Cyber Security

Policies and Threat Modeling in OT security

Motion Business Unit

Danfoss Drives - Italy, Merano

employees incl. S/C

~90

years experience in Drives

40+

R&D + Production Floor

7.000 m²

drives produced per year

70.000+

Our Team

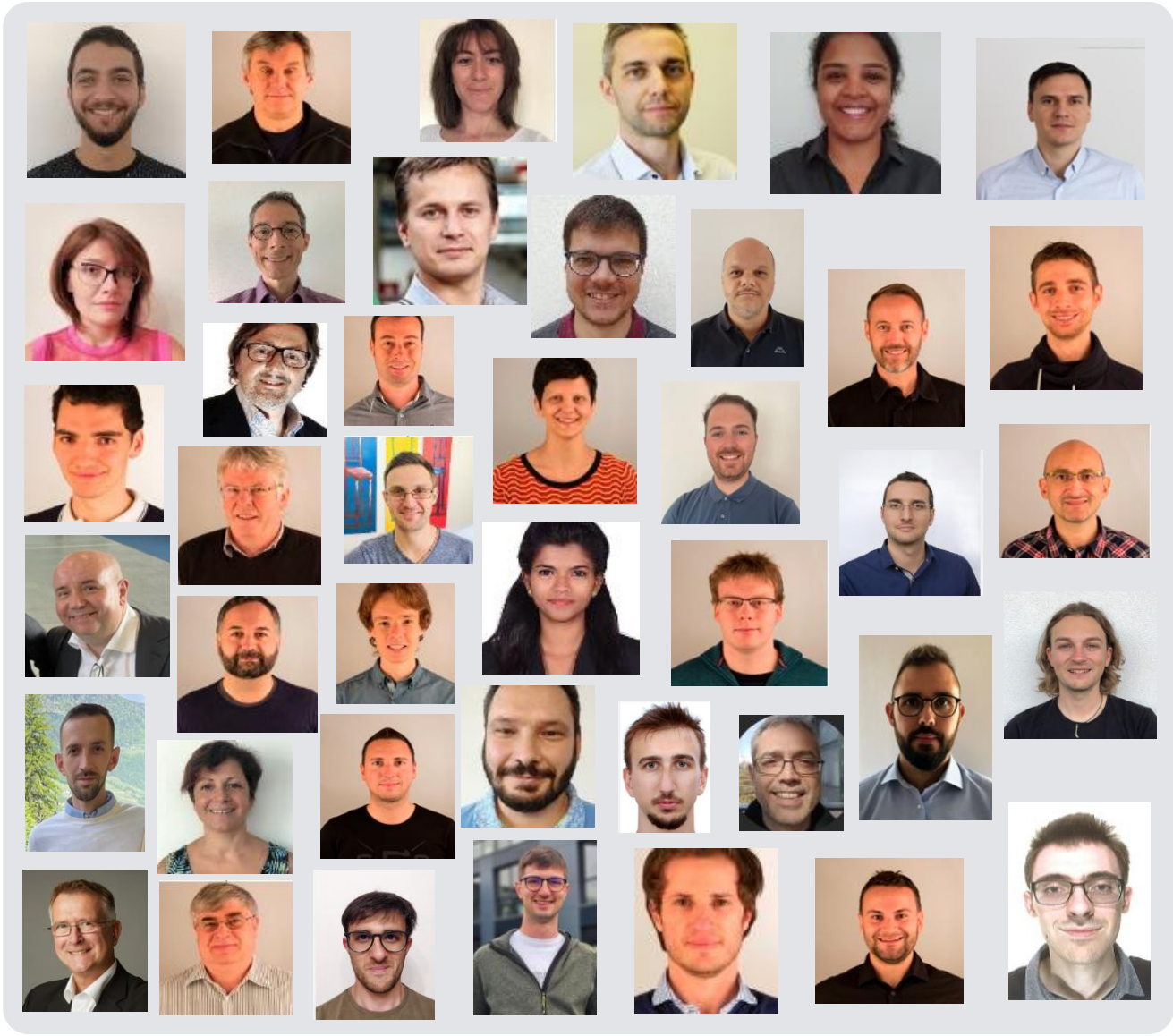
Core Competences

- Automation systems and RT field-busses
- Motor know-how and control – high dynamic
- Drive-Motor-Gear - Integrated solutions
- Machine integration
- High IP products
- Advanced Functional Safety
- Solution oriented mindset

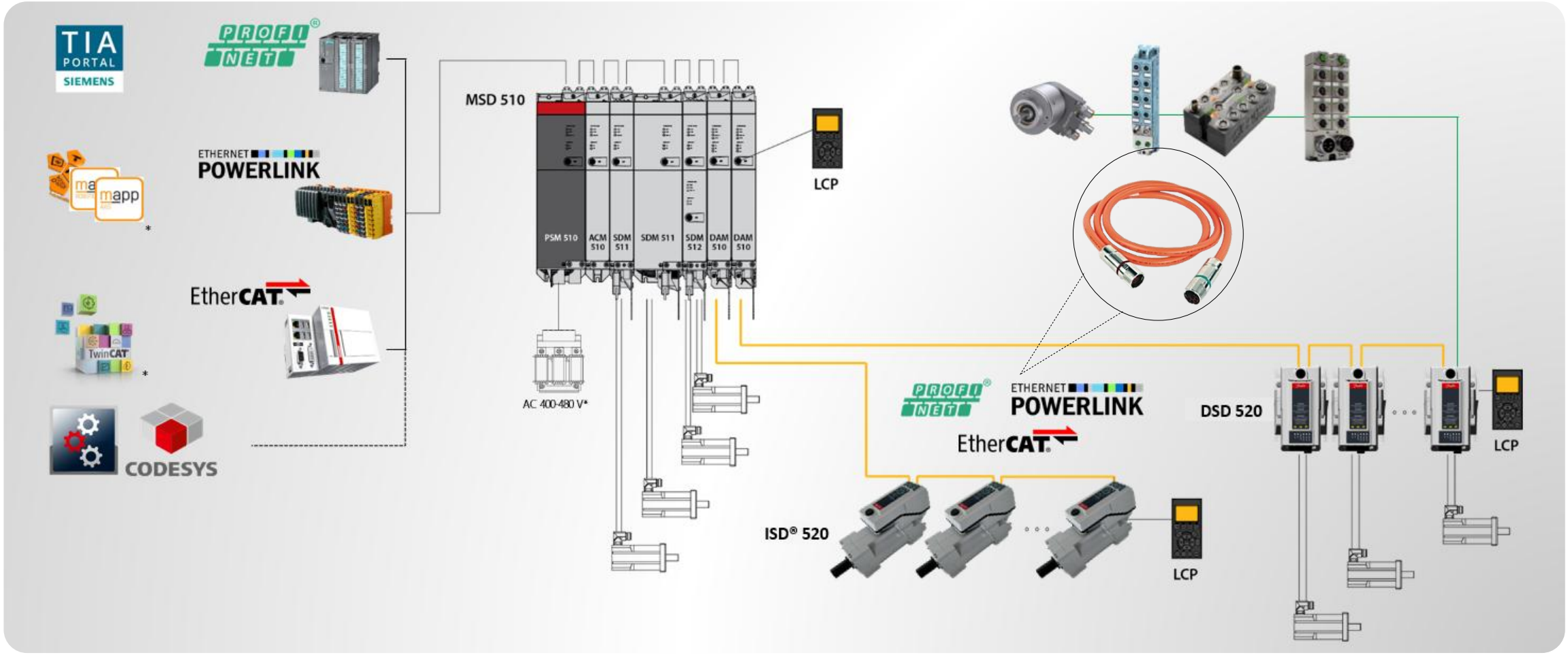
8 nationalities

17% women

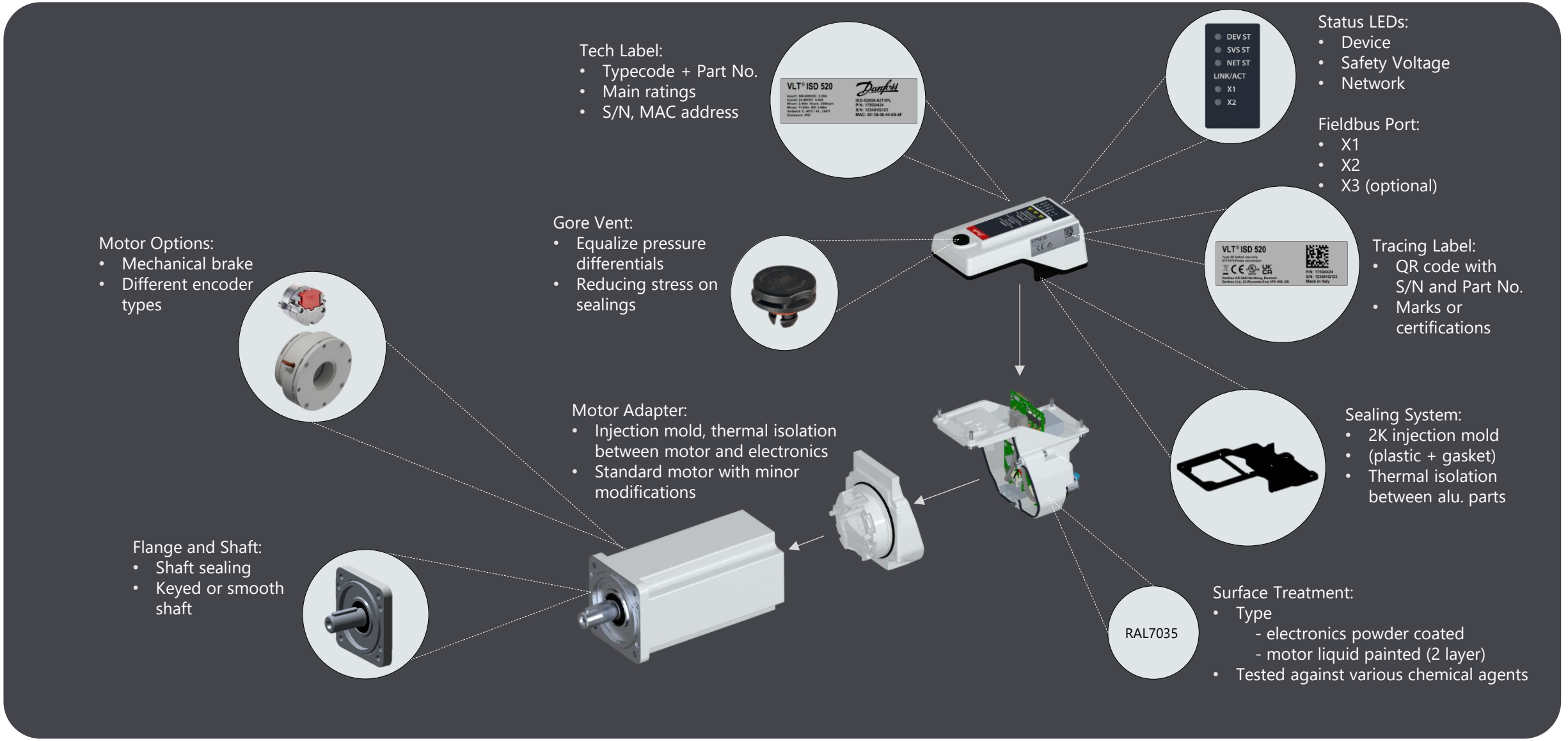
16 universities



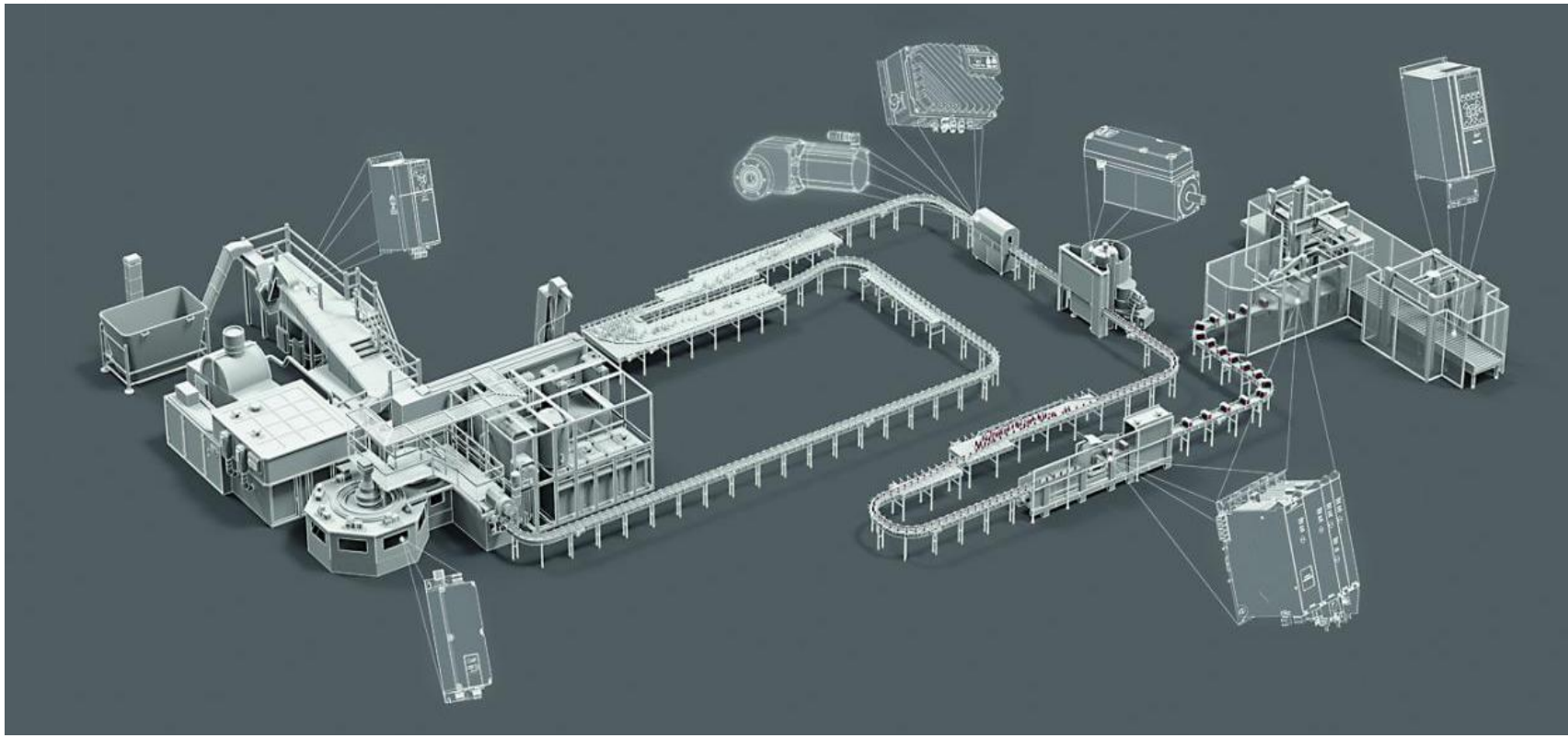
Seamless Integration into Automation Environments



Product Concept – Exploded View



Application



Cyber Security in the Context of Operational Technology (OT)

IT is the technology backbone of any organization

Monitoring, Managing and Securing Core Functions such as Email, Finance, HR

Devices are usually:

- Off-the-shelf
- Replaceable
- Lifespan 3-5 years

OT is for connecting, monitoring, managing, and securing an organization's industrial operations

Activities such as manufacturing, mining, oil and gas, utilities, and transportation, …

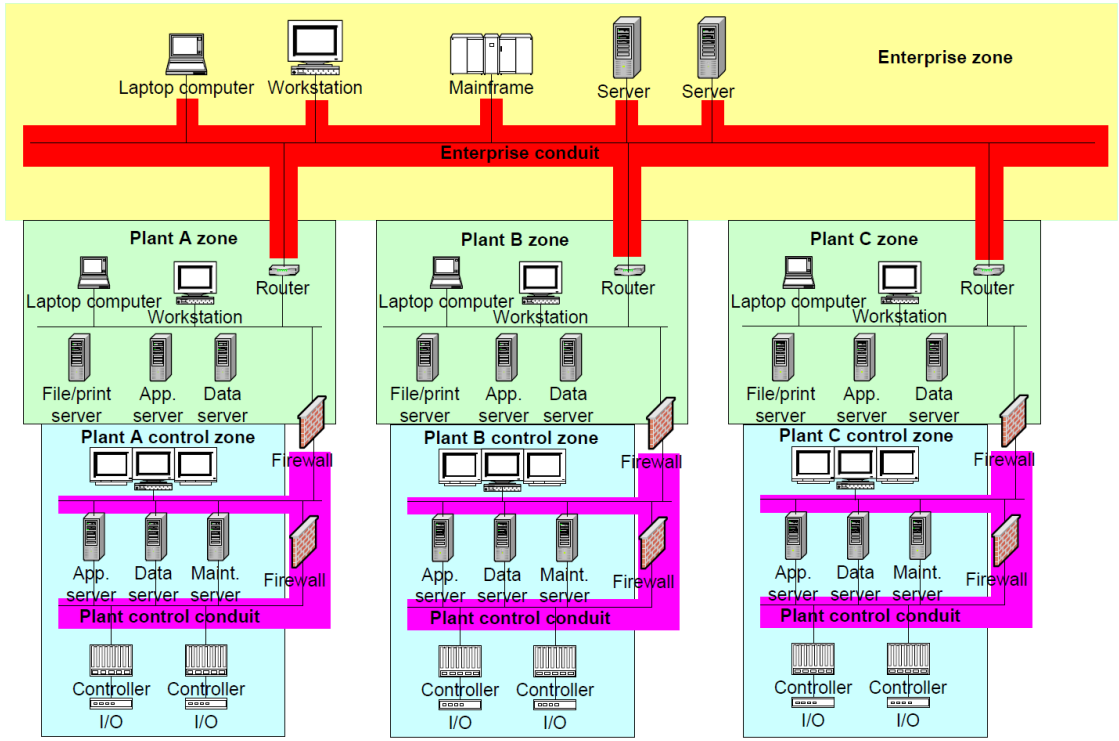
Devices are usually:

- Purpose-built
- Specialized
- Lifespan: Many years to decades

History of Cyber Security in OT

- OT device manufacturer have not considered cyber security protections (if not requested by application)
- OT system are relying on the assumption that IT and physical access protects the system

- Attacks from the last decade:
  - 2010: Stuxnet
  - 2011: Duqu
  - 2013: Havex
  - 2015: BlackEnergy
  - 2017: TRITON



The Cyber Resilience Act (EU) 2024/2847

- **Regularity Framework** to enhance cybersecurity standards of products with digital components.
- It requires manufacturers and retailers to **ensure cybersecurity throughout the lifecycle** of their products.
- Applies to both **hardware** (e.g., smart devices) and **software** (e.g., apps, IoT systems, etc)

Why CRA?

1. **Low cybersecurity in digital products:** widespread vulnerabilities and inconsistent security updates.
2. **Poor user awareness:** lack of information to choose and use products securely.

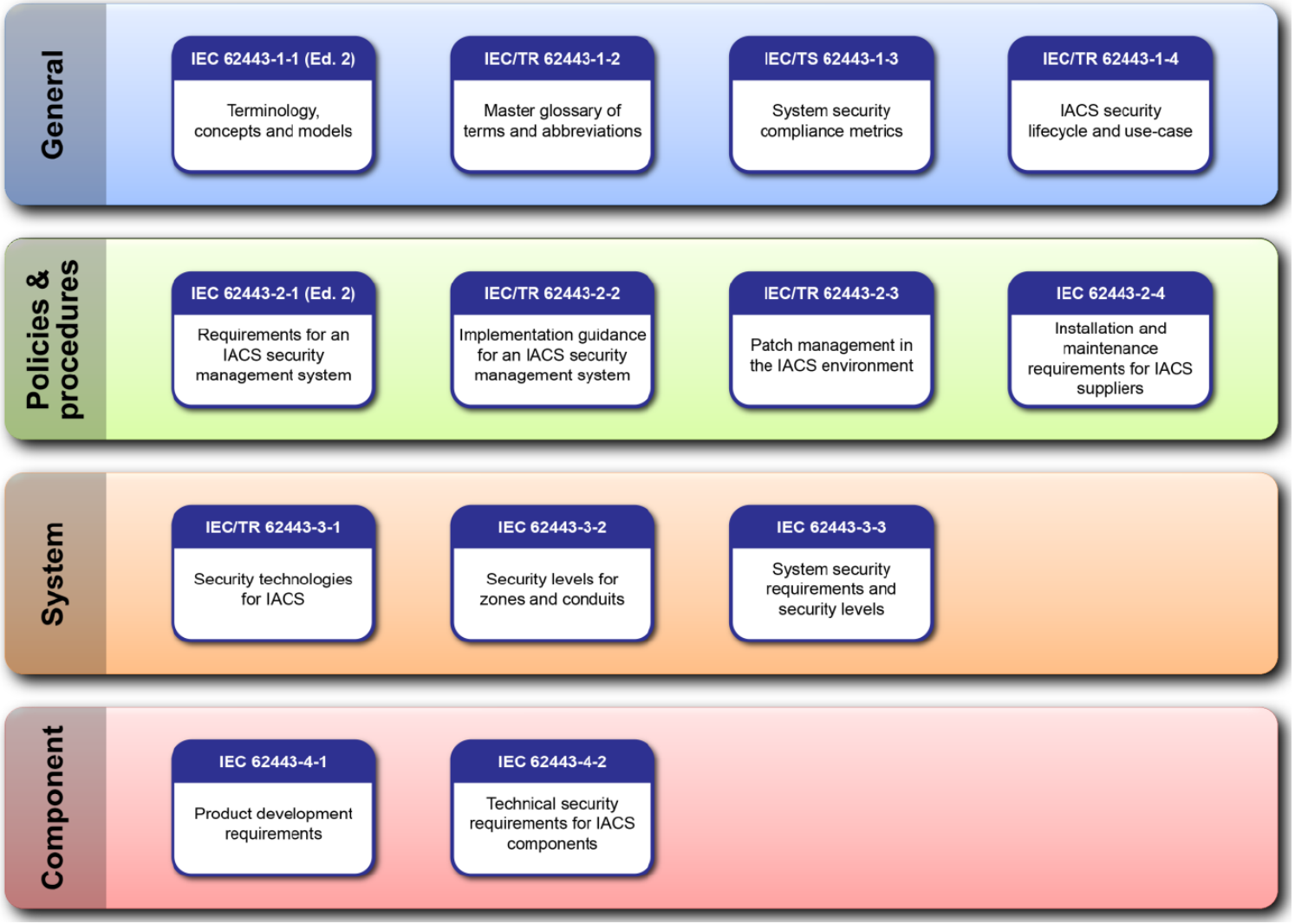
Simple core idea

Make digital products secure by design throughout their lifecycle

Introduces a new challenge

Adds legal complexity

The standard for CRA: IEC 62443



What are the Products in Scope?

- Has digital elements
- Cannot be connected directly or indirectly
- Made available on the market

- Has digital elements
- Can be connected directly or indirectly to other devices
- Made available on the market

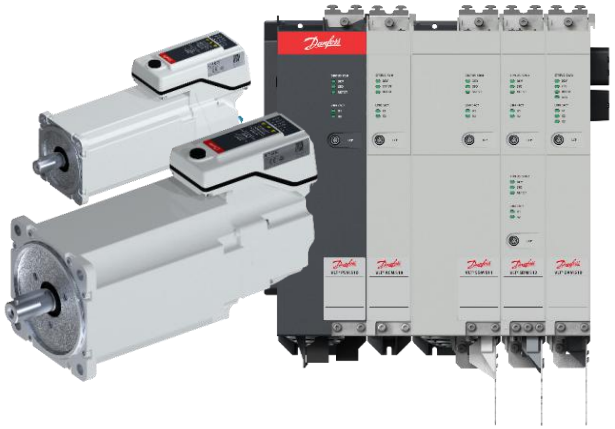
Optyma™ Control

- Has digital elements
- Can be connected directly or indirectly
- Made available on the market

What are the Products in Scope?

- Has digital elements
- Can be connected directly or indirectly
- Not made available on the market

- Has digital elements
- Can be connected directly to other devices
- Made available on the market



- Has digital elements
- Can be connected directly or indirectly
- Made available on the market

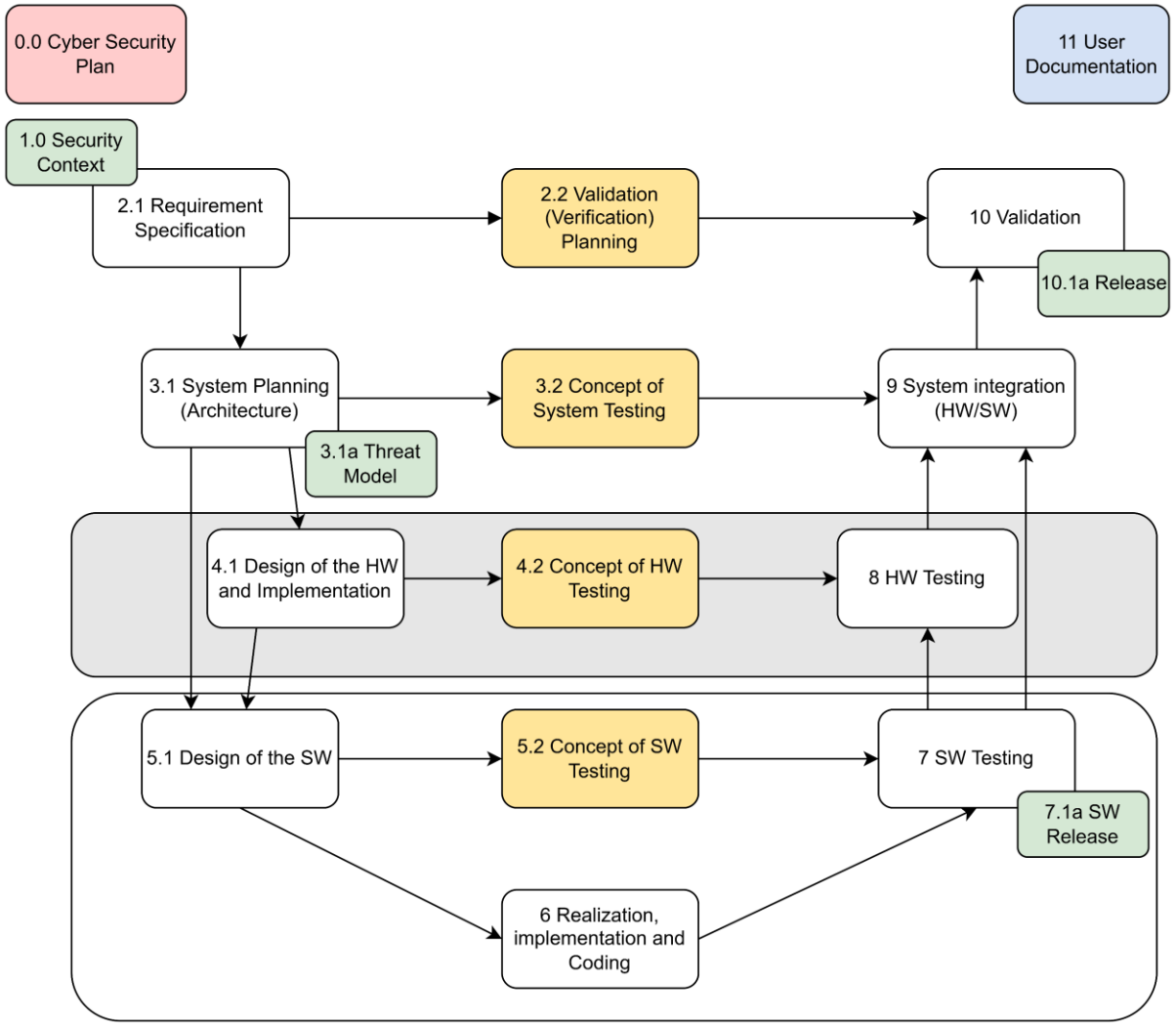
What about Open-Source Software?

Open-Source Software is **out of scope** of the CRA if they are used in Open-Source projects!

If Opens-Source Software is **in scope** of the CRA if they are used in commercial products!

-> The company selling the final product is the one with the obligations

The Non-Technical Part of Cyber Security



Threat Modeling

What is it?

- Structured process for identifying, analyzing and mitigating potential threats and vulnerabilities
- Proactive approach

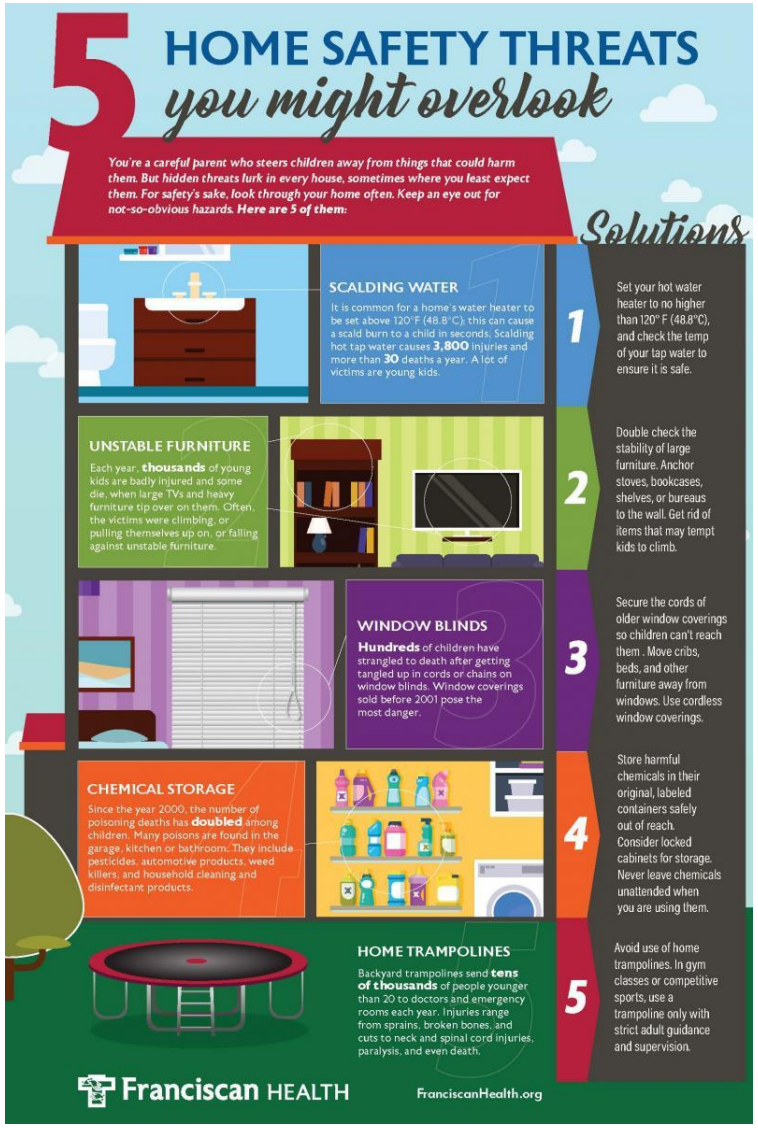
When to do it?

- Early in the concept phase
- A new feature is introduced
- Security incident occurs
- Architectural or infrastructural changes

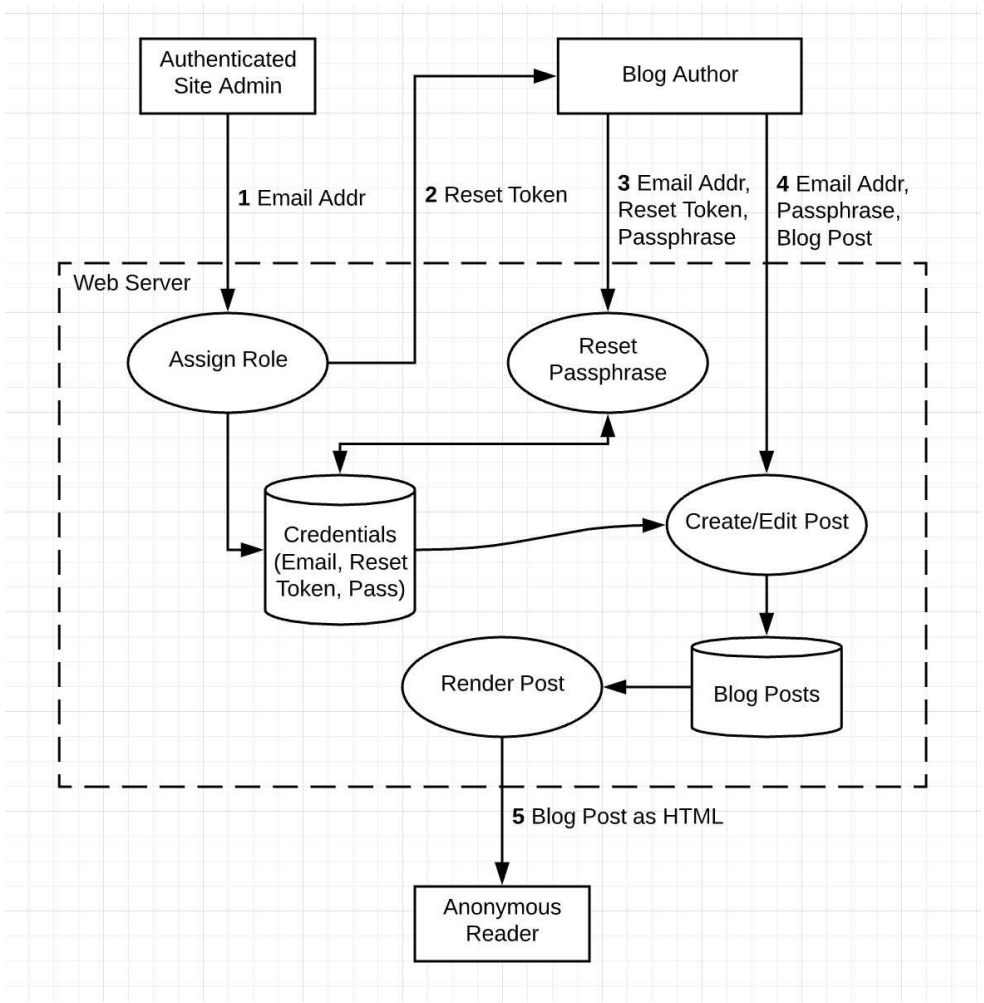
The four questions of threat modeling

- What are we working on?
- What can go wrong?
- What are we going to do about it?
- Did we do a good job?

Threat Modeling: Example



Threat Modeling: Example



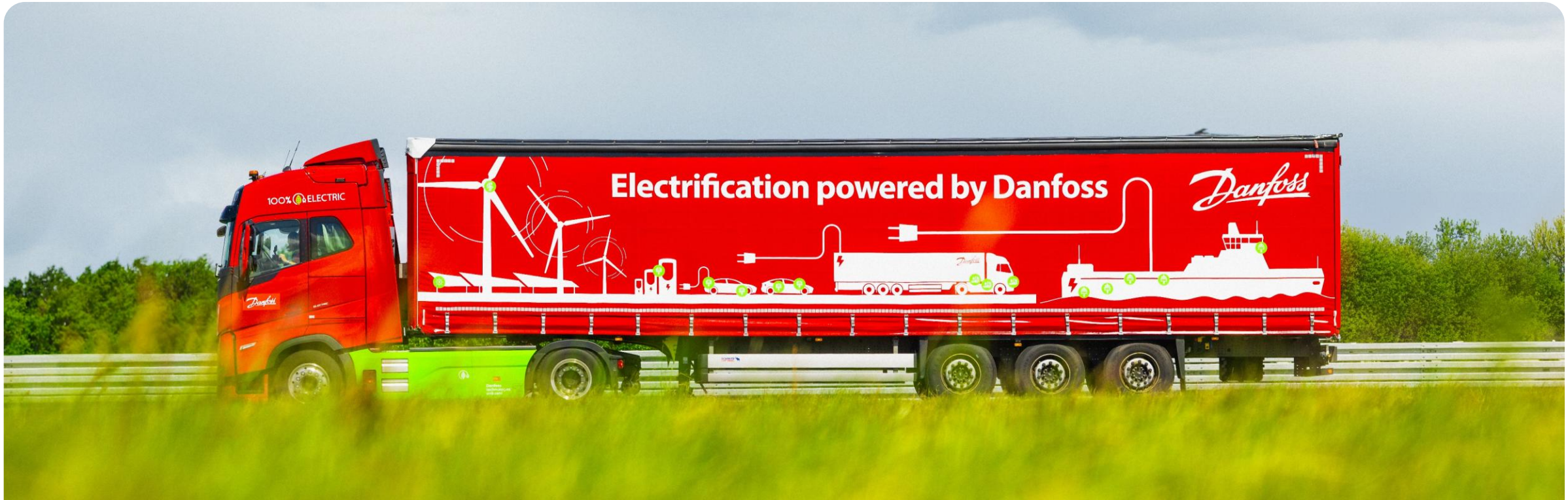
STRIDE THREAT MODEL

Enter your sub headline here

	Threat	Property Violated	Threat Definition
S	Spoofing	Authentication	Pretending to be something or someone other than yourself
T	Tampering	Integrity	Modifying something on disk, network, memory, or elsewhere.
R	Repudiation	Non-Repudiation	Claiming that you didn't do something or we're not responsible. Can be honest or false
I	Information Disclosure	Confidentiality	Providing information to someone not authorized to access it.
D	Denial of service	Availability	Exhausting resources needed to provide service.
E	Elevation of Privilege	Authorization	Allowing someone to do something they are not authorized to do.

Interested?

Internship opportunities: Talk to us or send your CV to jobs.merano.rd@danfoss.com



WORKSHOP

Motion Control with OPC UA

16:00
40 mins
07/11/2025

Crane Hall

TALK

OPC UA in Industrial Automation

17:20
15 mins
07/11/2025

Seminar 3


Danfoss