Proceedings of the Seventh International Conference on
Railway Technology: Research, Development and Maintenance
Edited by: J. Pombo
Civil-Comp Conferences, Volume 15, Paper 20.2
Civil-Comp Press, Edinburgh, United Kingdom, 2026
ISSN: 2753-3239, doi: 10.4203/ccc.15.20.2

Applying the New IEC 63452 OT Railway Cybersecurity Standard to Operators and System Integrators

H. Parkinson[1,2], D. Basher[2], G. Bamford[2], S. Parkinson[3] and J. Murray[2]

[1]University of Huddersfield, United Kingdom
[2]Digital Transit Limited, United Kingdom
[3]Department of Computer Science , University of Huddersfield United Kingdom

Abstract

IEC 63452 is a new international standard specifically designed to address operational technology (OT) cybersecurity in railway applications. To be published later in 2026, it adapts the widely used IEC 62443 series of industrial cybersecurity standards to the specific context and safety-critical requirements of the railway domain. This paper examines how IEC 63452 applies in practice from two complementary perspectives: that of the train operator (in this case also acting as railway duty holder and asset owner), and that of the system integrator responsible for delivering a new railway OT solution. Using a worked case study of an Automatic Train Protection (ATP) system for maintenance vehicles, the paper walks through the standard's lifecycle phases from stakeholder identification and system definition through to the detailed risk assessment, zone and conduit modelling, and determination of Target Security Level (SL-T) vectors. The paper identifies practical insights, challenges, and lessons learned from applying the standard, including the complexity of zone derivation, the use of the ERORAT threat assessment template, and the relationship between cybersecurity and functional safety under IEC 63452. The paper concludes with recommendations for organisations embarking on their first IEC 63452 assessment.

Keywords: railway cybersecurity; OT security; IEC 63452; IEC 62443; zone and conduit model; security level; system integrator; train operator; automatic train protection

1 Introduction

Modern railway systems are increasingly reliant on interconnected operational technology (OT) — spanning rolling stock, signalling, train control, and infrastructure management. While this connectivity brings operational benefits, it also introduces significant cybersecurity risks. High-profile incidents in other critical infrastructure sectors have demonstrated that OT environments can be targets for ransomware, state-sponsored intrusion, and supply chain compromise [1]. Railway systems are no exception: the European Union Agency for Cybersecurity (ENISA) has documented multiple significant cybersecurity incidents affecting rail operators in recent years [2].

Until recently, the railway sector lacked a purpose-built international cybersecurity standard. Operators and integrators instead adapted general OT security frameworks — principally the IEC 62443 series [3] — or the European railway-specific CENELEC technical specification TS 50701 [4]. IEC 63452, to be published in late 2026 [5], addresses this gap directly. Developed by IEC Technical Committee 9 (Electrical Equipment and Systems for Railways), it provides a lifecycle-based cybersecurity framework purpose-built for the railway domain, covering rolling stock, fixed installations, signalling, and operational management systems.

This paper makes two contributions. First, it examines the distinct obligations and perspectives of the two principal parties in a typical railway OT procurement: the train operator (acting as railway duty holder and asset owner) and the system integrator. Second, it presents a worked case study applying IEC 63452 Phases 0 through 5 to an ATP system for maintenance vehicles, demonstrating the practical application of the standard's asset modelling, risk assessment, zone and conduit derivation, and SL-T vector methodology.

The paper is structured as follows. Section 2 provides an overview of the standards landscape. Section 3 characterises the operator and system integrator perspectives under IEC 63452. Section 4 presents the ATP case study through Phase 5. Section 5 discusses key findings and challenges. Section 6 concludes with recommendations.

2 The Railway Cybersecurity Standards Landscape

The railway sector operates within a layered standards environment. Figure 1 illustrates the principal standards and their relationships.

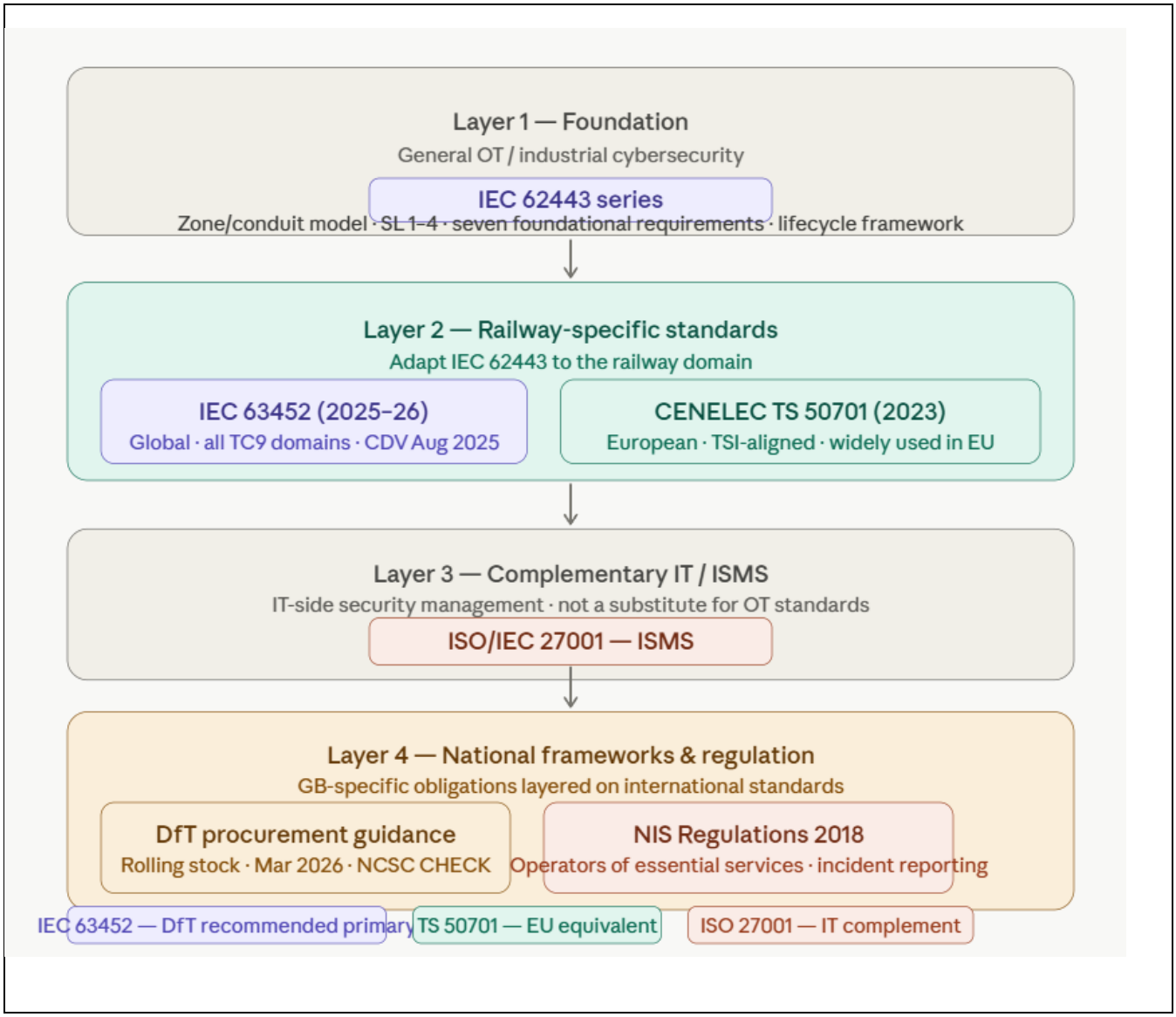

Figure 1: Railway cybersecurity standards hierarchy

IEC 62443 [3] provides the foundational industrial OT security framework and remains the primary reference for all railway-specific standards. It defines the zone and conduit model, security levels (SL 1–4), the concept of target versus achieved security levels, and the seven foundational requirements (FRs) that underpin all security level assessments.

CENELEC TS 50701 [4] is the European railway-specific technical specification, applicable to rail systems within the scope of European TSIs. It adapts IEC 62443 concepts to the CENELEC framework and is currently the most widely cited railway cybersecurity reference in European procurement.

IEC 63452 [5] builds upon both. It is developed by IEC TC 9 and is railway-domain-specific, covering rolling stock, trackside, and operational management systems globally. Unlike TS 50701, which is a technical specification, IEC 63452 will be a full international standard. It introduces railway-specific terminology, adapts lifecycle

phases to align with EN 50126 [6], and provides explicit guidance on the relationship between cybersecurity and functional safety.

In Great Britain, the Department for Transport (DfT) has issued guidance [7] specifically addressing the incorporation of IEC 63452 and IEC 62443 into rolling stock procurement specifications. This guidance, published in March 2026, makes IEC 63452 the recommended primary standard for GB passenger rolling stock procurements and introduces additional GB-specific obligations including mandatory NCSC CHECK penetration testing and a minimum 40-year asset lifecycle support expectation.

ISO/IEC 27001 [8] addresses IT-side information security management and is a complementary standard, required by the DfT guidance for suppliers of key IT-related services. It does not address OT environments directly and should not be used as a substitute for IEC 62443 or IEC 63452 in railway OT assessments.

3 Two Perspectives: Operator and System Integrator

3.1 The Train Operator as Asset Owner and Railway Duty Holder

Under IEC 63452, the train operator occupies two related but distinct roles. As the railway duty holder (RDH), it bears ultimate responsibility for the safety and security posture of the railway system. As the asset owner, it is responsible for establishing and maintaining an OT Cybersecurity Management System (CSMS) across all railway applications, independent of any individual project or procurement.

The operator's CSMS obligations under IEC 63452 Clause 5 include maintaining a railway OT cybersecurity policy (deliverable CP-01-01), a cybersecurity programme for each railway application (CP-01-02), and documented processes covering information sharing, competency management, asset inventory, supply chain management, and risk management. These obligations are ongoing and must be operational before any procurement activity commences.

In the procurement context, the operator acts as the contracting authority (CA). Key pre-tender obligations include performing an initial risk assessment of the operational context and sharing it with bidders, defining target security levels (or requiring bidders to propose them), establishing a Cyber Security Acceptance Gate regime aligned to the project lifecycle, and specifying assurance requirements. The DfT guidance [7] is explicit that these are CA obligations — they cannot be delegated to the supplier.

Post-acceptance, the operator is responsible for maintaining the Achieved Security Level (SL-A) throughout the asset's operational life. This includes continuous vulnerability management, coordinating patch deployment within the constraints of functional safety re-certification, operating or commissioning a Security Operations Centre (SOC) for monitoring, and managing significant incidents in accordance with the NIS Regulations 2018.

The key tension for the operator is balancing cybersecurity agility against the rigid safety certification constraints of railway OT. A security patch that would be deployed automatically in an IT environment may require a Change Control Board (CCB) process, safety re-assessment, and co-ordinated fleet-wide deployment before it can

be applied to a safety-critical OT subsystem. IEC 63452 acknowledges this explicitly, requiring operators to establish conflict resolution processes between cybersecurity updates and safety certification obligations.

3.2 The System Integrator

The system integrator (SI) is responsible for the design, development, integration, delivery, and commissioning of the railway OT solution. Under IEC 63452, the SI is the primary producer of the cybersecurity artefacts that demonstrate the solution meets the operator's security requirements. These include the Cybersecurity Management Plan (CSMP), the zone and conduit architecture, the risk assessment reports, the Cybersecurity Requirements Specification (CRS) response, the Software Bill of Materials (SBOM), and ultimately the Cybersecurity Case (CSC).

The SI's engagement with IEC 63452 begins at the bid stage, where it must propose security levels for the asset, demonstrate alignment with the operator's Cybersecurity Requirements Specification, and commit to a Cyber Security Acceptance Gate regime. The SI must also demonstrate that its own internal CSMS and supply chain management processes are adequate — in the DfT context, this typically means ISO/IEC 27001 certification or Cyber Essentials Plus for IT-related services and demonstrated supply chain cybersecurity obligations flowing down to sub-suppliers.

A defining characteristic of the SI's role is that cybersecurity activities must be integrated with — not separate from — the system engineering and functional safety lifecycle. IEC 63452 maps its cybersecurity activities to the EN 50126 [6] lifecycle phases (0–12), requiring the SI to coordinate cybersecurity risk assessments with RAMS assessments, ensure that cybersecurity controls do not introduce new safety hazards, and maintain the Cybersecurity Case alongside the Safety Case throughout the asset's life.

Table 1 summarises the principal obligations of each party across the key lifecycle phases.

Lifecycle Phase	Operator (Asset Owner / CA)	System Integrator
Phase 0–1: Concept	CSMS in place; initial risk assessment; share with bidders; define assurance regime	Identify stakeholders; establish team; agree methodology; respond to CRS
Phase 2–3: Definition	Confirm zone/conduit concept; approve threat environment description	Build asset model; map functions to assets; initial risk assessment; derive initial zone model
Phase 4–5: Design	Review and approve cybersecurity architecture; confirm SL-T; Gate 1 (Design Freeze)	Detailed risk assessment; ERORAT threat analysis; derive SL-T vectors per zone; define SecRACs
Phase 6–8: Implementation	Witness FAT; review SBOM; Gate 2–3	Secure-by-design architecture; apply controls; integration testing; pen test (Gate 4)
Phase 9–10: Acceptance	Accept Cybersecurity Case; formal acceptance; Gate 5 (APIS)	Deliver CSC; demonstrate SL-A ≥ SL-T; handover SBOM, documentation, training
Phase 11: Operation	Monitor SL-A; manage patches; operate SOC; incident management	Vulnerability advisories; patch support; update SBOM; participate in CCB
Phase 12: Disposal	Govern decommissioning; accept certificates of destruction	Secure data erasure; hardware disposal; final CSC closure

Table 1: Principal operator and system integrator obligations across the IEC 63452 lifecycle

4 Two Perspectives: Operator and System Integrator

4.1 System Description

The case study system is an ATP system designed to ensure that maintenance vehicles do not pass a particular track location at a speed that could lead to a collision. The system is a safety-critical onboard OT system interfacing with trackside ATP infrastructure via balise communication.

The system comprises eight primary assets: Logic Unit (A1-LU), Human Machine Interfaces front and rear (A2-HMI1, A2-HMI2), Antenna Communication Unit (A3-ACU), Antenna (A4-ANT), Braking Unit (A5-BU), Speed Sensors (A6-SS), Maintenance Unit (A7-MU), and the trackside Balise (A8). The asset architecture is illustrated in Figure 2.

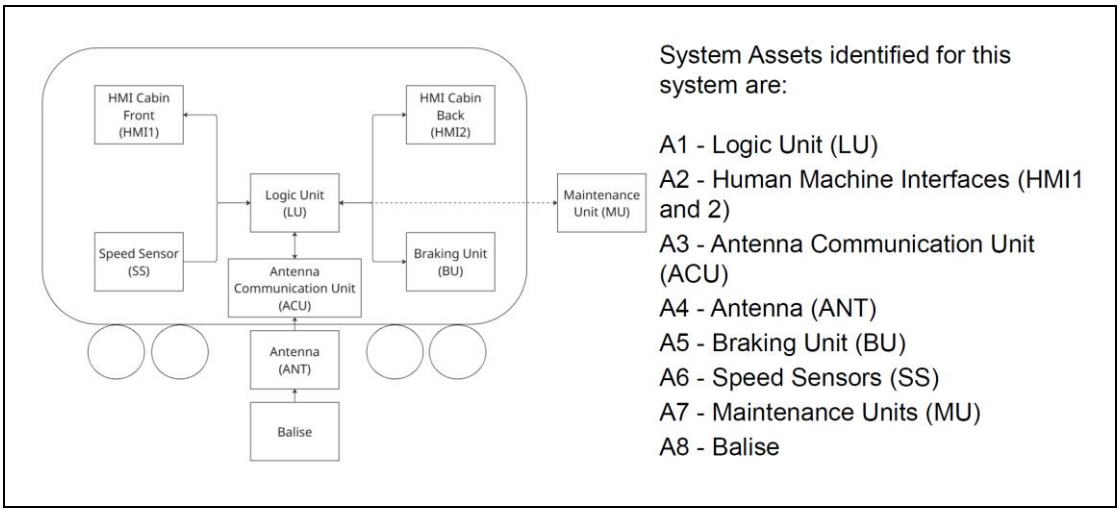

Figure 2: ATP system asset architecture

4.2 Phase 0–1: Stakeholder Identification and Methodology

The first phase of the IEC 63452 assessment establishes the stakeholder landscape and the cybersecurity assessment methodology. For the ATP case study, the stakeholder structure comprises three organisations: the Asset Owner (which in this case also acts as Railway Duty Holder and Maintenance Service Provider), the System Integrator, and the Product Supplier.

From the operator's perspective, Phase 0 requires the CSMS to be in place and for security policies, risk tolerance, and security requirements to be defined before the SI can begin its assessment. Where these are absent or undefined — a common practical challenge for operators new to IEC 63452 — the SI must establish a clear path forward with undefined security requirements rather than proceeding on assumptions.

The SI established an assessment team comprising: a cybersecurity lead responsible for the overall process and stakeholder interface; technical experts with system-specific knowledge of the ATP components; operational railway experts; risk managers to drive the structured risk process; and a documentation specialist. The team established the following assessment methodology: asset modelling; functional modelling; function-to-asset mapping; initial risk assessment; zone and conduit derivation; and detailed risk assessment to produce SL-T vectors.

4.3 Phase 2: System Definition — Asset and Functional Models

Phase 2 establishes the System Under Consideration (SUC), the asset model, and the essential functions that the system must provide. Essential functions are the critical capabilities the railway system must maintain to ensure safe and operational services — they are the foundation of the risk assessment because threats are assessed in terms of their impact on these functions.

For the ATP system, six essential functions were identified:

- F1: Processing HMI inputs, outputs and warnings
- F2: Reading Balise information from trackside

- F3: Monitoring the train speed continuously
- F4: Monitoring for dangerous approaches to the train stop
- F5: Applying the emergency brakes when required
- F6: Updating and maintaining the system

The function-to-asset mapping establishes which assets support which essential functions. This is critical because it determines the initial impact value of each asset: each asset inherits the highest impact rating from any function it supports. Table 2 shows the mapping for the ATP system.

Asset	F1	F2	F3	F4	F5	F6	Initial Risk Value
A1 – Logic Unit (LU)	✓	✓	✓	✓	✓	✓	A
A2.1 – HMI 1	✓						C
A2.2 – HMI 2	✓						C
A3 – ACU		✓					A
A4 – Antenna		✓					A
A5 – Braking Unit					✓		A
A6 – Speed Sensors			✓				A
A7 – Maintenance Unit						✓	C
A8 – Balise		✓				✓	A

Table 2: ATP function-to-asset mapping and initial risk values (A = Availability/Safety critical; C = Confidentiality relevant)

4.4 Phase 3–4: Zone and Conduit Derivation

The zone and conduit model is the cornerstone of IEC 63452's security architecture. Rather than performing a device-by-device risk assessment — impractical for complex railway systems — the standard groups assets with similar security characteristics into zones and then treats communication paths between zones as conduits subject to their own security controls.

IEC 63452 provides both mandatory criteria and guidance criteria for zone derivation. The SI applied these systematically:

Mandatory criteria applied:

- Safety-related assets grouped into dedicated zones — all ATP assets are safety-related, so this criterion did not further divide the initial grouping
- Temporarily connected devices in separate zones — applies to A7 (Maintenance Unit), which connects only during maintenance windows
- Wirelessly connected devices in separate zones — applies to A8 (Balise), which communicates via inductive coupling

Guidance criteria applied:

- Risk profile (integrity, availability, confidentiality) — separates HMI terminals (A2) into their own zone due to their lower safety criticality relative to the core control functions
- Operational function — separates the Logic Unit (A1) into its own zone given its criticality as the central safety decision-making component
- Physical and logical location — not applied as a further differentiator in this case

Applying these criteria systematically results in five zones for the ATP system:

- Z1 – Logic Unit (LU): the central safety-critical control zone
- Z2 – Balise: the trackside wireless interface zone
- Z3 – Antenna (ANT), Antenna Communication Unit (ACU), Braking Unit (BU), Speed Sensors (SS): the core operational sensor/actuator zone
- Z4 – HMI 1 and HMI 2: the driver interface zone
- Z5 – Maintenance Unit (MU): the temporarily-connected maintenance access zone

Four conduits were defined between these zones (Figure 3): C1 between Z4 (HMI) and Z1 (LU); C2 between Z1 (LU) and Z3 (operational sensors/actuators); C3 between Z3 and Z2 (Balise); and C4 between Z1 (LU) and Z5 (Maintenance Unit). The conduit between Z1 and Z5 (C4) is particularly significant as the maintenance interface is historically the most significant attack vector for railway OT systems.

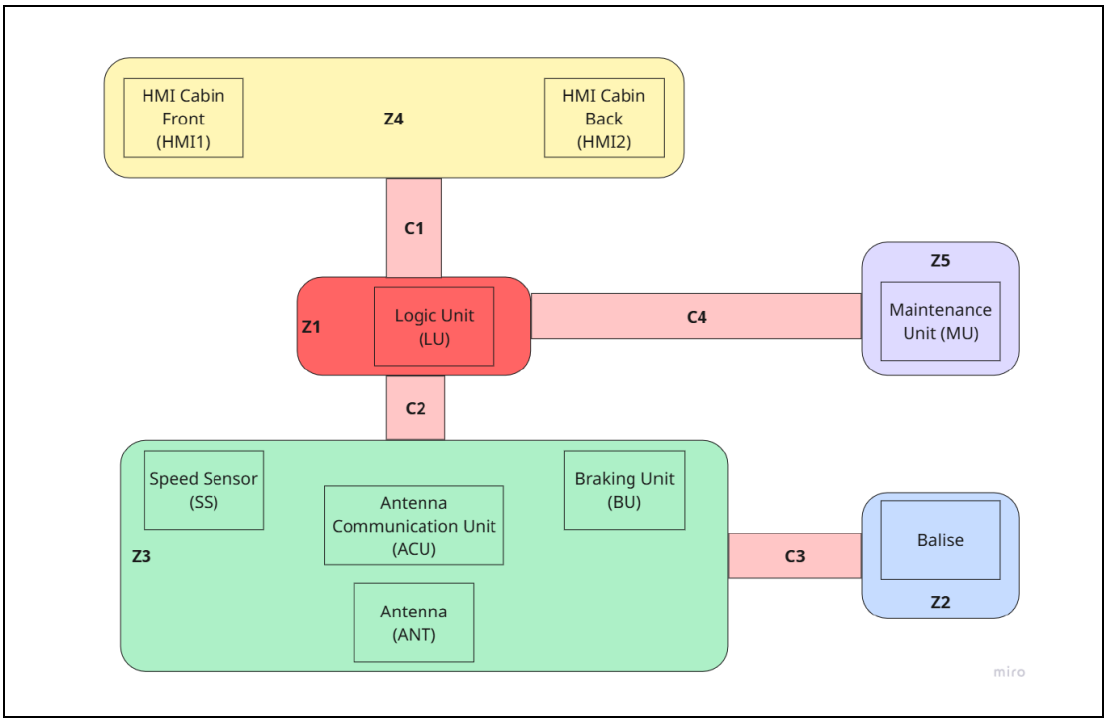

Figure 3: ATP five-zone and conduit model

4.5 Phase 5: Detailed Risk Assessment and SL-T Vector Determination

The detailed risk assessment for IEC 63452 is a structured process that combines threat identification, impact and likelihood assessment, and the derivation of the Target Security Level (SL-T) vector for each zone and conduit. The SL-T is not a single scalar value — it is a vector of seven values, one for each Foundational Requirement (FR) inherited from IEC 62443-3-3 [3]. These FRs are: Identification and Authentication Control (IAC); Use Control (UC); System Integrity (SI); Data Confidentiality (DC); Restricted Data Flow (RDF); Timely Response to Events (TRE); and Resource Availability (RA).

The case study used the ERORAT (ERTMS Risk and Operational Resilience Assessment Tool) threat assessment template [9], which draws threats from the BSI Grundschutz catalogue and maps each threat to the seven FRs. Each cell in the ERORAT matrix indicates which security property (Confidentiality — C, Integrity — I, Availability — A, or combinations) is at risk if that threat exploits a weakness in the corresponding FR category.

For each relevant threat, the assessor scores Exposure (how exposed is the zone to this threat, scale 1–3) and Vulnerability (how susceptible, scale 1–3). These combine to give a Likelihood score (1–5). Impact is scored separately for C, I, and A dimensions, and the maximum impact across dimensions gives the overall impact category (A–E). Likelihood and max impact combine in a risk matrix to give the Risk rating: Low, Medium, Significant, High, or Very High. These map directly to Security Levels: Medium → SL1; Significant → SL2; High → SL3; Very High → SL4.

Critically, the impact scores must be consistent with the FR mapping. If a threat only shows ‘C’ (Confidentiality) in the FR columns, only the Confidentiality impact carries a score. This ensures that the SL-T vector reflects the actual security properties at risk for each FR independently, rather than applying a worst-case scalar across all requirements.

The final SL-T vector for a zone is built by taking the maximum SL assigned to each FR across all relevant threats for that zone. For Zone Z1 (Logic Unit) in the ATP case study, applying threats from the Grundschutz catalogue relevant to the operational context produced the following SL-T vector (illustrative):

Foundational Requirement	Abbreviation	SL-T (Z1 – Logic Unit)
Identification and Authentication Control	IAC	3
Use Control	UC	3
System Integrity	SI	2
Data Confidentiality	DC	1
Restricted Data Flow	RDF	2
Timely Response to Events	TRE	3
Resource Availability	RA	3
Overall SL-T (scalar maximum)	—	3

Table 3: Illustrative SL-T vector for Z1 (Logic Unit) — SL-T = {3, 3, 2, 1, 2, 3, 3}

The vector — in this case {3, 3, 2, 1, 2, 3, 3} — reveals that strong authentication control (IAC=3), use control (UC=3), real-time event response (TRE=3), and availability (RA=3) are required, while data confidentiality (DC=1) carries a lower requirement, reflecting that the LU holds no commercially sensitive data but must reliably perform its safety functions against sophisticated attackers. This granularity is a key advantage of the vector approach over a single scalar: it allows proportionate, function-specific security controls rather than blanket over-engineering.

5 Key Findings and Challenges

5.1 Practical Benefits of the Standard

The IEC 63452 process provides a structured, evidenced, and lifecycle-integrated approach to railway OT cybersecurity that is absent from generic OT security frameworks. Several specific benefits emerged from the case study:

- The function-to-asset mapping (Phase 2) is an effective mechanism for anchoring cybersecurity risk to operational impact. By identifying what the system must do before assessing threats, the approach avoids over-weighting low-risk assets and ensures that safety-critical functions drive zone criticality determinations.

- The ERORAT template significantly reduces the burden of threat identification. Rather than requiring assessors to construct a threat catalogue from scratch, it provides a structured starting point from the BSI Grundschutz library that can be systematically filtered for relevance to the system under assessment.
- The SL-T vector methodology provides more proportionate and defensible security requirements than a scalar SL. Requiring SL=3 for data confidentiality in a zone with no commercially sensitive data would be disproportionate; the vector approach allows this to be set at SL=1 while maintaining SL=3 for safety-critical FRs.
- The integration of cybersecurity with the EN 50126 lifecycle is conceptually sound and provides a framework for coordinating with RAMS teams — something that previously lacked formal structure in many rail projects.

5.2 Challenges and Ambiguities

Several challenges and areas of ambiguity were identified during the case study that warrant attention from organisations approaching their first IEC 63452 assessment:

- Zone derivation complexity. The standard provides both mandatory and guidance criteria for zone derivation but leaves significant discretion to the assessor. This can result in widely varying zone models between assessors for the same system. Clearer decision rules or a more structured decision tree would reduce this variability.
- Conduit security level derivation. The rationale for performing a separate risk assessment on conduits — rather than simply inheriting the higher of the two adjacent zones' SL-T values — is not clearly articulated in the standard. Different interpretations between TS 50701 and IEC 62443 create further inconsistency.
- Security device boundary placement. The standard requires security devices to be located at zone boundaries, but the exact boundary between a zone and a conduit is not always unambiguous in practice, particularly for systems where the security device (e.g. a firewall) simultaneously functions as part of both the conduit and the protected zone.
- Initial risk assessment acceptance criteria. While the standard requires an initial risk assessment, it provides no explicit guidance on how the initial impact value should be accepted or whether it must be formally carried forward into the detailed assessment. In practice, this step can become a formality rather than a meaningful filter.
- Complexity and assessor resource. The full application of IEC 63452 through Phases 0–5 is time-consuming and requires multi-disciplinary expertise spanning cybersecurity, systems engineering, RAMS, and railway operations. Organisations should not underestimate the resource requirement, particularly for their first assessment.
- Functional model guidance. The standard mandates that threats are assessed in terms of impact on essential functions but provides limited cross-reference

to established systems modelling methodologies (e.g. functional hazard analysis) that have addressed this problem in depth. Greater alignment with existing systems engineering practice would be beneficial.

5.3 The Operator–Integrator Interface

A recurring practical challenge in the case study was the interface between operator and SI at the point where the CSMS must be established before the SI can begin its assessment. For operators new to IEC 63452, the CSMS may not yet exist at the start of a procurement. This creates a chicken-and-egg problem: the SI needs the operator's security requirements, risk tolerance, and threat environment description to perform its assessment, but the operator needs the SI's assessment to understand what security requirements to set.

The practical resolution is a phased approach in which the operator establishes a high-level initial risk assessment and threat environment description sufficient to initiate the SI's work, with the detailed assessment iterating between both parties. The DfT guidance [7] addresses this by requiring the CA to share an initial risk assessment with bidders as part of the ITT. The standard itself is less prescriptive on this sequencing, which is a gap.

6 Conclusions and Recommendations

IEC 63452 represents a significant and welcome step forward for railway OT cybersecurity. For the first time, the railway sector has a purpose-built international standard that integrates cybersecurity into the full EN 50126 lifecycle, provides railway-specific zone and conduit guidance, and establishes a structured risk methodology that yields proportionate, function-specific security requirements through the SL-T vector approach.

The case study demonstrates that the standard is applicable to real railway OT systems — including relatively constrained safety-critical systems such as the ATP system for maintenance vehicles — and that the assessment process is feasible with an appropriately composed multi-disciplinary team. The ERORAT template is a valuable practical aid that significantly reduces the burden of threat identification.

For organisations beginning their first IEC 63452 assessment, the following recommendations are offered:

1. Operators: Establish the CSMS, OT cybersecurity policy, and initial risk assessment before initiating any procurement. These are prerequisites, not deliverables of the procurement.
2. Operators: Use the initial risk assessment to define the threat environment description shared with bidders. Without this, bidders cannot make meaningful SL-T proposals and will be forced to make conservative assumptions that increase cost.
3. System integrators: Invest time in Phase 2 function-to-asset mapping. This is the analytical foundation for all subsequent risk assessment and zone derivation. Errors here propagate through the entire assessment.

4. Both parties: Use the ERORAT template or an equivalent structured threat catalogue as the starting point for the detailed risk assessment. Attempting to construct a threat catalogue from scratch is resource-intensive and risks significant gaps.
5. Both parties: Treat the SL-T vector as a design tool, not just a compliance metric. The vector's granularity allows security controls to be targeted precisely at the FRs where they are needed, avoiding disproportionate implementation cost.
6. Both parties: Plan for the cyber-safety interface from the outset. Cybersecurity controls must not compromise safety-critical functions, and security patches to safety-certified software require CCB process and safety re-assessment. This is not a bolt-on concern — it must be embedded in the project governance structure from Phase 0.

IEC 63452 will be the primary railway OT cybersecurity standard for decades to come. Organisations that invest in understanding and implementing it now — from both the operator and integrator perspectives — will be better positioned to manage the increasing cyber threat to railway systems and to meet the regulatory expectations of frameworks such as the NIS Regulations and the forthcoming Cyber Security Resilience Act.

References

[1] ENISA, "ENISA Threat Landscape for the Transport Sector," European Union Agency for Cybersecurity, Athens, 2023. Available: https://www.enisa.europa.eu

[2] ENISA, "Railway Cybersecurity — Security in the Railway Transport Sector," European Union Agency for Cybersecurity, Athens, 2020.

[3] IEC, "IEC 62443 Series — Security for Industrial Automation and Control Systems," International Electrotechnical Commission, Geneva, 2013–2023.

[4] CENELEC, "PD CLC/TS 50701:2023 — Railway Applications — Cybersecurity," BSI/CENELEC, Brussels, 2023.

[5] IEC, "IEC CDV 63452 ED1 — Railway Applications — Cybersecurity (Committee Draft for Vote)," International Electrotechnical Commission, Geneva, August 2025.

[6] CENELEC, "BS EN 50126-1:2017 — Railway Applications — The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)," BSI, London, 2017.

[7] Department for Transport, "Guidance on Rail Rolling Stock Procurement Specifications — Cyber-Security, Version 1.0," Land Transport National Security, DfT, London, March 2026.

[8] ISO/IEC, “ISO/IEC 27001:2022 — Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements,” ISO, Geneva, 2022.

[9] ERTMS Security Core Group, “ERORAT — ERTMS Risk and Operational Resilience Assessment Tool,” ERTMS Security Core Group, Brussels. Available: https://ertms.be/activities/ertms-security-core-group