(I)IoT Cyber Security SICK Linköping

Joakim Delbom / Fredrik Claesson, 2024-08-16

Cyberly / IoT World, Linköping Science Park

IT ALL STARTED IN A SMALL SHED

OUR ROOTS ARE IN SAFETY AND ENVIRONMENTAL PROTECTION

ERWIN SICK
Company founded in 1946

Our Purpose

SICK
Sensor Intelligence.

WE BELIEVE IN USING TECHNOLOGY FOR GOOD

- to protect people
- to free people from tedious tasks
- to preserve our planet

WE CONTRIBUTE TO A SUSTAINABLE FUTURE

- by co-creating dynamic and desirable solutions
- by working together as an inspiring network
- with vision, curiosity and courage

WE DELIVER SENSOR INTELLIGENCE.

- by combining the physics of sensing with electronics, software, data, learning, and empathy

Using “Sensor Intelligence.” in a smart way

As a customer, our solutions are open to you and to your systems

Detecting | **Identifying** | **Measuring** | **Protecting** | **Integrating** | **Controlling**

No matter which industry you are in

We will create an individual solution for your business needs

AUTOMOTIVE

BASIC MATERIALS

CONSUMER GOODS

ELECTRONICS

ENERGY

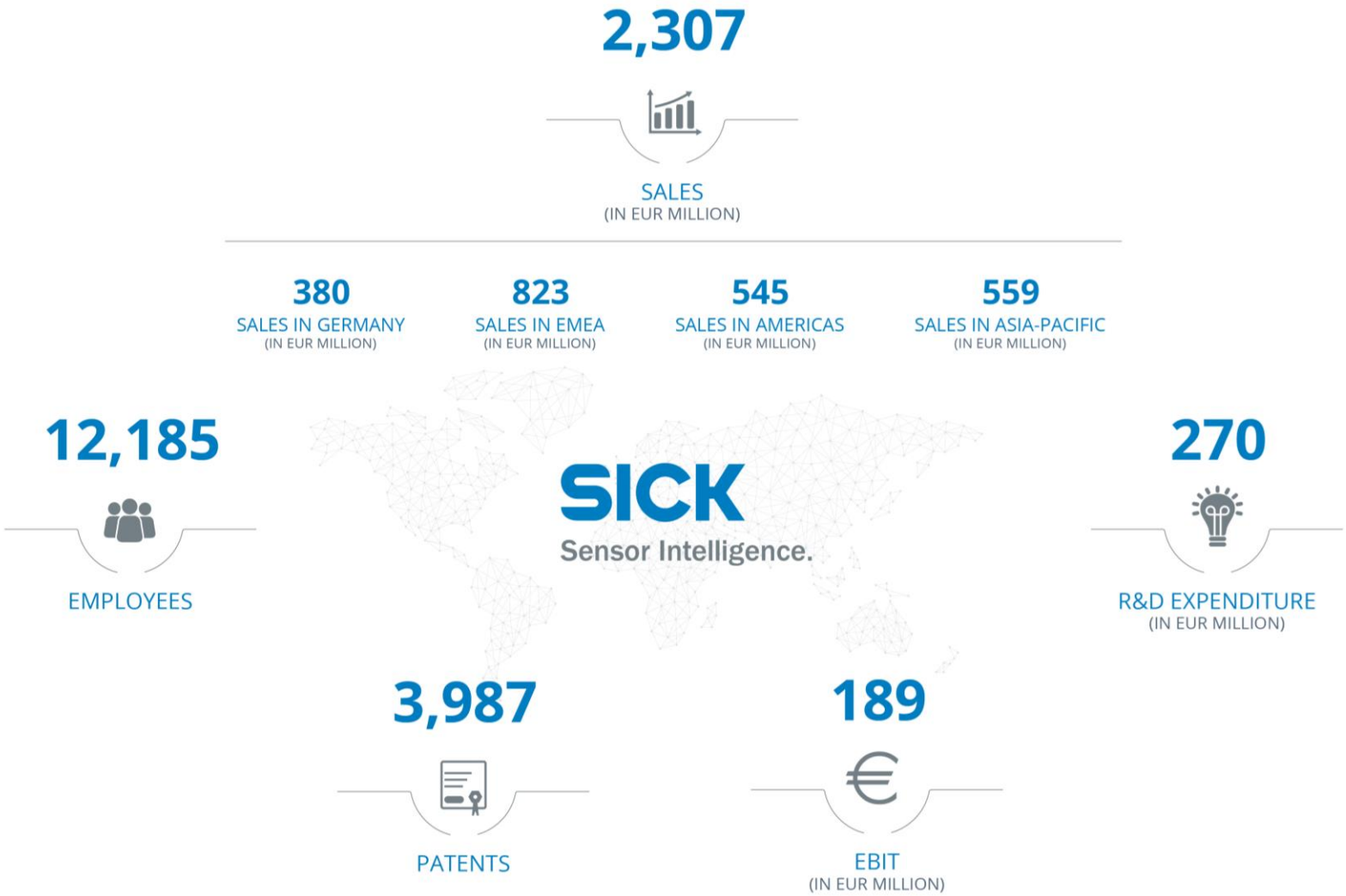
LOGISTICS

MACHINES & MOTION

MOBILITY & OUTDOOR AUTOMATION

SICK at a glance

Key figures (fiscal year 2023)



All markets


Germany
Sweden
China
Italy
USA
Japan
Malaysia
Hungary
Singapore
Subsidiaries and representative offices
Agencies
Production
Regional Competence Center
Development

SICK Linköping - at a glance

More than 35 years of Machine Vision technology

Founded in 1985 –
39 years of Machine Vision technology

Spin-off from Linköping University –
by Prof. Robert Forchheimer in 1985

Innovation Center for Machine Vision
in SICK since 2003

Product & Technology Development and **Marketing,** global responsibility for a subset of SICK's total product portfolio

100+ employees – **with high expertise** in Machine Vision market and technology

Core technology competences: **3D Imaging** technology, **Image Analysis** software, **Artificial Intelligence, GUI and Visualization** and **Robot Vision** solutions

Benefits from the **close connection to the Linköping University**

SICK Machine vision portfolio

Market excellence since the 1990s

2D machine vision

Accessories

3D machine vision

Systems

SensorApps

SICK APP SPACE

Software foundations

NOVA STREAM

Deep Learning

Best fit inline automation solutions in a wide range of industries

Consumer goods

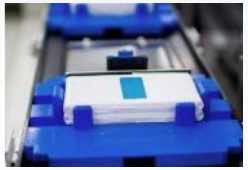
Electronics

Automotive

Wood

Food

Robotics



Battery

Intralogistics

Rail and road

Speaker

Fredrik Claesson, Cyber Security Specialist (2019-) and System Architect. At SICK since 2005.

Operational Technology ←→ Informational Technology

SICK
Sensor Intelligence.

IT is well known through

- Office networks
- Cloud services

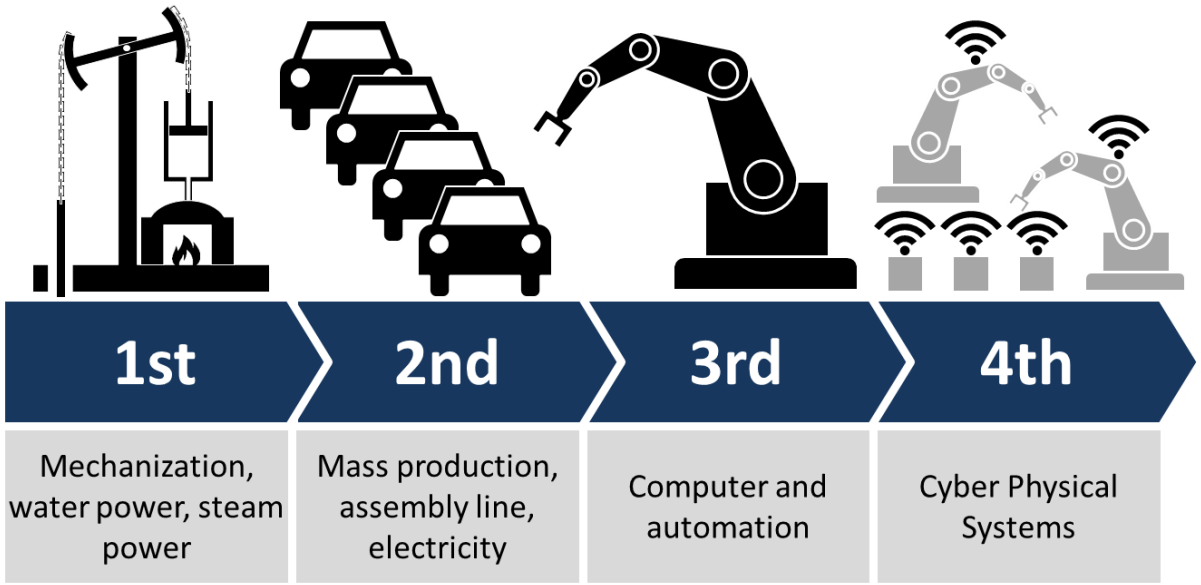
OT = control of the physical world, Industrial Control Systems (ICS), Industrial Internet of Things (IIoT)

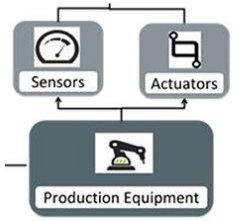
1. Robots
2. Conveyors
3. Manufacturing Machines
4. Sensors (light switches, cameras)

For OT system (Functional) Safety is an additional property to protect from damage.

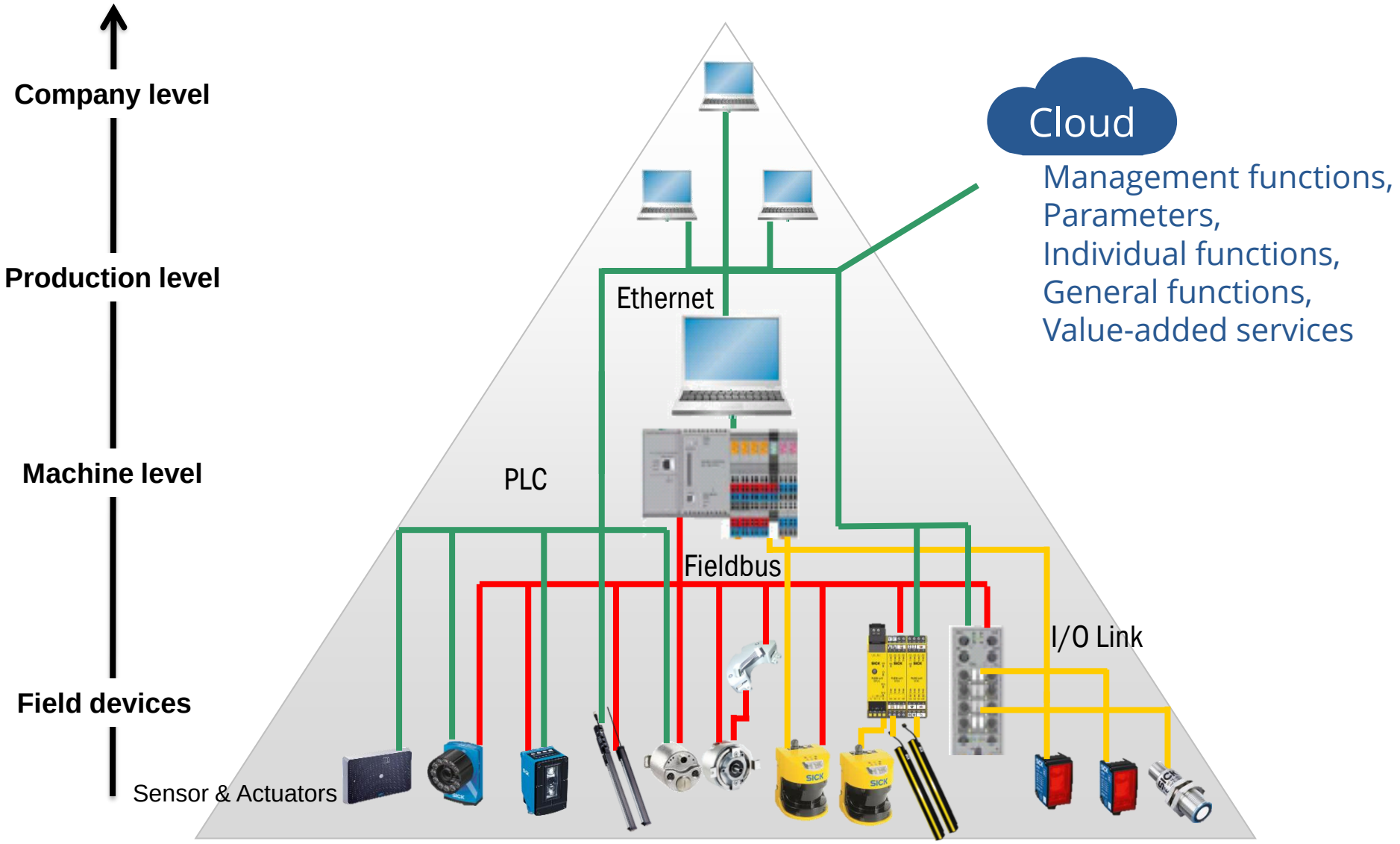
OT System have a very long lifecycle compared to Office IT – 10+ years from introduction to End-of-Life

Industry 4.0


1st
2nd
3rd
4th
Mechanization, water power, steam power
Mass production, assembly line, electricity
Computer and automation
Cyber Physical Systems


Sensors
Actuators
Production Equipment

Industry 4.0


Company level
Production level
Machine level
Field devices
Sensor & Actuators
Ethernet
PLC
Fieldbus
I/O Link
Cloud
Management functions,
Parameters,
Individual functions,
General functions,
Value-added services

Cyber Security Impact for Operational Technology

SICK
Sensor Intelligence.

Internet/Cloud connections → Remote attacks easier

Larger attack surface → More services running on the nodes

Requires Security knowledge to configure → Misconfiguration?

Industry is very slow in installing patches and updates

→ Old vulnerabilities still present

→ Installing updates can require re-qualification of machine

Reputation and trust of brand

Risks in practise

In Industrial systems:

- Often Digital I/O, Serial (RS232, RS485), Fieldbuses (CAN/EthernetIP/ProfiNet)
- Transition to Ethernet based communication → Mitigation of risks of remote access/exploits.
- Typical risks:
  - End-User or System Integrator connect a (misconfigured) VPN tunnel to their laptop for convenient maintenance.
  - Misconfigurated firewalls fail to protect the OT networks or are open to the IT network

With Cloud connection being introduced also into the OT networks

- New attack paths as OT devices needs to be secured against the new threats from cloud connections

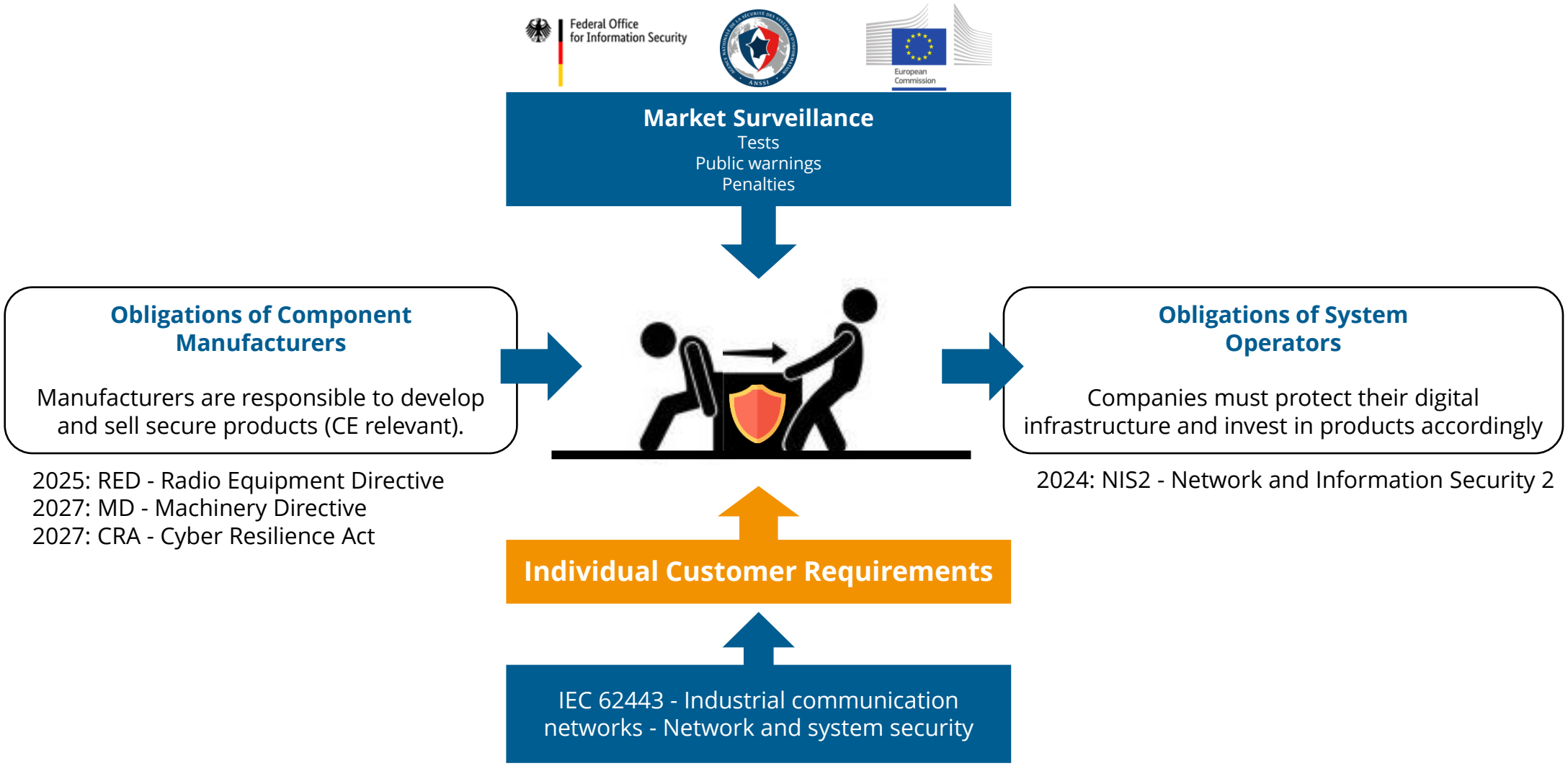
Critical Infrastructure and Personal Information

For SICK an important consideration is if the device is used in

- Applications in Critical Infrastructure
  - Typical examples: Food production, Logistics, and Transport
- Applications which handles sensitive personal information
  - Typical examples: Address labels on logistics applications.

Cybersecurity in the EU

Market requirements



Cybersecurity at SICK

Activities

The cybersecurity management system of SICK is based on the **IEC 62443** “Industrial communication networks – Network and system security” series of international standards. New products and their security features are developed based on the target market and intended use case. SICK applies the so-called defense in depth strategy and well-established standards in the field of encryption.

Secure development lifecycle

- SICK SDL implements risk based scalable requirements for products
- Development process certified according to IEC 62443-4-1
- New products will be developed according to a minimum subset of the standard, select products will comply fully.

Cybersecurity Test Center

- Inhouse test facilities
- Offers:
  - Achilles Test Suite
  - Penetration Tests
  - OpenVAS

PSIRT

- SICK Product Security Incident Response Team (SICK PSIRT)
- CSAF (Common Security Advisory Framework) certified provider.
- Encrypted communication channel for found vulnerabilities
- Advisories are published publicly
- RSS feed available for continuous information of customers

Actors and Security Levels

Example from IEC 62443:

Security Level 0: No protection

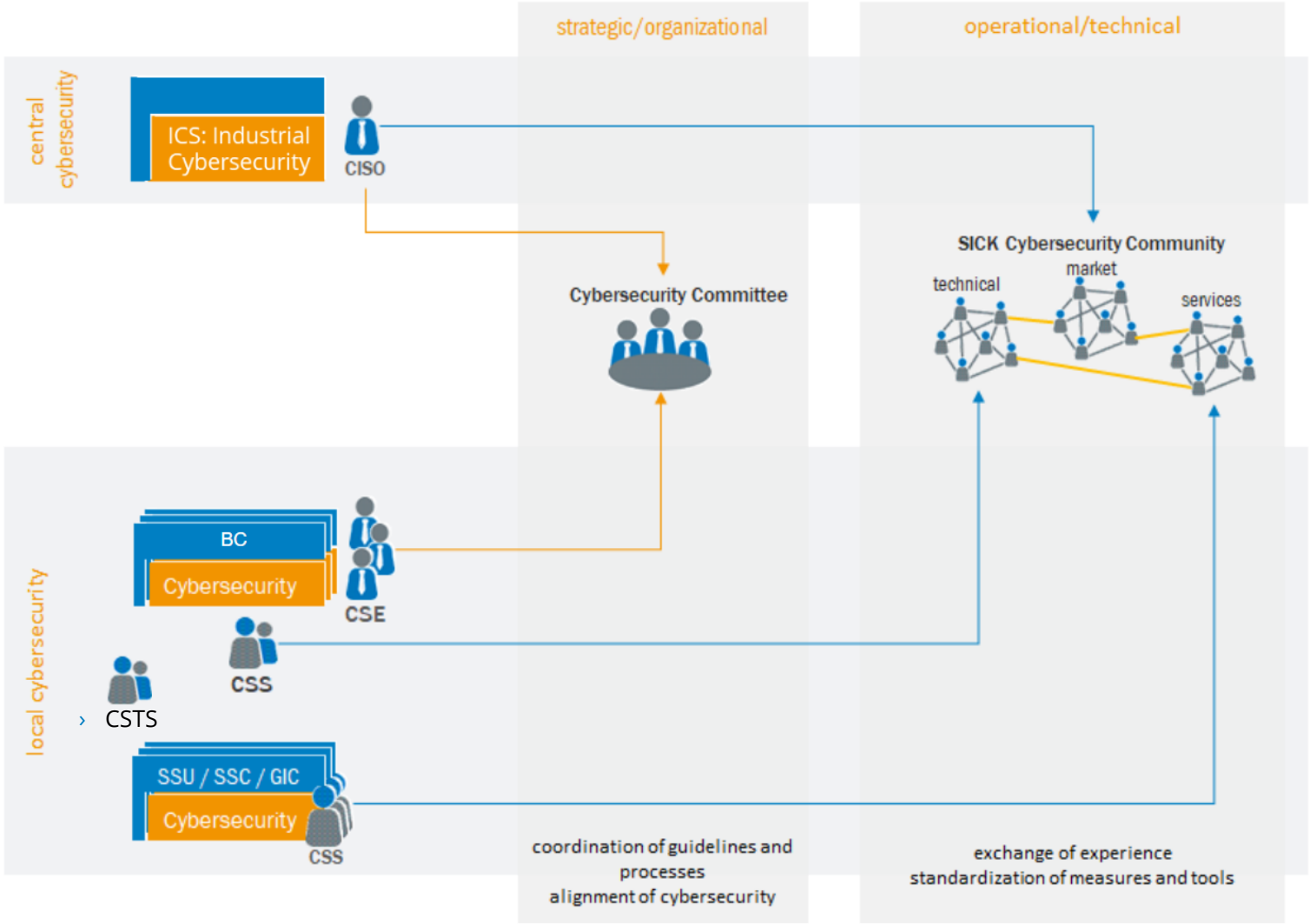
Security Level 1: Protection against unintentional or accidental misuse

Security Level 2: One person acting alone

Security Level 3: Criminal Organization with moderate resources

Security Level 4: Nation-state actor with extensive resources

SICK Cybersecurity Organization



CISO: Chief Industrial Security Officer

CSE: Cybersecurity Expert

CSS: Cybersecurity Specialist

CSTS: Cybersecurity Team Specialist

Outlook

- New EU directives are increasing focus on CyberSecurity for IIoT / OT in the next years.
- Cyber Security requirements are coming from two directions:
  - Regulatory requirements (for CE compliance)
  - Customer driven requirements (fulfil standards, implement specific security features)