

PRESS RELEASE

FOR IMMEDIATE RELEASE

Cyber security becomes a shared responsibility across the railway sector

Frauscher achieves IEC62443-4-1 certification for its secure development process

St. Marienkirchen bei Schärding, Austria, 22 July 2026: As railway systems become more connected, cyber security is evolving into a shared responsibility for manufacturers, system integrators and operators alike. New technologies bring efficiency and new capabilities, but they also introduce risks that need to be addressed at every stage of the supply chain. The EU Cyber Resilience Act (CRA) provides a framework for this responsibility. Frauscher Sensor Technology has been engaged in cyber security after it began extending its portfolio with software- and network-based solutions and has now reached a further milestone: certification to IEC62443-4-1:2018 for its Secure Development Lifecycle (SDL), issued by TÜV Süd on 7 May 2026.

New technologies, new responsibilities

Distributed system architectures, open network communication and real-time data exchange between operational technology (OT) and IT environments are changing how railway networks are built and operated. The same characteristics that make these systems more efficient also widen the range of points that need to be protected. Manufacturers need to build protection into products from the earliest design stages; system integrators need to carry that protection through into the finished installation; operators need organisational measures, such as access control and patch management, to keep systems secure over their lifetime. Cyber security is consequently no longer a topic for a single party in the supply chain; it concerns manufacturers, integrators and operators together.

A regulatory framework for shared responsibility

The EU Cyber Resilience Act reflects this shift. Having entered into force in December 2024, it introduces mandatory cyber security requirements for products with digital elements placed on the EU market. Reporting obligations for actively exploited vulnerabilities apply from 11 September 2026, with the remaining core obligations, including essential security requirements for new products, technical documentation and CE marking, applying from 11 December 2027. Railway-specific standards complement this general framework: IEC62443 and its railway-focused derivation TS 50701 translate these requirements into concrete measures for a safety-critical environment, while ensuring that changes made for security reasons, such as applying a patch, do not trigger a full safety re-approval process.

Frauscher's engagement with cyber security

Frauscher's own engagement with cyber security dates back to when the company began extending its portfolio beyond field elements into software- and network-based solutions, including Frauscher Insights and Frauscher Connect. While secure network communication for example has always been a major topic, the focus on cyber security grew in the years after, just as it did in the whole railway industry and beyond. Today, Frauscher has built up comprehensive in-house expertise and established connections both within the railway industry and across the wider cyber security field.

"Digital signalling with IP-based control of field elements is a key driver for increasing capacity at a lower total cost of ownership, and for higher availability through predictive maintenance. We have been developing our portfolio in this direction for years, and cyber security has to be a reliable, built-in part of these new architectures from the outset," says Florian Einböck, Head of Portfolio Strategy at Frauscher Sensor Technology.

Certification confirms the secure development process

IEC62443-4-1 defines requirements for a secure development lifecycle for products used in industrial automation and control systems. The certification, awarded by TÜV Süd on 7 May 2026, confirms that Frauscher's development process addresses three core principles at every stage:

- **Security by design**, with relevant security factors considered and documented from the outset
- **Security by default**, meaning products are delivered with secure configurations and settings
- **Security in implementation**, covering the testing and documentation needed to operate a system securely

A dedicated Product Security & Network Team is responsible for cyber security measures and activities across the full product lifecycle, including vulnerability management and penetration testing. Vulnerabilities identified in released products are handled by Frauscher's Product Security Incident Response Team (PSIRT), which publishes corresponding security advisories on the Frauscher PSIRT website; external researchers can also report findings directly to the PSIRT.

Shaping standards, not just following them

As an active part of the cyber security community within railways, Frauscher experts participate in working groups, for example at VDB and CENELEC. This exchange feeds directly back into product development. New solutions are developed to be cyber secure by design from the outset. Existing products such as the Frauscher Advanced Counter FAdC® – originally developed before security-by-design principles became standard – can also be brought up to current cyber security expectations without redesigning the safety-critical core.

"As a global market leader, we continuously extend our portfolio, with safety and security as a fundamental part of our ongoing commitment to our customers. On that basis, we can confidently state that products within the active portfolio that fall under the scope of the Cyber Resilience Act (CRA) and are placed on the market after 11 December 2027 will be compliant with the CRA," says Andrzej Bartnik, CTO, Frauscher Sensor Technology.

With its IEC62443-4-1 certification and its participation in industry standards bodies, Frauscher positions itself not only as a manufacturer responding to new regulation, but as a partner ready to engage with customers, integrators and industry bodies on the cyber security challenges that digitalisation brings to the railway sector.

Image	Text
	Andrzej Bartnik, CTO, Frauscher Sensor Technology
	Florian Einböck, Head of Portfolio Strategy, Frauscher Sensor Technology

Copyright Images: ©Frauscher Sensor Technology

About Frauscher

Frauscher Sensor Technology provides field elements for train detection and wayside object controlling, complemented by software, connectivity, and data transmission solutions with comprehensive life cycle services. Our global network of locations and partners ensures reliable supply chain management and customer support, forming a trusted foundation for rail network operators. Frauscher is part of Wabtec Corporation, a global provider of equipment, systems, and digital solutions for freight and transit rail industries.

Contact for enquiries and sample copies

Frauscher Sensortechnik GmbH

Fabian Schwarz | Public Relations

Gewerbestraße 1 | 4774 St. Marienkirchen | Austria

T: +43 7711 2920 9495 | E: pr@frauscher.com

www.frauscher.com

Information contained in this news release is current as of the date of the press announcement but may be subject to change without prior notice.
