MUNI
FI

C4e Programme 2: Critical Information Infrastructures and Secure Systems Design

Barbora Buhnova, **Summer School Blansko**, Aug/Sep, 2020

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

MUNI FI

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

MUNI FI

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

MUNI FI

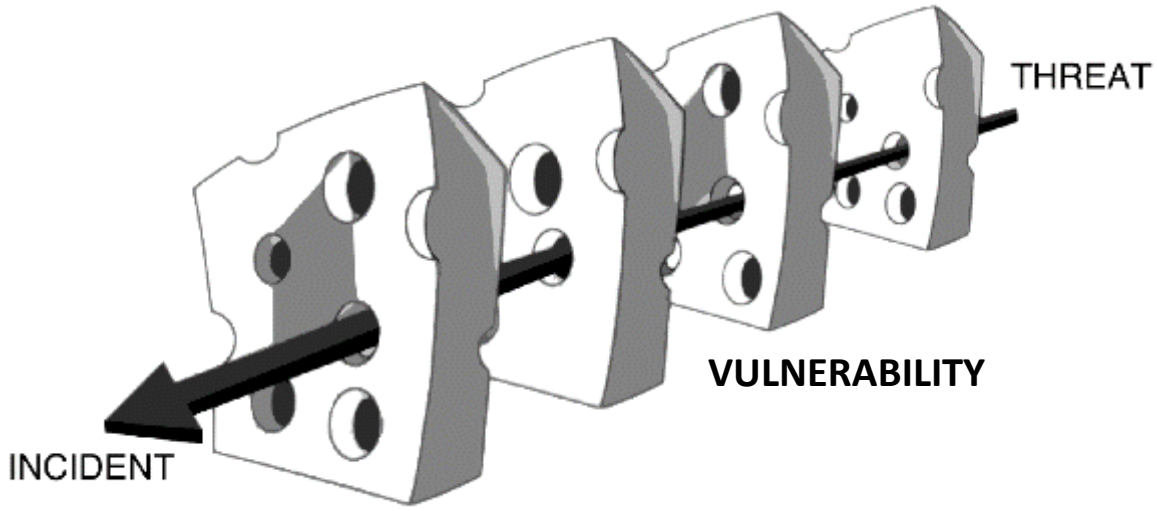
Critical Infrastructure

- 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.

MUNI FI

Intentional vs. Unintentional Issues and Causes

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



MUNI FI

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

MUNI FI

Czech CyberCrime Centre of Excellence C4e

Programme 2: Critical Information Infrastructures and Secure Systems Design

- Subprogramme 1 – Simulation and predictive analysis of critical infrastructures
- Subprogramme 2 – Formal verification of critical infrastructures
- Subprogramme 3 – Recommendations for critical infrastructure realization

MUNI FI

Contributors

Subprogram 1

- Stanislav Chren
- Lukáš Daubner
- Hind Bangui

Subprogram 2

- Jiří Barnat
- Ivana Černá
- Nikola Beneš
- Jan Mrázek

Subprogram 3

- Bruno Rossi
- Radek Ošlejšek
- Renate Motschnig
- Gerald Quirchmayr

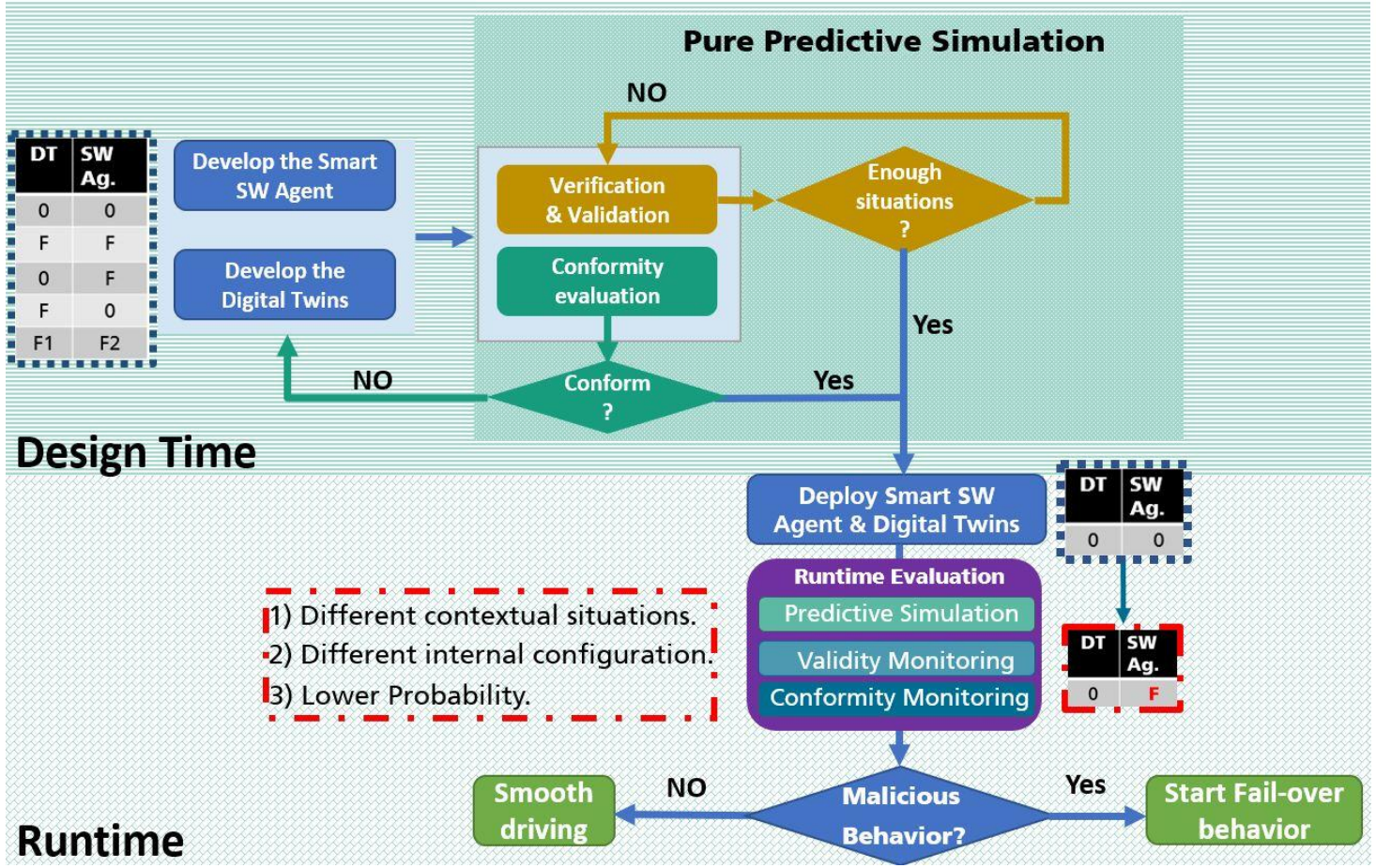
Additional contributors

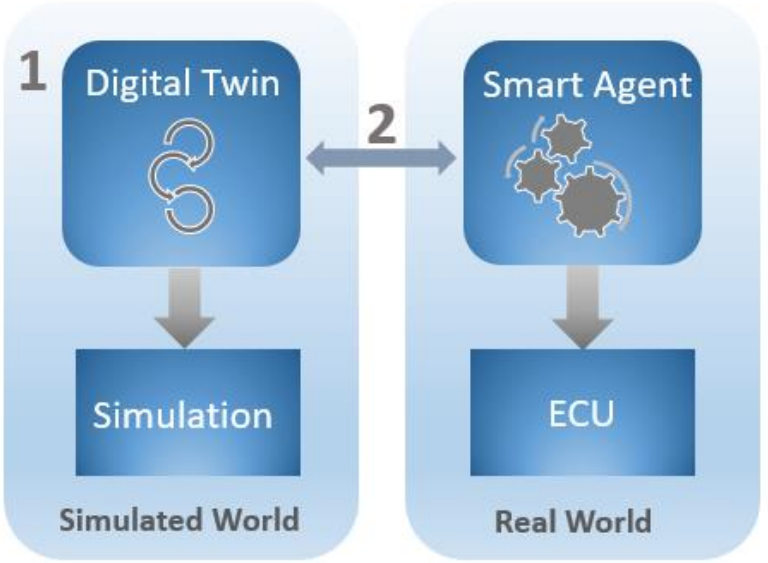
- Bacem Mbarek
- Pavel Loutocký
- Václav Stupka

MUNI FI

International cooperation

Building Trust in Digital Ecosystems





MUNI FI

International cooperation

Building Trust in Digital Ecosystems

- Recent publications
  - Cioroaica, Emilia, Thomas Kuhn, and Barbora Buhnova. "(Do not) trust in ecosystems." In Proceedings of ICSE NIER 2019 (CORE rank A*)
  - Cioroaica, Emilia, Stanislav Chren, Barbora Buhnova, Thomas Kuhn, and Dimitar Dimitrov. "Towards creation of a reference architecture for trust-based digital ecosystems." In Proceedings of SASI4 2019
  - Cioroaica, Emilia, Stanislav Chren, Barbora Buhnova, Thomas Kuhn a Dimitar Dimitrov. ”Reference Architecture for Trust-Based Digital Ecosystems”.
  - Cioroaica, Emilia, Barbora Buhnova, Thomas Kuhn, and Daniel Schneider. ”Building Trust in the Untrustable”. In Proceedings of ICSE SEIS 2020 (CORE rank A*)

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