Baggrundsinformation

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

Oktober 2025

Beskyttelse af virksomheder, maskiner og produkter

Safety og Industrial Security – Alt fra én og samme leverandør

Ostfildern, oktober 2025 – **Security-hændelser påvirker ikke længere kun IT-systemer, men i stigende grad også det omgivende produktionsmiljø (OT). Hændelser inden for Industrial Security omfatter ikke kun målrettede angreb, men også utilsigtede manipulationer. Opgaven for Industrial Security i produktionsmiljøer er at sikre maskiners og anlægs tilgængelighed samt maskindatas og maskinprocessers integritet og fortrolighed. Det højeste beskyttelsesmål er dog Functional Safety. For i sidste ende gælder følgende: Hvis virksomheder ikke har kontrol over deres data, er virksomheden og medarbejdernes sikkerhed i fare: Uden Security er der ingen Safety, og uden Safety er mennesket uden beskyttelse!**

I EU har man erkendt det stigende trusselsbillede, og lovgivningen er blevet tilpasset i overensstemmelse med dette: På virksomhedsniveau kræver **NIS 2-direktivet** foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i EU, f.eks. gennem et ledelsessystem for informationssikkerhed.

EU-maskinforordningen 2023/1230 indeholder nu bestemmelser om beskyttelse mod manipulation af maskiner og anlæg og kræver Industrial Security-foranstaltninger for de dele af maskinen, der påvirker Functional Safety.

Cyber Resilience Act (CRA) kræver Security-foranstaltninger for produkter med digitale elementer. Det omfatter også styringer, IO-systemer og andre komponenter, der anvendes i maskiner.

Virksomheder, maskiner og produkter – maskinproducenter og -driftsansvarlige står over for forskellige udfordringer og forskellige lovgivningsmæssige rammebetingelser på alle niveauer.

Topmoderne sikkerhed

Uafhængigt af, at lovgivningen har gjort Industrial Security obligatorisk, er der en række gode grunde til at beskæftige sig med emnet og søge rådgivning på et tidligt tidspunkt. Etablerede processer og betingelser for drift af maskiner kan fremme manipulation, hvis der ikke regelmæssigt sættes spørgsmålstegn ved dem. F.eks. betyder maskinernes lange levetid ofte, at de tilhørende systemer bliver gamle og på et tidspunkt ikke længere lever op til de nyeste standarder for Security. Disse systemer har huller i sikkerheden, som ikke længere kan lukkes, fordi leverandøren ikke længere tilbyder Security-opdateringer. Beskyttelse mod malware kan ofte heller ikke implementeres på slutmodulerne, fordi nogle af dem er for gamle, og deres ydeevne vil lide under det, hvilket kan føre til nedetid i produktionen.

Skridt for skridt til mere Industrial Security

I sidste ende er målet at sikre, at forretningsdriften forbliver beskyttet, men virksomheder skal overvinde forskellige udfordringer for at opnå dette: Det spænder fra at identificere de gældende lovkrav, finde og afhjælpe svage punkter i systemer, øge bevidstheden og uddanne medarbejdere til den efterfølgende implementering af kontroller. Eftersom Security er et såkaldt "moving target", er det også nødvendigt regelmæssigt at kontrollere maskinernes Industrial Security-status. Det er vigtigt at have klare ansvarsområder i virksomheden og en systematisk tilgang, der også omfatter opbygning af den nødvendige faglige viden.

Automatiseringsvirksomheden Pilz har indstillet sig på disse krav og opbygget en skræddersyet portefølje af serviceydelser til maskinproducenter og brugere på internationalt plan, som på helhedsorienteret vis omfatter alle aspekter af beskyttelsen af mennesker og maskiner. Eksperterne hos Pilz kender de aktuelle lov- og standardiseringskrav og inddrager dem i deres rådgivning. For at opbygge eller opdatere viden om Security i virksomheder suppleres tilbuddet med kurser. Den praktiske implementering sker også ved hjælp af produktløsninger fra Pilz, f.eks. tilbuddet om Identification and Access Management – I.A.M. for mere Safety og Industrial Security.

Skab det rette fundament

For at kunne sikre Industrial Security på deres egne maskiner har fagfolk inden for maskin- og anlægsfremstilling brug for velfunderet basisviden – især med hensyn til lovgivning og gældende standarder. Eksperterne fra Pilz videregiver denne knowhow på kurset "Principper for Industrial Security". Deltagerne lærer at forstå Security-trusler, passende beskyttelsesforanstaltninger og Best Practices i forbindelse med maskin- og netværkssikkerhed. Dermed lærer også nybegyndere inden for Security, hvilke foranstaltninger de kan bruge til effektivt at beskytte maskiner mod cyberangreb og manipulation på maskinelt produktionsniveau.

Med kvalifikationen til "CESA – Certified Expert for Security in Automation" tilbyder Pilz et todages ekspertkursus, der giver deltagerne indgående, aktuel viden om Security i overensstemmelse med de nyeste standarder, især med hensyn til standardserien IEC 62443 ("Industrielle kommunikationsnetværk – Netværks- og systemsikkerhed"). Derudover behandles praktiske foranstaltninger til risikonedsættelse, såsom adgangskontrol, øget sikkerhed for netværk

ved hjælp af tekniske midler samt organisatoriske foranstaltninger til reduktion af Security-risici. Deltagerne lærer, hvordan de kan anvende standarden korrekt og dokumentere, at deres automatiseringssystemer opfylder kravene til cybersikkerhed. Efter bestået eksamen modtager deltagerne det globalt anerkendte TÜV NORD-certifikat for "CESA - Certified Expert for Security in Automation".

Omsætning af teoretisk viden til praksis

Med udgangspunkt i de teoretiske principper og kurserne er det næste skridt i styrkelsen af Industrial Security at anvende strukturerede, praksisorienterede processer. Rådgivningen inden for Operational Technology (OT) skaber overgangen fra det teoretiske grundlag til implementerbare strategier. Ved hjælp af en trinvis fremgangsmåde identificeres svage punkter i komplekse systemer i forbindelse med Industrial Security Services, og der udvikles foranstaltninger til reduktion af risici. Resultatet er et altomfattende sikkerhedskoncept.

Fire trin, der giver mere Industrial Security

OT-Security-processen består af fire trin: analyse af beskyttelsesbehov, risikovurdering af Industrial Security, Industrial Security-koncept og verificering af Industrial Security-systemet.

I analysen af beskyttelsesbehovet finder virksomheden beskyttelsesbehovet for de enkelte "assets" i maskinen eller anlægget samt deres beskyttelsesmål. I det andet trin, risikovurderingen, overvejes alle risici og sandsynligheden for, at de indtræffer, for hvert delområde i systemets komplette livscyklus. Næste skridt er at skabe et detaljeret Industrial Security-koncept med strategier og foranstaltninger til forsvar mod og afbødning af risici

forårsaget af angreb, manipulationer og fejlbetjening. Der udarbejdes også politikker, regler og retningslinjer for systemets fortsatte sikre drift eller opbygning. I det sidste trin, Industrial-Security-System-verificeringen, kontrolleres de implementerede modforanstaltningers effektivitet.

Sikring af maskinens tilgængelighed

Processen med Industrial Security Services hjælper med at mildne eller forhindre cyberangreb. Antallet af utilsigtet udløste Security-hændelser falder også. Det øger maskinens tilgængelighed og sikrer i sidste ende omkostningsbesparelser og bevarelse af rentabiliteten.

Denne tilgang beskytter primært mennesker ved maskinen ved hjælp af passende Security-foranstaltninger. En Security-hændelse kan nemlig blive en hindring for Safety-foranstaltninger. F.eks. sikrer et lysgitter foran maskiner, at operatøren ikke træder ind i et farligt område. Men hvis en angriber er i stand til at påvirke den pågældende styring og mekanisme, kan lysgitterets beskyttende funktion ikke længere garanteres. Security beskytter Safety!

Ved selve implementeringen på maskinen giver det mening at tænke Safety og Security sammen. For uden Security ingen Safety, og uden Safety er mennesket uden beskyttelse.

Tydelig regulering: Hvem må gøre hvad på maskinen?

En maskines og dens operatørers sikkerhed står og falder med regulering af adgangen – uanset om det er for mennesker eller netværk. Adgangspunkter skal sikres mod uautoriseret adgang, så der f.eks. ikke opholder sig personer i farezonen, når maskinen er i drift. For ellers kan selv velment betjening eller vedligeholdelse af et anlæg – uanset om det er på stedet eller via et netværk – få fatale konsekvenser.

En vigtig komponent er Identification and Access Management (I.A.M.), som tydeligt regulerer autorisationer og adgang til maskiner og anlæg i en virksomhed. Hertil hører organisatoriske foranstaltninger og specifikationer samt passende sikkerhedsfunktioner. Et adgangsautorisationssystem som PITreader fra Pilz er her det passende produktmodul. Det gør det muligt for brugerne at opfylde kravene til beskyttelse af medarbejderne, beskyttelse mod erstatningsansvar, maksimal produktivitet og databeskyttelse.

Kun en helhedsorienteret tilgang til Safety og Security garanterer omfattende beskyttelse af mennesker og maskiner. Om og i hvilket omfang en virksomhed ønsker at beskæftige sig med Security, afgøres ikke længere af virksomheden. Det er nu et lovkrav. Inden for maskinproduktion er Security i form af Industrial Security ikke blot en opgave for IT, men en integreret del af designet og konstruktionen. Det kræver meget arbejde at implementere Security efterfølgende, og det betyder som regel mindre brugervenlighed, funktionalitet og produktivitet.

((Tegn: 9.784))

((Boks:))

Oversigt over EU-lovgivningen i forbindelse med Industrial Security:

Især i Europa reagerer lovgiverne på trusselsituationen med en række love. Det betyder, at Europa har de strengeste regler i verden. Men koordineringen er allerede i gang med andre lande, hvor

sådanne love også vil blive indført. Der må derfor forventes en global harmonisering af Industrial Security.

NIS 2: Flere pligter for virksomheder

NIS (Net- og InformationsSikkerhed) er et EU-direktiv, der skal styrke cybersikkerheden. Dette direktiv har eksisteret siden 2016 og har indtil videre været gældende for udbydere inden for kritiske infrastrukturer, herunder energi, transport, bank- og finanssektoren, sundhed, drikkevandsforsyning og -distribution samt digital infrastruktur. Udbydere i disse sektorer skulle træffe "passende sikkerhedsforanstaltninger" med hensyn til Security og indberette alvorlige cybersikkerhedshændelser. Det nye NIS 2-direktiv ((EU) 2022/2555 ... om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen) kræver, at betydeligt flere virksomheder træffer foranstaltninger til styring af cybersikkerhedsrisici i fremtiden. NIS 2 udvider sektorerne til f.eks. at omfatte fremstillings-/produktionsindustrien, herunder maskinproduktion og producenter af elektrisk udstyr.

Der kræves risikoanalyser og sikkerhedskoncepter for informationssystemer, beskyttelse af leveringskæden og personalets sikkerhed. Det omfatter også koncepter for adgangskontrol og anlægsadministration samt obligatoriske kurser for ledelsen.

Direktivet blev vedtaget af Europa-Parlamentet og Det Europæiske Råd i slutningen af 2022. Som alle EU-direktiver er NIS 2 ikke direkte gældende og bindende i de enkelte EU-medlemslande, men skal implementeres af medlemslandene i deres nationale lovgivning. Virksomheder gør klogt i at beskæftige sig med NIS 2 hurtigst muligt og foretage en omfattende Security-vurdering af virksomheden. Hertil hører f.eks. etablering af et ledelsessystem for informationssikkerhed (ISMS). Certificering i overensstemmelse med

informationssikkerhedsstandarden ISO 27001 er nyttig i denne sammenhæng.

NIS 2 med vindmøller som eksempel: Med NIS 2 skal maskinproducenter, som f.eks. en producent af anlæg til elproduktion (f.eks. vindmøller), i fremtiden også overholde kravene. Producenten af vindmøllen har til gengæld brug for automatiseringsløsninger, styringer eller sensorer. Over en vis størrelse er producenter af elektriske komponenter også omfattet af NIS 2. Og eftersom NIS 2 også foreskriver, at der skal tages hensyn til leverandørerne, skal en virksomhed som Pilz også sørge for sikre leveringskæder og stille krav til sine leverandører. NIS 2 omfatter således den komplette leveringskæde.

Den nye maskinforordning: Ingen CE-mærkning uden Security

I forbindelse med maskiners Functional Safety spiller maskindirektivet 2006/42/EF en særlig rolle.

Maskinproducenter har altid skullet gennemgå en passende overensstemmelsesvurderingsprocedure for at kunne importere maskiner til Europa. Slutningen på denne procedure er CE-mærkningen.

Offentliggjort i juni 2023 som den nye maskinforordning er kravene bragt op på det aktuelle, tekniske niveau. Eftersom det er en forordning, skal den ikke først omsættes til national lovgivning. Maskinproducenter har indtil 20. januar 2027 til at omstille sig til de nye krav og opfylde dem fra skæringsdatoen.

Maskinforordningen erstatter det tidligere maskindirektiv og gør i modsætning til sin forgænger cybersecurity obligatorisk. Mens maskindirektivet udelukkende drejede sig om Safety, er

beskyttelsesmålet Security medtaget i forordningen under "Protection against corruption" i "Essential health and safety requirements (EHSR)": Maskinens sikkerhedsfunktioner må ikke forringes ved utilsigtet eller forsætlig forfalskning.

Denne nye vej til CE-mærkning rejser en række nye spørgsmål for maskinproducenter og -driftsansvarlige, da de bliver nødt til at revidere deres eksisterende koncepter for Safety og Security.

Cyber Resilience Act: Security i hele produktets livscyklus

Ud over en betragtning af virksomheden og maskinerne er det også absolut nødvendigt at implementere Security-foranstaltninger direkte i modulerne (f.eks. styringer). I september 2022 fremlagde Europa-Kommissionen et udkast til en forordning, der har til formål at øge produkters cybersikkerhed. Denne Cyber Resilience Act (CRA) er rettet mod producenter af produkter med digitale elementer (hard- og software), som er i stand til at kommunikere med andre produkter. Det påvirker produkter fra både B2C-sektoren, som smartphones eller robotstøvsugere, og B2B-sektoren, som styringer og sensorer, samt rene softwareprodukter som operativsystemer eller selve maskinen.

Producenternes forpligtelse til at rapportere udnyttede svage punkter gælder fra 11.09.2026. Produkter med digitale elementer skal opfylde kravene i CRA fra 11.12.2027 for at måtte blive tilgængelige på markedet i EU. CRA er en EU-forordning og vil derfor være direkte gældende i EU's medlemslande

Hvor store konsekvenserne på grund af CRA rent faktisk vil være, afhænger af, hvilke kriterier der i sidste ende fastlægges for at klassificere produkterne. I henhold til CRA må man kun markedsføre produkter, der garanterer et passende cybersikkerhedsniveau – og

det gælder i et produkts komplette livscyklus. Security begynder altså under produktudviklingen. Pilz har derfor allerede i nogle år tilpasset sine udviklingsprocesser til IEC 62443-4-1 "Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements" og har f.eks. udviklet SecurityBridge, så den er dokumenteret "secure".

((Tegn: 6.062))

Pilz – The Spirit of Safety

Pilz er en global udbyder af produkter, systemer og serviceydelser til automatiseringsteknik. Som pioner inden for sikker automatisering skaber Pilz sikkerhed for mennesker, maskiner og miljø. Familievirksomheden, der blev grundlagt i 1948, har i dag hovedkvarter i Ostfildern ved Stuttgart og er repræsenteret over hele verden med 2.500 medarbejdere i 42 datterselskaber og filialer.

Den teknologisk førende virksomhed tilbyder automatiseringsløsninger til Safety og Industrial Security på maskiner. Disse løsninger omfatter sensorteknologi, styringsteknik og drevteknik – inklusive systemer til industriel kommunikation, diagnose og visualisering. Porteføljen afrundes af et internationalt program af serviceydelser med rådgivning, udvikling og kurser. Løsninger fra Pilz anvendes ikke kun inden for maskin- og anlægsproduktion, men også inden for mange andre brancher, som f.eks. intralogistik, emballage, jernbaneteknik og robotteknologi.

www.pilz.com

Pilz på sociale medier:

På vores social media-kanaler giver vi baggrundsinformationer om virksomheden og menneskene hos Pilz samt aktuel information i forbindelse med automatiseringsteknik.

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

Kontaktpersoner for pressen:

Martin Kurth

Erhvervs- og fagpresse
Tlf.: +49 711 3409-158
m.kurth@pilz.de

Sabine Karrer

Fag- og erhvervspresse
Tlf.: +49 711 3409-7009
s.skaletz-karrer@pilz.de

Jenny Skarman

Fagpresse

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

Eva Gellner-Rössle

Fagpresse

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