25.05.2023

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern
Tyskland
http://www.pilz.com

Pressmeddelande

Thomas Pilz: Safety och security för den digitala automationen

Ostfildern, 25.05.2023 - **(Det talade ordet gäller)**

Thomas Pilz

Security: Detta är vad lagen handlar om för industri och maskinteknik.

Standarder och lagar för säkerhet inom industrin genomgår just nu en radikal förändring. Denna förändrivs drivs framåt av security och artificiell intelligens (AI). För industrin i allmänhet och för maskin- och anläggningsteknik i synnerhet är tre nya eller kommande lagkrav relevanta när det kommer till security: EU-direktivet NIS 2, den nya maskinförordningen och Cyber Resilence Act.

Liksom vid den senaste årliga presskonferensen fokuserar jag på ämnet security och vill idag visa er hur omfattande effekterna blir för hela branschen.

NIS 2: Fler skyldigheter och sanktioner för fler företag

NIS (Network and Information Security) är ett EU-direktiv för att stärka cybersäkerheten. Direktivet har funnits sedan 2016 men har hittills gällt leverantörer inom området kritisk infrastruktur, bland annat energi, transport, bank och finans, hälsa, dricksvattensystem och digital infrastruktur. Leverantörer inom dessa sektorer har varit tvungna att vidta ”rimliga säkerhetsåtgärder” vad gäller på säkerhet och rapportera allvarliga cybersäkerhetsincidenter. Efterträdaren är NIS 2, som trädde i kraft i början av 2023 och måste införlivas i nationell lagstiftning av EU:s medlemsländer senast hösten 2024. Direktivet gäller nu även inom bland annat maskin- och fordonssektorn och för företag med fler än 50 anställda eller en årsomsättning på över 10 miljoner euro. Enligt VDMA påverkar detta cirka 9 000 företag i Europa. I framtiden kommer dessa företag att behöva bevisa att de vidtar tekniska, operativa och organisatoriska åtgärder som skydd mot security-incidenter. Detta omfattar initialt riskanalys av befintliga system, även i produktionsmiljöer, det vill säga OT (Operations Technology). Därefter följer utveckling och implementering av specifika processer och åtgärder som lösenordsskydd eller kryptering samt vidareutbildning och utbildning av anställda. Cybersäkerhetsincidenter måste rapporteras till berörda myndigheter inom 24 timmar. En annan nyhet är att leveranskedjorna uttryckligen tas med.

Sammanfattningsvis påverkar NIS 2 nu fler företag, utökar skyldigheterna och ger strängare sanktioner. Företag som underlåter att vidta åtgärder riskerar kännbara straff.

Cyber Resilence Act – security för produktens hela livscykel

I september 2022 presenterade EU-kommissionen ett utkast till förordning som syftar till att öka cybersäkerheten för produkter. Cyber Resilence Act riktar sig till tillverkare av produkter med digitala element. Detta omfattar både maskinvara och programvara (t.ex. fast program). Förordningen gäller både konsumentprodukter och produkter för industriella tillämpningar, såsom maskinstyrning. Enligt Cyber Resilence Act får endast produkter som garanterar en lämplig nivå av cybersäkerhet släppas på marknaden. Dessutom är tillverkare skyldiga att informera kunderna om säkerhetsluckor så snabbt som möjligt och att åtgärda dem. Förordningen påverkar därför hela livscykeln för en produkt. Detta innebär att tillverkare nu måste erbjuda programuppdateringar utöver den vanliga garantiperioden för att även avvärja framtida hot. Vi utgår från att förordningen antas i slutet av 2024.

Den nya maskinförordningen – obligatorisk cybersäkerhet

Det tredje nya security-kravet är EU:s maskinförordning. Den kommer publiceras snart. Eftersom det är en förordning behöver den inte införlivas i nationell lagstiftning. Maskintillverkarna har 42 månader på sig att uppfylla de nya kraven. Maskinförordningen ersätter det tidigare maskindirektivet och gör, till skillnad från dess föregångare, cybersäkerhet obligatorisk. Medan maskindirektivet enbart tog hänsyn till safety, ingår skyddsmål för security i förordningen under ”Protection against corruption” i ”Essential health and safety requirements EHSR”: Maskinens säkerhetsfunktioner får inte försämras genom oavsiktlig eller avsiktlig manipulering. Hittills är det känt att uppfyllandet av kraven i Cyber Resiliance Act leder till en presumtion om överensstämmelse för maskinförordningen.

Och nu: Vem ska ta hand om vad?
Vilken betydelse har lagkraven nu? Baserat på kraftproduktionssektorn skulle jag vilja presentera sambanden:
Hittills var det bara elleverantörer som berördes av NIS-direktivet. Med NIS 2 kommer även maskintillverkaren, som t.ex. tillverkare av kraftgenereringssystem (t.ex. vindkraftverk), i framtiden att behöva uppfylla kraven. Tillverkaren av vindkraftverket behöver i sin tur automationslösningar, styrningar eller sensorer, till exempel från Pilz. Över en viss storlek omfattas även tillverkare av elektriska komponenter av NIS 2. Och eftersom NIS 2 också ställer krav på att leverantörer ska beaktas måste ett företag som Pilz också säkerställa säkra leveranskedjor och ställa krav på sina leverantörer. NIS 2 täcker alltså hela leveranskedjan.

Maskinbyggare har alltid varit tvungna att gå igenom förfarandet för bedömning av överensstämmelse för att kunna importera maskiner till Europa och CE-märka dem. Med den nya maskinförordningen måste maskintillverkare nu bevisa att deras maskiner också är skyddade mot manipulation. Dessutom kommer tillverkaren av de elektriska komponenterna att omfattas av de framtida kraven i den planerade Cyber Resilence Act.

Sammanfattningsvis: Om och i vilken utsträckning ett företag vill syssla med security är inte längre någon bedömningsfråga för företaget. Nej, det är ett lagstadgat krav! Företag borde ta itu med NIS 2 så snart som möjligt och genomföra en holistisk security-bedömning för företaget. Detta innefattar till exempel utveckling av ett hanteringssystem för informationssäkerhet (ISMS) med certifiering enligt informationssäkerhetsstandarden ISO 27001.

Inom maskinteknik är security i form av industriell security inte bara en uppgift för IT, utan en integrerad del av utformningen och konstruktionen. Att implementera säkerhet i efterhand är alltid tidskrävande och innebär oftast förluster i användarvänlighet, funktionalitet och produktivitet. I riskbedömningen läggs nu security till safety. Utan security, ingen CE-märkning!

Standardserien IEC 62443 ger en bra orientering för tillverkare av produkter med digitala element. Till exempel beskriver den underordnade standarden IEC 62443-4-1 krav på en så kallad ”Security Development Lifecycle Process”.

EU har gått vidare med security-lagstiftningen och världens strängaste regler kommer att gälla i Europa. Men samordningen med andra länder är redan igång och liknande lagar kommer också att träda i kraft där. Australien har till exempel för närvarande kontakt med EU och kommer troligen att följa de europeiska standarderna. Vi kan därför förvänta oss en global harmonisering av industriell security.

Thomas Pilz

Öppna kommunikationsstandarder som en historisk uppgift

Hos Pilz är öppenhet och användarvänlighet en viktig del av utbudet. Vi vill erbjuda kunderna produkter som alltid motsvarar den aktuella tekniken, är lätta att hantera och passar i alla automationsarkitekturer.

Med SafetyBUS p, det första säkra fältbusssystemet, och med säker Ethernet SafetyNET p i realtid, formade vi utvecklingen av säker industriell kommunikation. Men tiden för egna företagslösningar är förbi. Vi gör allt som står i vår makt för att skapa industristandarder. Det är en historisk uppgift!

OPC UA

Avsedd för säker sammankoppling oavsett tillverkare i industrianläggningar är OPC UA (Open Platform Communications Unified Architecture). Kommunikationsprotokollet innehåller ett standardiserat (IEC 62541) gränssnitt för kommunikation mellan olika datakällor i industrin. Som medlem av OPC Foundation deltar medarbetare från Pilz såväl i styrkommittén som i tekniska arbetsgrupper för Field Level Communication-gruppen (FLC). Pilz fokuserar här på arbetsgruppen som arbetar med Safety (Safety over OPC UA).

Särskilt värdefullt här är vår know-how om användning av publisher/subscriber-tekniken (Pub/Sub) tillsammans med kraven på funktionssäkra fältbussprotokoll: I jämförelse med den klassiska master-/slave-arkitekturen kan med utbytas direkt med Pub/Sub-data mellan deltagare. Detta gör att OPC UA även kan användas för krävande, distribuerade automationsuppgifter. Här har Pilz särskild expertis, eftersom vår produkt SafetyNET p är det enda säkra Ethernet-baserade fältbussystemet som stöder Pub/Sub redan från början.

Vi gör goda framsteg i vårt arbete med funktionssäkerhet. Gruppen arbetar hand i hand med testmyndigheter om testspecifikationer och testsystem samt certifieringen av kommunikationsstackar för OPC UA Safety Version 1.05 har redan släppts.

IO-Link Safety
På sensornivå är automation redan ett stort steg längre vad gäller öppenhet. Här är kommunikationsprotokollet IO-Link Safety på väg att bli kommersiellt tillgängligt. Punkt-till-punkt-kommunikationen har flera fördelar, t.ex. förenklad installation (t.ex. genom standardiserad kabeldragning och inga parallellkabeldragningar), automatiserad och verktygsbaserad parametrering samt utökade diagnosmöjligheter.

För att även kunna använda IO-Link för säkerhetsrelaterade automationsuppgifter har Pilz arbetat intensivt inom IO-Link-communityt för att bygga ut tillhörande tester och certifieringar. Pilz-experter leder de två IO-Link Safety-arbetsgrupperna (för marknadsföring och teknik).

Vi kommer att presentera de första marknadsfärdiga sensorerna på SPS i november. Pilz strategi är att erbjuda ett komplett system, det vill säga sensorer, ställdon samt mastermoduler. Detta förenklar användningen för kunden och ökar prestandan.

Vi är övertygade om att framtidens automationslösningar kommer att utmärka sig genom sina funktioner: Hur bra är användargränssnitten, hur enkel är användningen, vilka ytterligare fördelar finns? Här finns mycket innovationskraft och stor potential för nya tillämpningar.

Thomas Pilz

Framtiden för säkerhet är dynamisk

Vad betyder digitaliseringen för skyddet för människa och maskin? Vilka tekniker uppfyller säkerhetskraven? Vilken roll har människan? Idag tar vi även en titt in i framtiden. Först de goda nyheterna: Människan står i centrum. Hennes roll blir även ännu större.

Människan som aktiv designer

Till exempel som i projektet ”Fluide Produktion” på Arena 2036. Pilz arbetar tillsammans med partner för att utveckla och implementera ett människocentrerat, cyberfysiskt produktionskoncept, särskilt för biltillverkning. Tanken bakom projektet är att bryta ned produktionsanläggningar i platsflexibla moduler så att dynamiska enheter kan formas och lösas upp igen vid behov. Modulerna är utformade med ett fokus på människans roll som aktiv designer av sin produktionsmiljö.

Från dessa krav uppkommer önskan om dynamisk säkerhet, det vill säga en mer flexibel anpassning av säkerhetsfunktionerna till de förändrade produktionsprocesserna och tillhörande skyddskrav. Mekanismerna tillåter t.ex. att robotar eller mobila plattformar inte måste nödstoppas när människor närmar sig arbetsområdet, utan kan arbeta vidare med reducerad (och därmed mindre farlig) hastighet och i framtiden även behärskar strategier för säkra undanmanövrar. Intelligenta sensorer och ställdon i fördelade system kommer i allt högre utsträckning att ta över styrsystemens funktioner och leda till en förbättrad växelverkan mellan maskinmoduler inbördes och mellan människa och maskiner.

Säkerhet i realtid
De dynamiska situationerna i framtida produktionsmiljöer ska kontrolleras och godkännas i realtid med hänsyn till säkerheten, så att skyddet av människa och maskin alltid kan garanteras. Slagordet är ”säkerhet i realtid”. Det är möjligt att olika maskiner – eller tillgångar i allmänhet – kommer att dela säkerhetsanordningar i framtiden. Det här är ”Shared Safety” som vi testar i SmartFactory KL. Med en sådan förståelse för säkerhet är en klassisk CE-märkning som ett resultat av ett analogt förfarande för bedömning av överensstämmelse uteslutet. Information om alla deltagande tillgångar måste finnas tillgänglig under körning. Nyckelorden här är den digitala typskylten och administrationsskalet.

I projektet ”Fluide Produktion” arbetar vi med andra framtidsämnen såsom identifiering (och därmed differentiering) av människor och föremål. Det är här användningen av artificiell intelligens kommer väl till pass. Risker kan sedan identifieras och bedömas med adaptiva AI-algoritmer. Den ”analoga” CE-märkningen är basskyddet. Men ytterligare åtgärder kan vidtas för att minimera risker, göra säkerheten ännu mer flexibel och bidra till mer produktivitet.

Bildtext:

Tekster og billeder kan også downloades på www.pilz.com. For at komme direkte til de relevante internetsider i Pressecenter, bedes du indgive følgende webkode på hjemmesiden. : **237512**

Pilz-koncernen

Pilz-koncernen är en global leverantör av produkter, system och tjänster för automationsteknik. Familjeföretaget med säte i Ostfildern har ca 2 500 medarbetare. Med 42 dotterbolag och filialer skapar Pilz säkerhet över hela världen för människor, maskiner och miljön. Som ledande aktör erbjuder vi kompletta automationslösningar med sensorteknik, styrteknik och driftteknik – inklusive system för industriell kommunikation, diagnostik och visualisering. Utbudet omfattar dessutom internationella tjänster för rådgivning, projektering och utbildningar. Pilz lösningar används förutom inom maskin- och anläggningskonstruktion även inom många andra branscher som t.ex. vindkraft, järnvägssystem och robotteknik.

www.pilz.com

Pilz på sociala nätverk

I våra kanaler på sociala medier finns mer information om företaget och personerna som jobbar på Pilz. Vi rapporterar även om den senaste utvecklingen inom automationstekniken.

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

Kontaktperson för journalister

Martin Kurth
Företags- och fackpress
+49 711 3409 - 158
publicrelations@pilz.com

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