Achtergrondinformatie

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern
Duitsland/Germany
www.pilz.com

Oktober 2025

Bescherming voor bedrijven, machines en producten

Safety en Industrial Security – alles van één leverancier

Ostfildern, oktober 2025 - **Security-incidenten komen niet meer alleen bij IT-systemen, maar steeds vaker ook in de productieomgeving (OT) voor. Gerichte aanvallen en ook onbewuste manipulatie worden beschouwd als incidenten op het gebied van Industrial Security. De taak van Industrial Security bij de productie is om de beschikbaarheid van machines en installaties alsmede de integriteit en vertrouwelijkheid van machinale gegevens en processen te garanderen. Het belangrijkste beschermingsdoel is echter functionele veiligheid. Als bedrijven immers geen controle meer hebben over hun gegevens, staat niet alleen het bedrijf zelf maar ook de veiligheid van hun medewerkers op het spel: zonder Security geen Safety en zonder Safety geen bescherming van mensen!**

Binnen de EU is er aandacht voor de toenemende dreiging en is de wet- en regelgeving dienovereenkomstig aangepast: Op bedrijfsniveau zijn in het kader de **NIS2-richtlijn** maatregelen vereist om een hoog gemeenschappelijk niveau van cyberveiligheid in de EU te waarborgen, bijvoorbeeld door middel van een informatiebeveiligingsmanagementsysteem.

De **EU-Machineverordening 2023/1230** beschrijft nu voor machines en installaties de bescherming tegen corruptie voor en verlangt Industrial Security-maatregelen voor die onderdelen van de machine die invloed op de functionele veiligheid hebben.

De **Cyber Resilience Act (CRA)** brengt nieuwe security-eisen met zich mee voor producten met digitale elementen. Daartoe behoren

ook besturingen, IO-systemen en andere componenten die in machines worden gebruikt.

Bedrijven, machines en producten – op elk niveau hebben machinefabrikanten en -exploitanten te maken met verschillende uitdagingen en verschillende wettelijke kaders.

State-of-the-art veiligheid

Ongeacht of de wet- en regelgeving Industrial Security verplicht stelt, zijn er goede redenen om in een vroeg stadium met dit onderwerp aan slag te gaan en advies in te winnen. Gangbare processen en omstandigheden voor de werking van machines kunnen namelijk manipulatie in de hand werken wanneer ze niet regelmatig onder de loep worden genomen. Een lange levensduur van machines betekent bijvoorbeeld vaak dat de bijbehorende systemen verouderd raken en op een gegeven moment niet meer aan de huidige security-normen voldoen. Deze systemen hebben beveiligingslekken die niet meer kunnen worden gedicht, omdat de aanbieder geen security-updates meer levert. Ook kan de beveiliging tegen schadelijke software vaak niet op de eindapparaten worden geïmplementeerd, omdat deze soms te oud zijn en hun performance daardoor zou verslechteren met als gevolg dat er productieonderbrekingen kunnen optreden.

Stap voor stap naar meer Industrial Security

Uiteindelijk gaat het erom dat de bedrijfsvoering beschermd blijft, maar daarvoor moeten bedrijven verschillende uitdagingen overwinnen: van het identificeren van de geldende wettelijke voorschriften, het detecteren en elimineren van zwakke plekken in systemen en het bewust maken en trainen van de medewerkers tot de aansluitende implementatie van controles. Aangezien security een zogenaamd “moving target” is, moet bovendien de status van de

Industrial Security van de machines regelmatig worden gecontroleerd. Het is belangrijk dat er sprake is van duidelijke verantwoordelijkheden binnen het bedrijf, evenals een systematische aanpak, waaronder het ontwikkelen van de benodigde expertise.

Het automatiseringsbedrijf Pilz heeft zich ingesteld op deze eisen en voor machinefabrikanten en gebruikers een dienstenportfolio op maat samengesteld die alle aspecten voor de bescherming van mens en machine omvat. De experts van Pilz kennen de huidige wettelijke en normatieve vereisten en nemen deze mee in hun advies. Om security-kennis in bedrijven te ontwikkelen of te actualiseren, wordt het aanbod aangevuld met trainingen. De praktische uitvoering vindt ook plaats met behulp van Pilz-productoplossingen, zoals het aanbod op het gebied van Identification and Access Management (I.A.M.) voor meer Safety en Industrial Security.

De juiste basis

Om Industrial Security op de eigen machines te garanderen, hebben vakmensen in de machine- en installatiebouw gedegen basiskennis nodig, vooral van wetgeving en geldende normen. De experts van Pilz geven deze knowhow door in de training "Fundamentals of Industrial Security". Deelnemers leren Security-bedreigingen, passende beveiligingsmaatregelen en best practices in de context van machine- en netwerkveiligheid te begrijpen. Hierdoor leren ook beginners op het gebied van security met welke maatregelen ze machines effectief kunnen beveiligen tegen cyberaanvallen en manipulatie bij de machinale productie.

Met de kwalificatie "CESA - Certified Expert for Security in Automation" biedt Pilz een tweedaagse expert cursus aan, die deelnemers diepgaande Security-kennis geeft op basis van de nieuwste normen, met name met betrekking tot de normen IEC 62443

(“Industriële communicatienetwerken - IT-beveiliging voor netwerken en systemen”). Bovendien worden er praktische risicobeperkende maatregelen, zoals toegangscontrole en het verbeteren van de netwerkbeveiliging met technische middelen, alsmede organisatorische maatregelen voor het verminderen van security-risico's behandeld. Deelnemers leren hoe ze de norm correct kunnen toepassen en hoe ze kunnen aantonen dat hun automatiseringssystemen voldoen aan de vereisten voor cyberveiligheid. Als de deelnemers slagen voor het examen, ontvangen ze het wereldwijd erkende TÜV NORD-certificaat “CESA – Certified Expert for Security in Automation”.

Theoretische kennis in de praktijk brengen

Voortbouwend op de theoretische basis en de trainingen is de volgende stap in het versterken van Industrial Security het toepassen van gestructureerde, praktijkgerichte processen. Advies ten aanzien van Operational Technology (OT) slaat een brug tussen de theoretische basis en praktijkstrategieën. Met behulp van een gefaseerde aanpak worden in het kader van Industrial Security Services de kwetsbaarheden in complexe systemen geïdentificeerd en maatregelen ontwikkeld om de risico's te minimaliseren, wat uiteindelijk resulteert in een integraal veiligheidsconcept.

Vier stappen voor meer Industrial Security

Het OT-Security-proces omvat vier stappen; analyse van de beschermingsbehoeften, Industrial Security-risicobeoordeling, Industrial Security-concept en Industrial Security-systeemverificatie.

Bij de analyse van de beschermingsbehoeften worden in het bedrijf de beschermingsbehoefte van de afzonderlijke "assets" in de machine of installatie alsmede hun beschermingsdoelen vastgesteld.

In de tweede stap, de risicobeoordeling, worden alle risico's en de waarschijnlijkheid van optreden beoordeeld en wel voor elk deel gedurende de complete levenscyclus van het systeem. In de volgende stap wordt een gedetailleerd Industrial Security-concept ontwikkeld, met strategieën en maatregelen voor het afwenden en verminderen van risico's als gevolg van aanvallen, manipulatie en verkeerde bediening. Ook worden er policies, regels en richtlijnen voor de verdere veilige werking of opbouw van het systeem opgesteld. In de laatste stap, de Industrial Security-systeemverificatie, wordt de effectiviteit van de geïmplementeerde tegenmaatregelen gecontroleerd.

Machinebeschikbaarheid waarborgen

Het Industrial Security Services-proces helpt cyberaanvallen te beperken of te voorkomen. Ook het aantal onbedoeld veroorzaakte security-incidenten neemt af. Dit verhoogt de machinebeschikbaarheid en zorgt uiteindelijk voor kostenbesparing en het behoud van de rentabiliteit.

Deze aanpak zorgt er vooral voor dat mensen bij de machine door middel van passende security-maatregelen zijn beschermd. Een security-incident kan namelijk een belemmering voor Safety-maatregelen vormen. Zo zorgt een lichtscherm voor machines er bijvoorbeeld voor dat de operator niet een gevarenzone instapt. Als een hacker echter de bijbehorende besturing en het mechanisme kan beïnvloeden, kan de beschermende functie van het lichtscherm niet meer worden gegarandeerd. Security beveiligt Safety!

Bij de concrete uitvoering bij de machine is een gemeenschappelijke benadering van Safety en Security dus zinvol. Want zonder Security geen Safety en zonder Safety geen bescherming van mensen.

Duidelijk geregeld: Wie mag wat bij de machine?

De veiligheid van een machine en haar operators staat of valt met het reguleren van de toegang – voor mensen of netwerken. Ingangen moeten worden beveiligd tegen onbevoegde toegang, zodat er bijvoorbeeld tijdens het bedrijf van de machine geen personen in de gevarenzone aanwezig zijn. Want zelfs het goedbedoeld bedienen of onderhouden van een machine – ter plekke of via een netwerk – zou fatale gevolgen kunnen hebben.

Een belangrijke bouwsteen is het Identification and Access Management (I.A.M.), dat rechten en de toegang op machines en installaties in bedrijven duidelijk regelt. Daartoe behoren organisatorische maatregelen en voorschriften alsmede geschikte veiligheidsfuncties. Een toegangsautorisatiesysteem zoals dat PITreader van Pilz is daarbij de juiste productbouwsteen. Hiermee kunnen gebruikers voldoen aan de eisen op het gebied van werknemersbescherming, aansprakelijkheidsbescherming, maximale productiviteit en de bescherming van uw gegevens.

Alleen een integrale benadering van Safety en Security waarborgt een uitgebreide bescherming van mens en machine. Of en in welke mate een bedrijf zich met security wil bezighouden, is niet langer iets dat het bedrijf naar eigen inzicht kan bepalen. Het is inmiddels wettelijk voorgeschreven. In de machinebouw is security in de vorm van Industrial Security niet alleen de taak van de IT, maar een integraal onderdeel van het ontwerp en de constructie. Het achteraf implementeren van security is omslachtig en betekent meestal een verlies aan gebruiksvriendelijkheid, functionaliteit en productiviteit.

((Tekens: 9.784))

((Kader:))

Een overzicht van de EU-wetgeving op het gebied van Industrial Security:

Vooral in Europa reageert de wetgever met een aantal wetten op de dreiging. Hierdoor gelden in Europa de strengste voorschriften ter wereld. Maar er vindt al afstemming met andere landen plaats en ook daar zullen dergelijke wetten er komen. Er valt dus een wereldwijde harmonisatie op het gebied van Industrial Security te verwachten.

NIS2: meer plichten voor bedrijven

NIS (Network and Information Security) is een richtlijn van de Europese Unie voor het versterken van de cyberveiligheid. Deze richtlijn is al sinds 2016 van kracht en gold tot nu toe voor aanbieders van kritieke infrastructuren, waaronder in de sectoren energie, verkeer, bankwezen en financiën, gezondheid, drinkwatervoorziening en -distributie en digitale infrastructuur. Aanbieders in deze sectoren moesten met het oog op security "passende veiligheidsmaatregelen" treffen en ernstige cyberveiligheidsincidenten melden. De nieuwe NIS2-richtlijn ((EU) 2022/2555 ... betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie) verplicht aanzienlijk meer bedrijven om in de toekomst risicobeheermaatregelen op het gebied van cyberveiligheid te nemen. NIS2 breidt de sectoren uit met bijvoorbeeld de producerende industrie, waaronder ook machinebouw en fabrikanten van elektrische apparatuur.

Risicoanalyses en veiligheidsconcepten voor informatiesystemen, de bescherming van de toeleveringsketen en de veiligheid van het personeel worden vereist. Ook concepten voor de toegangscontrole

en het beheer van installaties horen erbij, evenals verplichte trainingen voor het management.

De richtlijn werd eind 2022 aangenomen door het Europees Parlement en de Raad van de EU. Zoals alle EU-richtlijnen is ook NIS2 niet onmiddellijk van kracht en bindend in de afzonderlijke EU-lidstaten, maar moet deze richtlijn door de lidstaten worden omgezet in nationaal recht. Bedrijven doen er goed aan om zo snel mogelijk met NIS2 aan de slag te gaan en een uitgebreide security-beoordeling voor het bedrijf uit te voeren. Daartoe behoort bijvoorbeeld het opzetten van een beheersysteem voor informatiebeveiliging (ISMS). In deze context is een certificering volgens de informatiebeveiligingsnorm ISO 27001 nuttig.

NIS2 aan de hand van het voorbeeld van windturbines: met NIS2 moeten in de toekomst ook machinefabrikanten, zoals een fabrikant van installaties voor stroomopwekking (bijvoorbeeld windturbines), aan de voorschriften voldoen. De fabrikant van de windturbine heeft bijvoorbeeld automatiseringsoplossingen, besturingen of sensoren nodig. Vanaf een bepaalde omvang vallen ook fabrikanten van elektrische componenten onder NIS2. En aangezien NIS2 ook bepaalt dat rekening moet worden gehouden met leveranciers, moet ook een bedrijf als Pilz zorgen voor veilige toeleveringsketens en eisen stellen aan zijn leveranciers. NIS2 omvat dus de volledige toeleveringsketen.

De nieuwe machineverordening: zonder security geen CE-markering

De Machinerichtlijn 2006/42/EG speelt een belangrijke rol in het kader van de functionele veiligheid.

Machinefabrikanten moeten van oudsher een passende conformiteitsbeoordelingsprocedure, eindigend met de CE-markering, doorlopen om machines in Europa te kunnen invoeren.

De in juni 2023 opnieuw als Machineverordening gepubliceerde voorschriften zijn op de huidige stand van de techniek gebracht. Aangezien het om een verordening gaat, hoeft deze niet eerst in nationaal recht te worden omgezet. Machinefabrikanten hebben tot 20 januari 2027 de tijd om over te stappen op de nieuwe eisen en hieraan te voldoen.

De Machineverordening vervangt de huidige Machinerichtlijn en stelt, in tegenstelling tot haar voorganger, cybersecurity verplicht. Waar de Machinerichtlijn uitsluitend betrekking had op de Safety, is in de Machineverordening ook het beschermingsdoel security opgenomen onder "Protection against corruption" in de "Essential Health and Safety Requirements (EHSR)": de veiligheidsfuncties van een machine mogen niet worden beïnvloed door onopzettelijke of opzettelijke vervalsing.

Deze nieuwe weg naar de CE-markering werpt een aantal nieuwe vragen voor machinefabrikanten en -operators op, omdat ze hun bestaande veiligheidsconcepten voor Safety en Security zullen moeten herzien.

Cyber Resilience Act: security gedurende de gehele productlevenscyclus

Naast het beoordelen van het bedrijf en de machines is ook het direct implementeren van security-maatregelen in de apparaten (zoals besturingen) absoluut noodzakelijk. In september 2022 presenteerde de Europese Commissie een ontwerp van een verordening die de

cyberveiligheid van producten moet vergroten. Deze Cyber Resilience Act (CRA) is gericht op fabrikanten van producten met digitale elementen (hard- en software) die met andere producten kunnen communiceren. Het gaat om producten uit zowel de B2C-sector, zoals smartphones of robotstofzuigers, als de B2B-sector, zoals besturingen en sensoren, maar ook op om pure softwareproducten zoals besturingssystemen of de machine zelf.

De verplichting voor fabrikanten om misbruikte kwetsbaarheden te melden, geldt vanaf 11 september 2026. Producten met digitale elementen moeten vanaf 11 december 2027 voldoen aan de vereisten van de CRA, om in de EU op de markt te kunnen worden gebracht. De CRA is een EU-verordening en wordt daarom onmiddellijk van kracht in de EU-lidstaten.

Hoe groot de impact van de CRA daadwerkelijk zal zijn, hangt af van welke criteria er uiteindelijk worden toegepast voor het classificeren van de producten. Volgens de CRA mogen er alleen nog maar producten op de markt worden gebracht die een passend cyberveiligheidsniveau garanderen – en wel gedurende de gehele levenscyclus van een product. Security begint dus bij de productontwikkeling. Pilz stemt zijn ontwikkelingsprocessen daarom sinds enkele jaren ook af op de IEC 62443-4-1 “Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements” en heeft bijvoorbeeld de SecurityBridge aantoonbaar "secure" ontwikkeld.

((Tekens: 6.062))

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 hoofdkantoor in Ostfildern heeft op dit moment wereldwijd 2500 medewerkers in 42 dochterondernemingen en vestigingen in dienst.

De technologieleider biedt complete automatiseringsoplossingen voor Safety en Industrial Security op de machine aan. Deze omvatten sensoren alsmede besturings- en aandrijftechniek – inclusief systemen voor de industriële communicatie, diagnose en visualisering. Een internationaal dienstenaanbod met advies, engineering en trainingen completeert de portfolio. Oplossingen van Pilz worden niet alleen gebruikt in de machine- en installatiebouw, maar ook in heel veel andere branches zoals de intralogistiek, verpakkingsindustrie, spoorwegtechniek en robotica.

www.pilz.com

Pilz op sociale netwerken:

Op onze socialmediakanalen geven wij achtergrondinformatie over het bedrijf en de mensen bij Pilz en brengen wij nieuws op het gebied van automatiseringstechniek.

www.pilz.com/facebook
www.pilz.com/xing
www.pilz.com/youtube
www.pilz.com/linkedin

Contactpersoon voor de pers:

Martin Kurth

Bedrijfs- en vakpers
Tel.: +49 711 3409-158
m.kurth@pilz.de

Sabine Karrer

Vak- en bedrijfspers
Tel.: +49 711 3409-7009
s.skaletz-karrer@pilz.de

Jenny Skarman

Vakpers

Tel.: +49 711 3409-1067
j.skarman@pilz.de

Eva Gellner-Rössle

Vakpers

Tel.: +49 711 3409-7147
e.roessle@pilz.de