Cyber-security Excellence Hub in Estonian and South Moravia

Information Security Research Group
Institute of Computer Science
University of Tartu

https://infosec.cs.ut.ee

What is CHESS?

Develop a cross-border joint cybersecurity **research and innovation strategy** aligned with Czech and Estonian smart specialisation strategies and Europe's digital society and cyber-security goals

Develop a **training strategy** for both regions to increase cross border/sectoral cooperation and skills around the six priority areas

Raise visibility, citizen engagement, technology transfer, entrepreneurship training, staff exchange, and mutual learning in cyber-security

CHESS

Chess in CHESS

Bridging the minds, where cybersecurity prevails over the classic strategies

Internet of Secure Things

Security Certification

Verification of Trustworthy Software

Security Preservation in Blockchain

Post-Quantum Cryptography

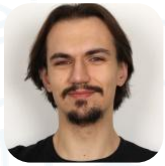
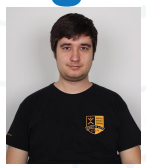
Human-centric Aspects of Cybersecurity

CHESS

Cyber-security Excellence Hub in Estonia and South Moravia

Internet of Secure Things

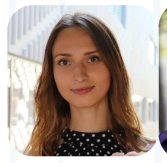


Security Certification

Verification of Trustworthy Software

Security Preservation in Blockchain



Post-Quantum Cryptography

Human-centric Aspects of Cybersecurity

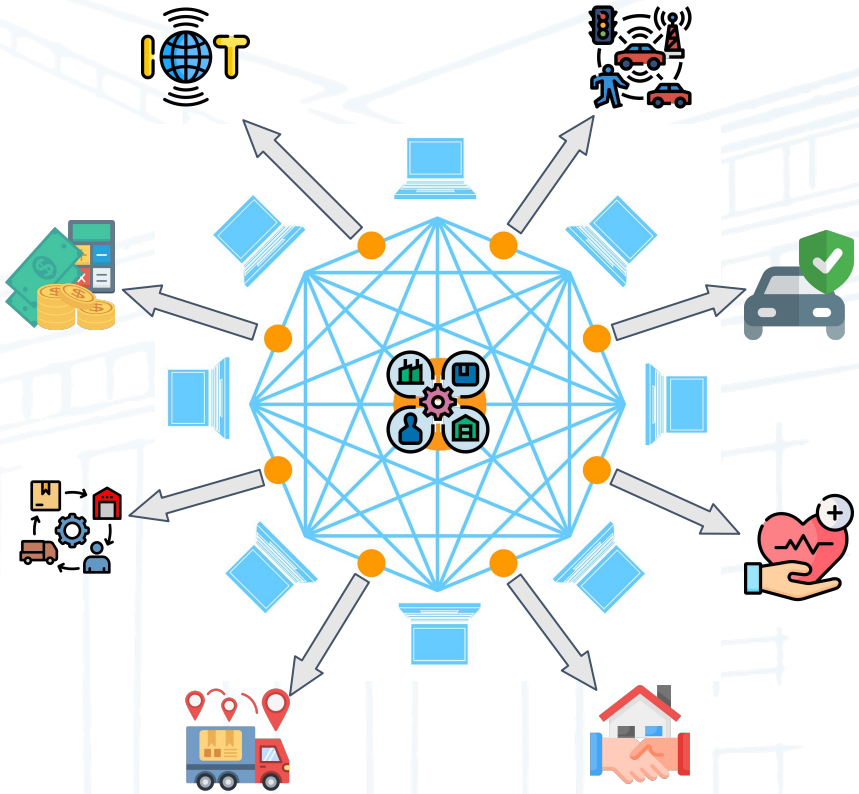
CHESS

Cyber-security Excellence Hub in Estonia and South Moravia

Security Preservation in Blockchain

Leading blockchain-related challenge area

Security Preservation in Blockchain



Decentralized and

distributed ledger technology that **securely** records and

verifies transactions across a

network of computers

https://chess-eu.cs.ut.ee/reseach-areas/security-preservation-in-blockchain/

Security Preservation in Blockchain

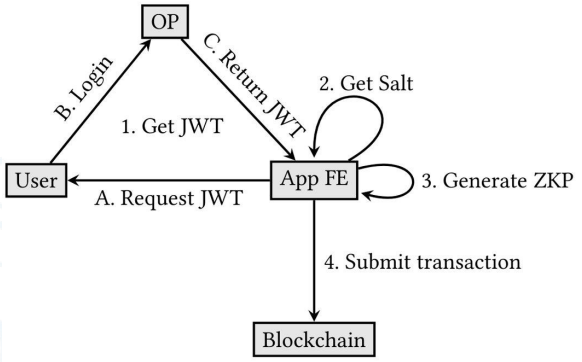
Do you need a **Blockchain**?

The answer is **CHESS**

https://chess-eu.cs.ut.ee/reseach-areas/security-preservation-in-blockchain/

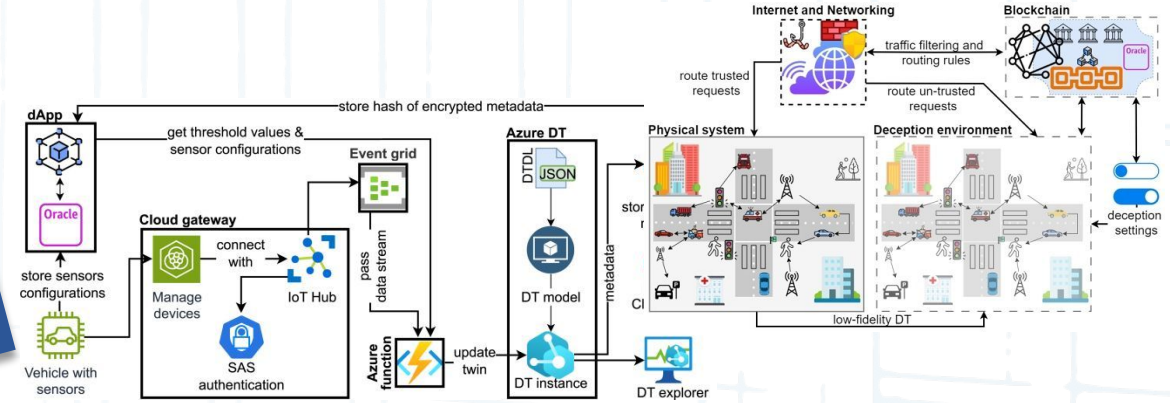
https://chess-eu.cs.ut.ee/reseach-areas/security-preservation-in-blockchain/

CHESS



Security Preservation in Blockchain

- Self-sovereign identity in the data exchange systems
- Blockchain for secure intelligent vehicles
- Blockchain operations protected by cryptographic hardware
- Coin Mixers for blockchain transactions privacy
- Methods for more compact and secure blockchains



CHESS

Cyber-security Excellence Hub in Estonia and South Moravia

Securing Organisational Identity

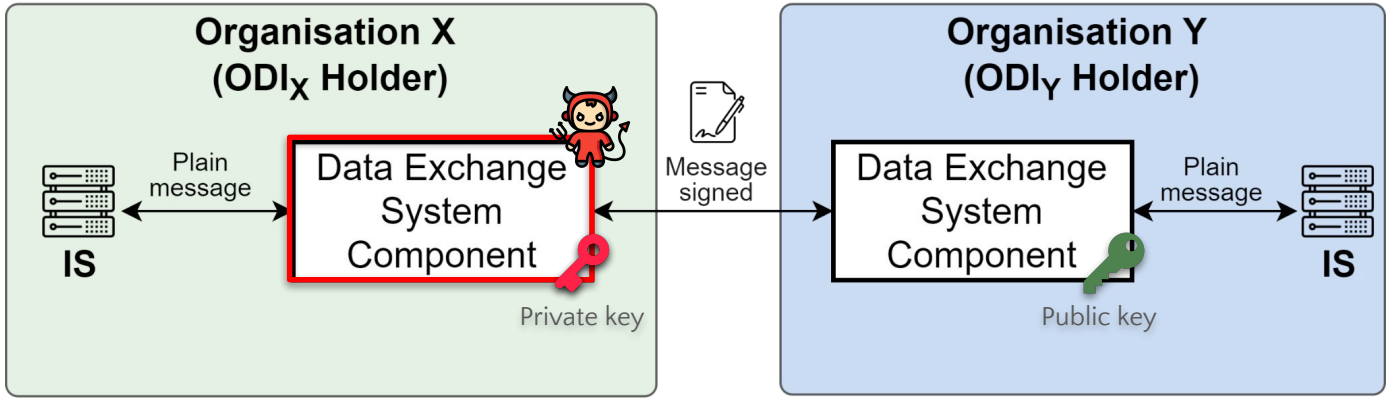
Securing Organisational Identity

Data Exchange Systems

- E-government infrastructure
- Private companies network

For example, X-Road and UXP

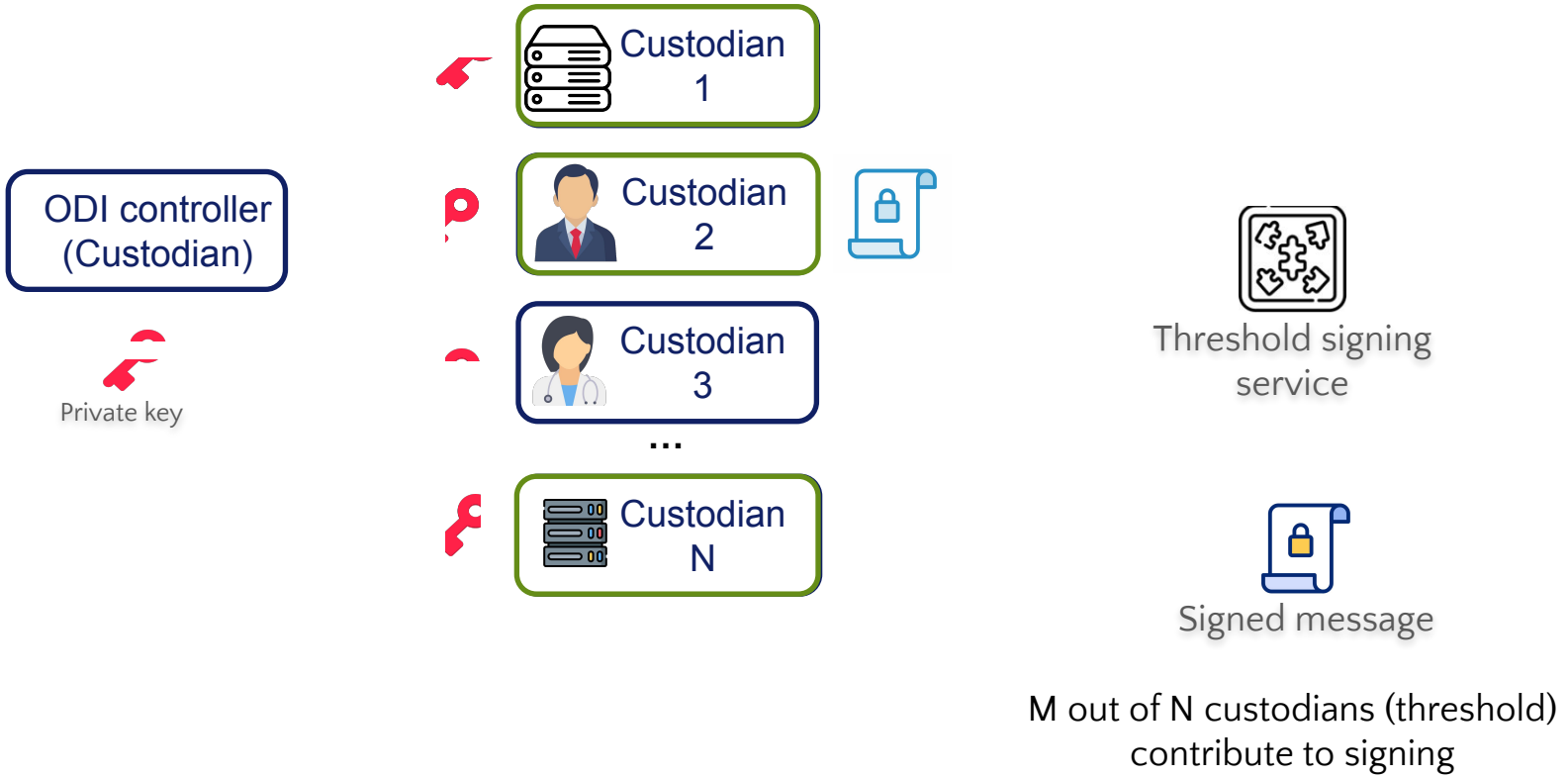
Organisational Identity



Distributed Key Management System (DKMS) for Organisational Identity

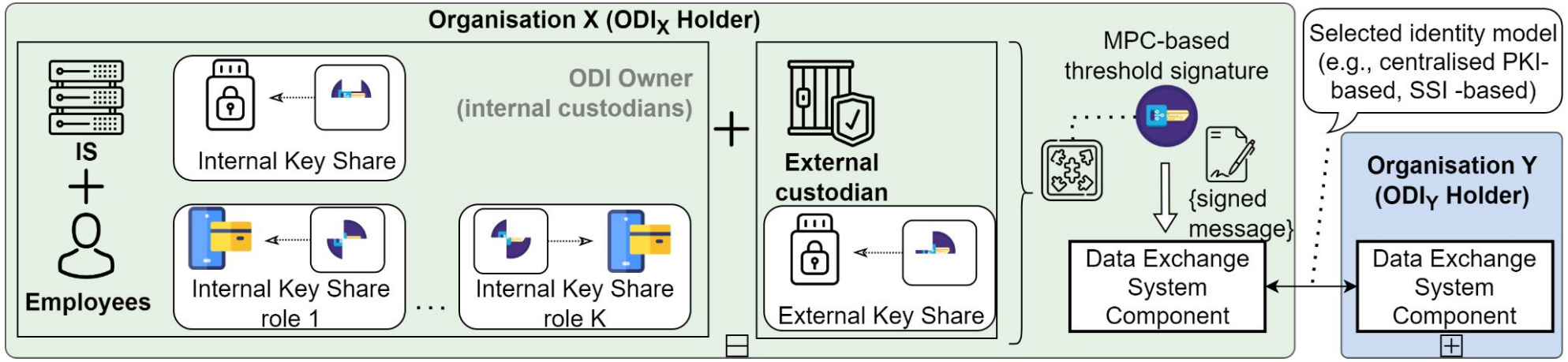
Mariia Bakhtina, Jan Kvapil, Petr Švenda, and Raimundas Matulevičius. “The Power of Many: Securing Organisational Identity Through Distributed Key Management”. In: Advanced Information Systems Engineering (CAiSE). Cham: Springer Nature Switzerland, 2024, pp. 475–491.

Distributed Key Management System (DKMS) for Organisational Identity



Mariia Bakhtina, Jan Kvapil, Petr Švenda, and Raimundas Matulevičius. "The Power of Many: Securing Organisational Identity Through Distributed Key Management". In: Advanced Information Systems Engineering (CAiSE). Cham: Springer Nature Switzerland, 2024, pp. 475–491.

Distributed Key Management System (DKMS) for Organisational Identity



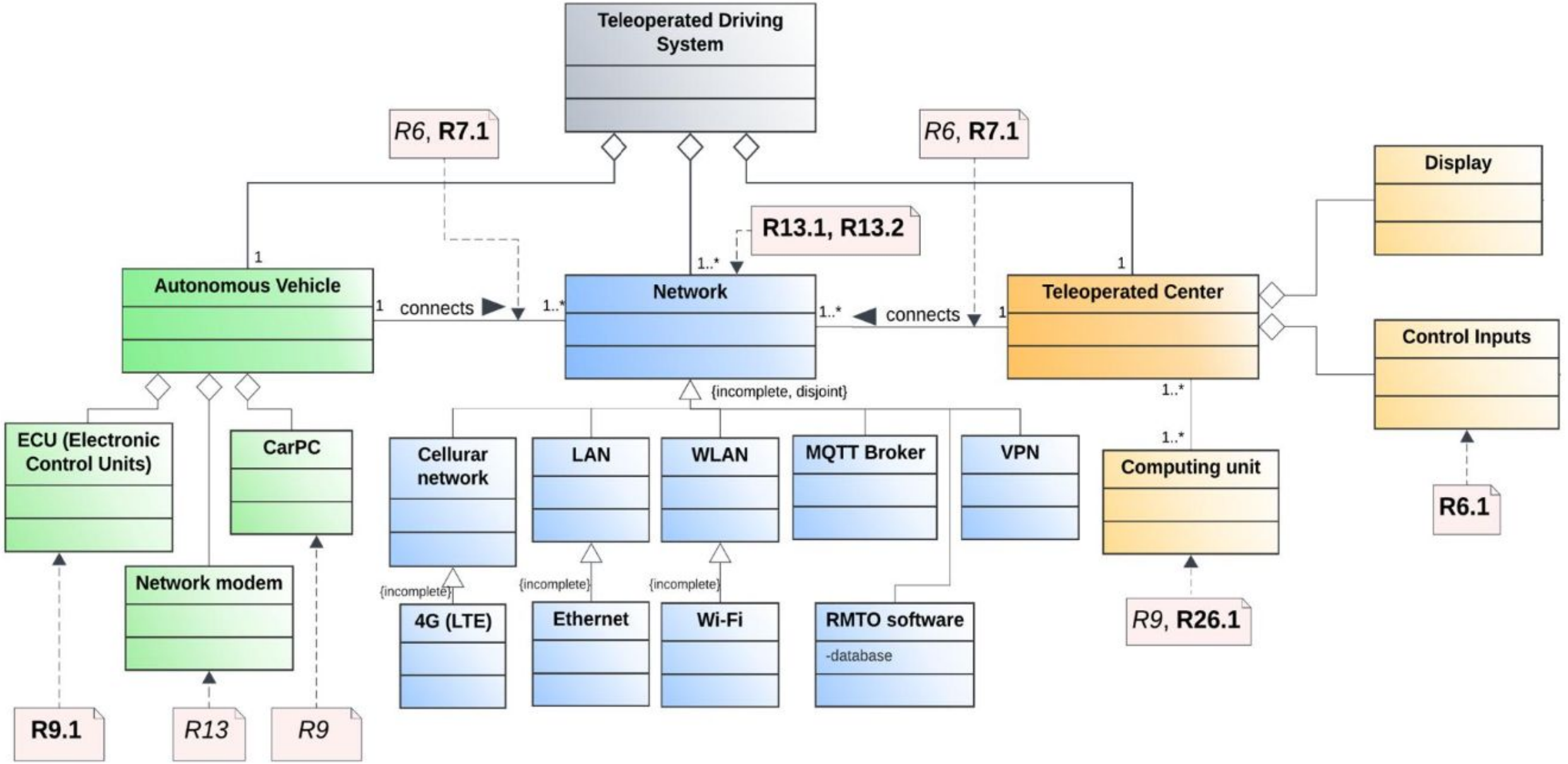
- Distribution of trust among the organisational parties – employees and IS components
- Maintaining access control in case of employee turnover
- Cryptographic enforcement of access policies

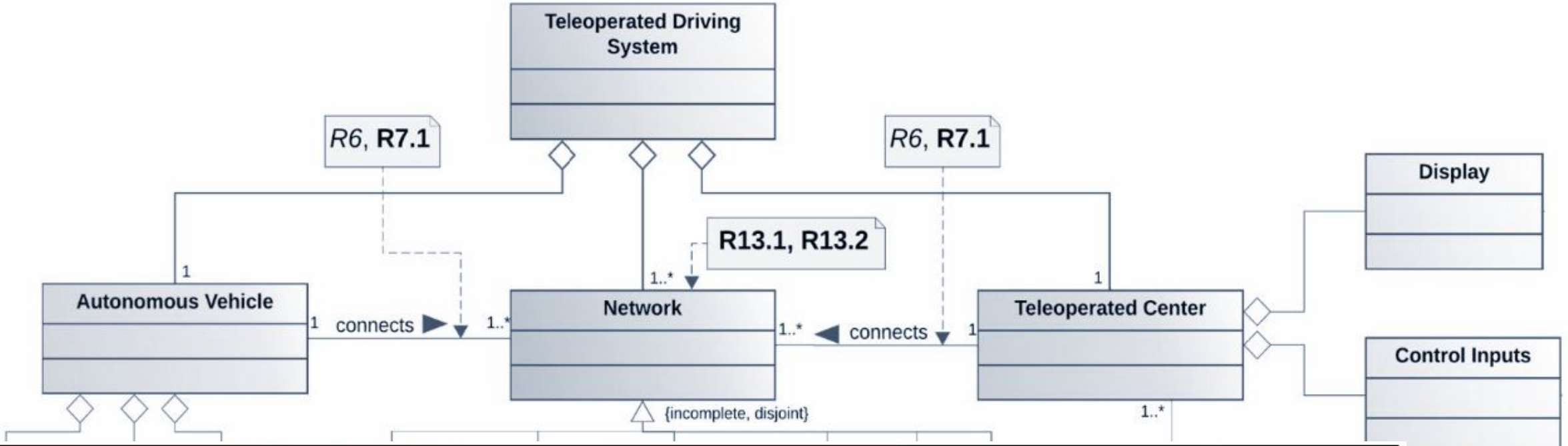
Mariia Bakhtina, Jan Kvapil, Petr Švenda, and Raimundas Matulevičius. "The Power of Many: Securing Organisational Identity Through Distributed Key Management". In: Advanced Information Systems Engineering (CAiSE). Cham: Springer Nature Switzerland, 2024, pp. 475–491.

CHESS

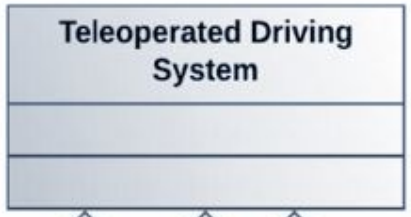
Cyber-security Excellence Hub in Estonia and South Moravia

Security Risk Management fo
Teleoperated Driving Systems


Teleoperated Driving System
R6, R7.1
R6, R7.1
R13.1, R13.2
Display
Autonomous Vehicle
connects
Network
connects
Teleoperated Center
Control Inputs
{incomplete, disjoint}
ECU (Electronic Control Units)
CarPC
Cellurar network
LAN
WLAN
MQTT Broker
VPN
Computing unit
R6.1
Network modem
{incomplete}
{incomplete}
{incomplete}
4G (LTE)
Ethernet
Wi-Fi
RMTO software
-database
R9.1
R13
R9
R9, R26.1



Risk-related Concepts				Assets-related Concepts	
ID	**Threat**	**Vulnerability**	**Impact**	**System Asset**	**Business Asset**
R6.1 [32, 33]	Unauthorised manipulation of control messages using replay attack	Vulnerabilities in *Control Input* devices	Negating the **integrity** of Steering Angle, Acceleration Commands, Braking Commands, Gear Selection, Activation of Additional Functions	Control Inputs	Steering Angle, Acceleration Commands, Braking Commands, Gear Selection, Activation of Additional Functions



R6, R7.1

R6, R7.1

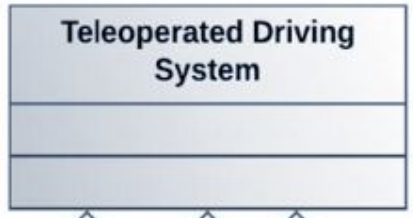
Display

ntrol Inputs

R6.1

Risk	Security Requirement	Security Control
R6.1. Unauthorised manipulation of control messages using replay attack	**SR1.** The TDS should generate unique secure session IDs for each new teleoperation session.	**SC1.** Implement a secure random session ID generation [38].
	SR2. The TDS should validate the session ID associated with each incoming control message to match it with the active session.	**SC2.** Implement session management and storage to check and verify session IDs [9].
	SR3. The TDS should add timestamps to all control messages.	**SC3.** Implement timestamp validation logic (e.g., reject messages older than 100 ms to 500 ms) [9].

ID					
R6.1 [32, 33]	tion of control messages using replay attack	*Input* devices	Angle, Acceleration Commands, Braking Commands, Gear Selection, Activation of Additional Functions		mands, Braking Commands, Gear Selection, Activation of Additional Functions



R6, R7.1

R6, R7.1

Display

Control Inputs

R6.1

Risk ID	BV	RRL	CC	BV_{norm}	RRL_{norm}	CC_{norm}	Score	Rank
R6.1	11	9	5	0.1818	0.6667	0.375	0.3659	5
R7.1	20	6	4	1.0000	0.3333	0.250	0.6500	2
R9.1	9	12	10	0.0000	1.0000	1.000	0.5000	3
R13.1	20	3	2	1.0000	0.0000	0.000	0.5000	3
R13.2	20	9	3	1.0000	0.6667	0.125	0.7250	1
R26.1	11	6	5	0.1818	0.3333	0.375	0.2659	6

Risk	Security Requirement	Security Control
R6.1. Unauthori… manipulat… control messages … replay att…		…lom ses- …agement … session … valida- …es older than 100 ms to 500 ms) [9].

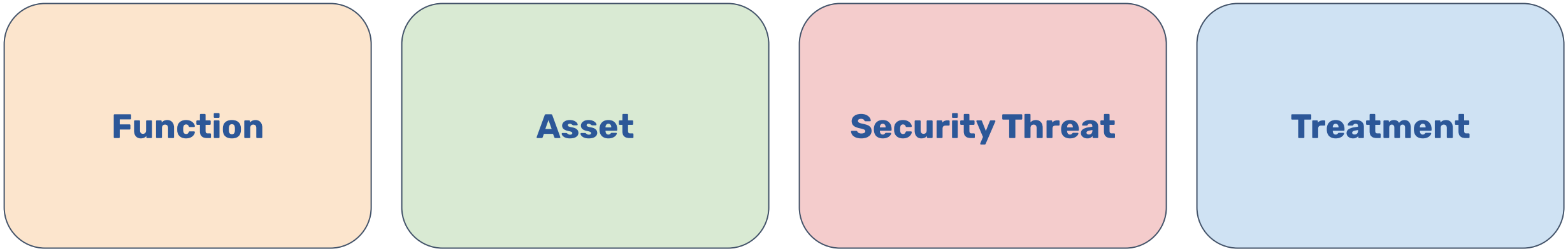
ID	T…				
R6.1 [32, 33]	U… r… tion of control messages using replay attack	*Input* devices	Angle, Acceleration Commands, Braking Commands, Gear Selection, Activation of Additional Functions		mands, Braking Commands, Gear Selection, Activation of Additional Functions

CHESS

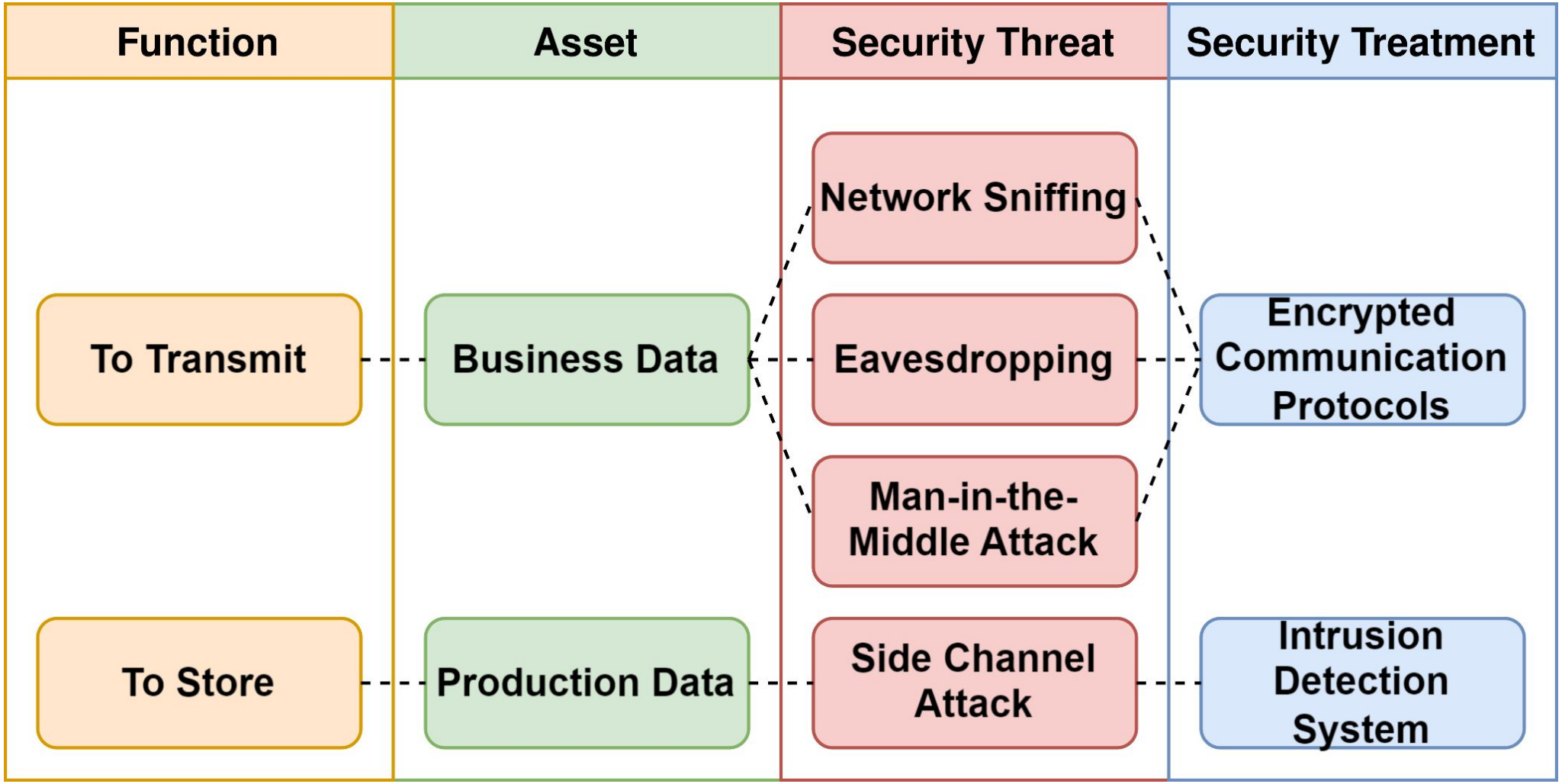
Cyber-security Excellence Hub in Estonia and South Moravia

Structured Approach to Cyber-Physical Security in Automated Manufacturing

The FAST approach



Example: FAST in Action



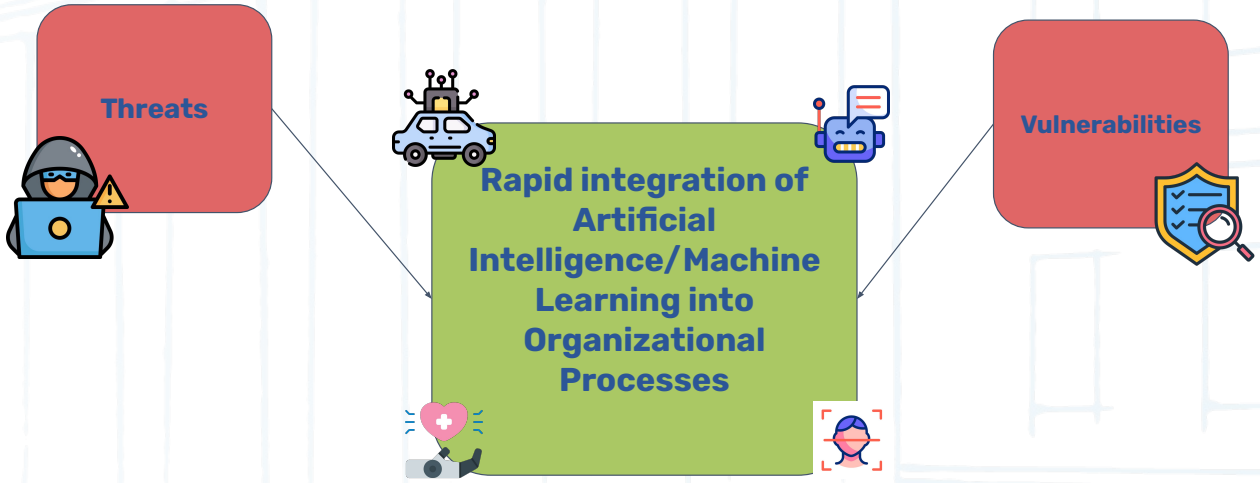
CHESS

Cyber-security Excellence Hub in Estonia and South Moravia

A Model for Security Risk Management in AI-Supported Applications

A model for security risk management in AI-supported applications

Why Secure AI/ML Systems?



Icons from https://www.flaticon.com/

A model for security risk management in AI-supported applications

Why Secure AI/ML Systems?

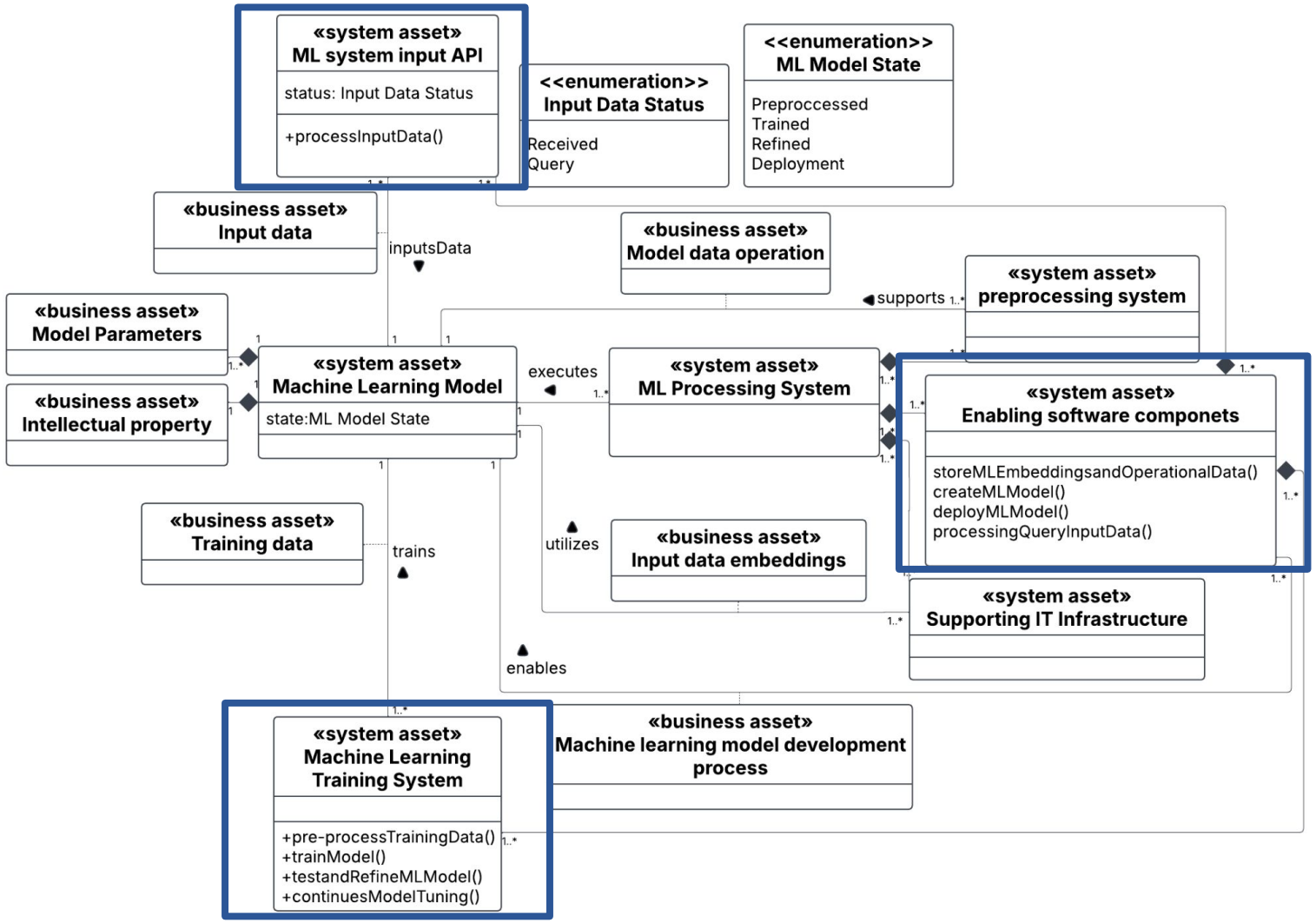
Regulations/Frameworks
- EU AI Act
- ISO/IEC
- NIST RMF
- MITRE ATLAS
- OWASP

Challenge Gaps → **Evolving Threat Landscape**, **Unified Framework for AI/ML Security** → **Development of a Conceptual Model to address AI/ML Security at each level of the lifecycle**

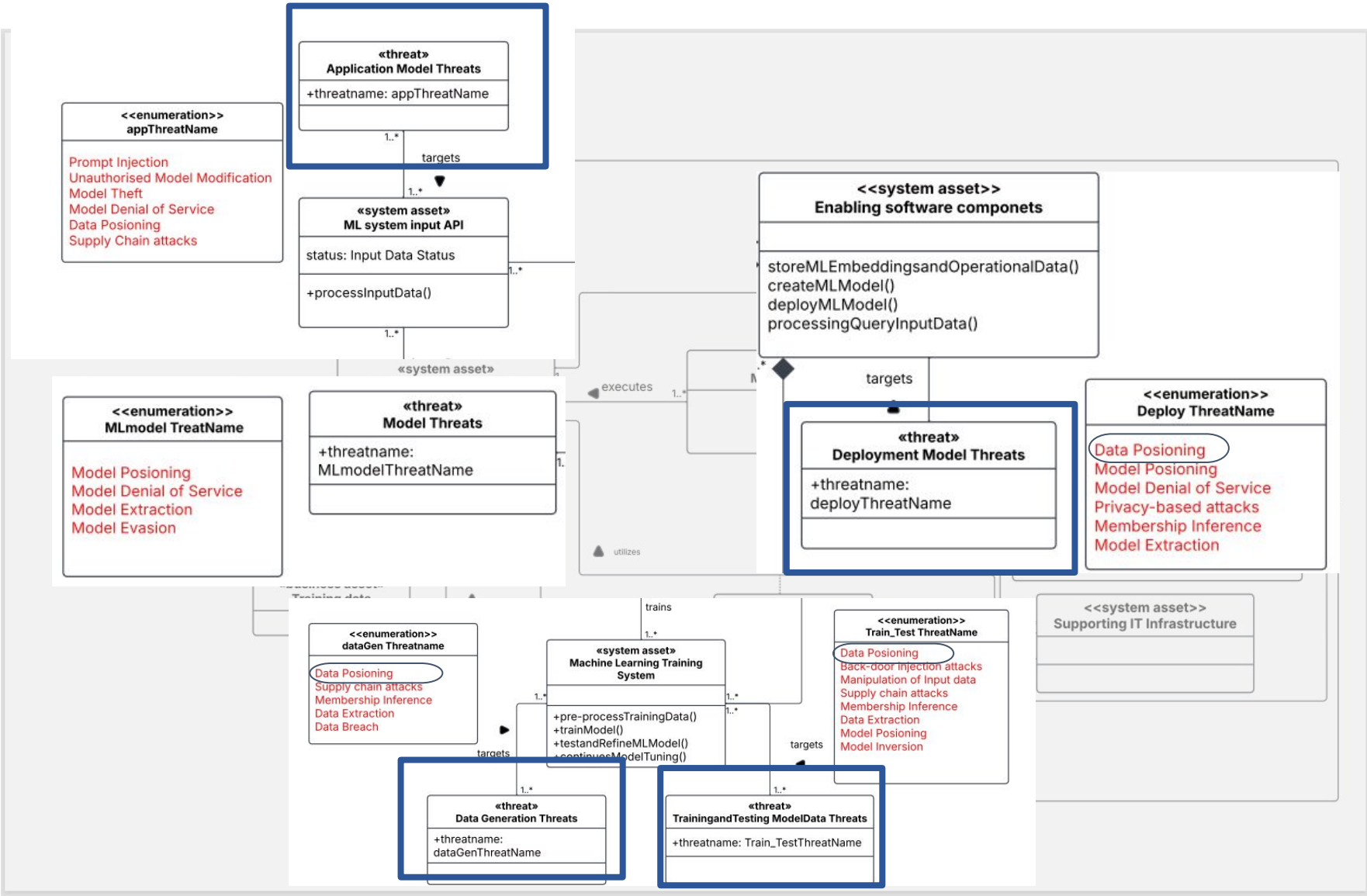
Related works

Model for SRM in AI/ML Systems

- Definition of the lifecycle of AI/ML system
- Definition of assets for AI/ML systems
- The activities taking place within each lifecycle phase
- Threat Modelling for AI

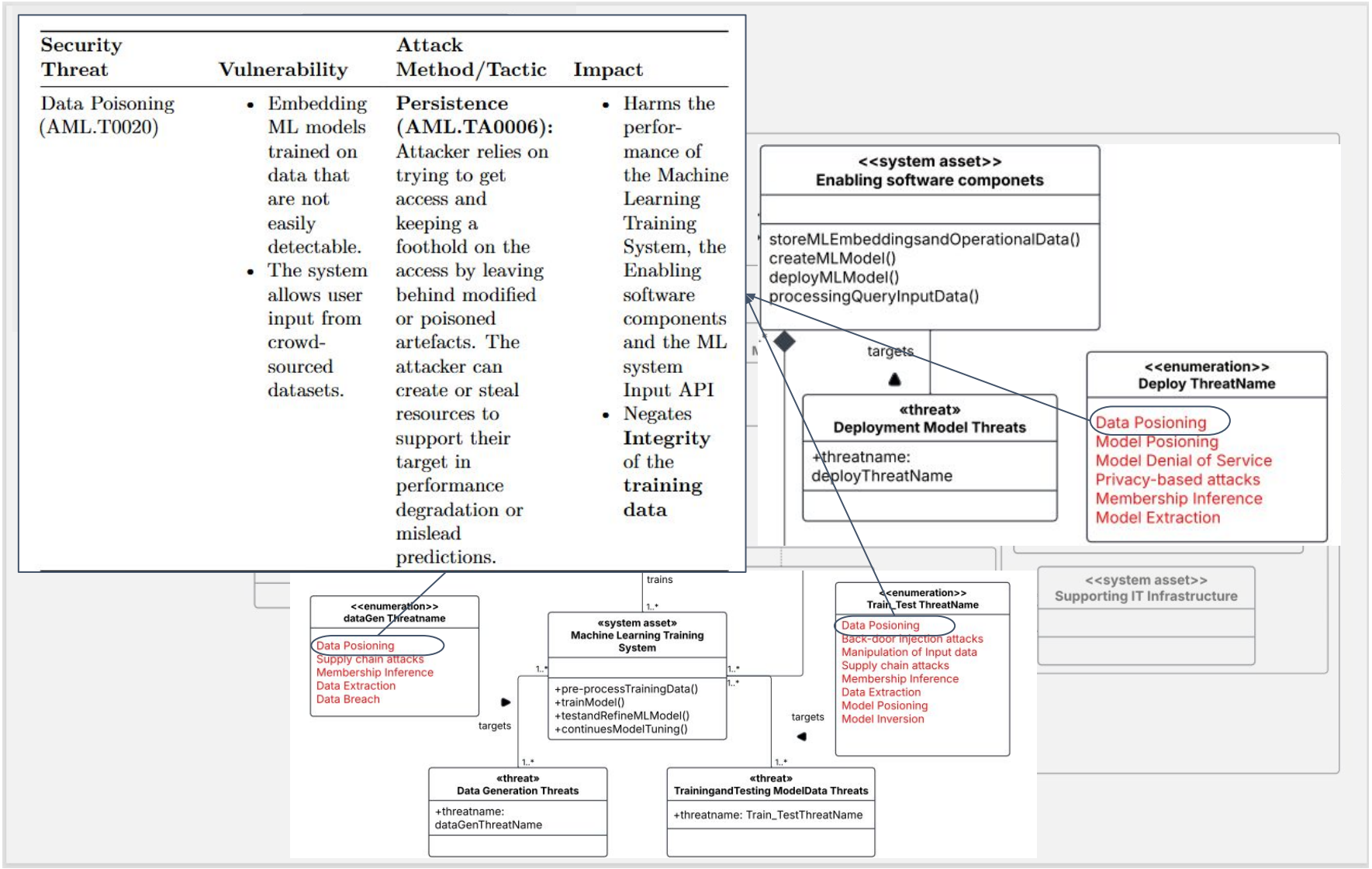


Threat Modelling for AI/ML Systems (When not How)



Model for SRM in AI/ML Systems

Security Threat	Vulnerability	Attack Method/Tactic	Impact
Data Poisoning (AML.T0020)	• Embedding ML models trained on data that are not easily detectable. • The system allows user input from crowd-sourced datasets.	**Persistence (AML.TA0006):** Attacker relies on trying to get access and keeping a foothold on the access by leaving behind modified or poisoned artefacts. The attacker can create or steal resources to support their target in performance degradation or mislead predictions.	• Harms the performance of the Machine Learning Training System, the Enabling software components and the ML system Input API • Negates **Integrity** of the **training data**



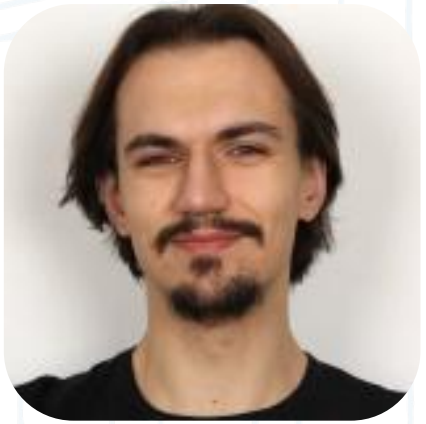
A model for security risk management in AI-supported applications

Interested to develop Secured AI/ML Systems?

CHESS

Cyber-security Excellence Hub in Estonia and South Moravia

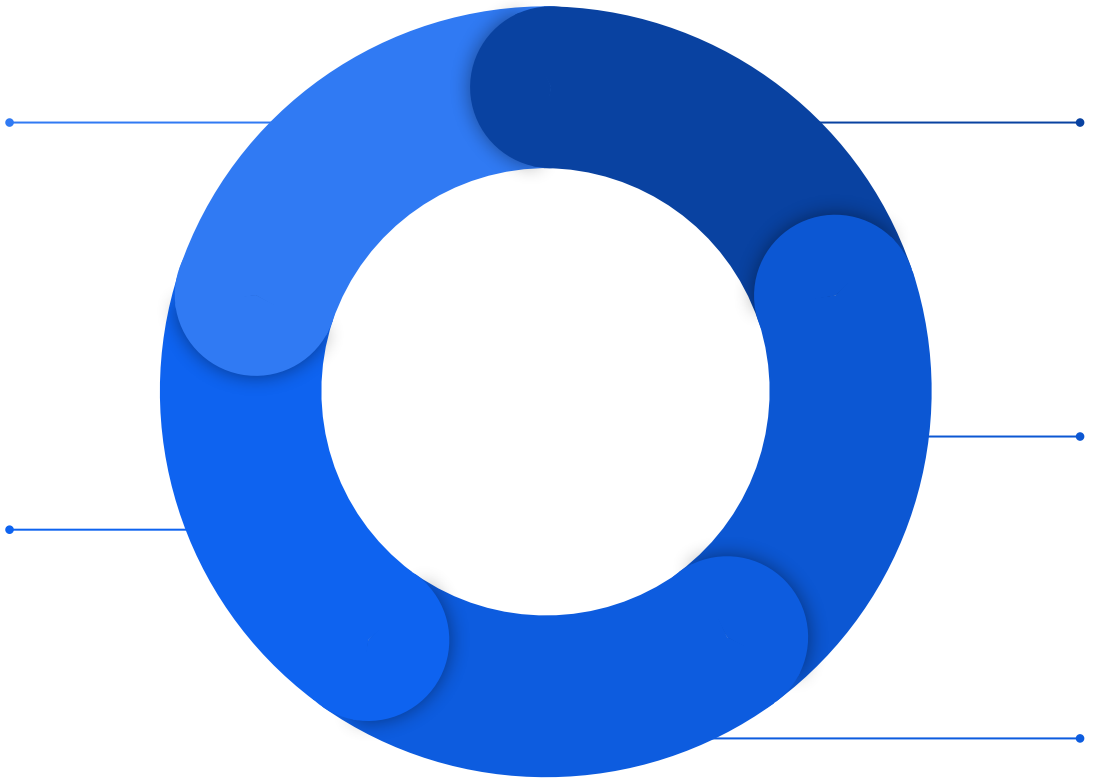
Forensic-Ready Software Development Framework



Forensic-Ready Software Development Framework

Assets, Risks, & Goals

Define Forensic Readiness Scenarios

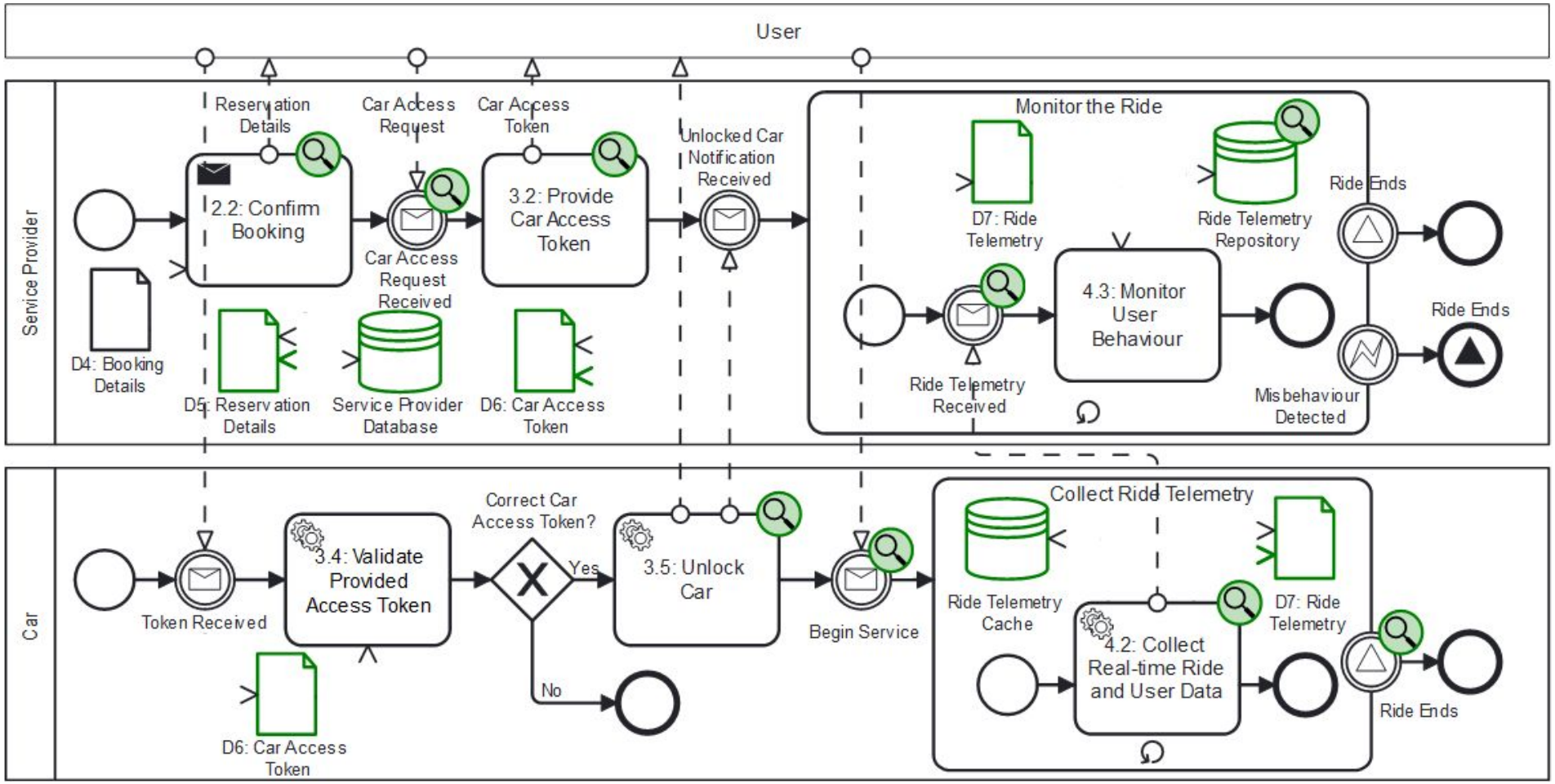


Evaluate & Verify

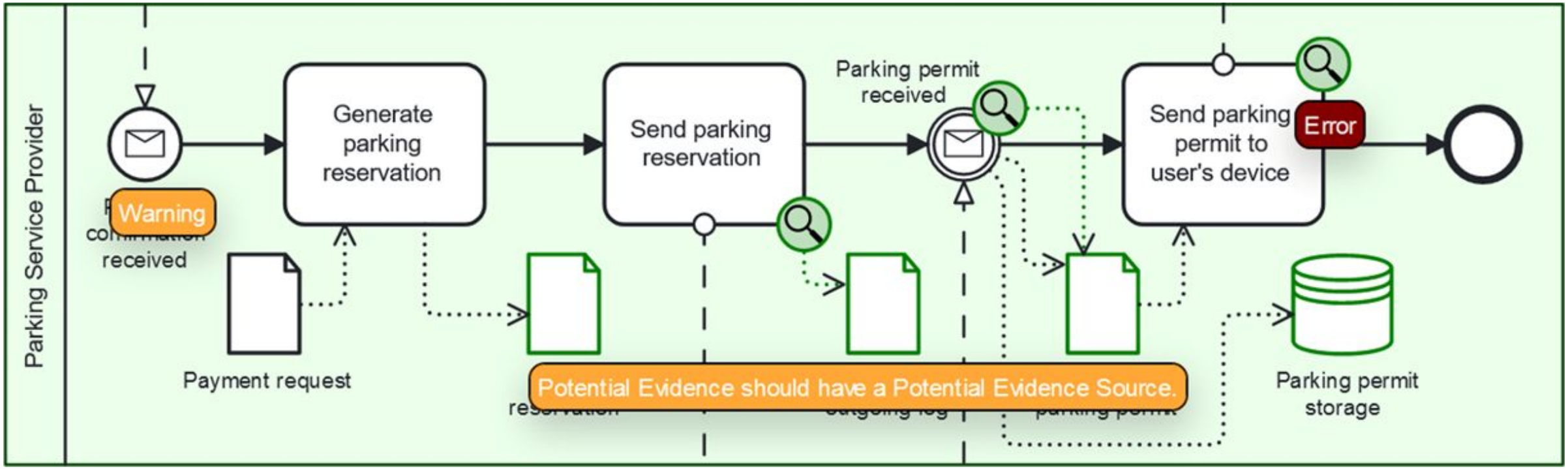
Implement Controls

Elicit Requirements

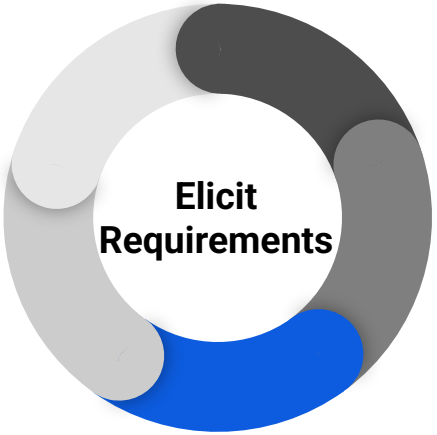
BPMN for Forensic-Ready Software Systems



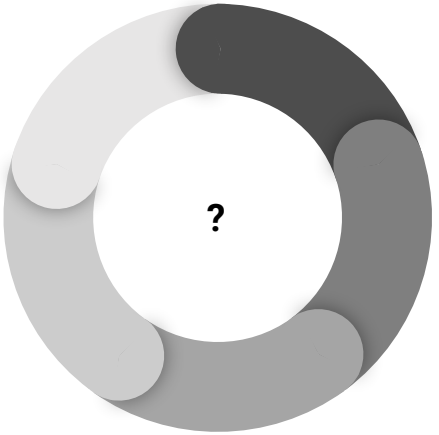
FREAS: Forensic-Ready Analysis Suite



Forensic Readiness vs. Privacy



What Can YOU Do for Forensic Readiness?



- Do you have an interesting case?
- Got an idea about forensic-ready systems?
- Does your system/method needs to work with evidence?
- Try FREAS: https://freas-tools.github.io/wiki/

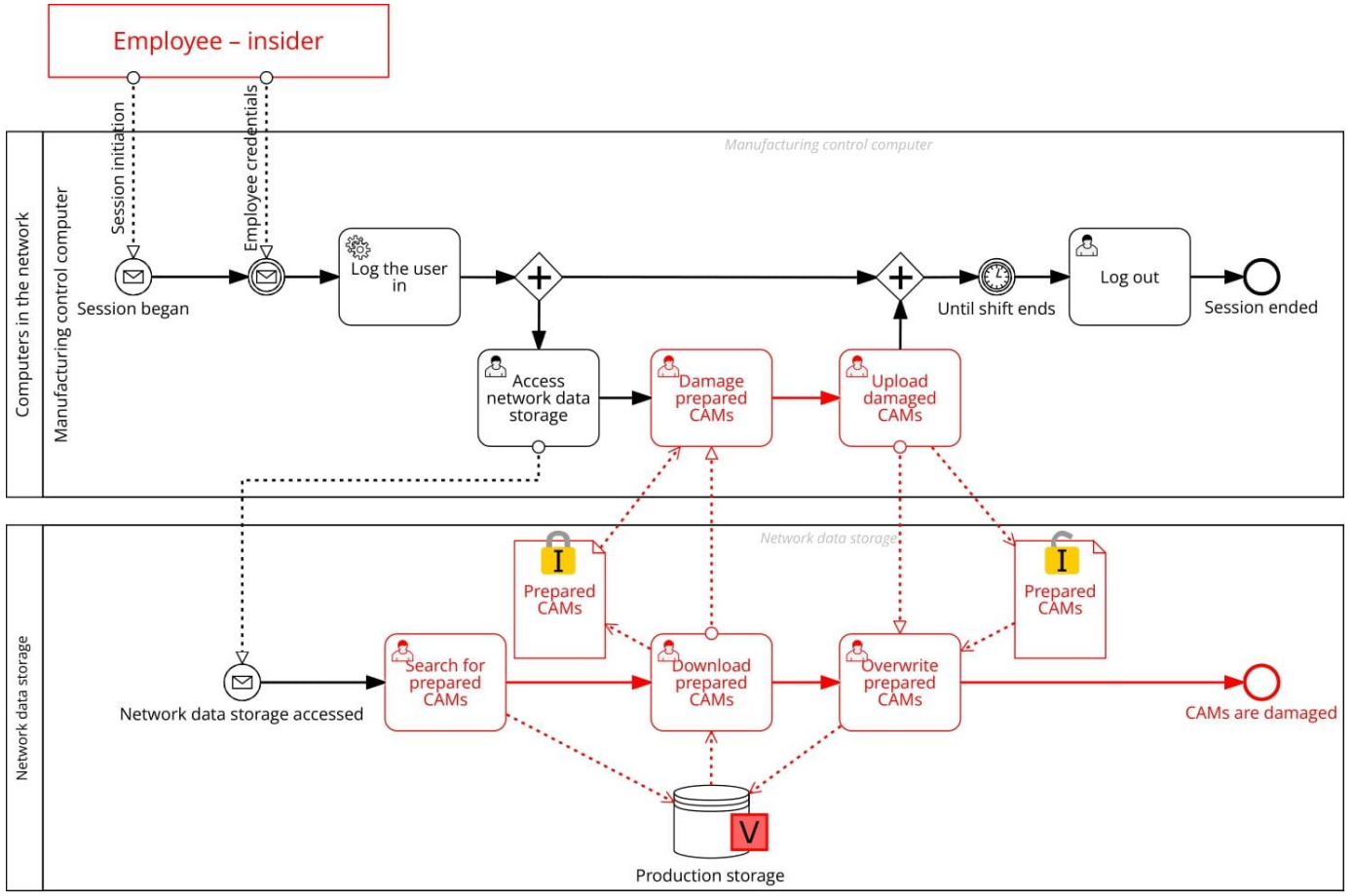
CHESS

Cyber-security Excellence Hub in Estonia and South Moravia

Process-Oriented Security Risk Management

Security risks in complex processes

- How to detect security risk outliers in the complex process execution and provide usable insights?

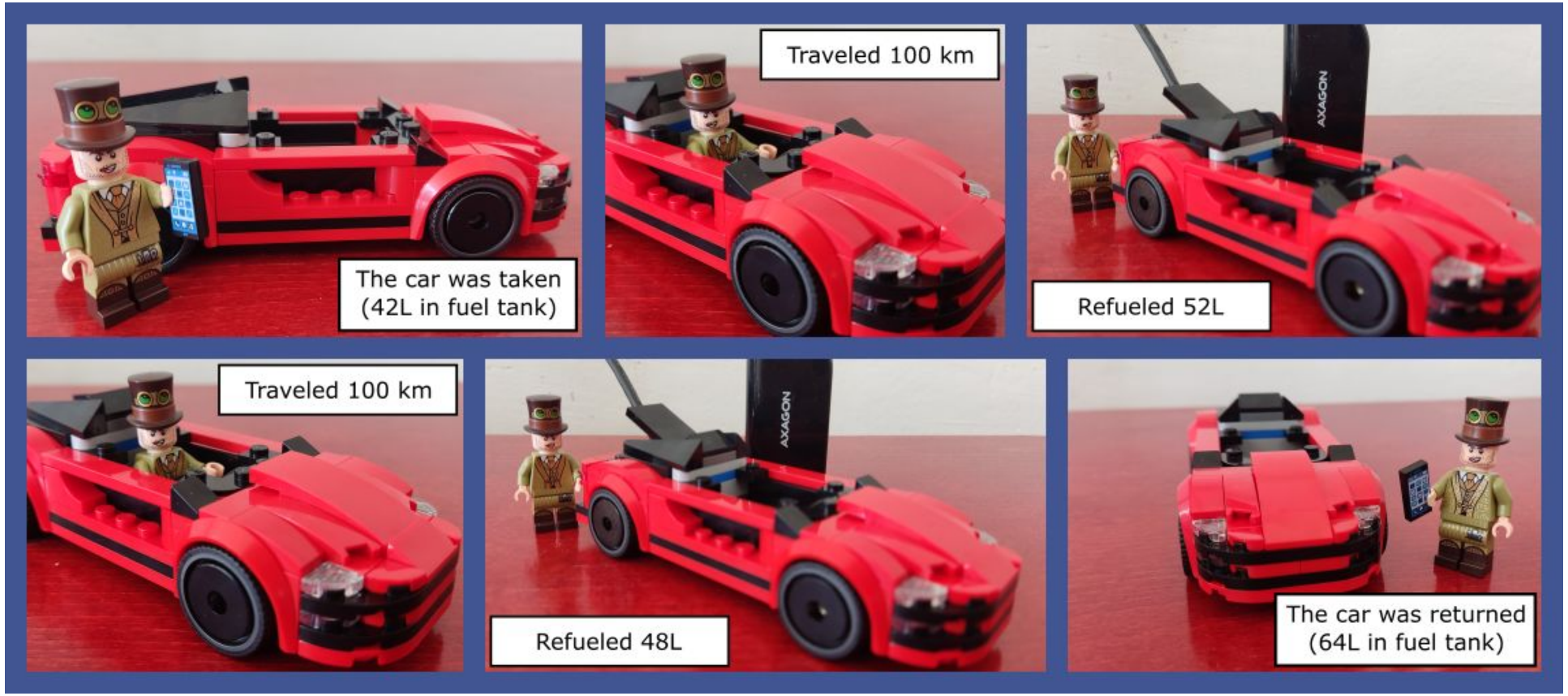


Car Sharing Case Study

- We partnered up with a Czech car sharing company Autonapůl.
- Identify carsharing processes and key assets.
- Develop normative process models.
- Define security risk scenarios.

Process Mining Utilization

- Conformance checking used to detect the outliers in the process execution.



- Visual analytics techniques allowing the analyst to gain insight and assess the severity of the security risk.

CHESS

Cyber-security Excellence Hub in Estonia and South Moravia

F4SLE: Framework for Security Level Evaluation

What is my security situation?

Technical failure

Assets?

Supply chain failure

How to stay competitive?

Cyberattacks

E-ITS

GDPR

ISO27001

NIS2

Reporting of security status to NSCS

F4SLE *Framework for Security Level Evaluation*

Self-assessment

Immediate result

All-hazard approach
ISO27001, NIS2, E-ITS, ENISA
Threat landscape report

Comparision benchmarks

- *Seeba, M., Matulevičius, R., & Toom, I. (2021, July). Development of the Information Security Management System Standard for Public Sector Organisations in Estonia. BIS2021*
- *Seeba, M., Mäses, S., Matulevičius, R. (2022). Method for Evaluating Information Security Level in Organisations. RCIS 2022*
- *Seeba,M., Affia, A.-a.,O., Mäses, S., Matulevičius, R. (2024) Create Your Own MUSE: a Method for Updating Security Level Evaluation Instruments. Computer Standards & Interfaces*

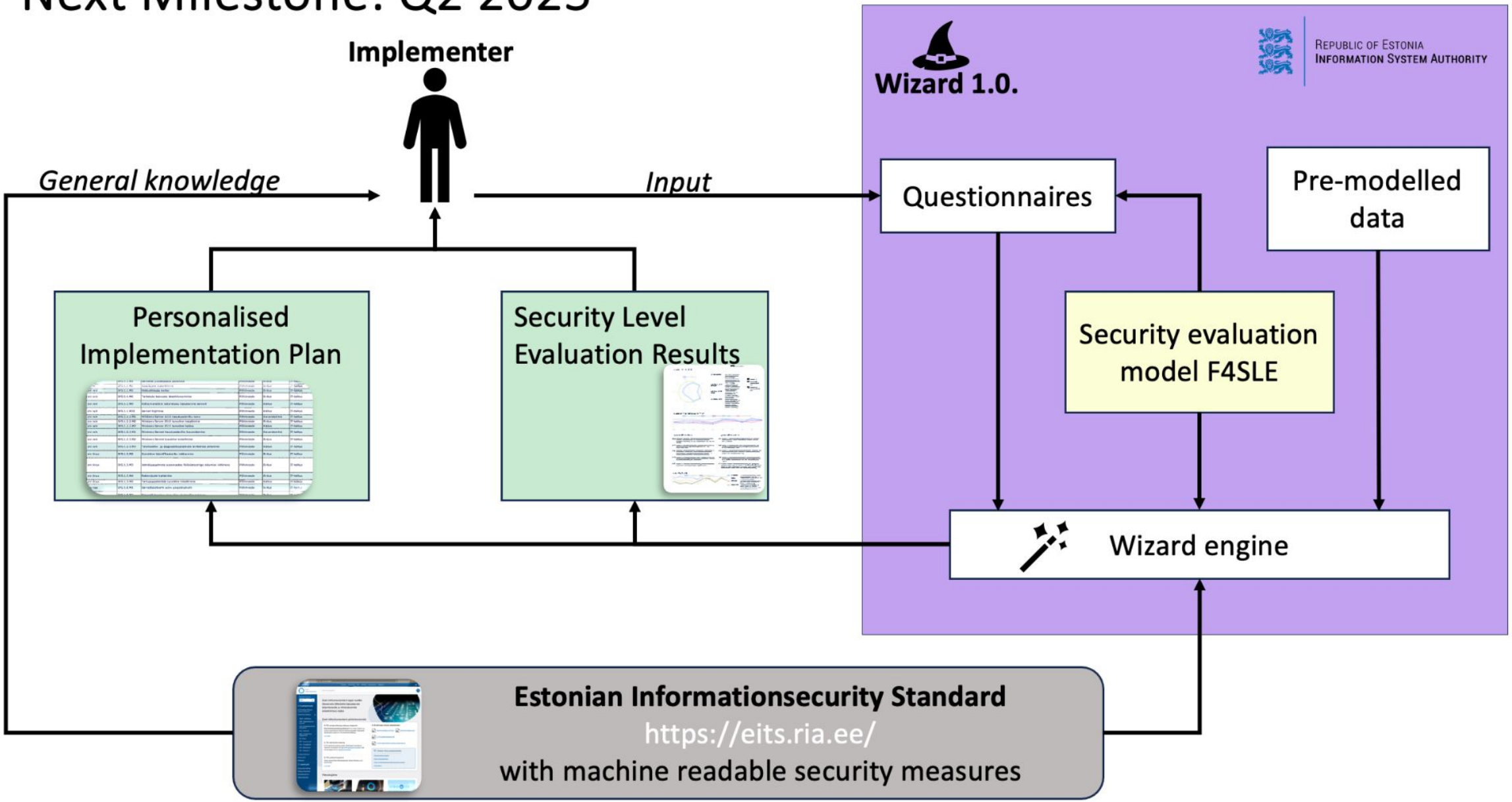
https://mass.cloud.ut.ee/massui/

User stories (data reuse by NIS2 Directive)

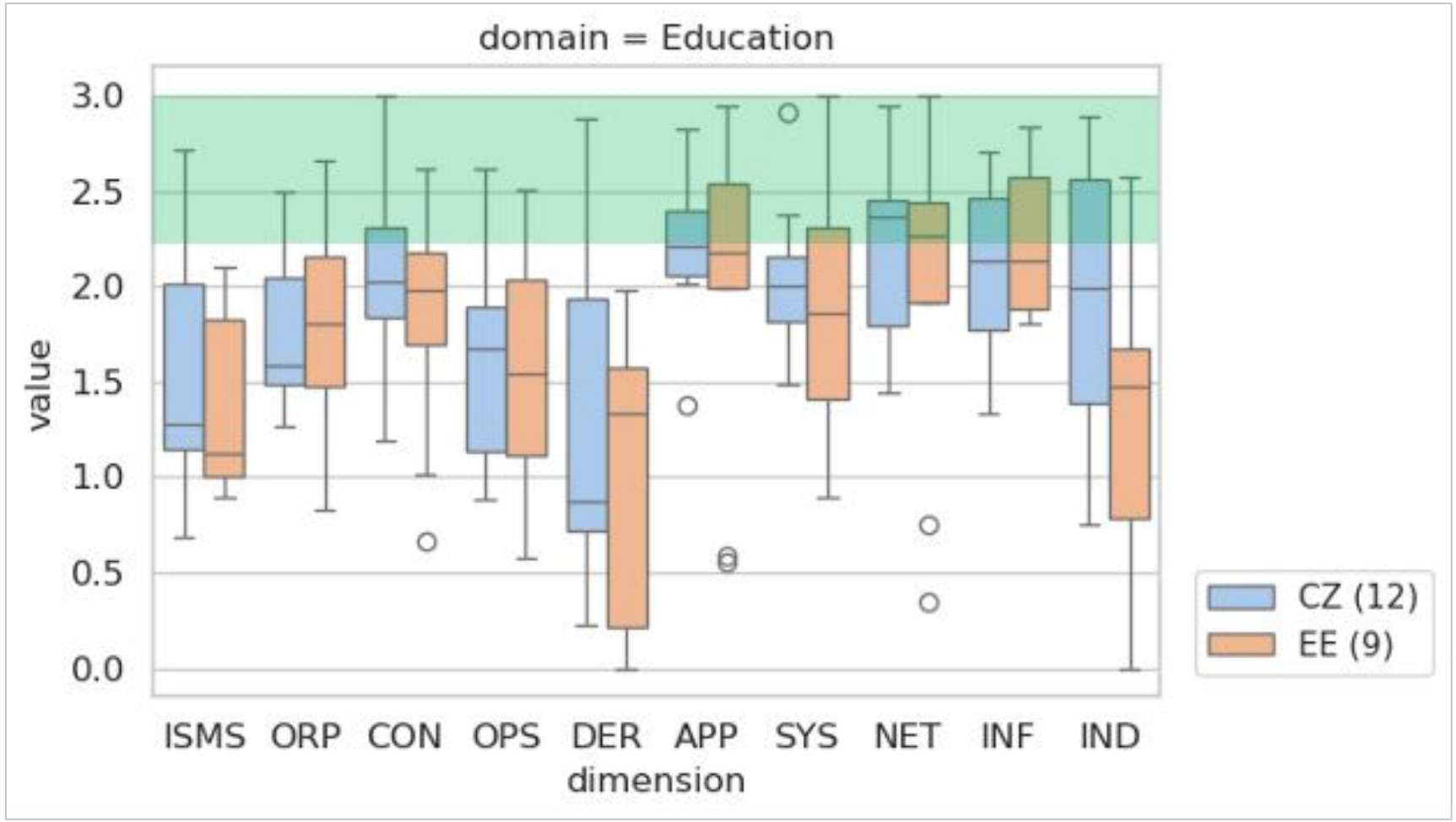
Policymaker	• Awareness, support measures, monitoring of changes
Supervisory	• Automatization, effectiveness
ENISA	• Awareness, comparability with oters (standardised sec. eval.)
Consultant	• Focuspoints, monitoring of changes
Organization	• Awareness, planning, benchmarking, replacement of audit?
Supplier	• Awareness, compliance, benchmarking

- *Seeba, M., Oja, T., Murumaa, M., P., and Stupka, V. (2023). Security level evaluation with F4SLE. ARES2023*
- *Seeba, M., Valgre, M., Matulevičius, R. (2025). Evaluating Organization Security: User Stories of European Union NIS2 Directive (will be published in June) CAISE2025*

Next Milestone: Q2 2025

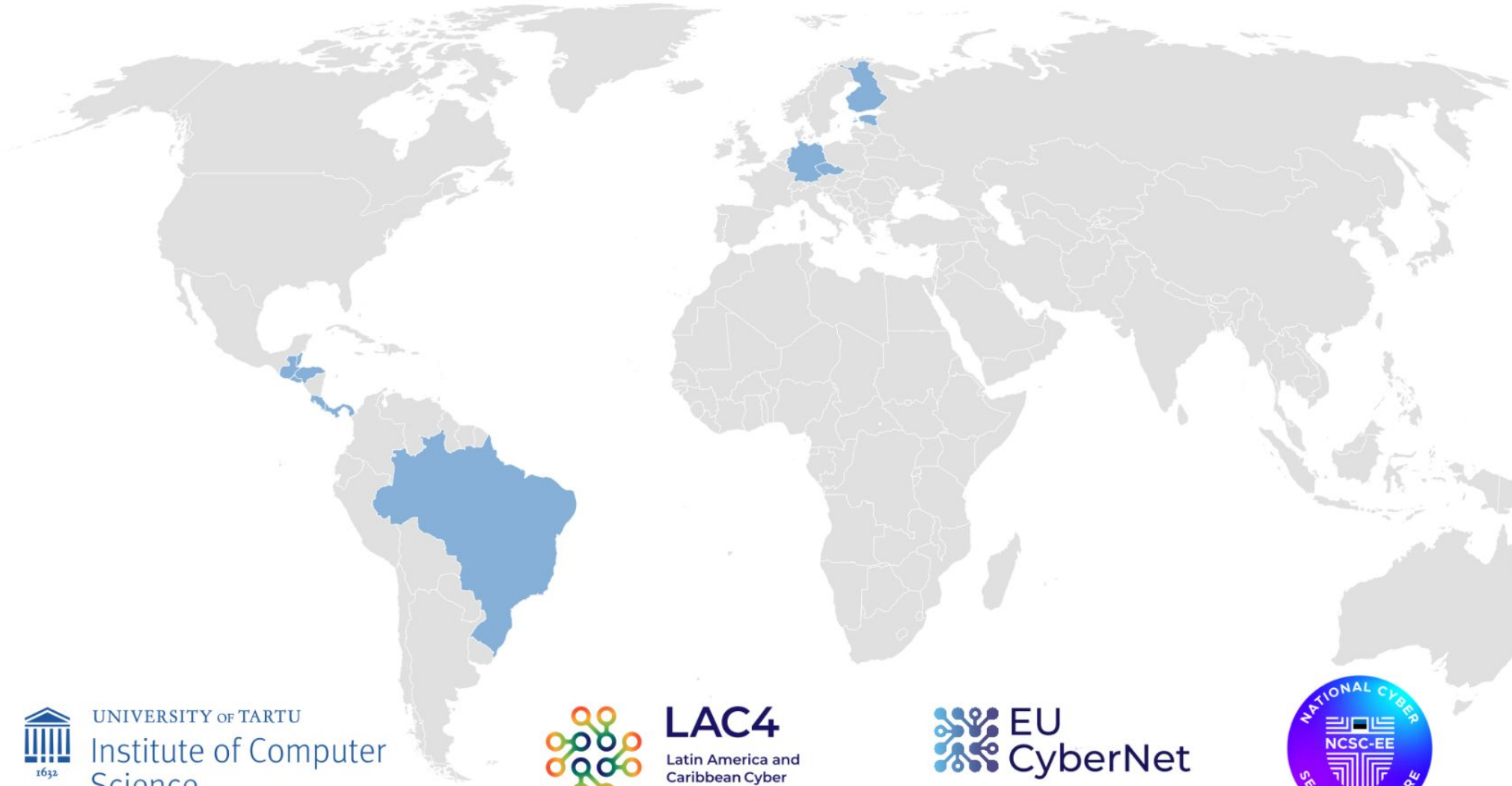


Estonia vs Czech - Education



https://mass.cloud.ut.ee/massui/

Dissemination by testing and training



UNIVERSITY OF TARTU
Institute of Computer Science

LAC4
Latin America and Caribbean Cyber Competence Centre

EU CyberNet

NATIONAL CYBER SECURITY CENTRE
NCSC-EE

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

Building blocks of security level evaluation (F4SLE)

F4SLE- *Framework for Security level Evaluation*

- Preparatory work by choosing standard
  - *Seeba, M., Matulevičius, R., & Toom, I. (2021, July). Development of the Information Security Management System Standard for Public Sector Organisations in Estonia. BIS2021* https://doi.org/10.52825/bis.v1i.43
- framework and principles
  - *Seeba, M., Mäses, S., Matulevičius, R. (2022). Method for Evaluating Information Security Level in Organisations. In: RCIS 2022. Lecture Notes in Business Information Processing, vol 446. Springer, Cham.* https://doi.org/10.1007/978-3-031-05760-1_39
- Content versions http://dx.doi.org/10.23673/re-298; http://dx.doi.org/10.23673/re-372

MUSE - *Method for Updating Security Level Evaluation Instruments*

- How to update the F4SLE
- process, principles, inputs
  - *Seeba,M., Affia, A.-a.,O., Mäses, S., Matulevičius, R. (2024) Create Your Own MUSE: a Method for Updating Security Level Evaluation Instruments. Computer Standards & Interfaces* https://doi.org/10.1016/j.csi.2023.103776

MASS – presenting and collecting tool

- tool to present F4SLE and collect data
- immidiate results to respondents and collecting privately aggregated results to central server
- *Master thesis project of Maria Pibilota Murumaa. (2023)* Designing a tool for security level evaluation framework https://thesis.cs.ut.ee/92895428-9fc4-4248-bc78-4a00b3e90101

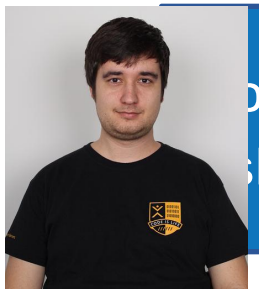
User Stories of Stakeholders

- Stakeholders who need security data of organisastions
- Collect data once and share with stakeholders
- *Seeba, M., Oja, T., Murumaa, M., P., and Stupka, V. (2023). Security level evaluation with F4SLE. ARES2023* https://doi.org/10.1145/3600160.3605045
- *Seeba, M., Valgre, M., Matulevičius, R. (2025). Evaluating Organization Security: User Stories of European Union NIS2 Directive (will be published in June) CAISE2025*

Framework for Security Level Evaluation

pperated Driving Systems

c-Ready e Development



ocess-Oriented Security sk Management

CHESS

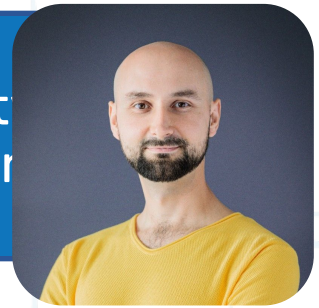
Cyber-security Excellence Hub in Estonia and South Moravia

Organisational Iden

Security Preserv Blockchain

A Model for AI-Su Applications

Cyber-Physical Securit Automated Manufactur



https://infosec.cs.ut.ee

CHESS

Cyber-security Excellence Hub in Estonia and South Moravia

X

https://x.com/CHESS_EU

Facebook:

https://www.facebook.com/ChessExcellenceHub

LinkedIn

https://www.linkedin.com/company/chess-cyber-security-excellence-hub/

https://chess-eu.cs.ut.ee

CHESS Cyber-Security Excellence Hub

@CHESS_EU · 16 subscribers · 11 videos

The Cyber-security Excellence Hub in Estonia and South Moravia (CHESS) brings together ...more

chess-eu.cs.ut.ee and 3 more links

Customize channel | Manage videos

Home | Videos | Posts

CHESS Brokerage Event

67 views • 6 months ago

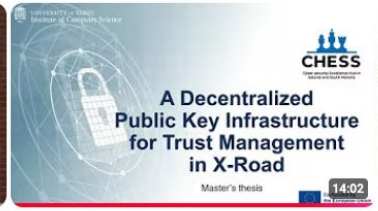
The first CHESS brokerage event brought together people from academia, industry, and governmental institutions in the field of cybersecurity.

More such events to come. Stay tuned!

For You

Why focusing on post-quantum migration is so important?

45 views • 6 months ago



A Decentralized Public Key Infrastructure for Trust Management in X-Road

64 views • 10 months ago

CHESS partner: University of Tartu

161 views • 10 months ago

Internet of Secure Things

75 views • 6 months ago

Videos

CHESS partner: Masaryk University

Introducing FREAS: Forensic-Ready Analysis Suite

CHESS Brokerage Event

67 views • 6 months ago

Internet of Secure Things

75 views • 6 months ago

Security Preservation in Blockchain

Why is post-quantum cryptography relevant today?

https://chess-eu.cs.ut.ee

SP2I 2025

at ARES 2025, Ghent, Belgium

Workshop Chair

- **Lukas Malina**
  Brno University of Technology, Czech Republic
- **Raimundas Matulevičius**
  University of Tartu, Estonia
- **Gautam Srivastava**
  Brandon University, Canada

Important Dates

- Submission: **5 May**
- Notification: **25 May**
- Conference: **August 11 – August 14**

https://2025.ares-conference.eu/program/sp2i/

NordSec 2025
Tartu, Estonia

General chair:

- **Raimundas Matulevičius**
  University of Tartu, Estonia

Program chair:

- **Liina Kamm**, Cybernetica, Estonia
- **Mubashar Iqbal**, University of Tartu, Estonia

Important Dates

- Submission: **17 August**
- Notification: **19 September**
- Conference: **12-13 November**

https://nordsec2025.cs.ut.ee/

NordSec is an annual research conference series that has been running since 1996. The NordSec conferences address a broad range of topics on IT security. The events bring together security researchers from the Nordic countries, Northern Europe, and beyond. In addition to being a venue for academic publishing, NordSec is an important meeting place for university faculty, students, and industry researchers and experts from the region.

The NordSec 2025 places a special emphasis on Security Certification and Standardisation, delving into certification practices and their role in mitigating vulnerabilities within certified products. This year's conference edition also underscores the evolving landscape of cryptographic protocols and the increasing influence of artificial intelligence and machine learning (AI/ML) on security and privacy research, recognising the unique challenges socio-technical system development poses. Key focus areas include complex societal infrastructures, healthcare, smart cities and communities, national security, and various industry sectors such as automotive, energy, and banking.

NordSec addresses a broad range of topics within cybersecurity to bring together computer security researchers and practitioners, encouraging interaction between academia and industry.

TOPICS OF INTEREST

- Applied cryptography
- Artificial intelligence and machine learning for cybersecurity and privacy
- Blockchains
- Cloud security
- Confidential computing
- Cryptanalysis
- Cryptographic protocols
- Cybercrime, warfare, and forensics
- Economic, legal, and social aspects of security and privacy
- Security certification and standardisation
- Formal analysis
- Hardware and smart card security
- Identity and access management
- Information flow security
- Intrusion detection and mitigation
- Language-based security
- Mobile, embedded, and Internet of Things security and privacy
- Operating system security
- Privacy-enhancing technologies
- Security and privacy engineering
- Security and privacy for artificial intelligence and machine learning
- Security education and training
- Security management and audit
- Security and privacy metrics
- Security and privacy protocols
- Social engineering and phishing
- Software security and malware
- Threat modelling and threat intelligence
- Trust and identity management
- Usable security and privacy
- Vulnerability testing
- Web application security

SUBMISSION GUIDELINES

Contributions should reflect original research, developments, studies, or experience. Submitted papers should be at most 16 pages (excluding references and appendices) in Springer LNCS format. Submitted papers must not substantially overlap with papers published or simultaneously submitted to a journal or a conference with proceedings.

Submissions not meeting the guidelines risk rejection without consideration of their merits. Authors of accepted papers must agree with Springer LNCS copyright and guarantee that their papers will be presented at the conference. By submitting a paper, you agree that at least one of the authors will physically attend the conference to present it. NordSec 2025 will publish fully digital online proceedings with Springer Nature in the LNCS series. All submissions will be peer-reviewed by at least three program committee members.

IMPORTANT DATES

Submission	17th August 2025
Notification	19th September 2025
Camera-ready	30th September 2025
Conference	12-13th of November 2025

ORGANIZERS

General Chair	Raimundas Matulevičius, University of Tartu, Estonia
Program Chairs	Liina Kamm, Cybernetica, Estonia
	Mubasar Iqbal, University of Tartu, Estonia
Organization Chair	Sedat Akleylek, University of Tartu, Estonia

TARTU ÜLIKOOL 1632 UNIVERSITAS TARTUENSIS

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

CYBERNETICA

NordSec 2025
Tartu, Estonia

General chair:

- **Raimundas Matulevičius**
  University of Tartu, Estonia

Program

- **Liin**
- **Mul**

Importar

- Submission: **17 August**
- Notification: **19 September**
- Conference: **12-13 November**

https://nordsec2025.cs.ut.ee/

Brokerage event in Delta

11. November, 2025

NordSec is an annual research conference series that has been running since 1996. The NordSec conferences address a broad range of topics on IT security. The events bring together security researchers from the Nordic countries, Northern Europe, and beyond. In addition to being a venue for academic publishing, NordSec is an important meeting place for university faculty, students, and industry researchers and experts from the region.

The NordSec 2025 places a special emphasis on Security Certification and Standardisation, delving into certification practices and their role in mitigating vulnerabilities within certified products. This year's conference edition also underscores the evolving landscape of

- Security certification and standardisation
- Security and privacy for artificial intelligence and machine learning
- Web application security

SUBMISSION GUIDELINES

Contributions should reflect original research, developments, studies, or experience. Submitted papers should be at most 16 pages (excluding references and appendices) in Springer LNCS format. Submitted papers must not substantially overlap with papers published or simultaneously submitted to a journal or a conference with proceedings.

Submissions not meeting the guidelines risk rejection without consideration of their merits. Authors of accepted papers must agree with Springer LNCS copyright and guarantee that their papers will be presented at the conference. By submitting a paper, you agree that at least one of the authors will physically attend the conference to present it. NordSec 2025 will publish fully digital online proceedings with Springer Nature in the LNCS series. All submissions will be peer-reviewed by at least three program committee members.

IMPORTANT DATES

Submission	17th August 2025
Notification	19th September 2025
Camera-ready	30th September 2025
Conference	12-13th of November 2025

ORGANIZERS

General Chair	Raimundas Matulevičius, University of Tartu, Estonia
Program Chairs	Liina Kamm, Cybernetica, Estonia
	Mubasar Iqbal, University of Tartu, Estonia
Organization Chair	Sedat Akleylek, University of Tartu, Estonia

TARTU ÜLIKOOL 1632 UNIVERSITAS TARTUENSIS

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

CYBERNETICA