

22.07.2026

Persbericht

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern

<https://www.pilz.com>

Security for Safety: Duidelijke structuren in het automatiseringsnetwerk

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

(Het gesproken woord geldt)

In de Machineverordening (EU) 2023/1230 wordt duidelijk vastgelegd: veiligheid werkt alleen betrouwbaar als veiligheidsrelevante functies tegen manipulatie zijn beveiligd. Moderne machines zijn digitaal verbonden, worden via software geconfigureerd en tijdens het gebruik aangepast. Elke onbevoegde wijziging – of deze nu opzettelijk of per ongeluk is aangebracht – kan ervoor zorgen dat beveiligingsmechanismen hun werking verliezen.

Daarom is security tegenwoordig geen bijkomstig onderwerp meer, maar een basisvoorwaarde voor een goed functionerende veiligheid. Het gaat erom de integriteit van alle veiligheidsrelevante componenten te waarborgen, zodat de beveiligingsfuncties precies op het juiste moment in werking treden wanneer dat nodig is.

Hoe normen en architectuurprincipes zorgen voor robuuste veiligheid

De normenreeksen IEC 62443 en de in ontwikkeling zijnde EN 50742 bieden hiervoor een duidelijk kader. Beiden pleiten voor een systematische beveiligingsarchitectuur die risico's beoordeelt, beveiligingsmaatregelen op gestructureerde wijze opbouwt en systemen duidelijk segmenteert.

Centraal staat het 'Zones and Conduits'-principe: systemen worden onderverdeeld in zones, waarbij de overgangen daartussen worden gecontroleerd. Deze aanpak maakt 'Defence-in-Depth' mogelijk, oftewel een gelaagde beveiligingsstrategie waarbij meerdere beveiligingslagen elkaar aanvullen en manipulatie aanzienlijk bemoeilijken.

In overeenstemming met de norm IEC 62443 hanteert Pilz een strikte scheiding tussen veiligheids- en standaardautomatisering. Veiligheidsfuncties draaien op aparte hardware en zijn zowel organisatorisch als technisch afgeschermd. Daardoor blijven ze onafhankelijk van updates, fouten of aanvallen in het standaardbereik. De kwetsbaarheid neemt af, evenals de onderhoudskosten.

Een belangrijke succesfactor hierbij is de mate van isolatie: hoe sterker de veiligheidsfuncties zijn gescheiden van het productie- en machinenetwerk, hoe beter ze worden beschermd. Gelijktijdig neemt de behoefte aan aanvullende security-maatregelen af.

Een beproefde aanpak is daarom om de apparaten die veiligheidsfuncties uitvoeren, onder te brengen in een apart netwerksegment. Het is van cruciaal belang dat dit segment correct wordt geconfigureerd door middel van toegangsrichtlijnen en aanvullende authenticatiemechanismen. Aangezien veiligheidssystemen in vergelijking met standaardautomatisering zeer stabiel zijn en zelden worden gewijzigd, kan deze strikte segmentering zowel vanuit het oogpunt van efficiëntie als vanuit het oogpunt van security goed worden toegepast. Het is echter belangrijk dat de vastgestelde maatregelen gedurende de gehele levenscyclus van de machine consequent worden gehandhaafd.

Juist bij grotere machines of complexe installaties speelt de beschikbaarheid van diagnosegegevens echter een belangrijke rol. Als er een storing optreedt, wil men snel kunnen achterhalen waarom het veiligheidssysteem in werking is getreden: is er een noodstop geactiveerd – en zo ja, welke? Is er een lichtscherf onderbroken – en op welke plek? Of is er misschien sprake van kortsluiting in de bedrading? Dergelijke informatie helpt om stilstandtijden aanzienlijk te verminderen en de installatie snel weer productief te maken. Bij diagnosegegevens gaat het niet alleen om „wat er kapot is“, maar vooral om „wat er precies is gebeurd“.

In een goed gesegmenteerde architectuur is het niettemin mogelijk om diagnosegegevens van het veiligheidssysteem door te sturen naar een standaard-SPS – op voorwaarde dat de toegang tot de eigenlijke veiligheidsfuncties binnen hun beveiligde zone strikt verboden blijft.

Voor eenvoudige toepassingen bieden veiligheidsrelais uit de PNOZ-serie een geschikte oplossing, terwijl voor complexere machines een op maat gemaakte oplossing met myPNOZ aan te raden is. Deze producten beschikken niet over netwerkfunctionaliteit en zijn daarom niet kwetsbaar voor aanvallen op afstand. Hierdoor worden zowel de ontwikkelingskosten als de eisen aan security-maatregelen tijdens het gebruik aanzienlijk verminderd. Daarnaast biedt PILZ een uitgebreid opleidings- en serviceprogramma aan – van de basisprincipes van Industrial Security tot CESA-certificering. De inhoud laat zien hoe architecturen met hoge veiligheid worden ontworpen, risico's worden beoordeeld en maatregelen op duurzame wijze worden verbeterd. Zo ontstaat expertise precies daar waar die nodig is: bij degenen die systemen plannen, ontwerpen en daarvoor verantwoordelijk zijn.

Wat deze aanpak concreet oplevert

De scheiding tussen veiligheid en standaardautomatisering biedt tal van voordelen – gedurende de gehele levenscyclus van een machine:

- Meer veiligheid: veiligheidsfuncties zijn beveiligd tegen onbedoelde wijzigingen – ongeacht wat er in het standaardgedeelte gebeurt.
- Minder werk: updates, certificeringen en aanpassingen hoeven niet dubbel te worden uitgevoerd.
- Minder complexiteit tijdens het gebruik: het bedienend personeel hoeft geen diepgaande kennis van security te hebben; de architectuur waarborgt de veiligheid automatisch.
- Meer flexibiliteit: onafhankelijke veiligheidssystemen zoals PNOZmulti 2 of myPNOZ kunnen merkonafhankelijk worden geïntegreerd.
- Lagere kosten: minder ondersteuning, minder licenties, minder ingrepen – en dus lagere Total Cost of Ownership.

Pilz combineert robuuste techniek, duidelijke structuren en gerichte bijscholing tot een 'Security for Safety'-strategie die aan de normen voldoet en in de dagelijkse praktijk echte voordelen biedt: veilig, begrijpelijk en duurzaam effectief.

Bijschrift:

Teksten en afbeeldingen om te downloaden kunt u vinden op:

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

Pilz - The Spirit of Safety

Pilz is een mondiale aanbieder van producten, systemen en diensten voor de automatiseringstechniek. Als pionier op het gebied van veilige automatisering creëert Pilz veiligheid voor mens, machine en milieu. Het in 1948 opgerichte familiebedrijf met de hoofdvestiging in Ostfildern is tegenwoordig met 2500 medewerkers in 42 dochterondernemingen en vestigingen op alle continenten vertegenwoordigd.

De technologieleider biedt complete automatiseringsoplossingen voor safety en industrial security op de machine. Die omvatten sensoren evenals besturings- en aandrijftechniek – inclusief systemen voor industriële communicatie, diagnose en visualisering. Een internationaal dienstenaanbod met advies, engineering en trainingen completeert het portfolio. Oplossingen van Pilz worden niet alleen gebruikt in de machine- en installatiebouw, maar ook in tal van andere sectoren, zoals intralogistiek, verpakkings- en spoorwegtechniek of op het gebied van robotica.

Pilz in sociale netwerken

Op onze socialmediakanalen vindt u achtergrondinformatie over ons bedrijf en de mensen achter Pilz. Ook houden we u hier op de hoogte van actuele ontwikkelingen op het gebied van automatiseringstechnologie.



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



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



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



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

Contactpersoon voor journalisten

Martin Kurth

Bedrijfs- en vakpers

+49 711 3409 - 0

publicrelations@pilz.com

Sabine Skaletz-Karrer

Vakpers

+49 711 3409 - 7009

s.skaletz-karrer@pilz.de