Baggrundsinformation

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

16. maj 2024

Beskyttelse af virksomheder, maskiner og produkter

Safety og Industrial Security – Alt fra én og samme leverandør

Ostfildern, 16. maj 2024 – **Security-hændelser påvirker ikke længere kun IT-systemer, men i stigende grad også produktionsmiljøet (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. Følgende gør sig gældende: Hvis virksomheden ikke har kontrol over sine data, er den og dens medarbejderes sikkerhed på spil: Uden Security ingen Safety, og uden Safety er mennesket uden beskyttelse!**

I EU har lovgiverne reageret på den skærpede trusselsituation: På virksomhedsniveau kræver **netværks- og informationssikkerhedsdirektivet NIS 2** implementering af et altomfattende styringssystem for informationssikkerhed.

Den **nye maskinforordning 2023/1230** indeholder nu bestemmelser om beskyttelse mod manipulation af maskiner og systemer og kræver sikkerhedsforanstaltninger 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.

Uafhængigt af, at lovgiverne har gjort Industrial Security obligatorisk, er der en række gode grunde til at beskæftige sig med emnet og søge rådgivning på et tidligt tidspunkt. Det skyldes, at mange processer og forhold for drift af maskiner begunstiger manipulation og derfor hurtigst muligt bør tages op til revision og ændres. 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.

Omfattende program af serviceydelser fra Pilz

I sidste ende er målet at sikre, at forretningsdriften forbliver beskyttet, men virksomhederne er nødt til at overvinde forskellige udfordringer for at opnå dette: Det spænder fra at identificere de gældende lovkrav, genkende og eliminere svagheder i systemerne, øge bevidstheden og uddanne medarbejderne til den efterfølgende implementering af kontroller. Da sikkerhed er et "mål i bevægelse", er det også nødvendigt regelmæssigt at kontrollere maskinernes Industrial Security-status.

Automatiseringsvirksomheden Pilz har tilpasset sig disse krav og opbygget et internationalt program af serviceydelser til maskinproducenter og brugere, som på en altomfattende måde inddrager alle aspekter til beskyttelse af mennesker og maskiner.

Tilbuddet spænder fra grundlæggende information og orienteringshjælp samt kurser til Industrial Security Consulting Service (ISCS), hvor konkrete projekter implementeres.

Med kvalificeringen til "CESA – Certified Expert for Security in Automation" tilbød Pilz allerede sidste år et todages ekspertkursus, der giver deltagerne kompakt Security-viden om den aktuelle situation inden for standarder. 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. Når prøven er bestået, får deltagerne det globalt anerkendte TÜV NORD-certifikat som "CESA – Certified Expert for Security in Automation".

Med det nye servicetilbud Industrial Security Consulting Service (ISCS) udvider Pilz det sikkerhedsrelaterede syn på maskiner til et altomfattende syn på Safety og Security. På grundlag af den gennemprøvede metodik for serviceydelser inden for funktionel maskinsikkerhed og Security-standardserien IEC 62443 har Pilz udviklet en række serviceydelser, som efter implementering sikrer, at virksomheder er godt rustet til Industrial Security og opfylder de gældende lovkrav.

Fire moduler, der giver mere Industrial Security

ISCS består af følgende fire moduler: Analyse af beskyttelsesbehovet, Industrial-Security-risikovurdering, Industrial-Security-koncept og Industrial-Security-systemverificering.

Ved analysen af beskyttelsesbehovet fastlægger Pilz' eksperter virksomhedens beskyttelsesbehov for de enkelte "aktiver" i maskinen eller anlægget og deres beskyttelsesmål. I det andet trin, risikovurderingen, overvejes alle risici og sandsynligheden for, at de

indtræffer, for hvert delområde i systemets komplette livscyklus. Eksperterne fra Pilz diskuterer derefter mulige løsninger med kunden for at afbøde de identificerede risici og mulige farer.

I det tredje trin udarbejder Pilz' eksperter et Industrial Security-koncept med strategier og foranstaltninger til forsvar mod og afbødning af risici, der skyldes angreb, manipulationer og betjeningsfejl. 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

Industrial Security Consulting Service hjælper med at afbøde 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.

Frem for alt sikrer ISCS, at mennesker ved maskinen er beskyttet med 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 en farezone. 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!

Maskinproducenter og brugere får dermed et program af serviceydelser fra Pilz, der tager hensyn til alle aspekter af beskyttelsen af mennesker og maskiner.

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.

Klare regler: 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. Hvis en autoriseret maskinoperatør befinder sig i denne farezone i forbindelse med vedligeholdelse, skal det sikres, at ingen andre personer har adgang til systemet på samme tid. For ellers kan selv velment betjening eller vedligeholdelse af et system – uanset om det er på stedet eller via et netværk – få fatale konsekvenser.

En vigtig komponent er et 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 medarbejderbeskyttelse, beskyttelse mod erstatningsansvar, maksimal produktivitet og databeskyttelse.

Med driftsvalgs- og adgangsautorisationssystemet PITmode fusion tilbyder Pilz det funktionsmæssigt sikre driftsvalg samt regulering af adgangsautorisationer til maskiner og anlæg. Hver operatør modtager de maskinautorisationer, der svarer til deres ansvar og kvalifikationer, på en RFID-kodet transponder. Anlægget kan derfor kun betjenes og styres af autoriserede personer i definerede driftstilstande. Det giver en høj grad af beskyttelse mod utilsigtede handlinger og manipulation.

Når systemet til valg af driftstilstand og adgangsautorisation suppleres med komponenterne i et modulopbygget beskyttelsesdørssystem, skabes der et sammenhængende

adgangskoncept til maskinen – ud fra Safety- og Security-synspunkter.

Selv den bedste sikring med beskyttelsesdøre nytter ikke noget, hvis data, knowhow og driftsprocesser ikke er tilstrækkeligt sikret mod uvedkommende adgang og manipulation, og en angriber udefra kan trænge ind i styringssystemet.

Industrial Firewall beskytter mod adgang udefra

Industrial Firewall SecurityBridge fra Pilz har til opgave at sikre automatiseringsnetværk mod adgang udefra. Den overvåger datatrafikken mellem pc og styring og reducerer dermed angrebsfladen for hackerangreb og manipulation. SecurityBridge beskytter ikke kun styringer fra Pilz mod manipulationer, men også styringer fra andre leverandører.

Pilz er overbevist om, at man kun kan garantere omfattende beskyttelse af mennesker og maskiner ved at se på Safety og Security som en helhed. 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: 10.173))

((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 med andre lande er allerede i gang, 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 netværks- og informationssikkerhedsdirektiv 2 EU 2022/2555 (NIS 2) vil kræve, at betydeligt flere virksomheder i fremtiden træffer risikostyringsforanstaltninger for cybersikkerhed. 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 andre EU-direktiver er NIS 2 ikke direkte gældende og bindende i de enkelte EU-lande, men skal

omsættes til national lovgivning af medlemslandene. EU's medlemslande skal omsætte direktivet til national lovgivning senest 18.10.2024. 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 20.01.2027 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 gennem 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.

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: 5.826))

Billeder

Billede 1

Grafik_aus_Prospekt_Schulungen_mit_Pilz_3c_ppt

Safety og Security fra en og samme producent: Pilz tilbyder et omfattende udvalg af løsninger med serviceydelser og produkter til Industrial Security på maskiner.

Billede 2:

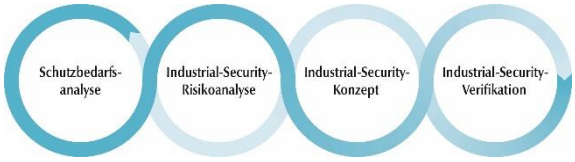
F_Services_ISCS_two_men_tablet_in_discussion_get1150297892_cold1_v0

Pilz lancerer serviceydelsen Industrial Security Consulting Service og hjælper virksomheder med at sikre deres maskiner og anlæg.

Copyright: © Westend61/[westend61] via Getty Images),© Pilz GmbH & Co. KG

Billede 3:

G_Cycle_Industrial_Security_de_v0



Servicetilbuddet Industrial Security Consulting Service fra Pilz består af fire moduler: Analyse af beskyttelsesbehovet, Industrial-Security-risikovurdering, Industrial-Security-koncept og Industrial-Security-systemverificering.

Copyright: Pilz GmbH & Co. KG

Billede 4:

F_Press_IAM_Man_using_PITreader_Key_Get1169337234_Get1169337153_cold1_v2

Omfattende Identification and Access Management regulerer adgangen til applikationen og sørger dermed for sikkerhedsfunktioners og -foranstaltningers integritet – inklusive Safety og Industrial Security.

Billede 5:

F_security_robot_man_virtual_world_Fot208731449_cold1_2019_06_v2

Industrial Security omhandler beskyttelse af produktions- og industrianlæg mod tilsigtet eller utilsigtet fremkaldte fejl. Målet er at sikre maskiners og anlægs tilgængelighed samt maskindatas og maskinprocessers integritet og fortrolighed.

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 i sociale netværk:

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/X
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

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

Hansjörg Sperling-Wohlgemuth
Kongres- og foredragsadministration
Tlf.: +49 711 3409-239
h.sperling@pilz.de