Masaryk University
Faculty of Informatics

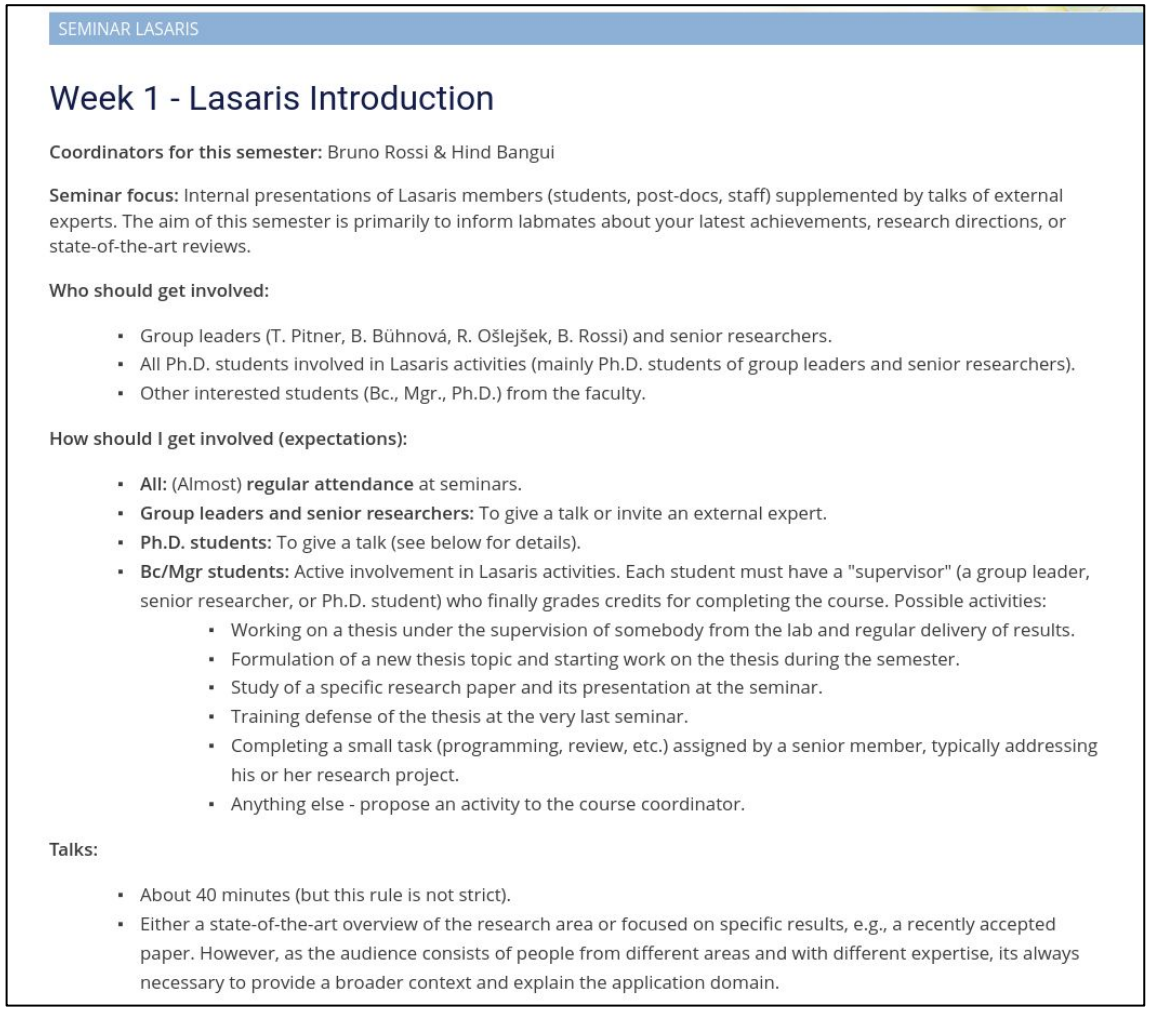
PV226 Seminar

Lab of Software Architectures
and Information Systems

Bruno Rossi
brossi@mail.muni.cz

Hind Bangui
Hind.bangui@mail.muni.cz

Introduction



SEMINAR LASARIS

Week 1 - Lasaris Introduction

Coordinators for this semester: Bruno Rossi & Hind Bangui

Seminar focus: Internal presentations of Lasaris members (students, post-docs, staff) supplemented by talks of external experts. The aim of this semester is primarily to inform labmates about your latest achievements, research directions, or state-of-the-art reviews.

Who should get involved:

- Group leaders (T. Pitner, B. Bühnová, R. Ošlejšek, B. Rossi) and senior researchers.
- All Ph.D. students involved in Lasaris activities (mainly Ph.D. students of group leaders and senior researchers).
- Other interested students (Bc., Mgr., Ph.D.) from the faculty.

How should I get involved (expectations):

- **All:** (Almost) **regular attendance** at seminars.
- **Group leaders and senior researchers:** To give a talk or invite an external expert.
- **Ph.D. students:** To give a talk (see below for details).
- **Bc/Mgr students:** Active involvement in Lasaris activities. Each student must have a "supervisor" (a group leader, senior researcher, or Ph.D. student) who finally grades credits for completing the course. Possible activities:
  - Working on a thesis under the supervision of somebody from the lab and regular delivery of results.
  - Formulation of a new thesis topic and starting work on the thesis during the semester.
  - Study of a specific research paper and its presentation at the seminar.
  - Training defense of the thesis at the very last seminar.
  - Completing a small task (programming, review, etc.) assigned by a senior member, typically addressing his or her research project.
  - Anything else - propose an activity to the course coordinator.

Talks:

- About 40 minutes (but this rule is not strict).
- Either a state-of-the-art overview of the research area or focused on specific results, e.g., a recently accepted paper. However, as the audience consists of people from different areas and with different expertise, its always necessary to provide a broader context and explain the application domain.

https://is.muni.cz/auth/el/fi/podzim2023/PV226/index.qwarp

About the hosts - Bruno Rossi

- Software Reliability & Software Quality
  - Mining Software Repositories
  - Evaluation of source code quality and evolution (e.g., Technical Debt)
  - Application of Software Reliability Growth Models (SRGMs) and metrics from Open Source Quality Models
- Microservices research
  - Anomaly detection of performance and reliability data
  - Migration of monoliths to microservices
  - Reconstructing architecture of microservices for simulators

About the hosts - Hind Bangui

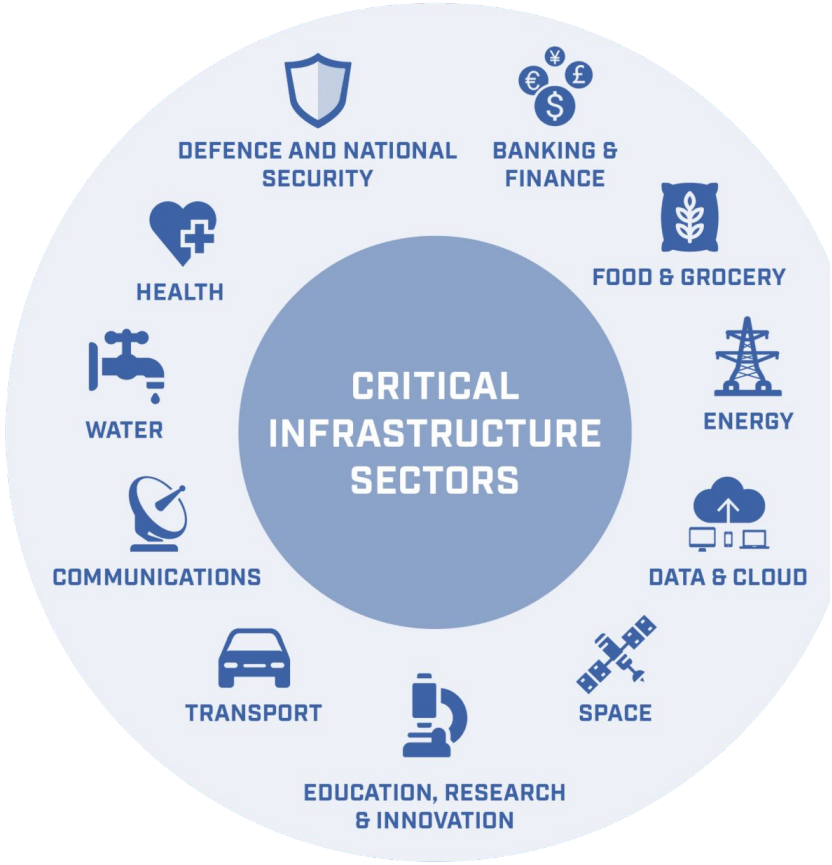
- Trust Management in IoT Ecosystems
  - Human-centric intelligent systems
  - Trust algorithms
  - Trust simulators
  - Trustworthy and resilient human-machine interaction
  - Ethics&Regulations
  - Trust in autonomous systems
  - Explainable and interpretable AI solutions for trustworthy systems
- Approaches for resilience and antifragility in IoT Ecosystems

Main Topic: Cybersecurity

Other Topics: Trust Management, AI, IoT, Human Behavior / Human-Machine Communication, Critical Infrastructures, Cyber-Physical Systems

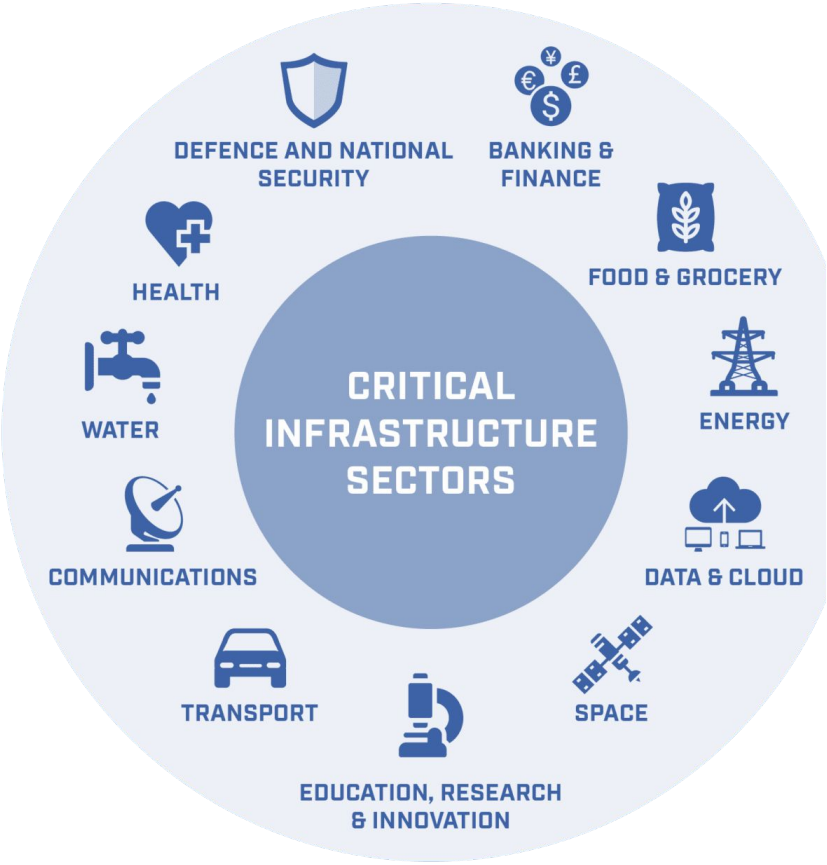
Critical Infrastructure Systems:
Digital Transformation

- Project:
  - CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence (CZ.02.1.01/0.0/0.0/16_019/0000822)
- Definition of Critical Infrastructures (CI): "Organizational and physical structures and facilities of such **vital importance to a nation's society and economy** that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences".



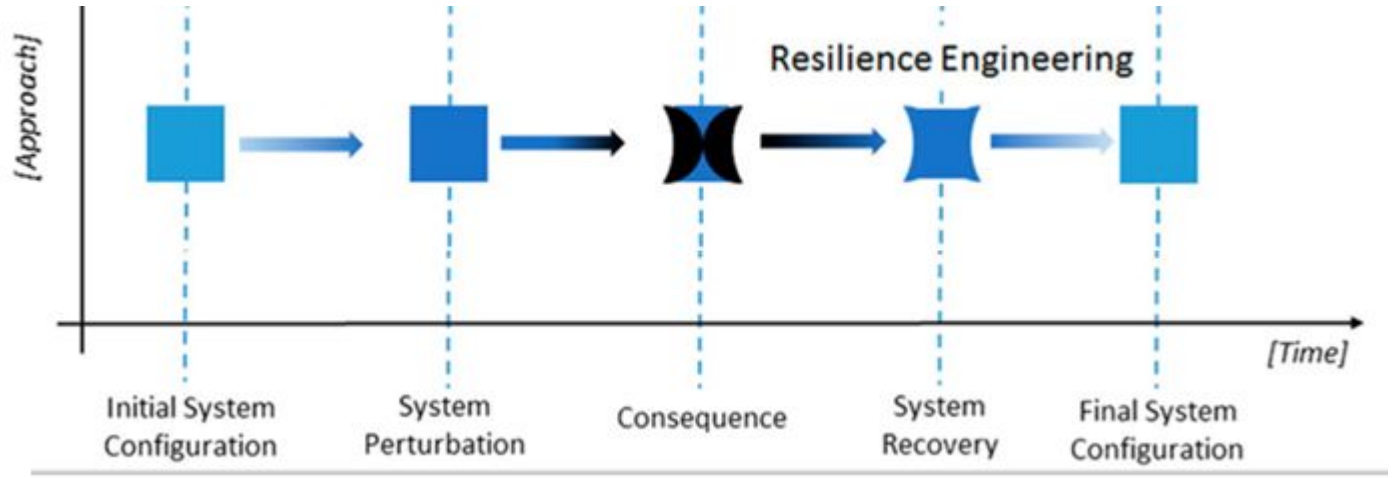
Critical Infrastructure Systems:
Digital Transformation

- A system is designed to operate in “mostly stable” situations.
- Systems are increasingly exposed to unexpected disruptive events.
- Frequent keywords in the literature when dealing with disruptions: “disruption”, “disturbance”, “disaster”, “hazard”, “crisis”, “catastrophic or traumatic event”, “failure”, “attack”, “shock”, and “X-Event (extreme event)”.



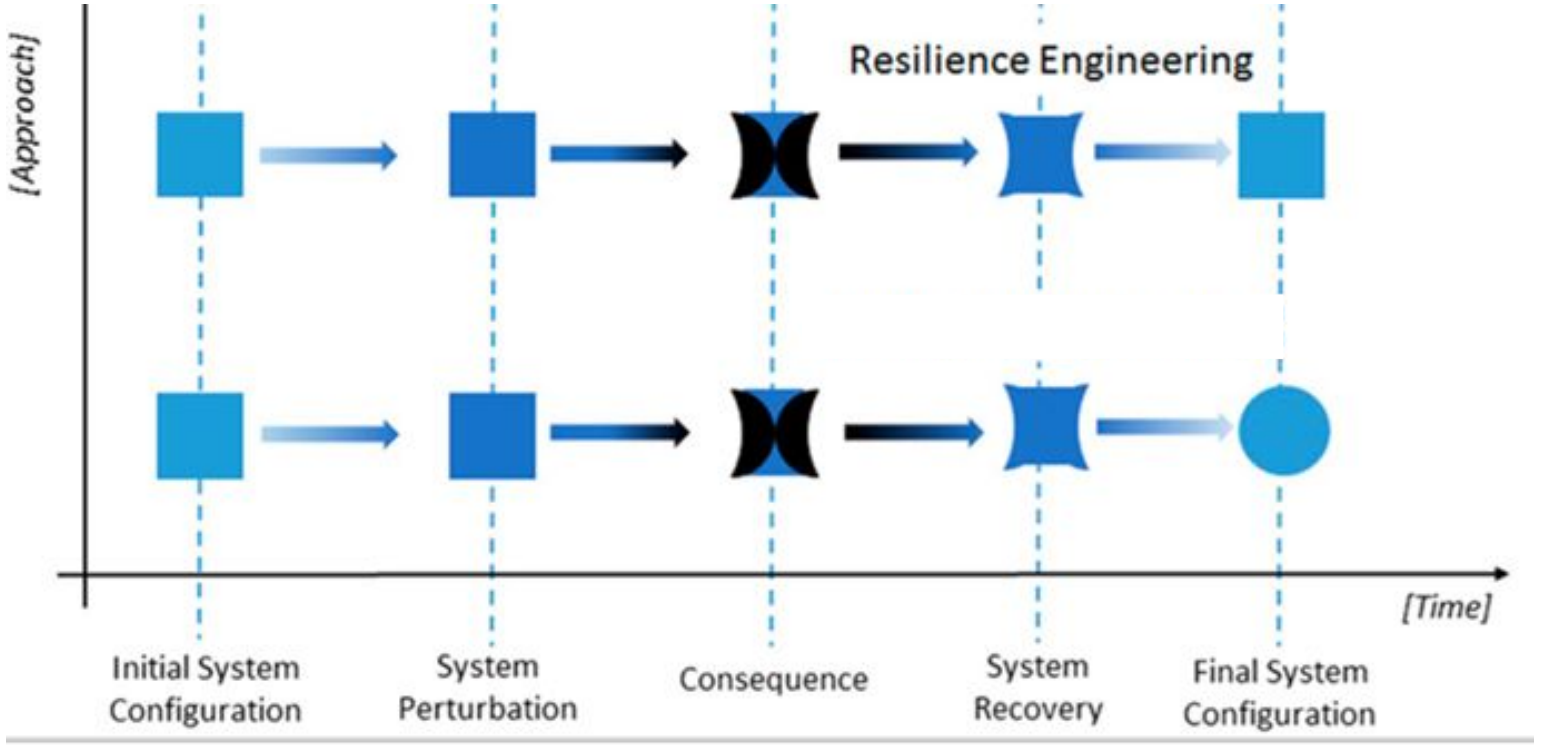
Critical Infrastructure Systems:
Digital Transformation

- Design strategies to mitigate risks and respond efficiently to risk incidents
  - Recover a system from sudden shocks,
  - Reduce the negative consequences of disruptions
  - Prepare for plausible future scenarios and learn from past experiences.
  - Prevent risky events from occurring (reducing vulnerability),



Critical Infrastructure Systems:
Digital Transformation

- The COVID-19 pandemic has shocked infrastructure systems in unanticipated ways.
- The COVID-19 pandemic represents a call for a major rethinking of how we approach infrastructure.



Critical Infrastructure Systems:
Digital Transformation

Digital Transformation during the COVID-19 pandemic

Domains	Response / Impact	Response	Underlying technology/ operation
Education	Widespread closure of educational institutions; access to labs is restricted; projects have been mothballed; fieldwork interrupted	Virtual learning environment (online teaching, presentation, assessment, and consultation); convocation online	Online video conferencing software, virtual labs on cloud
Conferences	In-person conferences banned;	Online presentation and discussion	Video streaming, Virtual conference software
Healthcare	Overcrowded hospitals, inability to meet the demands on them	Contact tracing, forecasting resource requirements, allotment of scare resources based on a patient's survivability, COVID-19 vaccine development, telehealth (online consultation with a doctor or medical professional);	AI, cloud computing, chatbot
Industry	Closure of some industries	Work from home, remote operations, automation and autonomous operation	Robots, automation, 3-D printing

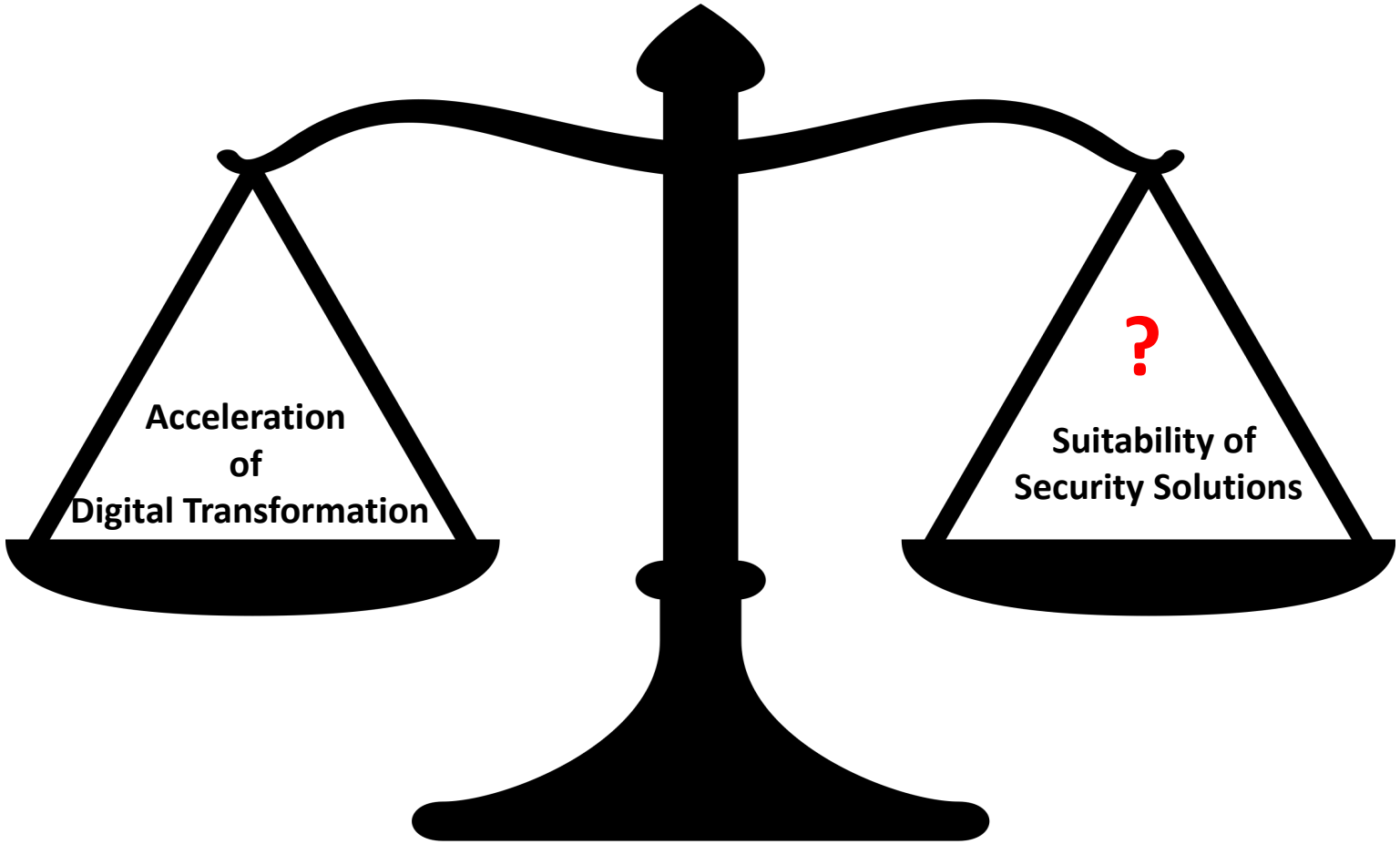
Critical Infrastructure Systems:
Digital Transformation

lasaris

Digital Transformation during the COVID-19 pandemic

Domains	Response / Impact	Response	Underlying technology/ operation
Government	Spike in demands from citizens for assistance, disruption to normal operations	Migration to online services	Cloud, the Web, Online meeting application
Business	Closure of business, avoidance of in-person retail shopping	Adherence to social distancing, services online, work from home	Chatbot, drone delivery, online meeting software, virtual office/desktop, remote access to work
Personal life and social interaction	Lockdown	Indoor activities	Phone, audio and video chats, streaming, online gaming
Retail	Stores closed, only online service, avoidance of retail shopping	Online shopping, home delivery	The Web, online payment, contactless payment
Entertainment	Entertainment venues (parks, cinema) closed, sports without spectators	Viewing online	Audio and video streaming, virtual reality

Critical Infrastructure Systems:
Digital Transformation



Critical Infrastructure Systems:

Changing the nature of criticality

- Definition of Critical Infrastructures (CI): “Organizational and physical structures and facilities of **such vital importance to a nation's society and economy** that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences“.
- **CHANGING NATURE OF CRITICALITY**
  - Some industries have been able to shift production from **non-essential** to **essential** products.
  - An Example**: Parks** are typically considered a **non-essential service**. However, during COVID-19, parks have proven their value by serving as field hospitals, providing alternative shelters for socially vulnerable groups, and promoting physical, emotional, and mental well-being.

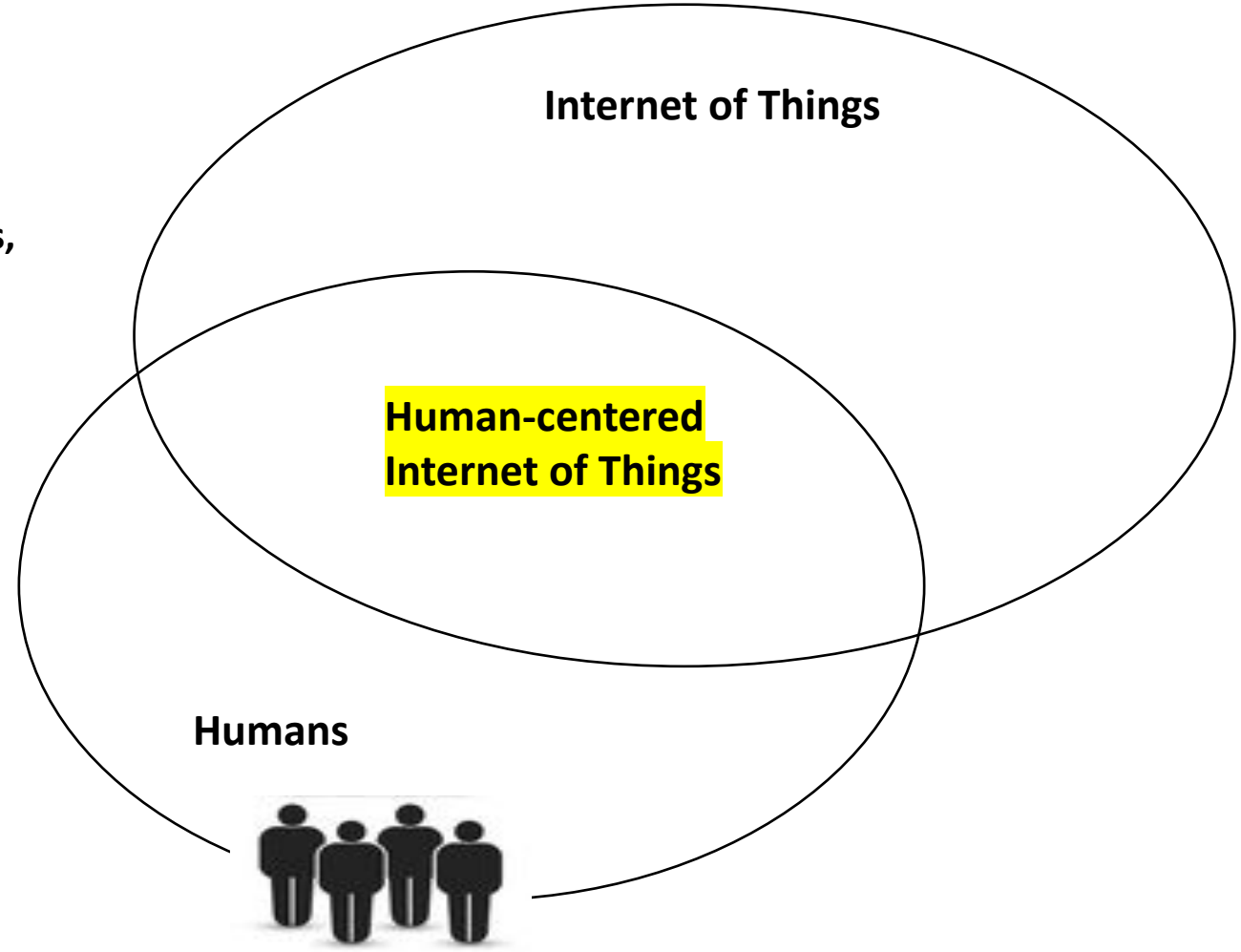
Critical Infrastructure Systems:

Changing the nature of criticality

- Definition of Critical Infrastructures (CI): “Organizational and physical structures and facilities of such **vital importance to a nation's society and economy** that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences“.
- **CHANGING NATURE OF CRITICALITY**
  - Defining which systems are CI results in **a prioritization** of resources **during** extreme events.
  - Critical infrastructure definitions should account for the changing services and functions of industries during hazards.
  - Treating criticality as **dynamic** appears crucial to identifying how to meet basic needs through infrastructure changes as hazards vary.
  - Thinking about the flexibility of security solutions.

Tracking Systems:
Privacy & Safety concerns

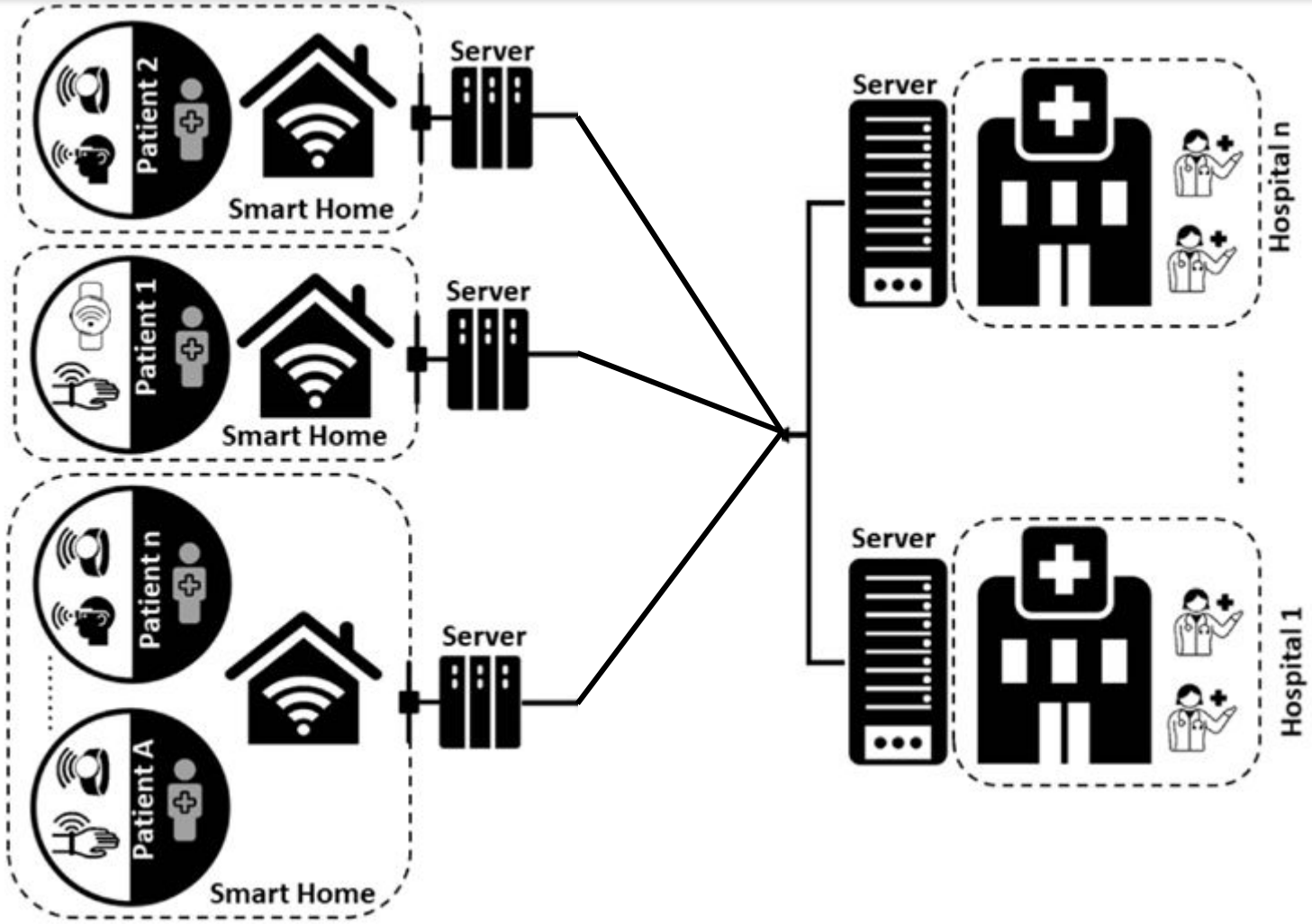
- **Human-centered Internet of Things (Human-centric Intelligent Systems, Human-Centric Intelligent Society)**



Tracking Systems:

Privacy & Safety concerns

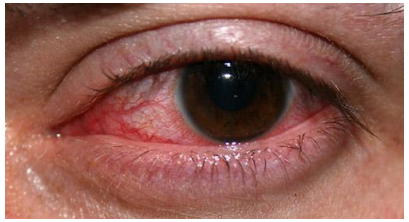
Example 1: Healthcare



Tracking Systems:
Privacy & Safety concerns

Example 2: Insurance

- Manage-How-You-Drive (MHYD) is an insurance scheme that considers the physiological and behavioral information of drivers to charge risk-based premiums.
- The behavior of a driver can be classified into two categories:
  - Driving behavior (like braking pressure and braking speed)
  - Non-driving behavior, which is a distraction (like smoking and texting on the phone).



- The MHYD physiological categories are fatigue and drowsiness,
  - Identifying fatigue by using biometric sensors to track the facial expressions and eye movements of drivers.

Talking to passenger

Adjusting hair

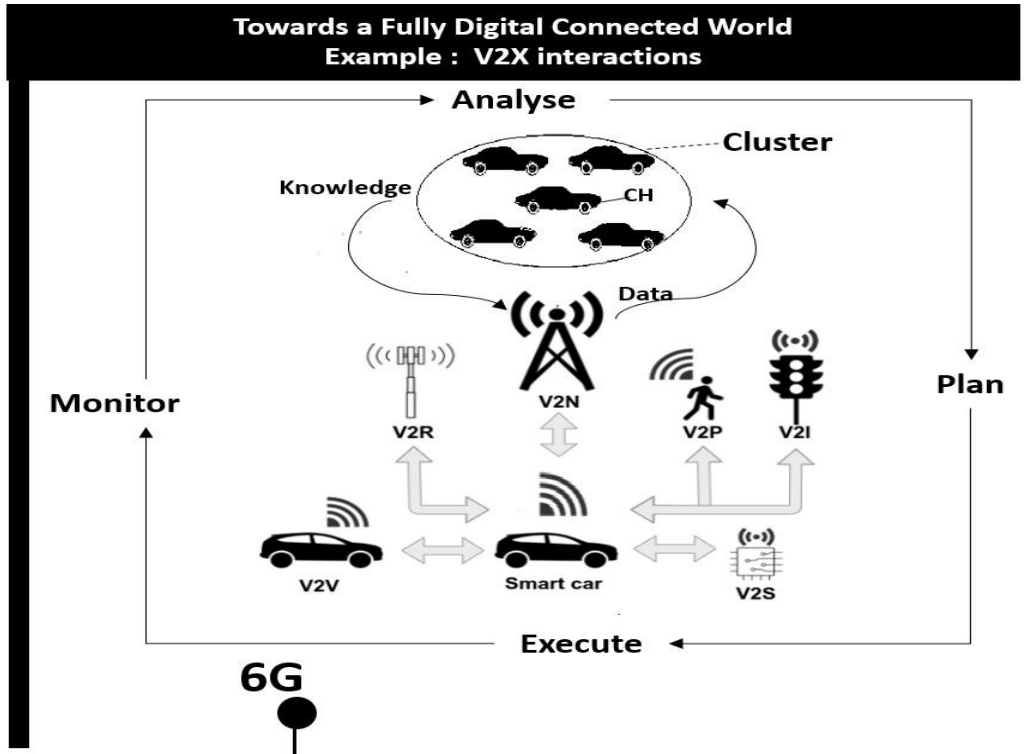
Reaching Behind

Drinking

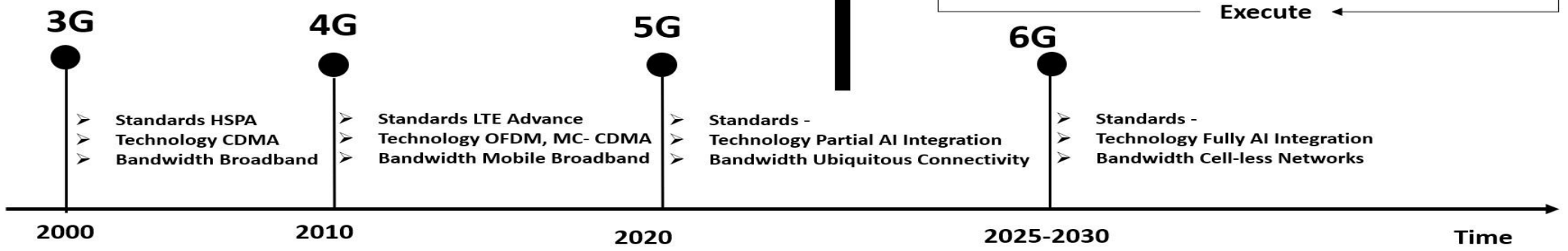
Tracking Systems:

Privacy & Safety concerns

- Smart mobility refers to the use of ICT in modern transport technologies to improve urban traffic.
- Vehicular Ad-hoc Network (VANET) is a typical smart mobility system.
- VANET comes under the subgroup of conventional Mobile Ad hoc Network (MANET).

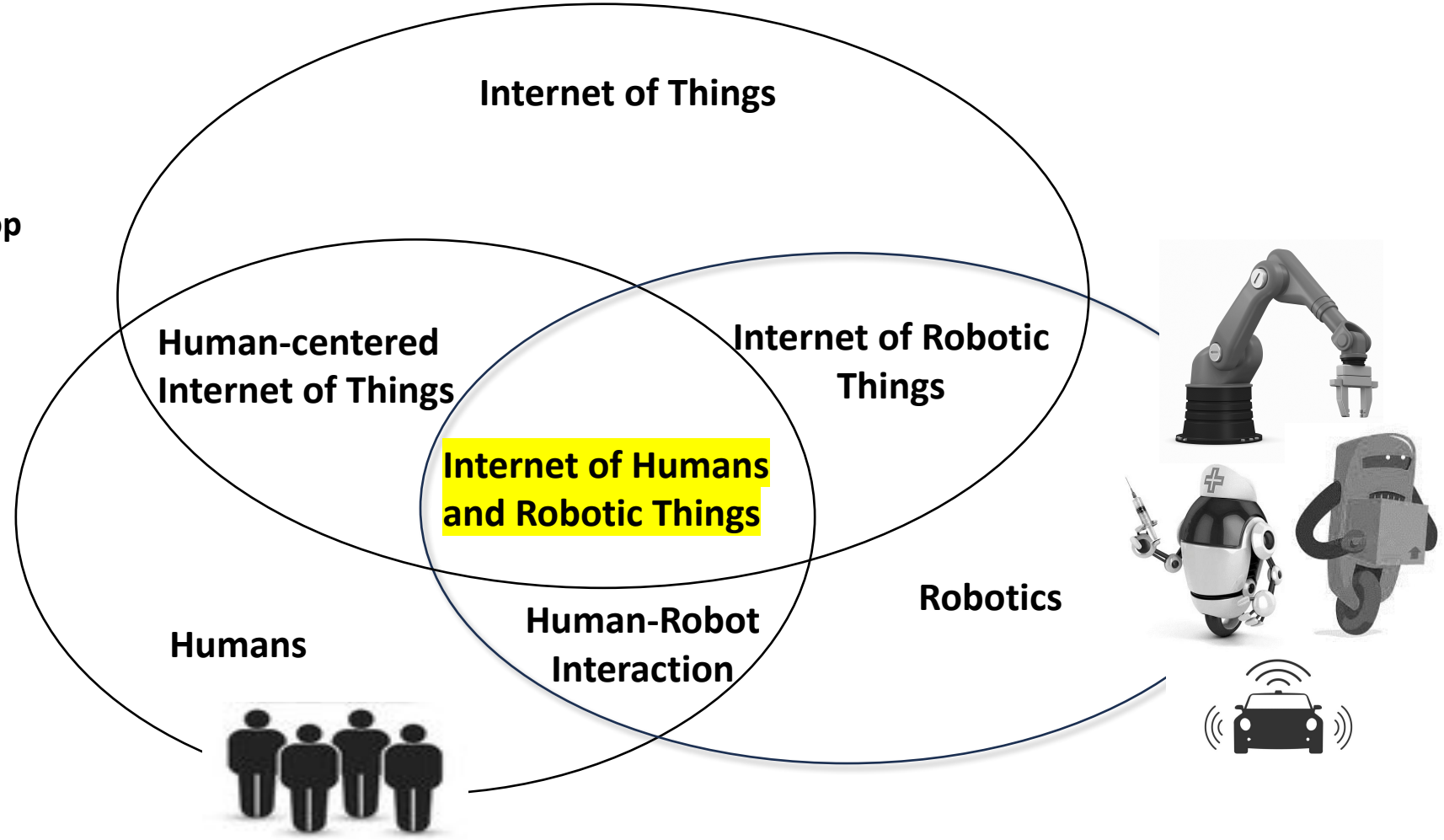


V2S: Vehicle-to-Sensor
V2I: Vehicle-to-Infrastructure
V2V: Vehicle-to-Vehicle
V2P: Vehicle-to-Pedestrian
V2R: Vehicle-to-Roadside Unit
V2N: Vehicle-to-Network Connections



Digital Ecosystems:
Social Values

- Human-centered Internet of Things
  (Human-centric Intelligent Systems,
  Human-Centric Intelligent Society)
  - Considering Human-in-the-IoT loop



Trust Management Simulator

- Trust management simulator for Wireless Sensor Networks.
  - Provide real-time events.
  - Test the effectiveness of reputation and trust models.
  - Designed in 2009
- The simulator is implemented using Java.
- A node can request resources from the neighboring node or send resources to the requesting node.
- The simulator allows the user to adjust several parameters such as the percentage of malicious nodes or the possibility of forming a collusion, among many others.
- **Main Task**: Use new Java frameworks to rebuild the simulator.