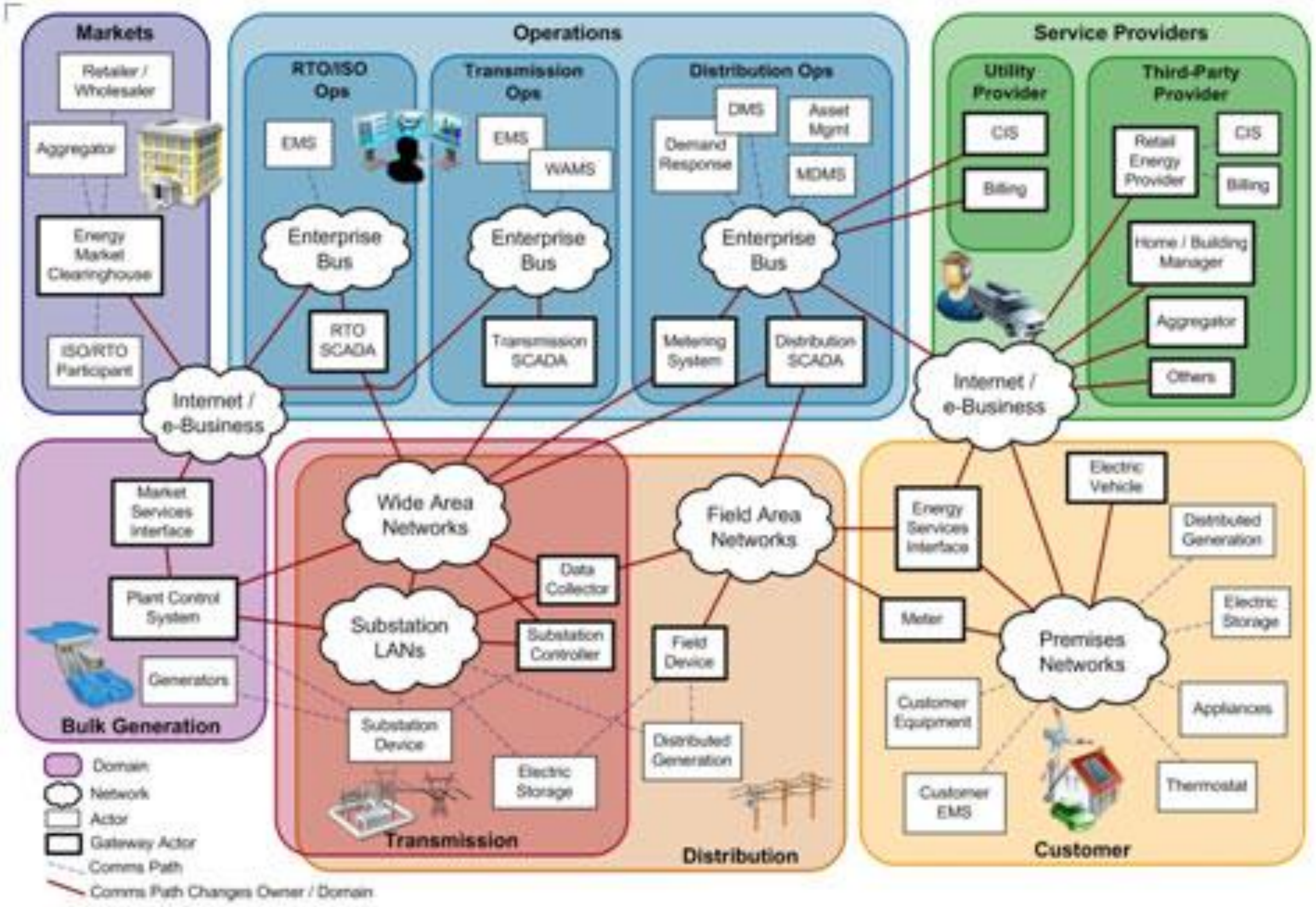
MUNI FI

SOFTWARE ARCHITECTURE

Motivating Example – Smart Grid

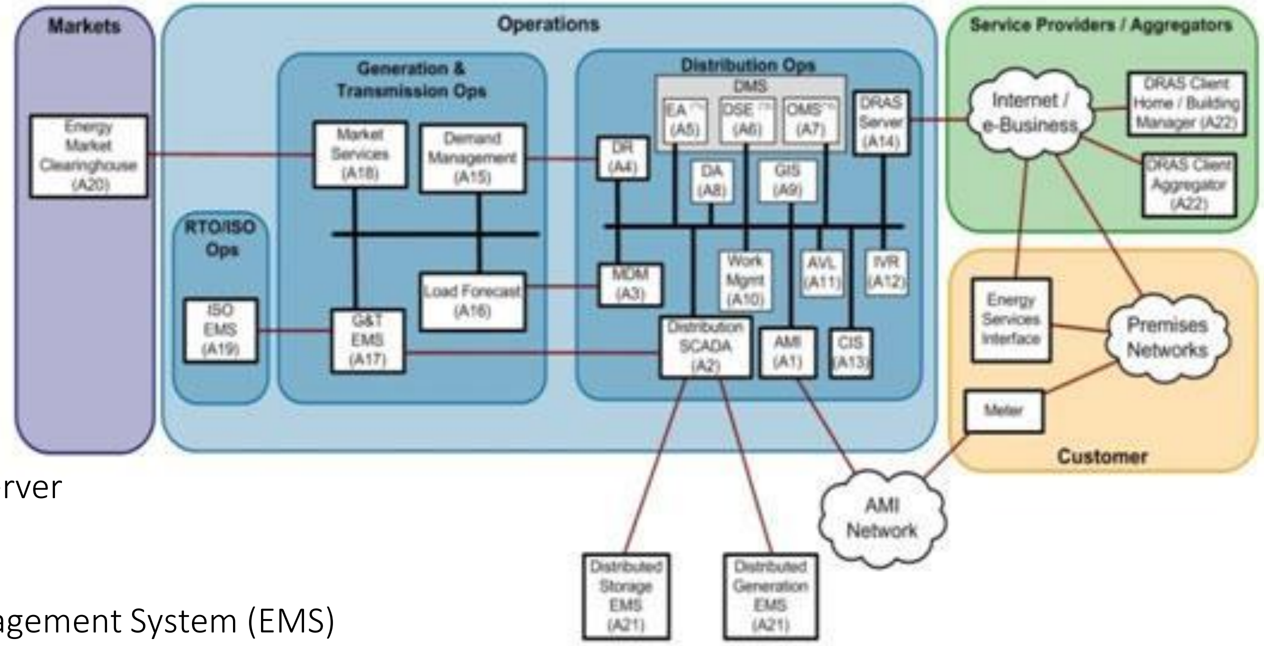


Smart Grid Conceptual Model – NIST



Smart Grid Conceptual Model – NIST

- (A1) Advanced Metering Infrastructure (AMI)
- (A2) Distribution domain Supervisory Control and Data Acquisition (SCADA)
- (A3) Meter Data Management (MDM) systems
- (A4) Demand Response (DR) systems
- (A5) Engineering Analysis (EA)
- (A6) Distribution State Estimation (DSE) systems
- (A7) Outage Management System (OMS)
- (A8) Distribution Automation systems
- (A9) Geographic Information System (GIS)
- (A10) Work Management (WM)
- (A11) Automatic Vehicle Location (AVL)
- (A12) Interactive Voice Response (IVR)
- (A13) Customer Information System (CIS)
- (A14) Demand Response Automation System (DRAS) Server
- (A15) Demand Management (DM)
- (A16) Load Forecast (LF)
- (A17) Generation and Transmission (G&T) Energy Management System (EMS)
- (A18) Market Services (MS)
- (A19) Regional Transmission Operator (RTO) /Independent System Operator (ISO) Energy Management System (EMS)
- (A20) Energy Market Clearinghouse
- (A21) Distributed Energy Resources (DER) Energy Management System (EMS)
- (A22) Demand Response Automation (DRAS) Client

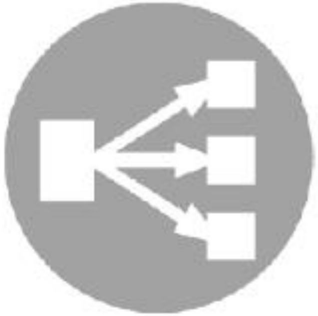


MUNI FI

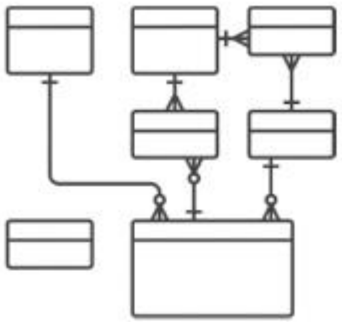
Dimensions and Guidelines

Quality Criteria

Architectural Tactics



Architectural Patterns



Reference Architectures

Technologies

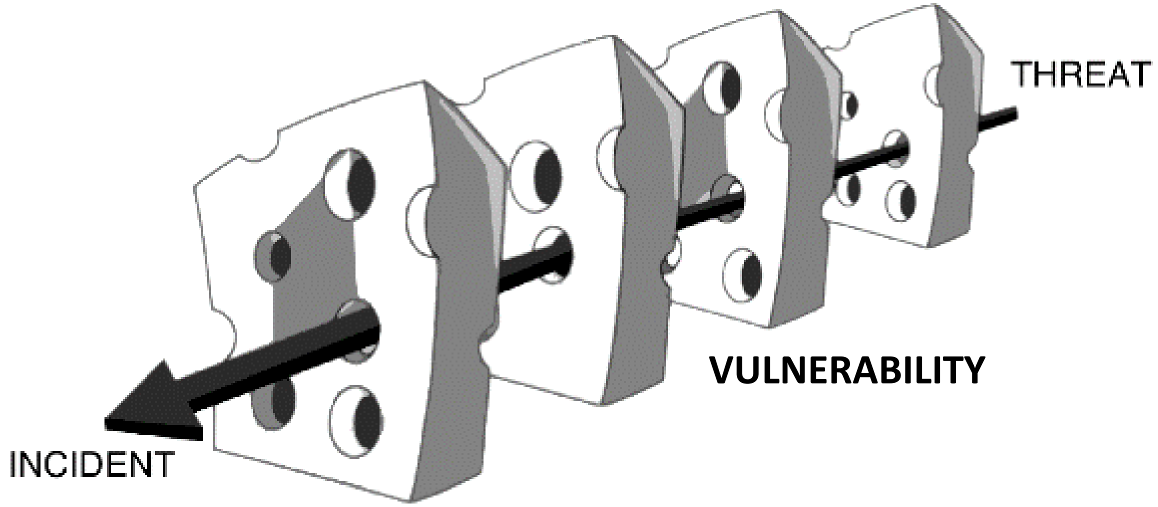
Risk Analysis and Policy

Quality Criteria

- **Reliability** – The probability of correct/failure-free system operation.
- **Availability** – The degree to which a system is fully operational, i.e. up and running.
- **Security** – The ability of a system to prevent unauthorized access and protect the confidentiality, integrity and availability of data.
- **Safety** – The ability of a system to operate without the danger of causing serious harm (e.g. human injury).
- **Robustness** – Degree to which a system is able to withstand an unexpected event without quality degradation.
- **Resilience** – The ability of a system to recover quickly after a disaster.

Intentional vs. Unintentional Issues and Causes

- **Threat/Vulnerability/Incident** – Security, Safety
- **Fault/Failure** – Reliability, Availability



MUNI
FI

Thank You for Your Attention

Czech CyberCrime Centre of Excellence C4e

- A multidisciplinary center that brings together expert academic departments to address complex cyberspace problems

MUNI

MUNI ICS

MUNI FI

MUNI LAW

NÚKIB

CONCORDIA

Cyber Security for Europe

National Cybersecurity R&D Laboratory

EUROPEAN UNION
European Structural and Investment Funds
Operational Programme Research, Development and Education

MINISTRY OF EDUCATION, YOUTH AND SPORTS

Barbora Buhnova, FI MU Brno
buhnova@fi.muni.cz
www.fi.muni.cz/~buhnova

MUNI FI