INDUSTRIAL CYBERSECURITY CENTER

2025 EDITION

POSITION PAPER

INDUSTRIAL CRA

Multisectoral

Edition: 2025

Paseo de las Delicias, 30 - 2nd floor
28045 Madrid (Spain)
+34 910 910 751
info@cci-es.org
www.cci-es.org
blog.cci-es.org
@info_cci
www.linkedin.com/in/centrociberseguridadindustrial

El **Centro de Ciberseguridad Industrial (CCI)** es The Industrial Cybersecurity Center (CCI) is an independent, non-profit organization whose mission is to promote and contribute to the improvement of Industrial Cybersecurity, in a context where organizations in sectors such as manufacturing or energy play a critical role in building today's society, as pillars of the welfare state.

CCI addresses this challenge through the development of research and analysis activities, opinion generation, preparation and publication of studies and tools, and the exchange of information and knowledge on the influence of both technologies (including their processes and practices) and individuals, regarding risks —and their managemen— derived from the integration of industrial processes and infrastructures into Cyberspace.

Today, CCI is the ecosystem and meeting point for entities —private and public— and for professionals affected by, concerned about, or engaged in Industrial Cybersecurity; and it is also the Spanish-speaking reference for the exchange of experiences and for energizing the sectors involved in this field.

TIPS

Alt+Left arrow to return to the previous view after following a hyperlink

Click in our icon and visit our website

Clicking on the **on the cover** will show CCI activity in each of those countries

Clicking on the **page number** will return you to the table of contents

TABLE OF CONTENTS

INTRODUCTION

The approval of the Cyber Resilience Act (**CRA**) by the European Union marks **a regulatory milestone by requiring essential cybersecurity requirements and vulnerability management obligations for all products with digital elements**. This progress is **key to building a safer and more trustworthy digital market.** However, **its direct application in the industrial context**, especially in OT (Operational Technology) systems, **introduces a level of complexity that makes compliance impossible under the current framework: without a specific adaptation, the CRA cannot be applied effectively, efficiently, or fairly in industrial environments.**

OT environments are not an extension of traditional IT, but domains with their own characteristics: critical infrastructures with **highly specialized technologies, product life cycles of 15 to 30 years, a high degree of customization by integrators, and a constant requirement for operational availability.** Unlike the IT world, where security updates can be deployed frequently and flexibly, **in OT it is often not feasible to apply patches immediately without compromising service continuity, the physical safety of people, or the environment.**

In addition, a large portion of the systems in operation were designed at a time when cybersecurity was not a functional requirement. This means that **applying the same regulatory criteria to these systems as to today's digital products can generate disruptions, extra costs, and non-compliance scenarios that are difficult to justify.**

For this reason, the Industrial Cybersecurity Center (CCI) proposes the development of a **multisectoral Industrial CRA**: an adaptation of the European regulation that takes into account the singularities of the OT environment, aligned with the principles of cyber resilience, but articulated with criteria of proportionality, technical feasibility, and shared responsibility. This approach makes it possible to align CRA requirements with the proportionality principle of NIS2 and CER, adapting regulatory demands to the OT context.

The approach of "substantial modification" and "contextual evaluation" is already applied in Railway Interoperability and in the Medical Devices Regulation. Article 7 of the Interoperability Directive allows exceptions when compliance compromises economic viability.

This proposal is aimed at facilitating regulatory compliance in the industrial sector through a reference sectoral guide, enabling manufacturers, engineering firms, integrators, and OT operators to address CRA requirements with realism, operational safety, and effectiveness.

The proposal from CCI for the regulatory development of an Industrial CRA will serve as the basis for an industrial multisectoral guide (Transport, Electricity, Oil & Gas, Water, Chemical, Food, Health, Metallurgy, Manufacturing, and Infrastructure). This proposal takes into account:

- The extended life cycle existing in OT (15–30 years).
- The high level of customization and dependency on third parties.
- Technical limitations for applying patches and updates.
- The need for interoperability, operational continuity, and component certification.

[1] *https://eur-lex.europa.eu/ES/legal-content/summary/interoperability-between-eu-information-systems-in-the-field-of-freedom-security-and-justice.html*

ADAPTATION OF THE CYBER RESILIENCE ACT (CRA) TO OT ENVIRONMENTS

Guiding principles of the multisectoral Industrial CRA

Industrial risk-based approach

Not all industrial digital products face the same threat conditions nor the same probability of materialization. To harmonize risk analyses across different industrial environments, the approach must focus on threat factors and their probability, considering their effect on operational safety, business continuity, and risk to people or the environment. Based on these factors, products may be classified into three risk classes: **low (important class I), medium (important class II), and high (critical).**

Balance between security and operational availability

Any security measure must be compatible with the operational and functional continuity of the system through a Compensating Security Plan (principle of **"operational cyber resilience"**).

Graduality in requirements by life cycle

The Industrial CRA must establish a classification based on the **product obsolescence cycle**, distinguishing between **new, updated, in active operation, in support mode, and end-of-life components**. This classification will make it possible to **align vulnerability management with the level of support and maintenance available**, prioritizing early risk mitigation in products close to obsolescence or without available security updates.

Shared responsibility and coordination

The Industrial CRA recognizes that cybersecurity in operational technology requires co-responsibility among manufacturers, integrators, and operators. A clear allocation of obligations and coordination mechanisms among all parts of the ecosystem must be established.

Non-disruptiveness and progressive compatibility

The Industrial CRA will be applied progressively to avoid disruptions in critical infrastructures. **Backward compatibility will be encouraged, and practical mitigations (such as segmentation, compensating monitoring, or hardening) will be prioritized instead of direct requirements that are impossible to implement due to technical limitations.**

A **functional equivalence mechanism** is proposed: if the system implements adequate and sufficient technical compensating measures (segmentation, local recovery, etc.), it should be considered compliant.

Objetivo de la CRA Industrial	Aplicación concreta en la CRA Industrial
Avoid schemes that benefit only certain manufacturers and certification bodies	Define shared compliance schemes involving manufacturers, engineering firms, integrators, and OT operators.
Do not impose product certifications without operational context	Product evaluation within its OT system makes it possible to meet the spirit of Article 5 of the CRA (security throughout the full life cycle). We propose contextualized product evaluation within the system, thus performing a system-level analysis aligned with IEC 62443-3-3
Include multisectoral representativeness in certification	Enable participation of sector associations in sectoral CRA schemes. ENISA should coordinate and facilitate multisectoral OT forums, together with associations (CECIMO, UNIFE, Orgalim, ...) and SMEs.
Recognize the slowness and rigidity of certification processes	Adopt progressive, agile, adaptive mechanisms compatible with critical infrastructures
Promote self-regulation platforms with regulatory mapping and compensating security plans	CCI will facilitate the use of platforms such as MACIN, RECIN, ESCIM, based on IEC 62443 and recognized good practices or IEC-CRA mappings
Identify interaction between CRA–NIS2–AI Act–GDPR regulations	Include a regulatory mapping matrix in the Industrial CRA guide and build, with ENISA/CCI, a “toolkit” for industrial companies, with special focus on SMEs..
Industrial supply chain security	Develop an industrial supply chain security kit (industrial SBOM + sector threat models) and phased transition mechanisms to avoid disruptions in OEMs holding stock of non-certified components.
Training in the application of the Industrial CRA	Sectoral training, in collaboration with ENISA, industrial associations, and SMEs, linked to the CCI ecosystem.

ESSENTIAL REQUIREMENTS ADAPTED TO OT PRODUCTS

Industrial environments require a specific adaptation of essential cybersecurity requirements, taking into account operational limitations, coexistence with legacy systems, and sector reference standards. This section defines how the principles of **security by design, operational resilience, and risk and vulnerability** management should be applied according to the OT context, ensuring functional protection without compromising availability or the safety of industrial processes.

Design and development

- OT-specific risk assessment (based on IEC 62443-4-1 and 62443-3-3, or sector-adapted technical specifications such as IEC TS 50701:2021 – Railway applications – Cybersecurity).
- Security by design, but allowing alternative or compensating compliance with equivalent technical controls (external monitoring, golden images, etc.) for legacy environments.
- Attack surface limitation considering physical and logical constraints (serial ports, unauthenticated protocols, etc.).

Security properties (CRA adaptation)

- Ability to rapidly restore the system after a failure or cyber incident.
- Ability to operate safely in degraded mode.
- Event logging with secure timestamping (without requiring continuous NTP synchronization).
- Data encryption only where technically feasible without affecting critical latency.

Vulnerability management

- Technical review periodicity every 6 or 12 months (not continuous) and within the product obsolescence cycle.
- Vulnerability management and mitigation plans contextualized to the OT environment.
- Security updates differentiated from functional updates.
- • Shared vulnerability management procedure with the integrator and operator (collaborative model).
- OT-specific repository for coordinated disclosure (avoid CVE disclosure if not applicable). Publication **should be limited in critical sectors under justified exceptions due to risk to critical infrastructures.**

Protection as a system under real OT conditions

Protection in OT environments cannot be based solely on conventional digital mechanisms on a single component or device. It must consider the physical, logical, and operational limitations of industrial systems and their integration with existing infrastructure. This section describes how to apply authentication, supervision, resilience, and traceability controls under real conditions, ensuring effective defense without compromising continuity or functional safety of operations.

Adapted authentication and access control

- Network-based authentication mechanisms (static MAC/IP, ACLs on industrial switches) when it is not possible to authenticate on the device.
- Role-based OT segmentation (operator, maintainer, engineer) using industrial firewalls or managed switches as a compensating control.

Supervision and detection from the infrastructure

- Integrity monitoring from external systems (hashes or periodic checks from HMI/SCADA) for devices without local monitoring capabilities.
- Detection of anomalous traffic in industrial protocols (Modbus, S7, DNP3) using passive tools (OT-friendly IDS/IPS).

OT resilience and recovery

- Implementation of restorable “golden images” via physical console or engineering interface for post-incident recovery.
- Manual or automatic isolation capability (relay, interlocking relay, physical switches) as a response to anomalous behavior.

Modular secure architecture

- Design of trust zones and OT perimeters with clearly separated minimal critical functions (IEC 62443-3-2).
- Secure interconnection between domains through OT demilitarized zones (OT DMZ) or industrial gateways with deep inspection.

Security compatibility in constrained components

- Implementation of minimal functional security: physical authentication (keys, switches), hardware protection (secure boot via jumper).
- External firmware validation in each load cycle from SCADA systems (checksum prior to loading into the PLC).

Traceability without full synchronization dependency

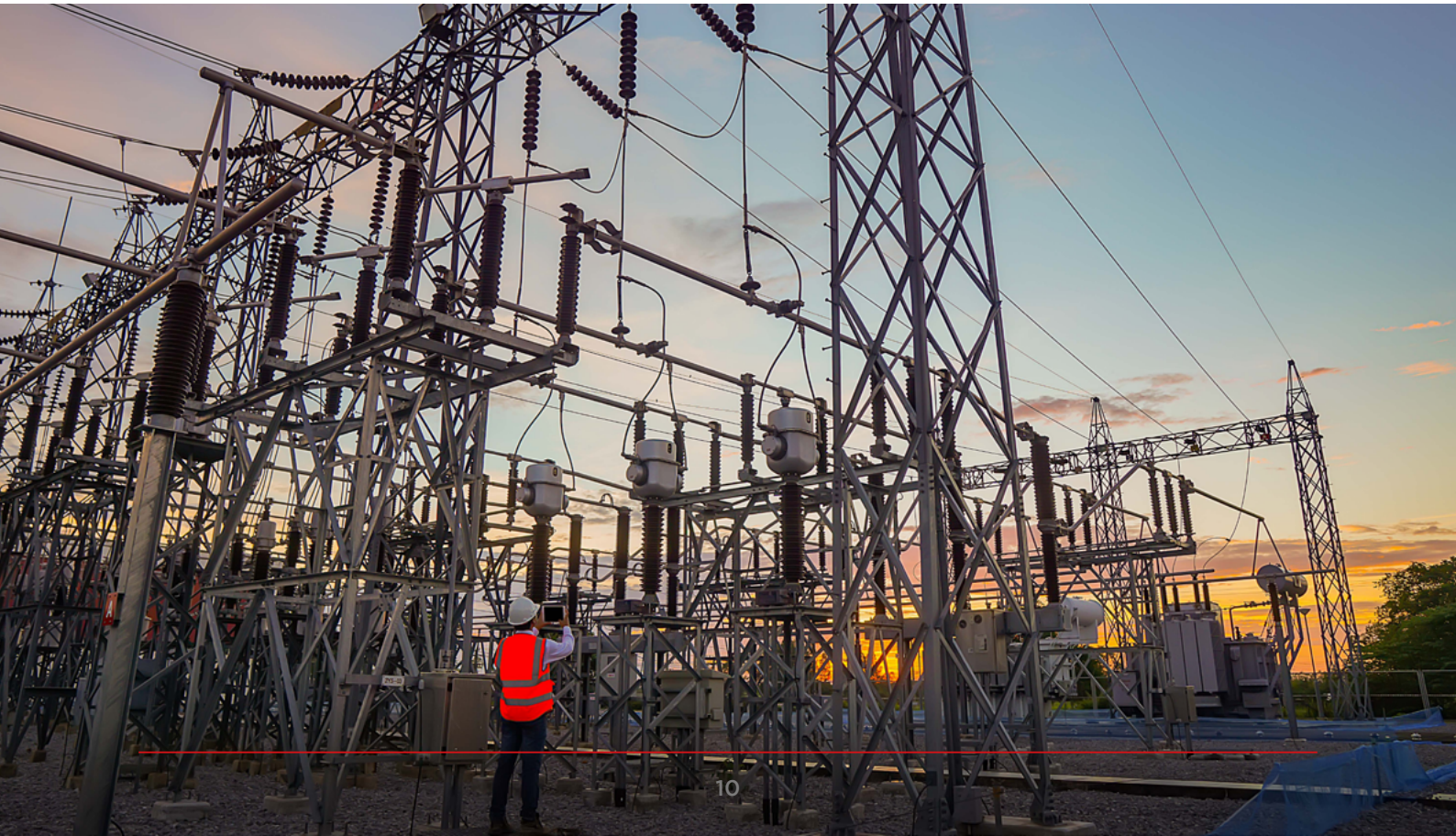
- Event logging with relative timestamping (marked from reference events) for systems without reliable RTC.
- Log storage in circular buffers and periodic collection from SCADA/OT EDR systems..

Secure configuration management

- Configuration comparison (running vs baseline) with periodic export from the engineering system.
- Digital signature of configuration and firmware files (even if not validated on the device, modification is detected during centralized collection).

Transition timelines and approach

STAGE	TIMEFRAME	COMMENT
CRA enters into force	2024 (already applicable)	According to the original text.
Start of Industrial CRA (OT)	June 2026	Pilot phase with sectoral guides.
Obligation for new products	December 2027	Same date as the general CRA. This is a *pilot phase with measurable results and traceability* that will facilitate extension to the rest.
Products already in operation	Until December 2032	5-year transition with “substantial modification” criteria.
Reporting obligation (Art. 14)	September 2027	Also applicable to existing industrial products.



Product classification and application context

OT product class	CRA level	Typical examples by sector	Classification criteria
Field devices	Important class I	Analog sensors, digital sensors, simple actuators, data acquisition units (DAU), non-critical monitoring IoT (temperature, humidity, vibrations)	No control logic; no autonomous execution capability; no direct remote access; limited impact in case of failure
SCADA and controllers	Important class II	Industrial SCADA, PLCs, RTUs, DCS, local control systems in production lines, HVAC controllers in plants, local automation	Control logic over physical processes; limited or indirect remote access; impact on operational continuity
OT network infrastructure	Important class II	Industrial switches, OT firewalls, industrial NAT, cell routers, industrial private networks, OT VPN access devices	Routes OT communications; does not execute control logic, but impacts availability and system visibility
Hybrid IT/OT systems	Important class II	Industrial gateways, industrial IoT devices, Historian, MES, industrial edge computing, connected analytics platforms	Integration between IT/ OT domains; exposed to interconnectivity risks; access to critical data; possible entry point to OT systems
Equipment in critical infrastructures (Electric, Transport, Water, SEVESO Chemical…)	Critical	PLCs in power grids (substation RTUs, IEDs), controllers in potable or wastewater plants, railway signaling systems (ERTMS, interlockings, TMS), controllers in SEVESO plants (reactors, boilers, tanks)	Severe impact on physical safety, environment, or continuity of essential service; possible target of high-impact attacks; subject to additional sector regulation (SEVESO, RED II, etc.)

Important Class I: A conformity assessment is required, but manufacturer self-assessment may be allowed in some cases.

Important Class II: Self-assessment is usually not sufficient. Third-party assessment is required, including vulnerability review and periodic updates.

Critical: Conformity assessment by a notified body is required, with periodic security reviews, active mitigation mechanisms, and rigorous cybersecurity-by-design processes.

Compliance requirements by role (Manufacturer, Integrator, Operator)

Requirement / Action	Manufacturer	Integrator	Operator
CRA Declaration of Conformity	✓		
Coordinated vulnerability management	✓	✓	✓
Life-cycle support (updates)	✓	✓	✓
Cybersecurity testing in OT environment	✓	✓	
Commissioning validation (conformity)		✓	✓
Continuous monitoring and periodic revalidation			✓
Security incident reporting	✓	✓	✓
Compensating security plan	✓*	✓*	✓

* Definition only

Key changes in Common Criteria for applicability in OT

1. Develop/adapt Protection Profiles (PPs) specific to OT components

Most PPs currently used (hardware security devices, network devices, TPMs) are focused on IT or generic products

Required change

Create OT-specific PPs for:

- PLCs (Programmable Logic Controllers).
- RTUs (Remote Terminal Units).
- IEDs (Intelligent Electronic Devices).
- Industrial gateways (Modbus, OPC UA).
- IoT gateways.
- SCADA systems and HMIs.

Follow an approach similar to ISA/IEC 62443-4-2 (technical requirements by type of industrial component).

2. Adjust Evaluation Assurance Levels (EALs) and requirements to OT life-cycle realiti

Higher EALs (EAL4, EAL5) require formal development and testing processes that many OT manufacturers do not follow. A multilevel certification is needed for use with the CRA, using modular approaches within the CRA.

Proposed changes

- Create evaluation profiles **justified by OT-specific risks** (latency, continuity, functional safety).
- Include models with **modular requirements**, less demanding but oriented to critical industrial environments.

3. Include OT threats and environmental conditions in security documents (ST)

Threats and assumptions (TOEs and SOs) are designed for IT environments, not industrial ones.

Proposed changes

- Include threats such as manipulation of physical signals, falsification of sensor data, denial of service against field devices, access to industrial buses, etc.
- Introduce **realistic OT operational conditions:** operation without shutdowns, remote access for maintenance, long update cycles.

4. Integrate interoperability with industrial protocols and zone-and-conduit architectures

Security in distributed and hierarchical architectures typical of OT is not considered.

Proposed changes

- Include in the profiles aspects of **secure interoperability between OT components:** authentication between PLCs and SCADA, segregation between IEC 62443 levels.
- Certify OT integration security, not only the individual product.

5. Incorporate functional safety indicators and sector regulatory requirements

Objective:

Integrate **functional safety (safety)** and **cybersecurity (security)** in a coherent framework that enables joint evaluation of OT systems' **operational reliability** and their **regulatory compliance** in each industrial sector.

Contexto:

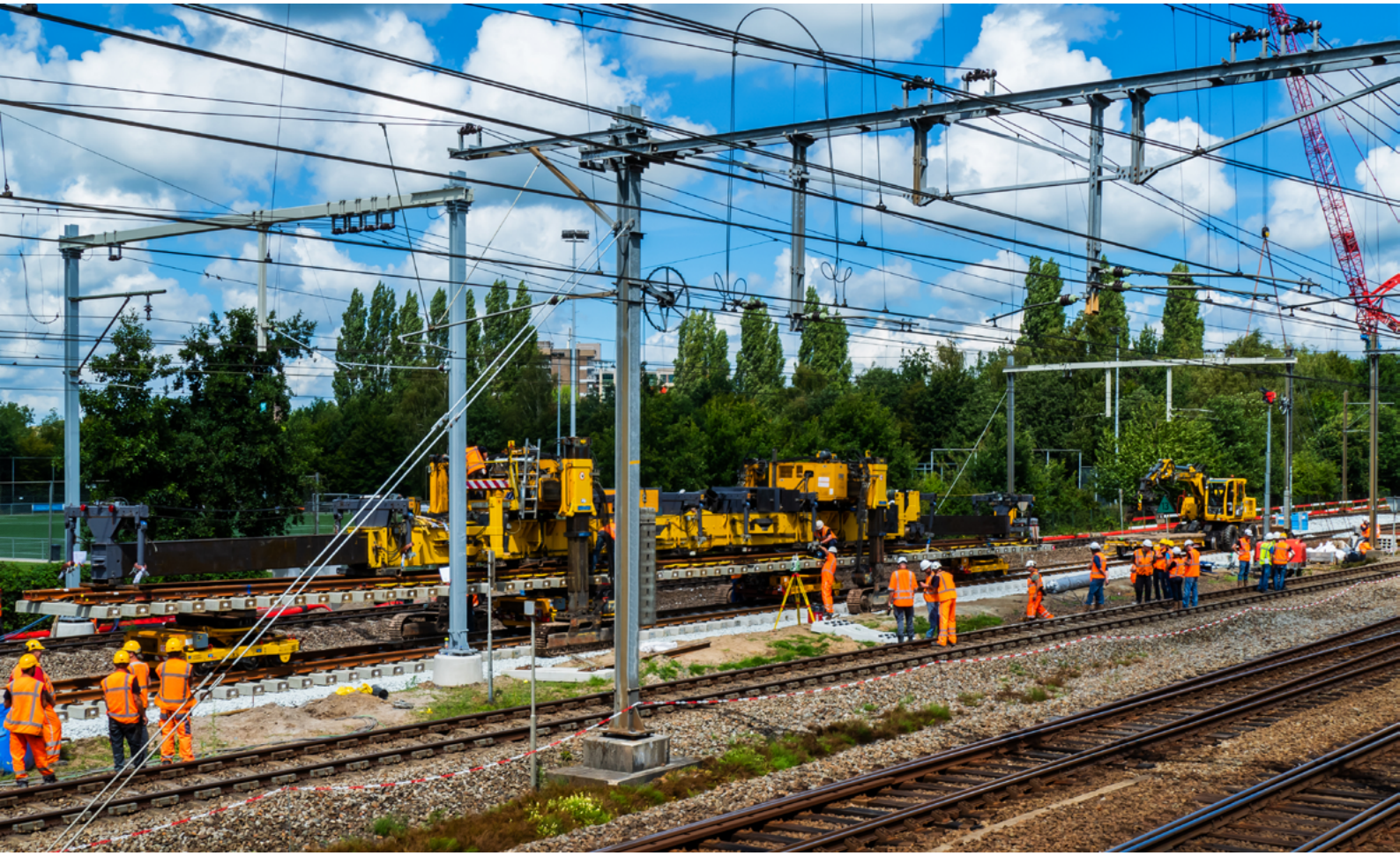
Some OT components are subject to functional safety standards such as **IEC 61508, IEC 61511, or IEC 62061,** which establish integrity levels and design and maintenance requirements. Integrating these with cybersecurity objectives is essential to ensure operational continuity and the protection of people and the environment.

Proposed changes:

- Include complementary **functional safety** information within Security Targets, incorporating data on SIL levels, fault detection mechanisms, and dependencies between control and protection functions.
- Establish **common functional safety and cybersecurity indicators** that allow measuring the combined performance of both domains.
- Promote **harmonization between European sector regulatory requirements** (energy, water, transport, manufacturing) and CRA and NIS2 compliance guides.

These changes require:

- **Pilot projects funded by Horizon Europe,** focused on multisector industrial *Pilot Projects* (PPs) (water, rail, energy, manufacturing), validating the practical integration of safety and security in real environments.
- **Inclusion of OT scenarios and threats within the EUCC (European Common Criteria)** scheme, to extend European recognition of certifications to industrial products and systems with functional safety impact.



Paseo de las Delicias, 30 - 2nd floor
28045 Madrid (Spain)

+34 910 910 751

info@cci-es.org
www.cci-es.org
blog.cci-es.org
@info_cci