ECCO
European Cybersecurity COmmunity

ECCO Community Group on Trusted Supply Chains

Knowledge-Sharing Webinar

Securing supply chains: an overview on challenges and regulatory initiatives

November 21st 2024

Agenda

- Introduction (5 min)
- Main Challenges in the Supply Chain – CISO Perspective (20 min) - Andrzej Bartosiewicz
- Regulation of Cybersecurity focusing on NIS2 / CRA (20 min) – Frank Blaimberger
- Q&A (15 min)

ECCO
European Cybersecurity COmmunity

ECCO Community Group on Trusted Supply Chains

Introduction

November 21st 2024

ECCO Community Working Groups

- Road-mapping
- Startups/Scaleups - SMEs support
- Human factors
- Skills
- Synergies on cybersecurity for Civilian and Space applications
- **Trusted supply chains**
  - **Chairs: Antonio Skarmeta and José Luis Hernández Ramos**
  - Participants: development of a “proto-community” based on the initial list of experts from ECSO and Pilots, and growing with additional people (44 members so far)
  - Objectives
    - Build community of experts on trusted supply chains and Strengthening Trusted and Resilient Supply Chain in Europe
    - Facilitate trusted information sharing about threats (to support prevention and response)
    - Propose a strategy, planning and recommendations to support the NCCs in the implementation of the Strategic Agenda’s Action Plan

Enhancing Supply Chain Security: Strategies, Case Studies, and Roadmapping

- Webinar today focused on:
  - Main challenges for a trusted supply chain with CISO perspective
  - Impact of regulatory landscape in trusted supply chain, specially NIS2/CRA

Planned webinars

- This event is part of a webinar series focused on European cybersecurity supply chain.

- List of webinars
  - Organizational and Operation Security in Trusted Supply Chains (March 19th)
  - Certification in the Lifecycle (May 7th)
  - Enhancing Supply Chain Security: Strategies, Case Studies, and Roadmapping (June 14th)
  - Paradigm shift from cybersecurity to cyber resilience (July 22nd)
  - Strengthening Trusted Supply Chains: Real-Time Attack Detection and Critical Dependency Analysis (November 15th)
  - Securing supply chains: an overview on challenges and regulatory initiatives (today)

ECCO
European Cybersecurity COmmunity

Main challenges in the supply-chain

Dr. Andrzej Bartosiewicz
Enigma SOI / CISO #Poland

Signal: +48.514375128

Securing supply chains: an overview on challenges and regulatory initiatives

SUPPLY-CHAIN

Target Attack (2013)

- The Target data breach is one of the earliest high-profile supply chain attacks. Hackers gained access to Target's systems through a third-party HVAC vendor.
- In September 2013, cybercriminals utilized an email-based phishing scam to trick an employee from Fazio Mechanical—an HVAC contractor and one of Target's third-party vendors—into providing their **credentials**.
- From there, the cybercriminals used these stolen credentials to infiltrate Target's network and install malware on a number of point-of-sale systems on November 15th.
- Using the vendor's credentials, the attackers breached Target's internal systems and stole payment card data from 40 million customers.

Asus Live Update Attack (2019)

In 2019, hackers compromised **Asus Live Update** software, which is used to deliver updates to Asus computers.

The malicious version was distributed to around 500,000 users, targeting specific computers in a rare case of a highly precise supply chain attack.

Operation ShadowHammer

Indeed, the goal of the attack was to surgically target an unknown pool of users, which were identified by their network adapters' MAC addresses. To achieve this, the attackers had hardcoded a list of MAC addresses in the trojanized samples and this list was used to identify the actual intended targets of this massive operation.

SolarWinds Attack (2020)

- One of the most well-known supply chain attacks is the **SolarWinds** attack.
- Hackers infiltrated SolarWinds, a provider of IT management software, and inserted malicious code into their popular Orion software.
- This compromised software was then distributed to thousands of customers worldwide, including U.S. government agencies and large private companies. The attackers gained access to sensitive data and systems of many of these organizations.
- More than 18,000 customers of SolarWinds had applied the „Sunburst update".

September 2019. Threat actors gain unauthorized access to SolarWinds network

October 2019. Threat actors test initial code injection into Orion

Feb. 20, 2020. Malicious code known as Sunburst injected into Orion

March 26, 2020. SolarWinds unknowingly starts sending out Orion software updates with hacked code

Kaseya Attack (2021)

Kaseya, a provider of IT management software, was targeted in 2021 by the **REvil** ransomware group. The hackers exploited vulnerabilities in Kaseya's software to deploy ransomware to its customers, affecting hundreds of companies globally. This attack led to widespread business disruptions.

The attack was carried out by exploiting a vulnerability in VSA (Virtual System Administrator), a **remote monitoring and management software** package developed by Kaseya.

VSAT HACK (2022)

The Viasat hack was a cyberattack against the satellite internet system of American communications company Viasat which affected their KA-SAT network.

On February 23, 2022, hackers targeted a VPN installation, in a Turin management center, which provided network access to administrators and operators.

The hackers gained access to management servers that gave them access to information about company's modems. After a few hours, the hackers gained access to another server that delivered software updates to the modems which allowed them (over-the-air update - OTA update) to deliver the wiper malware AcidRain.

On 24 February, 2022, the day Russia invaded Ukraine, thousands of Viasat modems went offline. The attack caused the malfunction in the remote control of 5,800 Enercon wind turbines in Germany and disruptions to thousands of organizations across Europe, totaling 30,000 modems.

Supply Chain Challenges

A supply chain refers to the network of external suppliers, service providers, and third-party vendors that contribute to an organization's operations by supplying **software**, **hardware**, or **services**. This can include everything from software development and cloud services to hardware components and consulting.

- Business resiliency
- Avoiding fines and penalties
- Maintaining Customer trust
- Protecting organizations against paying a ransom

Supply Chain Cybersecurity Standards

NIST SP 800-161

The **National Institute of Standards and Technology (NIST)** Special Publication 800-161, titled "Supply Chain Risk Management Practices for Federal Information Systems and Organizations," provides **guidelines for managing cybersecurity risks throughout the supply chain**. It outlines how to identify, assess, and mitigate risks from suppliers and vendors, and emphasizes integrating supply chain risk management (SCRM) into the organization's overall risk management framework.

CIS Controls (Version 8)

The **Center for Internet Security (CIS) Controls** provides a set of best practices for cybersecurity, including specific controls for managing supply chain risks.

Control 15, in particular, focuses on the secure configuration of hardware and software, including **third-party systems and supply chain management.**

IEC 62443

IEC 62443 is developed by the International Electrotechnical Commission (IEC) that provides a comprehensive framework for addressing cybersecurity in industrial automation and control systems (IACS). The standard defines security practices for both **product suppliers** and **system integrators** involved in delivering hardware, software, and services in industrial environments. It ensures that these **suppliers** adhere to secure development, deployment, and management practices.

Supply Chain Challenges

DORA RTS Risk of Supply Chain Attacks	GDPR Third-Party Data Breaches	Lack of Visibility into Third-Party Risks	Complexity of Managing Multiple Suppliers	27001 PCI-DSS 62443 SOC2 Inconsistent Security Standards Across Partners ...more
Weak Vendor Cybersecurity Controls	Difficulty in Real-Time Threat Detection	Compliance and Regulatory Challenges	Vendor Onboarding and Offboarding	Limited Resources for Risk Assessment
Supply Chain Interdependencies	Zero-Day Vulnerabilities in Supplier Networks	Challenges with Incident Response and Communication	Inadequate Security Audits	„Ad hoc" Remote Access

Regulatory Answer to the Supply Chain Risks for the Financial Sector

DORA

- Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on **digital operational resilience** for the financial sector.

Regulatory Technical Standards published by ESAa

- Draft Regulatory Technical Standards to specify the detailed content of the policy in relation to the **contractual arrangements on the use of ICT services supporting critical or important functions** provided by ICT third-party service providers as mandated by Regulation (EU) 2022/2554

DORA - Definitions

‘ICT third-party risk’ - *means an ICT risk that may arise for a financial entity in relation to its **use of ICT services** provided by **ICT third-party service providers** or by **subcontractors** of the latter, including through outsourcing arrangements*

‘ICT concentration risk’ *means an exposure to individual or multiple related critical ICT third-party service providers **creating a degree of dependency** on such providers so that the unavailability, failure or other type of shortfall of such provider may potentially endanger the ability of a financial entity to deliver critical or important functions, or cause it to suffer other types of adverse effects, including large losses, or endanger the financial stability of the Union as a whole;*

DORA Requirements

holistic ICT multi-vendor strategy

maintain and periodically test appropriate ICT business continuity plans

identify **key dependencies** on ICT third-party service providers

each **threat-led penetration test** shall cover several or all critical or important functions of a financial entity, and shall be performed on live production systems supporting such functions, including functions provided by ICT service providers

financial entities shall manage ICT third-party risk as an **integral component** of ICT risk within their ICT risk management framework

for ICT services supporting critical or important functions, financial entities shall put in place **exit strategies**

participation of ICT third-party service providers in the financial entities' ICT security **awareness programmes**

DORA - Contractual Agreements

(a) a clear and complete **description of all functions** and ICT services to be provided by the ICT third-party service provider, indicating whether subcontracting of an ICT service supporting a critical or important function, or material parts thereof, is permitted and, when that is the case, the conditions applying to such subcontracting;

(b) the locations, namely the regions or countries, where the contracted or subcontracted functions and ICT services are to be provided and where data is to be processed, including the **storage location**, and the requirement for the ICT third- party service provider to notify the financial entity in advance if it envisages changing such locations;

(c) provisions on **availability, authenticity, integrity and confidentiality** in relation to the protection of data, including personal data;

(d) provisions on ensuring access, recovery and return in an easily accessible format of personal and non-personal data processed by the financial entity in the **event of the insolvency**, resolution or discontinuation of the business operations of the ICT third-party service provider, or in the event of the termination of the contractual arrangements;

(e) service level descriptions, including updates and revisions thereof;

(f) the obligation of the ICT third-party service provider to provide assistance to the financial entity at no additional cost, or at a cost that is determined *ex-ante*, when an ICT incident that is related to the ICT service provided to the financial entity occurs;

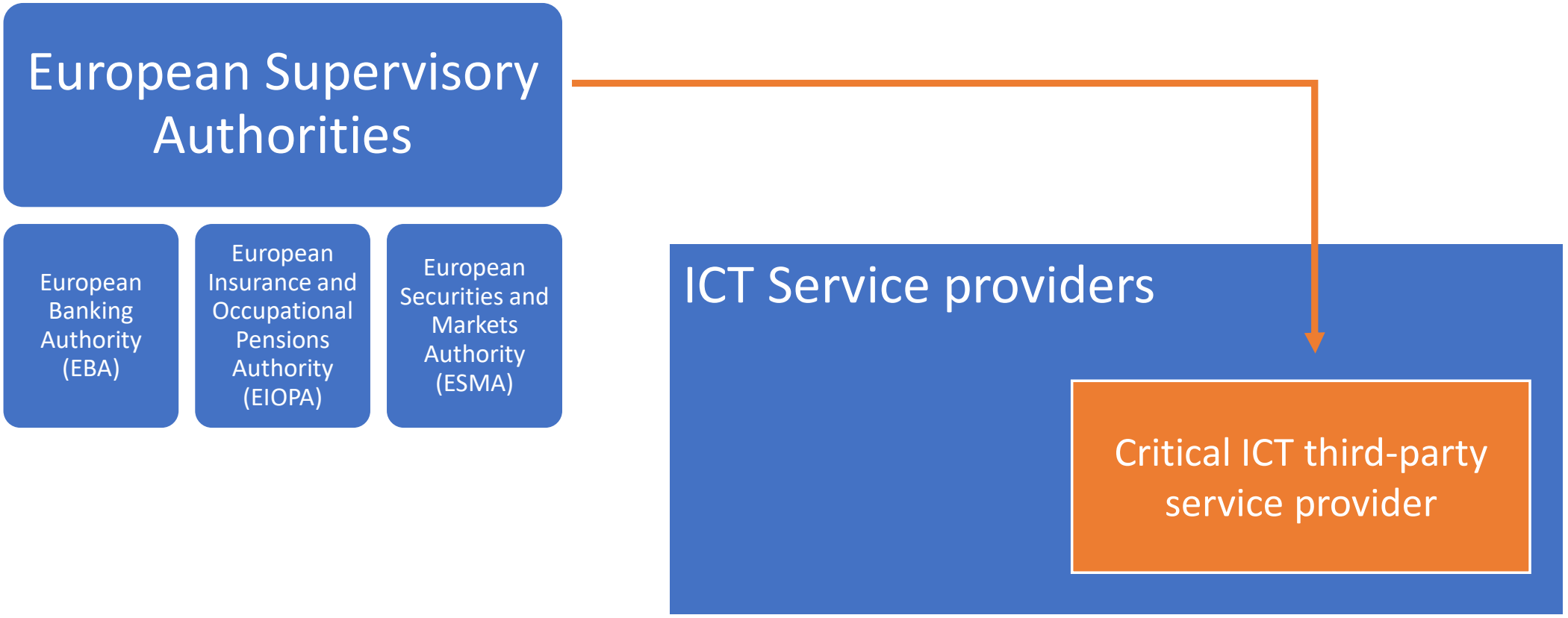
(g) the obligation of the ICT third-party service provider to fully cooperate with the competent authorities and the resolution authorities of the financial entity

(h) termination rights and related **minimum notice periods for the termination** of the contractual arrangements, in accordance with the expectations of competent authorities and resolution authorities;

(i) the conditions for the participation of ICT third-party service providers in the financial entities' ICT **security awareness programmes** and digital operational resilience training

DORA

Oversight Framework of critical ICT third-party service providers



Assessment of Critical Service Providers

(a) ICT requirements to ensure, in particular, the **security, availability, continuity, scalability and quality of services** which the critical ICT third-party service provider provides to financial entities, as well as the ability to maintain at all times high standards of availability, authenticity, integrity or confidentiality of data;
(b) the physical security contributing to ensuring the ICT security, including the **security of premises, facilities, data centres**;
(c) the **risk management processes**, including ICT risk management policies, ICT business continuity policy and ICT response and recovery plans;
(d) the governance arrangements, including an organisational structure with clear, transparent and consistent **lines of responsibility and accountability** rules enabling effective ICT risk management;
(e) the identification, monitoring and prompt **reporting of material ICT-related incidents** to financial entities, the management and resolution of those incidents, in particular cyber-attacks;
(f) the mechanisms for **data portability, application portability and interoperability**, which ensure an effective exercise of termination rights by the financial entities;
(g) the **testing of ICT systems, infrastructure and controls;**
(h) the **ICT audits**;
(i) the use of relevant **national and international standards** applicable to the provision of its ICT services to the financial entities

Critical Service Providers - Investigations

(a) examine records, data, procedures and any other material relevant to the execution of its tasks, irrespective of the medium on which they are stored;

(b) take or obtain certified copies of, or extracts from, such records, data, documented procedures and any other material;

(c) summon representatives of the critical ICT third-party service provider for oral or written explanations on facts or documents relating to the subject matter and purpose of the investigation and to record the answers;

(d) interview any other natural or legal person who consents to be interviewed for the purpose of collecting information relating to the subject matter of an investigation;

(e) request records of telephone and data traffic.

ECCO
European Cybersecurity COmmunity

Digital Transformation –

Regulation of Cybersecurity Focusing on NIS2 / CRA

Frank L. Blaimberger
TÜV SÜD - Global Head Advanced Manufacturing

Digital Transformation - CyberSecurity Regulation

ECCO
European Cybersecurity COmmunity

01	**CyberSecurity – Part of EU Legislative Framework**
02	CRA & NIS 2 – Rule it All ?
03	Testing, Inspection, Certification – In Real World
04	Static is not Enough - Digital Twin for Dynamic & Virtual Operation

Safety & Security today…

..based on 3 Pillars

1

Requirements for organization
Capability of people – certification of persons

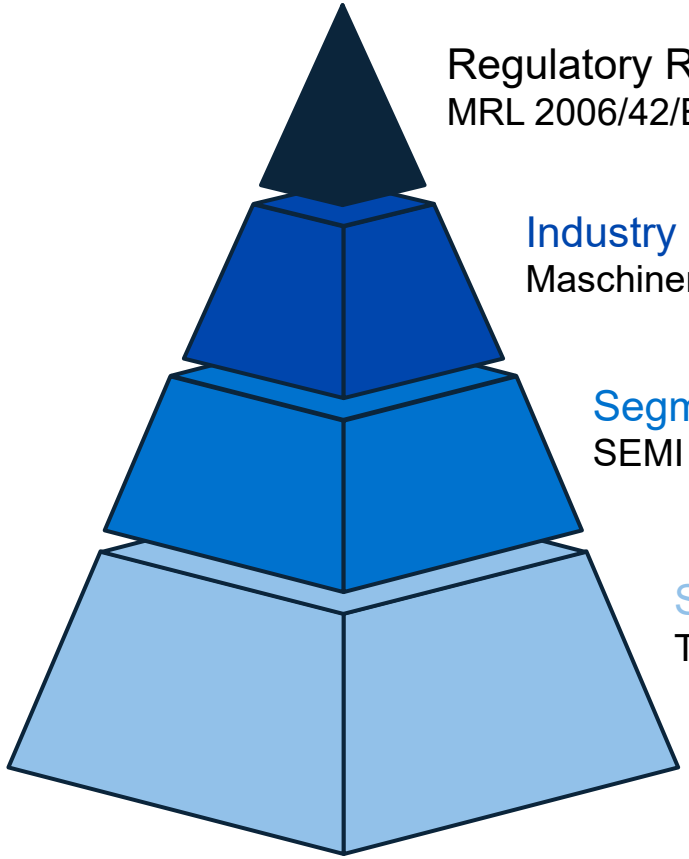
2

Requirements for development process
Process capability – process certification

3

Requirements for product
Product capability – certificate / factory audits

- Self-declaration is the most effective way
- How de we integrate “recombinant growth” into the process if no harmonized standards are available for innovation?



Regulatory Requirements
MRL 2006/42/EG, NEC/NFPA79

Industry Standards
Maschinensicherheits-Typ A-, B- und C-Normen

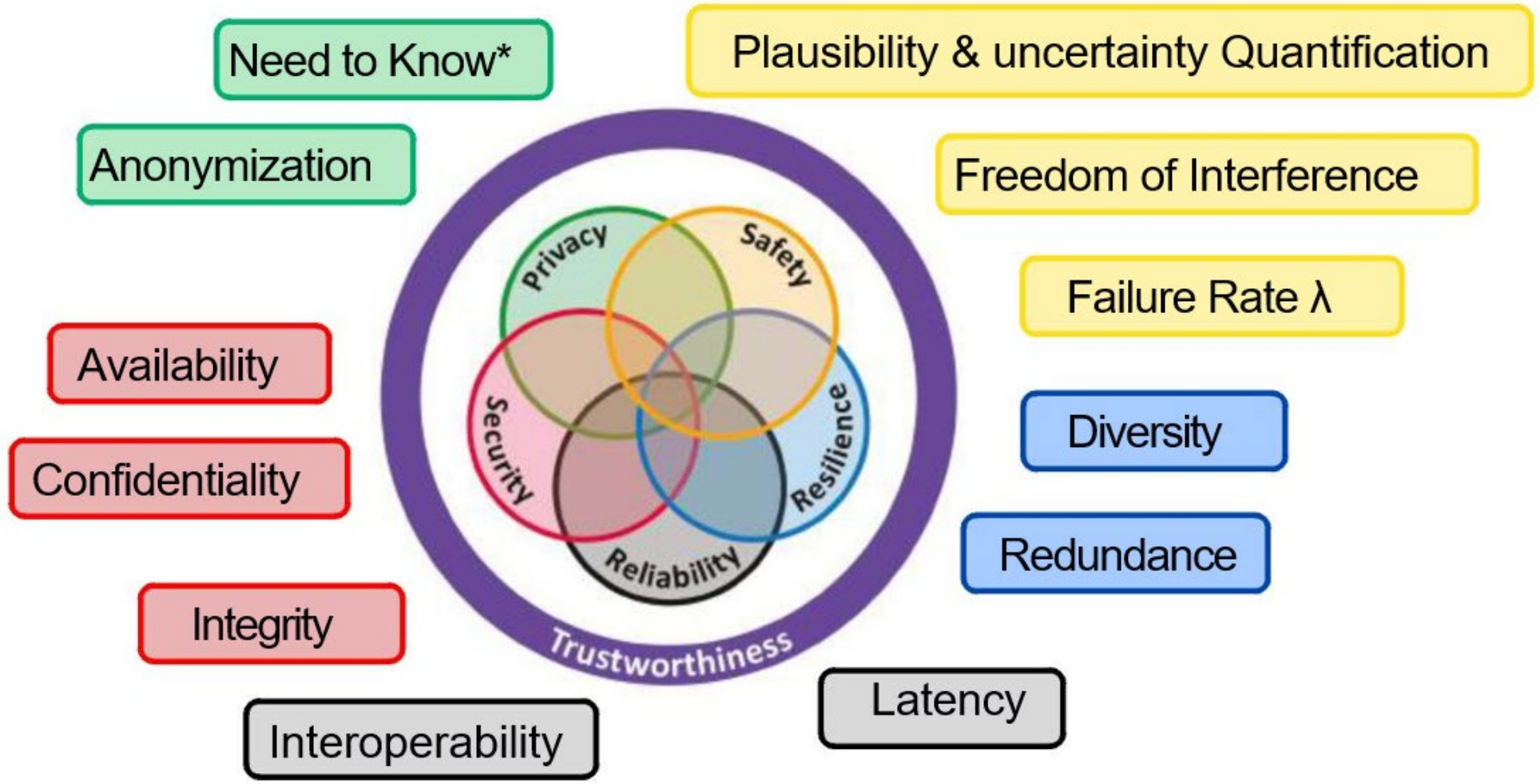
Segment Specific Standards
SEMI Standards, OEM Standards

Safety Documentation
Test Requirements, Test Data Sheets

The complete safety chain has to be **assessed and documented by paper**

Knowledge Economy Requires Trustworthiness

CyberSecurity is a Part of Trustworthiness



Source: IIC Industrial Internet Consortium

EU Regulation set the Focus on Thrustworthiness & Resilience

Machinery 2006/42/EC / 2023/1230

EMC 2014/30/EU

RED 2014/53/EU

LVD 2014/35/EU

ATEX 2014/34/EU

Pressure 2014/68/EU

:::

Machinery Regulation EU2013/1230

Cybersecurity Act COM 2019

AI Liability Regulation

Data Act COM 2022

Cyber Resilience COM 2023

Battery Regulation

:::

Trustwothiness… – Addresses new Regulation

..based on 4 Pillars

1

Requirements for organization Capability
of people – certification of persons

2

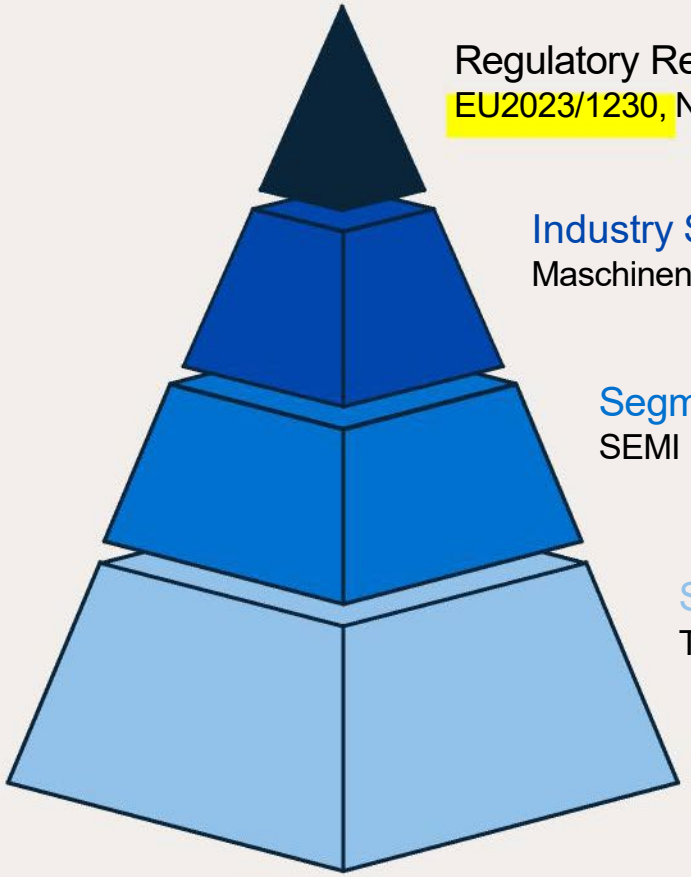
Requirements for development process
Process capability – process certification

3

Requirements for product
Product capability – certificate / factory audits

4

Monitoring and assessment
over the technical lifecycle
Impact of ML/AI, Security, SW. context and env. changes



Regulatory Requirements
EU2023/1230, NEC/NFPA79

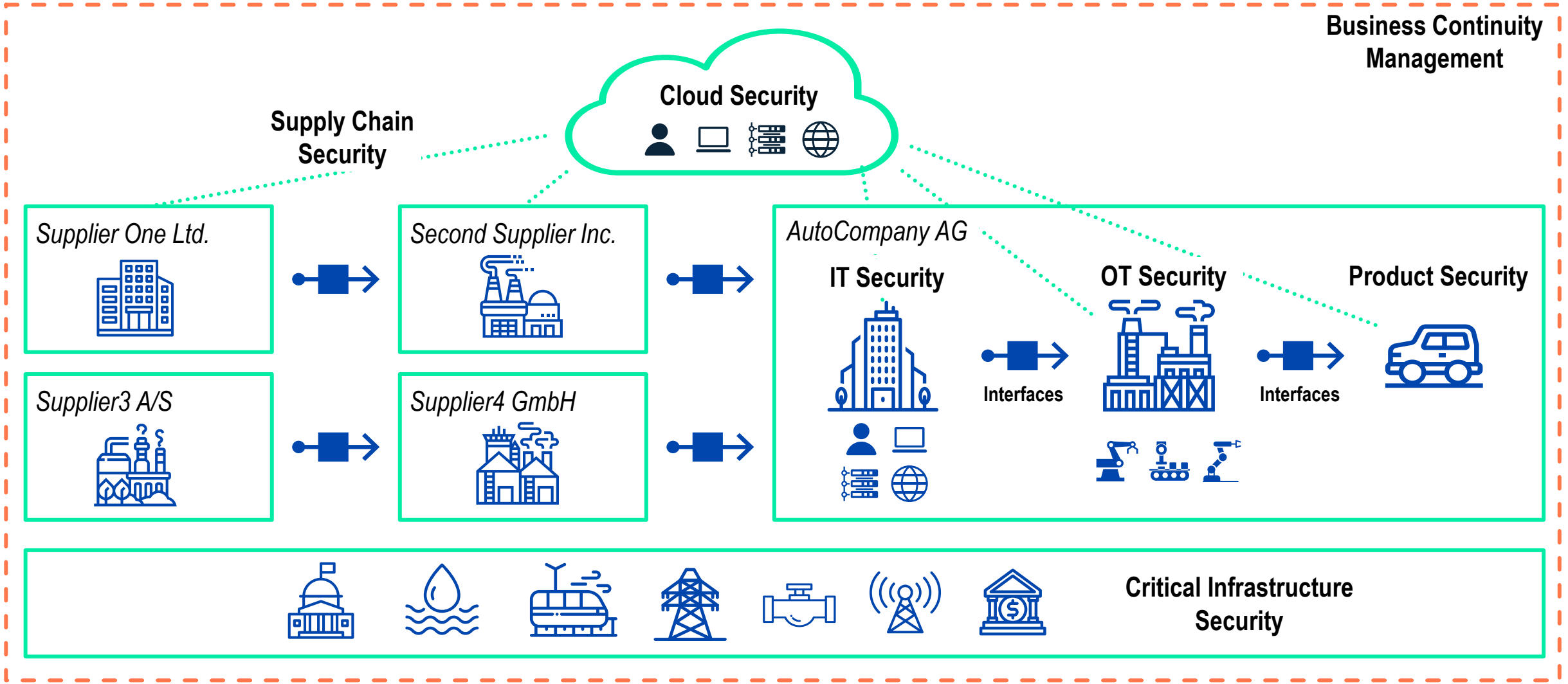
Industry Standards
Maschinensicherheits-Typ A-, B- und C-Normen

Segment Specific Standards
SEMI Standards, OEM Standards

Safety Documentation
Test Requirements, Test Data Sheets

The complete safety/security supply chain has to be assessed by utilizing **digital twins** & **continuously monitoring**

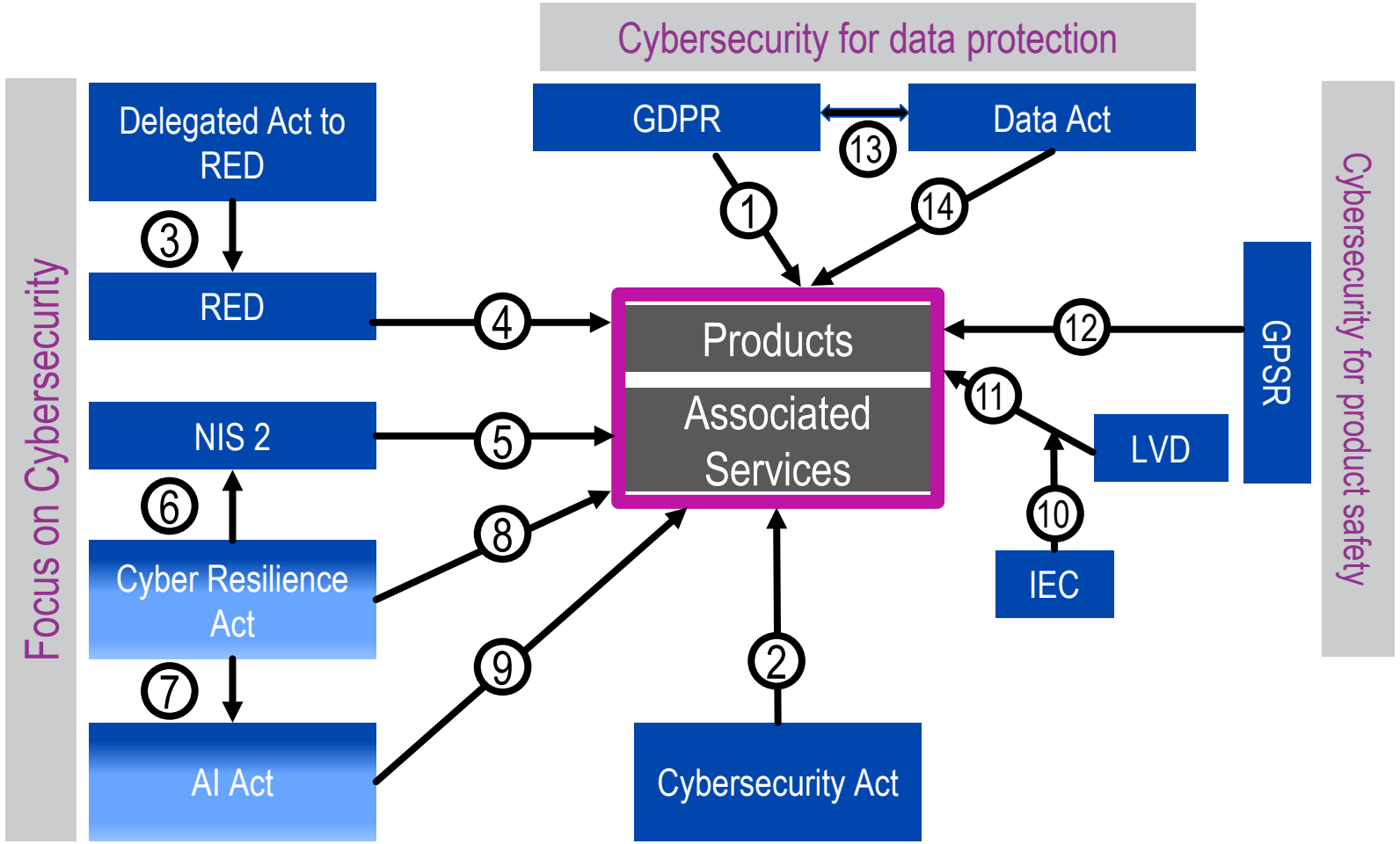
What is CyberSecurity @ Supply Chain



CyberSecurity Requirement Landscape

Requirements	Data & Governance	Cyber-security	Risk Management	Compliance and Conformity	Regulatory applicable
ISO/IEC and E/IEC, AI	**ISO/IEC 38507** Governance **ISO/IEC 42006** Auditor accreditation	**ISO/IEC 27090** Cyber security Artificial Intelligence **ISO/IEC 23894** AI-Risk Management	**ISO/IEC 24029** AI-Risk Management	**ISO/IEC CD 42001** Audit & certification of artificial intelligence **ISO/IEC CD 42006** Management systems **ISO/IEC 23894** AI-Risk Management	**AI Act**
Manufacturing, Power, Railways, Industry 4.0, Digital, IIOT	**NERC - CIP** Framework- Risk Management **NIS 2** Network and Information Security	**CLC/TS 50701** Railway Cyber Security **UR E26 & E27** Marine Cyber Security **IEC 61162-460** Ship navigation systems **CRA** Cyber Resilience Act **RED** Radio Equipment	**NIST SP 800-82** Framework- Risk Management	**IEC 62443** Conformity assessment **ISO 21434** Automotive CSMS	**CRA** **NIS 2** **RED** **NIST SP 800-82** **UR E26 & E27**

Europe Legislative Landscape's Impact on IoT / Industry



1. Defines data privacy requirements.
2. Establish a European cyber security certification framework.
3. Defines scope of security requirements.
4. Defines security requirement for radio equipment.
5. Defines Cybersecurity risk management measures for essential and important entities
6. Requires notified body for critical component used by essential entities.
7. Provide security conformance.
8. Defines Security requirement for the whole life cycle.
9. Defines compliance requirement for provider of high-risk AI.
10. Publishes international standard, updated with security. Then transposed to EN.
11. Defines requirement for safety.
12. Applies to consumer products when there are no specific provisions with the same objective.
13. GDPR prevails in case of conflict.
14. Defines data usage

Published

Draft

Digital Transformation - CyberSecurity Regulation

ECCO
European Cybersecurity COmmunity

01	CyberSecurity – Part of EU Legislative Framework
02	**CRA & NIS 2 – Rule it All ?**
03	Testing, Inspection, Certification – In Real World
04	Static is not Enough - Digital Twin for Dynamic & Virtual Operation

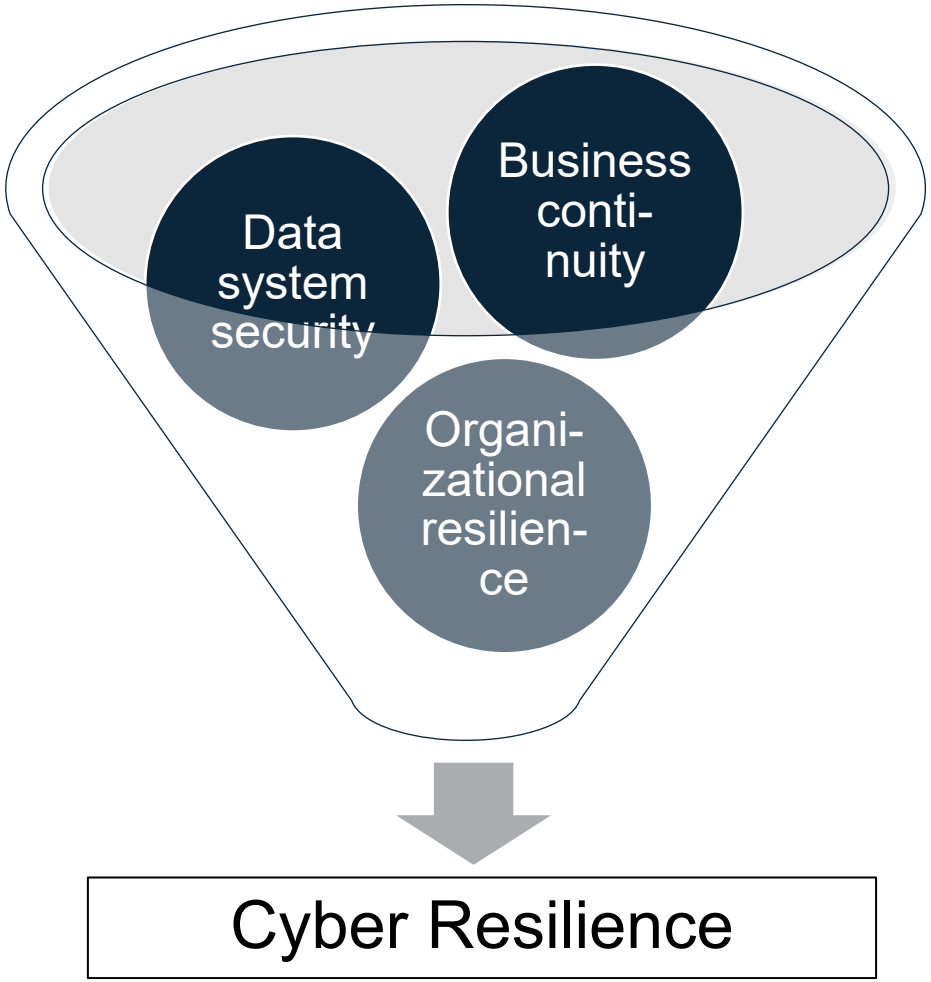
Network and Information System - NIS 2

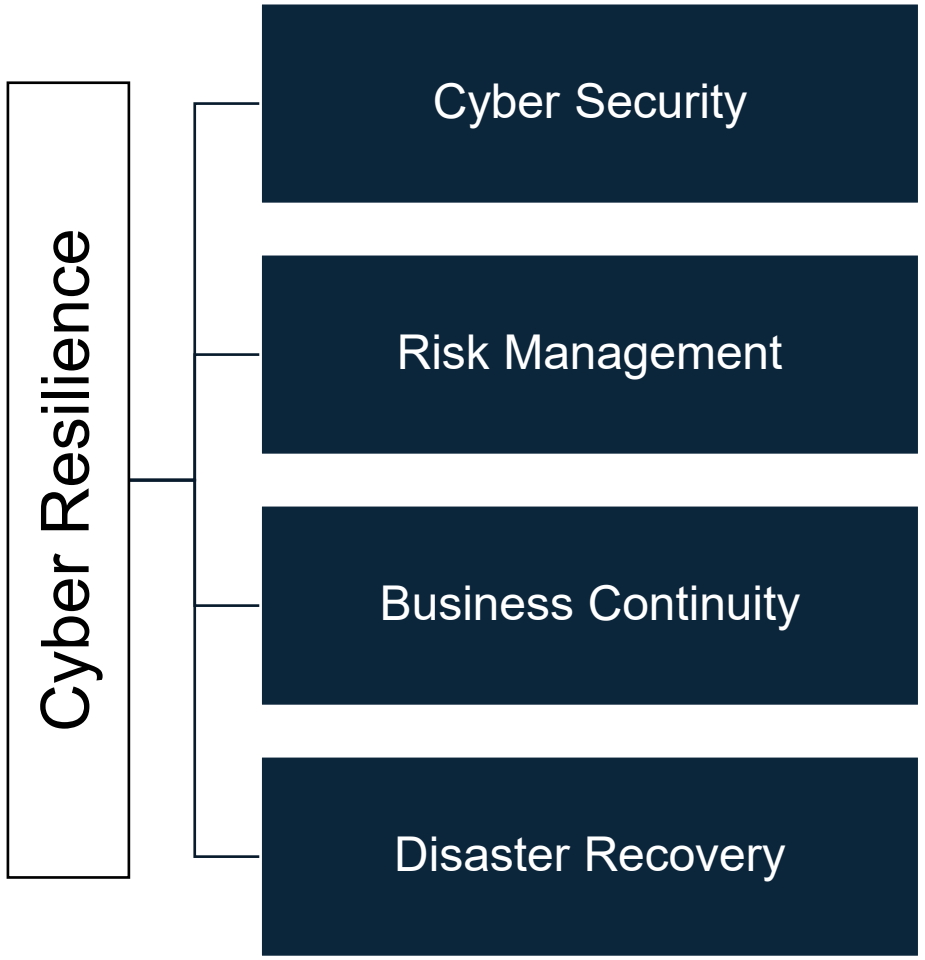
Why? -> To further improve the resilience and incident response capacities of public and private entities

How?

- Adding new sectors based on their criticality for the economy and society, and by introducing a clear size cap
- Reclassify entity into essential and important categories with the consequence of being subjected to different supervisory regimes
- Strengthens security requirements for the companies, by imposing a risk management approach providing a minimum list of basic security elements that have to be applied. The proposal introduces more precise provisions on the process for incident reporting, content of the reports and timelines
- Requiring individual companies to address cybersecurity risks in supply chains and supplier relationships.
- More stringent supervisory measures for national authorities, stricter enforcement requirements and aims at harmonizing sanctions regimes across Member States.

Understanding CyberResilience





CyberResiliant Act – What to do & Where to Spot

EU declaration of conformity
(Art. 28 / 32, Annex V / VI / VIII)

Goal: formally declare conformity
- public -

Internal assessment

Module A: internal control

Third-party assessment
(mandatory only for important / critical products)

Module H: quality assurance

Module B+C:
EU-type examination

EU cybersecurity certification scheme

Technical documentation
(Art. 31, Annex VII)

Goal: substantiate conformity
- not public -

Description, intended purpose

Cybersecurity risk assessment (Art. 13)

Vulnerability handling process
incl. SBOM, where applicable

Design information
Drawings, schemes, system architecture, interaction of system components, production and monitoring process

List of harmonised standards

Test reports (conformity assessment)

How support period was determined

Information & instructions to the user
(Art. 13, Annex II)

Goal: help user use product securely
- provided with product -

Intended purpose, essential functionalities

Security environment, security properties

Foreseeable circumstances / misuse that may lead to cybersecurity risk

Necessary measures for secure use:
(de-)commissioning, operations, changes affecting security, installation of security updates

Essential requirements (Annex I, to be detailed in harmonised standards)

During design

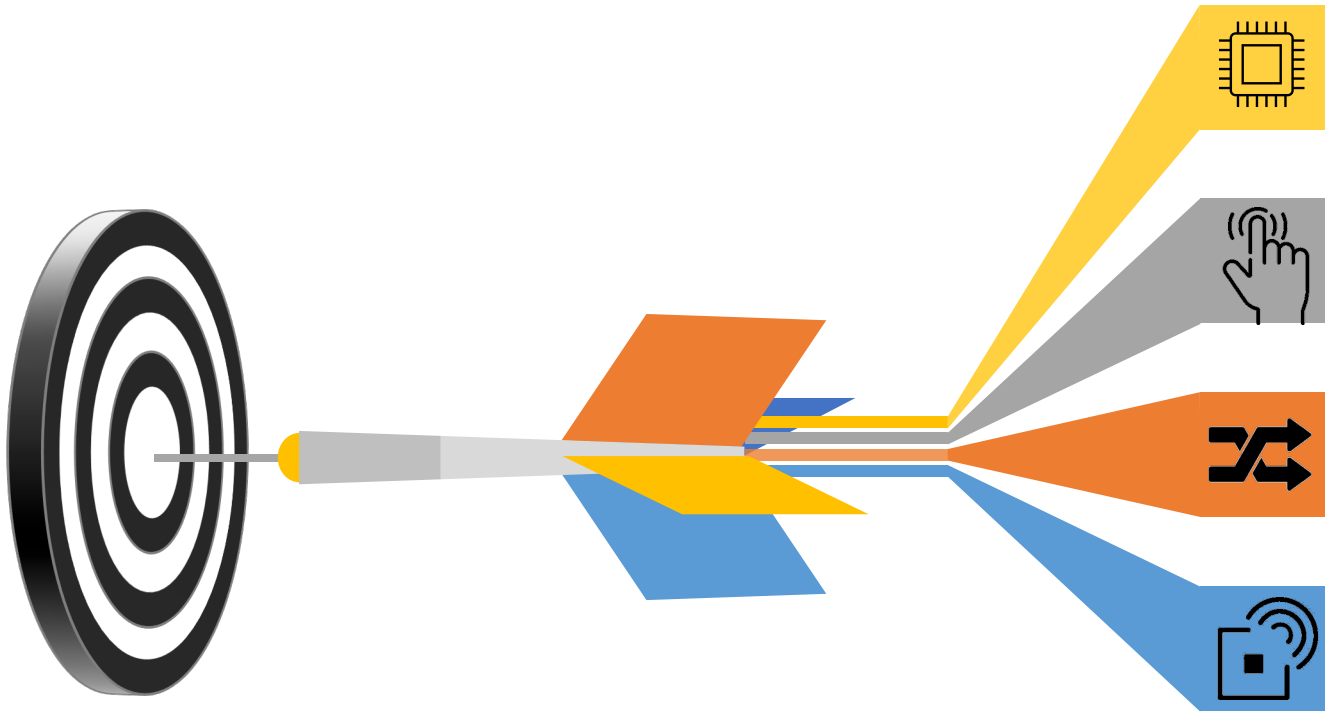
principles / incident prevention
- Integrity & confidentiality of data
- Availability of essential functions
- Access control, authentication
- Limitation of attack surface
- Minimisation of data use / secure removal

resilience / incident readiness
- Impact reduction in case of incident
- Minimise negative effect of incident on other services
- Logging
- SBOM

During operations

vulnerability and incident handling
- Publicly disclose fixed vulnerabilities (coordinated disclosure)
- Security updates: fast, free, automated, through secure distribution channel
- Regular tests and reviews

CRA – What is in Scope



Product with digital elements

Means a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately;

Intended purpose or reasonably foreseeable use

- Intended by the manufacturer, including the specific context and conditions of use, as specified in the instructions for use.
- Not necessarily the intended purpose but which is likely to result from reasonably foreseeable human behavior.

Direct or indirect

'indirect connection' means a connection to a device or network, which does not take place directly but rather as part of a larger system that is directly connectable to such device or network

Logical or physical

'logical connection' means a virtual representation of a data connection implemented through a software interface;.

Article 2:

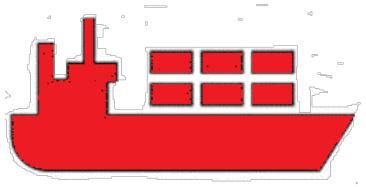
"This Regulation applies to products with digital elements made available on the market, the intended purpose or reasonably foreseeable use of which includes a direct or indirect logical or physical data connection to a device or network"

CRA – Out of Scope

2017/745 Medical devices
2017/746 In-vitro diagnostic medical

2018/1139
Civil aviation

2019/2144
Motor vehicles

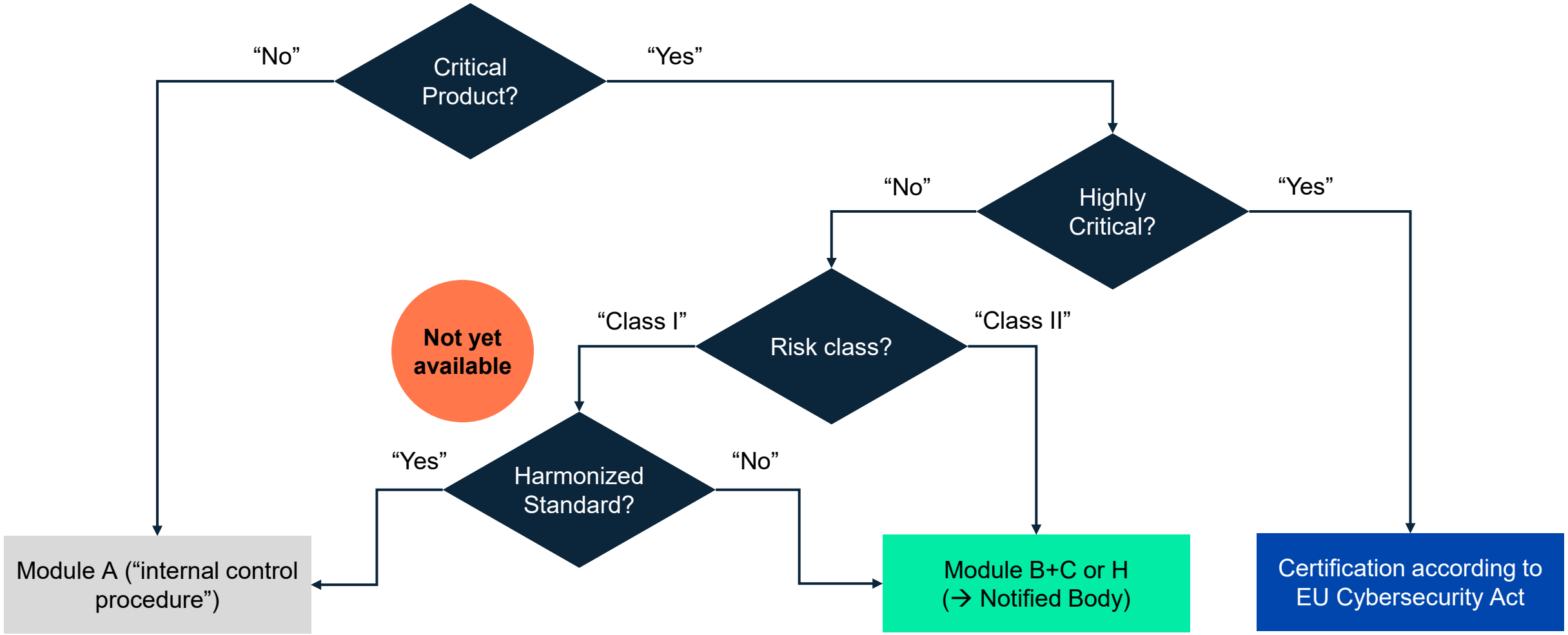


2014/90/EU
Marine equipment

Exclusively for national security or defense

Software-as-a-Service (SaaS),
(except in scope : remote data processing solutions relating to a product with digital elements)

Conformity Assessment Procedures

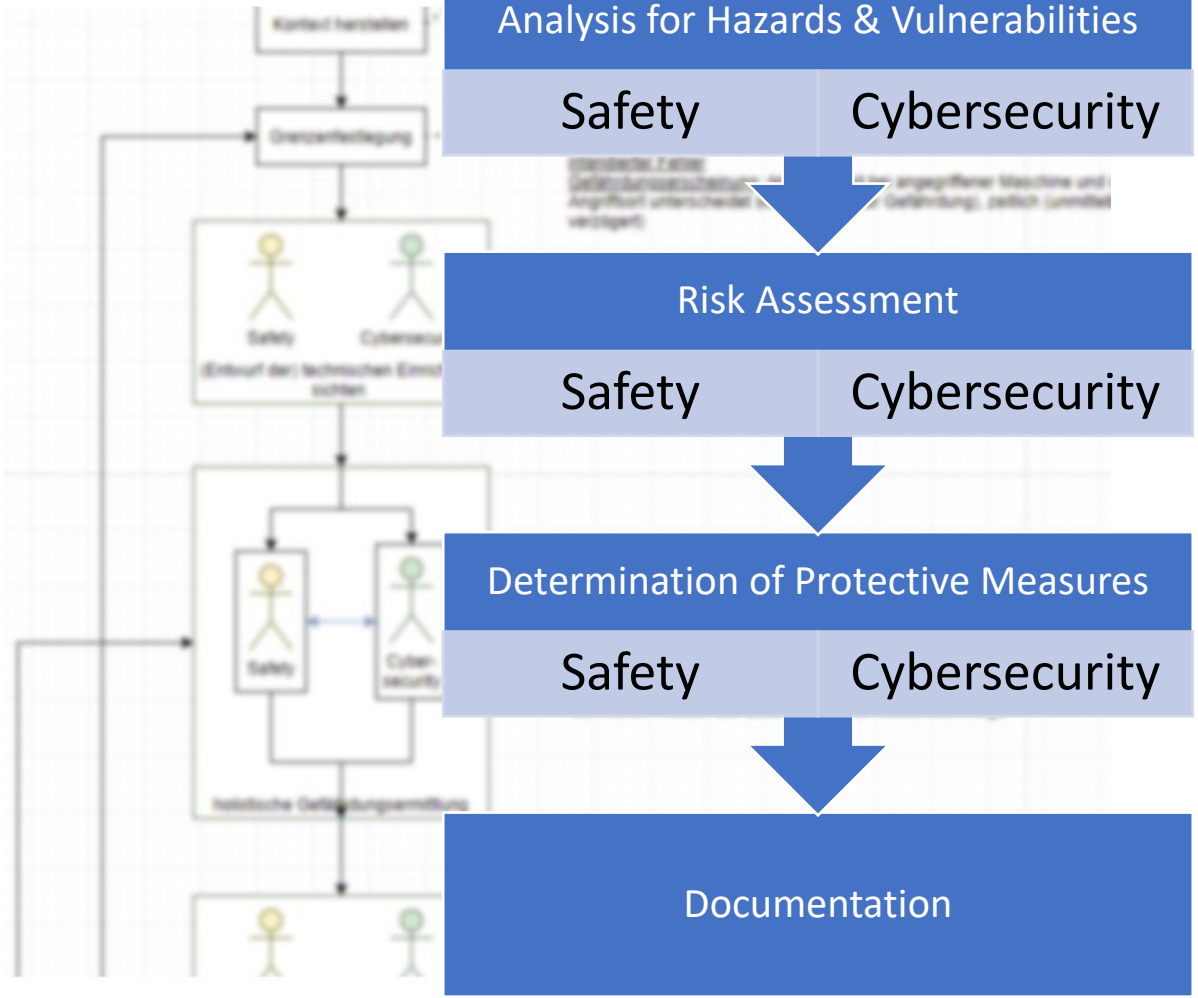


Digital Transformation - CyberSecurity Regulation

ECCO
European Cybersecurity COmmunity

01	CyberSecurity – Part of EU Legislative Framework
02	CRA & NIS 2 – Rule it All ?
03	**Testing, Inspection, Certification – In Real World**
04	Static is not Enough - Digital Twin for Dynamic & Virtual Operation

Basic Principles of Testing Inspection Certification



Analysis for Hazards & Vulnerabilities

Safety | Cybersecurity

Risk Assessment

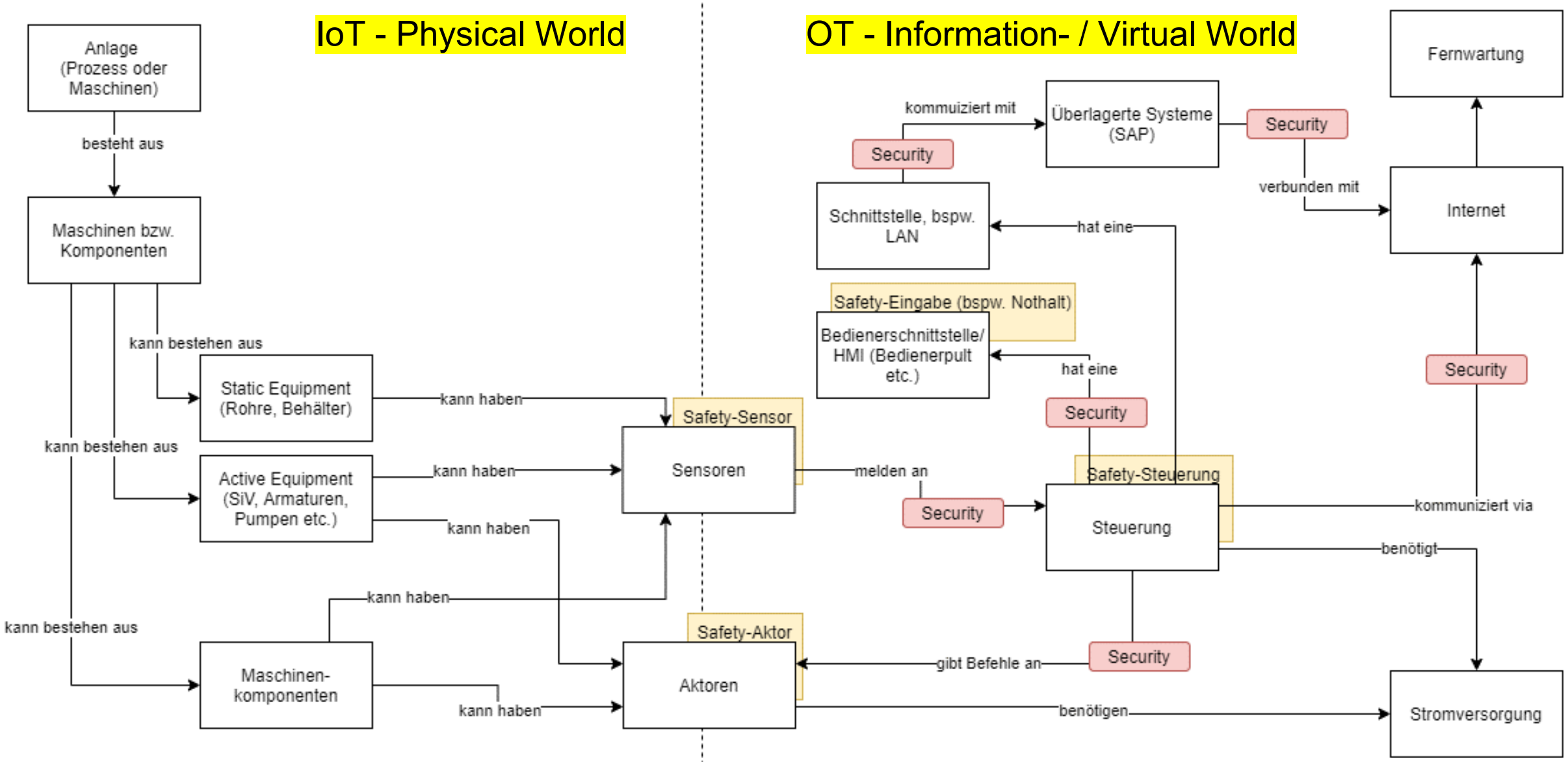
Safety | Cybersecurity

Determination of Protective Measures

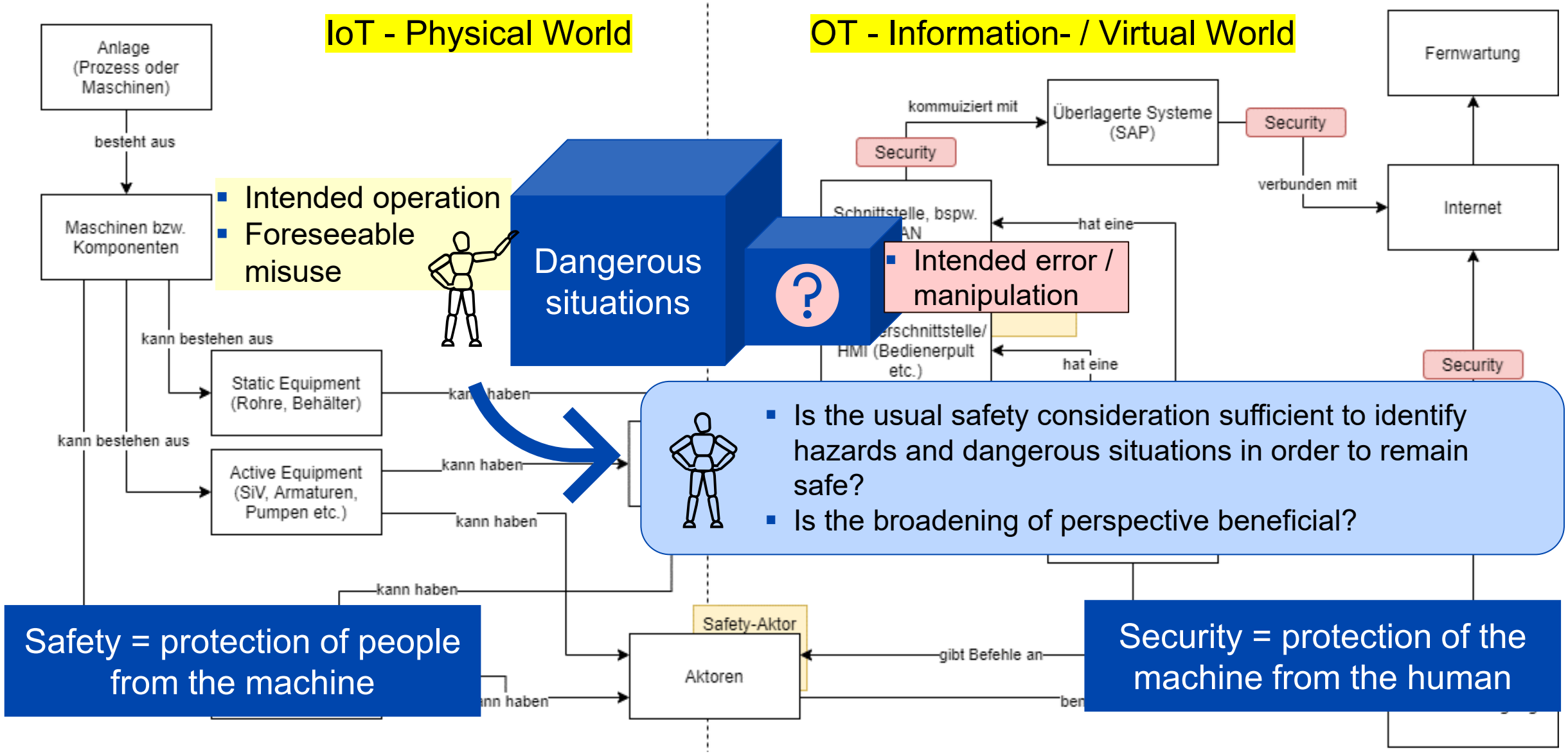
Safety | Cybersecurity

Documentation

Enhanced Risk Assessment – Cross Application Principles



Enhanced Risk Assessment – Cross Application Principles



Digital Transformation - CyberSecurity Regulation

ECCO
European Cybersecurity COmmunity

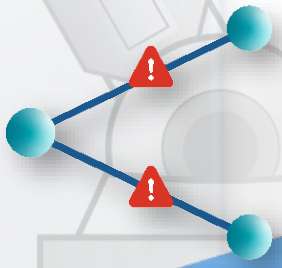
01	CyberSecurity – Part of EU Legislative Framework
02	CRA & NIS 2 – Rule it All ?
03	Testing, Inspection, Certification – In Real World
04	Static is not Enough - Digital Twin for Dynamic & Virtual Operation

Transition towards Advanced Manufacturing

Dedicated

Stand-alone component / machinery / process plant or system

Today

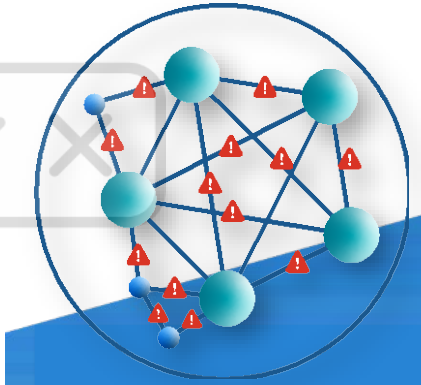


Connected

Convergence physical and digital world IT + OT

Example:
Industrial mobile robots
Modular process systems

- Interoperability
- Cyber-Security
- SW Testing



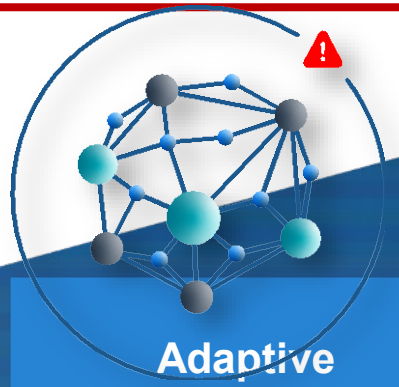
Modular & Flexible

Flexible configurations by digital twin implementation.

Processes and planning largely manual

Example:
Asset substitution @ runtime

- SW Validation & Quality
- Security & AI @ Safety
- Digital Twin @ Asset



Adaptive

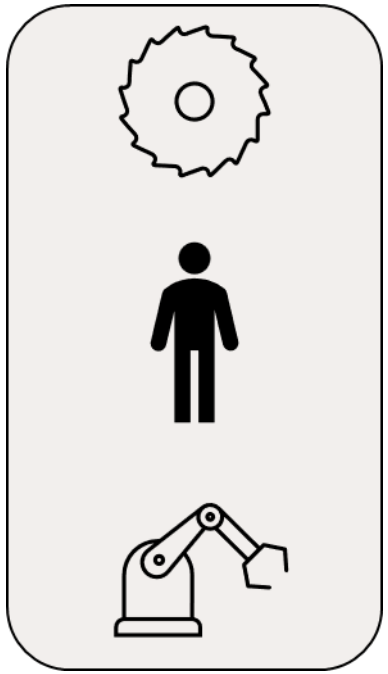
Adaptive and autonomous operating systems.

Ability to learn in order to optimize and stabilize

Example:
Operations continuity by safety adoptions caused on occurrences.

- SW Testing & Quality
- Security & AI @ Safety
- Digital Twin @ Asset & System
- Knowledge Dependency
- Runtime based Assessment

Why CyberSecurity matters for Dynamic Operation…



Physical

Safety & Secure @ Operation

of Connected
Components, Systems & Products …

Functional Safety
Mechanical Safety
Electrical Safety
Explosion Protection
:::

Safety / Function @ SW

Affekt

AI Tool & Systems

Affekt

Corrupt

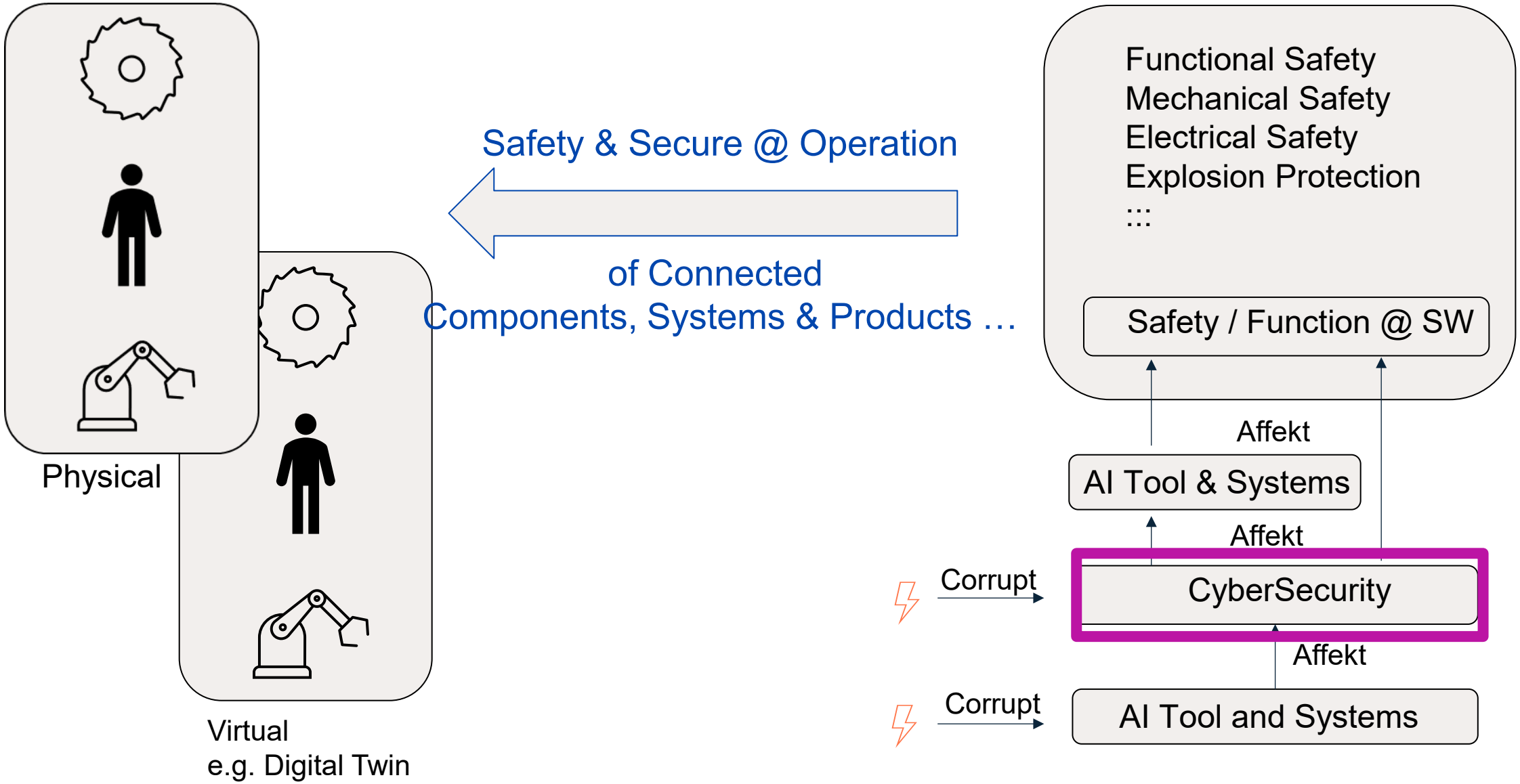
CyberSecurity

Affekt

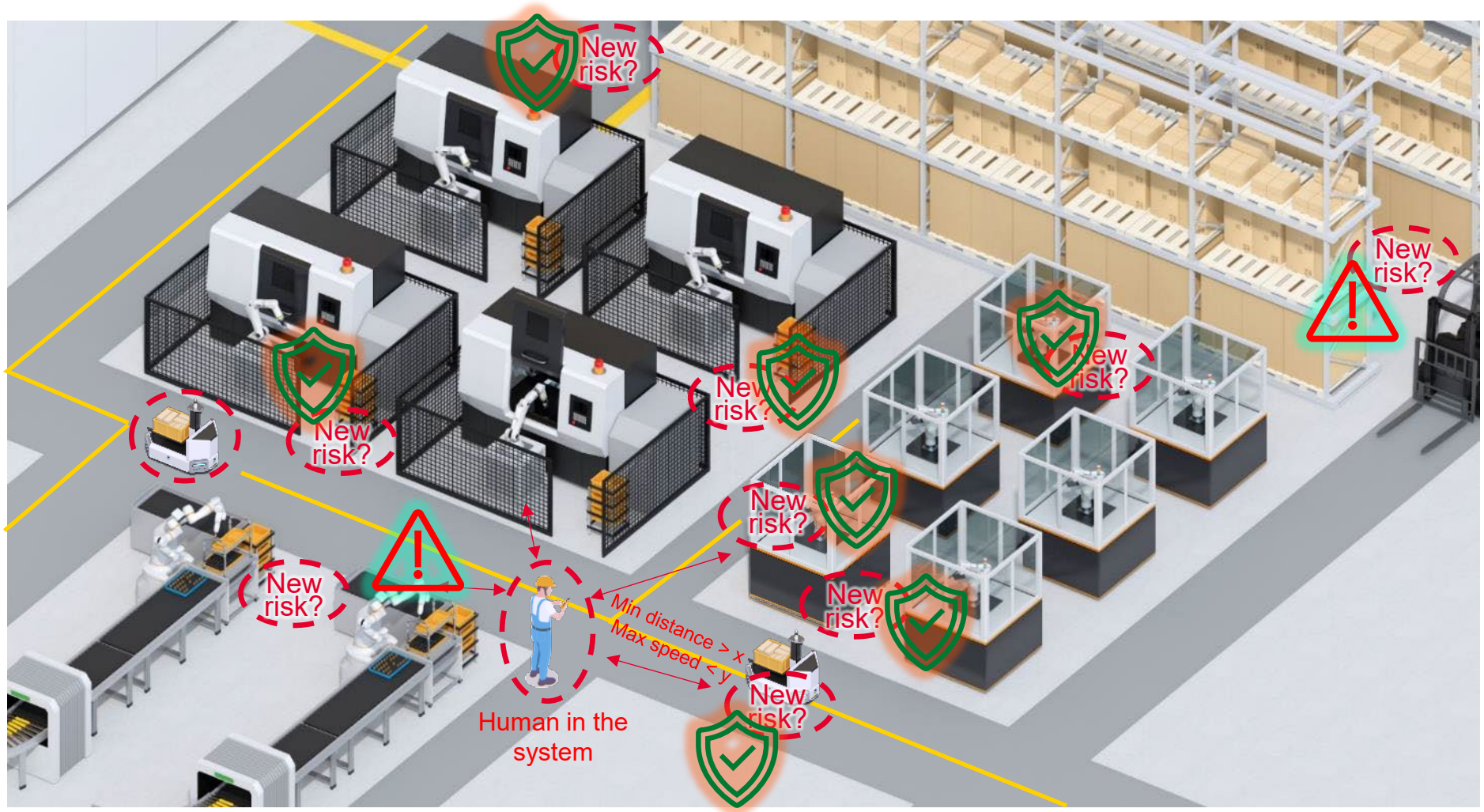
Corrupt

AI Tool and Systems

Why CyberSecurity matters for Dynamic Operation…



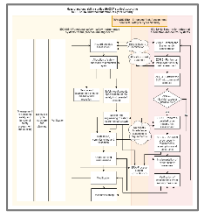
Example - Dynamic Risk Assessment



Outlook - Dynamic Certification → Assessment @ Runtime

Commissioning

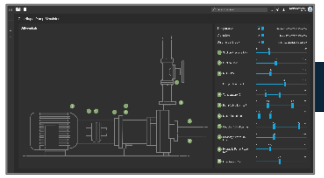
Safety Assessment

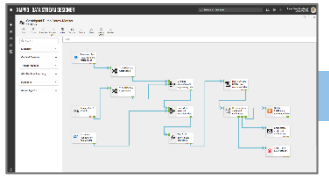


ERA (Cybersecurity)

Operation

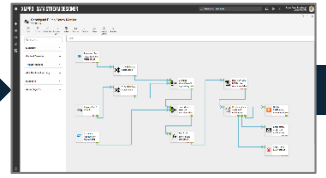
Simulator



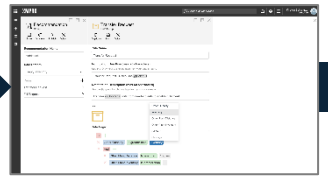


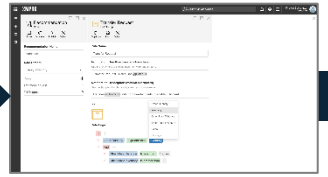
Runtime Data

Event Intelligence



Business Rules



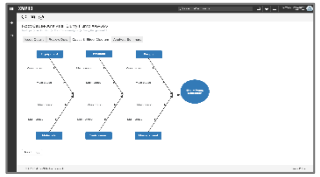


Safety Rules

Eventboard

Maintenance

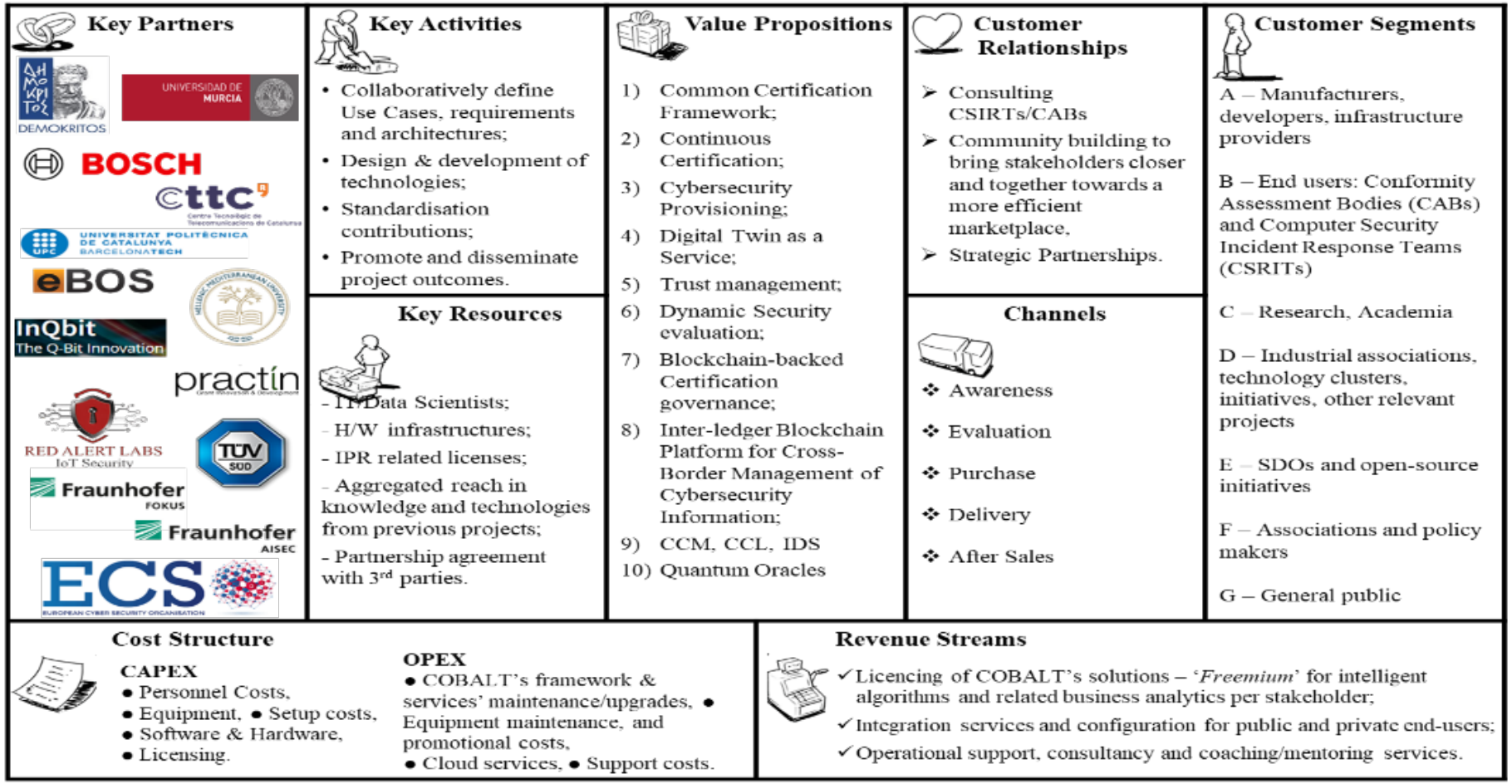
Inspection & RCA



Lifetime Assessment (AHM)

Dynamic Certification based on Digital Twin (Safety and Security Modeling)

TUV SUD is part of EU Dynamic Safety Tender „Cobalt“



TÜV SÜD: Certification scheme for dynamic cybersecurity at operation, Result Essimination towards CRA and AI-Act

Purpose: Dynamic CyberSecurity Certification Scheme for I40 Operation

Frank L. Blaimberger

VP – Advanced Manufacturing

Focus Topics:

- Test and Certification Industrial CyberSecurity for SW and AI
- Digital Compliance and AI/ML for Advanced Manufacturing Functional Safety, OT-Security and Interoperability
- Design & Test and System Engineering of Semiconductor Products & Systems and Power Electronics

Contact

Email: frank.blaimberger@tuvsud.com
Telephone: +49.175.5050.884

Follow us on:

tuvsud.com
info@tuvsud.com