

Security schützt Safety

„Zones and Conduits“ in Automatisierungsnetzwerken: Safety hat oberste Priorität



Die Maschinenverordnung macht es zur Pflicht: Industrial Security soll sicherheitsrelevante Funktionen vor Manipulation schützen – also Security als Voraussetzung für funktionierende Safety. Doch wie lässt sich ein Automatisierungsnetzwerk ganzheitlich absichern? Normen wie IEC 62443-3-2 und die kommende EN 50742 geben eine Richtung vor:

Systeme in Zonen trennen, Verbindungen kontrollieren – ein Prinzip, das sich quer durch aktuelle Empfehlungen von Verbänden und Experten findet. Pilz ist überzeugt: Die konsequente Trennung von Safety und sogenannter Standard-Automation ist der Schlüssel zu wirksamer Maschinensicherheit – getragen vom Defence-in-Depth-Prinzip und umgesetzt durch den Zones-and-Conduits-Ansatz.

Ein bildlicher Vergleich

Ein Haus kann solide und sicher gebaut sein: mit stabilen Wänden, feuerfesten Materialien, zuverlässiger Elektrik und funktionierenden Alarmanlagen. Diese bauliche Sicherheit steht exemplarisch für die Safety von Maschinen, bei denen konstruktive Maßnahmen, Sensorik und Schutzmechanismen ungewollte Gefährdungen verhindern sollen. Ein solches Haus bleibt jedoch nur dann sicher, wenn keine gezielten Eingriffe stattfinden. Manipulierte Heizungssteuerungen, sabotierte Stromkreise oder deaktivierte Alarmanlagen können ein objektiv sicher konstruiertes Gebäude in ein Risiko verwandeln. Auch in der Maschinenwelt wird die beste sicherheitstechnische Konstruktion wirkungslos, wenn sicherheitsrelevante Komponenten unautorisiert beeinflusst oder außer Kraft gesetzt werden.

Security übernimmt in diesem Bild die Rolle des äußeren Schutzes: robuste Türen, gesicherte Zugänge, überwachte Verbindungen und Barrieren gegen unerwünschte Eingriffe. Security schützt also nicht vor Unfällen selbst, sondern davor, dass Schutzmechanismen außer Kraft gesetzt werden – etwa durch Personen, die durch unberechtigte Betriebsartenwahl oder unautorisierte Handlungen zugreifen. Erst dadurch bleibt Safety verlässlich wirksam – Security for Safety.

Von der normativen Vorgabe bis zum Lösungsvorschlag

Die Maschinenverordnung (EU) 2023/1230 macht Security erstmals zu einer verbindlichen Voraussetzung für funktionierende Safety an Maschinen und Anlagen: Sicherheitsfunktionen dürfen weder durch absichtliche noch unbeabsichtigte Manipulation beeinträchtigt werden.

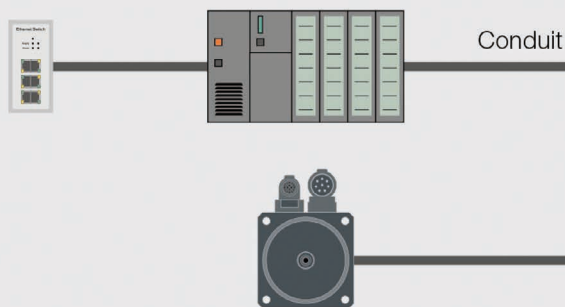
Genau daran knüpft die entstehende Norm EN 50742 an, die dabei helfen wird, die grundlegenden Security-Anforderungen der Maschinenverordnung zu konkretisieren. Die Norm definiert technische Details für den Schutz gegen Korruption und stellt klare Anforderungen an Hardware, Software und Daten, die sicherheitsrelevante Funktionen beeinflussen können. Die Norm deckt den gesamten Lebenszyklus ab – von Entwicklung über Betrieb bis zur Außerbetriebnahme.

Eine zentrale Rolle spielt daneben die bereits bestehende Normenreihe IEC 62443, die systematische Cybersicherheit für industrielle Automatisierungs- und Steuerungssysteme beschreibt. Sie bietet einen strukturierten Rahmen für Risikoanalysen, „Defence-in-Depth“ sowie das Prinzip der Segmentierung („Zones and Conduits“) und wird in der EN 50742 ausdrücklich als alternativer oder ergänzender Ansatz zur Sicherheitsabsicherung anerkannt. Zusammen bilden diese Normen den normativen Kern von Security for Safety: Sie verlangen, dass die digitale Integrität einer Maschine als Voraussetzung für ihre funktionale Sicherheit verstanden und entsprechend geschützt wird.

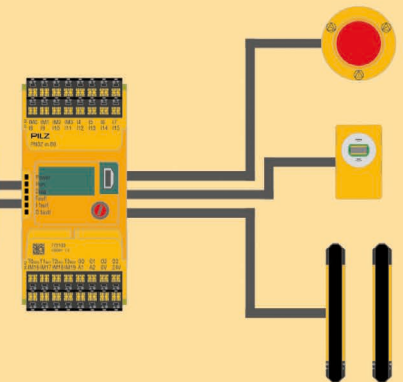
Warum „Zones and Conduits“ Maschinen sicherer macht

Zurück zum Bild des Hauses: Der Heizungsraum steht für eine Zone, die Verbindung zum Smart-Home-Gateway für den zugehörigen Verbindungspfad. Wird diese Verbindung manipuliert, lässt sich die gesamte Anlage beeinflussen – selbst wenn der Raum perfekt geschützt ist. Entscheidend ist daher nicht nur die Absicherung der einzelnen Bereiche, sondern ebenso die Sicherheit der Wege, die sie verbinden. Genau an diesem Punkt setzt das Prinzip „Zones and Conduits“ an.

Automation Zone



Safety Zone



Bereiche werden klar voneinander getrennt, und die Übergänge zwischen ihnen werden kontrolliert gestaltet. Wie in einem Haus, in dem Türen und zugewiesene Schlüssel festlegen, wer wohin gelangt, greifen in einer industriellen Anlage innerer Schutz (Safety) und äußerer Schutz vor Manipulation (Security) strukturiert ineinander.

Defence-in-Depth

Damit entsteht ein Schutzkonzept, das dem Prinzip Defence-in-Depth folgt: Sicherheit wird nicht durch eine einzige Barriere erreicht, sondern durch mehrere hintereinander geschaltete Schutzschichten. Wird eine Schicht überwunden, hält die nächste stand. Zonen bilden diese gestaffelten Räume, Conduits die kontrollierten Durchgänge zwischen ihnen. Auf diese Weise wird verhindert, dass eine einzige Schwachstelle das Gesamtsystem gefährdet – besonders dann, wenn es um Safety und damit um den Schutz von Menschen geht.

„Security for Safety“

Safety ist das oberste Schutzziel von Security. Im Mittelpunkt steht der Schutz der Safety, die wiederum den Menschen schützt. Deshalb wird Safety von der allgemeinen Maschinen-Steuerung, der so genannten Standard-Automation getrennt, und reduziert so die Exposition sicherheitsrelevanter Funktionen. Je deutlicher diese „Einheiten“ funktional separiert werden, desto weniger zusätzliche Sicherheitsmaßnahmen sind nötig, um sie zuverlässig zu schützen.

Vorteile

Die Vorteile dieser Herangehensweise zeigen sich über den gesamten Lebenszyklus einer Maschine hinweg. Werden Safety und Standardfunktionen getrennt, müssen bei einer Aktualisierung der Standardfunktionen die Safety-Funktionen nicht parallel rezertifiziert oder angepasst werden, was Wartungs- und Servicetätigkeiten deutlich redu-

ziert. Klassische Sicherheitscontroller benötigen zudem wesentlich seltener sicherheitskritische Updates als Standard-Controller, sodass durch die Trennung viele unnötige Eingriffe entfallen.

Auch technologisch eröffnet die Separation Vorteile: Ein eigenständiges Safety-System lässt sich frei mit unterschiedlichen Steuerungsherstellern kombinieren, während sich frei mit unterschiedlichen Steuerungsherstellern kombinieren, während integrierte Systeme häufig an spezifische Technologien gebunden sind. Gleichzeitig erhöhen separate Safety-Lösungen die Hürden für Angreifer, denn getrennte Systeme müssen einzeln kompromittiert werden, was Manipulation erheblich erschwert. Hinzu kommt, dass ein Standard-System bei Bedarf online sein kann, während die eigentlichen Safety-Funktionen abgeschaltet bleiben, wodurch dessen Angriffsfläche drastisch reduziert wird.

Zudem steigert diese Trennung von Safety- und Security-Automation mit jeweils optimal abgestimmten Security-Leveln die Effizienz aufgrund von verbesserter Planbarkeit von Sicherheits-, Wartungs- und Erweiterungsmaßnahmen. Änderungen am Standardprogramm erfordern dann keine Eingriffe in den sicherheitsrelevanten Teil, was den Programmier- und Anpassungsaufwand deutlich reduziert. Gleichzeitig wirkt sich die Trennung positiv auf Software- und Supportkosten aus, da in separaten Systemen häufig weniger Lizenz- und Servicegebühren anfallen.

Schutz durch Trennung

Die klare Trennung von Safety und Standard-Automation sorgt nicht nur für technische Robustheit, sondern auch für weniger Bedienfehler und geringere Schulungsanforderungen. Da sicherheitsrelevante Funktionen auf eigener Hardware laufen und organisatorisch sauber abgegrenzt sind, bleiben sie selbst dann geschützt, wenn im Standardprogramm Änderungen vorgenommen

werden. Fehler im Alltagsbetrieb gefährden die Safety dadurch nicht und Verantwortlichkeiten lassen sich klarer zuordnen.

Vorteile durch die Trennung

Ein entscheidender Vorteil dieses Ansatzes: Das Bedienpersonal beim Endanwender muss nicht tief in Security Themen eingearbeitet werden, da der Schutz der Safety-Funktionen bereits durch die architektonische Gestaltung gewährleistet ist. Die Trainings richten sich daher vor allem an diejenigen, die Security-Entscheidungen treffen oder Systeme auslegen – während die Bediener weiterhin sicher arbeiten können, ohne zusätzlichen Schulungsaufwand im Bereich Industrial Security. Dadurch entsteht eine praxisgerechte Rollenverteilung, die den Anlagenbetrieb vereinfacht und gleichzeitig das Schutzniveau nachhaltig erhöht.

Mehr Sicherheit durch klare Struktur

Eine wirksame Security-for-Safety-Strategie entsteht nicht durch Einzelmaßnahmen, sondern durch eine durchdachte Architektur, klare Verantwortlichkeiten und gezielte Kompetenzentwicklung. Mit dem konsequenten Fokus auf Defence-in-Depth und einer sauberen Trennung von Safety und Standard-Automation wird die Grundlage für widerstandsfähige Maschinen geschaffen. Sinnvoll sind praxisnahe Trainings und Beratung, damit Unternehmen diesen Weg souverän gehen können. So entsteht ein Sicherheitsniveau, das nicht nur Normanforderungen erfüllt, sondern im täglichen Betrieb spürbaren Mehrwert liefert: einfacher, robuster und nachhaltig wirksam.

Wer schreibt:

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. Der Technologieführer bietet komplette Automatisierungslösungen für Safety und Industrial Security an der Maschine. ◀