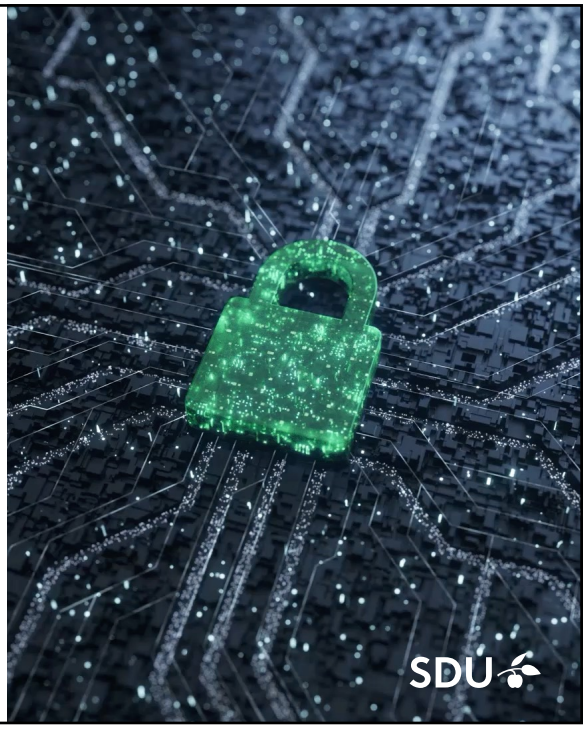
Centre for Industrial Software (CIS)

Cyber-Safe Lab

Centre for Industrial Software (CIS)
University of Southern Denmark
Sønderborg



1

Centre for Industrial Software (CIS)

Cyber-Safe Lab

Lars Ramkilde Knudsen
Professor

Mubashrah Saddiqa
Assistant Professor

Jukka Ruohonen
Assistant Professor

Bence Kanyok
Student Helper

To maintain **human trust** in digital technology systems and secure systems.

Research and disseminates **cyber-security knowledge**, tools and techniques to make systems cyber-safe. Special focus is on **IoT, mechatronic and robotic systems.**

Our Services

- Advanced cryptology including design and implementation
- Knowledge on tools and practices for cyber-secure software design and implementation
- Cyber-awareness methods and tools
- European cyber security regulations, requirements and implications for the information technology and software industries, including the recently enacted Cyber Resilience Act (CRA).

SDU

2

Centre for Industrial Software (CIS)

Cyber-Safe Lab @ SDU

Lars Ramkilde Knudsen
Professor

Cryptology

- Quantum-safe cryptology. If large quantum computers should be built one day, they will be able to break most of the cryptosystems used to secure communications on the Internet today. Therefore cryptographers have developed cryptosystems that seem to be secure also from attacks on quantum computes. However, there are very good reasons to be aware that these systems are new and they need to be analysed over several years yet, before there is common belief that they systems are secure.
- Format-preserving cryptology. This refers to encrypting in such a way that the output (the ciphertext) is in the same format as the input (the plaintext). This enables encrypted data to be used as clear data, e.g. for statistical purposes without violating strong restrictions from gpdr.

SDU

3

Centre for Industrial Software (CIS)

Cyber-Safe Lab

Mubashrah Saddiqa
Assistant Professor

Research with in technical, human, and educational dimensions of cybersecurity

- Advancing secure software practices in robotics and automation to mitigate cybersecurity risks.
- Developing secure architectures for communication in battery management systems
- Exploring human behavior's impact on cybersecurity risks in digital environments.
- Promoting diversity in cybersecurity education and fostering inclusivity through specialized training initiatives.

SDU

4

Centre for Industrial Software (CIS)

Cyber-Safe Lab – Research Projects

Mubashrah Saddiqa
Assistant Professor

1. Cyber Safe Robotics Project: Development of Secure Software

Key Focus: Cybersecurity improvement methods for software solutions. Introduction to tools for secure design and development of both software and hardware. Hands-on experience in applying secure software development practices within company environments.

Activities: Workshop with robotics companies:

- Core cybersecurity concepts.
- Understanding sources of vulnerabilities and threats.
- Best practices for secure software development.
- Operational Technology (OT) security, with real-world scenarios from the industry.
- Specific threats, attacks, and protection mechanisms in robotics.
- Awareness training using cybersecurity tool.

Next Workshop
27-05-25
Register here: https://odenserobotics.nemtilmeld.dk/34/

SDU

5

Centre for Industrial Software (CIS)

Cyber-Safe Lab – Research Projects

Mubashrah Saddiqa
Assistant Professor

1. Cyber Safe Robotics Project: Development of Secure Software

Development of Security Scanner:

- Beside training workshops, a security scanner specifically for robotics has been developed with the help of student helper and software engineer.
- Scanner will help users identify vulnerabilities at an early stag to secure robotic systems.
- A research paper is submitted.

Florian Girardo
Software Engineer

Bence Kanyok
Student Helper

Next Workshop
27-05-25
Register here: https://odenserobotics.nemtilmeld.dk/34/

SDU

6

Centre for Industrial Software (CIS)

Cyber-Safe Lab – Research Projects

2. AI-Powered Next Generation Battery Management System

Objective:

This project aims to provide intelligent battery management systems. By providing real-time actionable insights, remote updates, and robust security measures, the project will significantly improve EV batteries' efficiency, cost-effectiveness, and longevity.

Key Focus:

- Design phase analysis (TARA) and requirements/controls elicitation
- Creation of a BMS cybersecurity architecture by allocation of controls
- Implementation and integration of security controls with the designed architecture
- Verification and validation (inc. Penetration test) and fix of vulnerabilities

Funding:

Funded by Euro Star in collaboration with **Turkish engineering/consulting company mea-tec, CIS and CIE SDU.**

Starting from 01-07-25

SDU

7

Centre for Industrial Software (CIS)

Cyber-Safe Lab – Teaching

Objective:

To provide a secure, controlled, and interactive environment for students to learn, practice, and develop cybersecurity skills, fostering awareness, critical thinking, and hands-on experience in identifying, preventing, and mitigating cyber threats.

Key Focus Areas:

- Educating students on safe online behavior, password management, phishing threats, and social engineering tactics.
- Teaching ethical hacking techniques, vulnerability assessments, and penetration testing methodologies.
- Providing access to cyber tools and techniques.
- Facilitating students for cybersecurity events.
- One hackers' beginners' event in collaboration with DE DANSKMASTERSKBE around 100 students participated.

SDU

8

Centre for Industrial Software (CIS)

European cyber security regulations

- Cyber-security regulations recently enacted in the European Union (EU), including their requirements and implications for private sector companies and public sector organizations
- EU's recently agreed Cyber Resilience Act (CRA), which will be in force in 2027
- The work in the regulatory domain is further supported by additional work in empirical software engineering and software security, including security engineering

Jukka Ruohonen
Adjunkt
SDU Center for Industriel Software - CIS

SDU

9

Centre for Industrial Software (CIS)

Related Area: Trustworthy Systems Laboratory (TS Lab)

- Analyze software artifacts to discover vulnerabilities/defects and provide mitigation.
- Utilize AI/ML techniques and build intelligent predictive models to optimize the trustworthy operation of various Cyber-Physical Systems (including robotics and automation).
- Automated program repair, i.e., finding and repairing software vulnerabilities and bugs on the fly.
- Consultancy to enhance confidence in system trustworthiness.
- We focus on (but are not limited to) the following research lines:

- Research lines
- AI for Engineering Trustworthy Systems
- Android Security
- Model-Driven Engineering for Trustworthy Systems

SDU

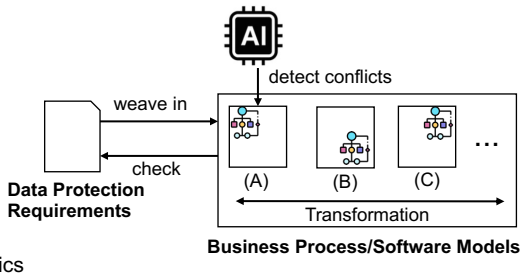
10

Centre for Industrial Software (CIS)

MDE For Engineering Trustworthy Systems: Compliance and Traceability Management

Model-Based Security and Privacy Analysis

- Support compliance with data protection regulations e.g., GDPR.



Model-Based Software Fairness

- Uncover potential discrimination on the basis of protected characteristics (e.g., Gender) from the onset of decision-making software development.

AI For Conflicts Management By Design

- Explore the potential benefits of using Large Language Models in *detecting*, *explaining* and *resolving* conflicts at Business Process Modeling phase.

Alignment and Traceability Management

- Support traceability of security requirements to design level verification.

SDU

Qusai Ramadan
SDU Center for Industrial Software (CIS)
qura@mmmi.sdu.dk
+45 65503719

11