25.05.2023

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

http://www.pilz.com

Persbericht

Thomas Pilz: Veiligheid en beveiliging voor de digitale automation

Ostfildern, 25.05.2023 - **(Het gesproken woord geldt)**

Thomas Pilz

Security: Dit is wat de industrie en de machinebouw wettelijk te wachten staat

De normen en wetten voor de veiligheid in de industriële omgeving bevinden zich momenteel op een omslagpunt. Hiervoor zijn de thema's Security en Kunstmatige intelligentie (AI) verantwoordelijk. Voor de industrie in het algemeen en voor de machine- en installatiebouw in het bijzonder zijn drie nieuwe of toekomstige wettelijke voorschriften relevant voor het thema Security: de EU NIS 2-richtlijn, de nieuwe machineverordening en de Cyber Resilience Act.

Net als in de persconferentie van vorig jaar richt ik mij op het thema Security en wil ik u vandaag laten zien hoe ingrijpend de gevolgen voor de hele industrie zullen zijn.

NIS 2: meer verplichtingen en meer sancties voor meer bedrijven

NIS (Network and Information Security) is een richtlijn van de Europese Unie om de cyberveiligheid te versterken. Deze richtlijn is sinds 2016 van kracht en geldt tot nu toe voor aanbieders in de sector kritieke infrastructuur, waaronder energie, verkeer, banken en financiële instellingen, 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 opvolger is NIS 2, die begin 2023 in werking is getreden en door de EU-lidstaten in het najaar van 2024 in nationaal recht moet zijn omgezet. De richtlijn geldt nu ook binnen onder meer de machinebouw en de automotive-sector, en wel voor bedrijven met meer dan 50 werknemers of een jaaromzet van meer dan 10 miljoen euro. Volgens het VDMA (Duits verbond voor machine- en installatiebouw) betreft dit ongeveer 9.000 bedrijven in heel Europa. In de toekomst zullen deze bedrijven moeten bewijzen dat zij technische, operationele en organisatorische maatregelen treffen om zich tegen security-incidenten te beschermen. In de eerste plaats omvat dit de risicoanalyse van bestaande systemen, ook in productieomgevingen, dus de OT (Operations Technology). Dit wordt gevolgd door de ontwikkeling en uitvoering van specifieke processen en maatregelen, zoals wachtwoordbeveiliging of encryptie, en door verdere opleiding en training van werknemers. Cyberveiligheidsincidenten moeten binnen 24 uur aan de verantwoordelijke instanties worden gemeld. Ook de expliciete opname van toeleveringsketens is nieuw. Kortom, NIS 2 geldt nu voor meer bedrijven, breidt de verplichtingen uit en voorziet in strengere sancties. Bedrijven die geen actie ondernemen, riskeren zware sancties.

Cyber Resilience Act – Security voor de volledige productlevenscyclus

In september 2022 presenteerde de Europese Commissie een ontwerpverordening om de cyberveiligheid van producten te vergroten. Deze Cyber Resilience Act is gericht op fabrikanten van producten met digitale elementen. Dit betreft zowel hardware als software (zoals bijvoorbeeld firmware). De verordening geldt zowel voor consumentenproducten als voor producten voor industriële toepassingen, zoals machinebesturingen. Volgens de Cyber Resilience Act mogen voortaan alleen producten op de markt worden gebracht die een passend niveau van cyberveiligheid waarborgen. Voorts zijn fabrikanten verplicht om klanten zo snel mogelijk te informeren over zwakke plekken in de beveiliging en deze te elimineren. De verordening heeft dus betrekking op de volledige levenscyclus van een product. Dit betekent dat fabrikanten nu ook na de gebruikelijke garantieperiode software-updates moeten aanbieden om ook toekomstige bedreigingen af te weren. Wij gaan ervan uit dat de verordening eind 2024 in werking treedt.

De nieuwe Machineverordening – cybersecurity als plicht

De derde nieuwe wettelijke security-eis is de Machineverordening van de EU. De publicatie daarvan is aanstaande. Aangezien het om een verordening gaat, hoeft deze niet eerst in nationaal recht te worden omgezet. Machinefabrikanten hebben 42 maanden de tijd om aan de nieuwe eisen te voldoen. De Machineverordening komt in de plaats van de vorige Machinerichtlijn en stelt, anders dan zijn voorganger, cybersecurity verplicht. Waar de machinerichtlijn uitsluitend betrekking had op Safety, is in de verordening 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. Tot dusver is bekend dat naleving van de eisen van de Cyber Resilliance Act leidt tot een vermoeden van overeenstemming voor de Machineverordening.

En nu: wie moet waarvoor zorgen?
Welke betekenis hebben de wettelijke vereisten nu? Ik wil de samenhangen illustreren aan de hand van de energieopwekkingssector:
Tot dusver had de NIS-richtlijn alleen betrekking op de elektriciteitsleverancier. Met NIS 2 zullen in de toekomst ook constructeurs van machines, zoals de fabrikant van apparatuur voor energieopwekking (bijv. windturbines), aan de eisen moeten voldoen. De fabrikant van de windturbine vraagt op zijn beurt om automatiseringsoplossingen, besturingen of sensoren van bijvoorbeeld Pilz. Boven een bepaalde omvang vallen ook fabrikanten van elektrische componenten onder NIS 2. En aangezien NIS 2 ook bepaalt dat rekening moet worden gehouden met leveranciers, moet een bedrijf als Pilz ook zorgen voor veilige toeleveringsketens en eisen stellen aan zijn leveranciers. NIS 2 bestrijkt dus de volledige toeleveringsketen.

Al heel lang moeten machinefabrikanten de conformiteitsbeoordelingsprocedure doorlopen, uitmondend in de CE-markering, om machines in Europa te mogen invoeren.
Met de nieuwe Machineverordening moeten machinebouwers nu bewijzen dat hun machines ook beveiligd zijn tegen manipulatie. Ten slotte is de fabrikant van de elektrische componenten onderworpen aan de toekomstige eisen van de geplande Cyber Resilience Act.

Samengevat: of en in hoeverre een bedrijf zich met Security wil bezighouden, is niet langer iets dat het bedrijf naar eigen inzicht kan bepalen. Nee, het is een wettelijke verplichting! Bedrijven doen er goed aan zo snel mogelijk met NIS 2 aan de gang te gaan en een integrale Security-beoordeling voor het hele bedrijf uit te voeren. Dit omvat bijvoorbeeld het opzetten van een beheersysteem voor informatiebeveiliging (ISMS) met certificering volgens de informatiebeveiligingsnorm ISO 27001.

In de machinebouw is Security in de vorm van Industrial Security niet alleen een taak voor IT, maar een integraal onderdeel van het ontwerp en de constructie. Security achteraf implementeren kost altijd meer tijd en geld en betekent meestal een verlies aan gebruiksvriendelijkheid, functionaliteit en productiviteit. In de risicobeoordeling komt bij de Safety nu ook de Security. Geen Security zonder CE-markering!

Voor fabrikanten van producten met digitale elementen biedt de normenreeks IEC 62443 een goede richtlijn. De ondergeschikte norm IEC 62443-4-1 beschrijft bijvoorbeeld eisen voor een zogenaamd "Security Development Lifecycle Process".

De EU heeft het voortouw genomen op het gebied van Security-wetgeving en Europa krijgt de strengste regelgeving ter wereld. Maar er is al coördinatie met andere landen en ook daar zullen dergelijke wetten komen. Australië bijvoorbeeld is momenteel in de uitwisselingsfase met de EU en zal waarschijnlijk de Europese normen volgen. Daarom valt een wereldwijde harmonisatie van Industrial Security te verwachten.

Thomas Pilz

Open communicatiestandaarden als historische taak

Bij Pilz zijn openheid en gebruiksvriendelijkheid essentiële kenmerken van het portfolio. Wij willen de klant producten aanbieden die altijd zijn gebaseerd op de laatste stand van de techniek, eenvoudig in het onderhoud blijven en zich voegen naar elke automatiseringsarchitectuur.

Met SafetyBUS p, het eerste veilige veldbussysteem, en met het veilige realtime-ethernet SafetyNET p hebben wij de ontwikkeling van veilige industriële communicatie vormgegeven. Maar de tijd van bedrijfseigen oplossingen is voorbij. We stellen alles in het werk om industrienormen te creëren. Dit is een historische opgave!

OPC UA

Voor veilige, fabrikantoverstijgende netwerken voor industriële installaties heeft de industrie overeenstemming bereikt over OPC UA (Open Platform Communications Unified Architecture). Dit communicatieprotocol voorziet in een gestandaardiseerde (IEC 62541) communicatiepoort voor de communicatie tussen verschillende gegevensbronnen in de industrie. Als medeoprichter van de OPC Foundation zijn medewerkers van Pilz actief in zowel de stuurgroep als de technische werkgroepen van de Field Level Communication (FLC)-groep. De focus ligt voor Pilz daarbij op de werkgroepen, waarin het om het onderwerp Safety gaat (Safety over OPC UA).

Bijzonder waardevol is de knowhow over het gebruik van publisher/subscriber-technologie (pub/sub) in combinatie met de eisen van functioneel veilige veldbusprotocollen. Anders dan bij de klassieke master/slave-architectuur kunnen met pub/sub gegevens rechtstreeks tussen deelnemers worden uitgewisseld. Hierdoor kan OPC UA ook worden gebruikt voor veeleisende, gedistribueerde automatiseringstaken. Pilz heeft hier bijzondere expertise in, omdat ons SafetyNET p, het enige veilige, op ethernet gebaseerde veldbussysteem is dat van meet af aan pub/sub ondersteunt.

Wij maken goede vorderingen met onze werkzaamheden op het gebied van functionele veiligheid. Hand in hand met keuringsinstanties werkt de groep aan testspecificaties en testsystemen en aan de certificering van communicatiestacks voor OPC UA Safety. Versie 1.05 is reeds uitgebracht.

IO-Link Safety

Op sensorniveau is automatisering al een grote stap verder wat betreft openheid. Hier staat het communicatieprotocol IO-Link Safety op het punt commercieel beschikbaar te komen. De point-to-point communicatie biedt veel voordelen, waaronder vereenvoudiging van de installatie (bijv. door gestandaardiseerde bekabeling en het wegvallen van parallelle bedradingen), een geautomatiseerde en door tools ondersteunde parametrering en uitgebreide diagnosemogelijkheden.

Om IO-Link ook voor veiligheidsrelevante automatiseringstaken te kunnen gebruiken, heeft Pilz in het kader van de IO-Link Community intensief gewerkt aan de betreffende uitbreiding met de bijbehorende tests en certificeringen. Experts van Pilz leiden de twee IO-Link Safety-werkgroepen (voor marketing en techniek).

Op de SPS in november zullen wij de eerste sensoren presenteren die rijp zijn voor de markt. Pilz streeft ernaar een compleet systeem, d.w.z. sensoren, actuatoren en master-modules, aan te bieden. Dit vereenvoudigt de toepassing voor de klant en verhoogt de prestaties.

Wij zijn ervan overtuigd dat automatiseringsoplossingen zich in de toekomst nog sterker zullen onderscheiden door hun functionaliteiten: hoe goed zijn de gebruikersinterfaces, hoe eenvoudig de bediening, welke extra functies bieden ze? Hier is ruimte voor sterke innovatie en er zullen enorme mogelijkheden voor nieuwe toepassingen ontstaan.

Thomas Pilz

De toekomst van de veiligheid is dynamisch

Wat betekent verdere digitalisering voor de bescherming van mens en machine? Welke technologieën voldoen aan de veiligheidseisen? Welke rol speelt de mens? Vandaag willen we ook een blik op de toekomst werpen. Eerst het goede nieuws: de mens staat centraal. Zijn rol wordt zelfs versterkt.

De mens als actieve ontwerper

Bijvoorbeeld in het project "Fluid Production" van Arena 2036. Pilz werkt samen met partners aan de ontwikkeling en implementatie van een op de mens gericht, cyberfysiek productieconcept, met name voor de productie van auto's. Het idee van het project is om productie-installaties op te splitsen in modules die qua locatie flexibel zijn, om naar behoefte dynamische eenheden te kunnen vormen en ontbinden. De modules zijn ontworpen met een centrale focus op de rol van de mens als actieve vormgever van zijn productieomgeving.

Uit al deze eisen groeit de wens naar dynamische veiligheid, dus een meer flexibele aanpassing van de veiligheidsfuncties aan de veranderende productieprocessen en de daarmee verbonden veiligheidseisen. Hierdoor is het bijvoorbeeld mogelijk dat robots of mobiele platforms niet plompverloren moeten worden stopgezet wanneer een mens het werkgebied betreedt, maar dat ze met een gereduceerde (en daarmee minder gevaarlijke) snelheid verder kunnen werken of nog beter: veilige uitwijkstrategieën kunnen beheersen. Intelligente sensoren en actuatoren in gedistribueerde systemen zullen hierbij steeds vaker de functies van besturingen overnemen en tot een betere interactie van machinemodulen onderling en van mens en machine leiden.

Veiligheid in real time

De dynamische situaties in de toekomstige productieomgevingen moeten met het oog op de veiligheid in real time worden gecontroleerd en vrijgegeven, zodat de bescherming van mens en machine te allen tijde gewaarborgd blijft. Het kernbegrip hier is "veiligheid in real time". Het is denkbaar dat verschillende machines - of activa in het algemeen - in de toekomst veiligheidsvoorzieningen zullen delen. Dit is de "Shared Safety" die we in de SmartFactory KL testen. Een klassieke CE-markering als resultaat van een analoge conformiteitsbeoordelingsprocedure is bij een dergelijk begrip van veiligheid uitgesloten. Informatie over alle betrokken activa moet in runtime beschikbaar zijn. Trefwoorden zijn hier digitaal typeplaatje en management tray.

In het reeds genoemde project "Fluid Production" werken we aan andere toekomstige onderwerpen zoals de identificatie (en daarmee onderscheiding) van mensen en objecten. Hier komt het gebruik van kunstmatige intelligentie om de hoek kijken. Risico's kunnen dan worden herkend en beoordeeld door adaptieve AI-algoritmen. De "analoge" CE-markering is daarbij de basisbescherming. Maar er kunnen nog meer maatregelen worden ingevoerd om de risico's tot een minimum te beperken, de beveiliging nog flexibeler te maken en bij te dragen aan een hogere productiviteit.

Bijschrift:

Teksten en foto's kunnen ook gedownload worden op www.pilz.com. Om direct naar de relevante internetpagina's in het perscentrum te gaan, voert u de volgende webcode in in de zoekfunctie op de homepage.: **237512**

Pilz Groep

De Pilz Groep is een mondiale aanbieder van producten, systemen en diensten voor de automatiseringstechniek. Het familiebedrijf met zijn hoofdkantoor in Ostfildern heeft ongeveer 2.500 medewerkers in dienst. Met 42 dochterondernemingen en vestigingen creëert Pilz veiligheid voor mens, machine en milieu. De technologieleider biedt complete automatiseringsoplossingen die sensoren, besturings- en aandrijftechniek omvatten – inclusief systemen voor de industriële communicatie, diagnose en visualisering. Een internationaal dienstenaanbod met advies, engineering en trainingen completeert het portfolio. Oplossingen van Pilz worden behalve in de machine- en installatiebouw ook in talrijke branches zoals bijvoorbeeld windenergie en spoorwegtechniek en in de robotica toegepast.

www.pilz.com

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://twitter.com/Pilz_INT

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

https://www.xing.com/companies/pilzgmbh%26co.kg

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

Contactpersoon voor journalisten

Martin Kurth
Bedrijfs- en vakpers
+49 711 3409 - 158
publicrelations@pilz.com

Sabine Skaletz-Karrer
Vakpers
+49 711 3409 - 7009
s.skaletz-karrer@pilz.de