

ERTMS[®] Sound Competition: Ensuring Fairness, Security, and European Interests. The UNIFE View

June 2026

UNIFE – The European Rail Supply Industry Association

 www.unife.org

 www.ertms.net

 UNIFE

 ERTMS[®]

ERTMS® (European Rail Traffic Management System) is an outstanding, freely available European standard for a railway signalling and management system that truly unlocks and drives vibrant competition across the rail sector. ERTMS® encompasses:

- **ETCS** - European Train Control System;
- **ATO** – Automated Train Operation and
- **RMR** – Railway Mobile Radio (2G (GSM-R) and 5G (FRMCS – Future Rail Mobile Communication System)).

By fostering interoperability and innovation, ERTMS® creates opportunities for all players to thrive in a dynamic market.

UNIFE is committed to sound and fair competition. We embrace new competitors as long as they play by the same rules on a genuine level playing field. This means full adherence to EU competition policy, which safeguards the Single Market by preventing distortions from anticompetitive practices, unlawful state aid, and unfair foreign subsidies.

We are confident that, with these strong safeguards in place, Europe's rail industry can continue to lead globally through excellence, innovation, and genuine open competition.

Safety and security aspects

As part of ERTMS®, ETCS truly stands at the heart of modern railway operations. It is the indispensable core system and a guardian of safety.

ETCS products represent highly complex systems, often comprising millions of lines of software code. Through advanced methods, UNIFE member companies demonstrate strong safety properties, including the absence of certain runtime errors, functional correctness with respect to specifications, and freedom from entire classes of defects. These achievements reflect the extraordinary efforts invested by the European rail supply industry in railway safety design and engineering.

However, a fundamental theoretical barrier remains: no general algorithm or proof procedure exists that can definitively determine, for any arbitrary software-based system, whether it harbours malicious elements.

CASE STUDY

SolarWinds and Heartbleed

The SolarWinds (a provider of IT management software) supply chain attack (2020) saw sophisticated malicious code inserted into trusted software updates, evading detection and compromising numerous high-profile targets worldwide. Nearly 18,000 customers downloaded and installed the compromised software updates that contained the hidden malicious code. The attackers gained initial access to a vast number of networks. From there, they exploited the backdoor to exfiltrate sensitive customer data and conduct prolonged espionage operations, often targeting high-value organisations to spy on additional entities in a cascading chain of breaches.

Similarly, the Heartbleed bug (2014), a severe vulnerability in a widely used software library, allowed attackers to extract sensitive data from server memory, remaining hidden despite extensive prior scrutiny of the codebase.

In both cases, even the most thorough auditing and review processes could not pre-emptively prove the complete absence of such critical flaws or intentional malice.

In practical terms, it is impossible to develop a tool, verifier, or analyser capable of reliably declaring a program or a sophisticated product like ETCS free of hidden malicious functions with absolute certainty. High-profile incidents like SolarWinds and Heartbleed underscore this reality. These examples illustrate the challenges we face and why trust, sustained vigilance and continuous improvement remain essential in safeguarding railway systems like ETCS.

In the worst-case scenario involving deliberate malicious actions, an improperly implemented on-board system could theoretically generate an untimely movement authority, override braking curves, or disregard temporary speed restrictions. Compromised odometry sensors through intentional biases or hidden backdoors might underreport distance or speed, potentially leading to inaccurate positioning and, in extreme cases, entry into occupied sections with risks of collisions.

Similarly, trackside systems could disrupt traffic by interfering with movement authorities (MA), failing to issue MA to connected trains, or – in the worst case - issuing overlapping MA to converging trains. Weak encryption or key management could open the door to man-in-the-middle attacks and message interception. Maliciously influenced communications might trigger unnecessary braking or simulate system failures, leading to avoidable stops, delays, and temporary loss of operational confidence.

Moreover, as ERTMS® evolves to meet new demands, embracing greater modularity for easier upgrades and maintenance, along with emerging possibilities for secure over-the-air software updates, the number of interfaces increases. This introduces additional considerations for cybersecurity and safety, including potential external connectivity beyond the traditional on-board control environment.

These scenarios underscore precisely why the European railway sector places such significant emphasis on formal verification, independent safety assessments, and adherence to rigorous standards. They also highlight the critical importance of collaborating with trusted and reputable partners. Moreover, even a valid certificate cannot, by itself, guarantee that a product or system is entirely free from malicious elements or vulnerabilities.



Trust and accountability

Ultimately, beyond all the technical safeguards, demonstrations of safety, reliability, and security, two elements stand out as truly foundational: trust and accountability.

By maintaining transparent truly European collaboration among manufacturers, operators, authorities, and lawmakers, we build and sustain the confidence that keeps passengers and goods safe, services dependable, and the entire railway ecosystem moving forward confidently into an even more connected future. The commitment across the sector to these principles is genuinely inspiring and positions ERTMS® as a model for safe, secure, high-performance rail signalling worldwide.

Bearing the above in mind, can we be assured that equivalent standards are applied to products and systems supplied from outside Europe, in particular from State-owned or -controlled entities?

The integrity of rail signalling, control, and operational technologies is non-negotiable when it comes to ensuring the safety of passengers, the protection of goods, and the reliability of train operations across the continent. UNIFE urged decisive action to prevent interference from high-risk third-country actors, emphasising risks tied to foreign dependencies, potential backdoors, and strategic vulnerabilities in embedded digital systems for signalling, control, and communications.

Supply chain security in rail goes beyond mere technical compliance. It encompasses geopolitical realities and the possibility of foreign influence, data access or malicious functions that could compromise safety and security. As stated earlier, proving the absence of such hidden risks in complex, opaque systems from suppliers not fully aligned with European standards with absolute clarity is indeed impossible in practice.

Moreover, in the absence of robust, comprehensive multilateral treaties with certain countries, pursuing liability for damages, injuries, or disruptions through European courts faces substantial hurdles abroad. Jurisdictional issues or procedural irregularities can significantly reduce the prospects of successful enforcement, leaving European stakeholders with limited practical remedies.

In this context, prioritising European rail suppliers as trusted partners represents a strategic imperative. Companies rooted in the European Union operate under stringent, transparent regulatory frameworks, share core European values on safety and security, and are fully accountable within the single market's legal ecosystem. This fosters genuine trust, seamless collaboration, and far greater assurance that systems will prioritise passenger safety, operational resilience, and the protection of Europe's transport sovereignty, especially as rail plays an increasingly key role in both civilian supply chains and military mobility.

Preserving Competence within Europe

While global competition can drive innovation and efficiency, Europe's ability to maintain full control and confidence over its critical rail infrastructure must remain a paramount priority. By championing homegrown expertise and rigorously vetting non-EU dependencies, we can uphold the highest standards of safety, security, and reliability for generations to come.

The European supply industry stands as a true global leader in the rail sector. To maintain this excellence, we must focus our energy on further positioning Europe at the forefront of this technology. Our priority should be creating seamless, positive experiences throughout the rollout process, rather than focusing on restrictions regarding third-country procurement.

In conclusion, investing in European railway expertise is not a move towards protectionism - it is an essential strategy for securing our sovereignty, safety, and long-term global competitiveness. It is vital that policymakers and operators prioritise transparent tenders that embrace lifecycle costs, security, and interoperability, actively choosing solutions that strengthen Europe's industrial and technological foundations. By committing to this strategy, we will ensure our sector is prepared to take the lead toward digitalisation, decarbonisation, and seamless, cross-border operations.





UNIFE-The European Rail Supply Industry Association

Avenue Louise 221

B-1050 Ixelles, Belgium

+32 2 626 12 60

general@unife.org

UNIFE – The European Rail Supply Industry Association

 www.unife.org

 www.ertms.net

 UNIFE

 ERTMS®