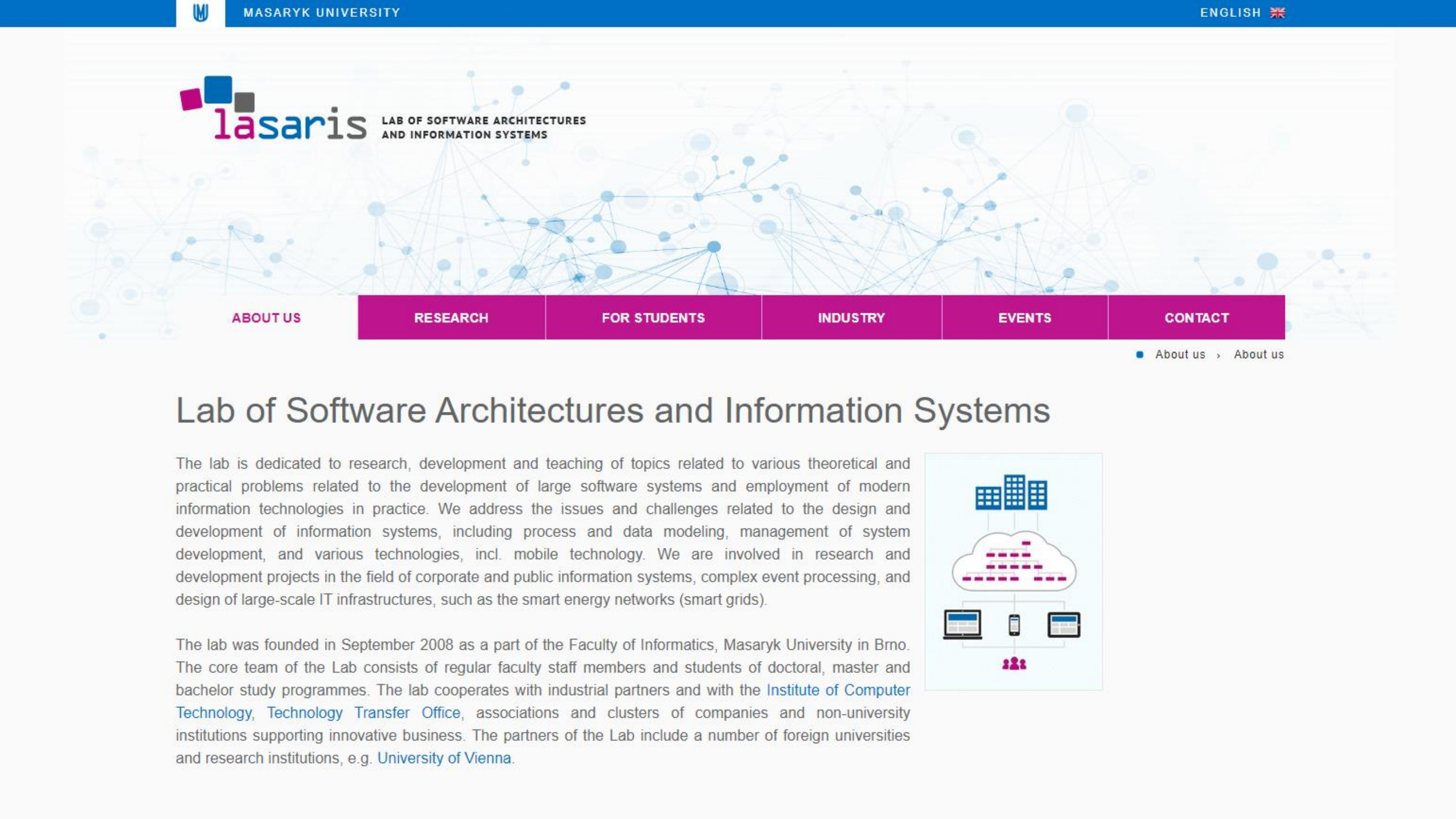
MUNI
FI

Welcome to the PV226 Lasaris Seminar

Barbora Buhnova, PV226 Lasaris Seminar, 2022

Organization of the Seminar

- Talks by seminar members and guests every week
  - Agenda in the interactive syllabus
- Choose the lab member you will be in contact with
  - Let me know who that will be
- To pass the course
  - Set an involvement together with your contact person (~26 hours)
  - Alternatively propose to give a talk at the seminar



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

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

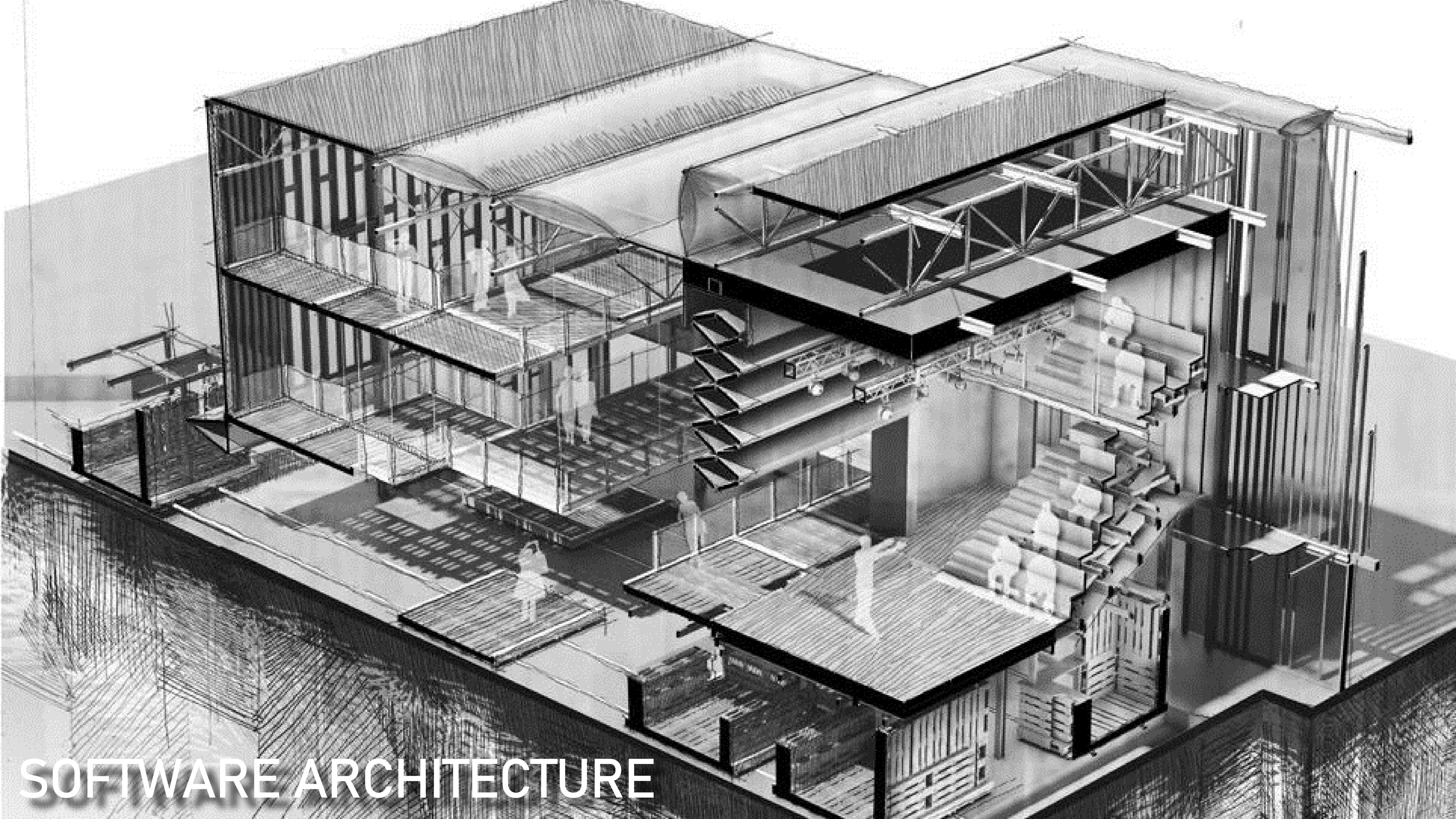
Critical Infrastructure Examples (continued)

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

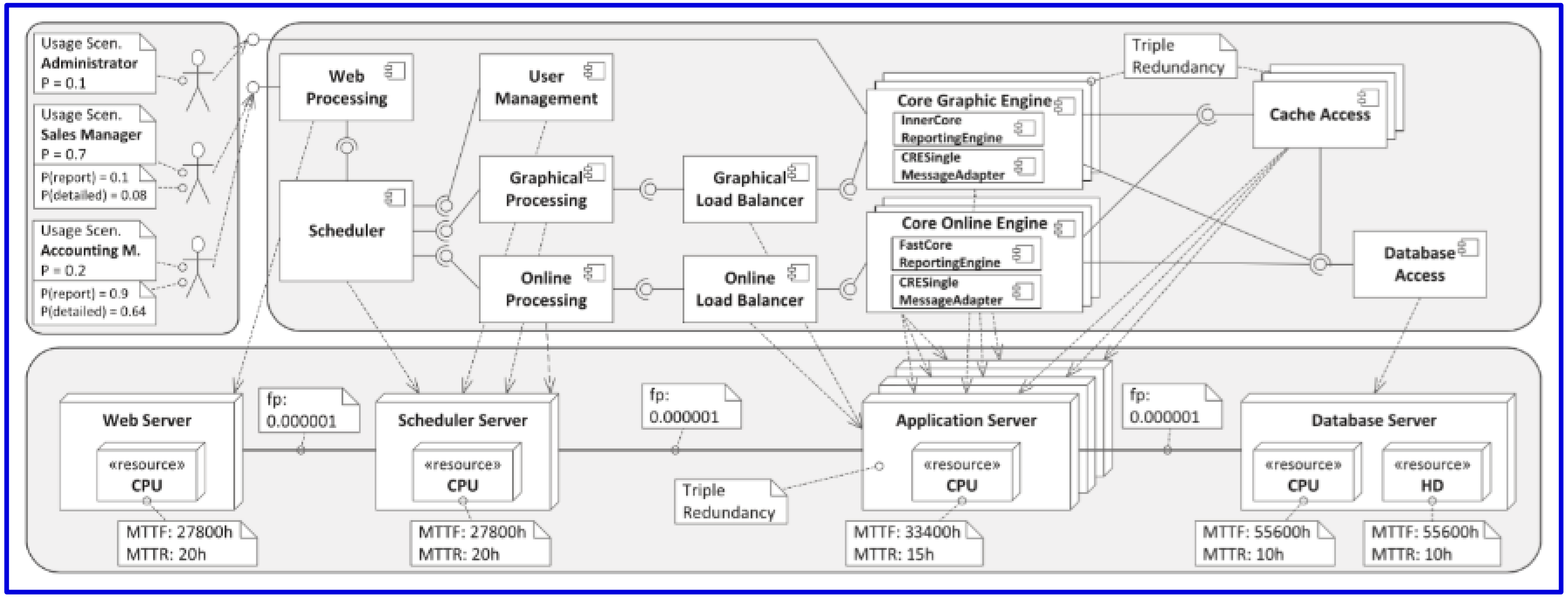
SOFTWARE ARCHITECTURE

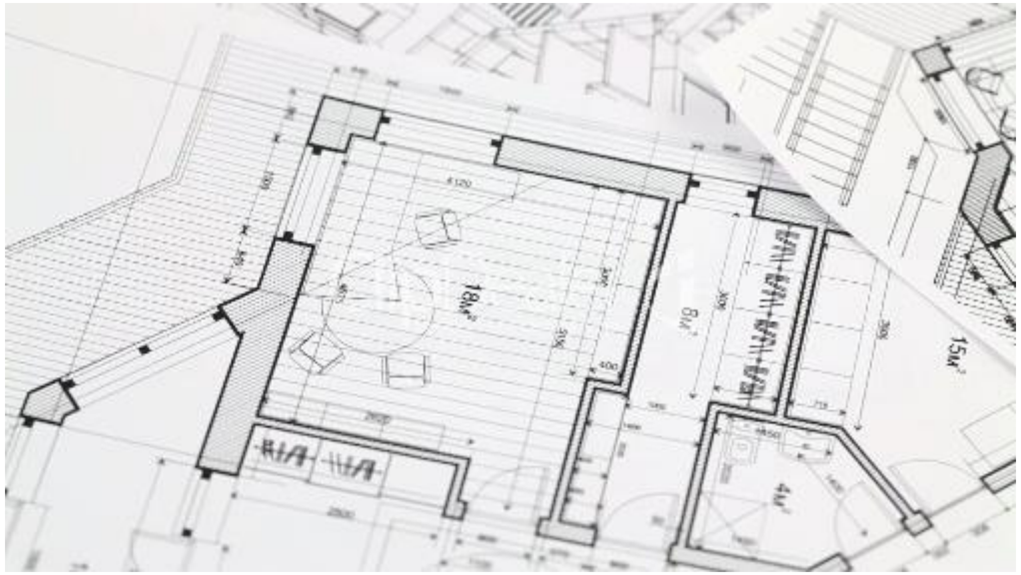


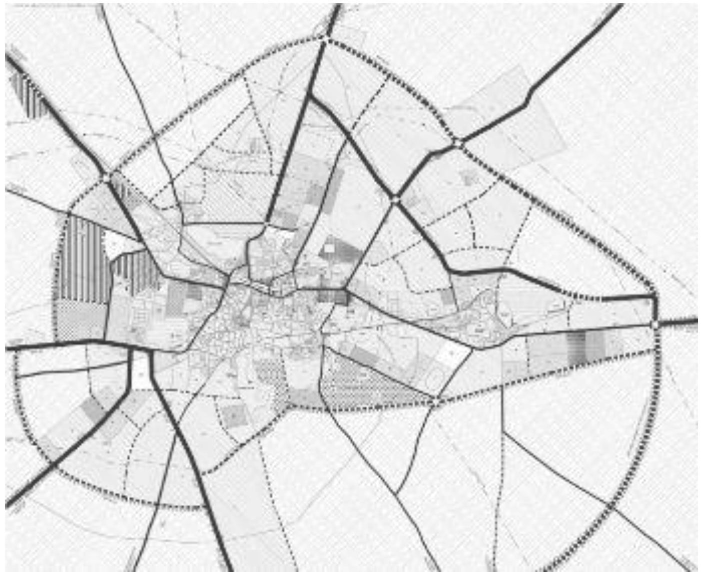
SOFTWARE ARCHITECTURE

SOFTWARE ARCHITECTURE

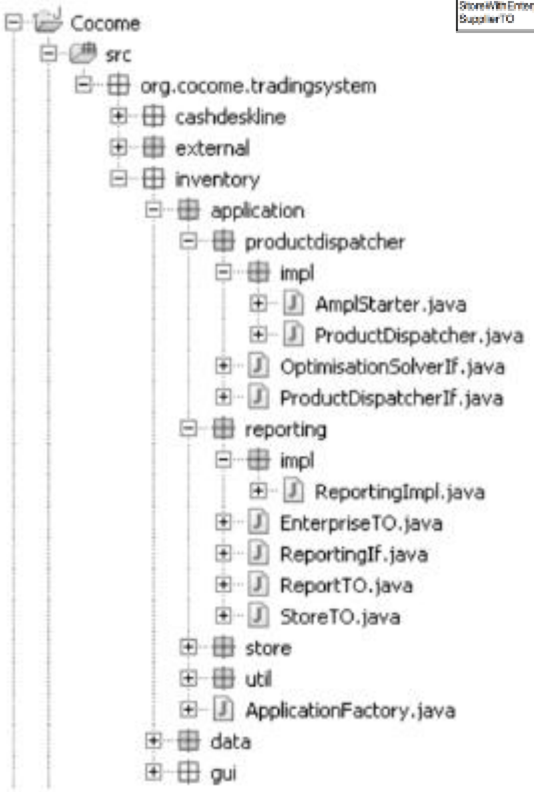
Software Architecture



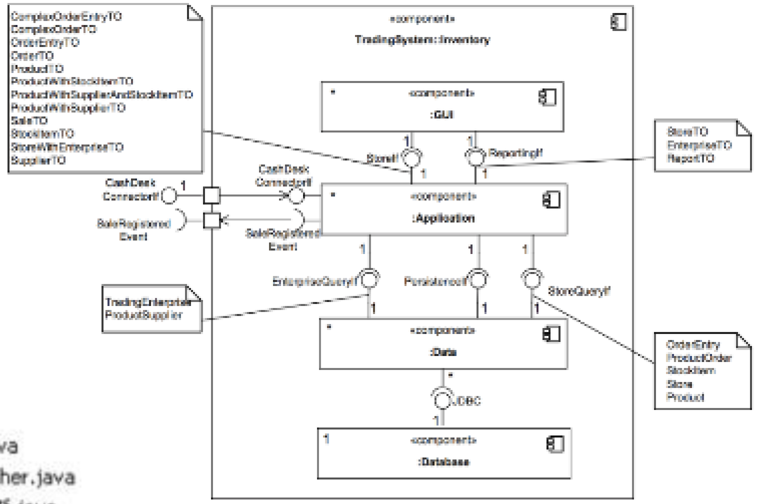


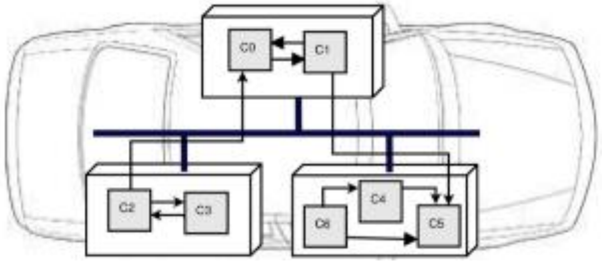


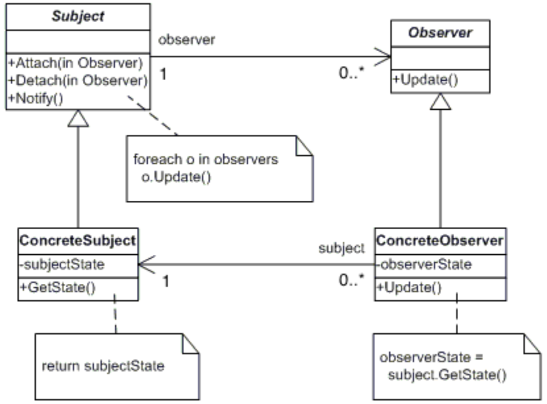
Where do we find SA?

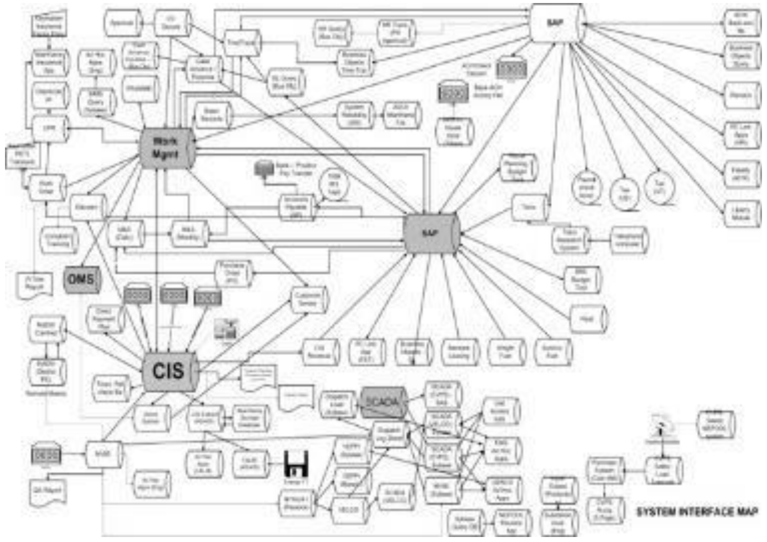


```
Cocome
  src
    org.cocome.tradingsystem
      cashdeskline
      external
      inventory
        application
          productdispatcher
            impl
              AmplStarter.java
              ProductDispatcher.java
            OptimisationSolverIf.java
            ProductDispatcherIf.java
          reporting
            impl
              ReportingImpl.java
            EnterpriseTO.java
            ReportingIf.java
            ReportTO.java
            StoreTO.java
          store
          util
          ApplicationFactory.java
        data
        gui
```









HOWEVER, ARCHITECTURE IS NOT ITS BLUEPRINT

What is then a SW Architecture?

Till 2000

- Software architecture refers to **the fundamental structures** of a software system… [IEEE 1471:2000]

Since 2000

- Software architecture encompasses **the set of significant design decisions** that shapes a software system… [RUP, 1998]

What is then a SW Architecture?

- The architecture is **the set of significant design decisions** that shape a software system, where significant is measured by cost of change. [Grady Booch, 2006]

- Expert developers' **shared understanding of the system design**.
- The decisions that you wish you could get right early. [Martin Fowler, 2015]

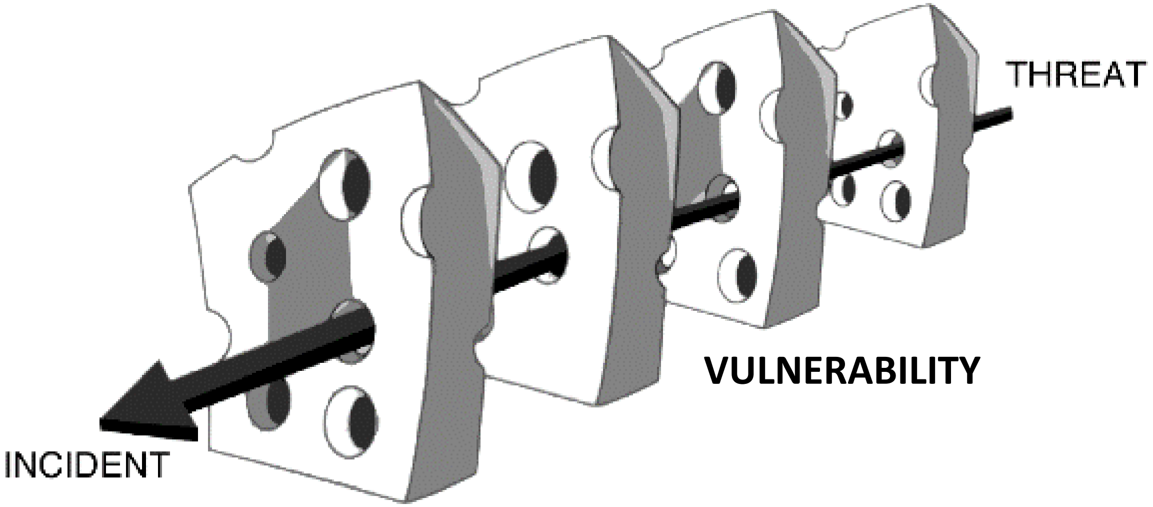
Those principles that drive all your future design decisions**.**

Quality Criteria

- **Reliability** – The probability of correct/failure-free system operation.
- **Performance** – The degree to which a system meets its requirements for timeliness, i.e. response time or throughput.
- **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

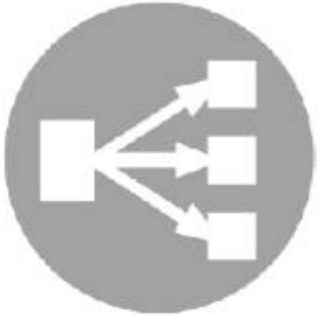
- **Threat/Vulnerability/Incident** – Security, Safety
- **Fault/Failure** – Reliability, Availability

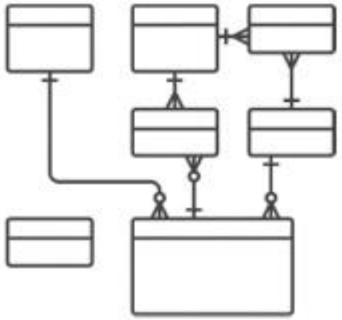


Dimensions and Guidelines

Quality Criteria

Architectural Tactics


Architectural Patterns


Reference Architectures

Technologies

Methods and processes

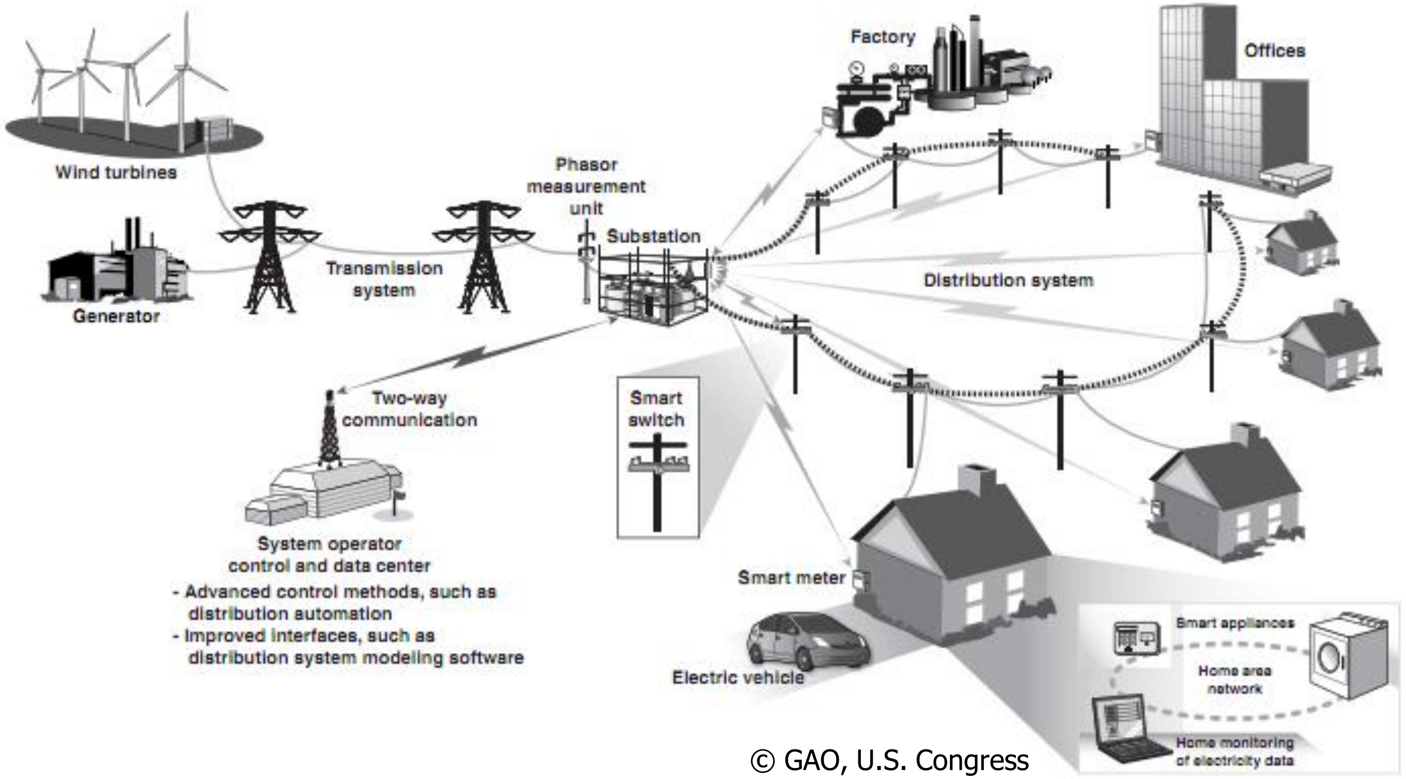
/ Pictures from Awais Rashid, University of Bristol

WHAT MAKES ARCHITECTING DIFFICULT?

Digitalization meets Critical Infrastructures

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



Wind turbines
Generator
Transmission system
Phasor measurement unit
Substation
Factory
Offices
Distribution system
Two-way communication
Smart switch
System operator control and data center
- Advanced control methods, such as distribution automation
- Improved interfaces, such as distribution system modeling software
Smart meter
Electric vehicle
Smart appliances
Home area network
Home monitoring of electricity data

© GAO, U.S. Congress

Context-related Challenges become really Critical

- 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

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:

Detection of insider attacks in organizations

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

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

Multi-Layer Model of CPS Fairues and their Dependencies

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

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

Adaptive Safety in Autonomous Ecosystems

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

Forensic-Ready software systems

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

Trust in Autonomous Ecosystems

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

NEED FOR EXTENSIVE MINDSET STRETCH

Bridging Communities & Thinking out of the Box

- Building trust in digital autonomous ecosystems
  - Technical, methodological, legal, psychological, sociological, environmental, economical and other aspects need to meet in one solution

- References
  - Cioroaica, Emilia, Thomas Kuhn, and Barbora Buhnova. **"(Do not) trust in ecosystems."** In Proceedings of ICSE NIER 2019
  - Cioroaica, Emilia, Barbora Buhnova, Thomas Kuhn, and Daniel Schneider. **”Building Trust in the Untrustable”**. In Proceedings of ICSE SEIS 2020

THANK YOU

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

MŠMT
MINISTRY OF EDUCATION, YOUTH AND SPORTS

FACULTAS ARTIS INFORMATICAE • UNIVERSITAS MASARYKIANA

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

MUNI FI