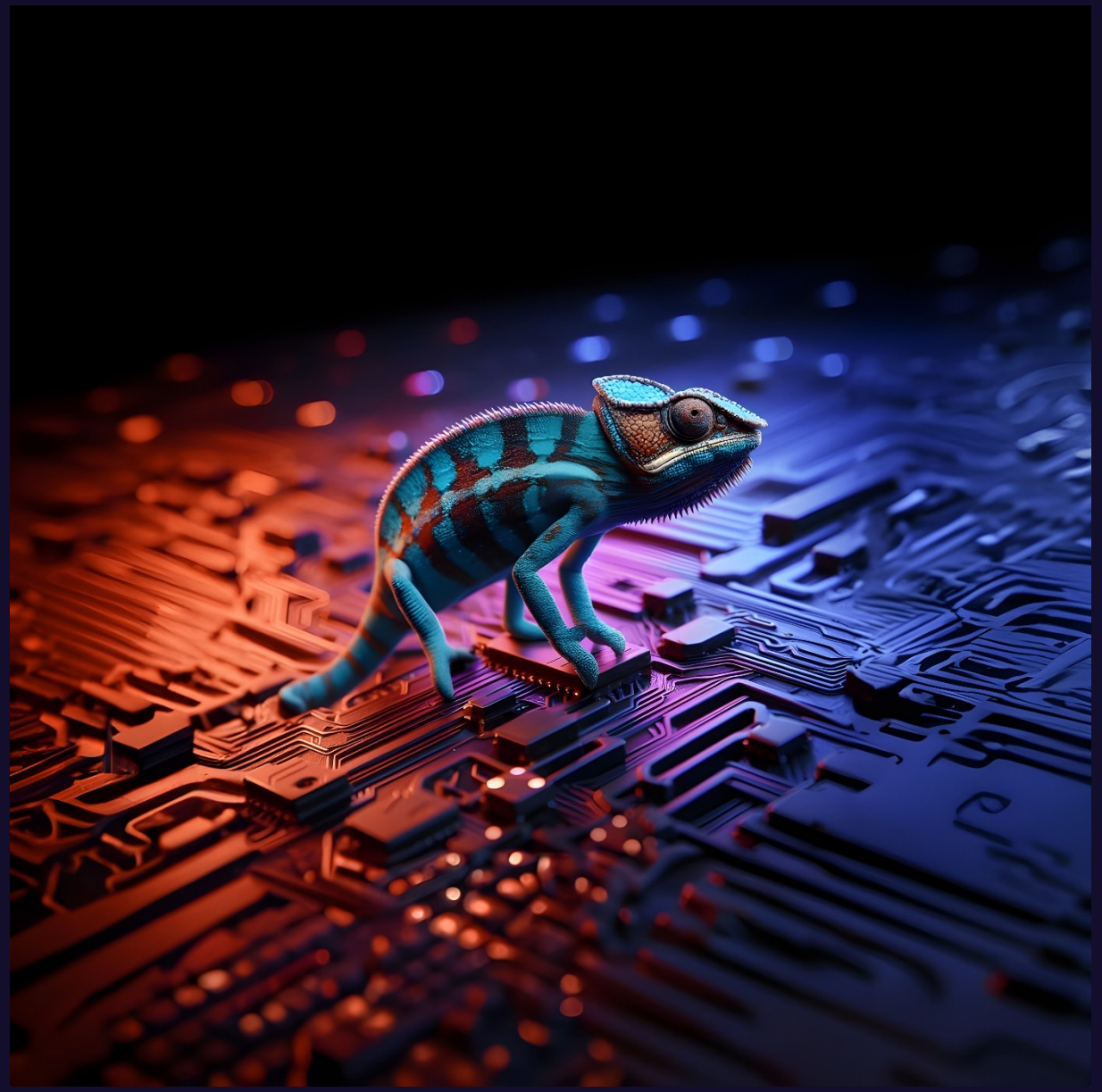
New regulations affecting embedded devices



Thursday Sept 26th 2024 15 EET

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

Most of today's hardware and software products with data interfaces will become illegal to place on EU market over a period of 3 years from now

FORBES > LIFESTYLE > CARS & BIKES

EU Cybersecurity Laws Kill Porsche's 718 Boxster And Cayman Early

Michael Harley Contributor ⓘ

Michael Harley is an author and a noted automotive industry expert.

Follow

Mar 28, 2024, 02:03am EDT

2023 Porsche 718 Cayman GT4 RS is unaffected by the EU legislation ©2024 PORSCHE CARS NORTH AMERICA

Cybersecurity laws in Europe are delivering an abrupt end to Porsche's popular Macan combustion-powered compact SUV, and now it appears that the same legislation is dooming the combustion-powered 718 Boxster convertible and the 718 Cayman coupe before their EV replacements are in showrooms. All three models are lost due to UN Regulation No. 155 (UN R155), which requires automakers to embed specific cybersecurity protections within the high-volume vehicles it sells —the European legislation takes effect on July 1, 2024.

Distributing software and connected products legally on EU market require creation of secure-by-design products and secure development lifecycle processes

Conformity of a product is examined separately for each individual unit that has been manufactured

Not per product model, type, batch, series, version, variant etc.!

EU Blue Guide

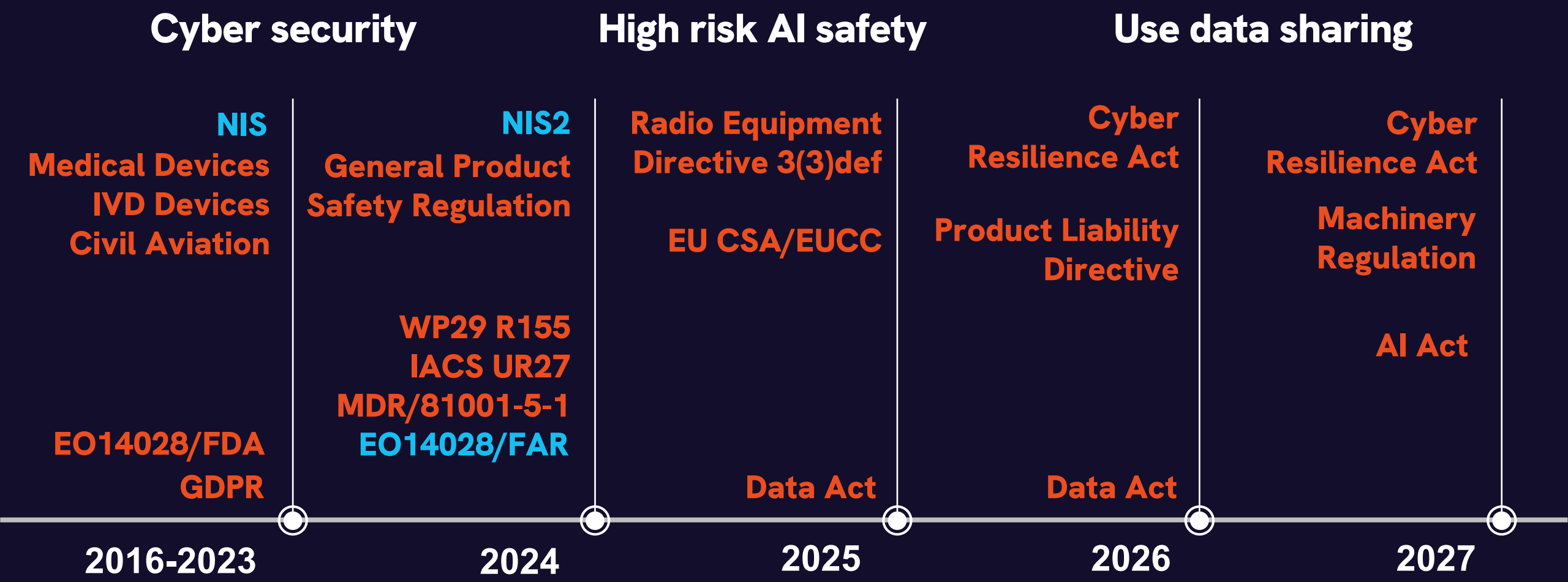
- A product is **placed on the market** when it is made available for the first time on the Union market, after the product has been manufactured and CE marked.
  Even though a product model or type has been supplied before new Union harmonisation legislation laying down new mandatory requirements entered into force, **individual units** of the same model or type, which are placed on the market after the new requirements have become applicable, must comply with these new requirements.
- A product is **made available on the market** when supplied for distribution, consumption or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge.
- **Putting into service** takes place at the moment of first use of an individual product within the Union by the end user for the purposes for which it was intended.

Radio Equipment Directive

- Article 10.1. When **placing** their radio equipment **on the market**, manufacturers shall ensure that it has been designed and manufactured in accordance with the **essential requirements set out in Article 3**.
  - Article 17.4 ~If hEN standards for Essential Requirements have not been published in OJ, a Notified Body is must be involved for EU-type examination (Annex III) or QMS (and tech docs) assessment (Annex IV)
- Article 6. Member States shall take appropriate measures to ensure that radio equipment is **made available on the market** only if it complies with this Directive.
- Article 7. Member States shall allow the **putting into service and use** of radio equipment if it complies with this Directive when it is properly installed, maintained and used for its intended purpose.

New regulations on Entities and Products start applying

Secure-by-design becomes mandatory for products and operational systems



Radio Equipment Directive 3(3)d applies on products that have a radio interface and internet connectivity

Some exceptions, e.g. MDR, IVDR, road tolling, civil aviation, national security radio equipment are out of scope.

Scope of applicable requirements depend on e.g. use environment

EN 18031-series will be reused in hEN standards for
- Cyber Resilience Act article 13
- perhaps in some way also Machinery Regulation 1.1.9 and 1.2.1?

Cyber Resilience Act - essential requirements

Properties of products with digital elements (Article 13 + Annex I.I)

"Risk based approach"

- Cyber security risk assessment covering whole product lifecycle
- Risk assessment describes processes used by manufacturer
- Requirements specification with justifications
- Due diligence related to 3rd party components

Support period (expected life time / min 5 years)

- Product made available without known exploitable vulnerabilities
- Keep processes for mass-manufactured products in conformance over whole support period
- Risk assessment maintained over support period

"Security Mechanisms" (Annex I.I)

- Product designed, developed and produced for appropriate level of cyber security based on risks
- Secure-by-default configuration
- Security update mechanism
- Access control and authentication mechanisms
- Secure storage, communication and integrity protection mechanisms
- Resilience and traffic control mechanisms
- Incident impact reduction via exploitation mitigation mechanisms
- Logging mechanism with opt-out mechanism for user
- Personal data minimization
- Data deletion mechanism
- Limit attack surfaces

Reporting obligations (Article 14 applies already OJ +21 months)

- Reporting of actively exploited vulnerability to CSIRT in 24/72 hours and final report in 14 days
- Reporting of severe incidents also to ENISA
- Information and instructions to impacted users
- Reporting to component supplier and sharing of fixes

Vulnerability handling requirements (Article 13 + Annex I.II)

Effective & regular security testing and reviews

- Vulnerability assessments
- Software bill-of-materials in machine-readable format

Coordinated vulnerability disclosure policy

- Single point of contact for receiving and disclosing info on vulnerabilities
- Public disclosure of vulnerability fixes in patches along with guidance for users
- Measures for sharing vulnerability information on product and 3rd party components

"Update management"

- Secure update distribution mechanism
- In relation risks, address vulnerabilities without delay
- Security updates separately from functionality updates where feasible
- Free-of-charge security updates, unless otherwise agreed in relation with tailor-made products with digital elements

Information and instructions to users (Article 13 + Annex II)

"Security specs"

- Unique identification of product
- Intended purpose, security environment provided by manufacturer, essential functionalities, and security properties
- Known or foreseeable circumstances related to intended use or reasonably foreseeable misuse of product that may lead to significant cybersecurity risks
- Technical security support offered by manufacturer and end-date for the support period related to vulnerability handling and security updates

"Security guidelines"

- Instructions for secure commissioning and use, how changes to product can affect security of data, installation of security updates, secure decommissioning, how to turn automatic security updates off
- Instructions for securely integrating the product to other products, if product is intended for integration.

"Contact info"

- Internet address for accessing EU declaration of conformity
- Contact information for reporting and receiving info about vulnerabilities
- Address to SBOM, if SBOM is disclosed by manufacturer

CRA draft standardization request

15 horizontal standards for essential requirements
22 vertical standards for Annex III products

Designing, developing, producing
- minimisation of personal and other data
- appropriate level of cyber security vs risks
- limitation of attack surfaces
- incident impact reduction mechanisms

Making available
- without known exploitable vulnerabilities
- with secure-by-default configuration

“Use”
- protection from / reporting of unauthorized access
- protecting confidentiality of data
- protecting integrity of data, commands, programs, configuration

“Detect”
- security information via internal activity monitoring with opt-out for user

“Resilience”
- protecting availability of essential and basic functions
- minimizing negative impact on other services & devices

“Vulnerability management”
- vulnerability handling process
- ensuring vulnerabilities addressability through security updates

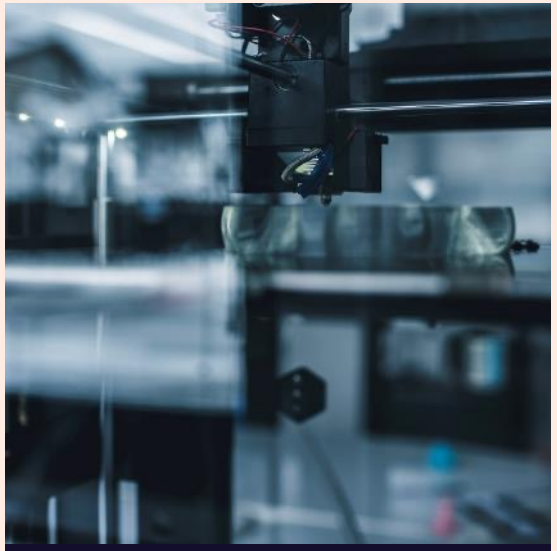
“Data processing”
- Removal or transfer of data and settings

Vertical standards
- hEN standard for each product listed in Annex III

Etteplan

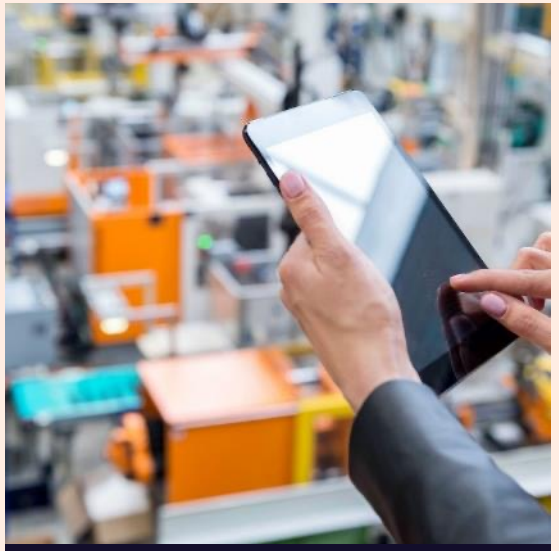
SOFTWARE & EMBEDDED SOLUTIONS

BRING INTELLIGENCE TO MACHINES AND BUSINESS PROCESSES



ENGINEERING SOLUTIONS

SUPPORT CUSTOMER'S PRODUCT DEVELOPMENT AND MACHINE MANUFACTURING



TECHNICAL COMMUNICATION SOLUTIONS

IMPROVE THE EFFICIENCY OF THE SERVICE BUSINESS OF EQUIPMENT MANUFACTURERS

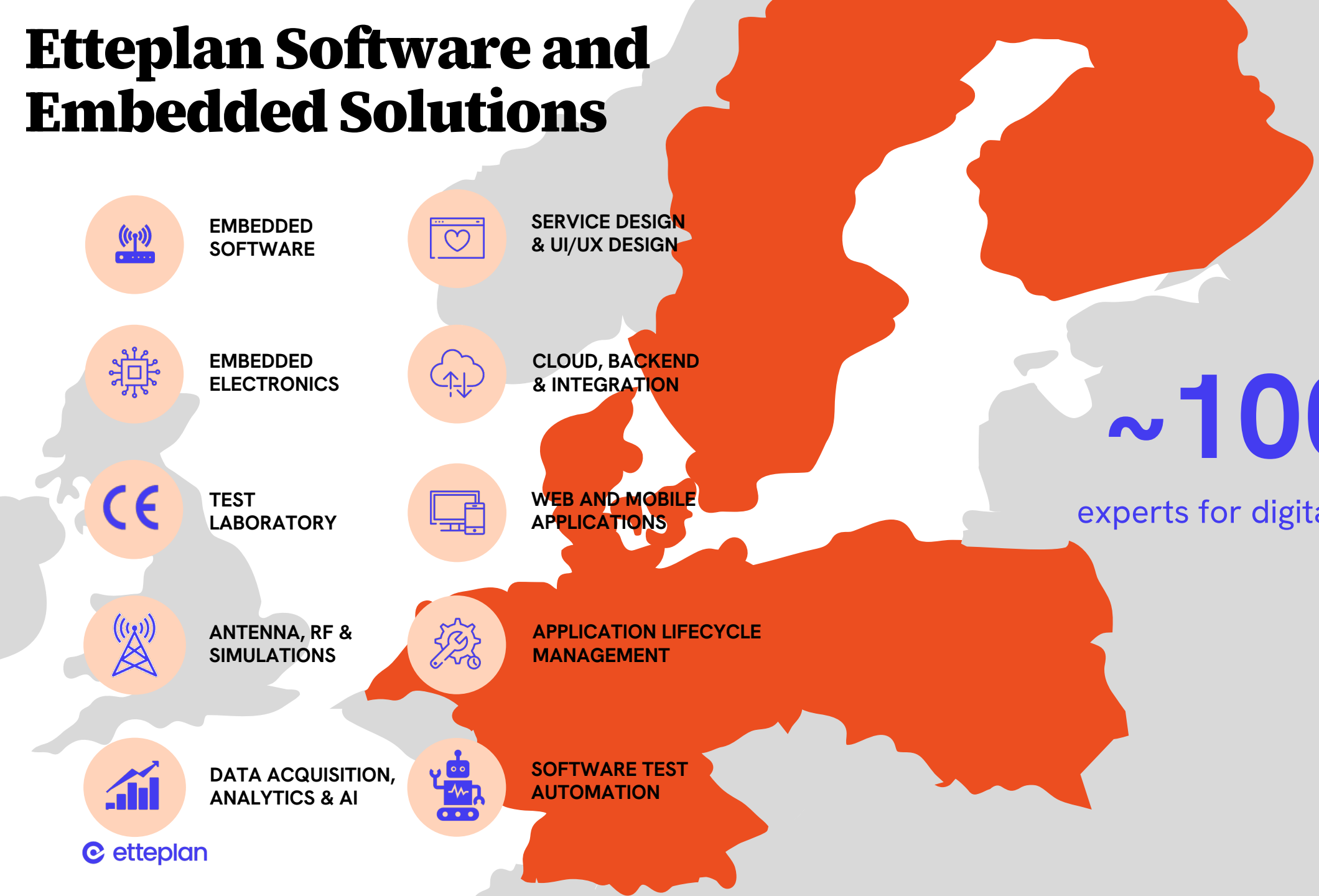
~4,000

INDUSTRY PROFESSIONALS

360

REVENUE, EUR MILLION 2023

Etteplan Software and Embedded Solutions



- EMBEDDED SOFTWARE
- EMBEDDED ELECTRONICS
- TEST LABORATORY
- ANTENNA, RF & SIMULATIONS
- DATA ACQUISITION, ANALYTICS & AI
- SERVICE DESIGN & UI/UX DESIGN
- CLOUD, BACKEND & INTEGRATION
- WEB AND MOBILE APPLICATIONS
- APPLICATION LIFECYCLE MANAGEMENT
- SOFTWARE TEST AUTOMATION

~1000

experts for digitalization

etteplan

ETTEPLAN'S VISION

We create solutions for smarter businesses

Etteplan invests into ISO 27001 & IEC 62443-4-1 certifications (NIS2 Managed Service Provider)

Etteplan's seven offices have successfully completed ISO 27001 certification

News Release - Published: 15.02.2023 - 10:00:00

→ **Back to Releases**

Etteplan web release February 15, 2023 at 10 a.m. EET

ISO 27001 certification has been issued by LRQA to seven Etteplan's offices, which are Espoo, Jyväskylä Mattilanniemi, Oulu, Linköping, Uppsala, Katowice and Wroclaw. All these offices have Software and Embedded Solutions' operations which are covered by the certification.

ISO 27001 is the only truly global information security standard. ISO 27001 certification is proof of planned and long-term information security management. Being an ISO 27001 certified company ensures the protection of information assets and hence reduces the probability of data breaches and business downtimes.

Etteplan has applied for the certification of IEC 62443-4-1 Secure Product Development Lifecycle process with CertX

News Release - Published: 15.08.2023 - 10:02:03

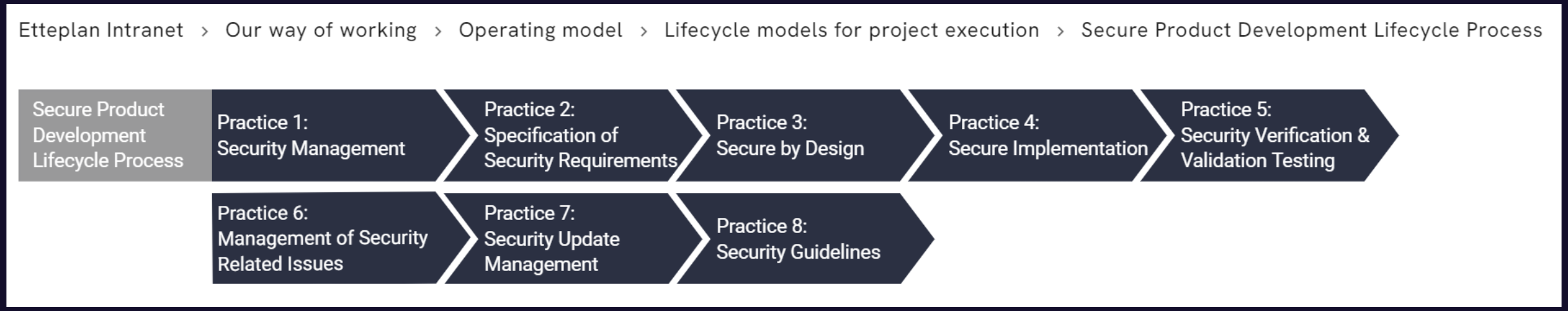
→ **Back to Releases**

Etteplan News release, August 15, 2023

Etteplan has applied for the certification of IEC 62443-4-1 Secure Product Development Lifecycle process with CertX

The EU has introduced the NIS2 directive to regulate cybersecurity in supply chains for software and devices, impacting large industrial equipment manufacturers. Etteplan has proactively invested in formal cybersecurity capabilities, obtaining ISO 27001 certification and pursuing IEC 62443-4-1 certification for their Secure Product Development Lifecycle (SPDL) process. This positions Etteplan to meet NIS2 directive Article 21 requirements starting in October 2024, and to continue to provide managed services related to software and equipment to customers.

Etteplan has a formal SPDL process according to IEC 62443-4-1 that is ready for certification



Roadmap for achieving conformity with new cyber security, AI and use data sharing requirements

STRATEGY/
TRAINING
WORKSHOP

REQUIREMENTS
SPECIFICATION
&
GAP ANALYSIS

WORK PACKAGES
PLANNING

CONFORMING
PRODUCTS
AND
RELATED
OPERATIONAL
SYSTEMS

CONFORMING
MANAGEMENT
SYSTEMS
(QMS, ISMS)

Milestones and challenges in becoming a manufacturer with cybersecure machinery products

PRODUCT SECURITY IDEA EMERGED

- Awareness building about what is product security
- Hiring product security specialists
- Obsolescence of products, services, platforms, supply chains
- Securing resources and funding over several budgeting periods

MULTI-YEAR BUDGET GRANTED

- Building SPDL processes and developing secure-by-design products
- Implement ISMS
- Organisational & cultural changes (R&D, IT, Quality + Security)
- Deploying a formal process to agile software development
- Onboarding the supply chain

SECURE-BY-DESIGN PRODUCTS LAUNCHED

- Getting price premium for secure-by-design products

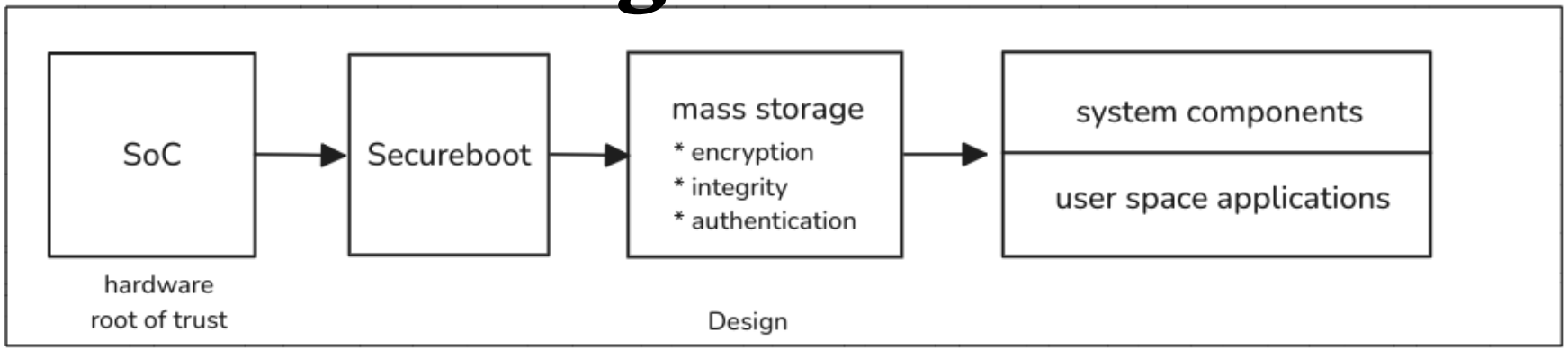
NEW BUSINESS WON

- Profitable execution of lifecycle maintenance activities (SBOM, reporting, updates…)

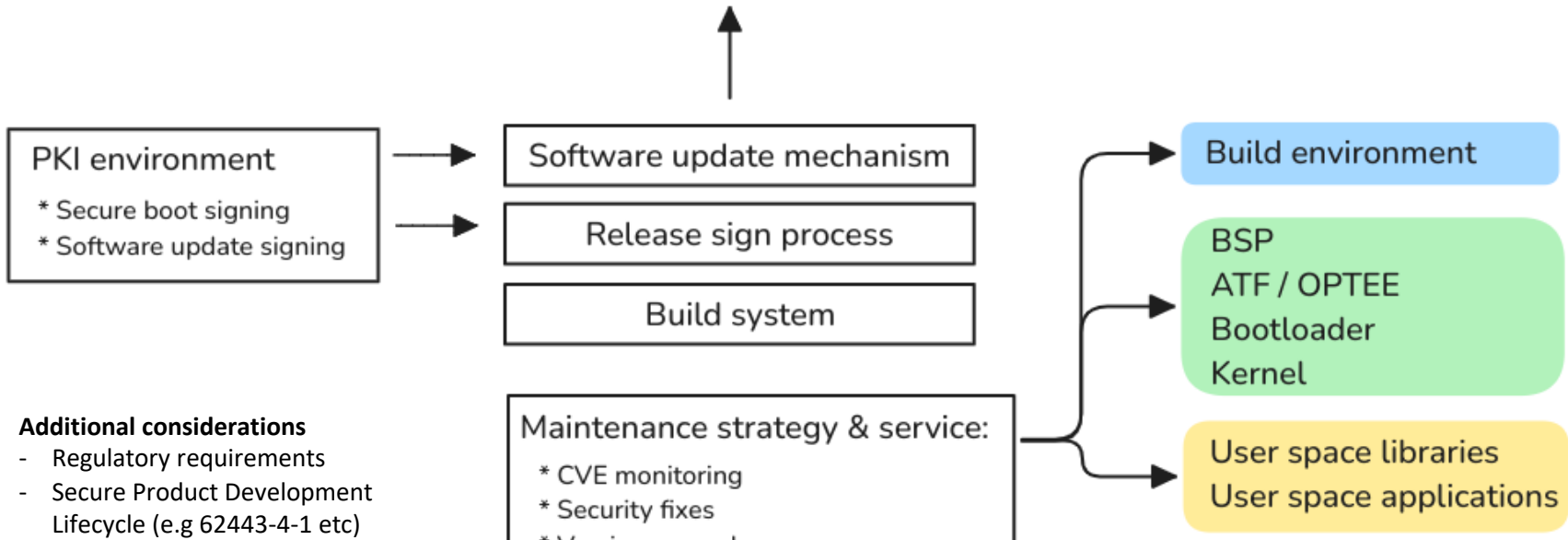
PROFITABILITY MAINTAINED

Secure-by-design embedded linux products require continuous maintenance for bugs and vulnerabilities

Products need certain security mechanisms/primitives, it boils down to chain of trust in



Security mechanisms/primitives require certain operational systems/related services



SW needs to be maintained as publicly known exploitable vulnerabilities will emerge

Additional considerations

- Regulatory requirements
- Secure Product Development Lifecycle (e.g 62443-4-1 etc)
- Information Security Management System (ISO 27001)
- Post-quantum crypto

etteplan

Etteplan's services for product cyber security

- **Cyber security regulations training**
- **Security requirements specification and gap analyses**
- **Secure-by-design product creation and maintenance**
  - Devices and equipment
    - Incl IEC 62443-4-2/3-3 certified products
  - Applications and digital services
    - Device management solutions / device security mechanisms built using Azure or AWS
  - Systems (IoT, manufacturing, etc)
- **Product security verification and validation**
- **Product security-related technical product information**
- **SPDL process implementation and certification support**