

22.07.2026

Pressemitteilung

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern
Deutschland
<https://www.pilz.com>

Security for Safety: Klare Strukturen im Automatisierungsnetzwerk

Ostfildern, 22.07.2026 - **Andreas Willert, Head of Industrial Security bei Pilz Österreich**

(Es gilt das gesprochene Wort)

Mit der Maschinenverordnung (EU) 2023/1230 wird klar geregelt: Safety funktioniert nur dann zuverlässig, wenn sicherheitsrelevante Funktionen gegen Manipulation geschützt sind. Moderne Maschinen sind digital vernetzt, werden über Software konfiguriert und im laufenden Betrieb angepasst. Jede unberechtigte Änderung – ob absichtlich oder versehentlich – kann Schutzmechanismen wirkungslos machen.

Deshalb ist Security heute kein Zusatzthema mehr, sondern Grundvoraussetzung für funktionierende Safety. Es geht darum, die Integrität aller sicherheitsrelevanten Komponenten sicherzustellen, damit Schutzfunktionen genau dann greifen, wenn sie gebraucht werden.

Wie Normen und Architekturprinzipien für robuste Sicherheit sorgen

Die Normenreihen IEC 62443 und die entstehende EN 50742 geben dafür einen klaren Rahmen vor. Beide fordern eine systematische Sicherheitsarchitektur, die Risiken bewertet, Schutzmaßnahmen strukturiert aufbaut und Systeme klar segmentiert.

Im Zentrum steht das „Zones and Conduits“-Prinzip: Systeme werden in Zonen unterteilt, die Übergänge dazwischen kontrolliert. Dieser Ansatz ermöglicht Defence in Depth, also eine abgestufte Sicherheitsstrategie, bei der mehrere Schutzschichten einander ergänzen und Manipulation erheblich erschweren.

Der IEC 62443 folgend, setzt Pilz auf eine strikte Trennung von Safety und Standard Automation.

Sicherheitsfunktionen laufen auf separater Hardware und sind organisatorisch sowie technisch abgeschottet.

Dadurch bleiben sie unabhängig von Updates, Fehlern oder Angriffen im Standardbereich. Die Angriffsfläche sinkt, der Pflegeaufwand ebenso.

Ein zentraler Erfolgsfaktor ist dabei der Grad der Isolation: Je stärker Safety-Funktionen vom Produktions- und Maschinennetzwerk getrennt sind, desto besser sind sie geschützt. Gleichzeitig reduziert sich der Bedarf an zusätzlichen Security-Maßnahmen.

Ein bewährter Ansatz ist es daher, die Geräte, die Safety-Funktionen ausführen, in ein eigenes Netzwerksegment zu überführen. Entscheidend ist die richtige Konfiguration dieses Segments durch Zugriffsrichtlinien sowie zusätzliche Authentifizierungsmechanismen. Da Safety-Systeme im Vergleich zur Standardautomatisierung sehr stabil sind und selten geändert werden, lässt sich diese strikte Segmentierung sowohl aus Effizienz- als auch aus Security-Perspektive gut umsetzen. Wichtig ist jedoch, dass die definierten Maßnahmen über den gesamten Lebenszyklus der Maschine konsequent aufrechterhalten werden.

Gerade bei größeren Maschinen oder komplexen Anlagen spielt jedoch die Verfügbarkeit von Diagnosedaten eine wichtige Rolle. Im Fehlerfall möchte man schnell nachvollziehen können, warum die Safety ausgelöst hat: Wurde ein Not-Halt betätigt – und wenn ja, welcher? Wurde ein Lichtgitter unterbrochen – und an welcher Stelle? Oder liegt möglicherweise ein Kurzschluss in der Verkabelung vor? Solche Informationen helfen dabei, Stillstandszeiten deutlich zu reduzieren und die Anlage schnell wieder produktiv zu betreiben. Dabei geht es bei Diagnosedaten nicht nur um „was ist kaputt“, sondern vor allem um „was ist genau passiert“.

In einer sauber segmentierten Architektur ist es dennoch möglich, Diagnosedaten der Safety an eine Standard-SPS weiterzuleiten – vorausgesetzt, der Zugriff auf die eigentlichen Safety-Funktionen innerhalb ihrer geschützten Zone bleibt strikt unterbunden.

Für einfache Anwendungen bieten Sicherheitsrelais der PNOZ Familie eine geeignete Lösung, während sich für umfangreichere Maschinen eine maßgeschneiderte Umsetzung mit myPNOZ empfiehlt. Diese Produkte verfügen über keine Netzwerkfähigkeiten und sind daher nicht aus der Ferne angreifbar. Dadurch reduzieren sich sowohl der Entwicklungsaufwand als auch die Anforderungen an Security-Maßnahmen im Betrieb erheblich. Ergänzend dazu bietet Pilz ein umfangreiches Trainings- und Serviceprogramm – von Grundlagen der Industrial Security bis hin zur CESA-Zertifizierung. Die Inhalte vermitteln, wie sichere Architekturen gestaltet, Risiken bewertet und Maßnahmen nachhaltig verbessert werden. So entsteht Kompetenz genau dort, wo sie benötigt wird: bei denjenigen, die Systeme planen, auslegen und verantworten.

Was dieser Ansatz konkret bewirkt

Die Trennung von Safety und Standard Automation bringt viele Vorteile mit sich – über den gesamten Lebenszyklus einer Maschine:

- Höhere Sicherheit: Safety-Funktionen sind gegen ungewollte Änderungen geschützt – unabhängig davon, was im Standardbereich passiert.
- Weniger Aufwand: Updates, Zertifizierungen und Anpassungen müssen nicht doppelt durchgeführt werden.
- Weniger Komplexität im Betrieb: Das Bedienpersonal braucht kein tiefes Security-Wissen; die Architektur sichert die Safety automatisch ab.
- Mehr Flexibilität: Unabhängige Safety-Systeme wie PNOZmulti 2 oder myPNOZ lassen sich herstellerübergreifend integrieren.
- Geringere Kosten: Weniger Support, weniger Lizenzen, weniger Eingriffe – und damit niedrige Total Cost of Ownership.

Pilz verbindet robuste Technik, klare Strukturen und gezielte Weiterbildung zu einer Security for Safety Strategie, die Normanforderungen erfüllt und im Alltag echte Erleichterungen schafft: sicher, verständlich und nachhaltig wirksam.

Bildunterschrift:

Texte und Bilder zum Download finden Sie unter:

<https://www.pilz.com/de-INT/company/press/messages/articles/249002>

Pilz - The Spirit of Safety

Pilz ist globaler Anbieter von Produkten, Systemen und Dienstleistungen für die Automatisierungstechnik. Als Pionier der sicheren Automation schafft Pilz Sicherheit für Mensch, Maschine und Umwelt. Gegründet 1948 ist das Familienunternehmen mit Stammsitz in Ostfildern heute weltweit mit 2.500 Mitarbeiterinnen und Mitarbeitern in 42 Tochtergesellschaften und Niederlassungen vertreten. Der Technologieführer bietet komplette Automatisierungslösungen für Safety und Industrial Security an der Maschine. Diese umfassen Sensorik sowie Steuerungs- und Antriebstechnik – inklusive Systemen für die industrielle Kommunikation, Diagnose und Visualisierung. Ein internationales Dienstleistungsangebot mit Beratung, Engineering und Schulungen rundet das Portfolio ab. Lösungen von Pilz kommen über den Maschinen- und Anlagenbau hinaus in zahlreichen Branchen zum Einsatz, wie etwa der Intralogistik, der Verpackung und der Bahntechnik oder im Bereich Robotik.

Pilz in sozialen Netzwerken

In unseren Social Media Kanälen geben wir Hintergrundinformationen über das Unternehmen und den Menschen bei Pilz. Wir berichten über aktuelle Entwicklungen und Trends in der Automatisierungstechnik.



<https://www.facebook.com/pilzINT>



<https://www.youtube.com/user/PilzINT>



<https://www.xing.com/pages/pilzgmbh-co-kg>



<https://www.linkedin.com/company/pilz>



<https://pilz-magazine.com/de/>

Kontakt für Presse

Martin Kurth
Unternehmens- und Fachpresse
+49 711 3409 - 0
publicrelations@pilz.com

Sabine Karrer
Fach- und Unternehmenspresse
+49 711 3409 - 7009
s.skaletz-karrer@pilz.de