



CYBERSTAND.eu

# Impacting the CRA

Defining standards for the future

**14:15 - 15:30**

**Breakout session 1:  
Product specific standards**



**Executive Room**

**Chair:** Kim Nordstrom, ETSI

**Panelists:**

Enrico Frumento, Smart meter gateways

Mohamad Hajj, Hypervisors

Kim Nordstrom, Consumer IoT

# Breakout session 1: vertical standards



Enrico Frumento

Smart meter gateways (#40)



Kim Nordström, ETSI

Standards for consumer IoT (#31-#34)



Mohamad Hajj

Hypervisors and Containers (#35)

[www.cyberstand.eu](http://www.cyberstand.eu)



Co-funded by  
the European Union



# Product Specific Standards – Smart Meter Gateways (SMGW)

CEN/CLC/JTC 13 WG6 Rapporteur Enrico Frumento

[www.cyberstand.eu](http://www.cyberstand.eu)



Co-funded by  
the European Union



**ECCC**  
EUROPEAN CYBERSECURITY  
COMPETENCE CENTRE

## Who am I

- ENRICO FRUMENTO, rapporteur CEN/CLC/JTC 13 WG6
- LinkedIn: [www.linkedin.com/in/enricofrumento/](https://www.linkedin.com/in/enricofrumento/)
- E-mail: [cenelec-wg6@cefriel.com](mailto:cenelec-wg6@cefriel.com)



## Forewords ...

## Who we are

CEN, CENELEC and ETSI officially recognised as European Standards Organizations  
(Regulation EU 1025/2012)



Standardization in various  
business sectors



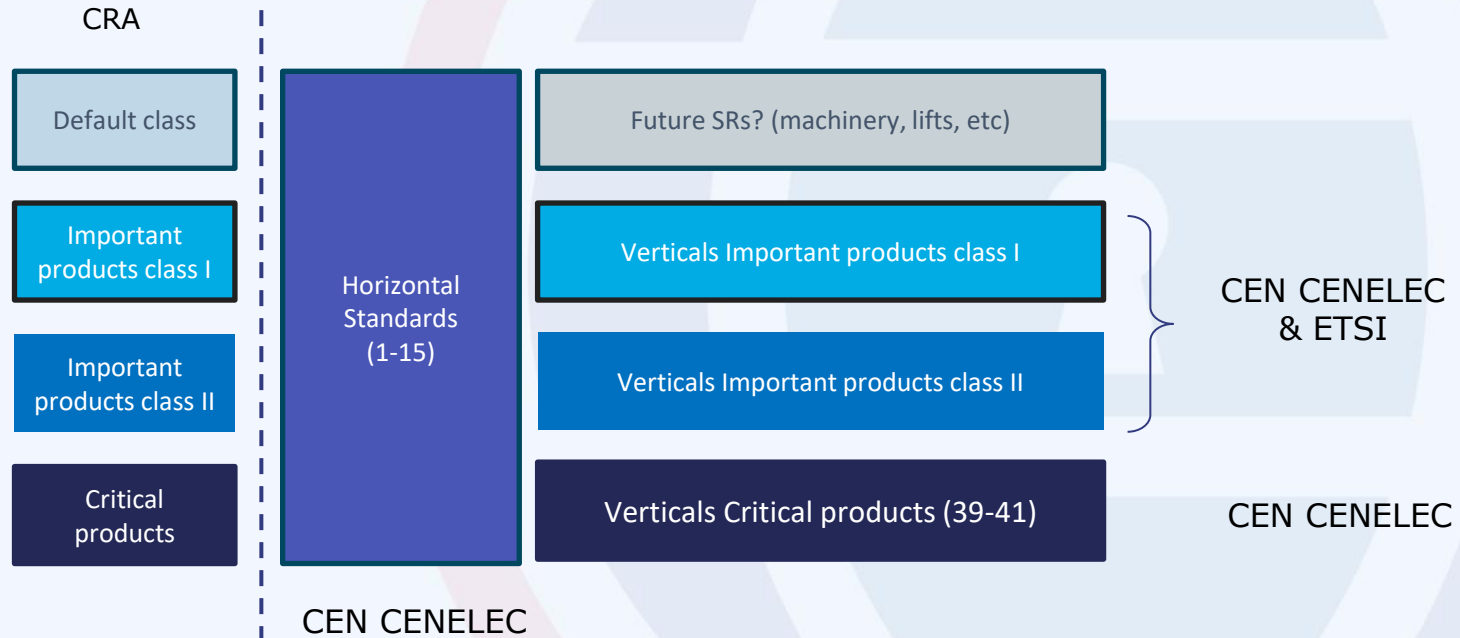
Standardization in the  
Electrotechnology sector



Telecommunications, broadcasting  
and other electronic communications  
networks and services

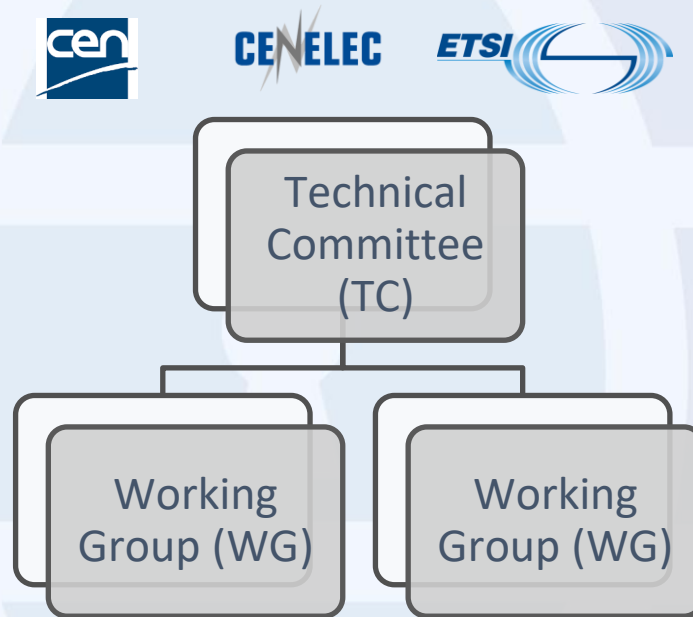


## Requested standards: entries 1-41 Annex 1 SReq



## How is the work organised?

- The standards are developed in Technical Committees (TC)
- Each TC has Working Groups (WGs)
- Each WG has a dedicated scope
- All requested standards are assigned to a Working Group according to the expected scope





## Entries 1-41 Annex 1 SReq

CEN-CLC/  
JTC 13 WG 9

#1 to 15  
Horizontal  
standards

### **CEN-CLC/JTC 13 WG 9 “Special Working Group on Cyber Resilience Act”**

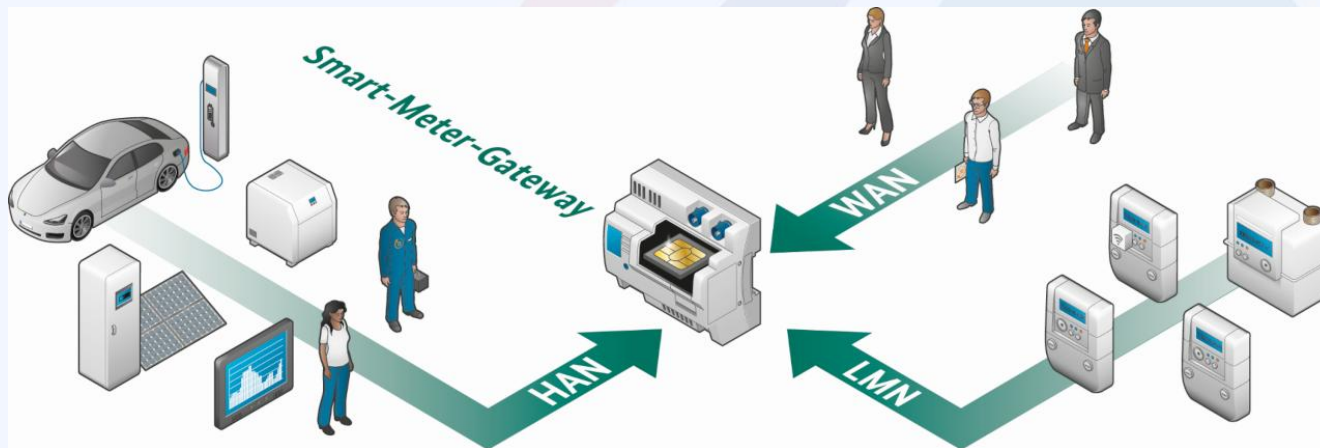
Principles for cyber resilience (line 1)  
Generic Security Requirements (line 2-14)  
Vulnerability handling (line 15)

## Standard development effort

- EU request for a harmonised standard for SMGWs
- Coverage of Article 2(23) of Directive 2019/944
- Presumption of conformity foreseen
- **Deadline for publishing: 30 October 2026**
- Ref. Standardisation Request from the Commission, Annex I (3.2.2025) – [Here](#)

### CEN/CLC/JTC 13 support the development of CRA-compliant standards

- Coverage of both horizontal and vertical standards
- WG6 leads the effort for SMGWs in **coordination with horizontal standards' guidelines defined by WG9 (general principles of cyber resilience, vulnerability handling)**



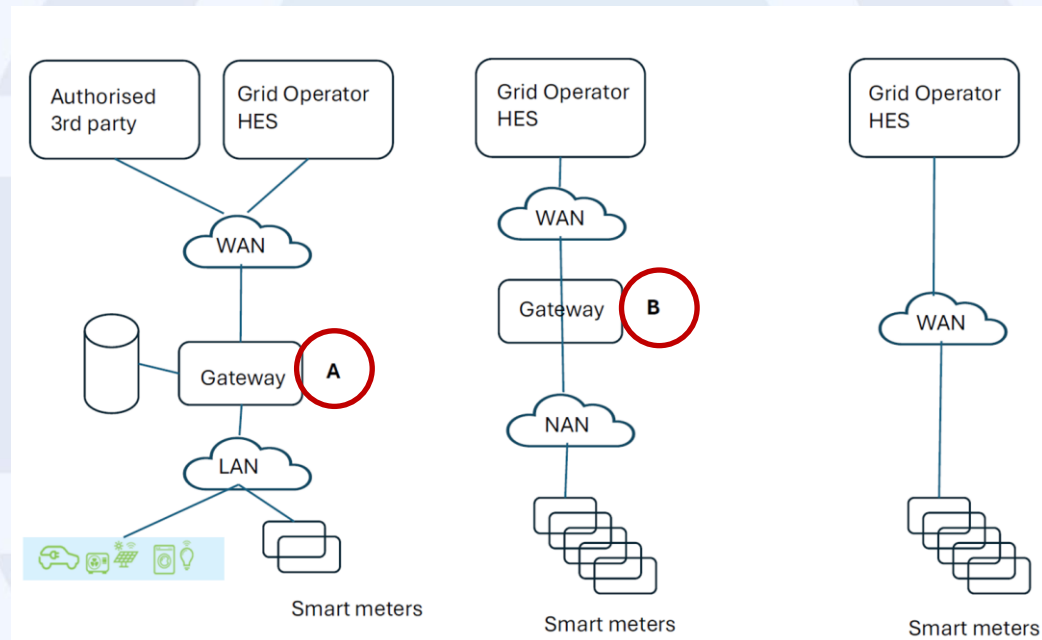
- **WAN:** Wide Area Network (either public or private)
- **LAN:** Local Area Network
- **NAN:** Neighbourhood Area Network
- **HES:** Head End System (for meter data collection)

## • Gateway A:

- typically located inside a consumer's premises
- able to control local consumption, generation and storage
- able to store and process metering data
- enables access by authorised 3rd parties
- considered a CRA critical gateway

## • Gateway B:

- typically located at the substation level (protected environment)
- connected to smart meters in a neighbourhood
- passes through encrypted metering data without decryption
- includes Data Concentrators and Remote Data Processing RDPs, if not autonomous



# Smart Meters vs Smart Meter Gateways

- Smart Meters: measure energy consumption
- Smart Meter Gateways (SMGW): aggregate, secure, and forward data to enable **secure communication** with utilities and third parties



Veo

## Smart Meter Gateways

Definition by the Directive on internal market for electricity 2019/944(EU), Article 2(23):

*“smart metering system” means an electronic system that is capable of measuring electricity fed into the grid or electricity consumed from the grid, providing more information than a conventional meter, and that is capable of transmitting and receiving data for information, monitoring and control purposes, using a form of electronic communication*

## Why security in SMGW context?

- Critical infrastructure component
- Risks: data interception, manipulation, unauthorised access, privacy, critical infrastructure take down in a cyber-warfare context, etc.
- **EU concern:** grid stability and user privacy

# Why security in SMGW context?

## Known Attacks

- Firmware manipulation and backdoors
- Access to historical consumption data
- Weak encryption in some deployments
- ENISA: lack of standardised, updated risk assessments



# Why security in SMGW context?

## Examples of Known Attacks

- **May 2023 – Denmark:** a significant sector-wide attack infiltrated 22 energy companies using operational-technology (OT) malware. Though specifics about smart meter gateways were limited, such gateways are considered part of the OT network for metering and grid control – [Source](#)
- Researches across Europe confirm that smart meter gateways are **vulnerable via firmware, network interfaces, and compromised SIM or API access (not only)**, opening doors to remote manipulation, data alteration, and even grid disruption – [Source](#), [Source](#)

## Classification of SMGWs by the CRA

Reference in the Standardization Request from the Commission, Annex I (3.2.2025):

- |     |                                                                                                                                                                                                                                                                            |
|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 40. | European standard(s) on essential cybersecurity requirements for smart meter gateways within smart metering systems <u>as defined in Article 2 (23) of Directive (EU) 2019/944</u> and other devices for advanced security purposes, including for secure cryptoprocessing |
|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

# Classification of SMGWs by the CRA

As defined by Article 7 of CRA, smart meter gateways fall within the category of **critical products**, entailing the **highest level of compliance obligations** by manufacturers producing such items:

## ANNEX IV

### CRITICAL PRODUCTS WITH DIGITAL ELEMENTS

1. Hardware Devices with Security Boxes
2. Smart meter gateways within smart metering systems as defined in Article 2, point (23) of Directive (EU) 2019/944 of the European Parliament and of the Council <sup>(1)</sup> and other devices for advanced security purposes, including for secure cryptoprocessing
3. Smartcards or similar devices, including secure elements

## Drafting more precise definition

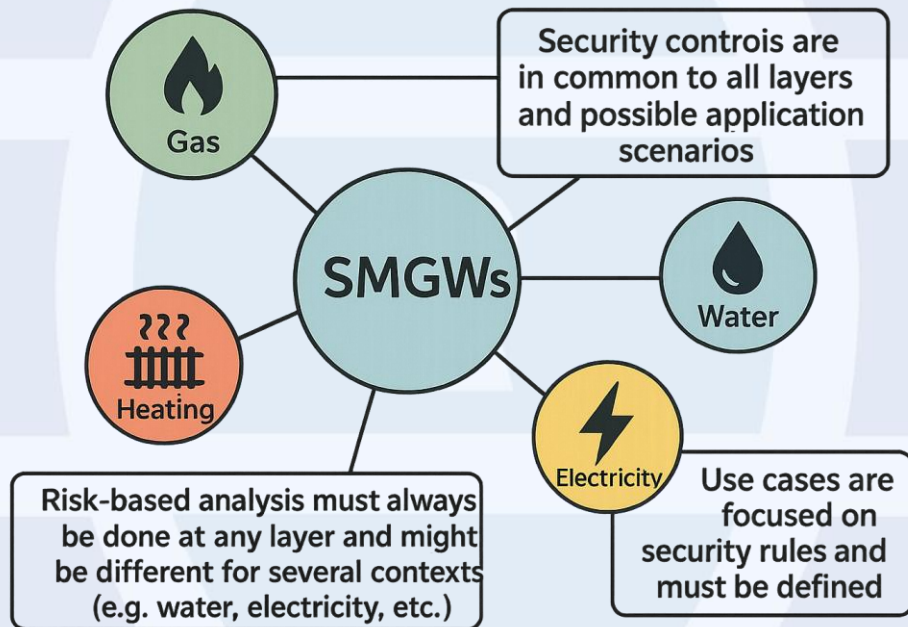
- Definition by the Draft of Implementing Regulation 13.3.2025:

This category includes but is not limited to smart meter gateways related to smart metering systems measuring electricity as defined in Article 2(23) of Directive (EU) 2019/944. It may also include other smart metering systems measuring consumption of other sources of energy such as gas or heat.

- The Implementing Regulation extends the definition of SMGWs to **other energy sources beyond electricity**
- Such industries have **some security requirements in common, but** also present specific requirements due to the **different risks** they are subject to

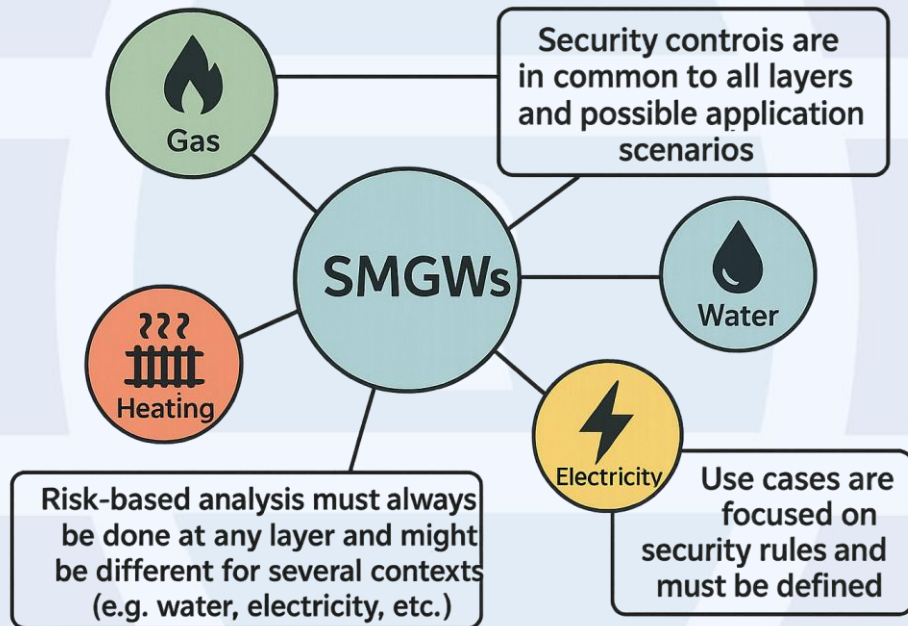
## Challenges arising!

- **Broaden** the range of SMGWs to encompass gas, water, and heat
- **Tailor** security requirements to the specific commodity and surrounding environment
- **Adopt** risk-based security rules that are targeted to specific use cases



## Challenges arising!

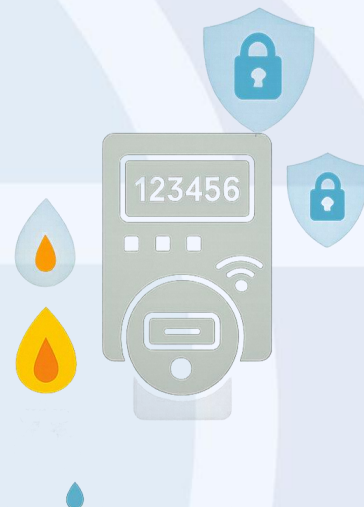
- Different environments imply **different risks** (e.g., the electricity grid is a bi-directional system while gas/water grids are often unidirectional)
- **Use-case sensitivity** is critical in risk evaluation
- The **strategic importance** of grids is relevant
- **Finding the proper depth of requirements** is necessary to avoid obsolescence and achieve proper coverage





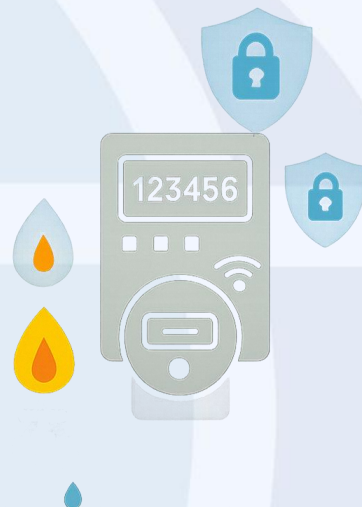
## Challenges arising!

- **Security Features of SMGWs vary across Europe**
- **Smart Meter Gateways (SMGWs) aren't one-size-fits-all**; they're a patchwork of varied security capabilities, shaped by differing national requirements
- **For example, Germany:** its BSI-backed Protection Profile (BSI-CC-PP-0073, TR-03109) mandates rigorous Common Criteria certification for SMGWs, setting a high bar
- **Elsewhere in the EU**, SMGW security levels — and what qualifies as 'critical' — remain instead undefined
- Such complexity raises fundamental questions we discussing: which devices must meet the Standard? **How do you draw the line?**
- **Presumption of Conformity**



## Which kind of challenge JTC 13 WG6 addresses

- These are precisely the kind of topics we are addressing in CEN/CLC/JTC 13 - WG6
- We announce an upcoming webinar on the smart meter gateway! While the date has yet to be confirmed, this event will include an engaging deep-dive session designed to connect with stakeholders. Details will be communicated via official CEN/CLC channels.





# Challenges arising!

## Modern risk assessment

- Risks must be considered along the whole device's lifecycle, from manufacturing to deployment
- The standard should **account for acceptable market practices**
- The assessment is relevant for cloud providers, integrators, and OEMs



## Call to Action

- Interested in joining the CEN/CLC/JTC 13 WG6?
  - Become a contributing member
  - Influence EU-wide cybersecurity requirements
  - Position your products early for CRA compliance
  - Gain visibility and technical insight
  - Embrace challenging task 🤔
- 
- ENRICO FRUMENTO, rapporteur WG6
  - Linkedin: [www.linkedin.com/in/enricofrumento/](https://www.linkedin.com/in/enricofrumento/)
  - E-mail: [cenelec-wg6@cefriel.com](mailto:cenelec-wg6@cefriel.com)





These are preliminary timelines that are essential to meet the deadline of October 2026.

# Thanks for your patience

[www.cyberstand.eu](http://www.cyberstand.eu)



Co-funded by  
the European Union



**ECCC**  
EUROPEAN CYBERSECURITY  
COMPETENCE CENTRE



European Standardization Organizations

# CRA vertical harmonised cybersecurity standard for Hypervisors & Container Runtime Systems

Presenter: Mohamad Hajj – Internet of Trust

Event: CYBERSTAND.eu – Impacting the CRA: Defining Standards for the Future

Date: 19 June 2025

Location: Brussels

# Agenda

- ▶ Development Timeline
- ▶ CRA classification and definition of Hyper and CRS
- ▶ Scope
- ▶ Relation with other ongoing CRA vertical standards
- ▶ Structure of the working draft
- ▶ Representative Use Cases
- ▶ Risk assessment methodology
- ▶ Security Requirements
- ▶ Security Levels and Requirement Selection
- ▶ Next Steps

# Development Timeline

- ▶ Developed under ETSI TC Cyber
- ▶ WI reference number : DEN/CYBER-EUS-0016EN 304 635
- ▶ Scope: Development of a vertical harmonised standard for cybersecurity requirements of hypervisors and container runtime systems, as defined under Article 10 of the CRA



# Why is this standard needed?

- ▶ Hypervisors and container runtime systems are classified as "Important Products" under Class II of the CRA.
- ▶ Virtualization & containerization are core technologies for cloud, telecom, and enterprise IT.
- ▶ Security weaknesses in hypervisors & containers can lead to system-wide compromise.
- ▶ A harmonized standard is essential to ensure compliance with the CRA requirements, providing clear security expectations for manufacturers, cloud providers, and enterprises.



# CRA classification and definition of Hyper and CRS

## ► **CRA Classification:** Important product, Class II

As defined in ANNEXES to the Commission Implementing Regulation on the technical description of the categories of important and critical products with digital elements pursuant to Regulation (EU) 2024/2847 of the European Parliament and of the Council:

### What is a Hypervisor?

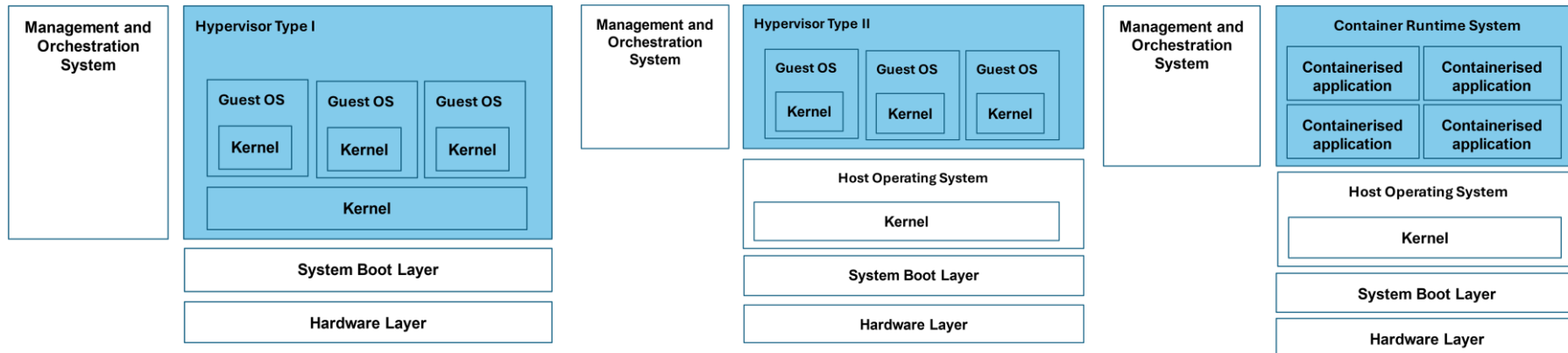
- Definition:  
A hypervisor is software that mediates access to physical resources and enables the execution of virtual machines (VMs).
- Deployment Types:
  - Type 1 Hypervisors: Run directly on hardware (bare-metal)
  - Type 2 Hypervisors: Run on top of a host OS
  - Hybrid Hypervisors: Combine aspects of both types
- Purpose:
  - Isolate and manage multiple VMs
  - Provide access control to CPU, memory, storage, and network

### What is a Container Runtime System (CRS)?

- Definition:  
A container runtime is software that manages the lifecycle of containers — lightweight, portable software packages that run isolated processes.
- Functionality:
  - Start/stop containers
  - Allocate system resources
  - Ensure process and file system isolation
- Virtualisation Type:
  - OS-level or application-level isolation

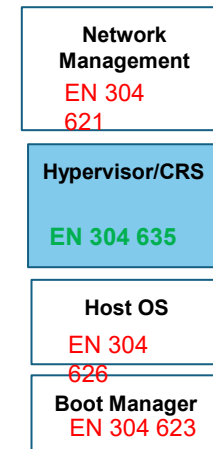
# Scope

- ▶ In-Scope
  - ▶ Hypervisor Type 1, Type 2
  - ▶ Container Runtime System
- ▶ Out of Scope:
  - ▶ HW
  - ▶ Host OS
  - ▶ Applications
  - ▶ Boot Layer
  - ▶ Management and orchestration



# Relation with other ongoing CRA vertical standards

- ▶ Other vertical CRA standards related to the operational environment of Hypervisors and Container Runtime Systems (CRS) are currently under development.
- ▶ Alignment is essential to ensure consistency across interconnected components.
- ▶ Related standards in progress:
  - ▶ EN 303 621 – Network Management
  - ▶ EN 303 626 – Host Operating System
  - ▶ EN 303 623 – Boot Managers



# Structuring options of the standard

## Option 1: One unified standard with modular parts

Part 1: Common security requirements

Part 2: Technology specific modules: Hypervisors, Container Runtime Systems

Part 3: Deployment models: Client, Server

- **Advantage:** Easy to reference and maintain as one standard; avoids fragmentation.
- **Challenge:** The document may become lengthy or complex.

## Option 2: Two standards

Standard A:  
Hypervisor (client, server)

Standard B:  
Container Runtime Systems (client, server)

- **Advantage:** Clear separation by technology.
- **Challenge:** Risk of overlap and inconsistency without a central coordinating document.

## Option 3: Core standard + Sub-standards

Main standard:  
General security requirements

Sub-standard A:  
Hypervisor (client, server)

Sub-standard B:  
Container Runtime Systems (client, server)

- **Advantage:** Promotes consistency and modularity; aligns well with how other EU standards are structured.
- **Challenge:** Requires coordination and clear mapping between the main and sub-documents.

- ▶ **Strong interest in Option 2 or 3**
- ▶ **No final decision has been made at this stage**

# Structure of the working draft

## Table of Contents

- ▶ Current drafting approach:
  - ▶ A single working document captures both generic and product-specific requirements
  - ▶ Designed to facilitate review and feedback
  
- ▶ Flexibility:
  - ▶ The structure allows for easy splitting into two or three separate standards if needed

✓ 4 Compliant Products
> 4.1 Hypervisor
> 4.2 CRS
✓ 5 Representative Use Cases
5.1 Purpose and Rationale
> 5.2 Use Cases for Hypervisors
> 5.3 Use Cases for CRS
5.4 Use Case to Risk Mapping Table
> 6 Security Levels and Requirement Selection
✓ 7 Security Problem Definition
7.1 Assets
7.2 Threats
7.3 Assumptions
7.4 Risk Assessment
✓ 8 Generic Security Requirements
8.1 Isolation
8.2 Integrity Protection
8.3 Authentication
8.4 Authorisation
8.5 Confidentiality Protection
8.6 Availability and Resilience
8.7 Logging
8.8 Patches and Updates
8.9 Secure Configuration
8.10 Secure by Default
8.11 Time Synchronisation
✓ 9 Instantiated Hypervisor Security Requirements
> 9.1 Hypervisor Requirements
9.2 Applicability of Hypervisor Requirements to Type I and Type II
✓ 10 Instantiated Container Security Requirements
> 10.1 CRS Requirements
✓ 10 Requirement Classification by Security Level
10.1 Hypervisor
10.2 CRS
11 Assurance Security Requirements
> Annex A (informative): Cybersecurity Risk Assessment Methodology
Annex B (informative): CRA Mapping Table
> Annex C (normative or informative): Threat-to-Requirement-to-Control Traceability Matrix
> Annex D (normative or informative): Use Case to Requirement Applicability Matrix

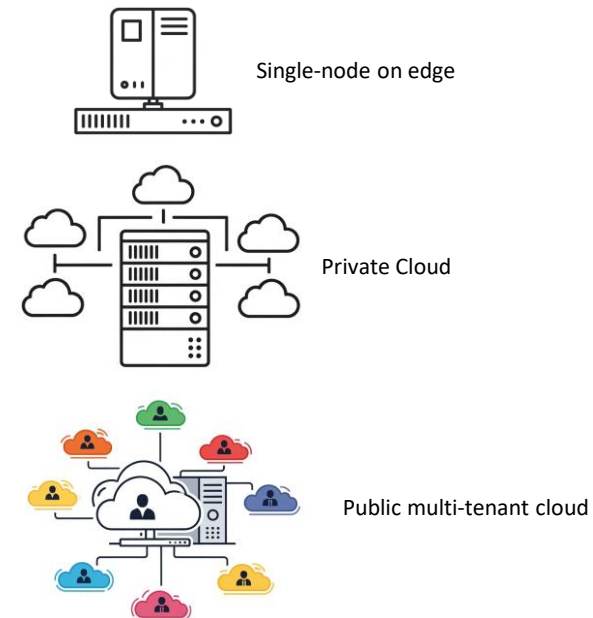
# Phased approach to standard creation

- ▶ Phase 1: Scope definition (In-scope, out of scope)
- ▶ Phase 2: Identification of representative use cases that reflect real-world deployment scenarios across product types.
- ▶ Phase 2: Definition of the SPM (Security Problem Definition): Assets, Threats, Assumptions
- ▶ Phase 3: Definition and classification of security requirements
  - ▶ Conduct a risk assessment based on the previously defined use cases and threat landscape.
  - ▶ Derive security requirements (both functional and assurance) aligned with the risk profile.
  - ▶ Introduce a classification approach for the requirements, enabling:
    - ▶ Clear prioritization based on risk
    - ▶ Flexibility for manufacturers to select applicable requirements based on the product type and use case

# Representative Use Cases (1/2)

- ▶ The CRA mandates a proportionality principle:
  - ▶ *Security measures must be appropriate to the cyber risks posed by the product (CRA, Recitals 30–33, Articles 6 & 10).*
- ▶ Use cases clarify:
  - ▶ What risks the product faces in different operating environments
  - ▶ What essential requirements (Annex I) are most relevant in each case

Product	Use Case	Description
Hypervisor	UC-H1	Single-node hypervisor on edge device for isolated, non-critical functions
Hypervisor	UC-H2	Enterprise private cloud hypervisor
Hypervisor	UC-H3	Cloud hypervisor in multi-tenant IaaS
CRS	UC-C1	Standalone CRS on edge device for isolated, non-critical functions
CRS	UC-C2	CRS integrated with on-prem orchestration
CRS	UC-C3	CRS as runtime for multi-tenant cloud



# Representative Use Cases (2/2)

- ▶ Not all use cases face the same threats.
  - ▶ E.g., a hypervisor in a cloud platform faces multi-tenant risks, unlike a standalone industrial node.
  
- ▶ CRA requirements apply differently.
  - ▶ Some requirements (e.g., runtime isolation) are critical in high-risk scenarios but less relevant in low-risk ones.
  
- ▶ Supports risk-based classification.
  
- ▶ Guides implementation and evaluation.
  - ▶ Helps both manufacturers and assessors tailor security requirements to the deployment context.



# Risk assessment methodology (1/3)

- ▶ The risk assessment methodology is detailed in a dedicated annex.
- ▶ It is intended as guidance to help manufacturers assess cybersecurity risks based on their product's use case and deployment context.
- ▶ The approach is aligned with the principles outlined in PT1.

## Likelihood Factors

Factor	Weight (x)	Description	Example Sub-Criteria
<b>1. Connectivity/Exposure</b>	x3	Extent of network exposure & access to untrusted networks	External Network Access, Internal Network Access
<b>3. Administrative Complexity</b>	x2	Complexity of management & number of administrators	Number of Admins, Admin Turnover, IAM Integration
<b>4. Configuration Volatility</b>	x1	Frequency of changes & scale of deployments	Change Frequency, Scale (No. of VMs/Containers)

## Impact Factors

Factor	Weight (x)	Description	Example Sub-Criteria
<b>2. Impact of Compromise</b>	x4	Severity of consequences on safety, operations, and data	Safety/Critical Infrastructure, Data Sensitivity/Loss
<b>5. Integration with Critical Systems</b>	x2	Dependence on & interaction with other critical systems	Orchestration Systems, Backup/Recovery Systems

# Risk assessment methodology (2/3)

## Step-by-Step: Calculate likelihood & impact scores

1. **Weighted sum:** Sum the scores of the sub-criteria within each factor, then multiply by the factor's weight.
  1. Total Likelihood Score = (Sum of Connectivity/Exposure Scores \* 3) + (Sum of Admin Complexity Scores \* 2) + (Sum of Config Volatility Scores \* 1)
  2. Total Impact Score = (Sum of Impact of Compromise Scores \* 4) + (Sum of Integration Scores \* 2)
2. **Map to levels:**
  1. **Likelihood score ranges:**
    1. 10-18: Rare (1)
    2. 19-29: Unlikely (2)
    3. 30-37: Possible (3)
    4. 38-42: Likely (4)
  2. **Impact score ranges:**
    1. 10-18: Low (1)
    2. 19-26: Medium (2)
    3. 27-32: High (3)
    4. 33-36: Critical (4)

Likelihood Impact	1=Rare	2=Unlikely	3=Possible	4=Likely
4=Critical	Medium	High	High	Critical
3=High	Medium	Medium	High	High
2=Medium	Low	Medium	Medium	High
1=Low	Low	Low	Low	Medium

**The intersection of the derived likelihood level and derived impact level determines the risk for that specific Use Case**

# Risk assessment methodology (3/3)

## Example: UC-H1 Hypervisor (Low Risk)

- Single-node, isolated, non-critical edge hypervisor. Containers host static applications.
- Key characteristics:
  - High isolation, minimal connectivity.
  - Low administrative complexity (1-2 admins, no IAM).
  - Static configuration, very small scale.
  - No impact on safety, critical infra, or sensitive data.
- Calculated scores:
  - Total Weighted Likelihood: 14 (Maps to Rare / Score 1)
  - Total Weighted Impact: 12 (Maps to Low / Score 1)
- Result (from Risk Matrix): Low Risk

Product	Use Case	Description	Risk Level
Hypervisor	UC-H1	Single-node hypervisor on edge device for isolated, non-critical functions	Low
Hypervisor	UC-H2	Enterprise private cloud hypervisor	Medium
Hypervisor	UC-H3	Cloud hypervisor in multi-tenant IaaS	High
CRS	UC-C1	Standalone CRS on edge device for isolated, non-critical functions	Low
CRS	UC-C2	CRS integrated with on-prem orchestration	Medium
CRS	UC-C3	CRS as runtime for multi-tenant cloud	High

# Security Requirements

## Exampe: Isolation

### Generic

REQ-GR-ISO-001: The product shall enforce isolation between workloads, administrative functions, and network domains to prevent unauthorised access, interference, or leakage across logical boundaries.

### Hypervisor

REQ-H-ISO-001: The Hypervisor shall enforce strict separation between virtual machines at CPU, memory, and I/O levels using hardware-assisted isolation mechanisms.

EXAMPLE: such hardware-assisted isolation mechanisms include Intel VT-x/AMD-V (CPU virtualisation), Intel EPT/AMD RVI (memory virtualisation), IOMMU (I/O virtualisation).

REQ-H-ISO-002: The Hypervisor shall isolate administrative functions and interfaces from guest workloads, preventing guest VMs from gaining unauthorized privileges over, influencing, or bypassing control plane operations.

EXAMPLE: such administrative functions and interfaces include VM lifecycle management, hypervisor CLI/API, remote APIs.

REQ-H-ISO-003: The Hypervisor shall enforce strict logical and/or physical isolation between the management network, guest VM networks, and any host network segments to prevent unauthorised access, interference, or leakage between these planes, thereby mitigating lateral movement and protecting administrative interfaces.

### CRS

REQ-C-ISO-001: The CRS shall enforce strict separation between containers at the process, filesystem, network, and resource usage levels using OS-level isolation mechanisms.

EXAMPLE: Such OS-level mechanisms include Linux namespaces (PID, NET, MNT, UTS, IPC, USER), cgroups (CPU, memory, I/O limits), seccomp, and SELinux/AppArmor profiles.

REQ-C-ISO-002: The CRS shall enforce separation between container workloads and host administrative functions, including the runtime's own control interfaces.

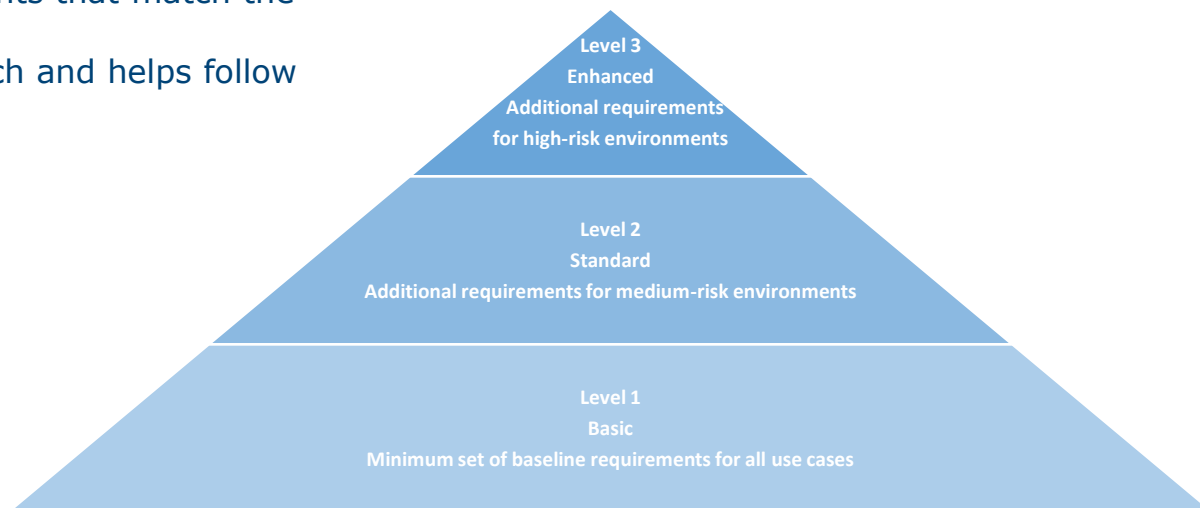
EXAMPLE: administrative functions include Docker socket, CRI interfaces, and control binaries executed with elevated privileges.

REQ-C-ISO-003: The CRS shall ensure management and orchestration interfaces are logically or physically isolated from container network traffic.

EXAMPLE: isolation may be implemented using separate CNI interfaces, service meshes, or host network restrictions.

# Security Levels and Requirement Selection (1/2)

- ▶ Security levels: What they mean
  - ▶ Three Security Levels for product requirements.
  - ▶ Help apply security requirements that match the product's risk.
  - ▶ Supports a risk-based approach and helps follow CRA rules.



# Security Levels and Requirement Selection (2/2)

## ► Requirement selection: How Manufacturers choose

### 1. Identify the most relevant use case

- Begin by consulting the provided example use cases to identify the one that most closely matches the product. These examples are intended as guidance and may not cover all deployment scenarios.

### 2. Use Case-based risk level assignment

- The example use cases are pre-mapped to risk levels using the proposed risk assessment methodology:
- UC-H1 / UC-C1 → Low-risk use case
- UC-H2 / UC-C2 → Medium-risk use case
- UC-H3 / UC-C3 → High-risk use case

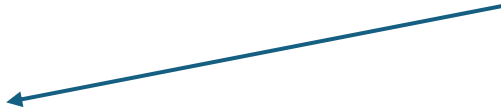
### 3. Handling custom or unlisted use cases

- If no example use case accurately represents the product context, manufacturers may define a custom use case. In such cases, the proposed risk assessment method could be applied to determine the appropriate risk level (Low, Medium, or High).

### 4. Determine the corresponding security level

- Once the risk level is established, it is used to select the appropriate Security Level, which drives the selection of applicable security requirements.

Product	Use Case	Description	Risk Level
Hypervisor	UC-H1	Single-node hypervisor on edge device for isolated, non-critical functions	Low
Hypervisor	UC-H2	Enterprise private cloud hypervisor	Medium
Hypervisor	UC-H3	Cloud hypervisor in multi-tenant IaaS	High
CRS	UC-C1	Standalone CRS on edge device for isolated, non-critical functions	Low
CRS	UC-C2	CRS integrated with on-prem orchestration	Medium
CRS	UC-C3	CRS as runtime for multi-tenant cloud	High



Use Case	Risk Level	Security Level	Notes
UC-H1 / UC-C1	Low	Level 1 – Basic	All requirements marked “Basic” are mandatory.
UC-H2 / UC-C2	Medium	Level 1 – Basic + Level 2 – Standard	Implement all requirements marked Basic + Standard.
UC-H3 / UC-C3	High	Level 1 – Basic + Level 2 – Standard + Level 3 – Enhanced	Implement Basic + Standard + Enhanced requirements.

# Next steps

- ▶ Continue developing the standard under ETSI TC CYBER WI
- ▶ Finalize the threat model
- ▶ Complete the risk assessment
- ▶ Define security requirements based on risks
- ▶ Check coverage against CRA essential requirements

# Call to action



- ▶ Collaboration with cloud providers, virtualization vendors, telecom operators, critical sectors, and regulators is crucial.
- ▶ ETSI delegates are invited to contribute to the standard development!
- ▶ Upcoming CEN-CENELEC events will provide structured opportunities for all stakeholders to review and provide feedback.
- ▶ Funding available via Cyberstand SSPs for contributions to this or any other vertical standard.



[www.cencenelec.eu](http://www.cencenelec.eu)

Follow us:    

Tag us [@Standards4EU](#)



# CRA harmonized standards for Consumer IoT products

Prepared by: Davide Pratone (ETSI EN 304 634 rapporteur)

For: CYBERSTAND - Impacting the CRA - Defining standards for the future

19/06/2025



# Agenda

- Consumer IoT Important Products
- ETSI WIs for the CRA Standardization Request
- Consumer IoT harmonized standard development



# Consumer IoT Important Products

REGULATION (EU) 2024/2847 – CRA set in Annex III the following Important Products with digital element (Class I):

- Smart home general purpose virtual assistants.
- Smart home products with security functionalities, including smart door locks, security cameras, baby monitoring systems and alarm systems.
- Internet connected toys covered by Directive 2009/48/EC of the European Parliament and of the Council that have social interactive features (e.g. speaking or filming) or that have location tracking features.
- Personal wearable products to be worn or placed on a human body that have a health monitoring (such as tracking) purpose and to which Regulation (EU) 2017/745 or (EU) No 2017/746 do not apply, or personal wearable products that are intended for the use by and for children



# Consumer IoT Important Products

Draft definitions from the ongoing CRA Implementing Regulation added some clarifications:

- Smart home general purpose virtual assistants.
  - Internet-connected products with digital elements that process natural language prompts allowing users to interact with the assistant and control connected devices in residential settings.
  - This category includes but is not limited to smart speakers and virtual assistant software that meet this definition.
- Smart home products with security functionalities, including smart door locks, security cameras, baby monitoring systems and alarm systems.
  - Products with digital elements intended to protect the physical security, including safety, of consumers in a residential setting and which can be controlled and managed remotely from other systems, as well as hardware and software intended to centrally control such products.
  - This category includes but is not limited to smart door locking devices, baby monitoring systems, alarm systems, home security cameras and smart smoke detectors
- Internet connected toys covered by Directive 2009/48/EC of the European Parliament and of the Council that have social interactive features (e.g. speaking or filming) or that have location tracking features.
  - Products with digital elements that are covered by Directive 2009/48/EC, connected or intended to be connected to internet, and that have embedded technologies that enable inbound and outbound communication, such as keyboard, microphone, speaker or camera, or technologies that enable tracking of the geographical location of the toy or its user, such as GPS or Bluetooth based functionalities.
  - This category does not include toys that do not track the full geographical location but merely detect the proximity of the toy to its user or to other toys.

# Consumer IoT Important Products

Draft definitions from the ongoing CRA Implementing Regulation added some clarifications:

- Personal wearable products to be worn or placed on a human body that have a health monitoring (such as tracking) purpose and to which Regulation (EU) 2017/745 or (EU) No 2017/746 do not apply, or personal wearable products that are intended for the use by and for children
  - Personal wearable products to be worn or placed on a human body that have a health monitoring purpose are products with digital elements that can be worn on the body directly or via clothing or accessories and that can, regularly or continuously, sense and further process information, including body metrics, relevant to the user's health, excluding products that fall within the scope of Regulation (EU) 2017/745 or of Regulation (EU) 2017/746.
  - This category includes but is not limited to fitness trackers, smartwatches, smart jewellery, smart clothing and sports apparel.
  - Personal wearable products that are intended for the use by and for children are products with digital elements which can be worn or placed on the body, directly or via clothing or accessories, of individuals under the age of 14.
  - This category includes but is not limited to child safety wearables.



# Consumer IoT Important Products



Smart speakers



Smart Door Lock



Internet Connected Toys



Smartwatches



Smartwatch with GPS tracking and Parental control



Complete baby monitoring system



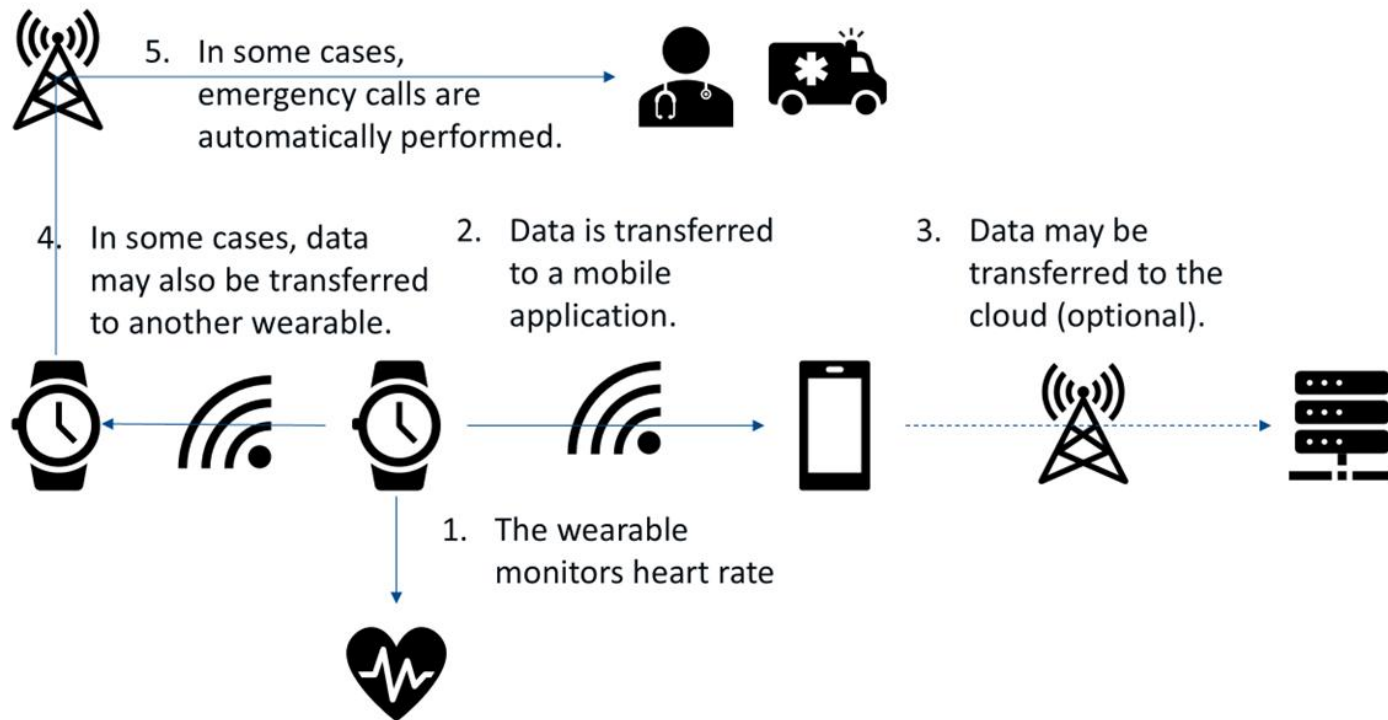
security cameras



Associated Mobile Applications

# Consumer IoT harmonized standard development

## Example of the use case scenario for the Wearable used for child safety





# Consumer IoT harmonized standard development

## Potential skeleton of an ETSI CRA Consumer IoT Vertical

1. Scope
2. Terms and Definitions
3. Requirements
  1. ECR CRA ANNEX I Part I (1)
    - a) Use a risk based approach following CEN/CLC JTC13 WG9 PT1
  2. ECR CRA ANNEX I Part I (2)
  3. ECR CRA ANNEX I Part II
    - b) Reference/Refine manufacturer's vulnerability handling requirements designed in CEN/CLC JTC13 WG9 PT3
4. Assessment Criteria
  1. ECR CRA ANNEX I Part I (1)
  2. ECR CRA ANNEX I Part I (2)
  3. ECR CRA ANNEX I Part II
5. Guidance (if appropriate)
  1. ECR CRA ANNEX I Part I (1)
  2. ECR CRA ANNEX I Part I (2)
  3. ECR CRA ANNEX I Part II
6. ANNEX Mapping to ETSI EN 303 645 / ETSI TS 103 701
7. ANNEX Covered/Not Covered Risks/Threats incl. rational

**Any questions?**

