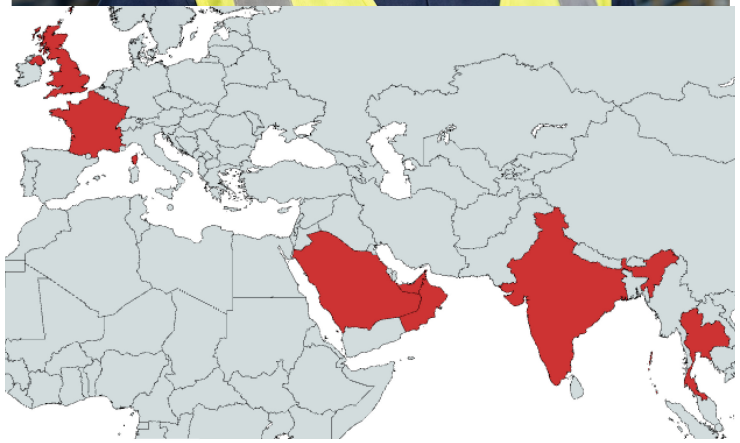
CENELEC

EUROPEAN COMMITTEE
FOR ELECTROTECHNICAL STANDARDIZATION

CLC/TC65X WG3-Vertical Standards

ACS Technical Requirements & Compliance under EN IEC 62443

srinath.pydi-narayana-rao@internetoftrust.com



- Lead Industrial cybersecurity consultant at Internet of Trust (IOTR) Paris, France
- Lead Process Automation projects expert at Schneider Electric Systems Chennai, India
- Lead Rapporteur for CLC/TC65X WG3 representing CENELEC to draft hENs for OT products
- Senior ISA Member
- Masters in Computer Science (Cybersecurity) Paris, France
- Bachelors in Engineering (Electronics & Instrumentation) Chennai, India
- Diploma in Engineering (Electronics & Communication) Chennai, India

CLC/TC65X WG3 “Cyber Security”

- Established in February 2020
- Scope
  - Observing the cybersecurity activities on IEC, ISO and other standardization bodies and fora
  - European mirror of IEC TC65/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/TC44X “*Safety of Machinery*”: WG2 (“*Protection against corruption*”)
- Convenors
  - Judith Rossebo, Kai Wollenweber
- Rapporteur
  - Srinath Pydi Narayana Rao

118 members

Overview EN IEC 62443 series

EN IEC 62443

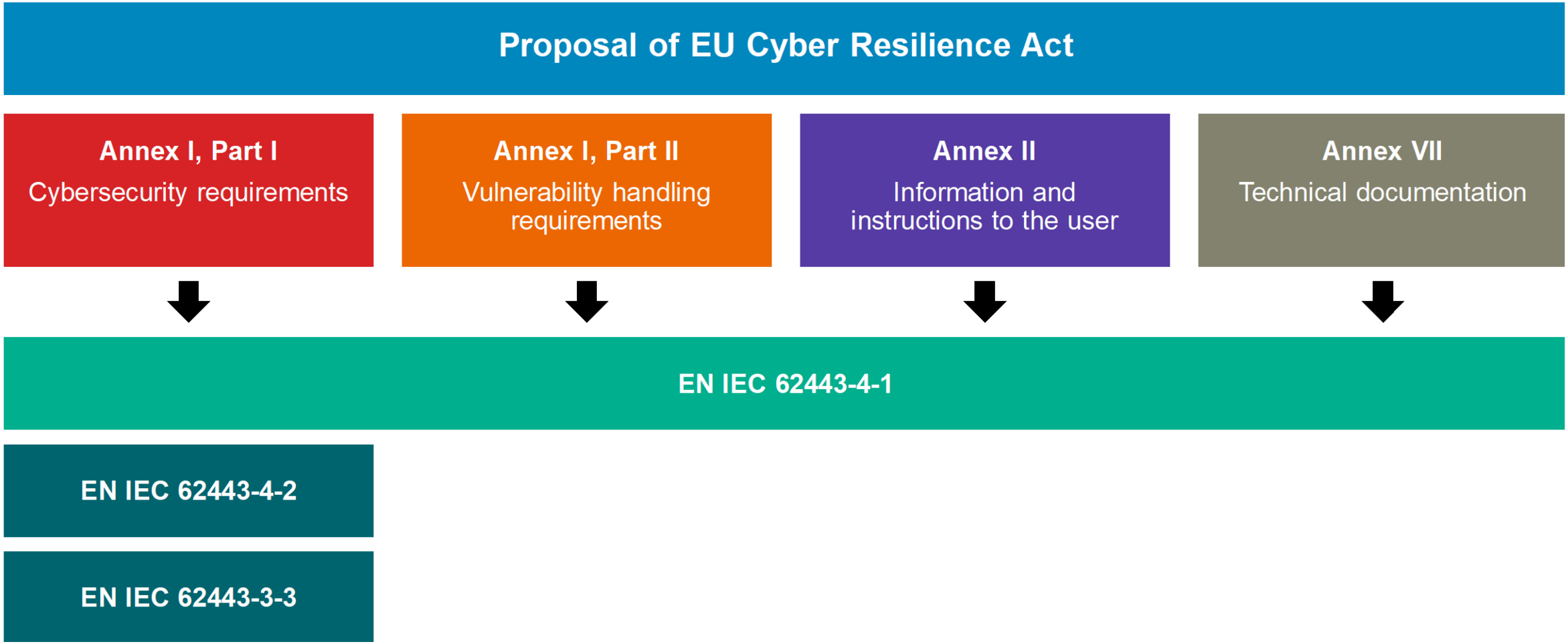
Security for Industrial Automation and Control Systems

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	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 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					

In progress / parallel vote

Published / adopted

CRA relevant parts of (EN) IEC 62443 series



CRA relevant parts of (EN) IEC 62443 series

- **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
- EN IEC TS 62443-6-2 "Security evaluation methodology for IEC 62443-4-2"
  - 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"

EU CRA: EN IEC 62443 based standardization framework
"Broad OT verticals"

Operational Technology (OT)

EN IEC 62443-4-1:prAA
Secure product development lifecycle

EN IEC 62443-4-2:prAA
(products = components)

EN IEC 62443-3-3:prAA
(products = systems)

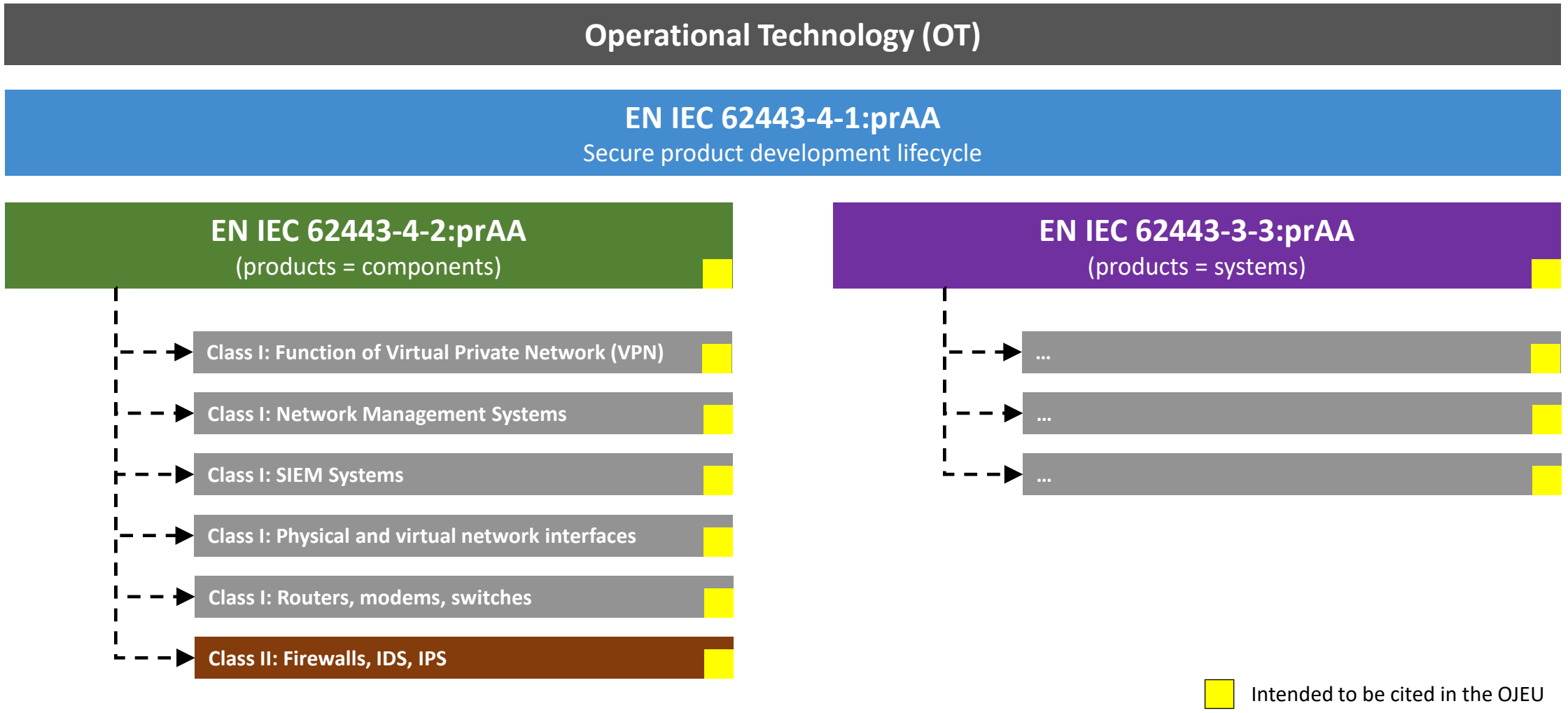
Future work, not part of Standardization Request M/606

Broad verticals are key, because they

- ensure quality for the development of vertical standards / profiles
- ensure consistency between vertical standards / profiles
- provide a solid basis for ensuring coherence with the PT1, PT2, and PT3 deliverables

Intended to be cited in the OJEU

EU CRA: EN IEC 62443 based standardization framework
Derived vertical product (category) standards ("profiles")



EU CRA: EN IEC 62443 based standardization framework
Scope of CRA standardization request

Operational Technology (OT)

EN IEC 62443-4-1:prAA [WI 81487]
Secure product development lifecycle

EN IEC 62443-4-2:prAA [WI 79973]
(products = components)

- **Class I: Function of Virtual Private Network (VPN)** [WI 81652]
- **Class I: Network Management Systems** [WI 81650]
- **Class I: SIEM Systems** [WI 81654]
- **Class I: Physical and virtual network interfaces** [WI 81651]
- **Class I: Routers, modems, switches** [WI 81653]
- **Class II: Firewalls, IDS, IPS** [WI 81649]

Intended to be cited in the OJEU

Current and upcoming activities

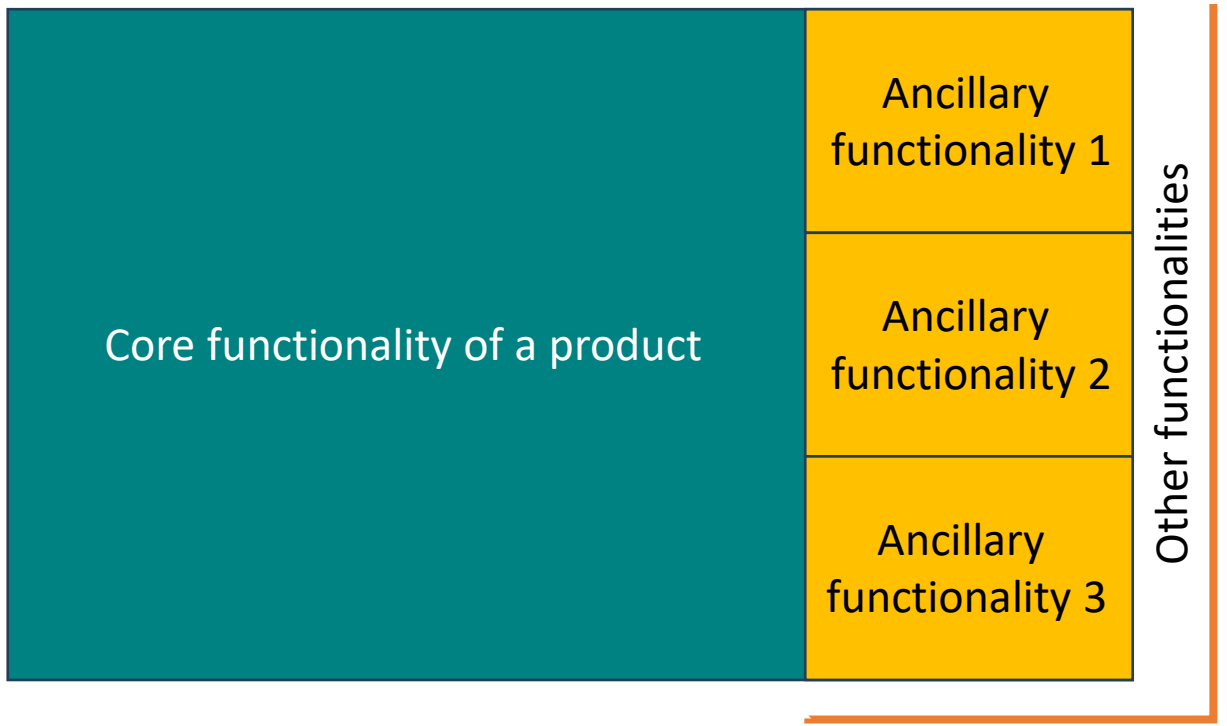
- EN IEC 62443-4-2:2019 → **EN IEC 62443-4-2:2019/A11:2026 – ENQ started from 17th March**
  - Monitor activities in CEN/CLC/JTC13 WG9 PT2 *"Common cybersecurity requirements"*
  - Adapt existing requirements (CRs) and requirement enhancements (REs) ✅
  - Adapt existing requirement rationales and add 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 Security Evaluation Methodology based on the EN IEC TS 62443-6-2 ✅
  - Detail the expected evaluation artefacts for each CR and RE ✅
  - Incorporate the Security Test Grades and Security Test Modules ✅
- EN IEC 62443-4-1:2018 → **EN IEC 62443-4-1:2018/A11:2026 ENQ started from 17th March**
  - Monitor and align with the activities in CEN/CLC/JTC13 WG9 PT1 *"General principles for cyber resilience*
  - Dependencies on CEN/CLC/JTC13 WG9 PT3 *"Vulnerability handling"* as normative reference in the vertical standards
  - Add *"applicability process"* ✅
  - Update/add requirements on the documentation of the *"intended use", "security context", "applicability"* ✅
  - Add *"cybersecurity risk management"* Practice ✅
  - Further specify 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
  - Call for experts ✅
  - Start of work October 2025 ✅
  - DC and HAS Consultation – ✅

CRA related deliverables

Title	Reference	WI
Broad vertical standards		
Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements	EN IEC 62443-4-1:prAA	81487
Part 4-2: Technical security requirements for IACS components	EN IEC 62443-4-2:prAA	79973
Part 3-3: System security requirements and security levels (on hold)	EN IEC 62443-3-3:prAA	79830
Vertical standards: "Security for OT – Part x: Security profile for…" (based on EN IEC 62443:prAA standards)		
Part 1: Firewalls and intrusion detection and prevention systems	prEN 50770-1	81649
Part 2: Network management systems	prEN 50770-2	81650
Part 3: Physical and virtual network interfaces	prEN 50770-3	81651
Part 4: Products with digital elements with the function of virtual private network	prEN 50770-4	81652
Part 5: Routers, modems intended for the connection to the internet, and switches	prEN 50770-5	81653
Part 6: Security information and event management (SIEM) systems	prEN 50770-6	81654

Product & Core functionality

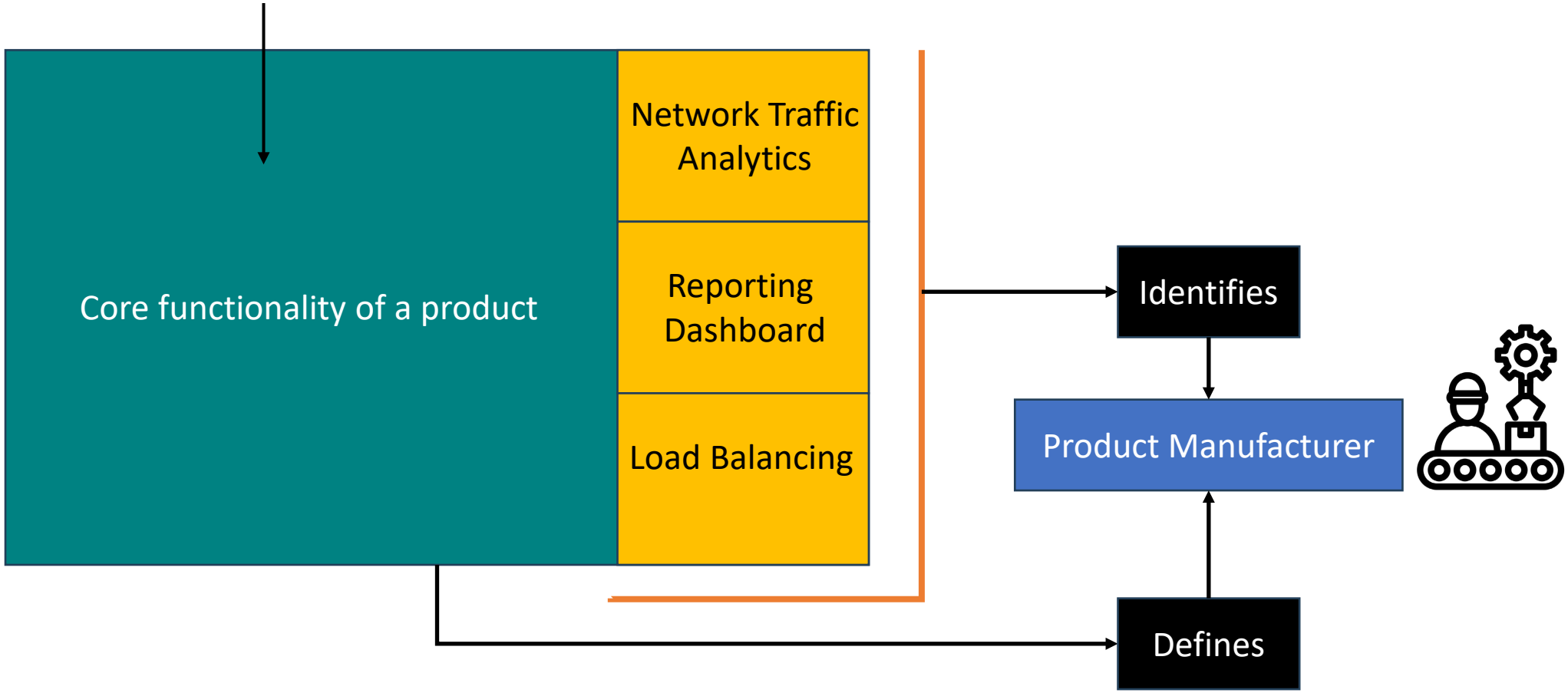
A product's core functionality refers to the product's main features and technical capabilities, without which it would not be able to meet its intended purpose



Source : Draft guidance from commission

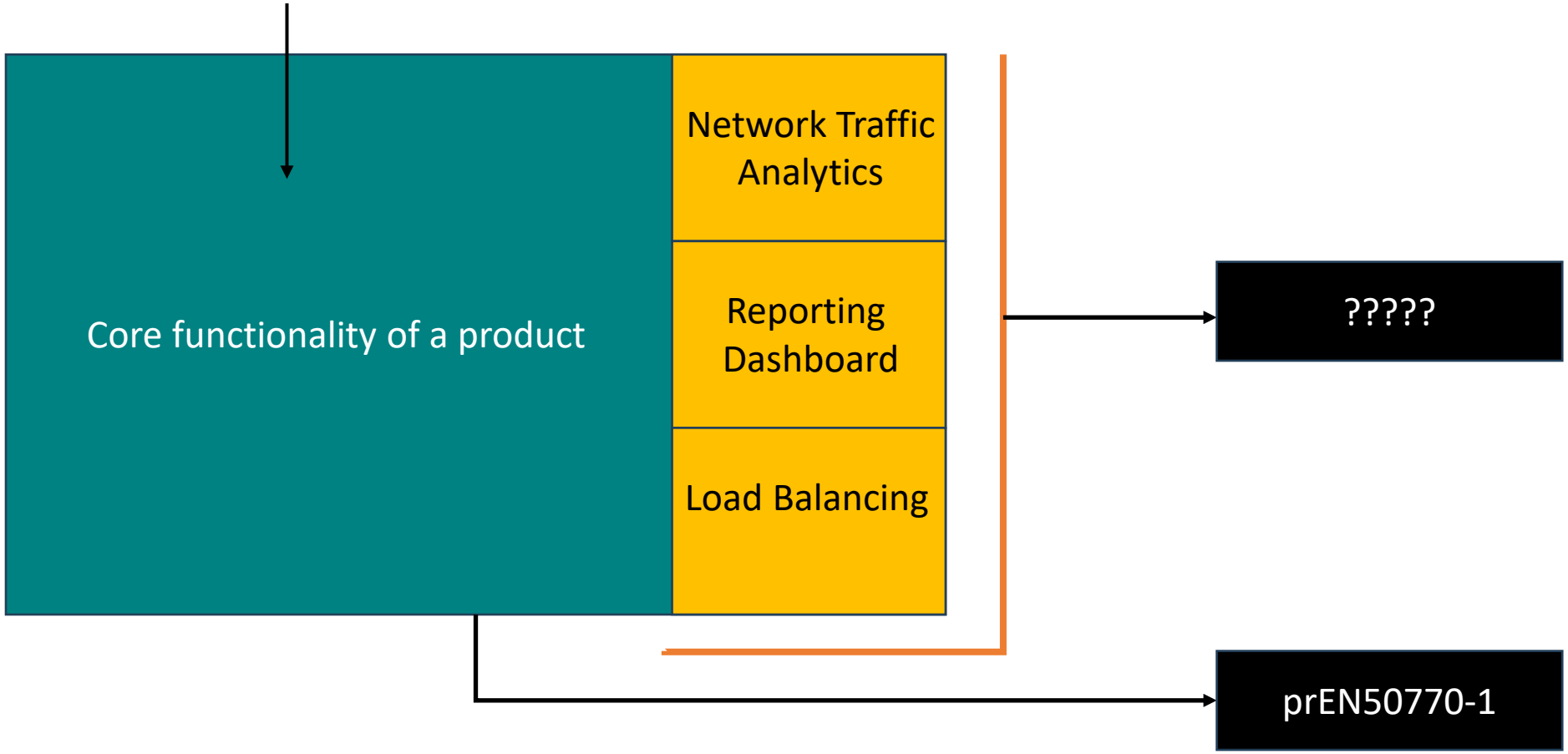
Example : Firewall

Firewalls are products with digital elements that protect a connected network or system from unauthorized access by monitoring and restricting data communication traffic to and from that network.



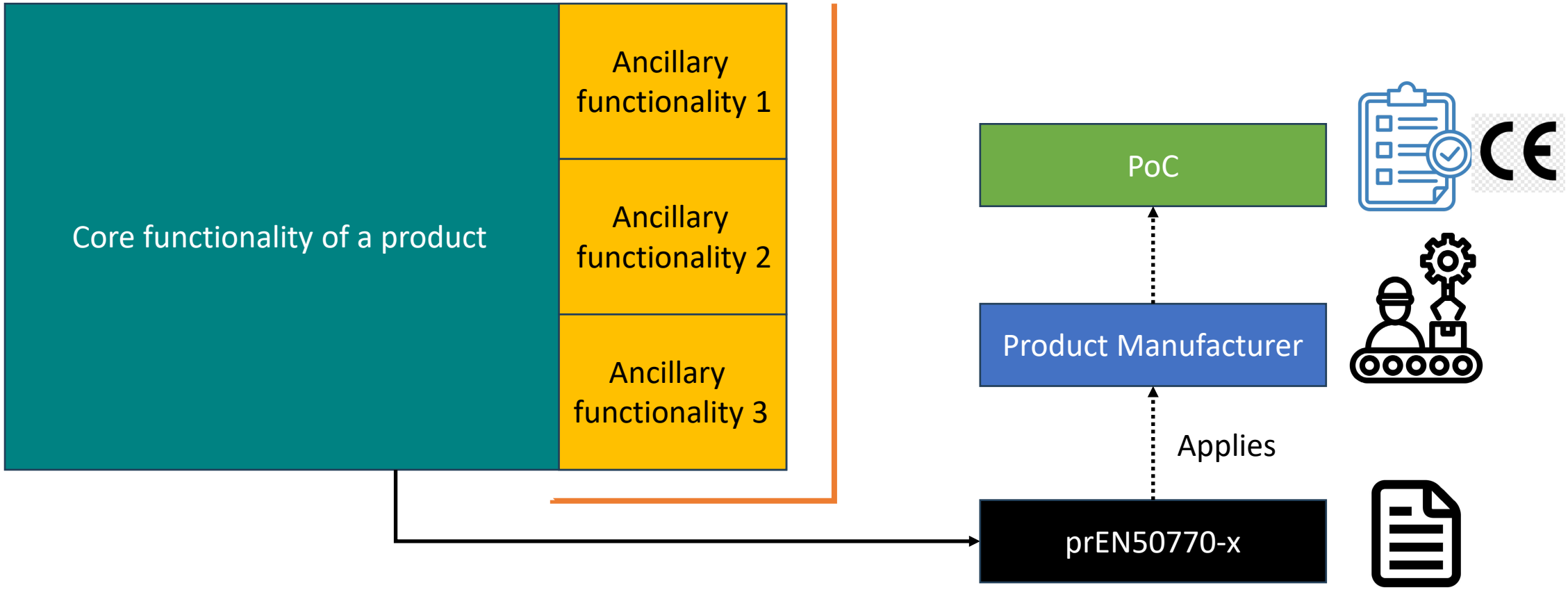
Core functionality & hENs

Firewalls are products with digital elements that protect a connected network or system from unauthorized access by monitoring and restricting data communication traffic to and from that network.



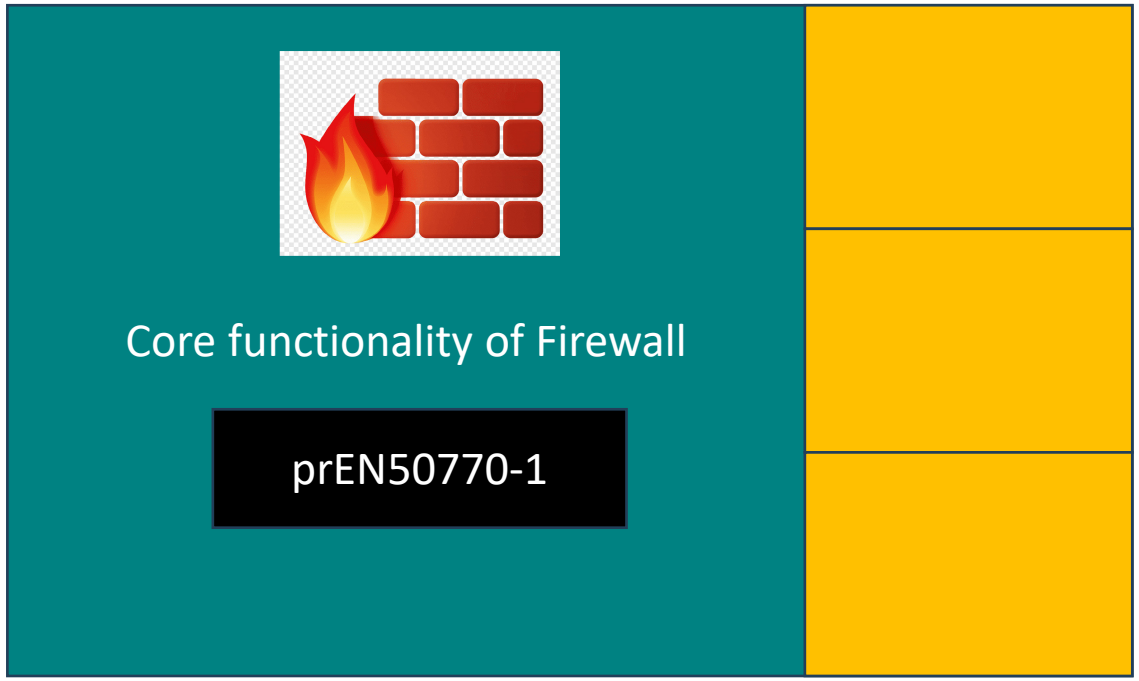
Core functionality, hENs & PoC

When product meets essential legal requirements through harmonized standards which are published in OJEU



Core functionality : Firewall

Firewalls are products with digital elements that protect a connected network or system from unauthorized access by monitoring and restricting data communication traffic to and from that network.



OT hENs : prEN50770-1

Clause 1: Scope

Clause 2: Normative Reference (EN IEC 62443-4-2:prAA)

Clause 3: Terms, Definitions & Abbreviations

Clause 4: Product Context

Clause 5: Technical Security Requirements

Clause 6: Conformance Assessment

Annex A: Security Analysis

Annex ZZ: Mapping CRA ESR with Technical Security Requirements

Clause 4 :Product Context

Clause 4.1: Product Functions

Clause 4.2: Product Architecture

Clause 4.3: Operational Environment

Clause 4.4: Distribution of Functions

Clause 4.5: Users

Result :

Clause 4.6: Usecases (Reference cases)

Context : Product Functions

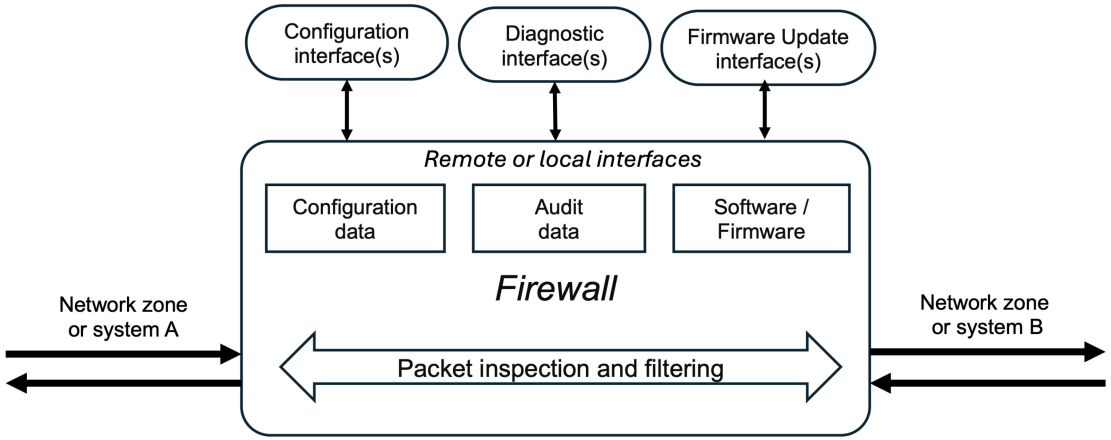
Product Function

Block unwanted traffic and allow desired traffic to pass. The network traffic may be physical or virtual. Network traffic allow/pass depends on configuration. Packet inspection and filtering is performed between the network interfaces

Assets

Configurations data, Audit data, Software/Firmware

Interfaces :configuration, Diagnostic, Firmware update (Physical or Virtual) (Remote or Local)



Context :Operational Environment

Operational Environment

Annex B : Product security context category of EN IEC 62443-4-1:prAA

Physical Access : Public /Limited/ Controlled

Communication Access : Public /Limited/ Controlled

4.3.1 Physical access levels

4.3.1.1 Public access

The product is physically exposed or easily reachable without access restrictions.

Examples include:

— the product is installed in an unlocked cabinet in the public areas

— the product placed in a public corridor

4.3.2 Communication access levels

4.3.2.1 Public access

The product's configuration, diagnostic or firmware update interfaces are easily accessible without any access restrictions over the network.

Examples include:

— the product's configuration, diagnostic or firmware update interfaces are accessible from an external IT network with unknown security measures

— the product's configuration, diagnostic or firmware update interfaces are directly accessible via the internet

Context: Users

Users

Annex B : Product security context category of EN IEC 62443-4-1:prAA

Persons : Ordinary/ Instructed/ Skilled

to the security assets for ordinary users are not anticipated.

Examples for instructed and skilled users include:

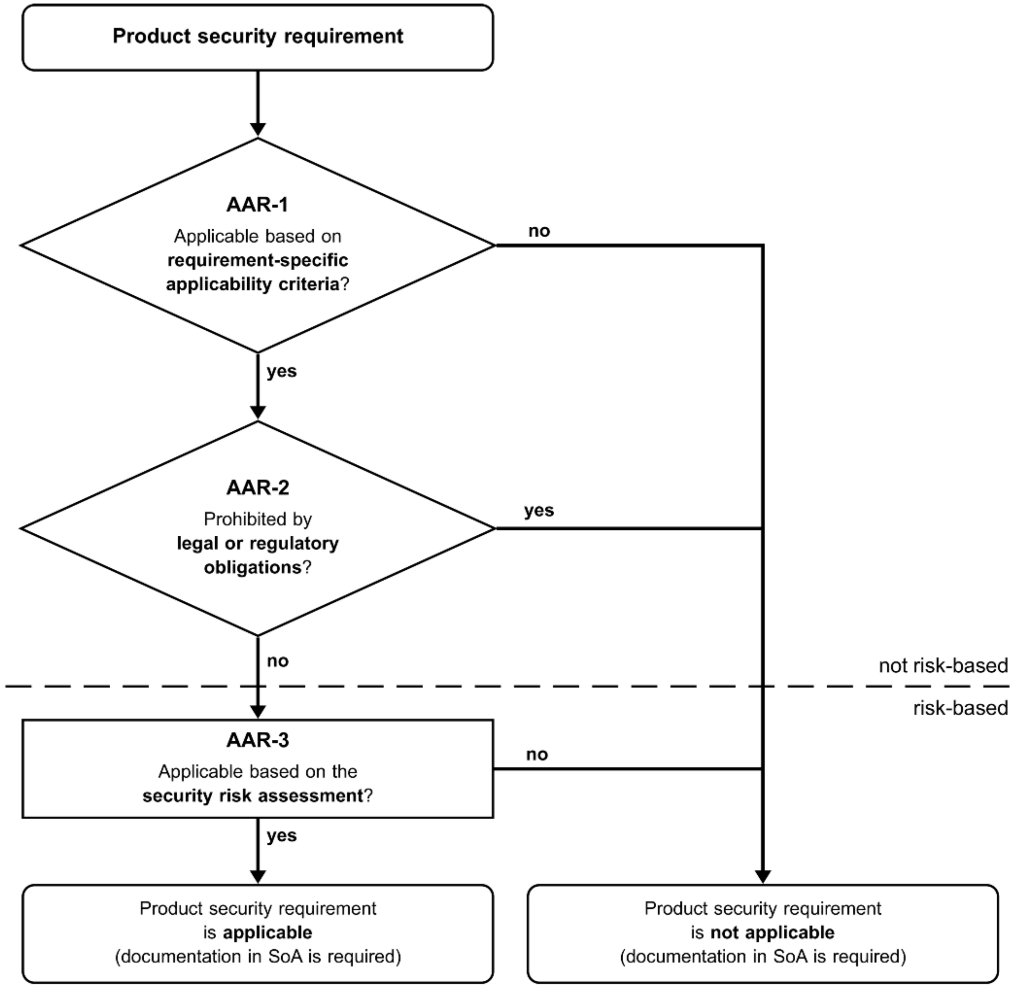
— capable to install, configure and update the firewall rules and polices

— knowledge of detection mechanisms and analyse attack patterns

- UC-1: Hardware-based firewall deployed in an OT environment, administered by instructed /skilled user
- UC-2: Virtual firewall deployed in an OT environment, administered by instructed /skilled user

Applicability Assessment (EN IEC 62443-4-1:PrAA Annex C)

Development of the Vertical Draft



AAR-1 & AAR-2 : Applicability Criteria

Development of the Vertical Draft

SRs and REs	Hardware based Firewall FW-UC-01	Virtual Firewall FW-UC-02	SoA
FR 1 – Identification and authentication control (IAC)			
CR 1.1 – Human user identification and authentication	Applicable	Applicable	
CR 1.1 RE (1) – Unique identification and authentication	Applicable	Applicable	
CR 1.1 RE (2) – Multifactor authentication for all interfaces	Applicable	Applicable	
CR 1.2 – Software process and device identification and authentication	Applicable	Applicable	
CR 1.2 RE (1) – Unique identification and authentication	Applicable	Applicable	
CR 1.3 – Account management	Applicable	Applicable	
CR 1.4 – Account Identifier management	Applicable	Applicable	
CR 1.5 – Authenticator management	Applicable	Applicable	
CR 1.5 RE (1) – Hardware security for authenticators	Applicable	Not Applicable	Virtual and host based firewalls don't have hardware.
CR 2.4 – Mobile code	Not Applicable	Not Applicable	Use case is HW based FW and the core functionality defined in UC doesn't contain docker containers or virtualisation to install mobile code
CR 2.4 RE (1) – Mobile code authenticity check	Not Applicable	Not Applicable	Use case is HW based FW and the core functionality defined in UC doesn't contain docker containers or virtualisation to install mobile code

5.5 CR 1.3 – Account management

5.5.1 Requirement

The component shall provide the capability to manage accounts directly or by supporting measures.

5.5.2 Rationale and supplemental guidance

A common approach for meeting this requirement would be the component delegating the valuation of authentication to a directory server (for example, LDAP or Active Directory) which provides the account management capabilities.

5.5.2.1 Applicability

The requirement is applicable for all components that supports more than one fixed administrative account.

AAR-3 : Security Analysis (Annex A)

Development of the Vertical Draft

A.1.26 Threat.MonitoringDataDisclosure

Threat Description: An attacker extracts sensitive monitoring data

A.1.26.1 Risk

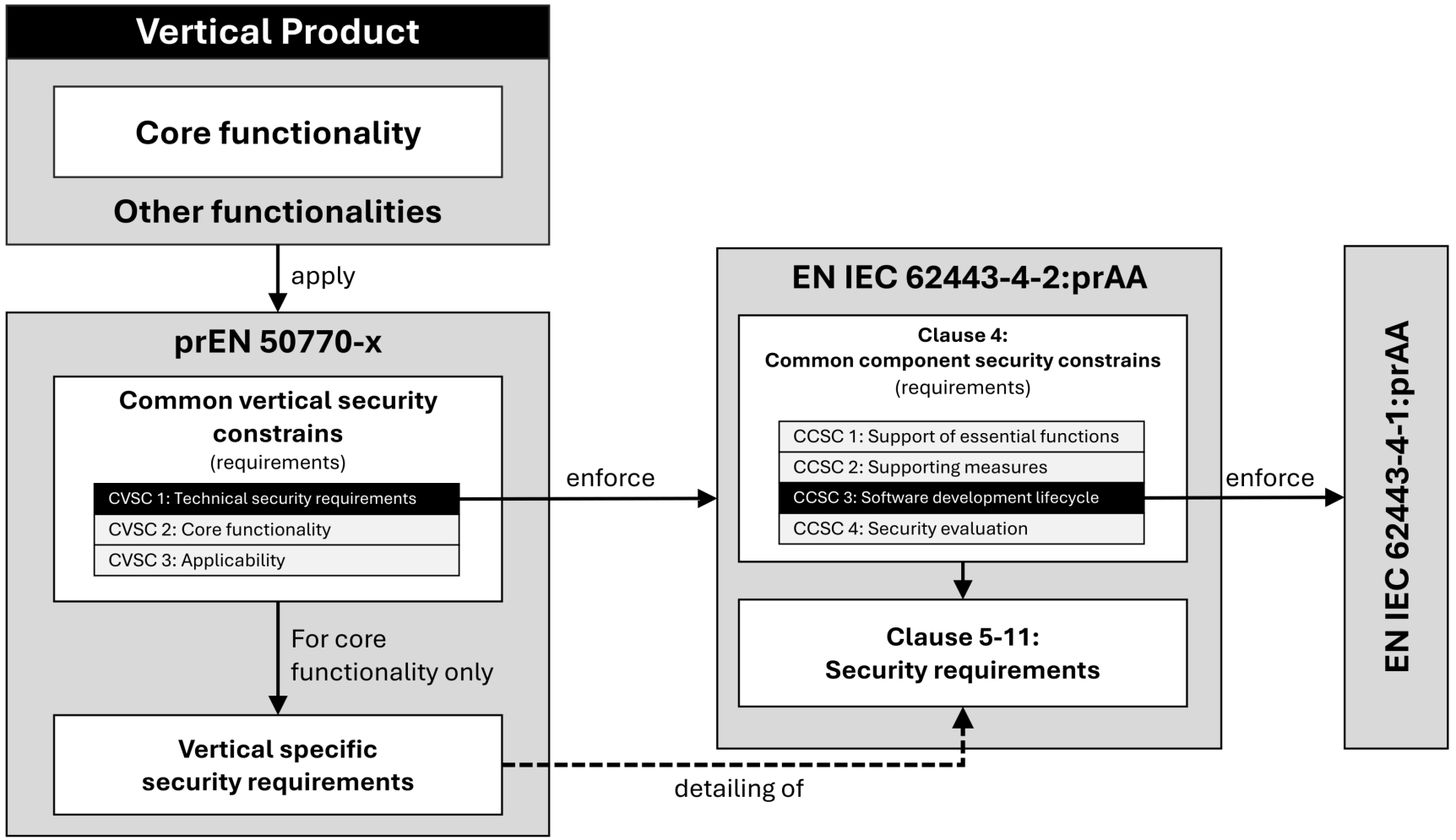
Monitoring data generated by the firewall as part of its monitoring functions is accessible without authorization. This provides an attacker the opportunity to extract audit records, event logs, security alerts, or other monitoring information. As a consequence, sensitive security relevant monitoring data is disclosed.

A.1.26.2 Mapping of component requirements

Table A.1 — Mapping of component requirements for Threat.MonitoringDataDisclosure

Physical Access			Communication Access			EN IEC 62443-4-2:2019/prAA:2026 Requirements for mitigation
Public	Limited	Controlled	Public	Limited	Controlled	
x			Independent			CR 4.1 – Information confidentiality CR 4.1 RE (1) – Confidentiality of sensitive information at rest CR 6.1 – Audit log accessibility
	x	x	x	x		CR 4.1 – Information confidentiality CR 6.1 – Audit log accessibility
	x	x			x	CR 6.1 – Audit log accessibility

Constraints



Constraints

5.1.2 CVSC 1 Technical security requirements

A firewall shall implement the technical security requirements according to EN IEC 62443-4-2:2019/prAA:2026, clauses (4-11).

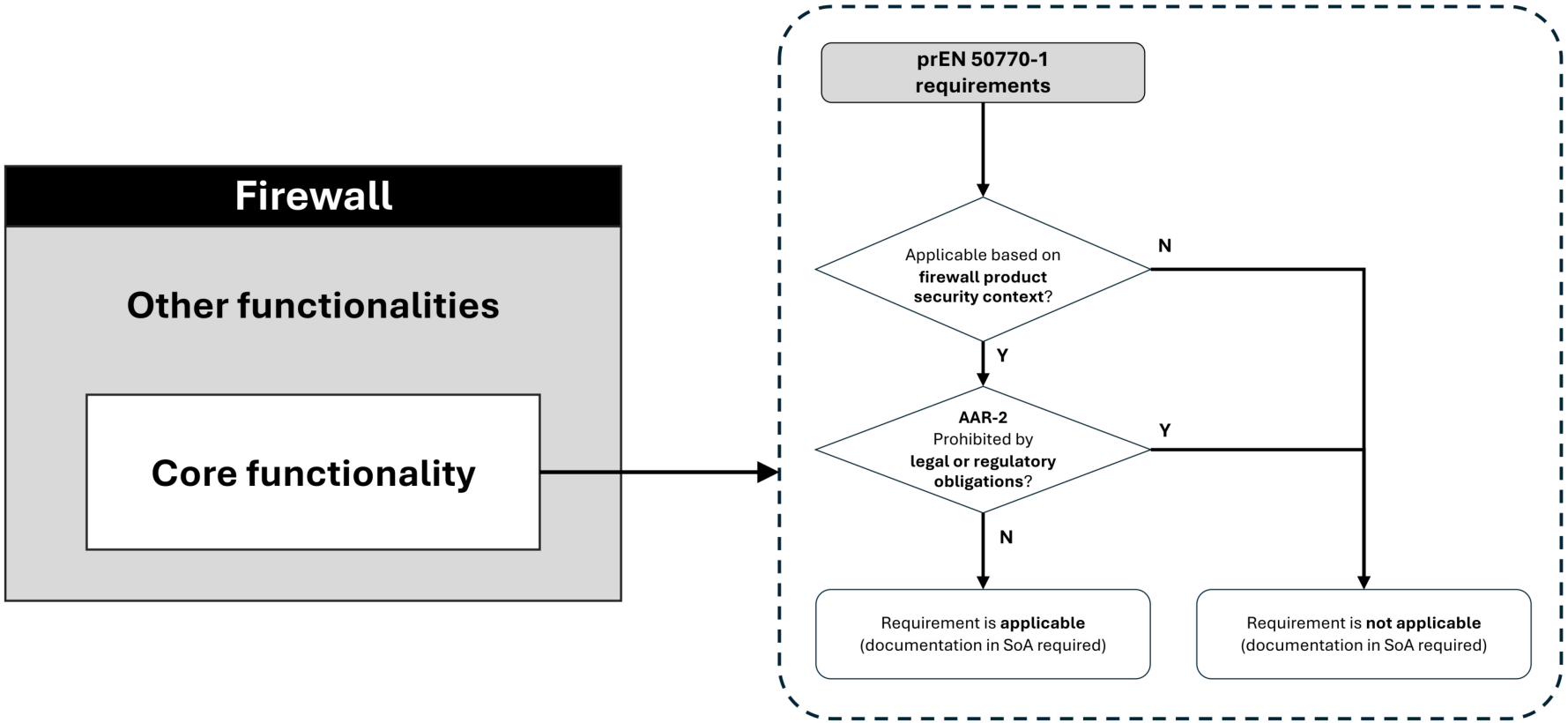
5.1.3 CVSC 2 Core functionality

A firewall shall implement all the requirements listed in subclauses 5.2 (for both hardware and virtual firewall), 5.3 (for Hardware firewall only) and 5.4 (for virtual firewall only), in accordance with its defined Product Context as defined in clause 4.

5.1.4 CVSC 3 Applicability

For the implementation of the requirements listed in subclauses 5.2 (for both hardware and virtual firewalls), 5.3 (for hardware firewalls only), and 5.4 (for virtual firewalls only) of this document, AAR1 and AAR3, as specified in Annex C of EN IEC 62443-4-1:2018/prAA:2026, shall not be applied.

Manufacturer Freedom on Core functionality



Technical Security Requirements

5.2.7 Requirement enhancements

5.2.7.1 CR 1.5 RE (1) Hardware security for authenticators

5.2.7.1.1 Requirement

See Requirement of CR 1.5 RE (1) [Reference to EN IEC 62443-4-2:2019/prAA:2026]

5.2.7.1.2 Rationale and supplemental guidance

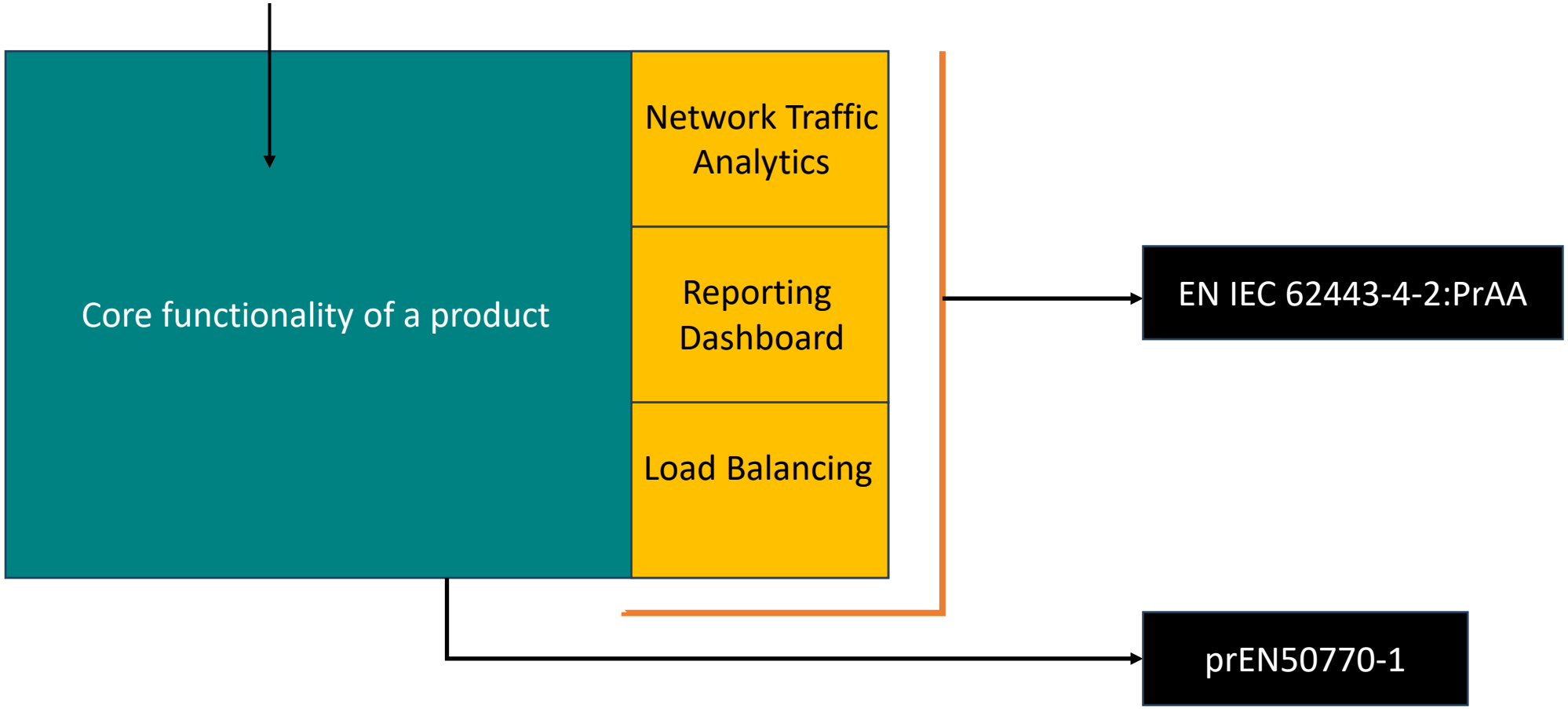
-

5.2.7.1.3 Product security context applicability

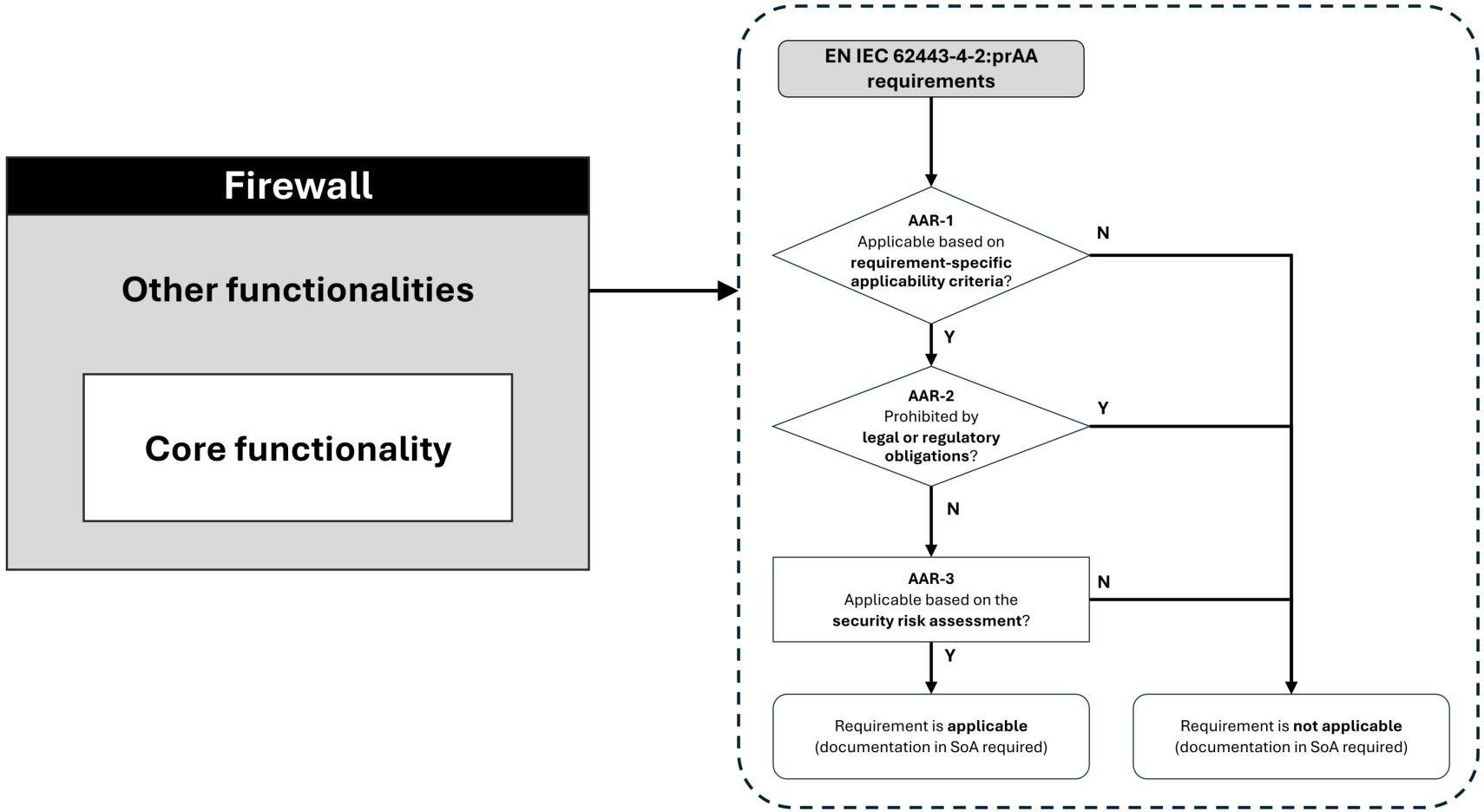
This requirement shall apply in a product security context with public physical access independent of the communication access.
This requirement shall apply for authenticators used to access the remote configuration interfaces, the remote diagnostic interfaces and the remote firmware update interfaces of the firewall.

Other Functionalities

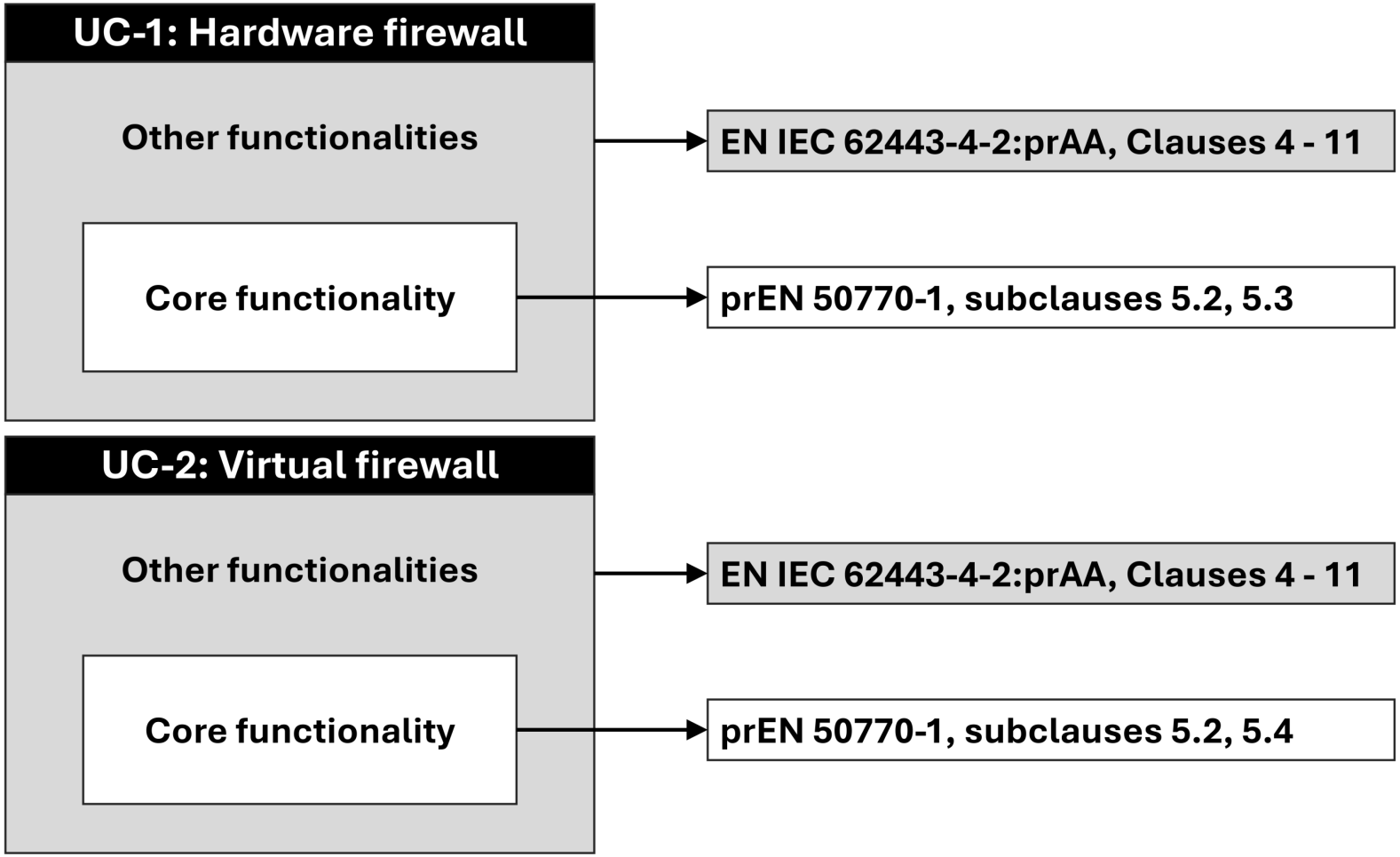
Firewalls are products with digital elements that protect a connected network or system from unauthorized access by monitoring and restricting data communication traffic to and from that network.



TSR : Other Functionalities



prEN 50770-1: Firewall



Questions???

www.cenelec.eu

Follow us:

Tag us @Standards4EU