

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



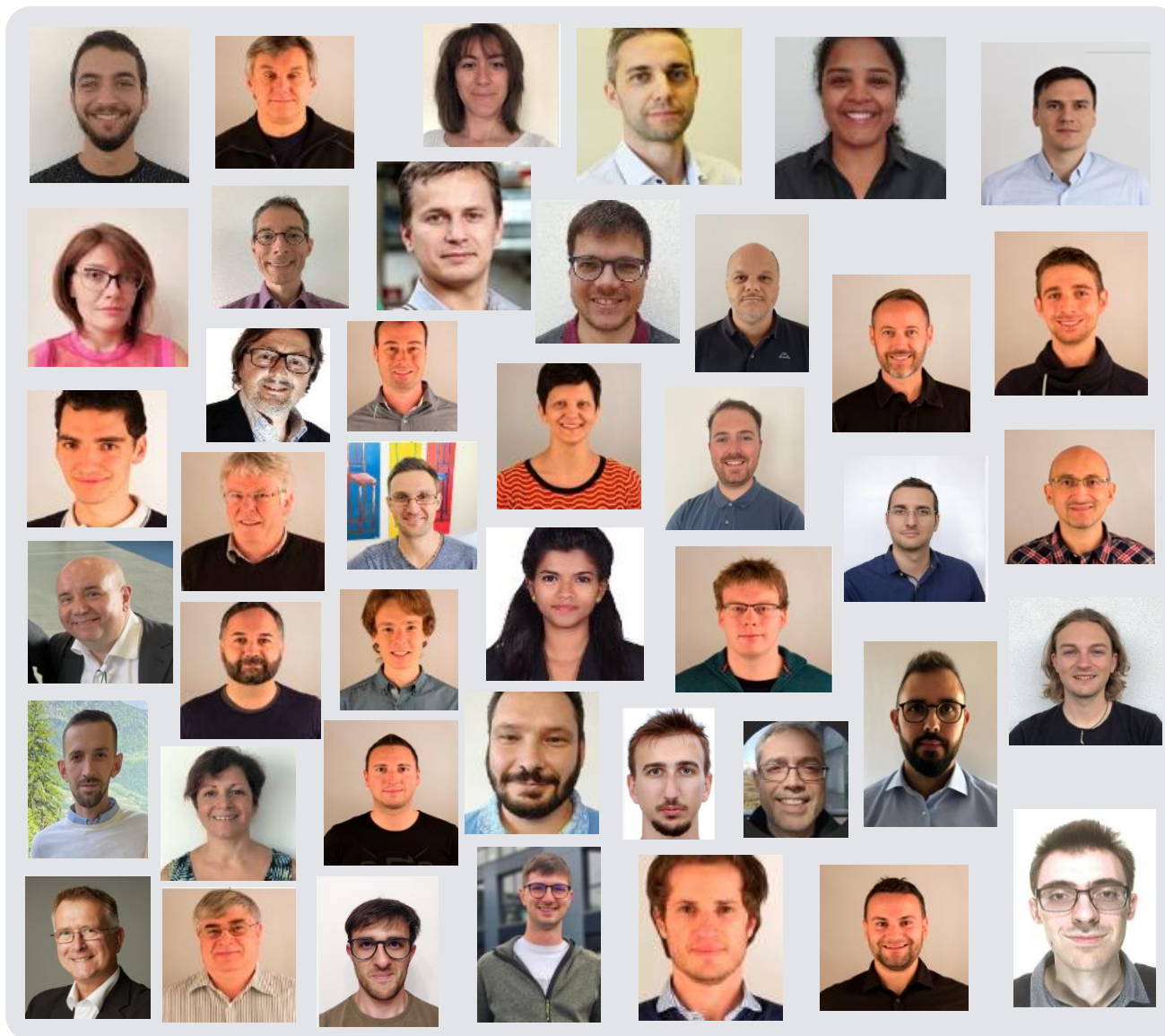
8 nationalities



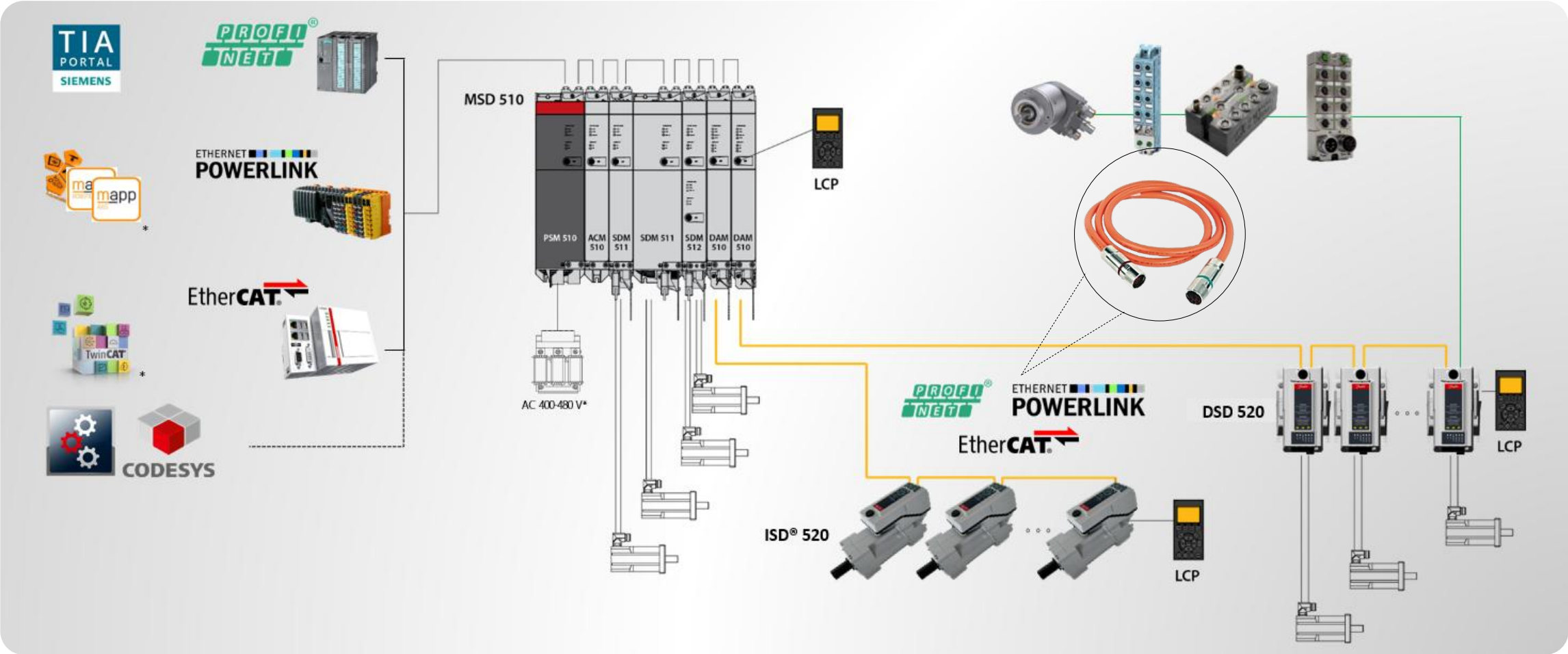
17% women



16 universities

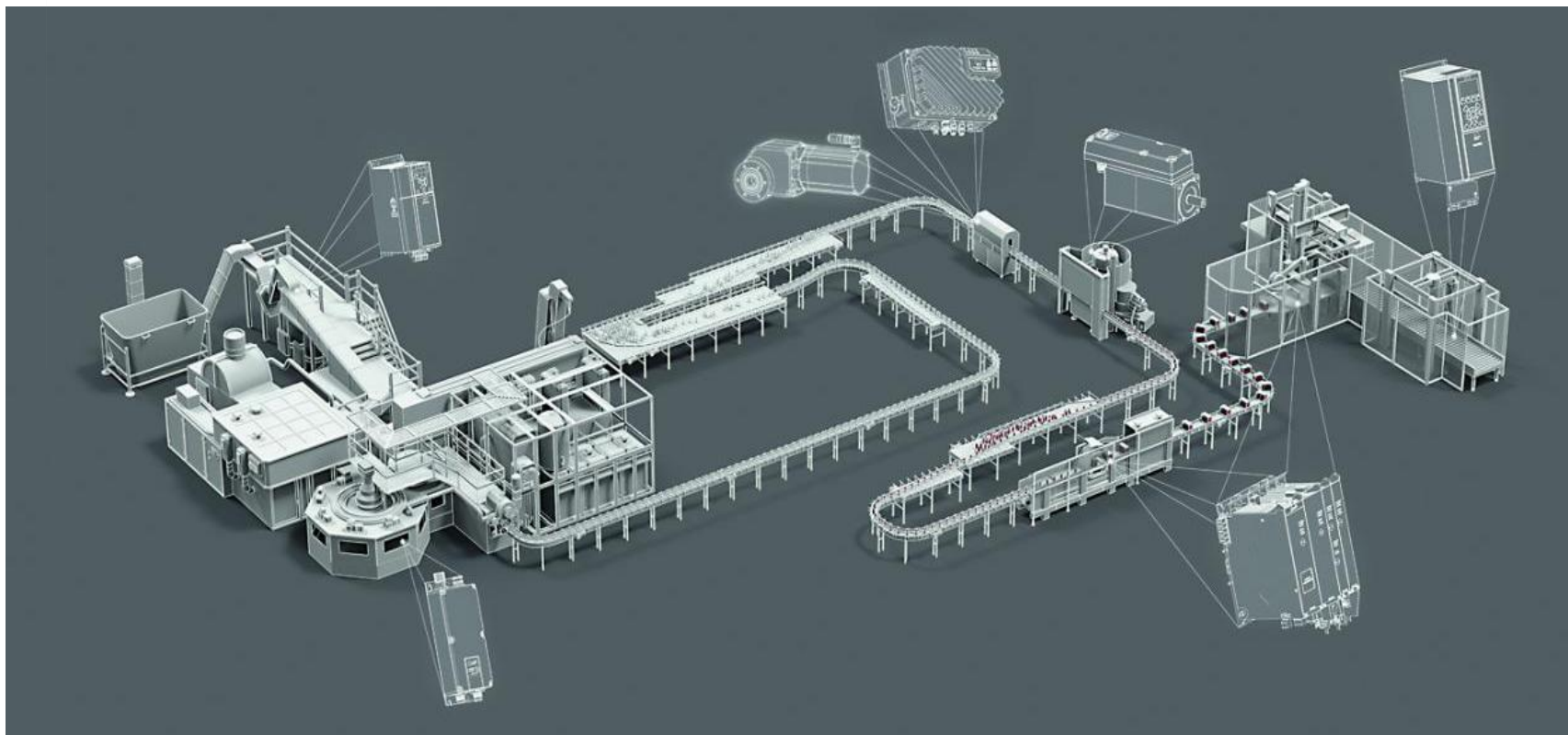


Seamless Integration into Automation Environments





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

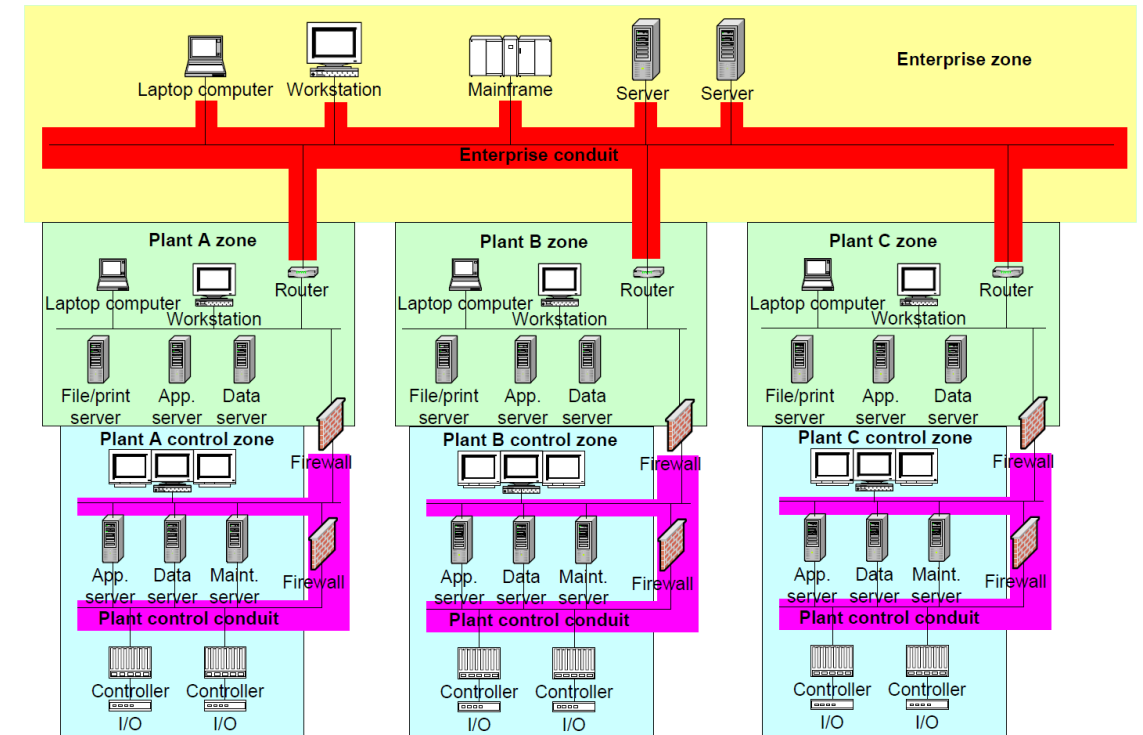
Activities such as manufacturing, mining, oil and gas, utilities, and transportation, ...

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.

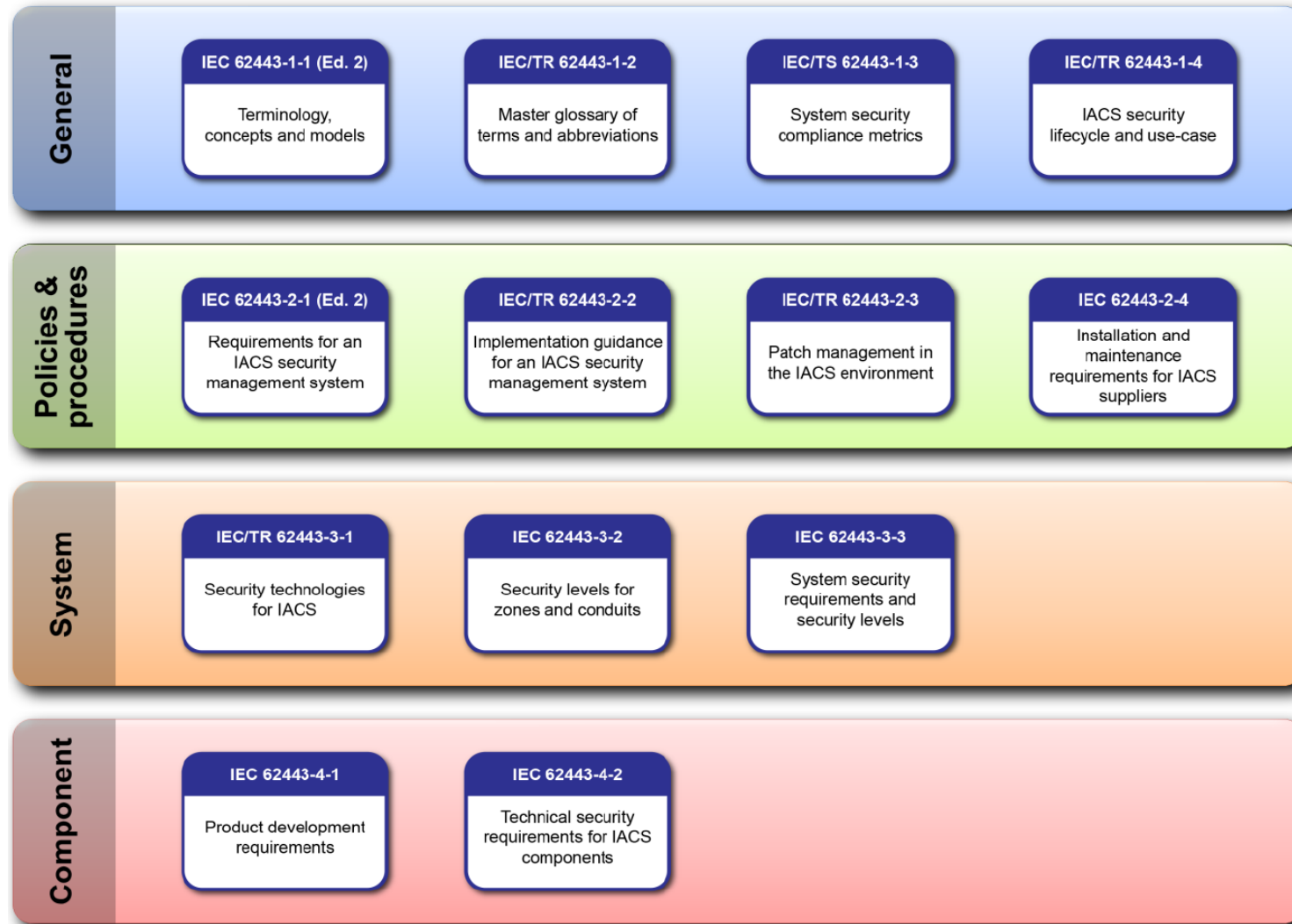
Simple core idea

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?

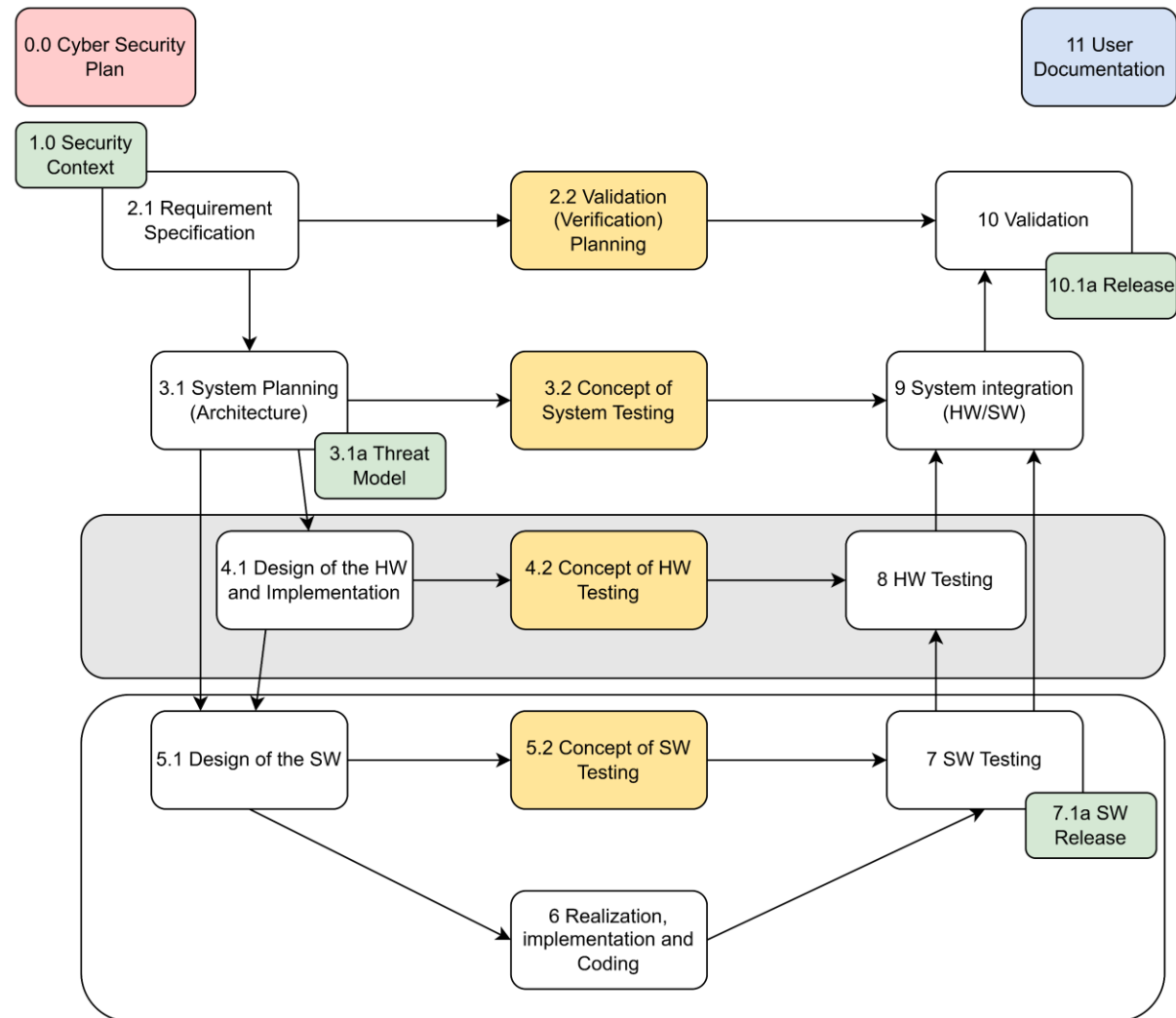


Open-Source Software is **out of scope** of the CRA if they are used in Open-Source projects!

If Open-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



5

HOME SAFETY THREATS

you might overlook

You're a careful parent who steers children away from things that could harm them. But hidden threats lurk in every house, sometimes where you least expect them. For safety's sake, look through your home often. Keep an eye out for not-so-obvious hazards. Here are 5 of them:



SCALDING WATER

It is common for a home's water heater to be set above 120°F (48.8°C); this can cause a scald burn to a child in seconds. Scalding hot tap water causes **3,800** injuries and more than **30** deaths a year. A lot of victims are young kids.



UNSTABLE FURNITURE

Each year, **thousands** of young kids are badly injured and some die, when large TVs and heavy furniture tip over on them. Often, the victims were climbing, or pulling themselves up on, or falling against unstable furniture.



WINDOW BLINDS

Hundreds of children have strangled to death after getting tangled up in cords or chains on window blinds. Window coverings sold before 2001 pose the most danger.



CHEMICAL STORAGE

Since the year 2000, the number of poisoning deaths has **doubled** among children. Many poisons are found in the garage, kitchen or bathroom. They include pesticides, automotive products, weed killers, and household cleaning and disinfectant products.



HOME TRAMPOLINES

Backyard trampolines send **tens of thousands** of people younger than 20 to doctors and emergency rooms each year. Injuries range from sprains, broken bones, and cuts to neck and spinal cord injuries, paralysis, and even death.

Solutions

1

Set your hot water heater to no higher than 120°F (48.8°C), and check the temp of your tap water to ensure it is safe.

2

Double check the stability of large furniture. Anchor stoves, bookcases, shelves, or bureaus to the wall. Get rid of items that may tempt kids to climb.

3

Secure the cords of older window coverings so children can't reach them. Move cribs, beds, and other furniture away from windows. Use cordless window coverings.

4

Store harmful chemicals in their original, labeled containers safely out of reach. Consider locked cabinets for storage. Never leave chemicals unattended when you are using them.

5

Avoid use of home trampolines. In gym classes or competitive sports, use a trampoline only with strict adult guidance and supervision.

Franciscan HEALTH

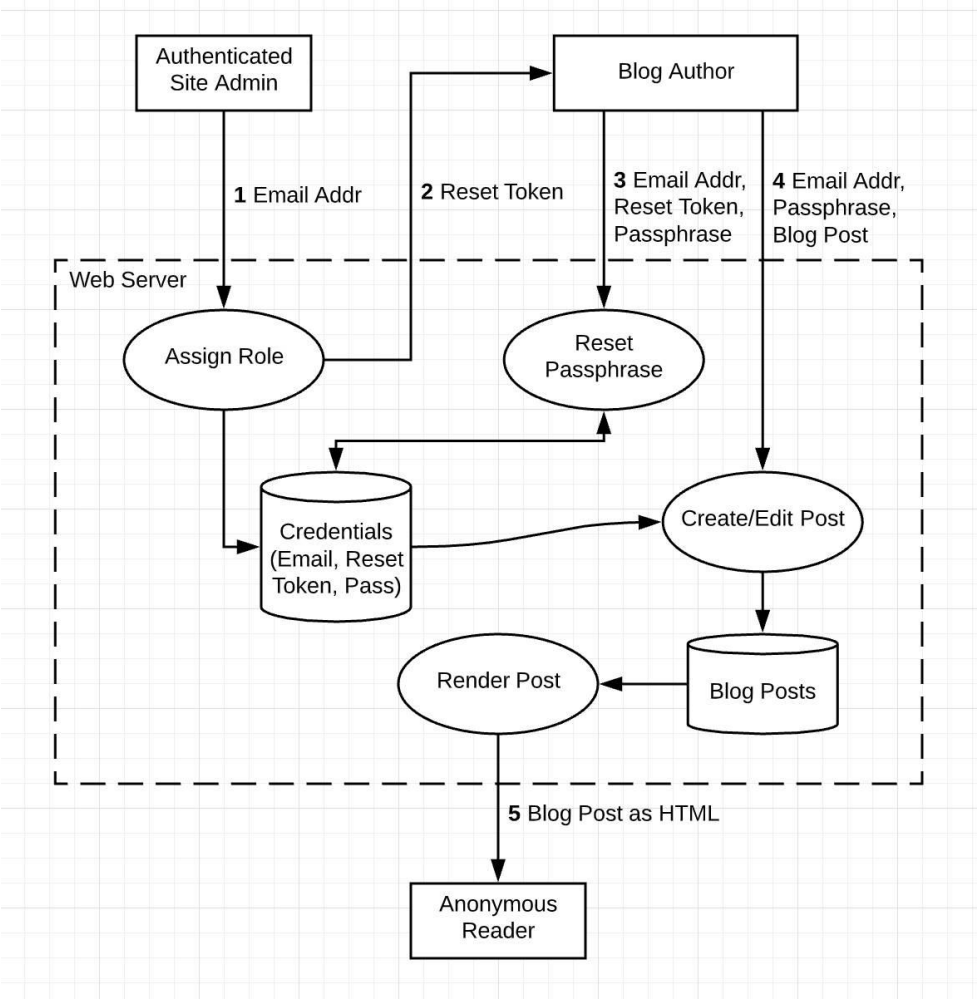
FranciscanHealth.org

VLT® FlexMotion™

Classified as Business

16

Threat Modeling: Example



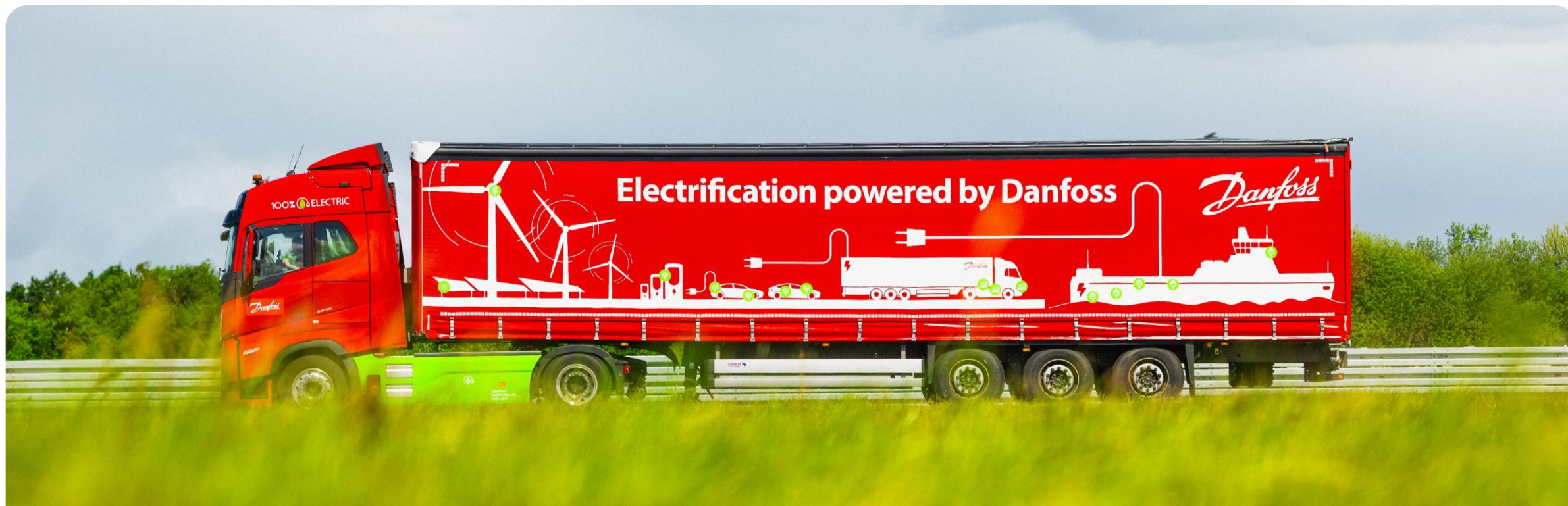
STRIDE THREAT MODEL

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

Crane Hall



16:00

40 mins
07/11/2025

Danfoss

TALK

OPC UA in Industrial Automation

Seminar 3

Danfoss

17:20

15 mins
07/11/2025



