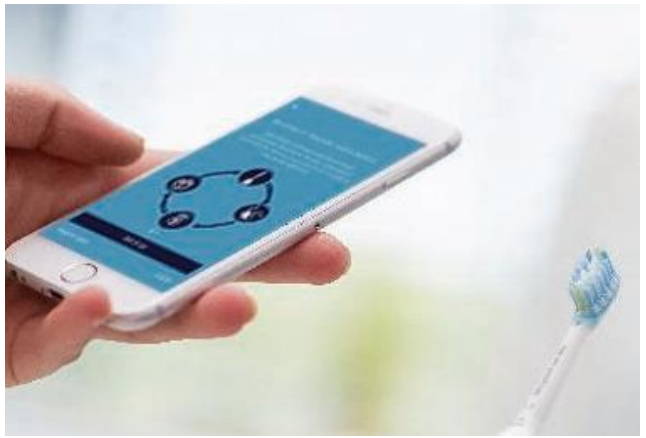
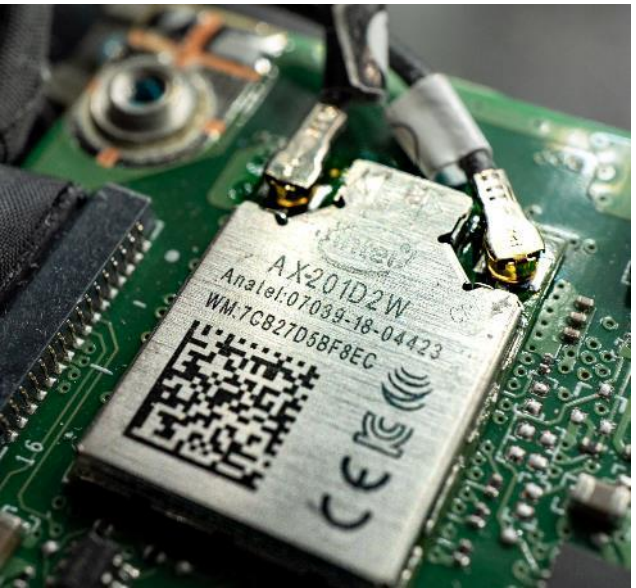
RED Delegated Act (EU) 2022/30 Standardization Request M585 ENQuiry Draft Review

CEN/CENELEC JTC 13/WG 8

2023-09-14

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 the commision:

- 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, ETSI, ANEC, APPLIA, EADPP, ENISA, ETUC, EURALARM, EUROSMART, GlobalPlatform, OSGP and SBMC
- 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	2023-11-16	
			+ 13 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	

Closing date for NEN = 2023-11-04

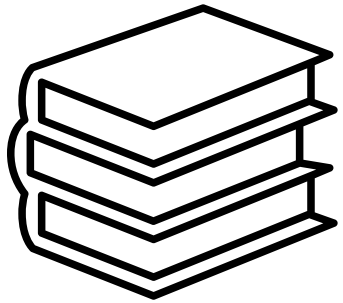
Introduction to the standards

prEN 18031-1 Common security requirements for radio equipment – Part 1: Internet connected radio equipment

prEN 18031-2 Common security requirements for radio equipment – Part 2: radio equipment processing data, namely Internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment

prEN 18031-3 Common security requirements for radio equipment – Part 3: Internet connected radio equipment processing virtual money or monetary value

Family of standards

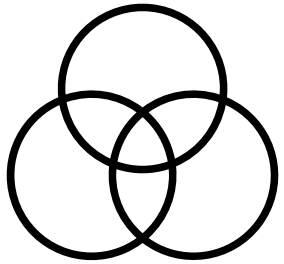


Each of the 3 standards address one of the essential requirements defined in articles 3.3.d, 3.3.e and 3.3.f of Directive 2014/53/EU and activated by the Commission Delegated Regulation (EU) 2022/30.

Document	Covers the essential requirements of	Addresses security assets and risks	Addresses network assets and risks	Addresses privacy assets and risks	Addresses financial assets and risks
prEN 18031-1 (JT013058)	3.3.(d)	✓	✓	×	×
prEN 18031-2 (JT013059)	3.3.(e)	✓	×	✓	×
prEN 18031-3 (JT013060)	3.3.(f)	✓	×	×	✓

Whether one or multiple standards need to be applied to a specific radio equipment is a consideration that must be made through a risk assessment by the economic operator.

Main requirements in the three standards

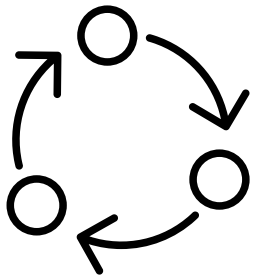


Requirement	3.3.(d)	3.3.(e)	3.3.(f)
[ACM] Access control mechanism	✓	✓	✓
[AUM] Authentication mechanism	✓	✓	✓
[SUM] Secure update mechanism	✓	✓	✓
[SSM] Secure storage mechanism	✓	✓	✓
[SCM] Secure communication mechanism	✓	✓	✓
[LGM] Logging mechanism	-	✓	✓
[DLM] Deletion mechanism	-	✓	-
[UNM] User notificiation mechanism	-	✓	-
[RLM] Resilience mechanism	✓	-	-
[NMM] Network monitoring mechanism	✓	-	-
[TCM] Traffic control mechanism	✓	-	-
[CCK] Confidential cryptographic keys	✓	✓	✓
[GEC] General equipment capabilities	✓	✓	✓
[CRY] Cryptography	✓	✓	✓

!

Note that the details of the requirements and assessment criteria and the number of sub-requirements will differ between the 3 standards.

Mechanisms, applicability & appropriateness



The standards use the concept of mechanisms to address specific security requirements to facilitate the applicability and appropriateness of the requirements to different types of equipment implementation and use.

The first requirement of a mechanism addresses the applicability. These requirements may have an ‘unless’ component that lists the potential conditions for which the mechanism is not required.

If it is determined that the mechanism is not applicable then all further requirements in that specific clause are no longer mandatory.

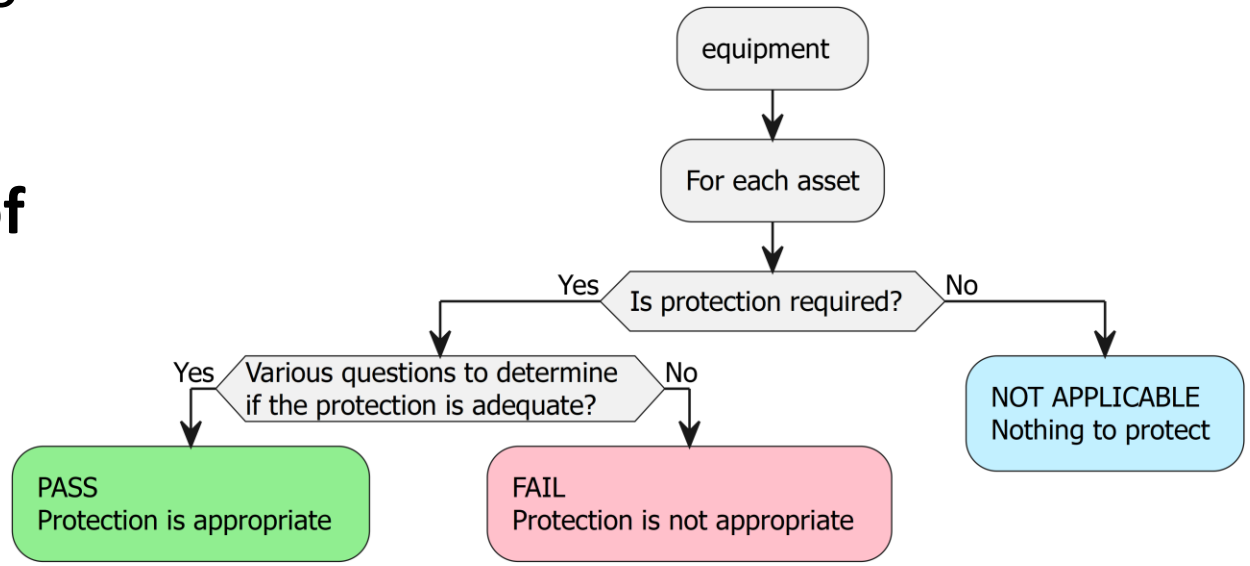
When a mechanism is required then the sufficiency is determined by evaluating the appropriateness type of the requirement and assessment criteria.

Any supporting requirements in the clause are applicable as well.

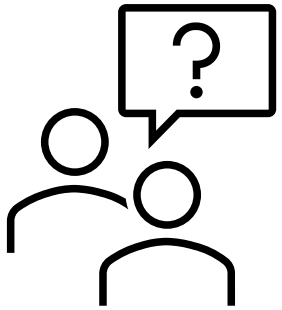
Decision trees

The standards provide **decision trees** to aid in the decision making and assessment to provide clear direction.

The decisions must be made for **each of the items specified**, for example when checking the applicability of a requirement on external interfaces, then the decision whether the appropriateness requirement and all further sub-requirements need to be fulfilled is determined for each external interface independently.



Example requirement – Applicability (3.3.d)



5 Requirements

5.1 [ACM] Access control mechanism

5.1.1 [ACM-1] Applicability of access control mechanisms

5.1.1.1 Requirement

The equipment shall use access control mechanisms to manage entities access to security assets and network assets, unless for security or network assets where:

— Its full public accessibility is the "equipment's reasonably foreseeable and intended use"; or

— the "foreseeable and intended operational environment of use" ensures that its accessibility is limited to authorized entities.

5.1.1.2 Rationale

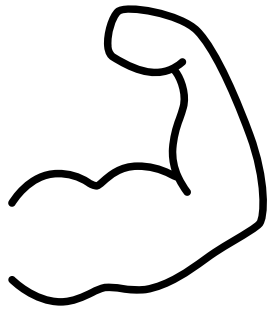
Security and network assets are exposed to unauthorized access attempts. Access control mechanisms limit the ability of any unauthorized entity to access these assets.

Examples of the influence of intended use and intended operational environment of use

These are just some examples, as we can't think of all exceptions for all equipment in all sectors and in all use cases!

- An external interface could be a network interface, some common network protocols such as DHCP (to obtain an IP address in the network) and NTP (to get current date/time from the network) are standard network **protocols that do not support access controls**
- Some equipment needs to be able to **communicate with legacy equipment**, in certain sectors like industrial environments a switch to secure protocols might take decades, therefor even new types of equipment must continue to support older (insecure) protocols
- Network segmentation significantly reduces the risk of using less secure network protocols (like mentioned above), and might be perceived as an adequate **security control measure in the network environment**
- A user interface of an industrial control system in a chemical plant might not have access controls as it always needs to be accessible at once, but with physical building access controls to enter the control room, it will be adequately protected as the environment provides **access controls in the physical world**
- Network interfaces that are **intended to be public**, for instance broadcasting Bluetooth advertising beacons, won't work with access controls

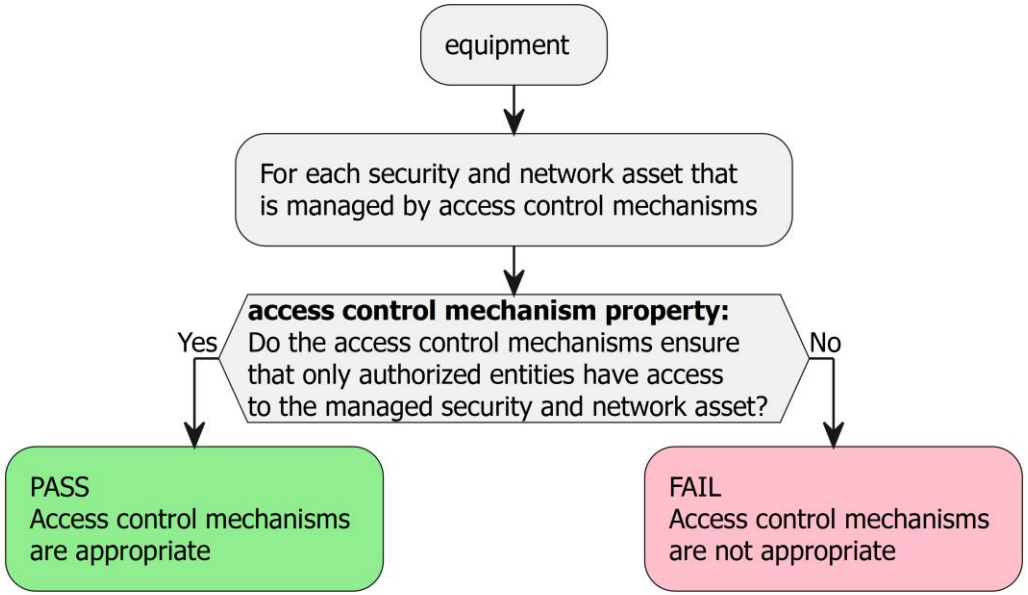
Example requirement – Appropriate (3.3.d)



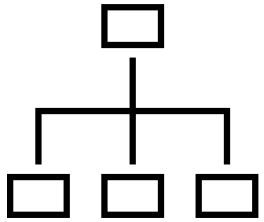
5.1.2 [ACM-2] Appropriate access control mechanisms

5.1.2.1 Requirement

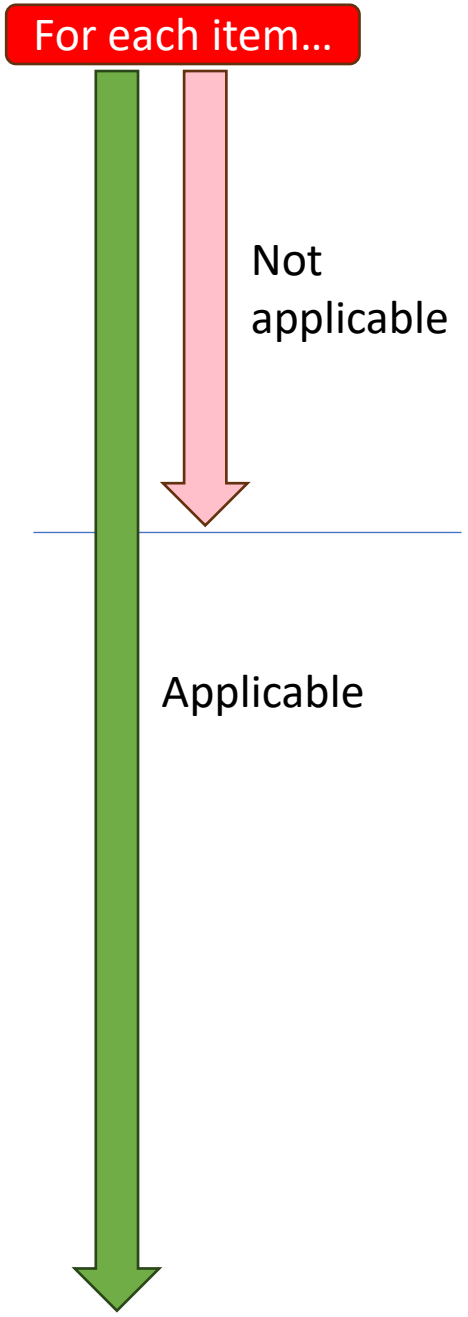
For each security and network asset that is managed by access control mechanisms, the access control mechanisms shall ensure that only authorized entities have access to the managed security and network assets.



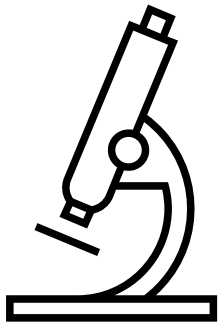
Structure (Clause 4)



Clause #	Title	Description on how to apply the standard
5.x	XXX **Mechanism**	Mechanism for each specific item (e.g., external interface or security asset)
5.x.1	XXX-1 **Applicability** of mechanisms	Applicability of the mechanism
5.x.1.1	Requirement	For each specific item determine and assess if the mechanism is required. Note: A mechanism might combine applicability and appropriateness in a single requirement.
5.x.1.2	Rationale	
5.x.1.3	Guidance	
5.x.1.4	Assessment criteria	
5.x.1.4.1	Assessment objective	
5.x.1.4.2	Required information	
5.x.1.4.3	Conceptual assessment	
5.x.1.4.4	Functional completeness assessment	
5.x.1.4.5	Functional sufficiency assessment	
5.x.2	XXX-2 **Appropriate** mechanisms	Appropriateness of the mechanism
5.x.2.1	Requirement	For each specific item for which the mechanism is required as determined by XXX-1, determine and assess if the mechanism is implemented sufficiently. Note: A mechanism might have multiple appropriateness sub-clauses to focus on specific properties.
5.x.2.2	Rationale	
5.x.2.3	Guidance	
5.x.2.4	Assessment criteria	
5.x.2.4.1	Assessment objective	
5.x.2.4.2	Required information	
5.x.2.4.3	Conceptual assessment	
5.x.2.4.4	Functional completeness assessment	
5.x.2.4.5	Functional sufficiency assessment	
5.x.y	XXX-# **Supporting** Requirements	Applicability and appropriateness of supporting requirements for the mechanism
5.x.y.1	Requirement	For each specific item for which the mechanism is required as determined by XXX-1, determine and assess if the supporting requirement needs to be implemented (there might be specific conditions, for instance if the equipment is a toy) and if it needs to be implemented, whether it is implemented sufficiently.
5.x.y.2	Rationale	
5.x.y.3	Guidance	
5.x.y.4	Assessment criteria	
5.x.y.4.1	Assessment objective	
5.x.y.4.2	Required information	
5.x.y.4.3	Conceptual assessment	
5.x.y.4.4	Functional completeness assessment	
5.x.y.4.5	Functional sufficiency assessment	



Assessments

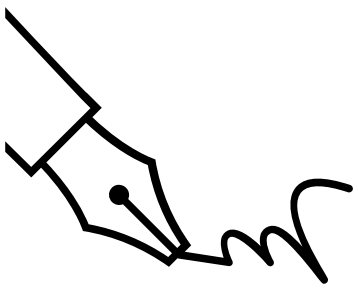


Assessments are conducted by examining the assessment cases, not all assessment cases might be provided for every mechanism:

- **Conceptual assessment**
  Examine if the provided documentation and rationale adequately provides the required evidence (for example the rationale why a mechanism is not applicable for a specific network interface).
- **Functional completeness assessment**
  Examine and test if the provided documentation is complete (for example use network scanners to verify that all external interfaces are properly identified, documented and assessed)
- **Functional sufficiency assessment**
  Examine and test if the implementation is adequate (for example run fuzzing tools on a network interface to check if it is resilient to attacks with malformed data)

Review suggestions

Review suggestions



- Provide comments via your national mirror committee(s) of CEN-CENELEC JTC 13 to ensure they are received and are processed in the formal ENQuiry.
- Start with reading “Annex A – Rationale” to understand the overall concepts used in the standards.
- **PLEASE** provide your comments with **line numbers**, **section numbers** and each comment with the proposed **corrected text** or **alternative proposals.**
- Check, align and provide comments across the three standards where possible (a lot of text is rather similar).
- Refrain from product type specific comments, please address any concerns in a general (horizontal) manner.

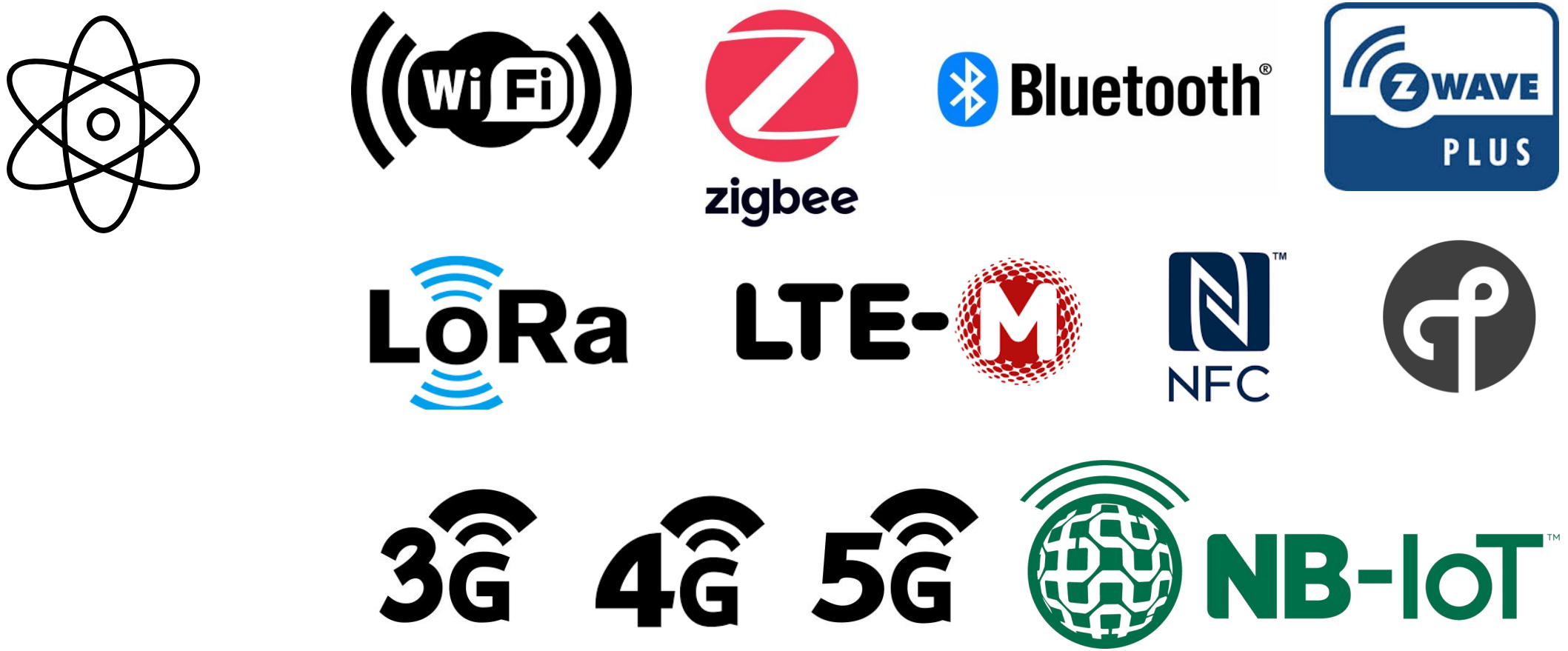
Overview main challenges

Most of the current (200+) RED harmonized standards have a very specific scope!

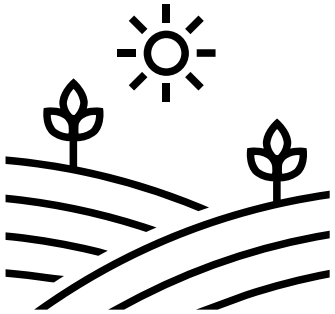
And these properties do not change over time, while cyber risks / vulnerabilities are a moving target

- **EN 302 977**
  Satellite Earth Stations and Systems (SES); Harmonised Standard for **Vehicle-Mounted Earth Stations (VMES) operating in the 14/12 GHz frequency bands** covering the essential requirements of article 3.2 of the Directive 2014/53/EU
- **EN 302 858-2**
  Electromagnetic compatibility and Radio spectrum Matters (ERM); Road Transport and Traffic Telematics (RTTT); **Automotive radar equipment operating in the 24,05 GHz up to 24,25 GHz or 24,50 GHz frequency range**; Part 2: Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive
- **EN 301 598**
  White Space Devices (WSD); **Wireless Access Systems operating in the 470 MHz to 790 MHz TV broadcast band**; Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive
- **EN 300 433**
  Citizens' Band (CB) radio equipment; Harmonised Standard covering the essential requirements of article 3.2 of the Directive 2014/53/EU
- **EN 301 406**
  Digital Enhanced Cordless Telecommunications (DECT); Harmonised Standard covering the essential requirements of Article 3(2) of Directive 2014/53/EU

Within short time, we need to address all products using various technologies in scope of (EU) 2022/30

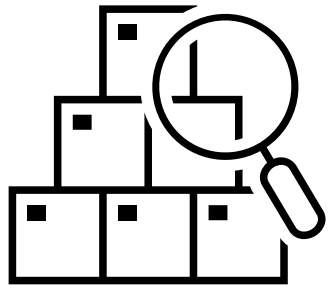


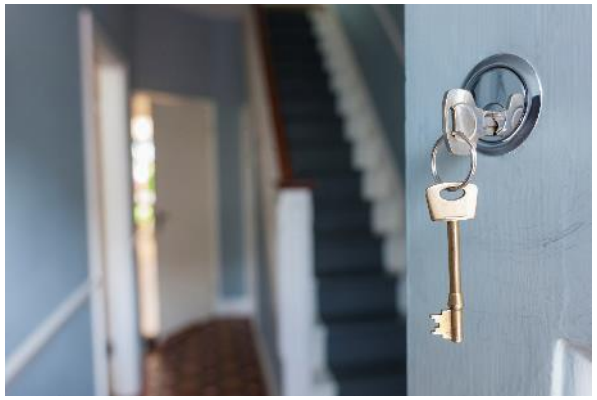
This horizontal scope includes a huge variety of equipment for vary different use environments…



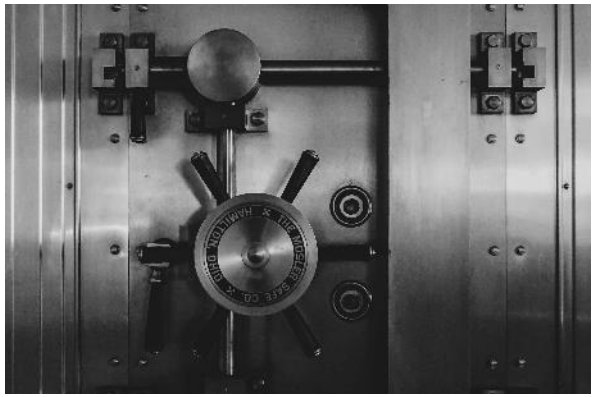
- Computers, cell phones, tablets, Single Board Computers, etc.
- Motor vehicles
- Civil aviation
- Road toll systems
- Childcare equipment
- Payment terminals (+ ATMs)
- Industrial equipment
- Agricultural equipment
- City automation
- Public transportation tracking systems
- Telecom infrastructure equipment
- Wireless networking equipment
  - Public infrastructure
  - Enterprise networks
  - Home routers
- Consumer IoT
  - Audio/video equipment
  - Home appliances
  - Home automation
  - Fitness equipment
  - Wearables
- Toys
- Any software product bundled with a (mini-)PC or other hardware (e.g., android tablet or Raspberry-Pi)!
- **And everything else using radio…** *except medical devices*

Requirement to “Protect the valuables in your house” has many appropriate solutions

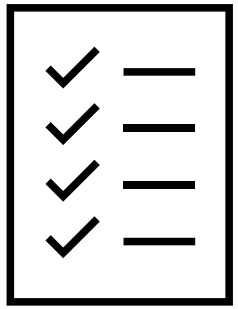




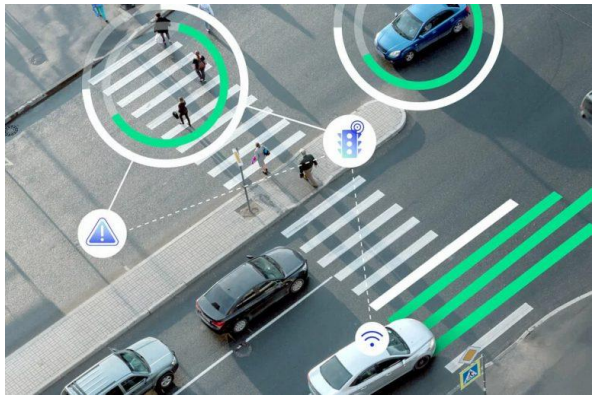
and combinations of…



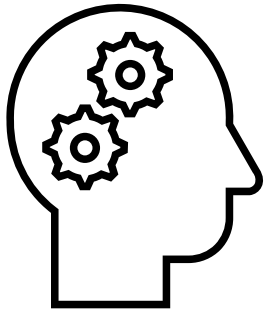
Also, the security protection levels that should be achieved are different across the various sectors



What is appropriate? (cost/benefit)



RED constrained to equipment requirements

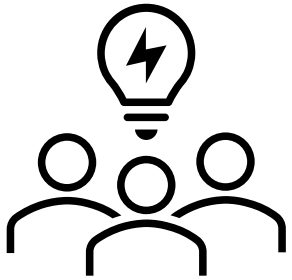


As cybersecurity threats and risk landscape are continuously changing, we typically address security with **security-by-design** processes and a **defense in depth** approach for the **equipment** itself and the **operational environment** it is used in, but under the RED we are constrained to **requirements for the equipment**.

Effective security management requires established security by design processes. This is not covered by these standards; they define **common security requirements** for equipment.

Note that we use the term "equipment" rather than term "product" as "radio equipment" is the legal term under the RED.

Addressing the horizontal scope

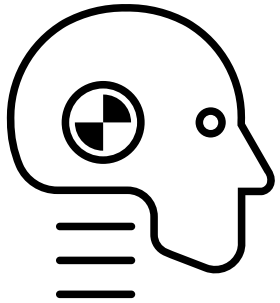


Another challenge is the **horizontal scope**, it soon became clear we could not discuss specific products while developing the standards as we got stuck in the details and conflicts.

If and how security objectives are to be achieved depends on the **intended use** and the **intended operational environment of use**. They influence the actual required implementation of security measures and the strength of those controls in a specific equipment.

A specific security measure might be appropriate for a product but might be too weak or strong for other products or even the same product when used in another environment.

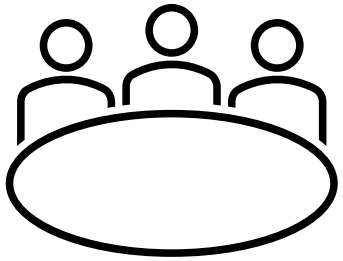
Security assessment & testing are subjective



Another main challenge is that the adequacy of most security mitigations are not measurable, there are no equivalents to a thermometer or frequency meter to measure the equipment's security posture or strict definitions when good is good enough, as:

- Many requirements are generic (addressing the horizontal scope);
- Intended use and the intended operational environment of use are unknown, and thus product specific risks are unknown;
- Most risks can be mitigated using all kind of different measures;
- We cannot “measure” the implementation strength of controls and even those that can, will lead to different outcomes (e.g., vulnerability scanners depend on the databases used and date the scan is run);
- Is dependent on the assessor’s knowledge and view of what is appropriate for a specific product in a specific environment;
- Security testing is partially done with negative testing (if you cannot break it in so many minutes/hours it is good enough, but it might break in the next second…, when do you stop?).

With these challenges, do the standards still achieve their goal?



- **YES**, as JTC 13/WG 8 experts we are confident that these standards will bring a significant improvement to the cybersecurity posture of products placed on the European market.
- These common security requirements and assessment criteria, of which some are only depending on documented evidence, does enforce the manufacturer to assess and address security risks for their product.
- The standards provide clear conditions on when and how to apply specific requirements, still recognizing the necessary implementation freedom, thereby also providing Market Surveillance Authorities with the appropriate tools to act.
- Very prescriptive requirements and assessment criteria could be addressed in product type specific (vertical) standards which can be developed on top of these horizontal standards (although this work most likely will be done under the CRA and not under the RED anymore).

Thank you,

Ben Kokx
Convenor of CEN-CENELEC JTC13/WG8

ben.kokx@philips.com