Secure Product Development Lifecycle - Equipment manufacturing's approach for regulatory compliance and competitive advantage

25.5.2022 Bruxelles

Antti Tolvanen, Sales Director, Etteplan Software & Embedded Solutions
antti.tolvanen@etteplan.com +358 45 864 3579

Etteplan
A growth company

Rapidly growing and developing engineering services company

Our customers are global machine and equipment manufacturers

We stand out by the high-level competence and service attitude

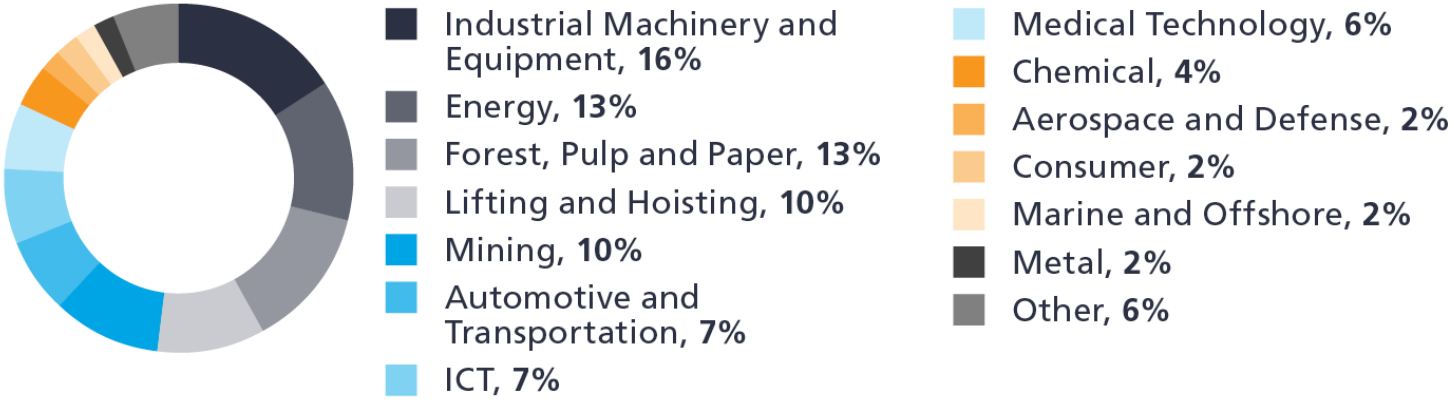
Founded 1983 | Nasdaq Helsinki Ltd

300.1
REVENUE, EUR MILLION 2021

> 3,800
INDUSTRY PROFESSIONALS

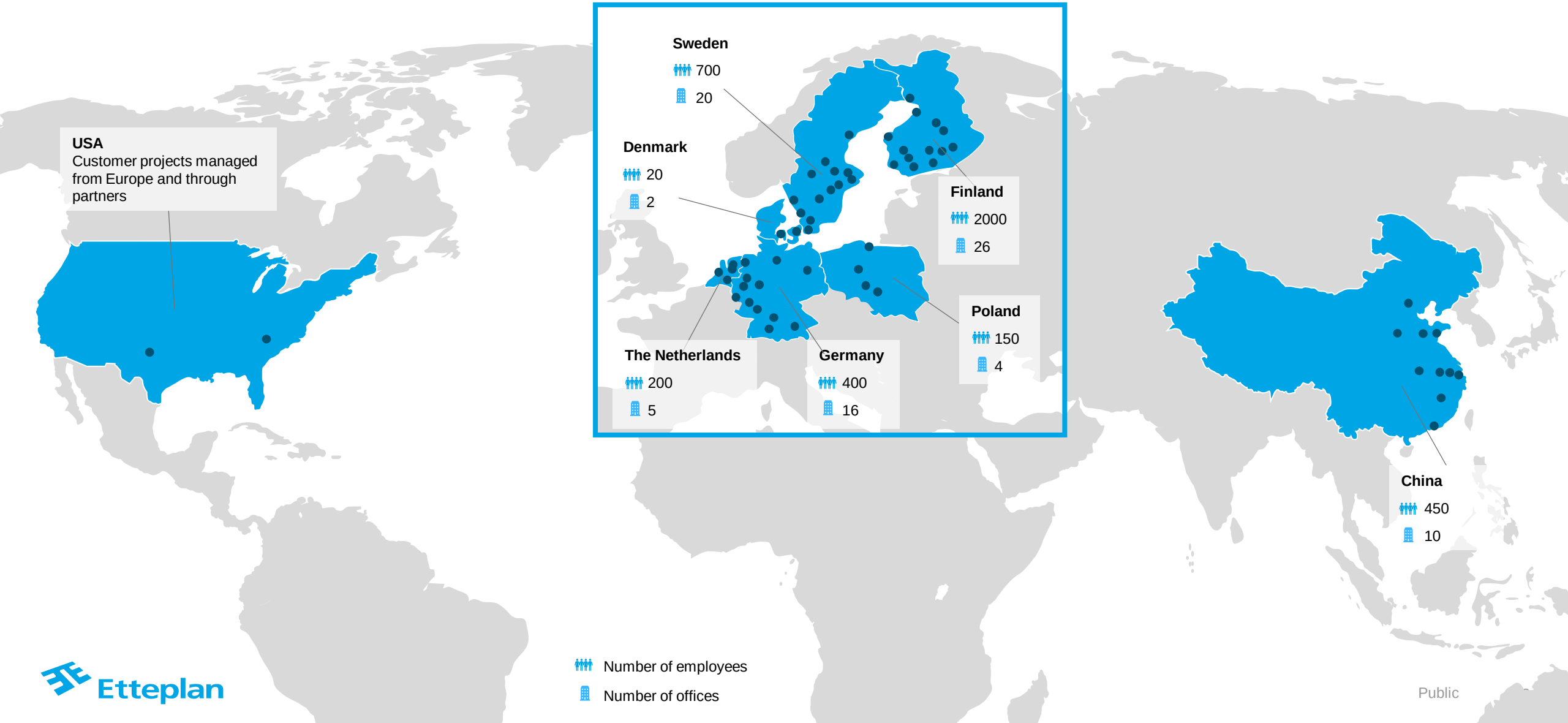
- **Software & Embedded**
- **Engineering**
- **Technical Documentation**

Revenue by customer segment 2021



Etteplan global presence

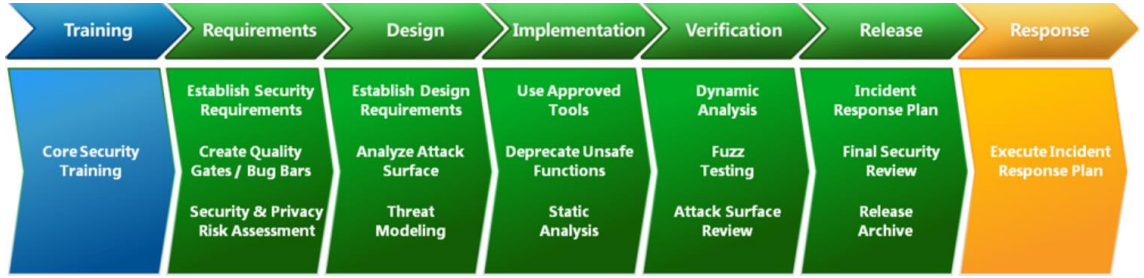
> 80 offices in Finland, Sweden, the Netherlands, Germany, Poland, Denmark, USA and China

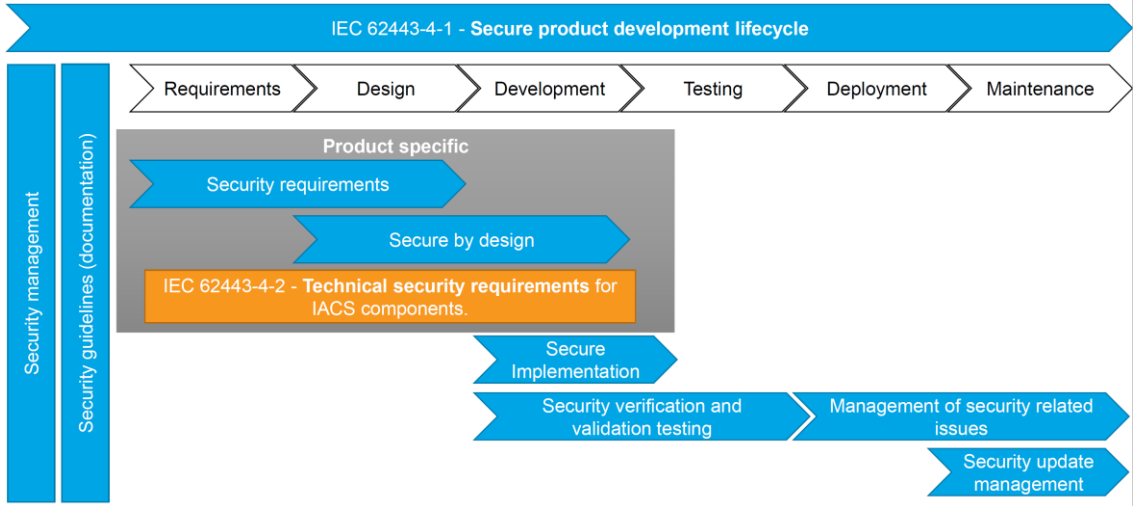


Etteplan

Etteplan started providing secure device and sw development services since beginning of 2021

- Security training
- Applicable security regulations and standards
- Threat model incl. safety and privacy risk assessment
- Security Requirements Specification
- Security Implementation Specification
  - Summarizes all documentation created over SPDL of the product
- Secure Implementation
  - RTOS, Embedded Linux, Azure…
- Security Guidelines
  - development, hardening, testing…
- Software & Hardware Bill-of-Materials
  - 3rd party SW dependencies
- Security test/verification
  - Planning – testing – reporting
- Application Lifecycle Management
- QMS / SPDL process development





https://www.microsoft.com/en-us/securityengineering/sdl
https://webstore.iec.ch/publication/33615

Agenda

From an equipment and software engineering company's perspective:

- Updates to cyber security and safety legislation
- Updates to General Terms & Conditions for Goods and Services
- Industry examples
- Conclusions and predictions

Sources

- European Parliament Legal Observatory
- Google

Cyber security becomes a regulatory requirement due to safety and privacy risks caused by connectivity, AI, autonomous robotics (and other new digital technologies)

By end of 2024, it looks like NIS2 will force companies to implement security requirements related to software

(~Member states shall adapt NIS2 into their laws 21 months after Entry into Force in EU)

Essential Entities

Energy
- Electricity
- District heating and cooling
- Oil
- Gas
- Hydrogen

Transport
- Air (commercial)
- Rail
- Water
- Road, **Smart Charging**

Banking

Financial market infra

Health
- Health care
- Pharma
- Critical medical devices

Water
- Drinking water
- Waste water

Digital infrastructure
- IEP, DNS, TLD
- cloud, data centre, content delivery, trust centre,
- public electronic communications
- **Managed Service Providers**
- **Managed Security Services Providers**

Public administration
- Central government
- NUTS levels 1-2

Space
- Ground based infra

Important Entities

Postal and courier services

Waste management

Chemicals production and distribution
- **Articles**

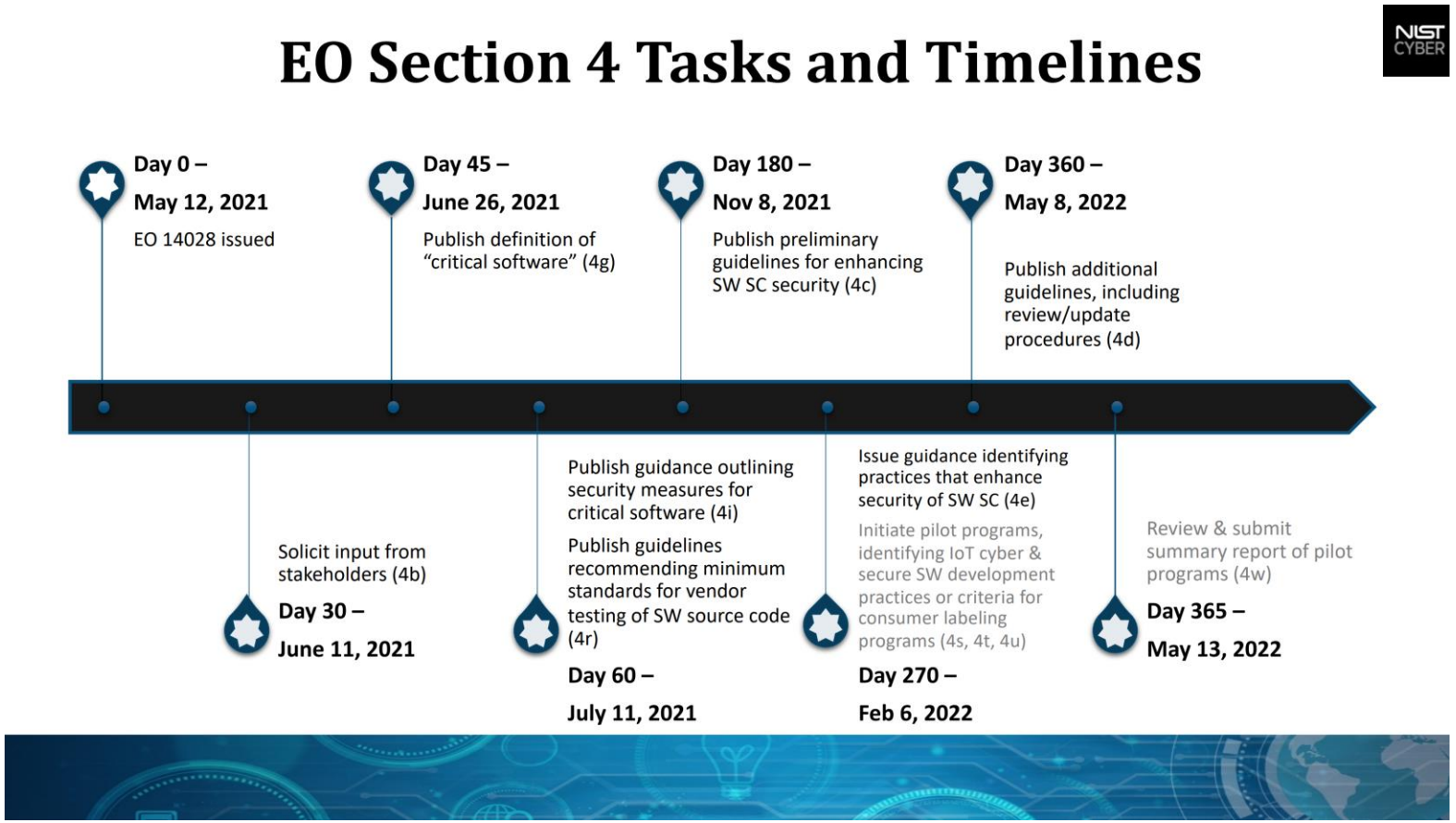
Food production, processing and distribution

Manufacturing
- Medical and IVD devices
- Computers, electronics, optics products
- Electrical equipment
- Machinery and equipment
- Motor vehicles, trailers-
- Other transportation equipment

Digital providers
- Marketplaces
- Search engines
- Social networking platforms

Article 18:
~Appropriate technical and organizational measures in network and information systems acquisition, development and maintenance

US Executive Order on Improving Nation's Security aims at Secure Development Lifecycle for everything involving SW, starting with Federal purchasing



Executive Order 14028, Improving the Nation's Cybersecurity | NIST

CE Declarations of Conformity for products and software need to be renewed

Offering	[Entry into force] Applies from (+Transitional period)	Regulation	hENs
Medical Devices & SW IVD Devices & SW	[5.5.2017] 26.5.2021/22 (+0-4 years)	Medical Device Regulation In Vitro Diagnostic Device Regulation	MDR 27.4.2024: IEC 81001-5-1 IEC 60601-4-5
Most Radio Equipment	[12.1.2022] 1.8.2024 (none)	Radio Equipment Delegated Acts	Under development
Artificial Intelligence	[H2 2022??] 2 years? (none?)	Artificial Intelligence Act	Development requested
Machinery Software ensuring safety functions	[H2 2022?] 2,5→4 years? (+1 year)	Machinery Regulation	Not yet requested (Functional Safety hENs refer to e.g. IEC 62443)
Physical Products (incl installed SW)	[H2 2022?] 0,5→1 year? (none?)	General Product Safety Regulation	Development requested, e.g. childcare products

In absence of hEN technical standards, Secure Product Development Lifecycle process is the only way in order to create design documentation as evidence

Regulation	Examples of security requirements (in original proposals)
Medical and IVD Device Regulations	For devices that incorporate software, or for software that are devices in themselves, the software shall be developed and manufactured in accordance with the state of the art, taking into account the principles of development life cycle, risk management, including information security, verification and validation.
General Product Safety Regulation	“the appropriate cybersecurity features necessary to protect the product against external influences, including malicious third parties, when such an influence might have an impact on the safety of the product” (“over the whole lifecycle” is in a latest amendment request)
RED Delegated Acts	(d) radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service; (e) radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected; (f) radio equipment supports certain features ensuring protection from fraud;
Machinery Regulation	~Connection to other devices (direct or indirect) shall not lead to hazardous situations ~Control systems shall be designed to withstand, where appropriate to circumstances and risks, malicious third parties attempting to create hazardous situations ~Safety critical hardware, software and data needs to be adequately protected against accidental & intentional corruption and collect evidence of legitimate & illegal interventions incl sw modifications

Cyber security is already a market requirement

Device and SW Manufacturers (and their suppliers), without Secure Product Development Lifecycle and Information Security Management System

will face disruption of their business models.

2019: EU Smart Grid Task Force recommended as EU CSA CS
ISO 27001 + IEC 62443

Smart grids task force

PAGE CONTENTS

Steering committee meetings

Expert group 1 – Smart grid standards

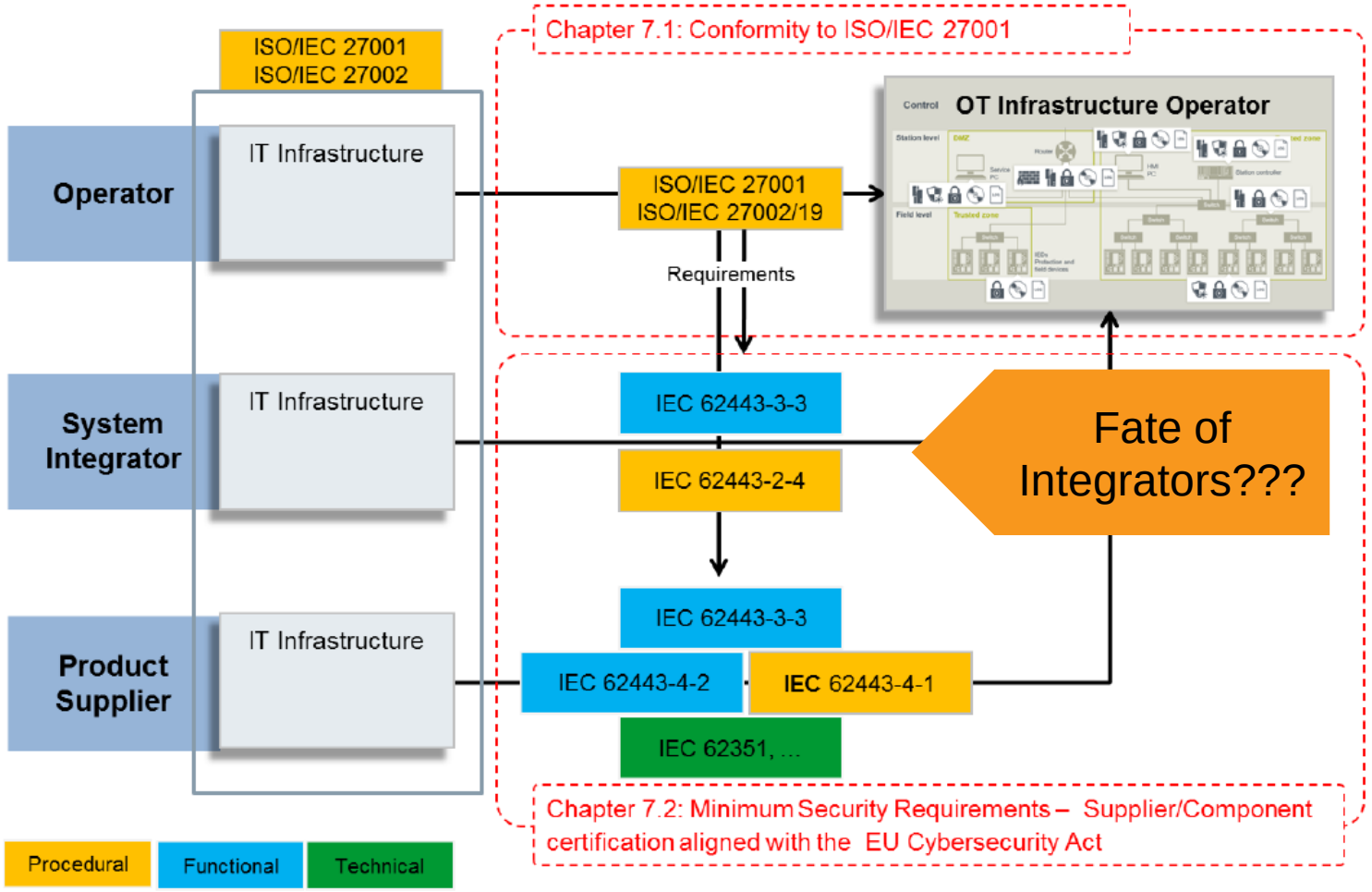
Expert group 2 – Regulatory recommendations for privacy, data protection and cyber-security in the smart grid environment

The Smart grids task force was set up in 2009 to advise on issues related to smart grid deployment and development. It consists of five expert groups which focus on specific areas. Their work shape EU smart grid policies and the policy framework.

Steering committee meetings

The minutes, presentations, and agendas of the Task Force's steering committee meetings.

Assurance	EU Cyber Security Act Security Level	IEC 62443 Security Level
Basic	Known basic risks for cyber incidents and cyber attacks	1-2
Substantial	Known cyber risks, cyber incidents and cyber attacks carried out by actors with limited skills and resources	2
High	Risk of state-of-the-art cyber attacks carried out by actors with significant skills and resources	3-4



https://ec.Europa.eu/energy/sites/ener/files/sgtf_eg2_report_final_report_2019.pdf

Cyber security is already a mandatory requirement in many global companies public GTCs for purchase of goods and services (source: google)

	~Secure Product Development Lifecycle	~Information Security Management System	Year
STORA ENSO	Applicable safety legislation	IT systems are secured; access control	2022
VALMET	Applicable laws&regulations, Industry security standards	ISO 27001,-2,-36,-701	2021
MAERSK	ISO 27001 + explicit SPDL requirements	Complete ISMS ISO 27001 meeting all requirements	2021
SIEMENS	IEC 62443 or ISO 27001	IEC 62443 or ISO 27001	2021
NELES	SPDL required for product development	ISMS controls required for organization	2021
METSO-OUTOTEC	EU Machinery Regulation		2020
GE HEALTHCARE	Explicit SPDL and tech requirements	Explicit ISO 27001 requirements	2020
SANDVIK	No malware, vulnerability disclosure		2020
JOHN DEERE	Liability of unforeseen safety hazards	Information Security Requirements	2020
HUSQVARNA	Comply with relevant laws, standards, regulations	ISMS covering all areas in ISO 27001	2020
FORTUM	Prevent alteration, improper access and malware		2020
WÄRTSILÄ	No malware, patching, vulnerability disclosure&mitigation		2019
SIGNIFY	Applicable safety laws, incl EU General Product Safety	Technical, organizational and physical sec. measures	2019
NOKIA	SPDL for high hardening and robustness		2019
KONE	Secure Development Lifecycle for digital solutions***		2018
ABB	Explicit SPDL and tech requirements		2017

GTC’s have or will be updated with cyber security requirements, like for privacy back in 2018

Industry examples

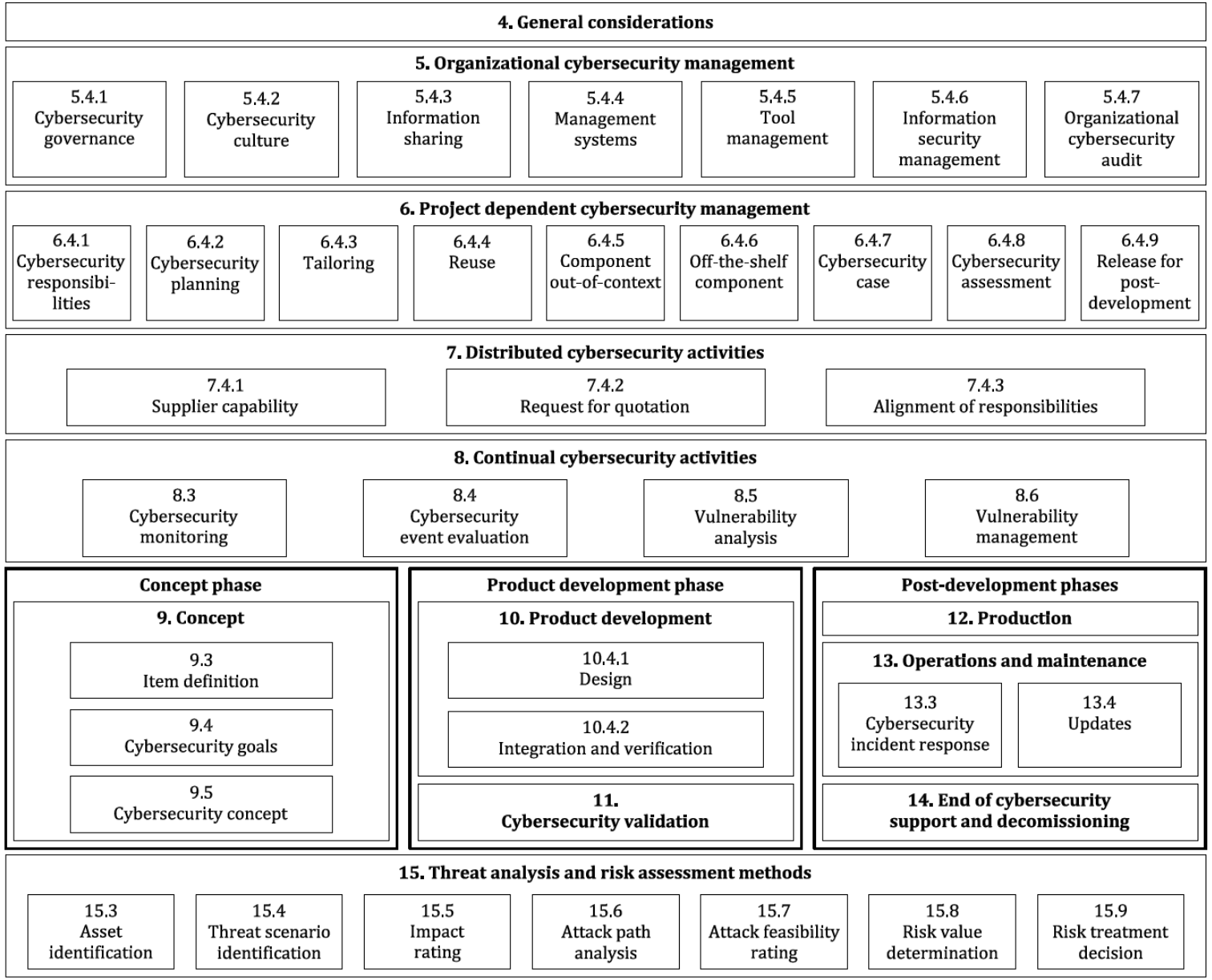
ISO/SAE 21434 Cybersecurity Engineering – Road Vehicles

Full scale cyber security management system (CSMS)

Requirements have rolled down the supply chains to Tier 1-3 during Q4/21-Q1/22

https://www.iso.org/standard/70918.html

Etteplan



Medical Devices
Secure Product Development Lifecycle is mandatory

EU

- Notified Bodies have already learned how to inspect cyber security design documentation
- Harmonised Security Standards (62443-4-based) expected 27.5.2024 for medical devices
  - Schedule for In Vitro Diagnostic Devices security hENs is not yet known

USA - FDA draft pre-market guidance 2022:

- Cybersecurity risks that are introduced by threats directly to the medical device or to the larger medical device system can be reasonably controlled through using a Secure Product Development Framework
- ANSI/ISA 62443-4-1 and UL 2900-2-1 are among FDA recognized standards for SPDF
- Effective guidance is from 2014…

USA – FDA response to NIST related to Executive Order 2021:

- Explicit, refutable Threat model
- List of clinically relevant Operational Technology cyber security risks
- Design requirements specification (=technical security requirements)
- Penetration testing plan and report, aligned with threat model
  - “testing to failure” principle to understand limits of intrusion tolerance and graceful failure
- Software Bill of Materials, including software & firmware and components,
- Instructions for installation and use that take security in consideration

https://ec.europa.eu/health/system/files/2022-01/md_cybersecurity_en.pdf
https://www.fda.gov/media/149954/download

Kaiser Permanente GTC – Edge Security Requirements

Some highlights:

- Compliance with FDA + much more
- No IoT-based business models
- SPDL mandatory
- Supplier liable for all residual risk if all KP edge requirements are not met

1. **General Compliance**
   1.1. **Compliance with FDA Guidance**. For all medical Devices, at a minimum the Supplier:
      1.1.1. Shall comply with all required and recommended practices set forth in the FDA Content of Premarket Submissions for Management of Cybersecurity in Medical Devices.
      1.1.2. Shall comply with required and recommended practices set forth in the FDA Post market Management of Cybersecurity in Medical Devices.
      1.1.3. Shall comply with cybersecurity industry-standard guidelines, requirements, and standards of any applicable regulatory body.

2. **Supplier Transparency**
   2.1. **Industry Standard Data Request.** Supplier shall provide a complete Manufacturer Disclosure Statement for Medical Device Security (MDS2) and a complete Software Bill of Material (SBOM) that outlines at a minimum: (i) All Open Source Software (OSS), (ii) as-built version of all OSS, (iii) all default user accounts, (iv) required KP Network ports and services for intended use of product, and (v) all folders and directories, including those that are hidden, relevant to the intended use of the product, (vi) software applications and versions required to perform intended use of products, such as Java or SQL.

   2.6. **Disclose Remote Access**. Supplier shall disclose to KP all accounts on Products for the remote use, maintenance, or administration of the Product . All accounts not required for KP use, maintenance, or administration of the Product shall be removed before Product delivery or during installation.

3. **Secure Product Design Process**
   3.1. **Security Development Lifecycle.** Supplier shall represent and warrant that it performed Security Assessments of potential Device security vulnerabilities, threats, and risks as part of Device manufacturing; and either remediates the Vulnerabilities or provides recommendations for risk mitigation.

https://supplier.kp.org/requirements-guidelines/privacy-security-technology/edge-security-requirements/

Signify globally first in lighting to certify SW life cycle process to 62443-4-1

Lighting is e.g. transportation critical infrastructure

May 7, 2020

Signify is the world's first lighting company with security certification for its connected lighting development process

Eindhoven, the Netherlands –Signify (Euronext: LIGHT), the world leader in lighting, is the first lighting company worldwide that has been awarded the security certification for its connected lighting development process (IEC62443-4-1) by DEKRA. This confirms that the company's development of connected lighting systems is based on a certified secure development process and illustrates the company's leadership in embedding security in all aspects of its innovations, products, systems, and services.

Central elements of the IEC62443-4-1 certification are a threat analysis based on the use case scenario and a product development process which ensures that all identified security requirements are implemented, verified, tested, and documented with traceability. Signify has satisfied all requirements in this process. In addition, Signify has demonstrated its ability to react fast and appropriately to newly discovered security vulnerabilities and publish security updates in a reliable manner.

International expert organization DEKRA evaluated Signify's development process on the IEC 62443-4-1 fundamental security requirements. "We are proud to award the IECEE CB and DEKRA SEAL certification to Signify. As global partner for a safe and connected world, we know that security is key in today's world. The IEC 62443 standards are the perfect tools to ensure safety and security at work, home and on the road," said Bram Holtus, Managing Director of DEKRA Certification B.V.

Signify meets all requirements set out in the standard by rigorously following its Signify Security Development Lifecycle (SDL) in all internal and external development activities. Major components of the SDL are a security risk analysis and threat modeling, code analysis verification and validation testing, and continuous vulnerability management.

"Connected lighting systems are core to our business and our future. This DEKRA certification is testament to our commitment to provide our customers with the most secure connected lighting products, systems and services. All of which are built on a strong foundation of industry standards, governance, and procedures.," said Harsh Chitale, Business Group Leader Professional at Signify. "As a growing group of businesses and governments are implementing connected technologies, maintaining the highest standards of security are both crucial and invaluable to us."

Eaton launched first product with dual UL29001-1 and IEC 62443-4 certifications

Reducing cybersecurity risk is critical. Eaton can help.

Eaton takes cybersecurity seriously. That's why we've developed a network card that has enhanced protection built-in. The Gigabit Network card is the first in the industry to meet both International Electrotechnical Commission (IEC) and Underwriters Laboratories (UL) cybersecurity requirements. The card was the first UPS network connectivity device to receive UL 2900-1 certification, which provides customers with confidence that it has been reviewed, tested and met the benchmark of this trusted brand. It is also the first to be certified to the IEC 62443-4-2 standard, which further underscores Eaton's commitment to unified global cybersecurity standards. While hardware that lives behind a firewall is thought of as fully-protected, that isn't always enough to keep hackers out.

What's the benefit to customers?

Encryption and Password management are the two key enhancements that make makes Eaton a leader in this space.

Encryption

- Uses the most current version of Transport Layer Security protocol (TLS)
- Only secure protocols enabled by default
- Firmware is signed and encrypted, and will not boot if tampered with
- Secure SMTP for email alerts

Password Management

- Requires change of password on setup
- Configurable requirements for password complexity
- Certificate based authentication in machine to machine connections – no username/password information saved on the client machine, separate certificates for each protocol

Etteplan

Source: google

Eaton General Terms and Conditions for Purchase

- Personal Data
- Information / Cyber Security Management System mandatory for suppliers
- Secure Product Development Lifecycle
  - Supplier is liable for any vulnerabilities that are exploitable and provide any kind of access to Eaton's systems for any purposes
  - →IoT denied

23. Data Security and Cybersecurity.

23.1 Supplier may receive or have access to information relating to identified or identifiable individuals ("Personal Data"), including Eaton employees, temporary workers, contractors, consultants, customers or suppliers. Personal Data, in whichever form, is of a very sensitive nature, and Supplier shall keep Personal Data strictly confidential and use it (i) only within the limits authorized by Eaton and for the purpose of Supplier's performance under the Order, and (ii) in accordance with all applicable laws, and where applicable, the Personal Data Processing Clauses available at http://www.eaton.com/content/dam/eaton/support/selling-to-eaton/files/po_terms/Personal-Data-Processing-Clauses.pdf and incorporated by reference.

23.2 Supplier shall operate and maintain an information and cybersecurity program, including administrative, physical and technical safeguards, designed to protect against and prevent any unauthorized use, access, processing, destruction, loss, alteration or disclosure of Confidential Information and Personal Data ("Security"). Upon the request of Eaton, Supplier shall provide proof of Supplier's Security and submit its processing facilities for audit of the processing activities covered by the Order. Such audit shall be carried out by Eaton or its agents with the required professional qualifications and a duty of confidentiality. Supplier shall immediately notify Eaton of any perceived, potential or actual breach to Supplier's Security ("Breach"), and provides a full description of the Breach, the impact and mitigation efforts. Supplier will then promptly (a) investigate, remediate, and mitigate the effects of the breach; and (b) provide Eaton with assurances reasonably satisfactory to Eaton that such breach will not recur. If Eaton determines that notices or other remedial measures are warranted, Supplier will, at Eaton's request and at Supplier's cost, undertake such remedial actions.

23.3 Any software provided by or on behalf of Supplier shall not contain any computer code or other mechanism that would allow Supplier or others to access information on Eaton's computers, networks or products for any purpose including viewing, transmitting or conveying such information to Supplier or any other party. If vulnerability is discovered in any software which may be exploited by others, Supplier agrees, at Supplier's cost, to immediately take all corrective actions necessary to prevent such exploitations or identify, contain, eradicate and recover Eaton's assets if an exploitation occurred.

Source: google

KONE is first company in elevator industry with IEC 62443-4-1 certification

- ISO/WD 8102-20 elevator & escalator cybersecurity standard will refer to IEC 62443:
  - Part 3-3: System security requirements and security levels
  - Part 4-1: Secure product development lifecycle requirements
  - Part 4-2: Technical security requirements for IACS components

- IEC 62443 does not cover cloud or the end-user applications, which are important parts of connected elevator systems. To secure the entire ecosystem, other standards, such as ISO 27001 are also needed.
  - KONE gained IEC 62443-4-1 certification in Summer 2021 for security critical SW components

Source: KONE, TÜV, Google

A challenge becomes an opportunity

Over the past few years, KONE has set out to address this uncertainty, turning the challenge into an opportunity to create and develop solutions that are as secure as they can be. As Katara proudly points out, KONE now boasts IEC 62443-4-1 certification, which confirms improved cybersecurity processes and industry-wide best practices.

"It helps us to build our systems in a way that ensures security by default," says Katara. "It gives us the framework to develop them so that they are as secure as possible, right down to contemplating the target profile of the potential attacker."

This, he explains, is important. Not every project needs top-tier cybersecurity built into it – especially when there is a cost involved. There's a difference between the level you might need in a small, three-story residential development and, say, an airport.

"We also need to have an incident response process so that if there is a cybersecurity problem, then we have a system in place to deal with it," says Katara. "This standard also helps with that."

Maersk

All requirements in 27001 need to be met by supplier ISMS, incl Secure Development and external auditing/certification

CE.01 If Maersk Data is in scope of this Service, the Supplier must have a documented 'Information Security Management System' (ISMS). The ISMS should cover all the requirements of an international Cyber Security standard (such as ISO27001, NIST etc) and be proven to be operating effectively through periodic internal and/or external audits by independent and qualified practitioners.

CE.02 As part of the Services, Supplier must align and maintain cyber security practices to a recognized cyber security standard (such as ISO27001, NIST, etc.) and maintain and annually submit to Maersk at thirdpartyassurance@maersk.com any cyber security certifications that are applicable to the Services, including the following reports: ISAE 3402, type II and ISAE 3000 or equivalent reports. Should any certification lapse, fail to be maintained/renewed or degraded during the certification period, Maersk Cyber Security Third Party Assurance team must be notified immediately at "thirdpartyassurance@maersk.com" together with information on when the security levels will be resumed, or an alternative cyber security solution that meets or exceeds the contractual requirements will be established. Failure to maintain security standards and/or certifications will be considered a material breach of the Agreement. If Supplier is unable to provide relevant certification of its facilities, systems and business units against an established cyber security standard (e.g. ISO27001, etc.) conducted by an independent third party, the Supplier must at its expense without undue delay and no later than 30 days upon its receipt, complete and return a cyber security self-assessment provided by Maersk.

https://vendorterms.maersk.com/cybersecurity

Etteplan

Conclusions and predictions

Minimum security capabilities for staying competitive in industrial products/sw and services

Secure Product Development Lifecycle process in QMS
(IEC 62443-4-1, MS SDL, OWASP, others)

Certified ISO 27001 ISMS

Future predictions

- **Neglecting cyber security –related market change is a strategic mistake**
  - Inability to place products and software on the market, or put them into use at customers
  - Inability to provide products and services, involving software or confidential data, to Essential and Important Entities
  - The market changes right now

- **IoT / Data based digital services will experience reduced profitability**
  - Much tighter security requirements from customers and regulators will increase development lifecycle costs for both software and devices, and cost increases impact also the supply chain
    - Upside of security cost increases is reduced risk of cyber security incidents and associated administrative fines
  - EU Data Act could make all data, generated by the use of products and services, freely available to the users and their third parties, thus challenging the whole business model

- **No EU CSA Certification schemes needed for products/software/services involving safety risks (=OT)?**
  - New Legislative Framework regulates safety and consequently also security in EU, via hENs or Notified Bodies, and perhaps including 3rd party security assessments/certifications?