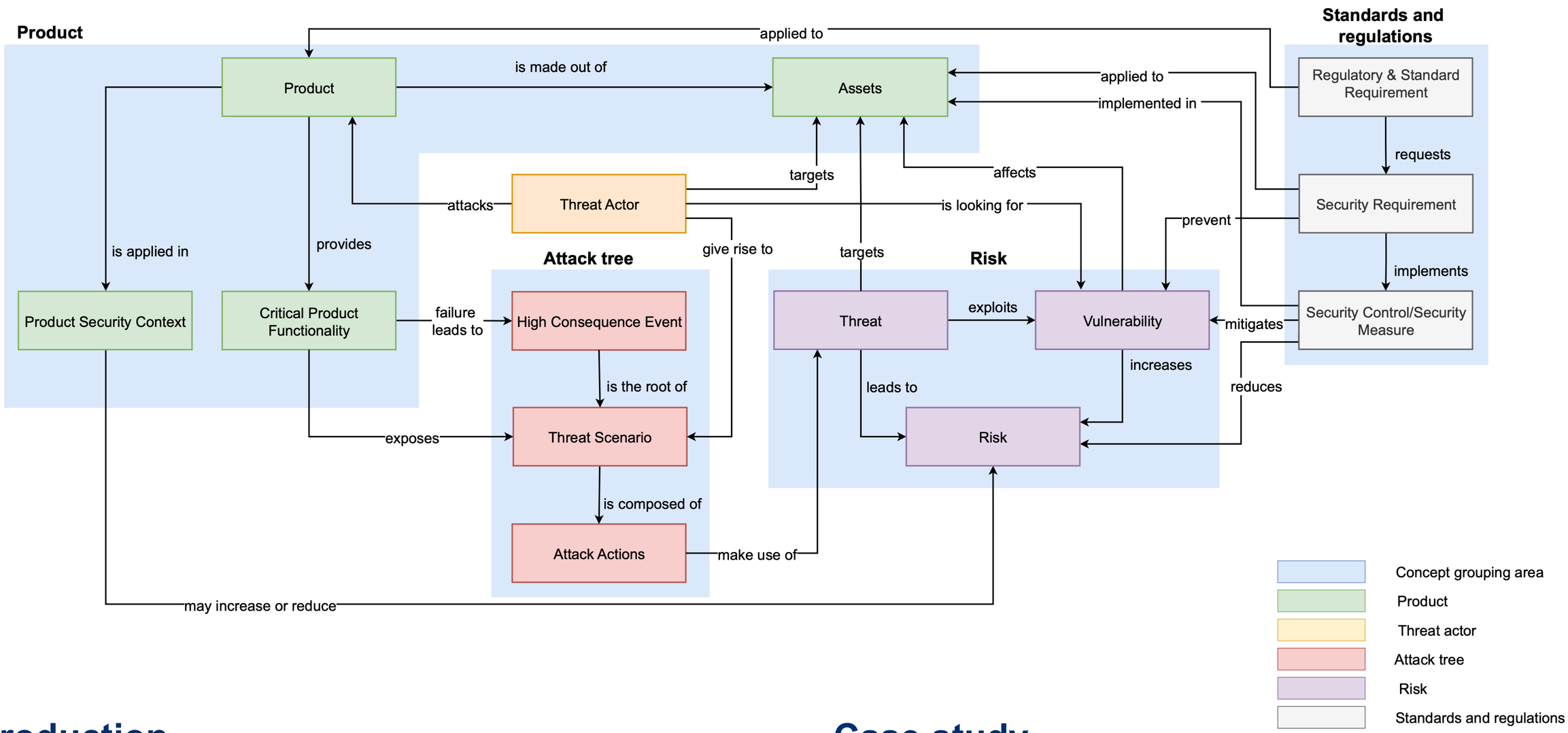
Secure Systems Group, Aalto University

Lija Bista, Philip Ginzboorg, Axel Beer

Risk based security requirement analysis methodology for Cyber-Physical System

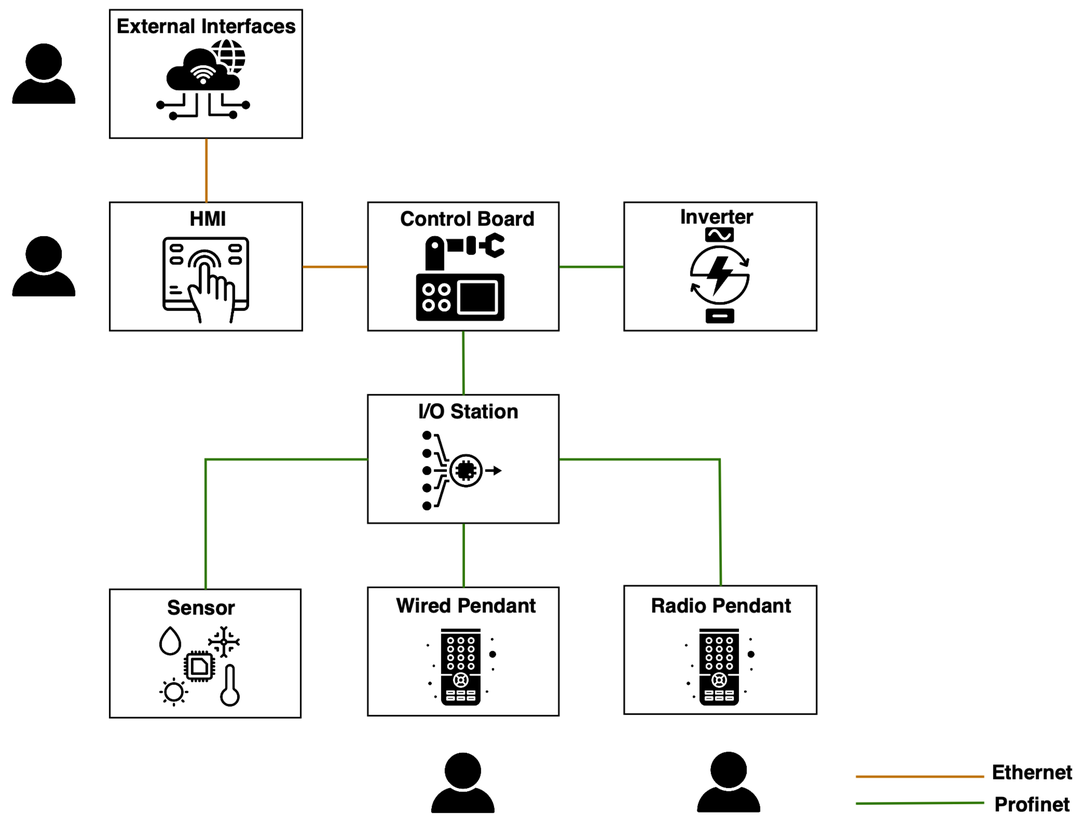


Introduction

- Cyber-Physical Systems (CPS) combine mechanical components with software, sensors, and network connectivity.
- The EU Cyber Resilience Act (CRA, 2024) introduces cybersecurity requirements for Products with Digital Elements (PDEs), which must be applied by December 2027.
- The CRA requires manufacturers to apply risk-based security requirements based on Annex I of CRA.
- Manufacturers need to decide which security features are essential based on the risk level of the product.
- Security terminology (e.g., threat, vulnerability, exploit, risk) has domain-specific meaning.
- Risk assessment and security requirement identification has to be carried out by software developers & engineers who are not security specialists.

Case study

Identified security requirements for CPS product using our methodology.



Objectives

- Review the literature on identifying product security requirements in CPS.
- Develop a methodology that adapts the IEC 62443-3-2 risk assessment process as a baseline to identify security requirements listed in IEC 62443-3-3 for the case company's product development.
- Summarize lessons learned.

Lessons learned

- Importance of well-defined terminology.
- Significant effort is needed to understand the product.
- Application of security standards and regulations demands both domain and security expertise, and substantial work.

Aalto University

Cyber Resilience Act, Regulation (EU) 2024/2847.

SFS-EN IEC 62443-3-2: Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design.

SFS-EN IEC 62443-3-3: Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels.