RESILTECH | Technologies for Resilience

Resiltech s.r.l.

Current challenges in applying cyber-security in railway signaling systems according to current available cyber-security standards

The Speaker

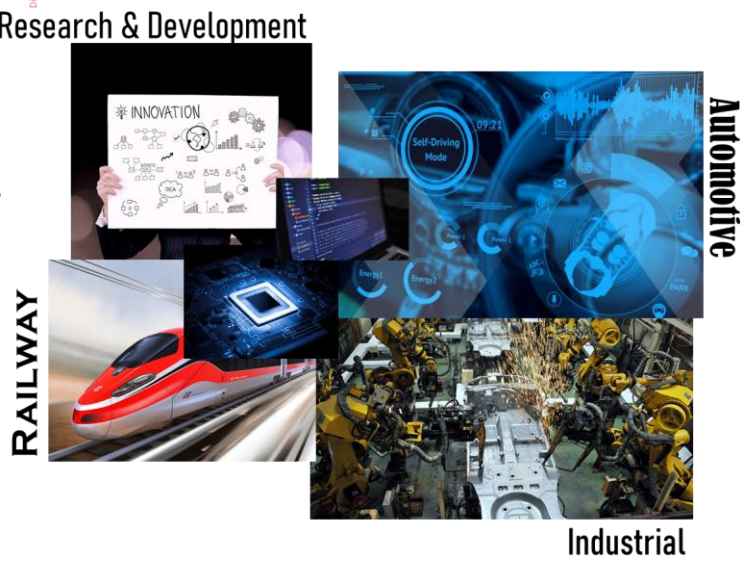
- Francecso Brancati
  - Francesco.Brancati@resiltech.com
- Present Position in ResilTech s.r.l.
  - Responsible for R&D innovations and co-funded projects
  - Responsible for Cybersecurity Services Business Development
- Education
  - MSc Degree, PhD in Computer Science
    - Università degli studi di Firenze
- Experience
  - Technical lead of ResilTech role in several R&D projects at EU level
  - Technical lead of safety critical SW development projects in Automotive area.
  - Member of the ISO TC22 / SC32 / WG8 Road Vehicle Functional safety
  - Member of the ISO TC22 / SC32 / WG11 Cybersecurity

ResilTech s.r.l.

Mission

To provide engineering consulting and design services to companies and public bodies mainly for, but not limited to, the field of resilient systems and infrastructures

ISO TC22/ SC32/WG8
ISO26262 functional safety
ISO TC22 / SC 32 / WG11
ISO 21434 cybersecurity

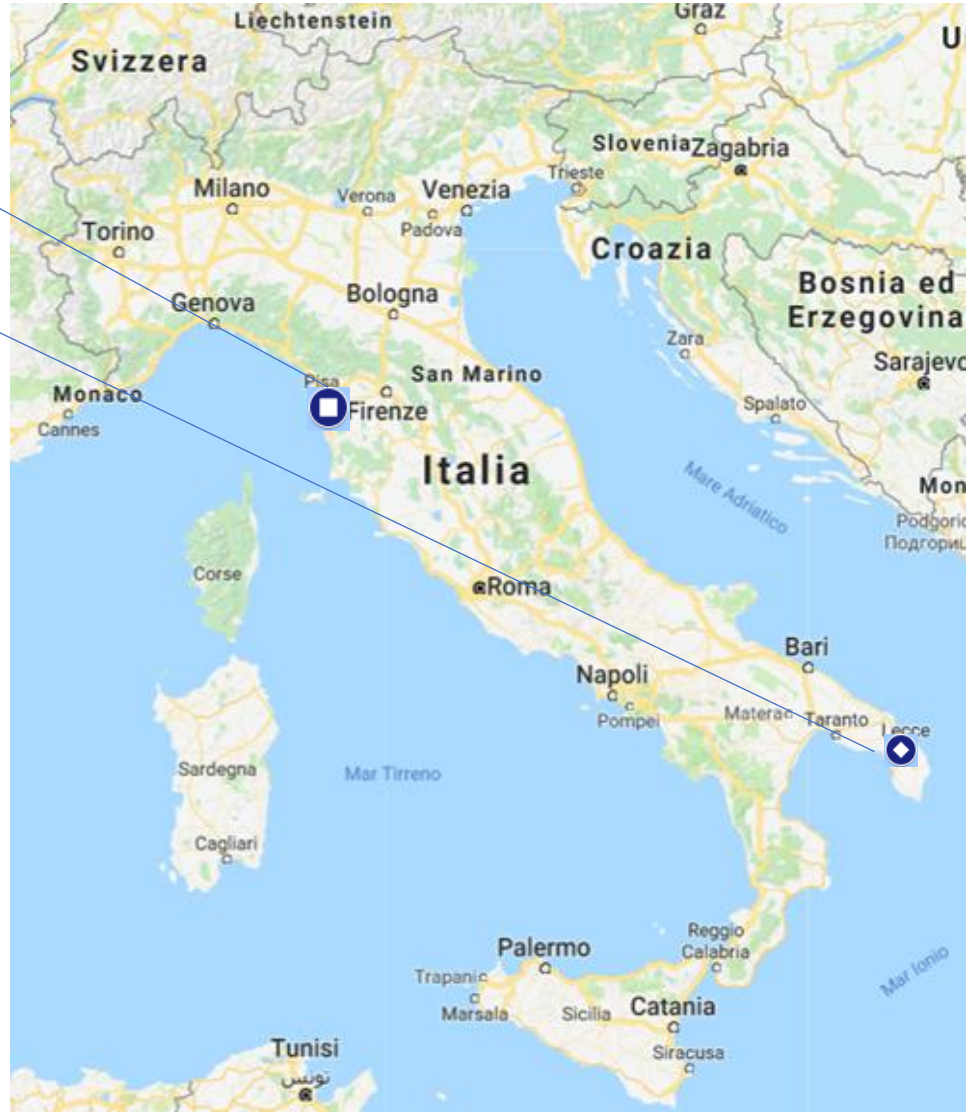


HeadQuarter

Piazza Nilde Iotti, 25
56025 - **Pontedera** (PI), Italy

Branch Office 1

Via dei Tufi, Palazzina BePilot
73100 – **Monteroni di Lecce**, Italy



GLOBAL CYBERSECURITY ALLIANCE

DITECFER
DISTRETTO PER LE TECNOLOGIE FERROVIARIE L'ALTA VELOCITÀ E LA SICUREZZA DELLE RETI

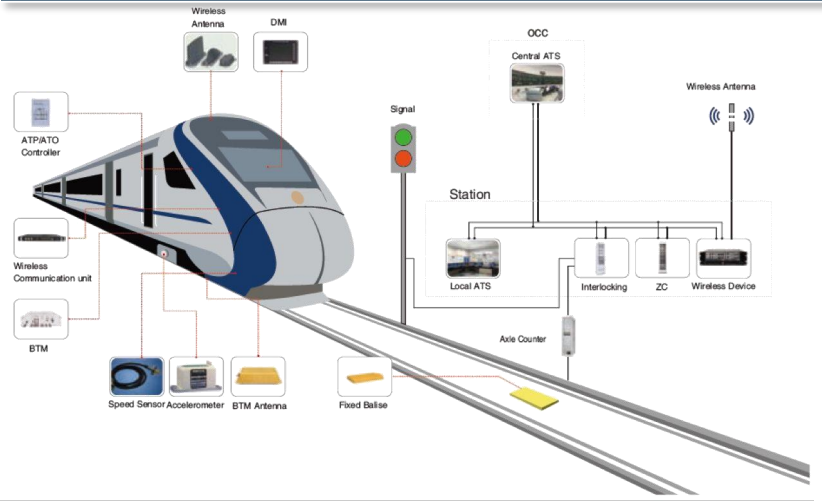
Arm Functional Safety Partner
Design Services

FuSa SIG
Xen Project

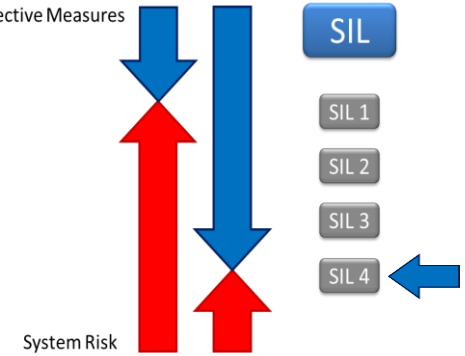
CUNA Commissione Tecnica di Unificazione nell'Autoveicolo
Ente federato all'UNI

Member of CISQ Federation
RINA
ISO 9001:2008
Certified Quality System

Railway/Metro Specific Resiltech Offering

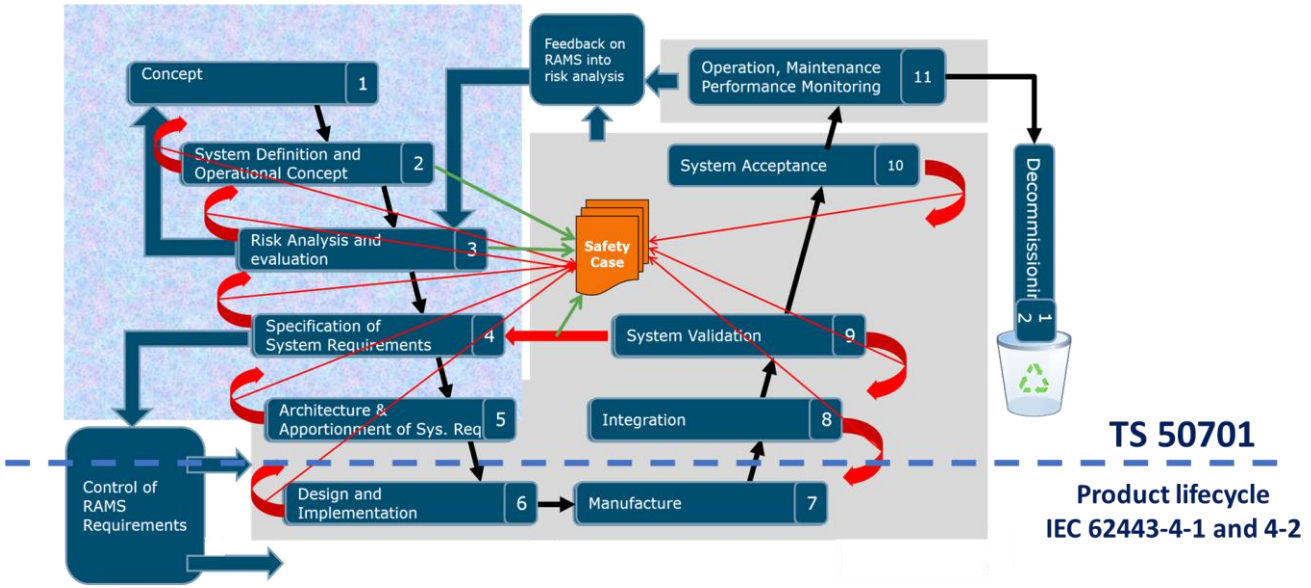


- **System Level Activities (EN 50126):**
  - Planning of RAMS activities
  - System model definition
  - Risk Analysis and Evaluation
  - Specification of Safety Requirements
  - System level Verification and Validation
  - Development of Safety Case documentation

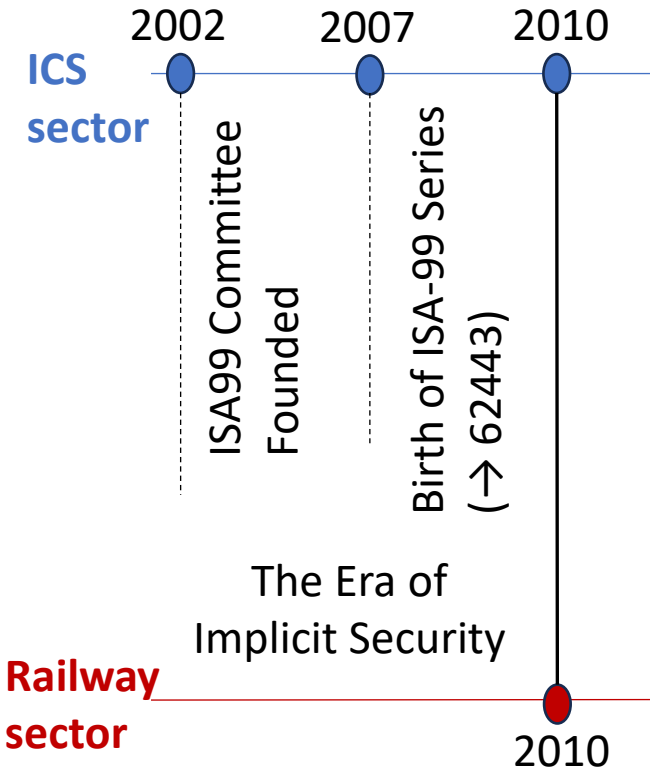


- **Software Specific RAMS Analyses (En 50128)**
  - Support to SW architecture design
  - SW-FMEA
  - FTA, RDB
  - Static and Dynamic Code Verification
  - Unit and Integration Testing
  - On-board Testing
- **Component Specific RAMS Analyses (En 50129)**
  - MTBHE analysis
  - (C)-FMEA analysis
  - Validation (In-Lab and On-Board testing)

- **Cybersecurity (CLC/TS 50701, IEC 62443)**
  - 50701 System level Cybersecurity Activities
  - 62443 Product Compliance



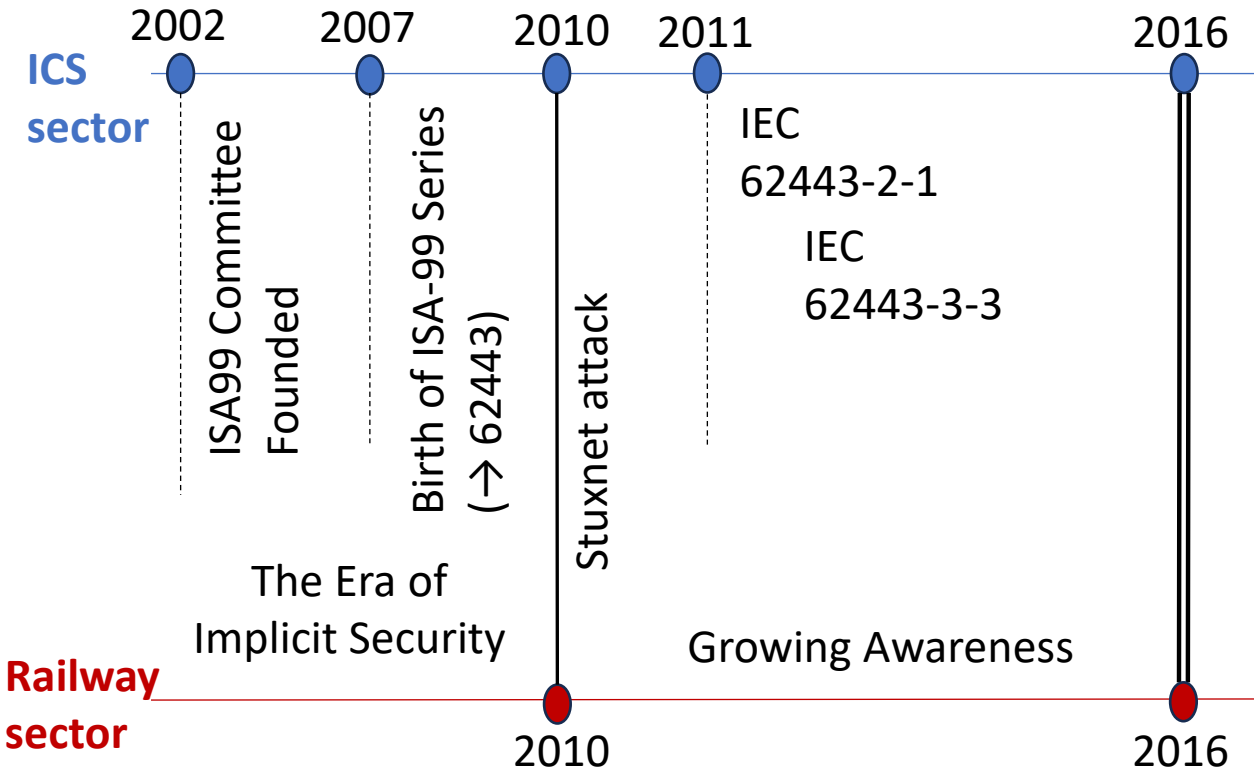
Cybersecurity Awerness evolution in ICS and Railway domain



- **2002 – ISA99 Committee Founded**
  - The **ISA99** committee (International Society of Automation) is established to address **cybersecurity for Industrial Control Systems (ICS)**.
  - First initiative to formalize protection for OT systems, independently from IT security.
- **2007 – Birth of ISA-99 Series (→ 62443)**
  - ISA publishes the first specifications under the ISA-99.x series.
  - These documents are later adopted by **IEC TC65** and renamed as **IEC 62443**, initiating a structured approach to ICS security.

- **2000–2010: The Era of Implicit Security for RAILWAY**
  - Railway systems — including **signaling**, **ETCS**, **SCADA**, and **interlocking** — were traditionally considered **inherently secure**.
  - Security relied on:
    - **Isolated networks** (air-gapped architectures)
    - **Proprietary protocols**
    - Strict **Safety Integrity Levels (SIL)** as part of RAMS processes
  - Cybersecurity was not addressed explicitly, but rather **assumed as a byproduct of safety**

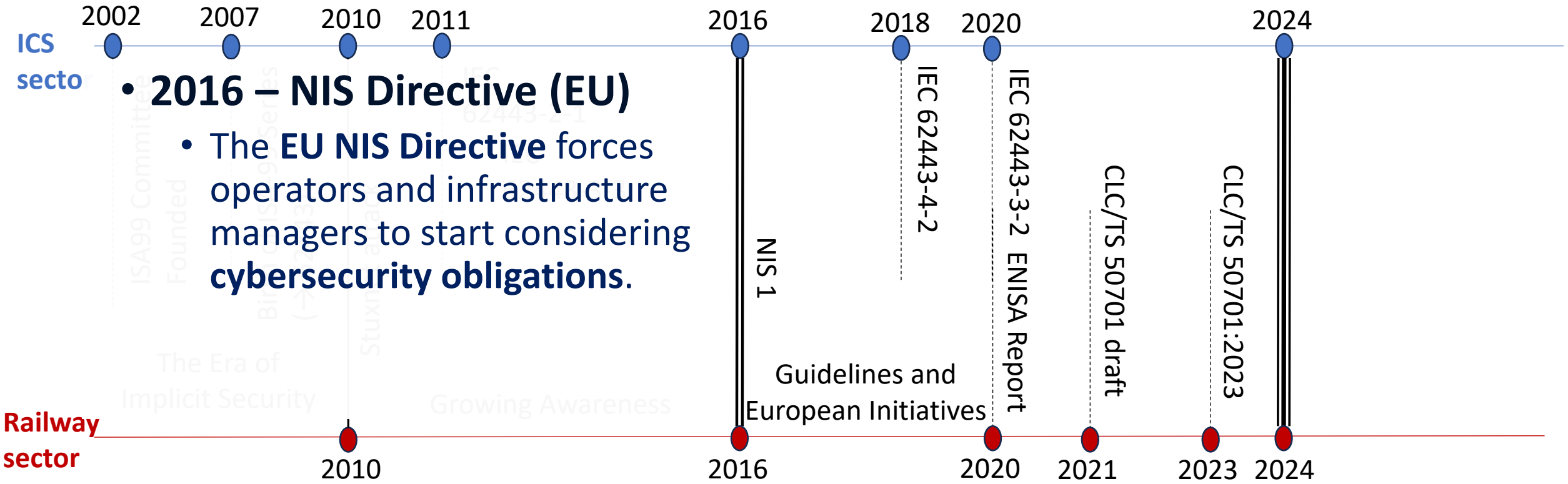
Cybersecurity Awerness evolution in ICS and Railway domain



- **2010 – Stuxnet and Growing Awareness**
  - **Stuxnet** demonstrates that air-gapped systems (such as industrial or railway control) can be compromised.
  - Raises awareness in the transportation sector, including **ERTMS/ETCS**, signaling, interlocking.

- **2011 – IEC 62443-2-1**
  - First official publication: defines **security policies and practices for asset owners**.
  - Sets the foundation for lifecycle-based cybersecurity.
- **2013 – IEC 62443-3-3**
  - Provides **system-level requirements** for securing industrial architectures in terms of **Security Levels (SL)** and **Foundational Requirements (FR)**.

Cybersecurity Awerness evolution in ICS and Railway domain

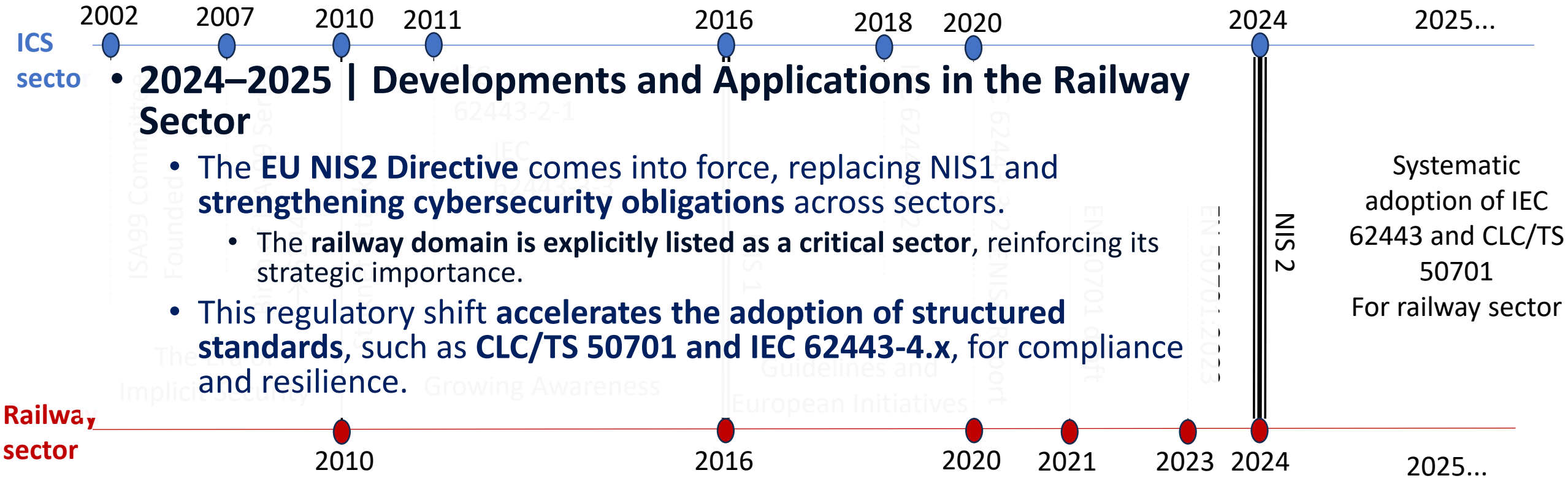


- **2016 – NIS Directive (EU)**
  - The **EU NIS Directive** forces operators and infrastructure managers to start considering **cybersecurity obligations**.

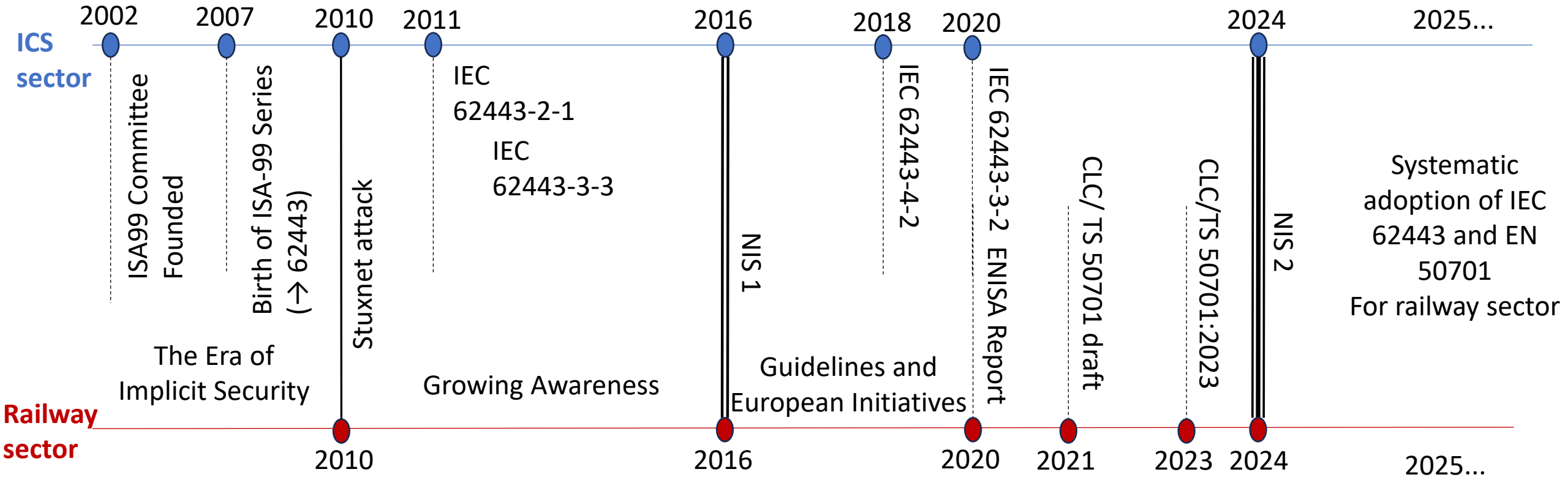
- **2017–2019 – Guidelines and European Initiatives**
  - Documents like **UIC 624**, **ENISA good practices**, and Horizon 2020 projects (e.g. **X2Rail**, **Shift2Rail**) begin to shape railway cybersecurity practices.
  - Emphasis on **risk-based approaches** and **security-by-design**.

- **2020 – ENISA Report and Birth of CLC/TS 50701**
  - ENISA highlights the lack of a **harmonized standard** for railway cybersecurity.
  - Work begins on **CLC/TS 50701**, led by **CENELEC TC 9X**, drawing heavily from **IEC 62443**.

Cybersecurity Awerness evolution in ICS and Railway domain



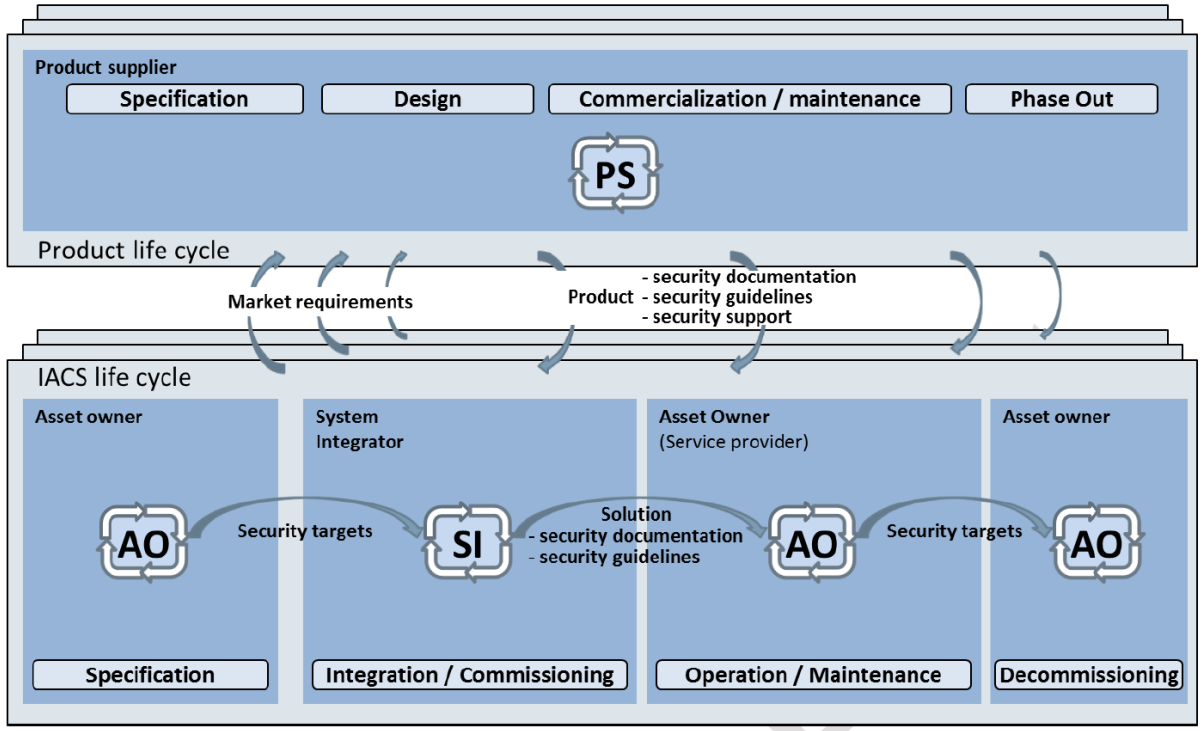
- **CLC/TS 50701** is increasingly adopted as a **de facto requirement** in European railway projects, **including new ETCS/ERTMS installations**, and is recommended by ERA for the management of cybersecurity risks.
  - Railway operators have begun integrating **IEC 62443 with SIL/Safety frameworks**, despite known challenges in reconciling **safety** with **security**.


ICS sector
2002
2007
2010
2011
2016
2018
2020
2024
2025...
ISA99 Committee Founded
Birth of ISA-99 Series (→ 62443)
Stuxnet attack
IEC 62443-2-1
IEC 62443-3-3
NIS 1
IEC 62443-4-2
IEC 62443-3-2 ENISA Report
CLC/ TS 50701 draft
CLC/TS 50701:2023
NIS 2
Systematic adoption of IEC 62443 and EN 50701 For railway sector
The Era of Implicit Security
Growing Awareness
Guidelines and European Initiatives
Railway sector
2010
2016
2020
2021
2023
2024
2025...

Roles and Responsibilities: IEC 62443 Framework

- The **IEC 62443 framework** defines clear roles and responsibilities in IACS cybersecurity, involving three key actors:
  - **AO - Asset Owners** – define operational needs and acceptable risk levels.
  - **SI - System Integrators** – perform risk assessment and determine the required SL-T for each zone and conduit.
  - **PS - Product Suppliers** – develop and deliver products with declared SL-C levels.

- The **interaction between roles** is essential:
  - The SL-T identified by the integrator becomes a **market requirement** for the supplier.
  - The supplier must provide components with **SL-C ≥ SL-T** to meet integration requirements.



The 62443 Security Levels

- IEC 62443 Security levels provide a qualitative approach to addressing security.
  - Meant to be used to
    - compare and manage the security of zones within an organization.
    - select IACS devices and countermeasures to be used within a zone
    - to identify and compare security of zones in different organizations across industry segments.
- The 62443 series define SLs in terms of five different levels.
  - Levels increases with complexity of threats to be mitigated
  - Technical countemeasures complexity increases with SLs
- Three types of SLs:
  - **SL-T**, determined through a detailed risk assessment, measure the level of protection needed for a particular zone, system or component.
  - **SL-C,** is the level of protection that a particular component or system is capable to provide if properly configured.
  - **SL-A,** is the level of security provided by the current configuration of the zone, system or component.

Different System/Components Requirements for each **Foundational Requirements**

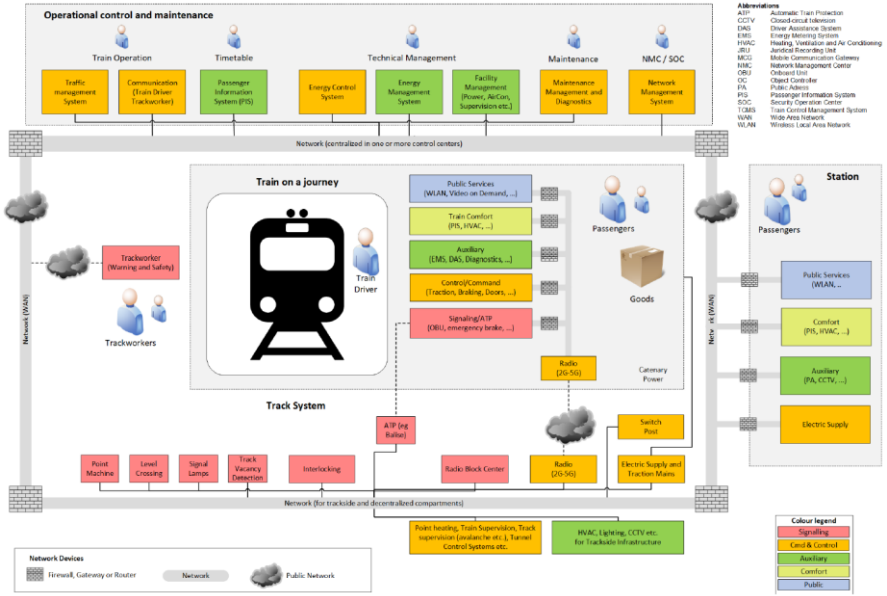
	Protection from unintentional or accidental actors	*Protection from intentional actors with limited capabilities*	*Protection from intentional actors with moderate technical capabilities*	*Protection from highly skilled and persistent actors*
Foundational Requirements (FR)	**SL 1**	**SL 2**	**SL 3**	**SL 4**
FR1 – Identification and Authentication Control	Use of hard-coded credentials	Unique user/device ID and granting password complexity	TLS certificate-based authentication	Mutual TLS authentication with HSM acceleration
FR2 – Use Control	Basic user-groups check and file/directory permissions check	Static RBAC	Dynamic RBAC with enforcement of dynamic SoD policies	Centralized role enforcement
FR3 – System Integrity	Signature checking when loading firmware	Verification of the filesystem at boot time	Runtime integrity monitoring	Secure Boot (implemented through Chain-of-Trust)
FR4 – Data Confidentiality	No protection (encryption, restriceted access, policy	AES-128 encryption	TLS v1.2 or VPN	TLS v1.3 with PFS session encryption
FR5 – Restricted Data Flow	VLAN separation	Setting and managing firewall rules	DPI (Deep Packet Inspection) firewall	Implementing separation gateway and zoning enforcement
FR6 – Timely Response to Events	Local alerting	Logging system events. Monitoring system with watchdog	Remote alerting	Support incident detection and autonomous response / SOC
FR7 – Resource Availability	Simple metwork filtering	Detecting DoS attacks using heuristics measurements	Rate limiting	Protocol hardening and hardware redundancy

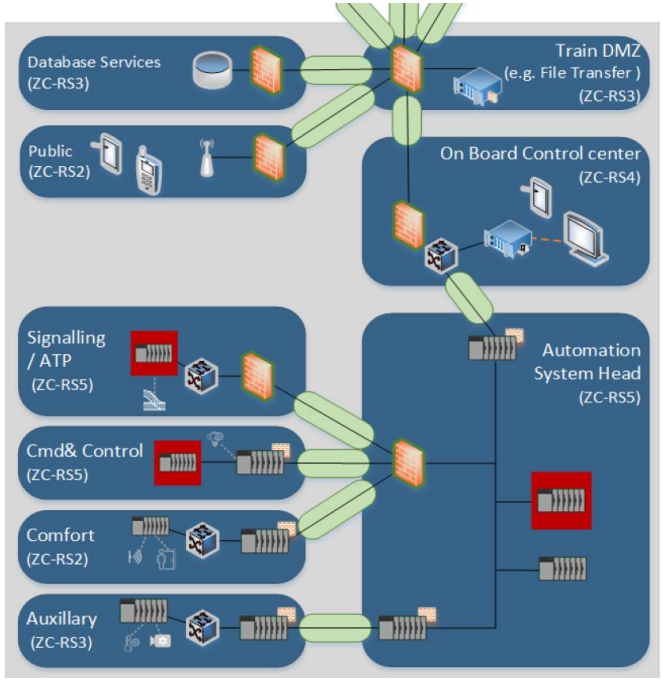
SL-T can be defined for each FRs -> Vector based approach:

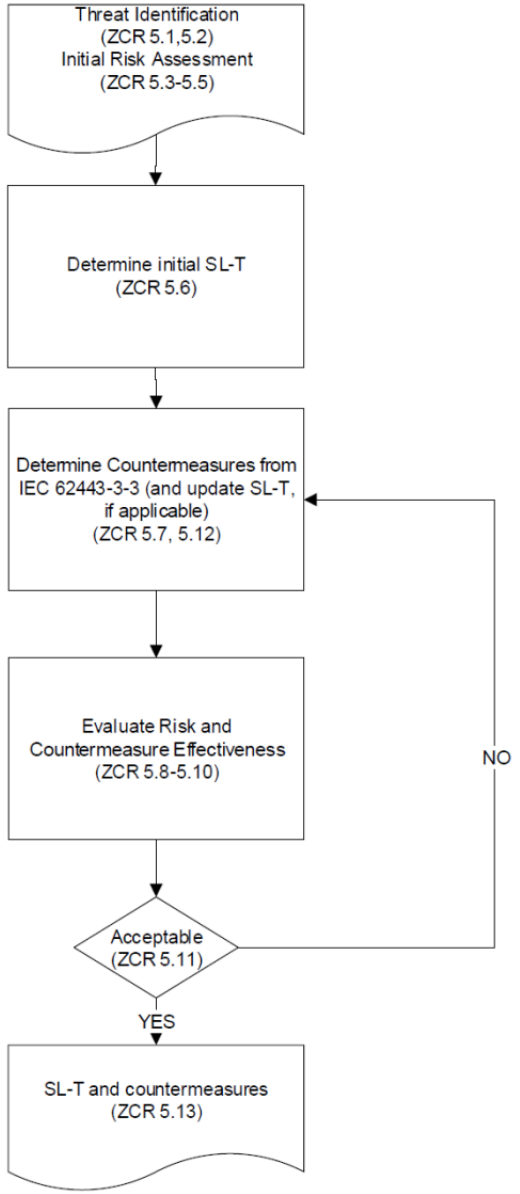
FLAT: SL-T=X VS Vector Based: SL-T =[IAC,UC,SI,DC,RDF,TRE,RA]

CLC/TS 50701

- The CLC/TS 50701 contextualize the IEC 62443 approach to the **railway domain**, preserving its **core principles** but applying them to railway-specific architectures and use cases.
- The standard includes a **high-level architectural overview of railway systems**, covering both onboard and trackside components
- its **appendix provides an example of how to define zones and conduits** in a railway environment, highlighting key segments such as the **onboard signalling control zone**







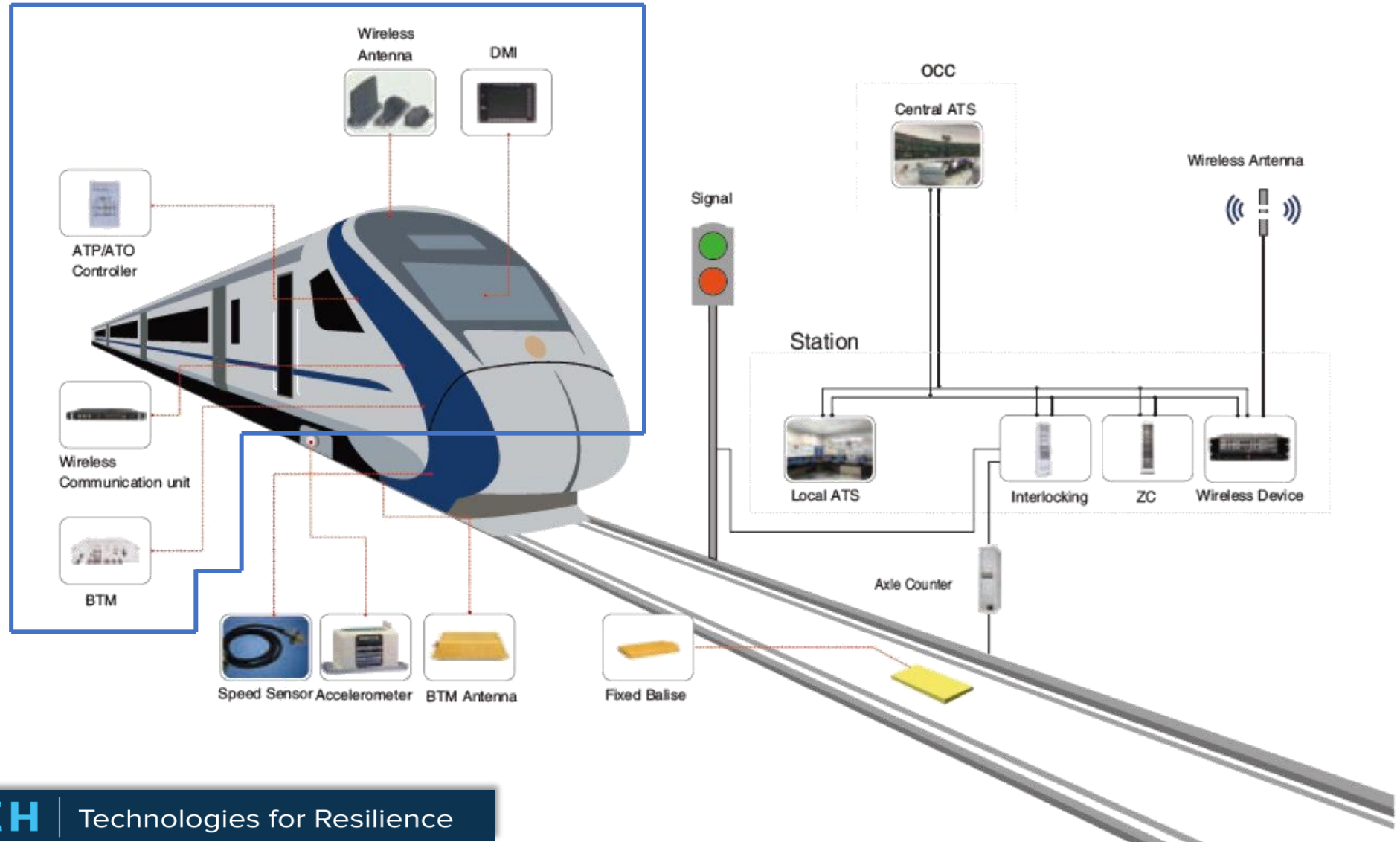
- A common industrial practice is to keep same granularity and to assign a flat SL-T to each zone... E.g. on board equipment -> SL-T 3

SL-T: Theory vs Practice

- Lack of clear methodology
  - According to **IEC 62443-3-2 and CLC/TS 50701**, SL-T is derived from a **risk assessment** process (e.g. likelihood × impact).
  - However, the standards lacks a clear methodology for SL-T determination
  - The result is that many actors go for a Flat and generic SL-T assignment.
- How to deal with well established specification
  - In the railway sector, cybersecurity must coexist with well-established safety processes and standards.
    - **EN 50126 / EN 50128 / EN 50129 (RAMS Standards)**
    - **UNISIG Subsets (e.g., SUBSET-026, SUBSET-036, SUBSET-091)**
    - **TSI CCS (Technical Specifications for Interoperability – Control Command and Signaling)**
- This leads to **real-world implementation gaps**:
  - **Unrealistic SL-T values** in case of technical limitations are ignored.
  - **Overdesign** of less-critical system components increasing complexity and cost.
  - **Budget-driven Security** when budget constraints override risk-based priorities.

A few examples from signalling onboard systems

SL-T 3 is usually assigned to the ATP-Signalling zone onboard components for signalling



Example#1: The DMI

- **DMI (Driver Machine Interface):** The DMI is the human-machine interface of the onboard ETCS/ERTMS system.
  - It displays critical driving information (e.g., target speed, operating mode) and receives input from the driver (e.g., confirmations, data entry, mode changes).
  - It is connected to the European Vital Computer (EVC) but does **not communicate externally** or make autonomous decisions.
- **Contextual Analysis**
  - It operates **entirely within the onboard domain**.
  - It has a **limited attack surface**.
  - limited exposure and local physical protections.
- **Examples Technical Requirements (IEC 62443-4-2) that shall be implemented according to SL-C 3**
  - Multi-factor authentication for interface access.
  - Cryptographic integrity validation of displayed data.
  - Protection against spoofing or manipulation of operator input.
  - TLS based communication with EVC.
- Assigning SL-T 3 to the DMI **solely because it is part of the onboard system** may lead to overdesign.
  - A justified SL-T should be based on:
    - Its **actual risk exposure**.
    - Its **supporting (not autonomous) role** in decision-making.
    - Actual **Impact** of threats.

Example#2: the OTM Transmission Module

- **OTM (Onboard Transmission Module):** The OTM is responsible for **receiving telegrams from Balises**.
  - The communication between Balise and OTM is **air-gapped**, unidirectional, and based on **passive electromagnetic field activation**.
  - Balises **do not initiate communication** or perform any active protocol negotiation or cryptographic exchange.
- **Contextual Analysis**
  - The **UNISIG SUBSET-036** specification strictly defines the physical and logical interface between Balise and onboard antenna.
    - **Minimal protocol design:** The communication is intentionally simple to ensure high reliability and compliance with safety-critical requirements.
    - **No support for authentication or encryption:** Due to strict interoperability and performance constraints, SUBSET-036 does not allow or define any cryptographic protections.
    - **Data is transmitted in clear text,** with trust placed in the physical security of the trackside system and the design of the safety mechanisms.
- Imposing SL-T 3 on the OTM based on generic threat assumptions may be **incompatible with the technical constraints** of the **onboard-trackside** interface.
- It may result in:
  - **Infeasible or non-compliant requirements** with existing UNISIG specifications.
  - **Unjustified implementation costs**, without meaningful security gain.
- Security for this interface must be designed **with full awareness of architectural limitations**.

Example#3: EURORADIO communication Module

- **The EURORADIO** module handles **wireless communication** between the onboard unit and the **Radio Block Center (RBC)**, operating over **GSM-R**.
  - The link carries **safety-relevant data**, such as Movement Authorities, position reports, and supervision parameters.
  - To meet **SL-T 3 expectations**, features like **authentication, integrity protection**, and ideally **encryption** are required.
- **Contextual Analysis**
  - **Key provisioning is rarely handled at the product level**.
  - It is often **delegated to system integrators** or operators, outside the component's direct scope.
  - Standards like **UNISIG SUBSET-037** define message integrity but **do not mandate automated key distribution**.
- **Consequences**
  - The communication stack may technically support cryptographic functions, **but without valid and actively managed keys, no real protection is achieved**.
  - There's a **risk of false compliance**: the component satisfies SL-C formally, but **fails to provide meaningful security** in practice.
- The effectiveness of protection depends entirely on the **system-level key management infrastructure**, which may be undefined or inconsistent.

Example 4# JRU (Juridical Recording Unit):

- The **JRU** records safety-critical and legally relevant data from the onboard unit (e.g. speed, braking, driver inputs, ETCS messages).
  - It serves a role similar to a **black box**, enabling post-incident analysis, audits, and legal accountability.
  - It is **write-only during operation**, with **no runtime external interfaces**, and data retrieval typically occurs **offline via physical access**.
- **Contextual Analysis**
  - The **attack surface is minimal**: no runtime network connectivity, no interactive services.
  - The **feasibility of attacks (AFR)** is extremely low — most threats would require physical access or hardware tampering.
  - High SLs imply **strong runtime security requirements** (e.g. access control, cryptographic protections) that may be disproportionate or redundant.
- **Consequences**
  - Applying SL-3 or above may demand:
    - Full implementation of 62443-4-2 runtime controls (authentication, session management, event logging).
    - **Cryptographic protections** that are not meaningful during operation (data are not transmitted or accessed online).
  - Risk of **overengineering** a closed system with no realistic attack vectors.
  - Security efforts may be directed at **runtime protections only** while **neglecting physical and supply chain threats**, which represent **the actual risk** for the JRU.

Lessons from the Case Studies

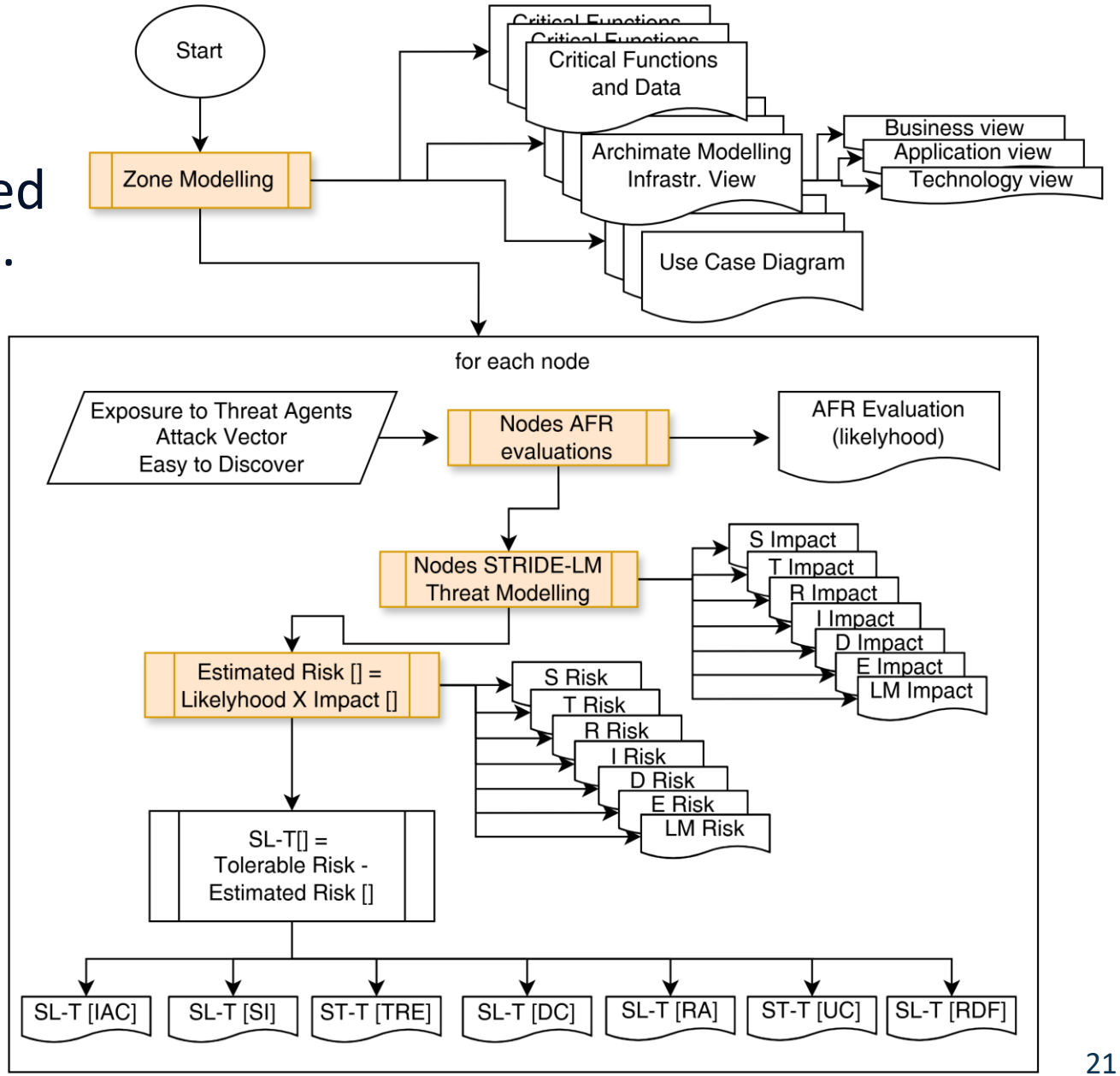
- **Too high-level zoning** leads to inconsistent SL-T assignments:
  - components with vastly different roles and exposure are treated identically, resulting in under- or overprotection.
- **Flat and non-vectored requirements**:
  - although IEC 62443 allows security properties to be treated independently (per Foundational Requirement), this flexibility is often **not applied in practice**.
- **Existing constraints from railway standards (e.g. UNISIG)** are frequently overlooked:
  - applying generic SL-T requirements without acknowledging **technical limitations or interoperability rules** leads to non-compliance or design conflicts.
- **Need for change:**
  - The current SL-T assignment practice often lacks **granularity, context-awareness**, and **risk alignment**.
  - This highlights the need for a more **structured, transparent, and functionally traceable methodology**.
- **Ongoing activities @RESILTECH in the application of EN 50701 point toward:**
  - A **more precise and systematic approach** to Security Level Target definition.
  - The introduction of **asset- and function-specific analysis**, in line with real-world exposure and impact.
  - **Security requirements (SL-T)**, tailored to each asset's role and constraints.

Overview of a Context-Aware Methodology for SL-T Assignment

- **Objective**
  Provide an overview of the structured methodology used to assign a tailored SL-T value for each node in a zone, based on real exposure and functional impact.

STRIDE-LM	IEC 62443-4-2 FRs
SPOOFING	FR1 [IAC] - Id. & access control
TAMPERING	FR3 [SI] - System Integrity
REPUDIATION	FR6 [TRE] - Timely resp. to event
INFORMATION DISCLOSURE	FR4 [DC] - Data Confidentiality
DENIAL OF SERVICE	FR7 [RA] - resource availability
ELEVATION OF PRIVILEDGE	FR2 [UC] - Use Control
LATERAL MOVEMENT	FR5 [RDF] - Restricted Data Flow

- **Key Message**
  A node's SL-T must reflect the real risk posed by specific threats to its functions — not just its presence in a zone.



Challenges Recap & Possible Methodological Solutions

- **Initial Challenges**
  - SL-T levels often defined **flat per zone**, without reflecting functional context.
  - Lack of **guidance in standards** on how to assign SL-T practically.
  - Risk of **overdesign** (e.g. SL-C 3 on DMI, JRU) due to one-size-fits-all approach.
  - **Incompatibility** with existing railway standards (e.g. UNISIG protocols).

- **Possible Methodological Solutions**
  - Introducing a **function-by-function analysis** using STRIDE-LM per node.
  - Producing an **SL-T vector per Foundational Requirement**, based on real threats and impacts.
  - Justifying **SL-C values below the zone SL-T** when appropriate.
  - Narrowing the gaps on **compatibility with legacy constraints and standards**.

- **Closing Message**
  SL-T is not a label — it's the result of a reasoned, documented, and repeatable process.