MIC MRA Workshop

Cybersecurity in the current situation in Europe

March 2024 • MIC MRA Workshop • Matthias Springer

Cybersecurity in the current situation in Europe

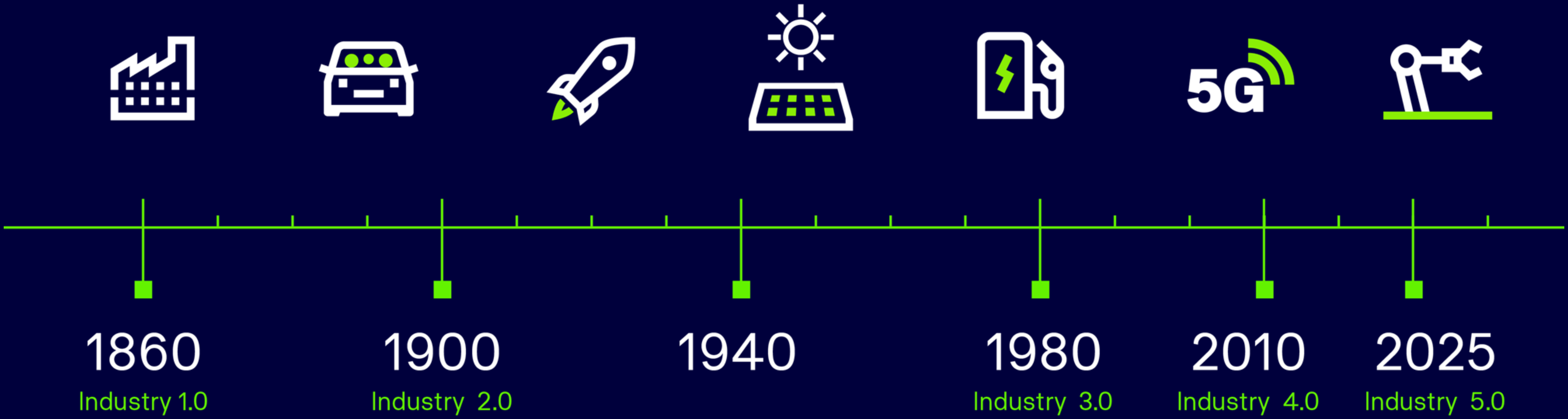
Matthias Springer

Senior Vice President Functional Safety and Security

TÜV NORD CERT GmbH, Essen, Germany

Keeping People and technology safe

For more than 150 years. Every day, worldwide



1860
Industry 1.0

1900
Industry 2.0

1940

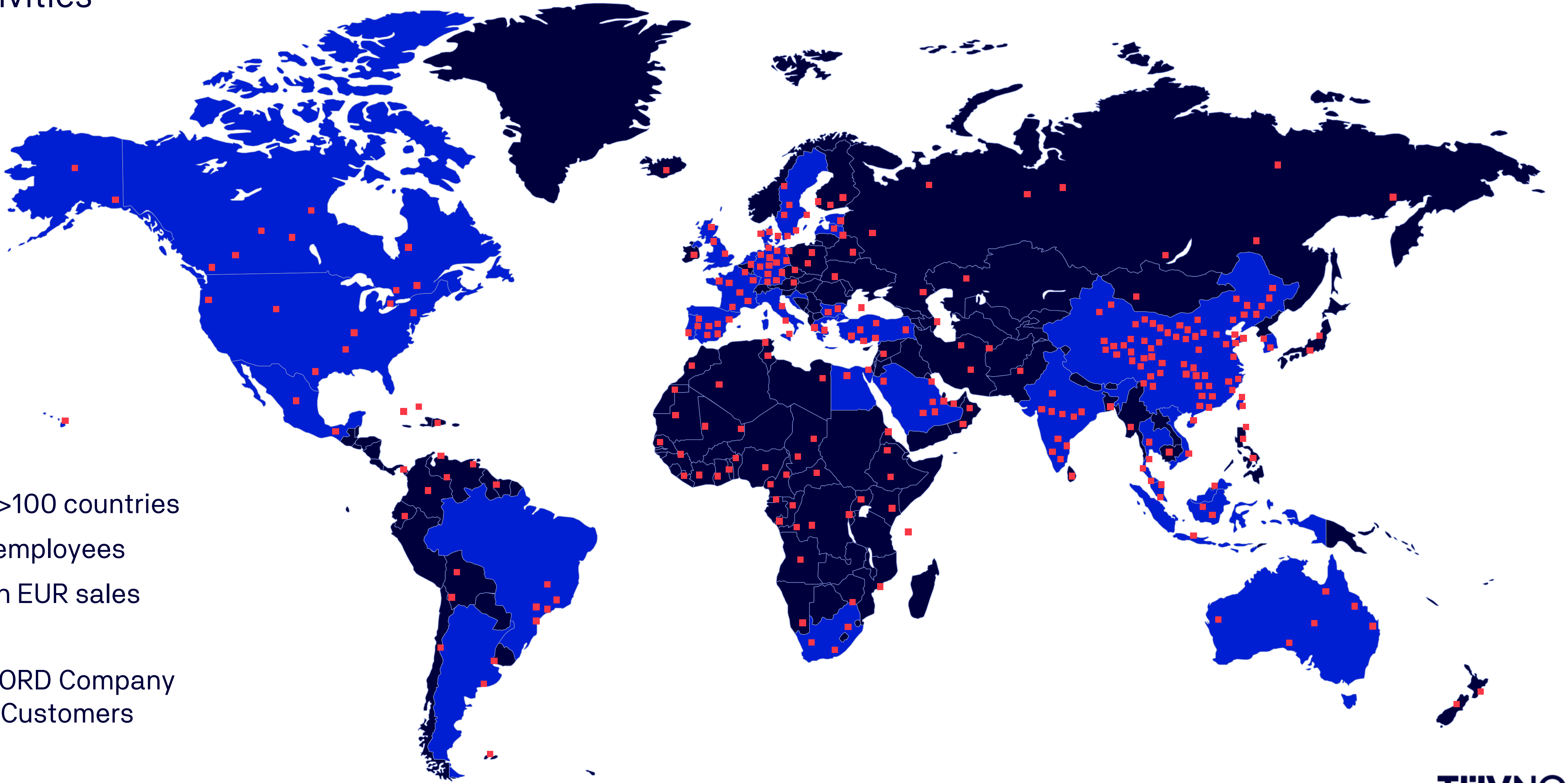
1980
Industry 3.0

2010
Industry 4.0

2025
Industry 5.0

Global expertise – local services

Our activities



Active in >100 countries

>14,000 employees

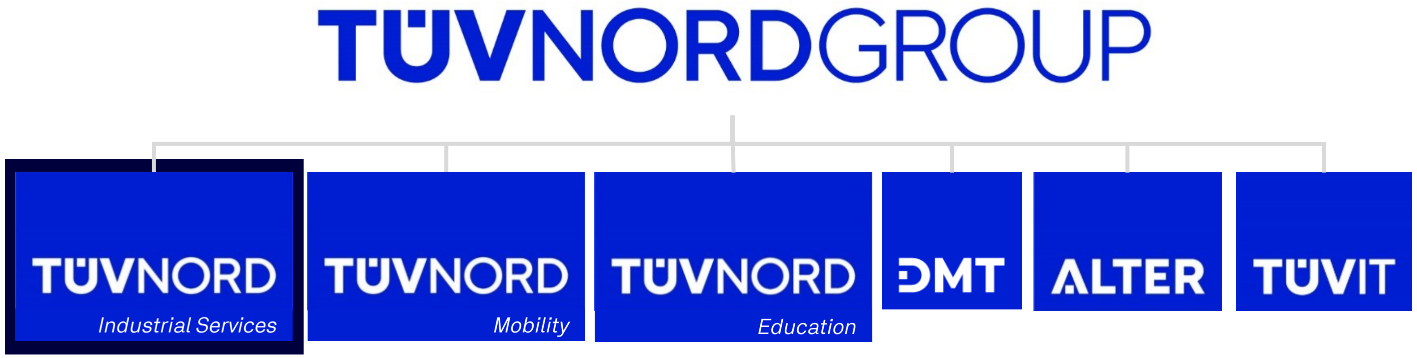
~1.4 billion EUR sales

🟦 TÜV NORD Company

🟥 Large Customers

TÜV NORD GROUP

TÜV NORD GROUP is among the leading global technology service provider delivering TICCET services



TÜVNORDGROUP

TÜVNORD Industrial Services

TÜVNORD Mobility

TÜVNORD Education

DMT

ALTER

TÜVIT

Core Services:

- Testing
- Inspection
- Certification
- Consulting
- Engineering
- Training

Business Units

- **Industrial Services**
- Mobility
- Engineering & Natural Resources
- Aerospace
- Training
- Information Technology

1,552
Revenue EURm (FY 2023)

>15,000
Employees worldwide

86 Group companies of which **44** are located abroad

Actual Security Regulations

Already in force

- GDPR (General Data Protection Regulation)
  - Privacy by design & default / security by design
- NIS 2 (Network Information Security)
  - Providers of Essential Services (Critical Infrastructure)
  - Digital Services Providers
  - → NESAS CCS-GI for 5G
- Cyber Security Act / Cyber Resilience Act
  - Framework and Development of the European Certification Schemes
    - IoT, IIoT
    - Consumer Goods
    - 5G, Cloud Services
- MDR (Medical Device Directive)
  - CE Marking for Medical Devices
- RED (Radio Equipment Directive)
  - CE marking for products with radio (GSM, WiFi, Bluetooth etc.)

Vertical Specific Directives and Regulations

- General Product Safety Directive 2001/95/EC
  - Safety & Security under all product regulations
- Low Voltage Directive 2014/35/EC
  - CE marking for electrical equipment
- Machinery Regulation 2023/1230/EC
  - CE marking for machinery equipment

enisa cen CENELEC

European Approach for Cybersecurity Certification

Horizontal Framework

Risk-based Approach

Basic

Substantial

High

* New Legislative Framework

EU CYBERSECURITY ACT
THE LATEST EU'S LEGISLATION TO ADVANCE CYBERSECURITY ACROSS EUROPE

Government Authorities, Regulators

Scheme owners, Accreditation Bodies

Interest Groups of Industry

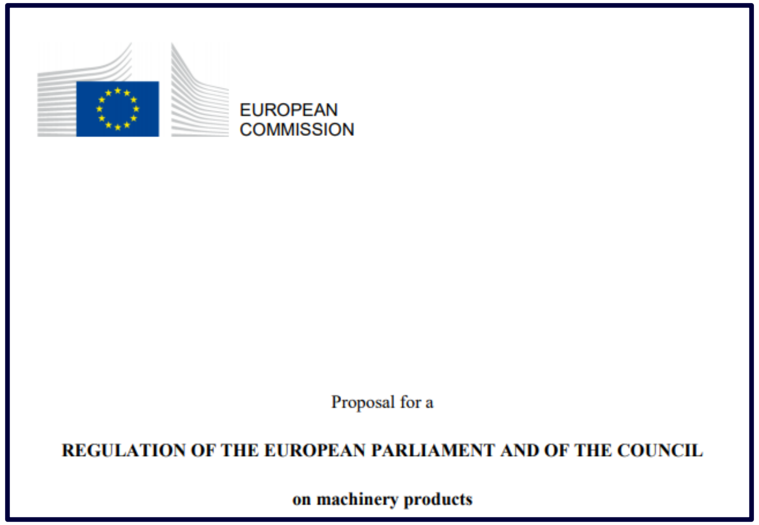
Cybersecurity Act / Cyberresiliance Act
REGULATION (EU) 2019/881 & 2019/1020

Railway Safety Directive			Low Voltage Directive			Machinery Directive			Medical Device Directive		Radio Equipment Directive
Infra-structure / Trackside	Oper. control and maint.	On-board	Toys	White Goods	Wear-abels	Robots	Sensor Actuator	…	Respirator Insulin pump	AAL Society 5.0	Smart Home Applications

enisa
STANDARDS
STANDARDISATION IN SUPPORT OF THE CYBERSECURITY CERTIFICATION
Recommendations for European standardisation in relation to the Cybersecurity Act
DECEMBER 2019
ROLLING PLAN FOR ICT STANDARDISATION 2019

* product harmonization legislation in line with Decision 768/2008/EC

European Legislative Approach



EUROPEAN
COMMISSION

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on machinery products

New Machinery Regulation

In a digital market driven by the Internet of Things and AI powered systems, vulnerability to cyberattacks of factories and critical infrastructures is a de facto concern and a growing threat. For example, some industrial processes nowadays are conveniently managed through mobile apps. While such remote controls might increase production's efficiency, they also create targets for cyber-attacks. This means that cybersecurity has a direct impact on workplace safety, and that the cybersecurity of industrial control systems and networks has therefore become a prerequisite.
Consideration to the threats and vulnerabilities described above needs to be given as early as the design stage by employing "security by design" solutions.

Integration of Cyber Security in the new Machinery Regulation
to ensure Essential Health and Safety Requirements (EHSR).
Cyber Security is central element and mandatory for Machinery compliance.

Cyber Resilience Act

The Act will

- Ensure that products with digital elements placed on the EU market have fewer **vulnerabilities** and that
- manufacturers remain responsible for cybersecurity throughout a product's life cycle;
- Improve **transparency** on security of hardware and software products;
- Business users and consumers benefit from better protection
- **Provide harmonised rules** for the placing on the market of connected hardware and software products;

Manufacturers will have to

→ **report actively exploited vulnerabilities and incidents**;

→ Once sold, manufacturers must ensure that for the **expected product lifetime vulnerabilities are handled effectively**;

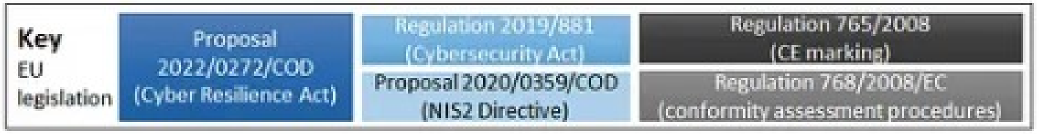
→ **Clear and understandable instructions** for the use of products with digital elements;

→ **Security updates** to be made **available for at least five years**

Timeline

- **Economic operators and Member States will have two years to adapt to the new requirements**. The obligation to report actively exploited vulnerabilities and incidents will apply after one year.

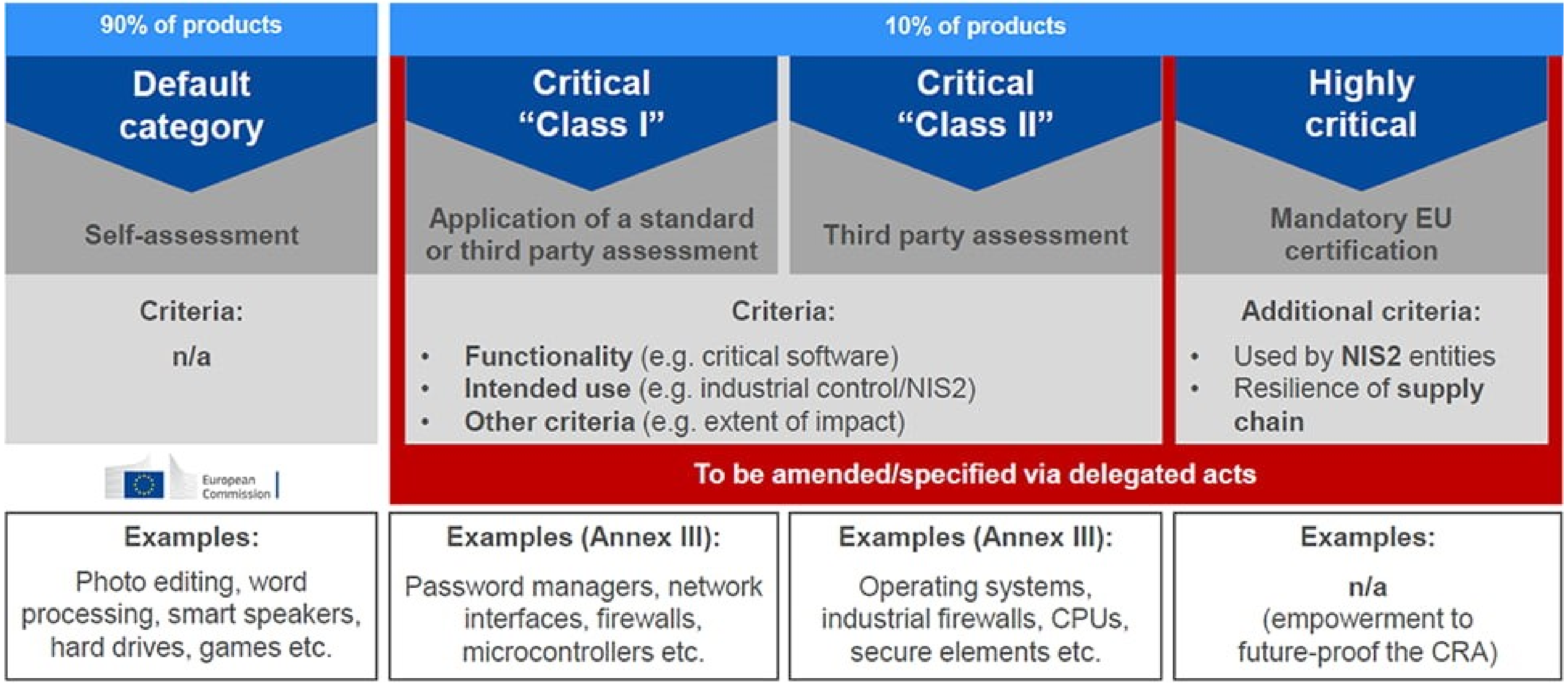
Cyber Resilience Act



Key EU legislation	Proposal 2022/0272/COD (Cyber Resilience Act)	Regulation 2019/881 (Cybersecurity Act)	Regulation 765/2008 (CE marking)
		Proposal 2020/0359/COD (NIS2 Directive)	Regulation 768/2008/EC (conformity assessment procedures)

Affected Products

- Differentiation between self assessment and third party assessment
- Criteria and examples for categories are to be fixed by delegated act
- Risk Analysis will be the basis for decision
- Third party assessment beneficial in case of uncertainty
- Self-assessment for safety critical components not possible



90% of products	10% of products		
Default category	Critical "Class I"	Critical "Class II"	Highly critical
Self-assessment	Application of a standard or third party assessment	Third party assessment	Mandatory EU certification
Criteria: n/a	Criteria: • **Functionality** (e.g. critical software) • **Intended use** (e.g. industrial control/NIS2) • **Other criteria** (e.g. extent of impact)		Additional criteria: • Used by **NIS2** entities • Resilience of **supply chain**
	To be amended/specified via delegated acts		
Examples: Photo editing, word processing, smart speakers, hard drives, games etc.	Examples (Annex III): Password managers, network interfaces, firewalls, microcontrollers etc.	Examples (Annex III): Operating systems, industrial firewalls, CPUs, secure elements etc.	Examples: n/a (empowerment to future-proof the CRA)

Figure – courtesy from European Commission

Cyber Resilience Act

Take-aways

- All Product manufacturers of connected devices affected
- CE-conformity includes Cybersecurity
- Machine Regulation conformity **does not show implicitly CRA conformity**
- Generic CRA obligations are covered by IEC 62443-4-1

Generic CRA requirements

→ **report actively exploited vulnerabilities and incidents**;

→ Once sold, manufacturers must ensure that for the **expected product lifetime** or for a period of five years (whichever is the shorter), **vulnerabilities are handled effectively**;

→ **Clear and understandable instructions** for the use of products with digital elements;

→ **Security updates** to be made **available for at least five years**

- Foreseen harmonized standards for **presumption of conformity**:
  - IEC 62443-4-1 & -4-2
  - ETSI EN 303 645 [or similar]
  - ISO/IEC 15408

IEC 62443 compliance effects presumption of conformity with CRA and Machinery Regulation

Radio Equipment Directive Delegated Act

Essential requirements of Article 3(3)

- *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;*

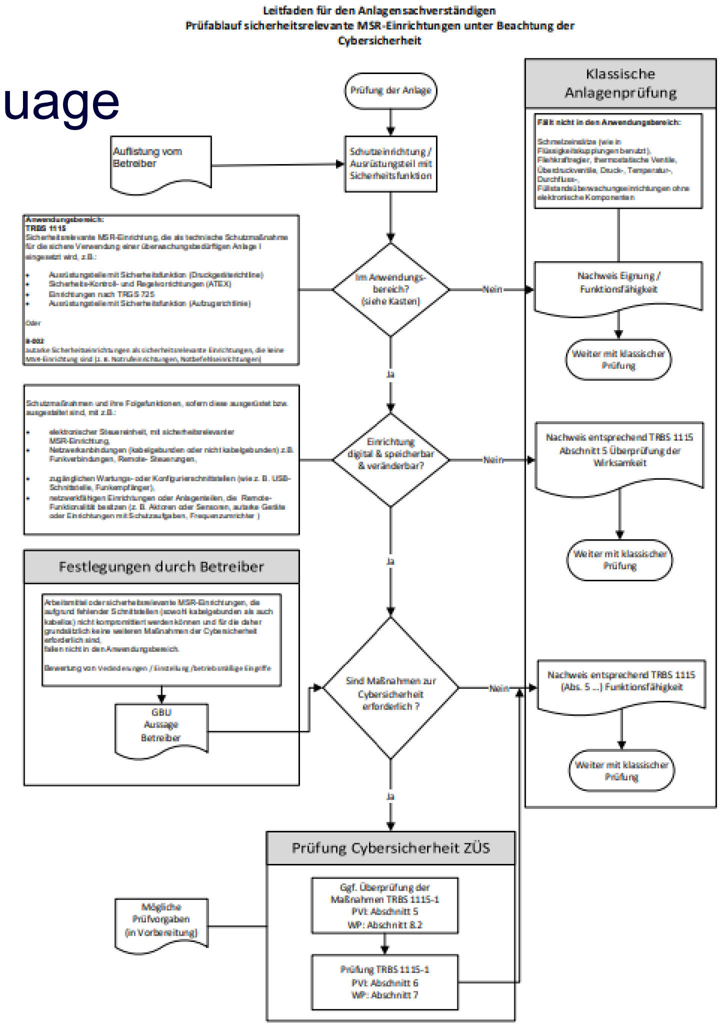
Conformity assessment

- **Self-assessment**
  - Using harmonised standards
- **Third-party conformity assessment**
  - In any case
  - Notified body to be involved
- **Once performed:**
  - Declaration of conformity
  - CE marking
  - Manufacturer becomes responsible to the MSA

→ Potential harmonized standards for **presumption of conformity**: EN 303 645 [or similar]

TRBS 1115-1 : Cybersecurity for Operators

Sorry, only in German language



Leitfaden für den Anlagensachverständigen
Prüfablauf sicherheitsrelevante MSR-Einrichtungen unter Beachtung der Cybersicherheit

Prüfung der Anlage

Auflistung vom Betreiber

Schutzeinrichtung / Ausrüstungsteil mit Sicherheitsfunktion

Anwendungsbereich:
TRBS 1115
Sicherheitsrelevante MSR-Einrichtung, die als technische Schutzmaßnahme für die sichere Verwendung einer überwachungsbedürftigen Anlage I eingesetzt wird, z.B.:

- Ausrüstungsteile mit Sicherheitsfunktion (Druckgeräterichtlinie)
- Sicherheits-Kontroll- und Regeleinrichtungen (ATEX)
- Einrichtungen nach TRGS 725
- Ausrüstungsteile mit Sicherheitsfunktion (Aufzugsrichtlinie)

Oder

B-002:
autarke Sicherheitseinrichtungen als sicherheitsrelevante Einrichtungen, die keine MSR-Einrichtung sind (z. B. Notrufeinrichtungen, Notbefehlseinrichtungen)

Im Anwendungsbereich? (siehe Kasten)

Schutzmaßnahmen und ihre Folgefunktionen, sofern diese ausgerüstet bzw. ausgestattet sind, mit z.B.:

- elektronischer Steuereinheit, mit sicherheitsrelevanter MSR-Einrichtung,
- Netzwerkanbindungen (kabelgebunden oder nicht kabelgebunden) z.B. Funkverbindungen, Remote- Steuerungen,
- zugänglichen Wartungs- oder Konfigurierschnittstellen (wie z. B. USB-Schnittstelle, Funkempfänger),
- netzwerkfähigen Einrichtungen oder Anlagenteilen, die Remote-Funktionalität besitzen (z. B. Aktoren oder Sensoren, autarke Geräte oder Einrichtungen mit Schutzaufgaben, Frequenzumrichter)

Einrichtung digital & speicherbar & veränderbar?

Festlegungen durch Betreiber

Arbeitsmittel oder sicherheitsrelevante MSR-Einrichtungen, die aufgrund fehlender Schnittstellen (sowohl kabelgebunden als auch kabellos) nicht kompromittiert werden können und für die daher grundsätzlich keine weiteren Maßnahmen der Cybersicherheit erforderlich sind, fallen nicht in den Anwendungsbereich.

Bewertung von Verbindungen / Einstellung /betriebsmäßige Eingriffe

GBU Aussage Betreiber

Sind Maßnahmen zur Cybersicherheit erforderlich ?

Prüfung Cybersicherheit ZÜS

Ggf. Überprüfung der Maßnahmen TRBS 1115-1
PVI: Abschnitt 5
WP: Abschnitt 8.2

Prüfung TRBS 1115-1
PVI: Abschnitt 6
WP: Abschnitt 7

Mögliche Prüfvorgaben (in Vorbereitung)

Klassische Anlagenprüfung

Fällt nicht in den Anwendungsbereich:

Schmelzeinsätze (wie in Flüssigkeitskupplungen benutzt), Fliehkraftregler, thermostatische Ventile, Überdruckventile, Druck-, Temperatur-, Durchfluss-, Füllstandsüberwachungseinrichtungen ohne elektronische Komponenten

Nachweis Eignung / Funktionsfähigkeit

Weiter mit klassischer Prüfung

Nachweis entsprechend TRBS 1115 Abschnitt 5 Überprüfung der Wirksamkeit

Weiter mit klassischer Prüfung

Nachweis entsprechend TRBS 1115 (Abs. 5 ...) Funktionsfähigkeit

Weiter mit klassischer Prüfung

Compliance Requirements

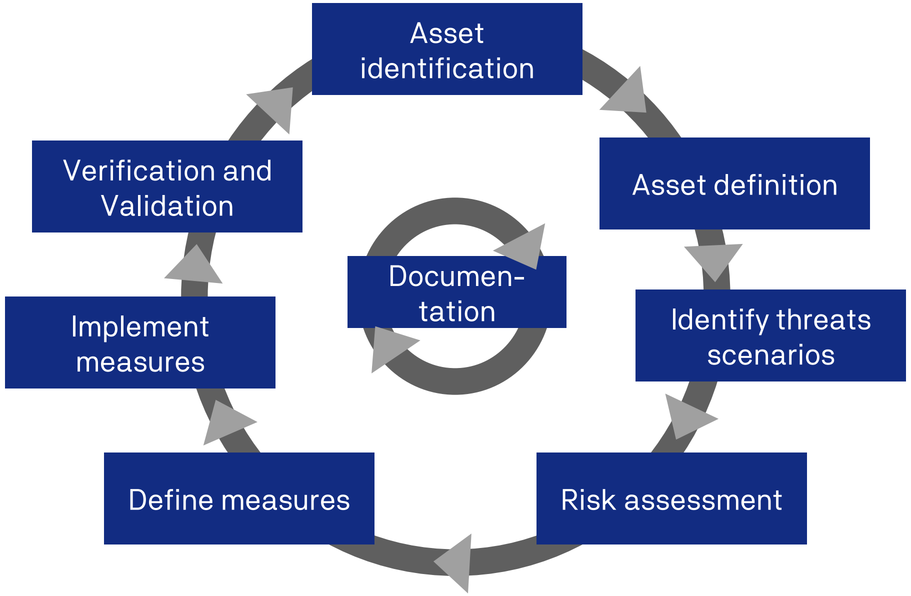
Section 3: **Risk assessment** - assess threats and derive measures

Section 4: **Implementation** of the measures

Section 5: **Verification** of the effectiveness of the measures before first use

Section 6 +7: **Testing** the work equipment / system requiring monitoring

Section 8.2: **Regular checks** of functionality

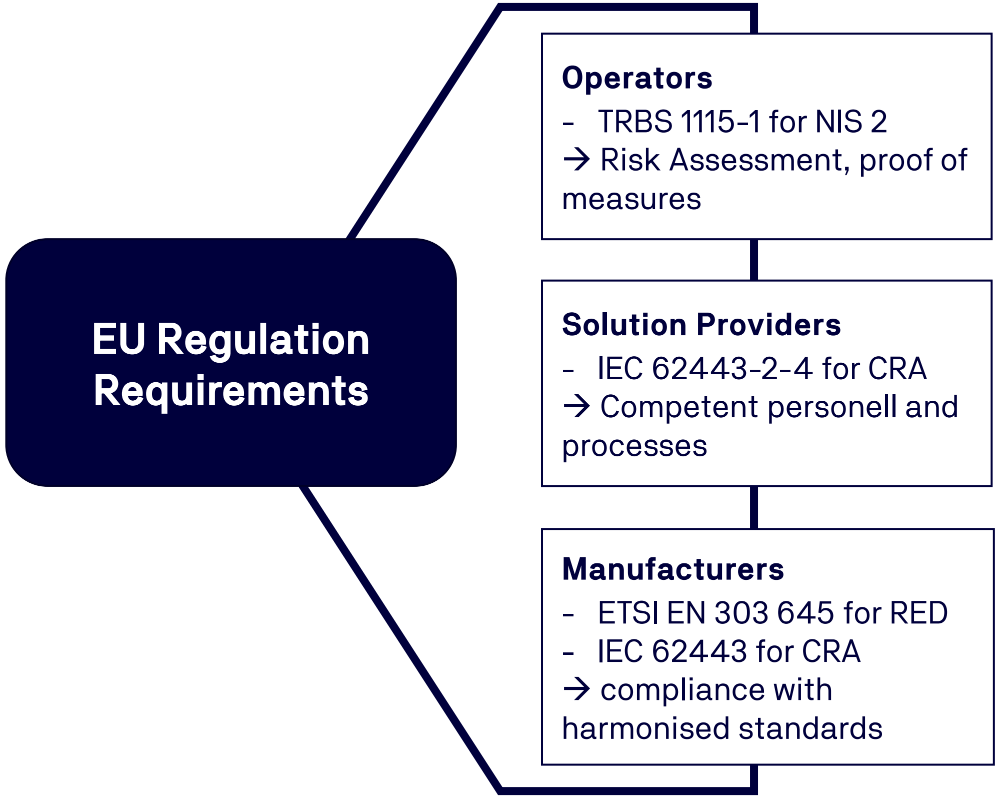


TÜVNORD

Take Aways

European Cybersecurity Regulation

- NIS 2, CRA, RED most affecting Cyber Regulations in EU
- Mandatory requirements to place products in EU market
- Top down regulation for all logical layers (Operators, Solution Provider and Product Manufacturers)
- Integration of requirements in vertical directives/regulations (e.g. Machine Reg., MDR)
- IEC 62443 series and ETSI EN 303 645 as main standards for presumption of conformity



EU Regulation Requirements

Operators
- TRBS 1115-1 for NIS 2

→ Risk Assessment, proof of measures

Solution Providers
- IEC 62443-2-4 for CRA

→ Competent personell and processes

Manufacturers
- ETSI EN 303 645 for RED
- IEC 62443 for CRA

→ compliance with harmonised standards

TÜVNORD

Questions?

Matthias Springer

T.: 0160 888 3299

M.: mspringer@tuev-nord.de