

PRESSEMITTEILUNG

ZUR SOFORTIGEN VERÖFFENTLICHUNG

Cyber Security wird zur gemeinsamen Aufgabe der gesamten Bahnindustrie

Frauscher erhält IEC62443-4-1-Zertifizierung für seinen sicheren Entwicklungsprozess

St. Marienkirchen bei Schärding, 22. Juli 2026: Mit zunehmender Vernetzung von Bahninfrastrukturen wird Cyber Security zu einer Verantwortung, die Hersteller, Systemintegratoren und Betreiber gemeinsam tragen. Neue Technologien bringen Effizienz und neue Möglichkeiten, aber auch Risiken, die auf jeder Stufe der Lieferkette berücksichtigt werden müssen. Der EU Cyber Resilience Act (CRA) bildet dafür den regulatorischen Rahmen. Frauscher Sensortechnik beschäftigt sich mit Cyber Security, seit das Unternehmen sein Portfolio um software- und netzwerkbasierte Lösungen erweitert hat, und hat nun einen weiteren Meilenstein erreicht: die Zertifizierung nach IEC62443-4-1:2018 für den sicheren Entwicklungsprozess (Secure Development Lifecycle, SDL), ausgestellt von TÜV Süd am 7. Mai 2026.

Neue Technologien, neue Verantwortung

Der Aufbau und Betrieb von Bahnnetzen ändert sich zunehmend durch Faktoren wie verteilte Systemarchitekturen, offene Netzwerkkommunikation und Datenaustausch in Echtzeit zwischen Betriebstechnik (OT) und IT-Umgebungen. Dieselben Eigenschaften, die diese Systeme effizienter machen, vergrößern zugleich die Anzahl der Punkte, die geschützt werden müssen. Hersteller müssen Schutzmaßnahmen bereits in den frühesten Entwicklungsphasen in ihre Produkte einbauen, Systemintegratoren müssen diesen Schutz in die fertige Installation übertragen, und Betreiber benötigen organisatorische Maßnahmen wie Zugriffskontrolle und Patch-Management, um Systeme über ihren gesamten Lebenszyklus hinweg sicher zu halten. Cyber Security ist damit nicht mehr die Aufgabe eines einzelnen Akteurs in der Lieferkette, sondern betrifft Hersteller, Integratoren und Betreiber gemeinsam.

Ein regulatorischer Rahmen für gemeinsame Verantwortung

Der EU Cyber Resilience Act spiegelt diesen Wandel wider. Er ist im Dezember 2024 in Kraft getreten und führt verbindliche Cyber Security-Anforderungen für Produkte mit digitalen Elementen ein, die auf dem EU-Markt in Verkehr gebracht werden. Die Meldepflicht für aktiv ausgenutzte Schwachstellen gilt ab dem 11. September 2026, die übrigen zentralen Pflichten – darunter grundlegende Sicherheitsanforderungen für neue Produkte, technische Dokumentation und CE-Kennzeichnung – ab dem 11. Dezember 2027. Bahnspezifische Normen ergänzen diesen allgemeinen Rahmen: IEC62443 und die davon abgeleitete, bahnspezifische Norm TS 50701 übersetzen diese Anforderungen in konkrete Maßnahmen für ein sicherheitskritisches Umfeld und stellen zugleich sicher, dass Security-bedingte Änderungen – etwa das Einspielen eines Patches – keine vollständige Safety-technische Neuzulassung erfordern.

Frauschers Engagement für Cyber Security

Frauschers eigenes Engagement für Cyber Security reicht zurück in die Zeit, als das Unternehmen sein Portfolio über Feldelemente hinaus um software- und netzwerkbasierte Lösungen erweiterte, darunter Frauscher Insights und Frauscher Connect. Sichere Netzwerkkommunikation etwa war schon immer ein zentrales Thema, doch der Fokus auf Cyber Security insgesamt wuchs in den darauffolgenden Jahren – ebenso wie in der gesamten

Bahnindustrie und darüber hinaus. Heute verfügt Frauscher über umfassende interne Expertise und hat Verbindungen innerhalb der Bahnindustrie sowie im weiteren Feld der Cyber Security aufgebaut.

„Digitale Signaltechnik mit IP-basierter Steuerung von Feldelementen ist ein zentraler Treiber für mehr Kapazität bei geringeren Gesamtbetriebskosten und für höhere Verfügbarkeit durch vorausschauende Wartung. Wir entwickeln unser Portfolio seit Jahren in diese Richtung, und Cyber Security muss von Anfang an ein verlässlicher, integrierter Bestandteil dieser neuen Architekturen sein“, erklärt Florian Einböck, Head of Portfolio Strategy bei Frauscher Sensortechnik.

Zertifizierung bestätigt den sicheren Entwicklungsprozess

IEC62443-4-1 definiert Anforderungen an einen sicheren Entwicklungsprozess für Produkte, die in industriellen Automatisierungs- und Steuerungssystemen eingesetzt werden. Die von TÜV Süd am 7. Mai 2026 verliehene Zertifizierung bestätigt, dass Frauschers Entwicklungsprozess auf jeder Stufe drei Kernprinzipien berücksichtigt:

- Security by Design: relevante Sicherheitsfaktoren werden von Anfang an berücksichtigt und dokumentiert
- Security by Default: Produkte werden mit sicheren Konfigurationen und Einstellungen ausgeliefert
- Security in Implementation: umfasst die Tests und die Dokumentation, die für den sicheren Betrieb eines Systems erforderlich sind

Ein eigenes Product Security & Network Team ist für Cyber Security-Maßnahmen und -Aktivitäten über den gesamten Produktlebenszyklus hinweg verantwortlich, einschließlich Schwachstellenmanagement und Penetration Tests. Schwachstellen, die in bereits veröffentlichten Produkten identifiziert werden, bearbeitet das Product Security Incident Response Team (PSIRT) von Frauscher, das entsprechende Sicherheitshinweise auf der PSIRT-Website des Unternehmens veröffentlicht; externe Akteure können Erkenntnisse ebenfalls direkt an das PSIRT melden.

Standards diskutieren und befolgen

Als aktiver Teil der Cyber Security-Community der Bahnindustrie beteiligen sich Frauscher-ExpertInnen an Arbeitsgruppen, etwa bei VDB und CENELEC. Dieser Austausch fließt direkt in die Produktentwicklung zurück. Neue Lösungen werden von Anfang an nach dem Prinzip „Cyber Secure by Design“ entwickelt. Auch bestehende Produkte wie der Frauscher Advanced Counter FAdC® – ursprünglich entwickelt, bevor Security-by-Design-Prinzipien zum Standard wurden – können ohne Neugestaltung des safety-relevanten Kerns auf aktuelle Cyber Security-Anforderungen gebracht werden.

„Als Weltmarktführer erweitern wir unser Portfolio kontinuierlich, wobei Safety und Security ein grundlegender Bestandteil unseres langfristigen Engagements für unsere KundInnen sind. Auf dieser Basis können wir mit Zuversicht feststellen, dass Produkte aus unserem aktiven Portfolio, die in den Anwendungsbereich des Cyber Resilience Act (CRA) fallen und nach dem 11. Dezember 2027 in Verkehr gebracht werden, die Anforderungen des CRA erfüllen werden“, sagt Andrzej Bartnik, CTO, Frauscher Sensortechnik.

Mit seiner IEC62443-4-1-Zertifizierung und seiner Mitwirkung in Normungsgremien positioniert sich Frauscher nicht nur als Hersteller, der auf neue Regulierung reagiert, sondern als Partner, der bereit ist, gemeinsam mit Kund:innen, Integratoren und Branchenverbänden die Cyber Security-Anforderungen anzugehen, die die Digitalisierung für die Bahnindustrie mit sich bringt.

Bild	Text
	Andrzej Bartnik, CTO, Frauscher Sensortechnik
	Florian Einböck, Head of Portfolio Strategy, Frauscher Sensortechnik

Copyright Bildmaterial: ©Frauscher Sensor Technology

Über Frauscher

Frauscher Sensortechnik liefert Feldelemente für die Zugdetektion und streckenseitige Objektsteuerung, ergänzt durch Software-, Konnektivitäts- und Datenübertragungslösungen sowie umfassende Life Cycle Services. Unser weltweites Netzwerk aus Standorten und Partnern gewährleistet zuverlässiges Supply Chain Management und Kundenbetreuung – eine vertrauensvolle Grundlage für Bahnbetreiber. Frauscher ist Teil der Wabtec Corporation, einem globalen Anbieter von Ausrüstung, Systemen und digitalen Lösungen für die Güter- und Personenverkehrsbahnindustrie.

Rückfragen und Kontakt für Belegexemplare

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.
