TARTU ÜLIKOOL
1632

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

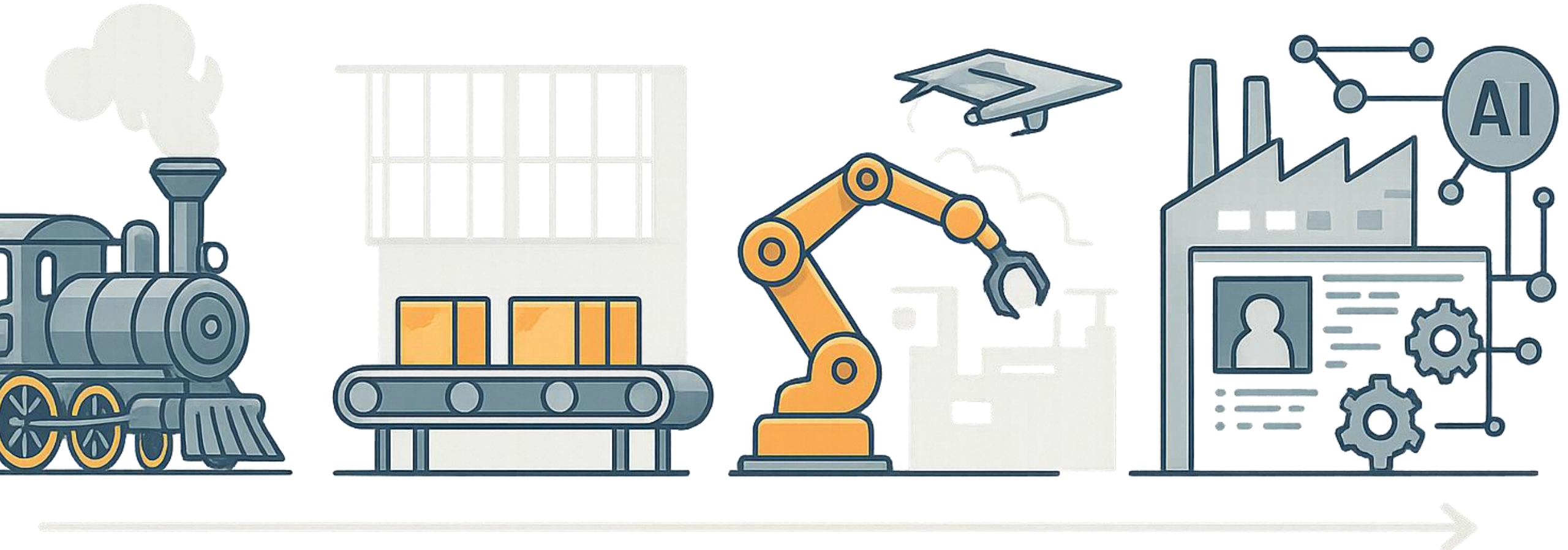
Security in Automated Manufacturing: A Function-Driven Approach

Vjatšeslav Antipenko

Supervisor: Prof. Raimundas Matulevičius

Institute of Computer Science
University of Tartu

CaiSE 2025, Vienna, Austria, 18.06.2025


AI

Why This Matters

🏭 Digitalisation boosts efficiency — **but expands attack surfaces**.

🔗 Supply chain interconnectivity **amplifies risk**.

⚠️ Operational Technology systems face **impactful threats**: downtime, damage, and loss.

🧱 **Standards exist** (ISO, NIST) — but are too heavy for SMEs.

🧩 **Service providers dominate**, guidance is lacking, and budgets are tight.

Design Science

Phase 1

Conceptual Development

Phase 2

Regulatory Alignment

Phase 3

Simulation-Based Validation

Phase 4

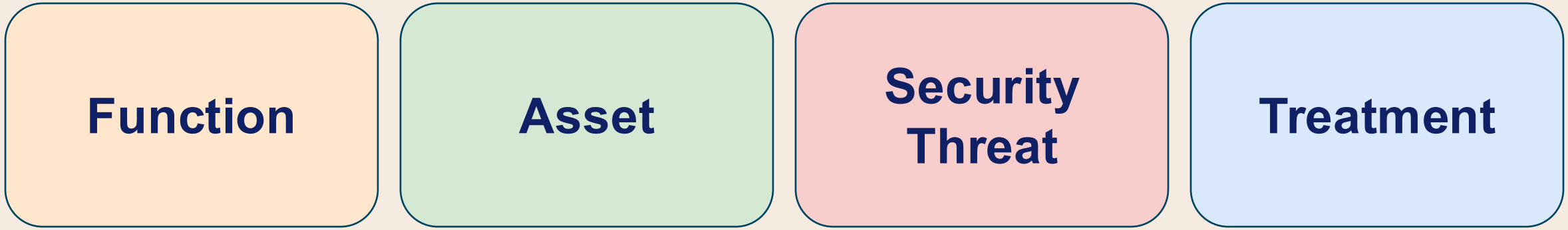
Industry Adaptation

Phase 1:

RQ1: How can security risks in automated systems be managed?

- Review existing frameworks & Risk management methods
- Identify limitations in classification models
- Develop a function-based security classification model

Phase 1: The FAST approach

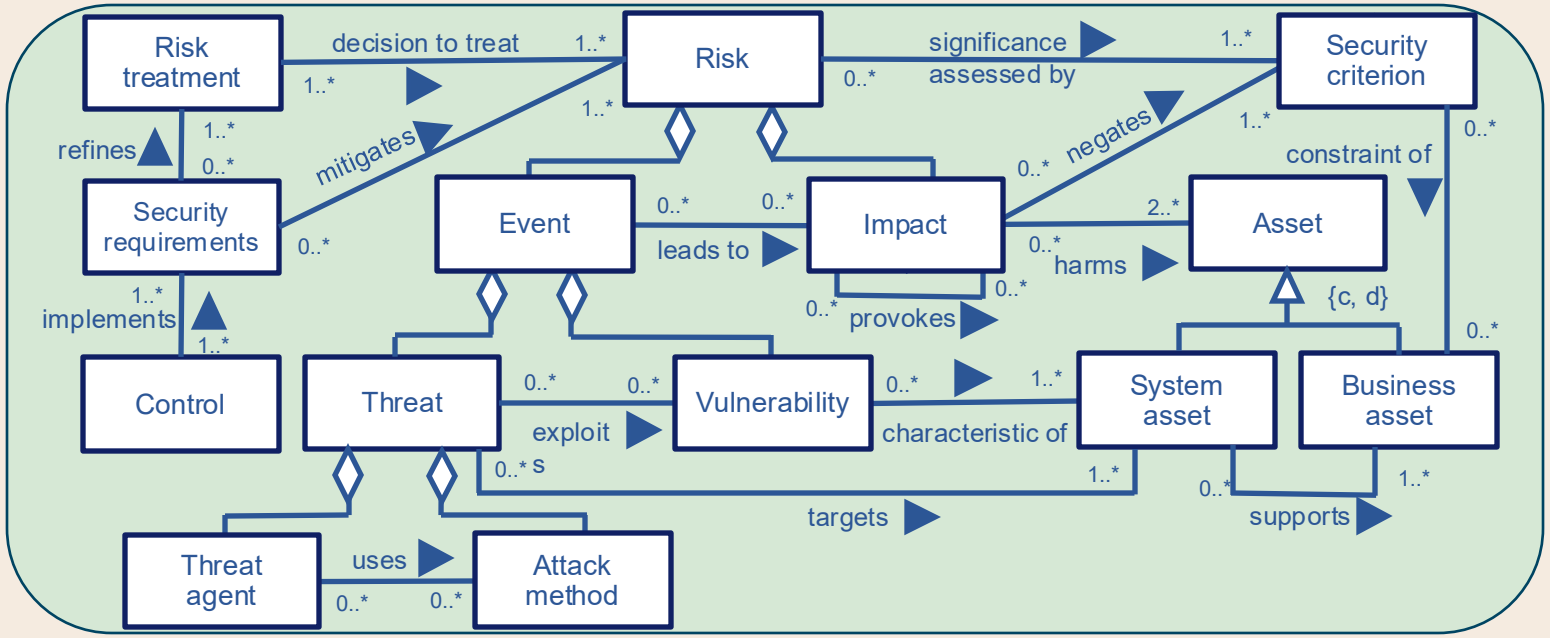


Antipenko, V., & Matulevičius, R. (2025). Functional security in automation: The FAST approach. The practice of enterprise modeling. PoEM 2024 (Vol. 538).

Phase 1: Components

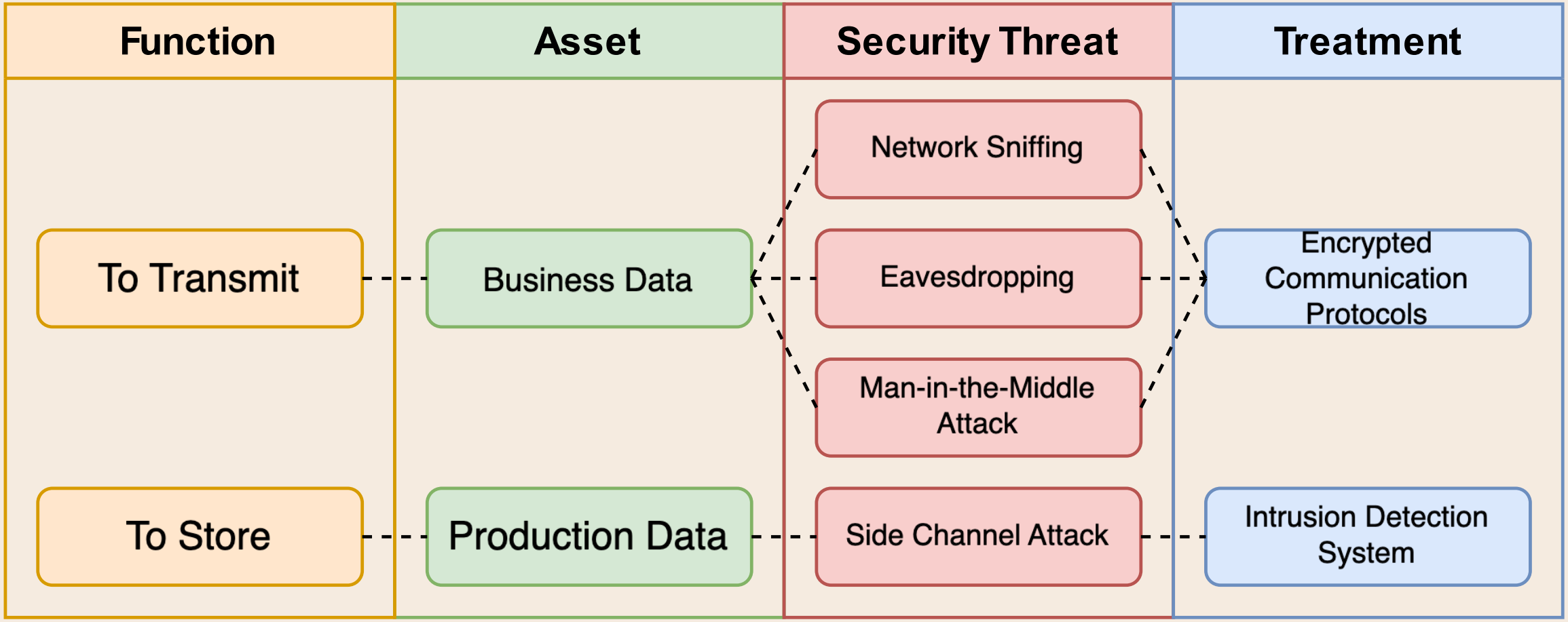
To capture | To store | To mani-pulate | To transmit | To retrieve | To display

Category	Description
Spoofing	Impersonating another entity
Tampering	Altering data or processes
Repudiation	Denying an action with no evidence
Information Disclosure	Exposing sensitive information
Denial of Service	Disrupting availability of service
Elevation of Privilege	Gaining unauthorized rights



1. Alter, S. (2006). The work system method: Connecting people, processes, and IT for business results. Work System Method.
2. Matulevičius, R. (2017). Fundamentals of secure system modelling. Springer International Publishing.
3. Howard, M., & Lipner, S. (2006). The security development lifecycle (Vol. 8). Redmond: Microsoft Press.

Phase 1: The FAST breakdown



Phase 1

Conceptual Development

Phase 2

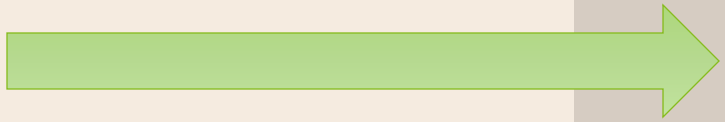
Regulatory Alignment

Phase 3

Simulation-Based Validation

Phase 4

Industry Adaptation



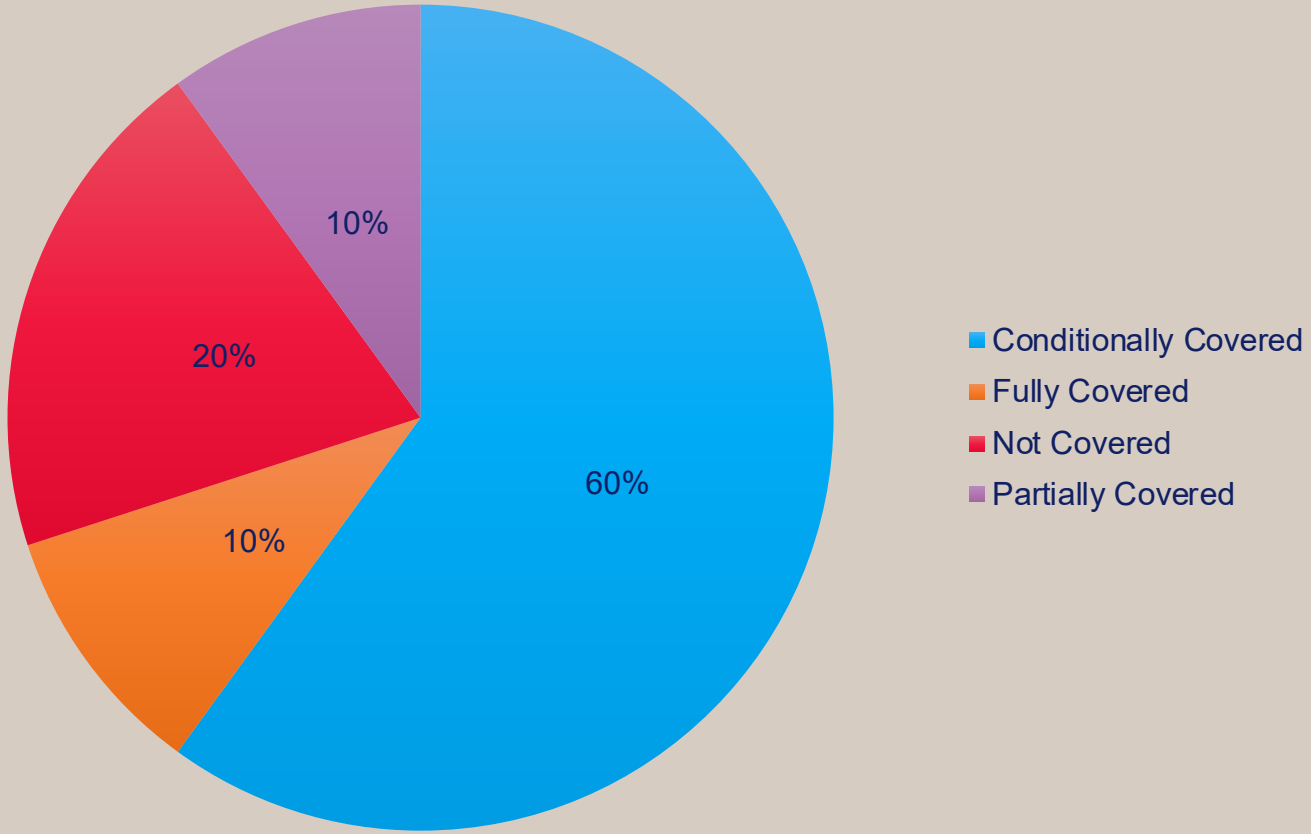
Phase 2:

RQ2: How does FAST **support compliance** with NIS2 and CRA?

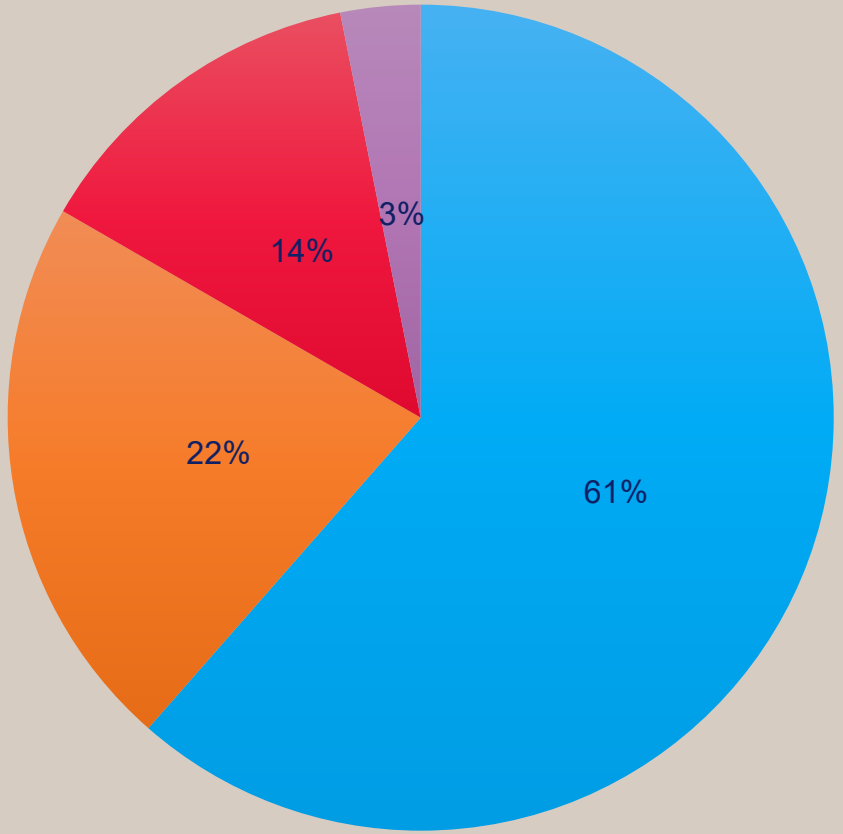
- Map FAST to NIS2 and CRA
- Identify compliance gaps & propose adaptations
- Develop compliance guidelines

Phase 2: sneak peak

NIS2 coverage distribution by FAST



CRA coverage distribution by FAST



Phase 1

Conceptual Development

Phase 2

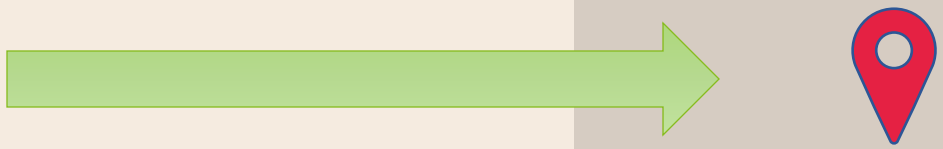
Regulatory Alignment

Phase 3

Simulation-Based Validation

Phase 4

Industry Adaptation



Phase 3:

RQ3: How effectively does the FAST approach **identify**, **classify**, and **mitigate** security threats in a **simulated** environment?

- Test FAST in a digital twin simulation
- Evaluate effectiveness in identifying and mitigating threats
- Validate functional classification in controlled environments

Phase 1

Conceptual Development

Phase 2

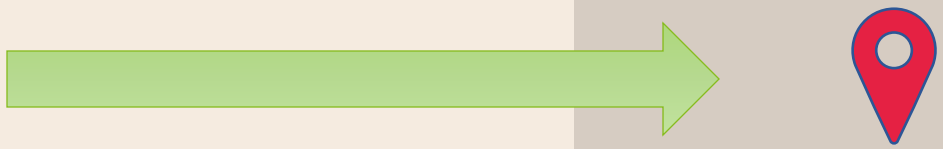
Regulatory Alignment

Phase 3

Simulation-Based Validation

Phase 4

Industry Adaptation



Phase 4:

RQ4: What are the **organisational**, **technical**, and **economic barriers** to implementing FAST in real-world manufacturing environments, and how can they be mitigated?

- Pilot FAST in real-world manufacturing
- Analyse implementation challenges
- Develop an industry adaptation roadmap

Phase 1

Conceptual Development

Phase 2

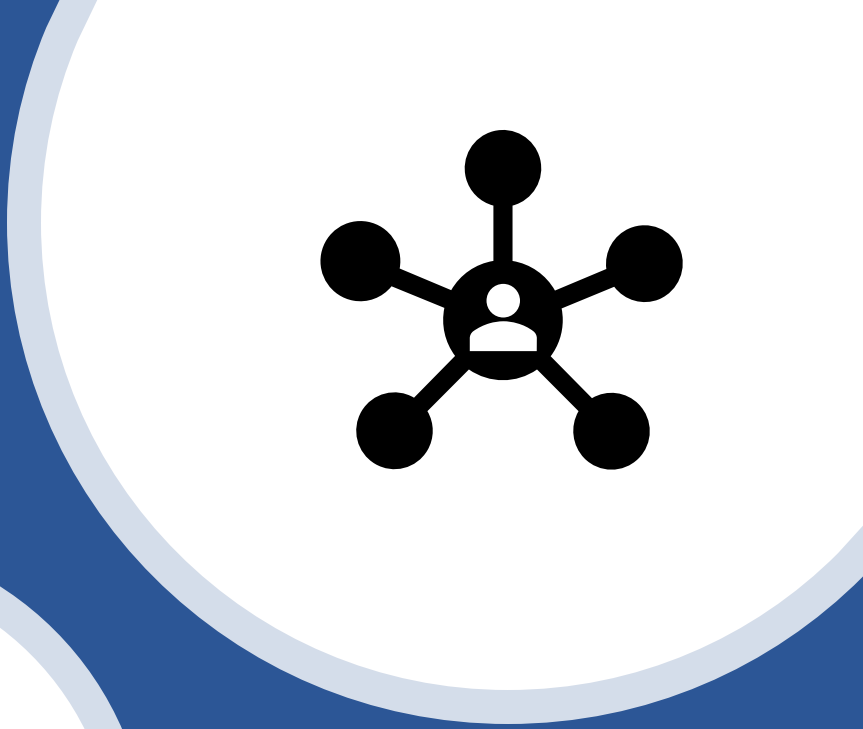
Regulatory Alignment

Phase 3

Simulation-Based Validation

Phase 4

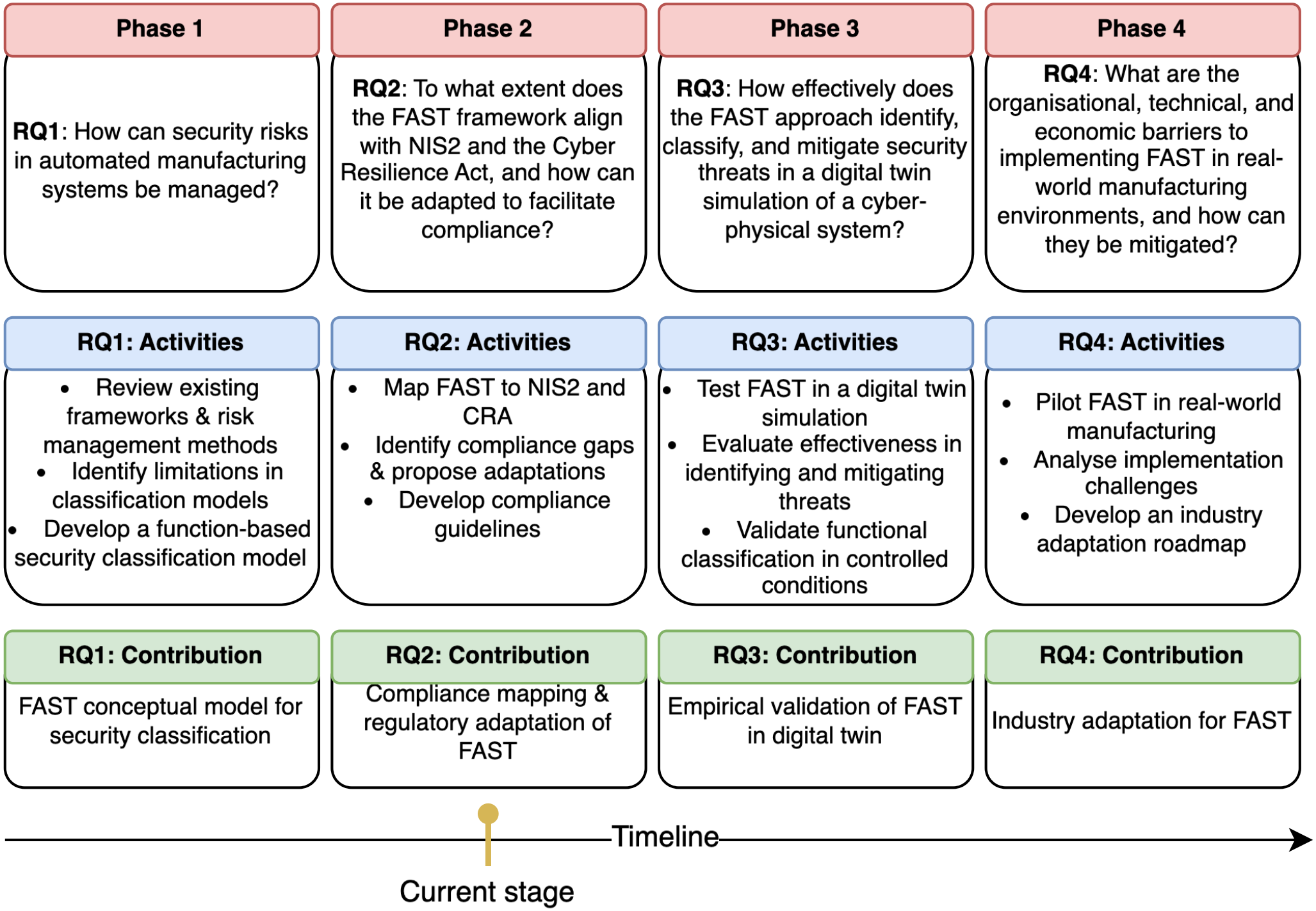
Industry Adaptation



Further inquiries, collaborations:

Vjatšeslav Antipenko
vjatseslav.antipenko@ut.ee

https://infosec.cs.ut.ee


Phase 1
Phase 2
Phase 3
Phase 4
RQ1: How can security risks in automated manufacturing systems be managed?
RQ2: To what extent does the FAST framework align with NIS2 and the Cyber Resilience Act, and how can it be adapted to facilitate compliance?
RQ3: How effectively does the FAST approach identify, classify, and mitigate security threats in a digital twin simulation of a cyber-physical system?
RQ4: What are the organisational, technical, and economic barriers to implementing FAST in real-world manufacturing environments, and how can they be mitigated?
RQ1: Activities
Review existing frameworks & risk management methods
Identify limitations in classification models
Develop a function-based security classification model
RQ2: Activities
Map FAST to NIS2 and CRA
Identify compliance gaps & propose adaptations
Develop compliance guidelines
RQ3: Activities
Test FAST in a digital twin simulation
Evaluate effectiveness in identifying and mitigating threats
Validate functional classification in controlled conditions
RQ4: Activities
Pilot FAST in real-world manufacturing
Analyse implementation challenges
Develop an industry adaptation roadmap
RQ1: Contribution
FAST conceptual model for security classification
RQ2: Contribution
Compliance mapping & regulatory adaptation of FAST
RQ3: Contribution
Empirical validation of FAST in digital twin
RQ4: Contribution
Industry adaptation for FAST
Timeline
Current stage