Cybersecurity Testing and Certification

Ted Strandberg

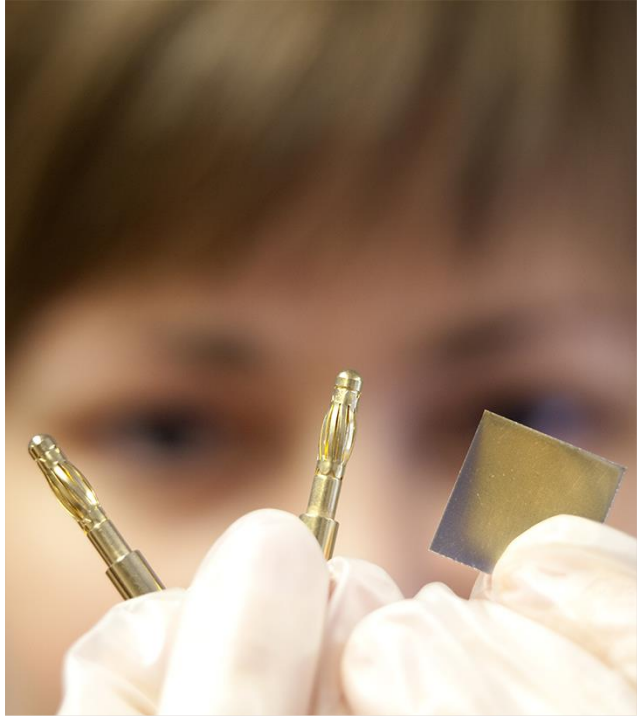
Linköping Science Park

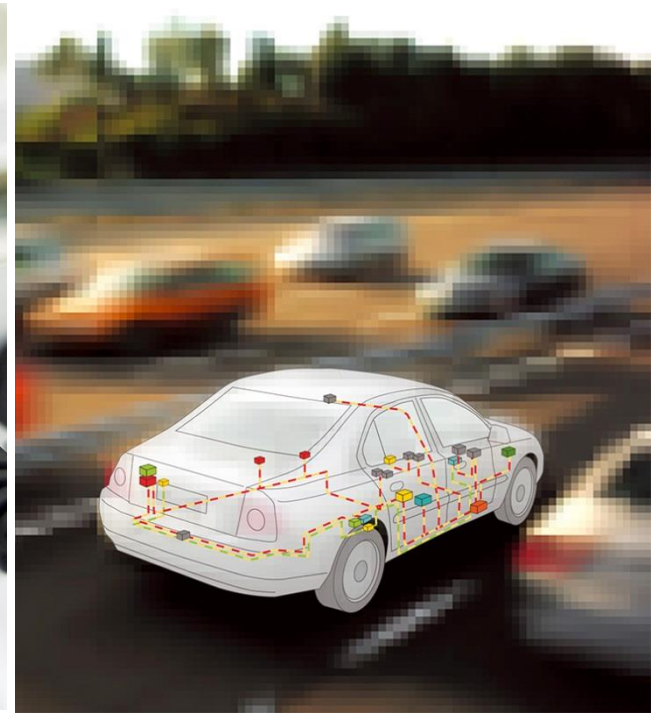
August 2023

Research Institutes of Sweden

SAFETY AND TRANSPORT

Electrification and Reliability



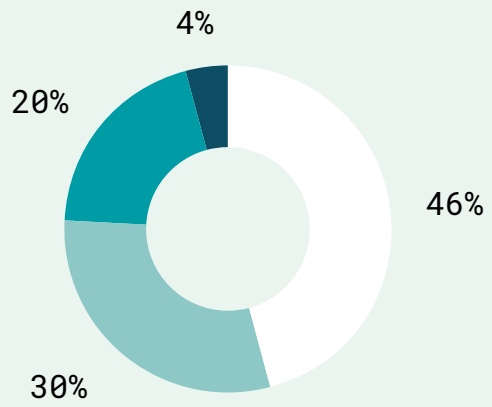


3,993

SEK million, net sales

Operating results: 22 SEK million

Operating margin: 0,6%



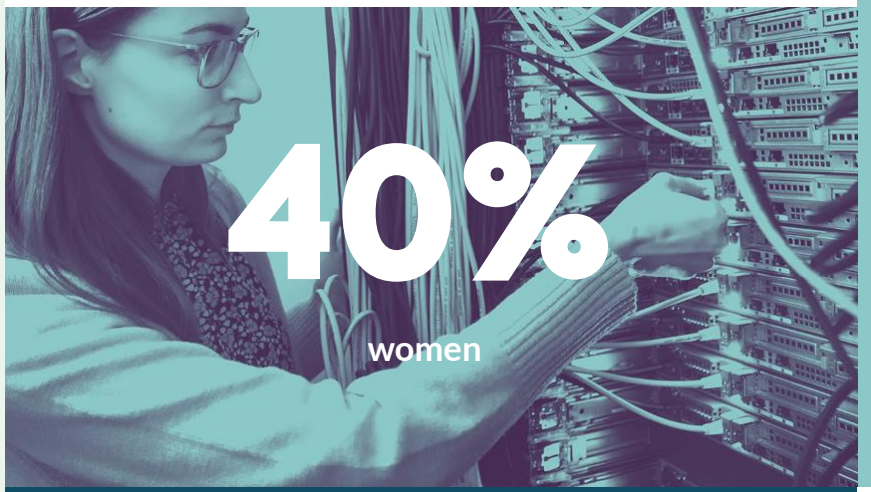
Distribution of net sales

Business sector	1,831 MSEK
Public funds	1,179 MSEK
State funds	812 MSEK
EU funds	171 MSEK

Nearly

3,300

employees



130+

Testbeds and demonstration environments

We are represented at

35

locations around Sweden

78

Customer Satisfaction Index

Alla siffror avser 2022.

Testbeds at RISE, Research Institutes of Sweden

RI.
SE

Functional safety

Machine safety

Alarm systems

Taximeters

Reporting centres for taxi traffic

Control systems and devices

Measuring instruments

Cyber-security

Medical technology

SAFE CONTROL SYSTEMS

RISE OFFERS IN CYBERSECURITY

Professional training and education

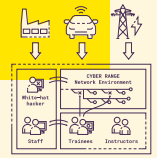
- Cyber security for developers
- Cyber security for boards and management teams
- Purple team exercises to train defense of infrastructure and systems (both technical and organizational dimensions)

Testing of products and services

- Penetration tests of software, hardware or infrastructure to detect vulnerabilities and deficiencies
- Analysis of system architecture from a cybersecurity perspective

Sector-specific digital twins

- Testing, analysis and training in realistic environments where it is not possible or too risky to implement this in the real, operational environment



Safe and confidential environment

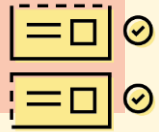
- Opportunity to discuss sensitive issues without risk of eavesdropping with security-classified personnel

Cybersecurity research

- Provides conditions for certain types of applied research, e.g. how cyber range can be used.

Cybersecurity certification

- EU Cyber Security Act*
- Verified by RISE*
- Information security management system
- Product certifications



** Under development*

GLOBAL CHALLENGES

- Digitalisation
- Globalisation
- Urbanisation
- Changing demographics
- Climate change
- Resource utilisation
- Pandemics

Every 11 seconds there is a **ransomware attack**

Ransomware attacks alone are estimated to have cost the world roughly **€20 billion** in 2021

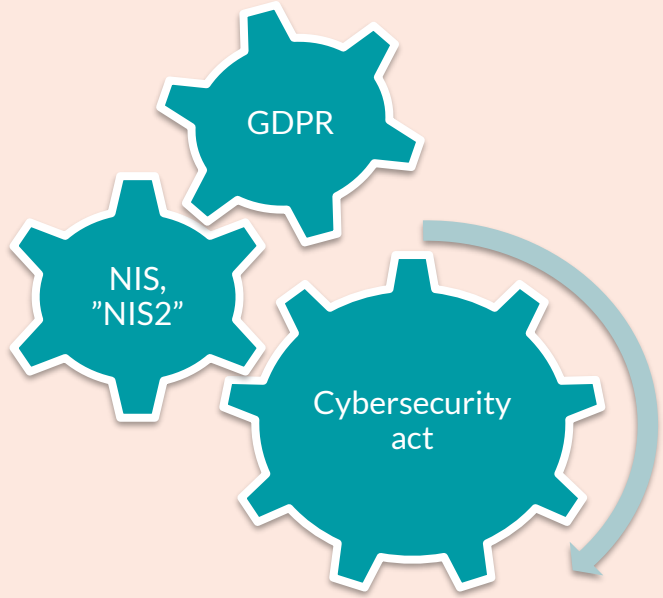
The **global annual cost** of cybercrime was estimated to be **€5.5 trillion** in 2021

RI. SE

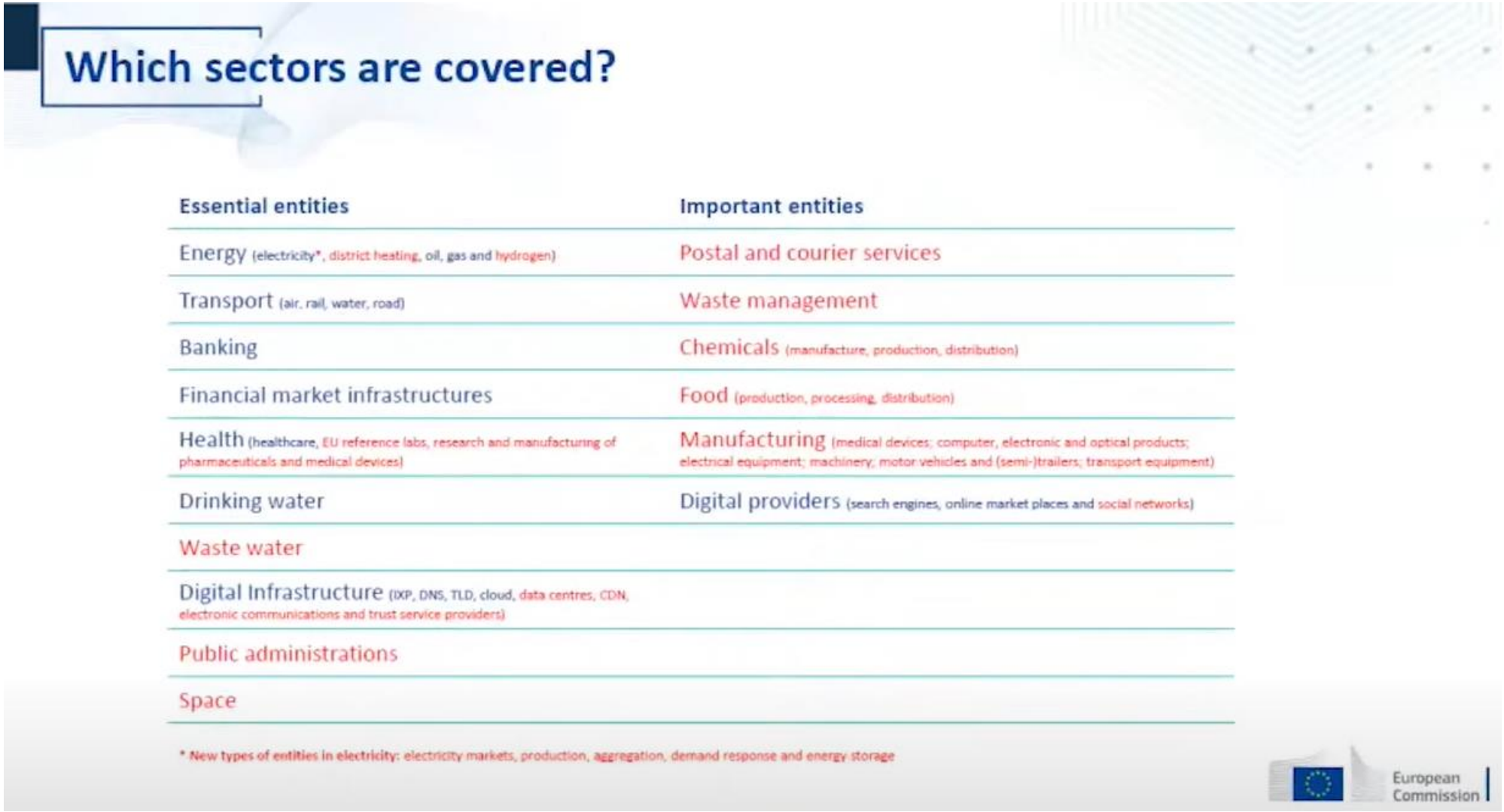
Cybersecurity Initiatives EU

- Directive on security of network and information systems (NIS)
- General Data Protection Regulation (GDPR)
- Cybersecurity Act
- Cyber Resilience Act

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY



Cybersecurity Initiatives EU - NIS and NIS2



Cybersecurity Initiatives EU – Cybersecurity Act

Cyber security act, certification schemes:

- Cloud services
- (IoT)
- 5G
- Common Criteria

EUCS – Certification for Cloud services

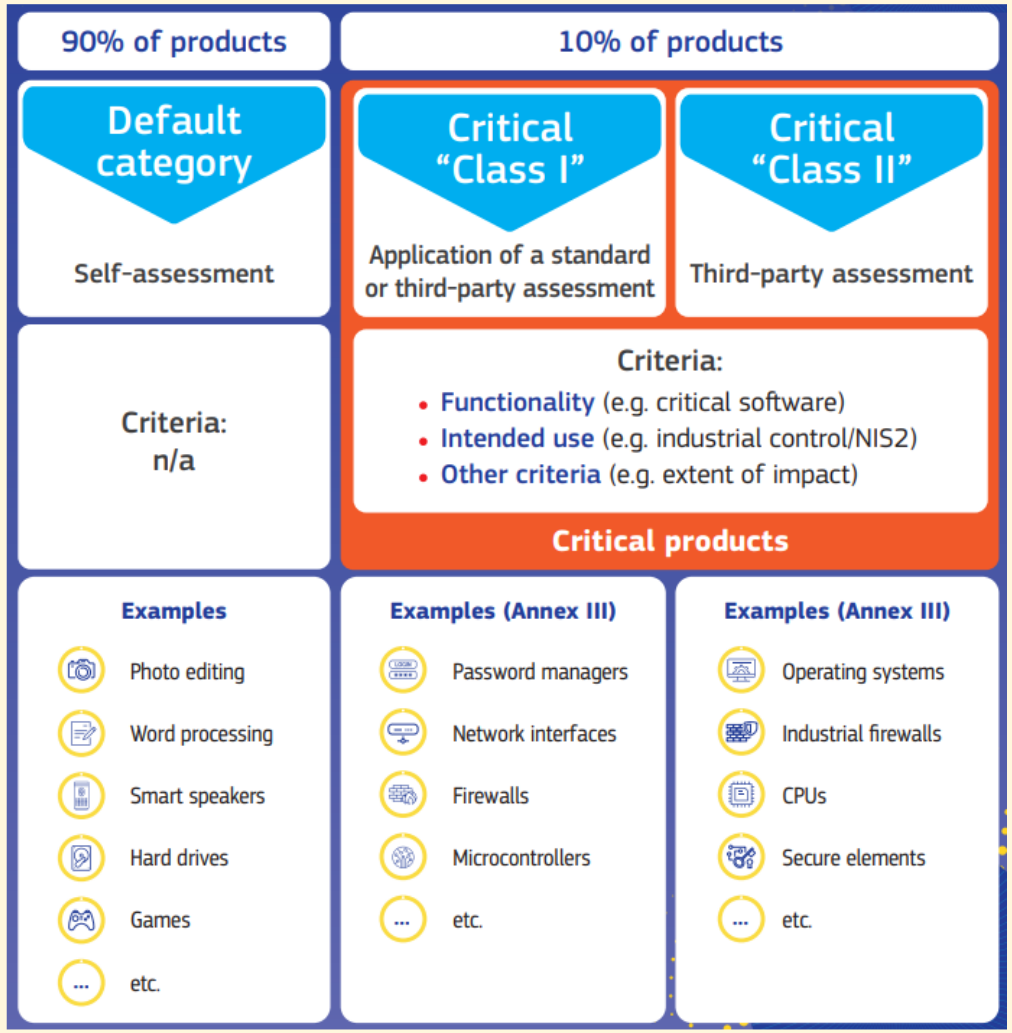
- Based on existing standards, e.g. ISO 27000, C5 etc
- Estimated to be the first certification scheme

1.2.3 Assurance levels

The requirements defined in the present Annex are labelled Basic, Substantial or High:

- Requirements labelled Basic apply to all assurance levels.
- Requirements labelled Substantial apply to levels Substantial and High, and they will in most cases be considered as guidance for level Basic (*i.e.*, the reference method to achieve the Basic requirements, which are often less detailed).
- Requirements labelled High only apply to level High.

Cyber Resilience Act (CRA)



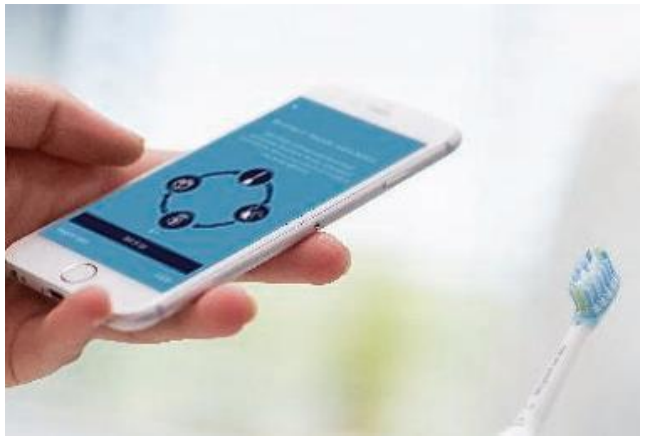
CE marking procedure in EU part 1

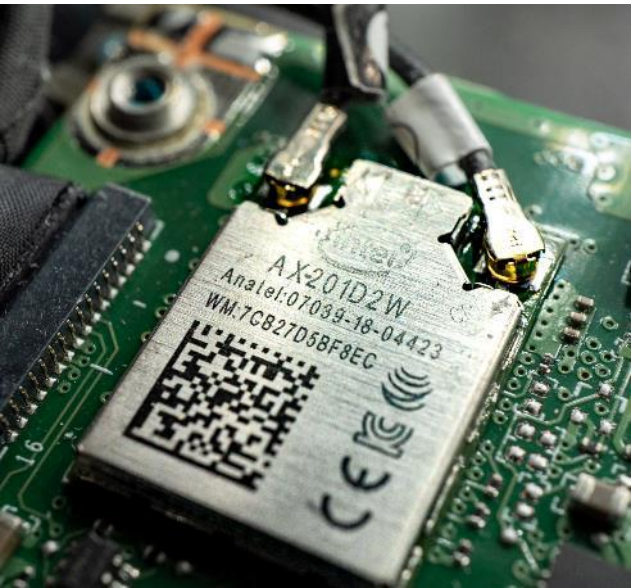
- CE marking is a declaration by the manufacturer, issued in the form of a **Declaration of Conformity** (DoC). In some cases, a Notified Body must be used.
- The CE mark must cover all applicable directives, if a product is in scope of more than one directive. Generic information on CE marking can be found in the **Blue Guide**. Not all product categories may be CE marked. See this page for product categories that are applicable for CE marking: https://single-marketeconomy.ec.europa.eu/single-market/ce-marking/manufacturers_sv
- The Declaration of Conformity (DoC) must be based on Technical Documentation (TD) held by the manufacturer. The DoC and the TD must be continuously revised whenever requirements/standards are updated or added.
- **Risk assessment is required** by several directives, manufacturer is responsible for performing the assessment and documenting the assessment results.
- Each produced sample of a product which leaves the control of the manufacturer must comply with the requirements in force at that time (product samples already in store at retailers are still OK to sell).

CE marking procedure in EU part 2

- In some cases, a Notified Body (NB) must be used. Example of such cases are if a **Harmonised Standard** (listed in the Official Journal) is used only in part, or if it is **not used** at all.
- The Notified Body **performs a third-party review** of the Technical Documentation (TD) held by the manufacturer. The review can cover all articles, or only specific articles selected by the manufacturer.
- If the review is successful, the **Notified Body will issue a Type Examination Certificate** (TEC). The TEC is a statement which confirms that the Notified Body agrees with the manufacturers own assessment that the product fulfils all of the essential requirements of the Directive. (The TEC is not an approval or a certification !)
- If an Notified Body has been used, the Declaration of Conformity (DoC) must list the TEC reference. The TEC becomes part of the TD.
- The TEC is **only valid for the specific configuration that was part of the review**, so the TEC may need to be revised whenever requirements/standards are updated or added for the product. The Manufacturer must inform the Notified Body if changes are applied to the product covered by the issued TEC.
- Further information about the Notified Body function can be found in the Blue Guide.

RED delegated regulation (EU) 2022/30 and Standardization request M585





RED Delegated Regulation (2022/30) activates RED requirements 3.3.d/e/f

- 3.3.d “radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service”
- 3.3.e “radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected”
- 3.3.f “radio equipment supports certain features ensuring protection from fraud”

The delegated regulation which was published on the 12th of January 2022, states in recital (1):

“Protection of the network or its functioning from harm, protection of personal data and privacy of the user and of the subscriber and protection from fraud are elements that support protection against cybersecurity risks”.

RED Delegated Regulation (2022/30) scope for RED requirements 3.3.d/e/f

- RED Article 3.3(d) – to ensure network protection – applies to:
  - radio equipment that can communicate itself over the internet, whether it communicates directly or via any other equipment (‘internet-connected radio equipment’)
- RED Article 3.3(e) – to ensure safeguards for the protection of personal data and privacy – applies to the following equipment when capable of processing personal data or traffic data and location data:
  a) internet-connected radio equipment other than referred to in points b), c) or d);
  b) radio equipment designed or intended exclusively for childcare;
  c) radio equipment falling under the Toys Directive (2009/48/EC);
  d) radio equipment designed or intended, whether exclusively or not exclusively, to be worn on, strapped to, or hung from the body or clothing worn by human beings
- RED Article 3.3(f) – to ensure protection from fraud – applies to:
  - internet-connected radio equipment, if that equipment enables the holder or user to transfer money, monetary value or virtual currency.

RED Delegated Regulation (2022/30) exemptions for 3.3.d/e/f

- The following radio equipment is fully exempted from RED Articles 3.3(d), 3.3(e) and 3.3(f):
  - Medical devices under Regulation (EU) 2017/745 and (EU) 2017/746
- The following radio equipment is exempted from RED Articles 3.3(e) and 3.3(f), but article 3.3(d) still applies:
  - Radio equipment under Regulation (EU) 2018/1139 (civil aviation)
  - Radio equipment under Regulation (EU) 2019/2144 (motor vehicles)
  - Radio equipment under Directive (EU) 2019/520 (road toll systems)

The standardization request

An amendment to extend the SR was adopted by COM, in final approvals:

- hENs – 30 June 2024
- Application – 1 august 2025

Standardization Request (M585)

Harmonised standards in support of the essential requirement set out in Article 3(3), point (d/e/f), of Directive 2014/53/EU for the categories and classes specified by Delegated Regulation (EU) 2022/30 shall contain technical specifications that ensure at least that those radio equipment, where applicable:

d 1. include elements to monitor and control network traffic, including the transmission of outgoing data;

d 2. is designed to mitigate the effects of ongoing denial of service attacks;

def 3. implement appropriate authentication and access control mechanisms;

def 4. are provided, on a risk basis, with up-to-date software and hardware at the moment of placing on the market that do not contain publicly known exploitable vulnerabilities as regards harm to the <d><e><f>;

def 5. are provided with automated and secure mechanisms for updating software or firmware that allow, when necessary, the mitigation of vulnerabilities that if exploited may lead to <d><e><f>;

def 6. protect the exposed attack surfaces and minimise the impact of successful attacks.

ef 7. protect stored, transmitted or otherwise processed <e> <f> against accidental or unauthorised storage, processing, access, disclosure, unauthorised destruction, loss or alteration or lack of availability of <e> <f>;

e 8. include functionalities to inform the user of changes that may affect data protection and privacy;

ef 9. log the internal activity that can have an impact on <e> <f>;

e 10. allow users to easily delete their stored personal data, enabling the disposal or replacement of equipment without the risk of exposing personal information;

<d> = network or its functioning or misuse of network resources, <e> = personal & location data protection and privacy, <f> = financial or monetary data

CEN/CENELEC JTC 13/WG 8 “Special Working Group RED Standardization Request”

- JTC 13/WG8 was established on July 7, 2022, to address the RED Standardization Request.
- JTC 13/WG8 currently has 202 committee members representing:
  - 19 National bodies
  - Liaisons/partners: CEN, CENELEC, ISO, ANEC, APPLIA, ESMIG, ETSI, EURALARM, EUROSMART and SBS
- Convenor: Ben Kokx
- Secretariat: NEN (Astrid de Haes & Reyhan Cigdem)
- JTC 13/WG8 is on a tough meeting schedule, in the past year we scheduled 53 meetings of which 8 full week hybrid plenary meetings and countless sub-team meetings to prepare the deliverables.

UPDATED

RED Delegated Regulation hENs Updated Schedule			
Stage Code	**Stage**	**Target date**	**Duration**
10.99	Decision on WI Proposal	2022-10-14	
			+ 16 weeks
20.60	Circulation of 1st WD	2023-02-03	
			+ 27 weeks
30.99	Acceptance of ENQ draft	2023-08-11	
			+ 3 weeks
40.20	Submission to Enquiry	2023-09-01	
			+ 12 weeks
40.60	Closure of Enquiry	2023-11-24	
			+ 12 weeks
45.99	Acceptance of FV draft	2024-02-16	
			+ 3 weeks
50.20	Submission to Formal Vote	2024-03-08	
			+ 8 weeks
50.60	Closure of Formal Vote	2024-05-03	
			+ 4 weeks
60.55	DOR/Ratification	2024-05-31	
			+ 4 weeks
60.60	DAV/Definitive text available	2024-06-28	

ETSI EN 303645 and SSF 1120-1 - IOT Connected Devices

- Swedish Theft Prevention Association Standard for consumer IoT devices
- Introduced on 27th May 2021
- SSF 1120-1 requirements are derived from ETSI EN 303645
- Explained various information process of consumer IoT
- Examples of IoT:
  - Home automation
  - IP/web cameras
  - Digital locks
  - Connected alarms
  - Smart TVs

Professional Training and Education

- Introduction to Cybersecurity
- Road vehicles – Cybersecurity engineering ISO/SAE 21434
- Cybersecurity for developers
- About critical Cybersecurity
- Cybersecurity for Consumer IoT – ETSI EN 303645 / SSF 1120-1
- Cybersecurity for Industrial Applications IEC 62443

https://www.ri.se/en/center-for-cybersecurity/events-and-workshops

RI.
SE

Accredited cybersecurity assessments

Standards for security in connected products:

- ISO 27000 — Information security management systems
- IEC 62443 — Industrial communication networks – Network and system security
- IEC 62443-4-1 — Secure product development lifecycle
- IEC 62443-4-2 — Technical security for components
- ETSI EN 303645 — Cyber Security for Consumer IoT
- SSF 1120-1 — IoT Connected devices
- IEC 60335-1 — Household and similar electrical appliances, Annex U

- OWASP
- Other cybersecurity related product specific standards

RI. SE

EC Type Examination Certificate

SC0534-13

Issued by Notified Body No. 0402 according to 2006/42/EG, the Machinery Directive, annex IX, regarding:

Electrohydraulic Control System IQAN-MC3

Issued to

Parker Hannifin Manufacturing Sweden AB

Mölnlycke Fabriker 14, SE-435 35 Mölnlycke, Sweden

Reg.number: 556045-9470

Product description and product name

Electrohydraulic Control System IQAN-MC3, programmable controller for use in mobile machinery applications intended for implementation of safety functions.

Hardware version is 20077717 Rev. L . Software version is 5.02.12.

Technical documentation

The manufacturer's technical file, latest dated 2018-04-06.

Certificate

RISE Research Institutes of Sweden AB, Notified Body No. 0402, hereby certifies that the manufacturer's technical file and the product have been inspected in accordance with the procedure described in Directive 2006/42/EG, the Machinery Directive, annex IX and found to fulfil the requirements, in respect of products listed in annex 4, paragraph 21 (Logic units to ensure safety functions).

The certification is verified by a type test in accordance with EN 61508 (SIL 2). According to EN 62061, the design of complex programmable electronic subsystems shall conform to the relevant requirements of EN 61508. By using Table 3 in EN ISO 13849-1:2015 it can be shown that this corresponds to PL d.

The Council Directive 2006/42/EC is implemented in Swedish Law by the national regulation AFS 2008:3. RISE Certification Rule SPCR 305 has been applied.

Miscellaneous

The manufacturer's information, in English, on installation and safety, has been inspected and found to fulfil the relevant requirements of the Directive.

Validity

This certificate was first issued on 2013-04-11 covering V3.00 of the embedded software. This updated and renewed certificate is based on, and covers, V 5.02.12 of the embedded software and remains valid as long as the conditions laid down in the specifications in reference are not modified significantly or at the latest until 2023-04-11.

Lennart Aronsson

Jan Jacobson

Certificate No. SC0534-13 | issue 4 | 2018-04-11

RISE Research Institutes of Sweden AB |
Box 857, SE-501 15 Borås, Sweden
Phone: +46 10-516 50 00
certifiering@ri.se| www.ri.se

SP

CEN CENELEC

THANKS!

Ted Strandberg

ted.strandberg@ri.se

+46 10 516 6093

Research Institutes of Sweden

SAFETY AND TRANSPORT
Electrification and Reliability