



European Standardization Organizations

CRA Standards Unlocked: From EN IEC 62443 to CRA: OT Cybersecurity for Important products Class I & II

*We start at
15:00 CET*



Els SOMERS

Project Manager

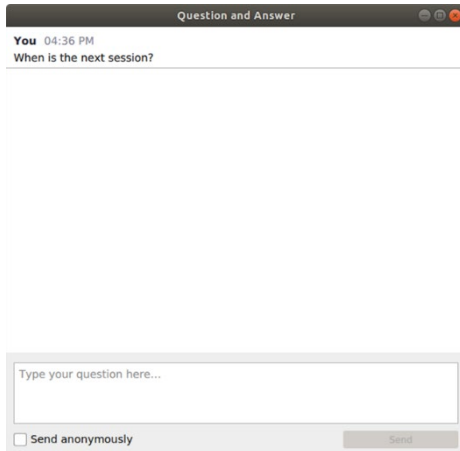
Public Relations

CEN-CENELEC

esomers@cencenelec.eu

Get the most out of the webinar today

- ▶ You are muted
- ▶ Use the Q&A panel to submit your questions



Question and Answer

You 04:36 PM
When is the next session?

Type your question here...

☐ Send anonymously Send

- ▶ Talk about us with #training4standards #standards4CRA
 - ▶ On X [@Standards4EU](#)
 - ▶ On Bluesky [@cen-cenelec.bsky.social](#)
 - ▶ On LinkedIn www.linkedin.com/company/cen-and-cenelec

► Introduction

- CRA standards and the standardization request
- What is a harmonized standard?
- Technical work
- Funding opportunities

► Presentation on CRA Standards Unlocked: From EN IEC 62443 to CRA: OT Cybersecurity for Important products Class I & II' (Rapporteur Srinath Pydi Narayana Rao)

Your speakers today



Lucia LANFRI

Project Manager Electrotechnology
Standardization & Digital Solutions



Srinath Pydi NARAYANA RAO

Rapporteur CLC/TC 65X WG 3,
work items related to OT of
several CRA standardization
deliverables

- ▶ A **Standardization Request (SReq)** is a formal document issued by the European Commission (EC) to European Standardization Organizations (ESOs)—namely CEN, CENELEC, and ETSI—asking them to **develop, revise, or update harmonized standards** to support **EU policies or legislation**.
- ▶ M/606 “CRA” : [eNorm Platform](#)
- ▶ This request was accepted by CEN, CENELEC and ETSI

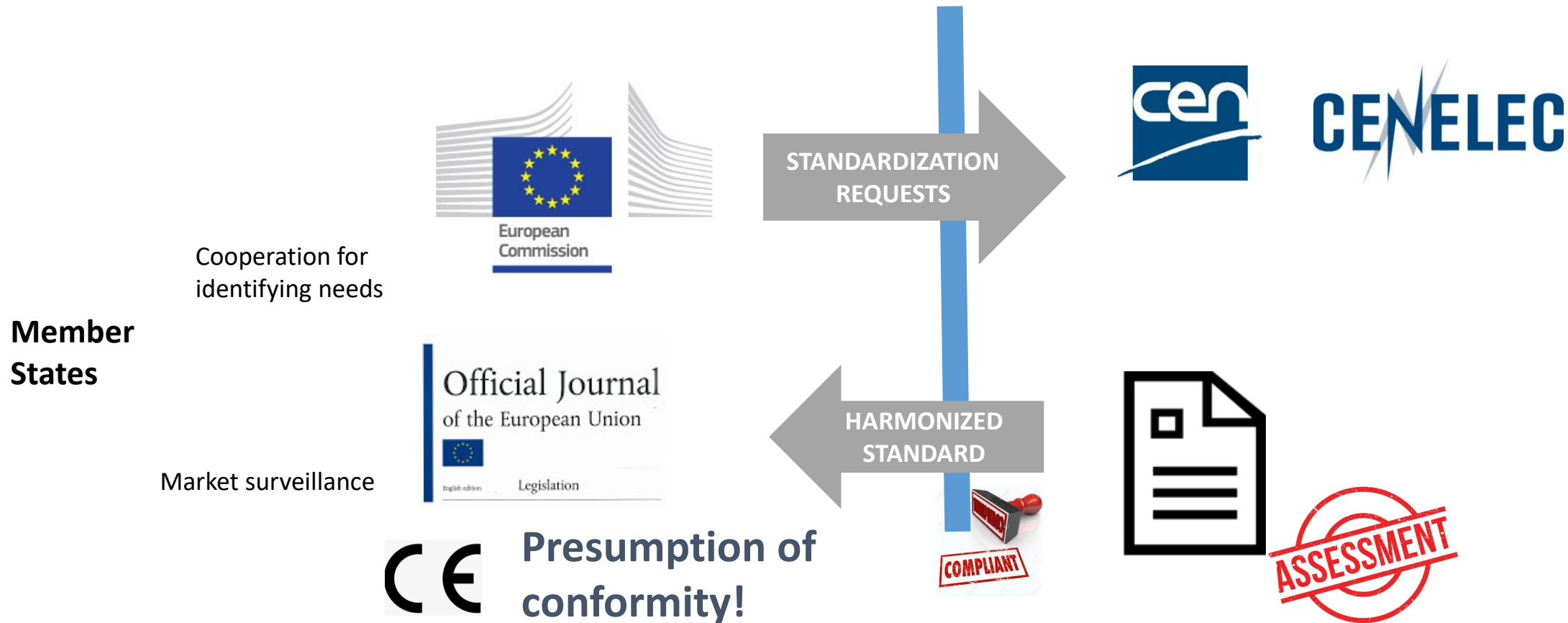
What is a harmonized standard?



- ▶ A harmonized standard is a European standard developed by recognized European Standards Organizations.
- ▶ It is created following a standardization request from the European Commission to one of these organizations
- ▶ Their use is voluntary
- ▶ Manufacturers, other economic operators, or conformity assessment bodies can use harmonized standards to demonstrate that products, services, or processes comply with relevant EU legislation. They are free to choose another technical solution to demonstrate compliance with the mandatory legal requirements.
- ▶ The CRA is a first of its kind regulation, so no standards currently exist that specifically cover the CRA essential requirements.

Regulation 1025/2012 – Assessment, citation and Presumption of conformity

Reflects regulatory objectives!

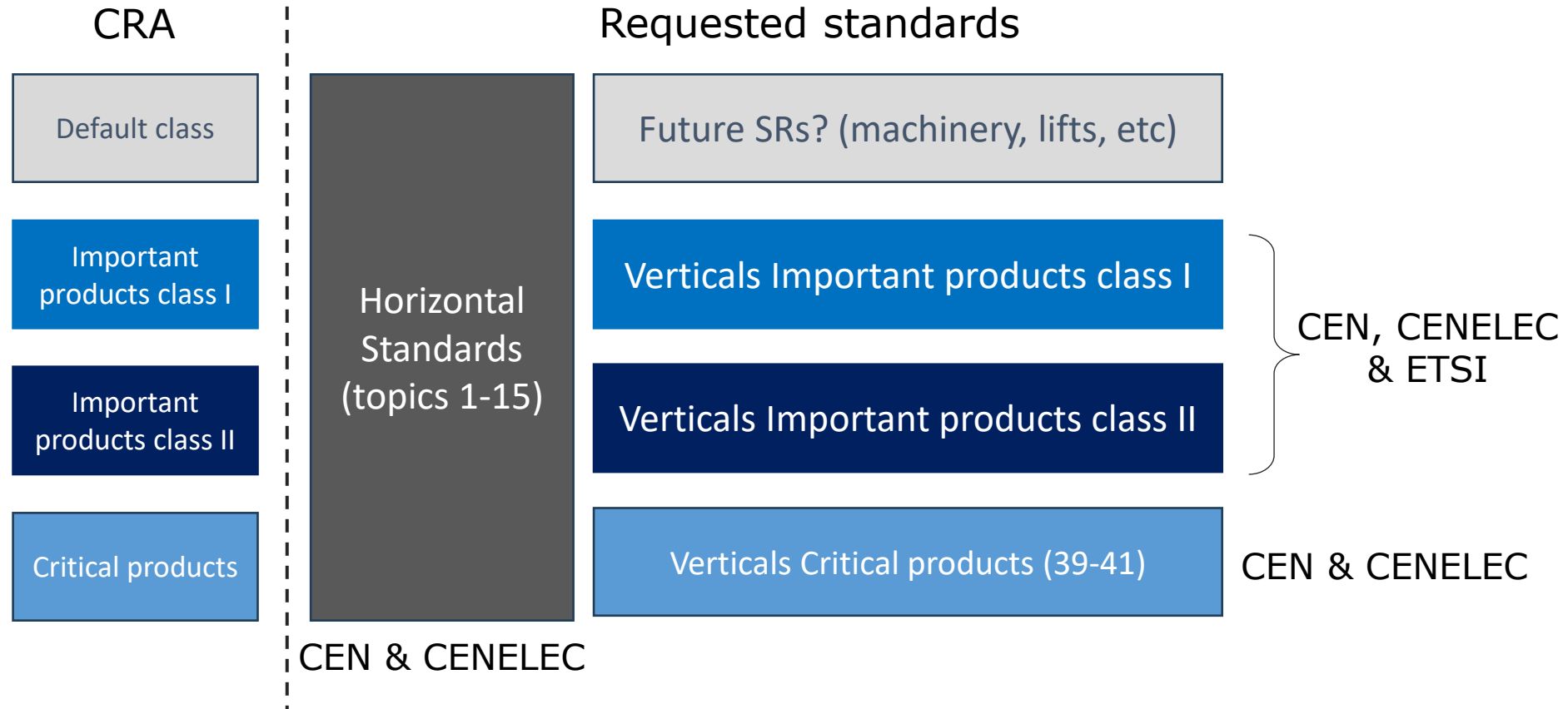


CRA Harmonized standards

- ▶ Standards requested and work programme
- ▶ How is the work organized?
- ▶ What are the timelines?
- ▶ How to participate?

Requested standards

41 topics, 2 'types' of deliverables: horizontals and verticals



Correlation between the requested standards on M/606 and the technical committees at CEN, CENELEC and ETSI



ANNEX I
List of new European Standards to be drafted

Reference information		Deadline for the adoption by the ESOs
Horizontal standards for security requirements relating to the properties of products with digital elements		
1.	European standard(s) on designing, developing and producing products with digital elements in such a way that they ensure an appropriate level of cybersecurity based on the risks	30/08/2026
2.	European standard(s) on making products with digital elements available on the market without known exploitable vulnerabilities	30/10/2027
3.	European standard(s) on making products with digital elements available on the market with a secure by default configuration	30/10/2027
4.	European standard(s) on ensuring that vulnerabilities in products with digital elements can be addressed through security updates	30/10/2027
5.	European standard(s) on ensuring protection of products with digital elements from unauthorised access and reporting on possible unauthorised access	30/10/2027
6.	European standard(s) on protecting the confidentiality of data stored, transmitted or otherwise processed by a product with digital elements	30/10/2027
7.	European standard(s) on protecting the	30/10/2027

M/606	Technical Committee(s)		Standard title	Last realized stage	Deadline for adoption
Topics M/606 - Annex I	TC ref.	TC title			
Line 1: European standard(s) on designing, developing and producing products with digital elements in such a way that they ensure an appropriate level of cybersecurity based on the risks					
1	CEN-CLC/ITC 13 WG 9	Cybersecurity and Data Protection	Cybersecurity requirements for products with digital elements — Principles for cyber resilience	10.99 - NWI - New Work Item adopted	2026/08/30
Lines 2-14 - European standard(s) CRA essential requirements					
2 to 14	CEN-CLC/ITC 13 WG 9	Cybersecurity and Data Protection	Cybersecurity requirements for products with digital elements – Generic Security Requirements	10.99 - NWI - New Work Item adopted	2027/10/30
Line 15: European standard(s) on vulnerability handling for products with digital elements					
15	CEN-CLC/ITC 13 WG 9	Cybersecurity and Data Protection	Cybersecurity requirements for products with digital elements – Vulnerability Handling	10.99 - NWI - New Work Item adopted	2026/08/30
Line 16: European standard(s) on essential cybersecurity requirements for identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers					
16	CEN/TC 224 WG 17	Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment	Identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers : criteria to fulfill with the essential requirements from regulation 2024/2487 (CRA)	TC decision taken	2026/10/30
Line 17: European standard(s) on essential cybersecurity requirements for standalone and embedded browsers					
17a	ETSI CYBER-EUSR	ETSI TC Cyber Working Group for EUSR	European standard(s) on essential cybersecurity requirements for embedded browsers	PWI - Proposed Work Item created	2026/10/30
17b	ETSI CYBER-EUSR	ETSI TC Cyber Working Group for EUSR	European standard(s) on essential cybersecurity requirements for standalone browsers	PWI - Proposed Work Item created	2026/10/30
Line 18: European standard(s) on essential cybersecurity requirements for password managers					
18	ETSI CYBER-EUSR	ETSI TC Cyber Working Group for EUSR	European standard(s) on essential cybersecurity requirements for password managers	PWI - Proposed Work Item created	2026/10/30
Line 19: European standard(s) on essential cybersecurity requirements for software that searches for, removes, or quarantines malicious software					
19	ETSI CYBER-EUSR	ETSI TC Cyber Working Group for EUSR	European standard(s) on essential cybersecurity requirements for software that searches for, removes, or quarantines malicious software	PWI - Proposed Work Item created	2026/10/30
Line 20: European standard(s) on essential cybersecurity requirements for products with digital elements with the function of virtual private network (VPN)					
20a	ETSI CYBER-EUSR	ETSI TC Cyber Working Group for EUSR	European standard(s) on essential cybersecurity requirements for products with digital elements with the function of virtual private network (VPN)	PWI - Proposed Work Item created	2026/10/30
20b	CLC/TC 65X WG 3	Industrial-process measurement, control and automation	Security Profile for products with digital elements with the function of virtual private network (VPN)	00.60 - PWI - Preliminary Work Item created	2026/10/30
Line 21: European standard(s) on essential cybersecurity requirements for network management systems					
21a	ETSI CYBER-EUSR	ETSI TC Cyber Working Group for EUSR	European standard(s) on essential cybersecurity requirements for network management systems	PWI - Proposed Work Item created	2026/10/30
21b	CLC/TC 65X WG 3	Industrial-process measurement, control and automation	Security Profile for network management systems (based on IEC 62443)	00.60 - PWI - Preliminary Work Item created	2026/10/30
Line 22: European standard(s) on essential cybersecurity requirements for Security information and event management (SIEM) systems					
22a	ETSI CYBER-EUSR	ETSI TC Cyber Working Group for EUSR	European standard(s) on essential cybersecurity requirements for Security information and event management (SIEM) systems	PWI - Proposed Work Item created	2026/10/30
22b	CLC/TC 65X WG 3	Industrial-process measurement, control and automation	Security Profile for security information and event management (SIEM) systems (based on IEC 62443)	00.60 - PWI - Preliminary Work Item created	2026/10/30
Line 23: European standard(s) on essential cybersecurity requirements for boot managers					
23	ETSI CYBER-EUSR	ETSI TC Cyber Working Group for EUSR	European standard(s) on essential cybersecurity requirements for boot managers	PWI - Proposed Work Item created	2026/10/30

Important products under the CRA

CEN/TC 224 WG 17

ETSI TC Cyber EUSR

CLC/TC 47X WG 1-4

CLC/TC 65X WG 3

CEN-CLC/JTC 13 WG 6

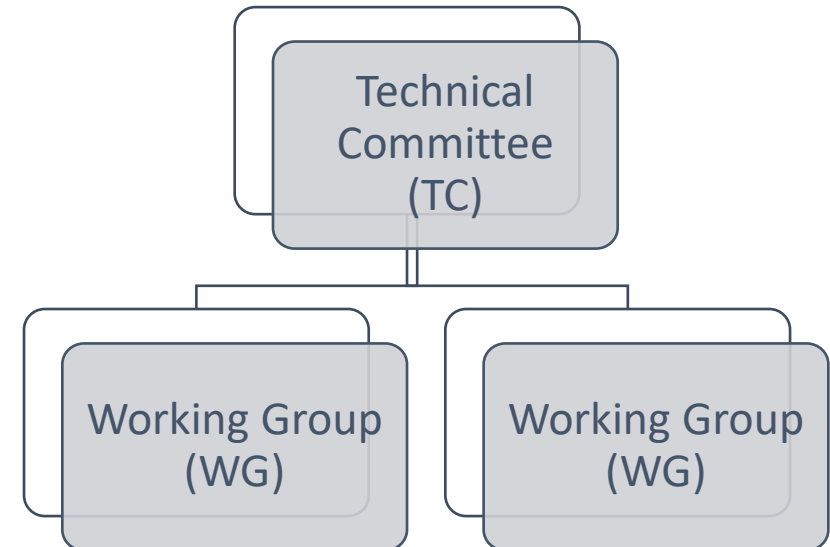
CLC/TC 65X 'Industrial-process measurement, control and automation'

Developments on vertical standards based on EN IEC 62443 series

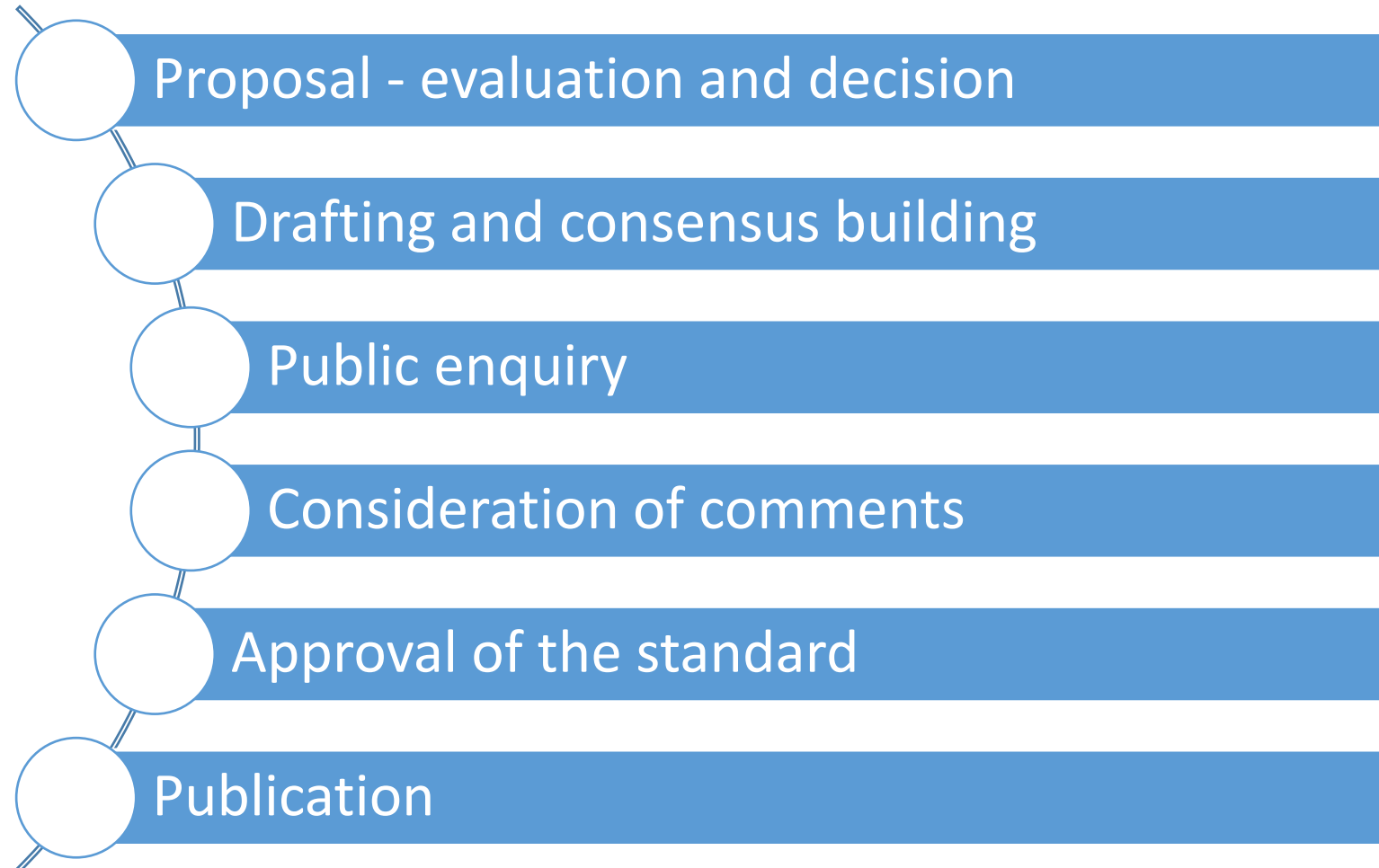
- products with digital elements with the function of virtual private network (VPN) (#20)
- network management systems (#21)
- Security information and event management (SIEM) systems (#22)
- physical and virtual network interfaces (#25)
- routers, modems intended for the connection to the internet, and switches (#27)
- firewalls, intrusion, detection and/or prevention systems, including specifically those intended for industrial use (#36)

How is the work organized?

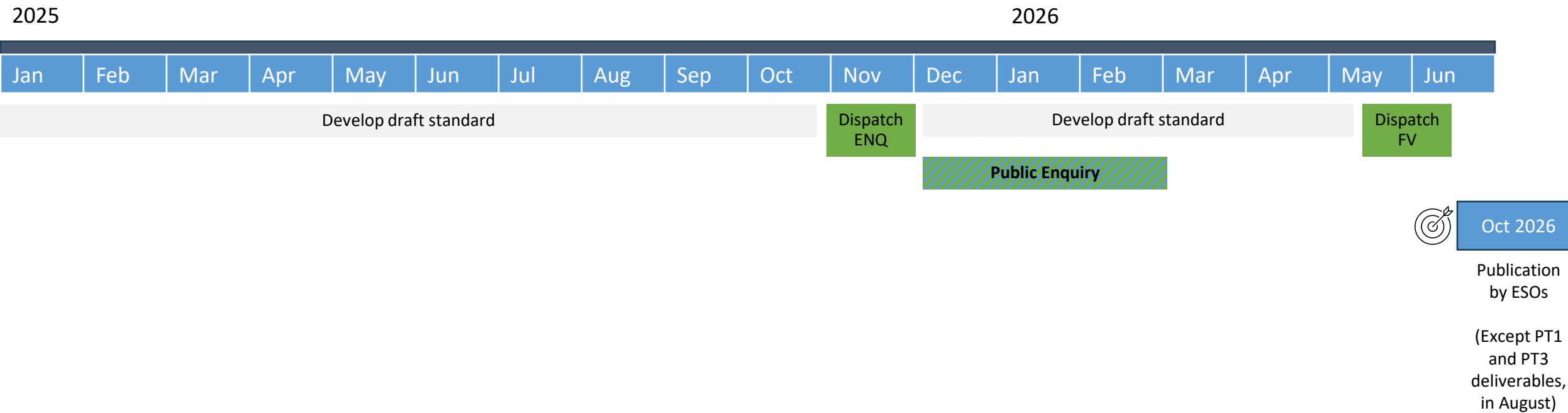
- ▶ The standards are developed in Technical Committees (TC)
- ▶ Each TC has Working Groups (WGs)
- ▶ Each WG has a dedicated scope



How are standards made?

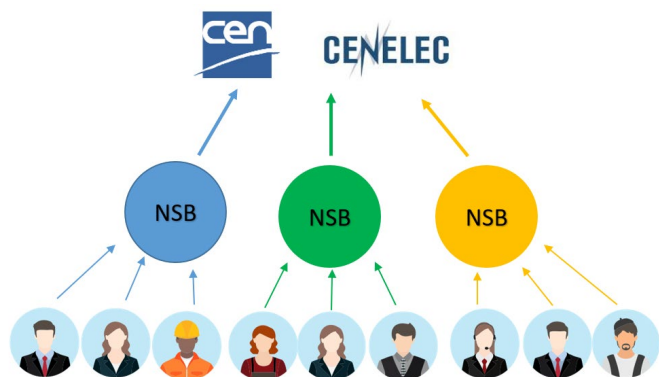


High level expected timeline



How to participate?

- CEN and CENELEC Members in 34 countries
- Participation can take place via the national members



How to participate?

Does your organization
have European
headquarters?



Yes

In which country?

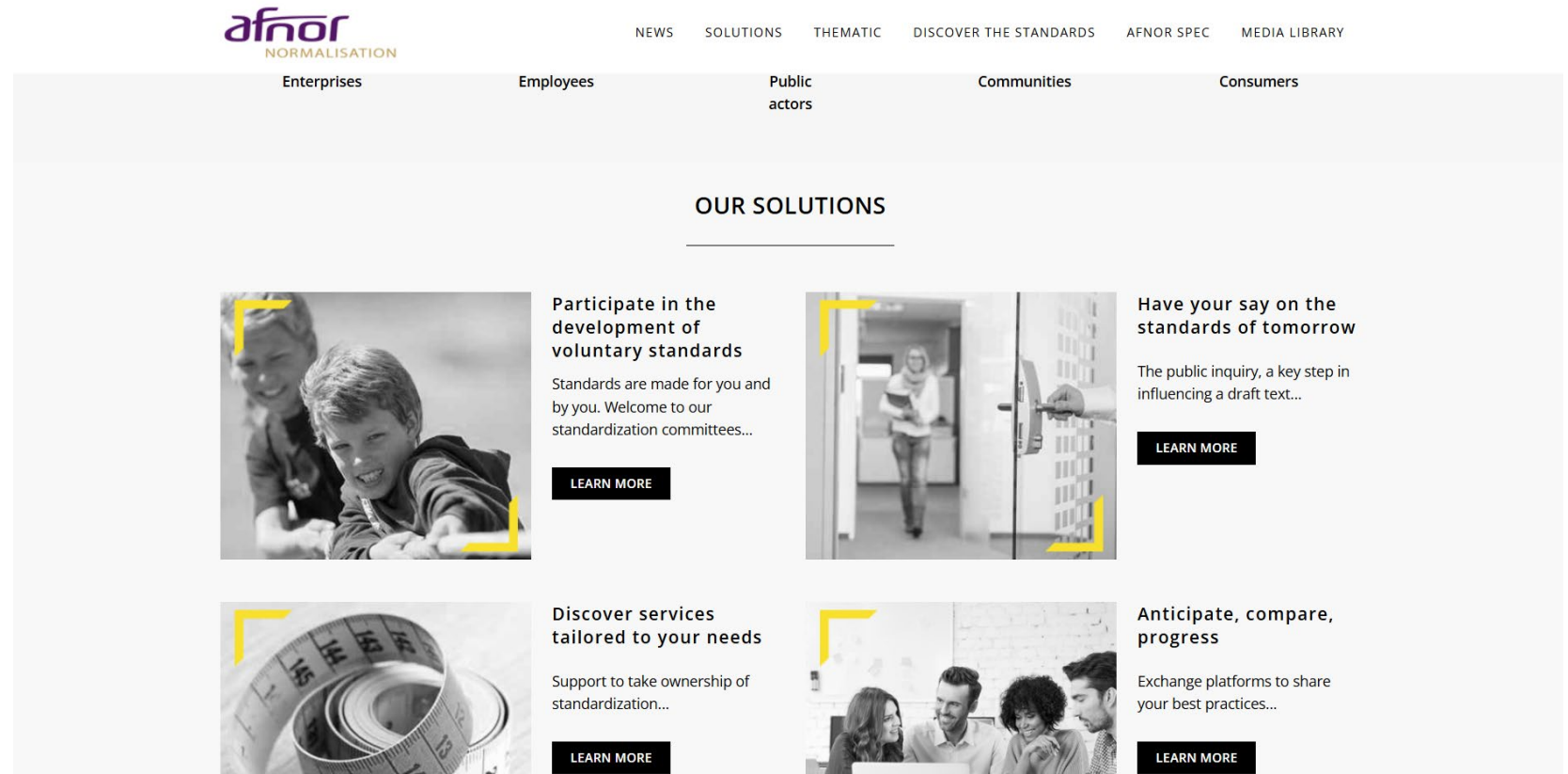
Example: France

Search for your
national committee







Each national committee has a website

- Overview of CEN Members: [link](#)
- Overview of CENELEC Members: [link](#)



The screenshot displays the AFNOR website's 'OUR SOLUTIONS' section. The header includes the AFNOR logo and navigation links: NEWS, SOLUTIONS, THEMATIC, DISCOVER THE STANDARDS, AFNOR SPEC, and MEDIA LIBRARY. Below the header, a row of categories is visible: Enterprises, Employees, Public actors, Communities, and Consumers. The main content area is titled 'OUR SOLUTIONS' and features four cards, each with an image, a title, a brief description, and a 'LEARN MORE' button.

Image	Title	Description	Button
	Participate in the development of voluntary standards	Standards are made for you and by you. Welcome to our standardization committees...	LEARN MORE
	Have your say on the standards of tomorrow	The public inquiry, a key step in influencing a draft text...	LEARN MORE
	Discover services tailored to your needs	Support to take ownership of standardization...	LEARN MORE
	Anticipate, compare, progress	Exchange platforms to share your best practices...	LEARN MORE

Fun Debate



800+



Webinar's Topic



Renowned Speaker





EUROPEAN COMMITTEE
FOR ELECTROTECHNICAL STANDARDIZATION

EN IEC 62443 Series to CRA

OT Cybersecurity for Important Products Class I & II

Know your Speaker



- ▶ I'm Srinath PYDI NARAYANA RAO – “yes, my name is long”
- ▶ Based in Paris, France and originally from Chennai, India
- ▶ Lead Rapporteur for OT related CRA activities “CLC/TC 65X WG3 Cyber Security”
- ▶ Lead OT Cybersecurity Consultant at Internet of Trust
- ▶ 4 years of experience in OT-IT-5G cybersecurity consulting
- ▶ 9 years of experience in process automation at Schneider Electric Systems
- ▶ Senior ISA member
- ▶ Certified IEC 62443 IC32 Fundamental Specialist



- ▶ Established in February 2020
- ▶ Scope
 - ▶ Observing the cybersecurity activities on IEC, ISO and other standardization bodies and fora
 - ▶ European mirror of IEC TC 65/WG10 (*"cybersecurity for operational technologies"*), responsible for the development of the IEC 62443 series
 - ▶ Responsible for **adopting the IEC 62443 series to support the Single European Market**
- ▶ Liaisons
 - ▶ CEN-CLC JTC13 *"Cybersecurity and data protection"*: WG8 (Delegated Regulation RED), WG9 (CRA)
 - ▶ CLC/TC 44X *"Safety of Machinery"*: WG2 (*"Protection against corruption"*)
- ▶ Convenors
 - ▶ Judith Rossebo, Kai Wollenweber
- ▶ Rapporteur
 - ▶ Srinath Pydi Narayana Rao

The EU "Cyber Resilience Act" specifies

- rules for the making available on the market of products with digital elements (PDEs) to ensure the cybersecurity of such products
- **essential cybersecurity requirements for the design, development and production** of PDEs, and obligations for economic operators in relation to those products with respect to cybersecurity
- **essential cybersecurity requirements for the vulnerability handling processes** put in place by manufacturers to ensure the cybersecurity of PDEs during the time the products are expected to be in use, ...
- rules on market surveillance, including monitoring, and enforcement of the rules and requirements

Presumption of conformity provided by

- **harmonized standards** (hENs) published in the Official Journal of the EU (OJEU)
- common specifications
- cybersecurity certification schemes adopted pursuant to (EU) 2019/881 (EU CSA)

- ▶ Standards are technical specifications and are therefore useful and effective in promoting and disseminating *"good technical practices"* and *"technical solutions"*.
- ▶ **Standards are in themselves of voluntary application.**
 - ▶ → EN IEC 62443-based hENs are only an option
- ▶ **Manufacturers**, even when using harmonised standards, the references of which are published in the OJEU, **remain fully responsible for assessing all the risks of their product** to determine which essential (or other) requirements are relevant.
- ▶ Suppose references to harmonized standards have been published in the Official Journal of the European Union (OJEU). In that case, they provide a ***presumption of conformity*** with the essential or other legislative requirements they aim to cover.
- ▶ A harmonised standard may contain specifications relating not only to essential requirements but also to other non-regulated issues.

Definition by **IEC TC 65 JAG26**

(Horizontal security function for OT linked to TC 9, TC 44, TC 57, TC 61, ISO/IEC JTC 1/SC 27)

Operational Technology (OT)

Technology for detecting, managing or causing change through the monitoring or control of a physical entity.

Machinery

HMIs

DCS, RTU & PLCs

Sensors & Detectors

Automation Software's

Embedded Computes

CRA for OT & EN IEC-62443 Series



CRA Standards for OT Products



EN IEC-62443 Series Standards

Why hENs based on the EN IEC 62443 series?



EN IEC 62443 series

- ▶ is widely used and accepted by the market, specifically in industrial environments and critical infrastructures
 - ▶ Maritime (IACS UR E26 "Cyber Resilience of Ships", E27 "Cyber Resilience of On-Board Systems and Equipment")
 - ▶ Railway (TS 50701 "Railway applications – Cybersecurity")
 - ▶ Medical
 - ▶ ...
- ▶ provides a mature basis for the development of related hENs → timely availability of hENs
- ▶ can rely on an expert community within standardization → timely availability of hENs
- ▶ includes procedures to derive product / product-group / vertical specific hENs ("profile")
- ▶ provides the possibility to broaden the scope to overcome the focus on "*Industrial Automation Control Systems (IACS)*"

Overview IEC 62443 series



IEC 62443											
Security for Industrial Automation and Control Systems											
General		Policies & Procedures		System		Component		Security Profiles		Evaluation	
1-1	Terminology, concepts and models	2-1	Security program requirements for IACS asset owners	3-1	Security technologies for IACS	4-1	Secure product development lifecycle requirements	5-x	IEC 62443 security profile x	6-1	Security evaluation methodology for IEC 62443-2-4
		2-2	IACS security protection scheme	3-2	Security risk assessment for system design	4-2	Technical security requirements for IACS components			6-2	Security evaluation methodology for IEC 62443-4-2
1-3	Performance metrics for IACS security	2-3	Patch management in the IACS environment	3-3							
1-4	IACS security lifecycle and use-cases	2-4	Security program requirements for IACS service providers								
1-5	Scheme for IEC 62443 security profiles	2-5	Implementation guidance for IACS asset owners								
1-6	Application of the IEC 62443 standards to the Industrial Internet of Things										

Overview EN IEC 62443 series



EN IEC 62443					
Security for Industrial Automation and Control Systems					
General		Policies & Procedures		System	
				Component	
				Security Profiles	
				Evaluation	
1-1	Terminology, concepts and models	2-1	Security program requirements for IACS asset owners	3-1	Security technologies for IACS
		2-2	IACS security protection scheme	3-2	Security risk assessment for system design
1-3	Performance metrics for IACS security	2-3	Patch management in the IACS environment	3-3	System security requirements and security levels
1-4	IACS security lifecycle and use-cases	2-4	Security program requirements for IACS service providers		
1-5	Scheme for IEC 62443 security profiles	2-5	Implementation guidance for IACS asset owners		
1-6	Application of the IEC 62443 standards to the Industrial Internet of Things				
				4-1	Secure product development lifecycle requirements
				4-2	Technical security requirements for IACS components
				5-x	IEC 62443 security profile x
				6-1	Security evaluation methodology for IEC 62443-2-4
				6-2	Security evaluation methodology for IEC 62443-4-2

In progress / parallel vote

Published / adopted

CRA relevant parts of (EN) IEC 62443 series



Proposal of EU Cyber Resilience Act

Annex I, Part I
Cybersecurity requirements



Annex I, Part II
Vulnerability handling
requirements



Annex II
Information and
instructions to the user



Annex VII
Technical documentation



EN IEC 62443-4-1

EN IEC 62443-4-2

EN IEC 62443-3-3

- ▶ **EN IEC 62443-4-2 “Technical security requirements for IACS components”**
 - ▶ Scope: “Product” = (IACS) components
 - ▶ Application of EN IEC 62443-4-1 mandatory
 - ▶ Covers EU CRA Annex I Part I (2) Essential Cybersecurity Requirements

- ▶ **EN IEC 62443-3-3 “System security requirements and security levels”**
 - ▶ Scope: “Product” = (Control) system (incl. machines), consisting of (IACS) components
 - ▶ Covers EU CRA Annex I Part I (2) Essential Cybersecurity Requirements

- ▶ **EN IEC 62443-4-1 “Secure product development lifecycle requirements”**
 - ▶ Mandatory application specified in EN IEC 62443-4-2
 - ▶ Covers EU CRA Annex I Part I (1) and Part II Essential Cybersecurity Requirements

- ▶ **IEC TS 62443-6-2 “Security evaluation methodology for IEC 62443-4-2” (Draft)**
 - ▶ Procedure for evaluating IEC 62443-4-2 requirements that have been implemented in a product following an IEC 62443-4-1 compliant secure product development lifecycle

- ▶ **EN IEC TS 62443-1-5 “Scheme for IEC 62443 security profiles”**
 - ▶ Procedure for specifying “security profiles”

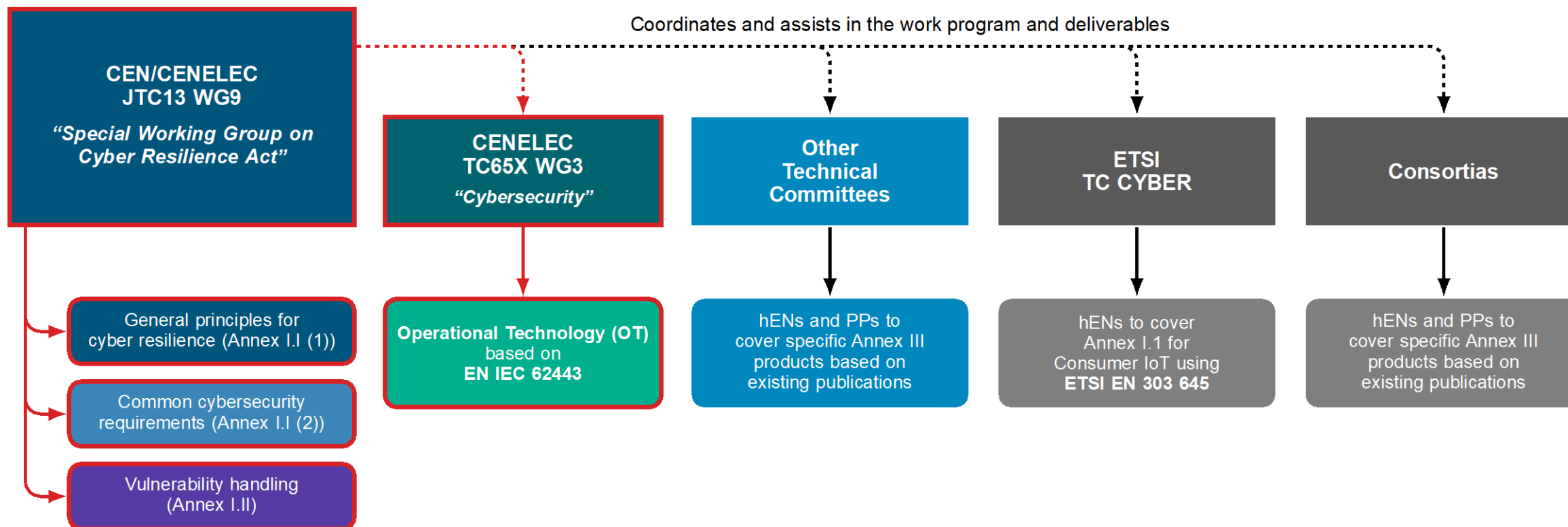
CRA relevant parts of (EN) IEC 62443 series



EN IEC 62443					
Security for Industrial Automation and Control Systems					
General		Policies & Procedures		System	
				Component	
				Security Profiles	
				Evaluation	
1-1	Terminology, concepts and models	2-1	Security program requirements for IACS asset owners	3-1	Security technologies for IACS
		2-2	IACS security protection scheme	3-2	Security risk assessment for system design
1-3	Performance metrics for IACS security	2-3	Patch management in the IACS environment	3-3	System security requirements and security levels
1-4	IACS security lifecycle and use-cases	2-4	Security program requirements for IACS service providers		
1-5	Scheme for IEC 62443 security profiles	2-5	Implementation guidance for IACS asset owners		
1-6	Application of the IEC 62443 standards to the Industrial Internet of Things				

	Process Requirements
	Technical Requirements
	Evaluation Requirements

EU CRA: CEN-CENELEC organizational structure



EU CRA: CEN-CENELEC standardization framework

CEN/CLC JTC13 WG9 focus



“Horizontal”

General principles for cyber resilience (PT1)

Annex I, Part I (1)

Common cybersecurity requirements (PT2)

Annex I, Part I (2)

Vulnerability handling (PT3)

Annex I, Part II

“Vertical”

Important / Critical products with digital elements

Routers, modems, switches

Standalone and embedded browsers

...

CLC/TC65X WG3

Operational Technology (OT)

based on EN IEC 62443 series

Routers, modems, switches

...

...



Intended to be cited in the OJEU

EU CRA: CEN-CENELEC standardization framework

Other TCs, except CLC/TC 65X WG3



“Horizontal”

General principles for cyber resilience (PT1)

Annex I, Part I (1)

Common cybersecurity requirements (PT2)

Annex I, Part I (2)

Vulnerability handling (PT3)

Annex I, Part II

“Vertical”

Important / Critical products with digital elements

Routers, modems, switches

Standalone and embedded browsers

...

CLC/TC65X WG3

Operational Technology (OT)

based on EN IEC 62443 series

Routers, modems, switches

...

...



Intended to be cited in the OJEU

EU CRA: CEN-CENELEC standardization framework

CLC/TC65X WG3 focus



“Horizontal”

General principles for cyber resilience (PT1)

Annex I, Part I (1)

Common cybersecurity requirements (PT2)

Annex I, Part I (2)

Vulnerability handling (PT3)

Annex I, Part II

“Vertical”

Important / Critical
products with digital elements

Routers, modems, switches

Standalone and embedded browsers

...

CLC/TC65X WG3

Operational Technology (OT)

based on EN IEC 62443 series

Routers, modems, switches

...

...



Intended to be cited in the OJEU

“Horizontal”

General principles for cyber resilience (PT1)

Annex I, Part I (1)

Common cybersecurity requirements (PT2)

Annex I, Part I (2)

Vulnerability handling (PT3)

Annex I, Part II

“Vertical”

Important / Critical products with digital elements

Routers, modems, switches

Standalone and embedded browsers

...

CLC/TC65X WG3

Operational Technology (OT)

based on EN IEC 62443 series

Routers, modems, switches

...

...



Intended to be cited in the OJEU

EU CRA: EN IEC 62443 based standardization framework

“Broad OT verticals”




Operational Technology (OT)

based on EN IEC 62443-4-1
Secure product development lifecycle

?

based on EN IEC 62443-4-2
(products = components)

based on EN IEC 62443-3-3
(products = systems)

 Intended to be cited in the OJEU

An IEC 62443 security profile is a defined subset of IEC 62443 requirements, which are contextually mapped e.g., to:

- ▶ a **specific application domain** (e.g., discrete manufacturing, process industry);
- ▶ an **area of activity** (e.g., integration, patch management);
- ▶ the **intended operational environment and the security context** of a product (component, system) or automation solution within that environment; or
- ▶ **particular type(s) of product(s).**

CRA Standardization Request (Annex I)

Class I: European standard(s) on essential cybersecurity requirements for

- ▶ #20: products with digital elements with the function of virtual private network (VPN)
- ▶ #21: network management systems
- ▶ #22: Security information and event management (SIEM) systems
- ▶ #25: physical and virtual network interfaces
- ▶ #27: routers, modems intended for the connection to the internet, and switches

Class II: European standard(s) on essential cybersecurity requirements for

- ▶ #36: firewalls, intrusion detection and/or prevention systems, including specifically those intended for industrial use

EU CRA: EN IEC 62443 based standardization framework

Scope of CRA standardization request



Operational Technology (OT)

based on EN IEC 62443-4-1
Secure product development lifecycle

?

based on EN IEC 62443-4-2
(products = components)

Profiles based on
EN IEC TS 62443-1-5

Class I (5): Function of Virtual Private Network (VPN)

Class I (6): Network Management Systems


Class I (7): SIEM Systems

Class I (10): Physical and virtual network interfaces

Class I (12): Routers, modems, switches

Class II (2): Firewalls, IDS, IPS

- Align to the current state of the art
- Ensure consistency between verticals/profiles
- Speed-up the development of verticals/profiles

 Intended to be cited in the OJEU

EU CRA: EN IEC 62443 based standardization framework

Derived vertical product (category) standards ("profiles")

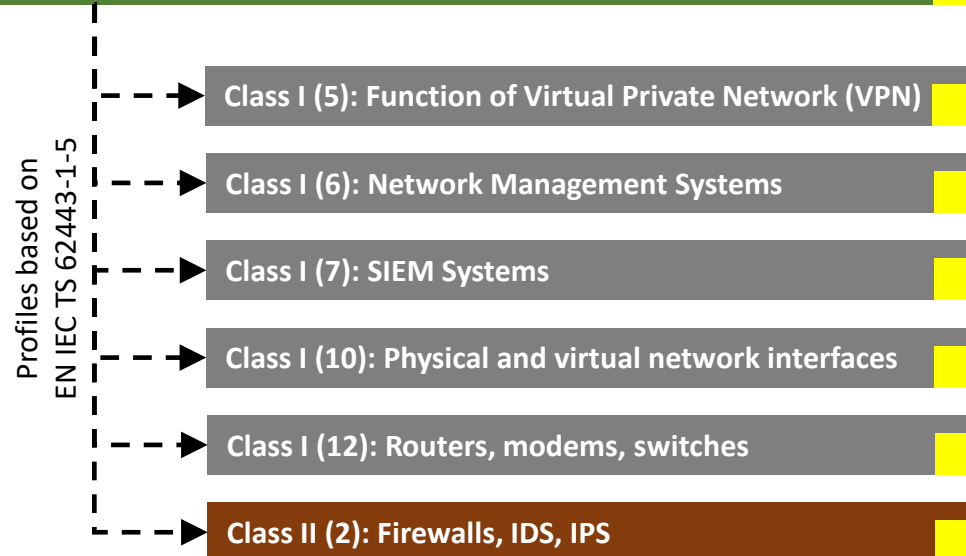


Operational Technology (OT)

based on EN IEC 62443-4-1
Secure product development lifecycle


?

based on EN IEC 62443-4-2
(products = components)



based on EN IEC 62443-3-3
(products = systems)



 Intended to be cited in the OJEU

CENELEC TC65X

CENELEC TC65X WG3 Cyber Security

Other WG's

Convenors: Judith Rossebo, Kai Wollenweber

81487 – EN IEC 62443-4-1:2018/prAA
Secure product development lifecycle

79973 – EN IEC 62443-4-2:2019/prAA
(products = components)

Profiles based on
EN IEC TS 62443-1-5

WI 81652 – prEN 50XXX-4

WI 81650 – prEN 50XXX-2

WI 81654 – prEN 50XXX-6

WI 81651 – prEN 50XXX-3

WI 81653 – prEN 50XXX-5

WI 81649 – prEN 50XXX-1

- Rapporteur: Srinath Pydi Narayana Rao

- ▶ Re-use of
 - ▶ EN IEC 62443-4-2
 - ▶ EN IEC 62443-3-3
 - ▶ EN IEC 62443-4-1 as the secure product life cycle
 - ▶ EN IEC TS 62443-6-2 as the basis for the evaluation approach
 - ▶ EN IEC TS 62443-1-5 for deriving product specific vertical standards (hENs)
- ▶ Adapt ("*common modification*"*) the current relevant standards of the EN IEC 62443 series to **also**, but not exclusively, address the essential cybersecurity requirements of the CRA
- ▶ Re-use as much as possible from the existing standards and modify/amend only where necessary
- ▶ Addressing different products / product-categories specified in EU CRA Annex III
- ▶ Limit potential market disruption due to unavailability of hENs

* A European common modification to an International Standard is an alteration of, addition to or deletion from its content. It is approved by CENELEC NCs and forms part of the EN.

- ▶ **EN IEC 62443-4-2:2019 → EN IEC 62443-4-2:2019/A11:2026**
 - ▶ Adapt existing requirements (CRs) and requirement enhancements (REs)
 - ▶ Adapt existing requirement rationales and add rationales for each REs
 - ▶ Add new REs and rationales to address CRA's essential cybersecurity requirements
 - ▶ Add applicability criteria for all CRs and REs
 - ▶ Incorporate the EN IEC TS 62443-6-2 evaluation approach
 - ▶ Detail the expected evaluation artefacts for each CR and RE
 - ▶ Specify the Security Level based acceptance criteria for each CR and RE

- ▶ **EN IEC 62443-4-1:2018 → EN IEC 62443-4-1:2018/A11:2026**
 - ▶ Monitor and align with the activities in CEN/CLC/JTC13 WG9 PT1 "*General principles for cyber resilience*", specifically regarding "*cybersecurity risk management*"
 - ▶ Update/add requirements on the documentation of the "*intended use*" and "*security context*"
 - ▶ Further specify/clarify expected development artefacts as an outcome of applying an EN IEC 62443-4-1 compliant product life cycle process

- ▶ Develop / derive the six vertical standards based on draft EN IEC 62443-4-2:2019/A11:2026

EU CRA – EN IEC 62443-4-1 Gap Analysis

EU CRA – EN IEC 62443-4-2 Gap Analysis

STEP

1

ANNEX I

ESSENTIAL CYBERSECURITY REQUIREMENTS

Part I Cybersecurity requirements relating to the properties of products with digital elements

- (1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.
- (2) On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:
 - (a) be made available on the market without known exploitable vulnerabilities;
 - (b) be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state;
 - (c) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them;

(2) (c)	ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them;	DM-1: Receiving notifications of security-related issues DM-3: Assessing security-related issues DM-4: Addressing security-related issues DM-5: Disclosing security-related issues Practice 7: Security update management (SUM)	Gap: Support for automatic updates (with an opt out) is not addressed
---------	---	---	--

EU CRA – EN IEC 62443-4-1 Gap Analysis

EU CRA – EN IEC 62443-4-2 Gap Analysis

(2) (c)	ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them;	EDR/HDR/NDR 3.10: Support for updates	Gap: Support for automatic updates (with opt out) is not addressed in -4-2 There is no requirement on support for updates for software applications independent from the component where the software is installed. However, SW updates are indirectly addressed in EDR/HDR/NDR 3.10 RE (1) but controlled by the HW product.
---------	---	---------------------------------------	---

How to Progress



EN IEC 62443-4-1:2018/A11:2026

EU CRA – EN IEC 62443-4-1 Addressing Gaps

STEP

2

EU CRA – EN IEC 62443-4-2 Addressing Gaps

EN IEC 62443-4-2:2019/A11:2026

EN IEC 62443-4-2:2019

7.11	CR 3.9 – Protection of audit information.....	51
7.11.1	Requirement.....	51
7.11.2	Rationale and supplemental guidance.....	51
7.11.3	Requirement enhancements	51
7.11.4	Security levels	51
7.12	CR 3.10 – Support for updates.....	52
7.13	CR 3.11 – Physical tamper resistance and detection.....	52
7.14	CR 3.12 – Provisioning product supplier roots of trust.....	52
7.15	CR 3.13 – Provisioning asset owner roots of trust.....	52
7.16	CR 3.14 – Integrity of the boot process	52
8	FR 4 – Data confidentiality.....	52
8.1	Purpose and SL-C(DC) descriptions.....	52
8.2	Rationale	52

11	Practice 7 – Security update management.....	42
11.1	Purpose	42
11.2	SUM-1: Security update qualification	42
11.2.1	Requirement.....	42
11.2.2	Rationale and supplemental guidance.....	42
11.3	SUM-2: Security update documentation	42
11.3.1	Requirement.....	42
11.3.2	Rationale and supplemental guidance.....	43
11.4	SUM-3: Dependent component or operating system security update documentation	43
11.4.1	Requirement.....	43
11.4.2	Rationale and supplemental guidance.....	43
11.5	SUM-4: Security update delivery	43
11.5.1	Requirement.....	43

EN IEC 62443-4-1:2018

[This is a preview - click here to buy the full publication](#)

IEC 62443-4-1:2018 © IEC 2018

– 5 –

11.5.2	Rationale and supplemental guidance.....	43
11.6	SUM-5: Timely delivery of security patches.....	44
11.6.1	Requirement.....	44
11.6.2	Rationale and supplemental guidance.....	44

EN IEC 62443-4-2:2019/A11:2026

(c)	CR 3.10 RE(2): <i>Components shall provide the capability to support automatic updates with a clear and easy to use opt-out mechanism</i>
-----	--

EN IEC 62443-4-1:2018/A11:2026

SUM-6: Support of automatic updates

Requirement

A process shall be employed to ensure that security updates for all supported products and

Harmonize with Horizontals



EN IEC 62443-4-1 – PT1 Mapping

PT1 Subparagraph	IEC 62443-4-1 Requirement ID	IEC 62443-4-1 Requirement Title
4.1 General	SM-1	Development process
4.1 General	SM-2	Identification of responsibilities
4.2 Risk-Based approach for cybersecurity	SR-2	Threat model
4.2 Risk-Based approach for cybersecurity	SR-3	Product security requirements
4.2 Risk-Based approach for cybersecurity	SR-4	Product security requirements content
4.3 Security by Design	Practice 3	Secure by design
4.3 Security by Design	SD-1	Secure design principles
4.3 Security by Design	SD-4	Secure design best practices
4.4 Secure by Default	SD-2	Defense in depth design
4.4 Secure by Default	SD-3	Security design review
4.5 Transparency	SG-1	Product defense in depth
4.5 Transparency	SG-2	Defense in depth measures expected in the environment
5.1 General	SM-3	Identification of applicability
5.1 General	SM-5	Process scoping

Harmonize with Horizontals

EN IEC 62443-4-2 – PT2 Mapping

correspondence:		X
supplemental:		S
mapped by WG3:		X
stats: [num X] / [num S] or [num X]		
IEC/EN 62443-4-2 Requirements		
FR 1 – Identification and authentication control		
CR 1.1 – Human user identification and authentication	6/3	
CR 1.1 RE (1) – Unique identification and authentication	1/6	
CR 1.1 RE (2) – Multifactor authentication for all interfaces	2/6	
CR 1.2 – Software process and device identification and	7/0	
CR 1.2 RE (1) – Unique identification and authentication	1/5	
CR 1.3 – Account management	1/5	
CR 1.4 – Identifier management	1/5	
CR 1.5 – Authenticator management	2/5	
CR 1.5 RE (1) – Hardware security for authenticators	2/5	
CR 1.6 – Wireless access management	6/4	

Supplier Objectives from PT2																			
		(a) no known vulnerability		(b) secure by default				(c) security updates								(d) access control			
		WG3_mapping	VulnerabilityManagementProcess	WG3_mapping	SecureDefaultDesign	SecureStartupConfig	FactoryReset	WG3_mapping	Updateability	AvailabilityOfUpdates	UpdateMechanism	AutomaticUpdates	TimelyUpdates	UserUpdateNotification	PostponeUpdates	WG3_mapping	AccessControlConcept	AccessControl	AccessControlReport
		0	0/0	11	1/1	1/1	1/2	3	1/1	1/1	1/1	1/0	0/1	0/0	0/0	10	6/26	6/26	2/5
		2														10	4/19	4/19	
																X	X	X	
																X	S	S	
																X	S	S	
																X	X	X	
																X	S	S	
																X	S	S	
				X												X	S	S	
				X												X	S	S	
																X	X	X	

correspondence: X

supplemental: S

mapped by WG3: X

stats: [num X] / [num S] or [num X]

Harmonize with Horizontals



EN IEC 62443-4-1 – PT3 Mapping

Clause ID	Clause Title	Requirements	IEC 62443-4-1
PRE-1	Policy on coordinated vulnerability disclosure	[PRE-1-RQ-01] A policy on coordinated vulnerability disclosure shall be created, put in place and adhered to.	DM-1
		[PRE-1-RC-01] The coordinated vulnerability disclosure policy should be based on EN ISO/IEC 29147:2020 Clause 9.	DM-1
PRE-2	Capability to receive reports	[PRE-2-RQ-01] One or more state of the art mechanisms shall be provided to receive reports of potential vulnerabilities found in products.	DM-1
PRE-3	Contact Information	[PRE-3-RQ-01] The contact information for reporting of potential vulnerabilities discovered in the product, or third party components shall be published.	DM-1
PRE-4	Secure communications	[PRE-4-RQ-01] Reporting methods shall implement secure communication methods in accordance with EN ISO/IEC 29147:2020 Clause 5.8.2.	DM-1
PRE-5	Product identification	[PRE-5-RQ-01] The product shall be unambiguously identified.	Gap
		[PRE-5-RQ-02] At least the following information shall be provided with the product: —Manufacturer —Product name —Product version	Gap

- ▶ According to CRA Article 13(3), for any product in the scope of the CRA
- ▶ Based on Intended Use or Security Context
- ▶ Based on Technical Capability

- Article 13, 3.

- The cybersecurity risk assessment shall be documented and updated as appropriate during a support period to be determined in accordance with paragraph 8 of this Article. That cybersecurity risk assessment shall comprise at least an analysis of cybersecurity risks based on the intended purpose and reasonably foreseeable use, as well as the conditions of use, of the product with digital elements, such as the operational environment or the assets to be protected, taking into account the length of time the product is expected to be in use. The cybersecurity risk assessment shall indicate whether and, if so in what manner, the security requirements set out in Part I, point (2), of Annex I are applicable to the relevant product with digital elements and how those requirements are implemented as informed by the cybersecurity risk assessment. It shall also indicate how the manufacturer is to apply Part I, point (1), of Annex I and the vulnerability handling requirements set out in Part II of Annex I.

Definition “Intended use”: the use for which a product is designed by the product supplier, describing the explicit and implicit assumptions about the product’s properties and capabilities

Note 1 to entry: The **product security context** is derived from the intended use

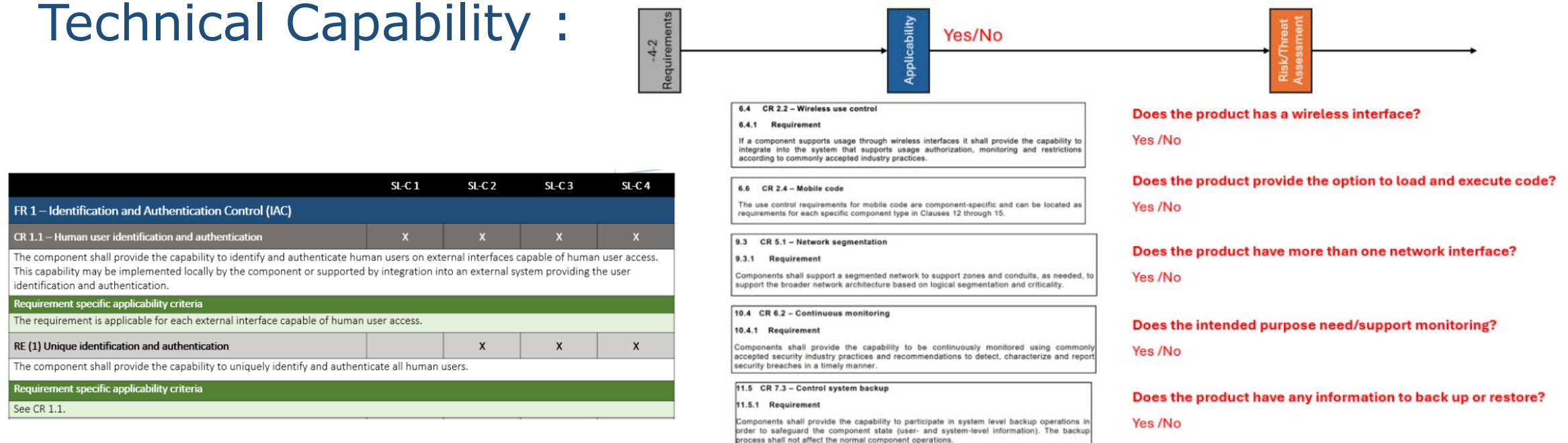
Intended Use & Technical Capability



Intended Use: Unmanaged Switch

This equipment is intended to switch all Ethernet traffic between ports without any filtering, management, monitoring or logging

Technical Capability :



- ▶ Based on **IEC TS 62443-6-2** "Security evaluation methodology for IEC 62443-4-2" (Draft)
- ▶ Evaluation Process, Requirements and Activities
- ▶ Artefacts
- ▶ Acceptance criteria

7.12.3.2.3 Applicability

See CR 3.10.

7.12.3.2.4 Evaluation

- Description of implementation of the automatic download
- Description of the notification mechanism(s)
- Description of the implementation of the scheduling of updates
- Description on why automatic updates shall be supported or are precluded
- Description of roll-back mechanism, if applicable

7.12.3.2.5 Acceptance criteria

7.12.3.2.5.1 SL-C 1

N/A

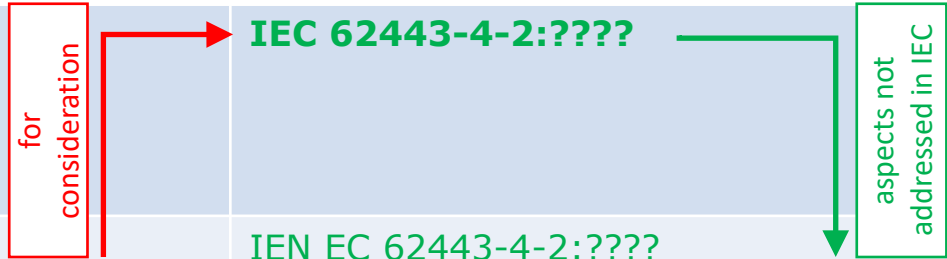
7.12.3.2.5.2 SL-C 2

- a) updates are automatically downloaded

Today, tomorrow, the future



	Today	CRA deadlines (2026)	Future (????)
International level (IEC)	IEC 62443-4-2:2019	IEC 62443-4-2:2019	IEC 62443-4-2:????
European level (CENELEC)	EN IEC 62443-4-2:2019	EN IEC 62443-4-2:2019 EN IEC 62443-4-2:2019/A11:2026	IEN EC 62443-4-2:???? EN IEC 62443-4-2:????/A11:????
National level (e.g. Germany)	DIN EN IEC 62443-4-2:2019	DIN EN IEC 62443-4-2:2026	DIN EN IEC 62443-4-2:????



Timelines – Broad verticals & verticals



Work Items (WI)	Drafting	Publication
Broad verticals (4-1 & 4-2)	Ongoing & Completion by September 2025	December 2026
Verticals (Firewall, VPN...)	From October 2025 to March 2026	November 2026

Call for Experts



EUROPEAN COMMITTEE FOR ELECTROTECHNICAL STANDARDIZATION (CENELEC)

TECHNICAL COMMITTEE No. 65X: Industrial-process measurement, control and automation

Call for experts to develop the vertical European standards, to address the demanded security profiles by the CRA assigned to TC65X WG3

CLC/TC 65X decided via a CIV ballot (TC65X-SEC408-RV) to create preliminary work items to address the vertical deliverables below requested by the CRA.

- *M/606 #20: Products with digital elements with the function of virtual private network (VPN)*
- *M/606 #21: Network management systems*
- *M/606 #22: Security information and event management (SIEM) systems*
- *M/606 #25: Physical and virtual network interfaces*
- *M/606 #27: Routers, modems intended for the connection to the internet, and switches*
- *M/606 #36: Firewalls, intrusion detection and/or prevention systems, including specifically those intended for industrial use*



Action

National Committees are kindly invited to appoint expert(s) to participate in the work by filling the table below and uploading it onto CLC/TC 65X Collaboration Platform by **3rd October 2025** at the latest. Appointed experts should also be registered to the IEC/CENELEC Expert Management System by their National Committee.

Table to be filled by the National Committee for their Nomination of expert(s)

Country:			
First name	Last name	Email	WI number

Deadline : 3rd October 2025

Questions???

Contact : Srinath Pydi Narayana Rao
Email : srinath-pydi-Narayana-rao@internetoftrust.com

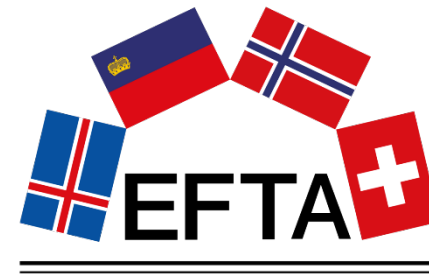
www.cenelec.eu

Follow us:



Tag us @Standards4EU

Funded work



- ▶ With thanks to EISMEA and EFTA grants N 101232696 and N 101196779 making the STAN4CR and STAN4CR2 projects.
- ▶ These grants support the work of the rapporteurs working on the CRA at CEN, CENELEC and ETSI and dissemination and stakeholder events such as this webinar.
- ▶ Visit our website for more information on the CRA standards:
- ▶ www.stan4cra.eu
- ▶ Expert funding is available at Cyberstand.eu