INDUSTRY 5.0 CONFERENCE · RAKVERE, 14 MAY 2026

FROM RESEARCH TO REALITY

Bridging Cybersecurity Research and Industrial Practice

Shaymaa Mamdouh Khalil
Early-Stage Researcher
shaymaa.khalil@taltech.ee

14.05.2026

Production stopped by a cyberattack

Manufacturing is the #1 targeted sector globally for cyberattacks. (IBM X-Force 2025)

JAGUAR LAND ROVER · SEP 2025

5 weeks

Zero cars produced

Most damaging cyberattack in British history
Thousands of workers sent home
Losses exceeded $1.5 billion

SMEG · SEP 2024

Suspended operation

Second attack in 6 years

Employees were sent home
Production halted
IT systems down : production management, logistics, HR, accounting

In industrial systems, a cyberattack can damage equipment, harm the environment, and put people at risk.

Understand your system first

Threat Modeling

1. What are we working on?
2. What can go wrong?
2. What are we going to do about it?
3. Did we do a good enough job?

Ref: threatmodelingmanifesto.org

TM vs Risk Assessment

Both consider impact. But risk assessment also considers probability. Threat modeling does not.

In industrial systems, if the impact is severe enough, even a low probability threat must be taken seriously.

Where to Start

You cannot secure what you do not know.

Start with an inventory of your assets, connections, and data flows. This is how you answer the first question: what are we working on?

A threat model is not a one-time exercise

Building a Secure-by-Design Microgrid

01

Systematic Review

https://doi.org/10.1016/j.cose.2023.103543

Mapped 36 published studies on threat modeling for ICS. STRIDE, originally developed by Microsoft, was the most widely referenced method, but none of the studies provided clear guidance on how to apply it to ICS. This gap motivated the next two steps.

02

New Methodology

https://doi.org/10.1016/j.cose.2022.102950

We developed a structured methodology for applying STRIDE to industrial control systems, filling the gap the review identified.

03

BRIDGE Framework

https://doi.org/10.1016/j.cose.2026.104906

A nine-stage process connecting design-phase threat analysis to penetration testing. We used it to plan and guide the security testing of the newly deployed TalTech microgrid.

Published in

Computers & Security

Elsevier
A leading cybersecurity research journals

As part of a €1,075,450 EU-funded Smart City project, we set out to build a secure-by-design microgrid with real pilot sites in Tartu and PAKRI Industrial Park. To do this, we first needed to find the right threat modeling method.

A collaboration between researchers from different departments at TalTech, cybersecurity, power engineering, and software science, building a smart microgrid with AI-based energy management.

How industry found us and what we built together

How It Started

Goldilock Secure Ltd. read our paper and reached out to collaborate.

Together, funded by NATO DIANA, we built a manufacturing CPS testbed with enterprise, OT, and field layers, SCADA, EMS and PLCs.

We ran two attack scenarios: denial-of-service on the web application, and an attacker pivoting into the OT layer.

Cyber Resiliency Testing

Cyber resiliency: the ability to anticipate, withstand, recover from, and adapt to a cyberattack. (NIST SP 800-160)

- We applied the MITRE Cyber Resiliency Use Case (CRUC) method.
- Developed specific measurement equations for each mission objective in the industrial context.
- The testbed remains at TalTech for future research and collaboration.

DOI: 10.1109/ICIT64854.2026.11491056

Ways to start a collaboration with TalTech.

MSc Thesis

A student works on your real challenge under academic supervision.

Internship

Hosting a student/staff member in your company for a determined period.

Industrial PhD

A researcher works partly in your company, producing results that stay with both sides.

Who to contact

CYBERSECURITY MSc THESIS

Shaymaa.Khalil@taltech.ee

INTERNSHIP OR IT COLLABORATION

Sirli.Kasepuu@taltech.ee
Business Coordinator, School of IT

INDUSTRIAL PhD OR BROADER COLLABORATION

taltech.ee/en/PhD/industrial-phd
Krister.Kalda@taltech.ee
Head of Industry Cooperation

LET'S START THE CONVERSATION

TAL TECH

The threats already exist.

The real question is whether you choose to prepare before an incident occurs.

Questions?