

"Zones and Conduits" i automatiseringsnetværk: Security beskytter safety

Safety har højeste prioritet

Ostfildern, juli 2026 – **Maskinforordningens bestemmelser gør det obligatorisk: Industrial security skal beskytte sikkerhedsrelevante funktioner mod manipulation – altså security som en forudsætning for fungerende safety. Men hvordan sikres et automatiseringsnetværk på en helhedsorienteret måde? Standarder som IEC 62443-3-2 og den kommende EN 50742 angiver retningslinjer: Opdel systemer i zoner, kontroller forbindelserne – et princip, der går igen i de aktuelle anbefalinger fra brancheorganisationer og eksperter. Pilz er overbevist om, at en konsekvent adskillelse af safety og såkaldt standardautomatisering er nøglen til effektiv maskinsikkerhed – baseret på princippet "Defence-in-Depth" og implementeret gennem "Zones and Conduits"-tilgangen.**

Et hus kan være bygget solidt og sikkert med stabile vægge, brandsikre materialer, pålidelige elinstallationer og velfungerende alarmanlæg. Denne konstruktionsmæssige sikkerhed er et godt eksempel på safety ved maskiner, hvor konstruktionsmæssige foranstaltninger, sensorer og beskyttelsesmekanismer skal forhindre utilsigtede farer. Et sådant hus forbliver dog kun sikkert, hvis et ikke udsættes for målrettet indtrængen. Manipulerede varmestyringer, saboterede strømkredse eller deaktiverede alarmsystemer kan gøre en bygning, der er konstrueret efter alle sikkerhedsmæssige standarder, til en risiko. Selv inden for maskinverdenen mister selv den bedste sikkerhedsmæssige konstruktion sin virkning, hvis

sikkerhedsrelevante komponenter uautoriseret påvirkes eller sættes ud af funktion.

Security spiller i denne sammenhæng rollen som den ydre beskyttelse: robuste døre, sikrede indgange, overvågede forbindelser og barrierer mod uønsket indtrængen. Security beskytter altså ikke mod selve ulykkerne, men mod at sikkerhedsmekanismerne sættes ud af kraft – for eksempel af personer, der får adgang ved at vælge en uautoriseret driftsform eller ved uautoriserede handlinger. Kun på den måde kan safety forblive pålidelig – security for safety.

Fra de normative krav til løsningsforslaget

Med Maskinforordning (EU) 2023/1230 bliver security for første gang en obligatorisk forudsætning for, at safety-funktionerne på maskiner og anlæg fungerer korrekt: Sikkerhedsfunktionerne må ikke kompromitteres hverken ved bevidst eller utilsigtet manipulation. Det er netop dette, som den nye standard EN 50742 tager udgangspunkt i, og den vil bidrage til at konkretisere de grundlæggende security-krav i Maskinforordningens rammer. Standarden fastlægger tekniske data vedrørende beskyttelse mod korruption og stiller klare krav til hardware, software og data, der kan påvirke sikkerhedsrelevante funktioner. Standarden dækker hele livscyklussen – fra udvikling over drift til driftsophør. En central rolle spiller desuden den eksisterende standardserie IEC 62443, som beskriver systematisk cybersikkerhed for industrielle automatiserings- og styresystemer. Den udgør en struktureret ramme for risikoanalyser, "Defence-in-Depth" samt princippet om segmentering ("Zones and Conduits") og anerkendes udtrykkeligt i EN 50742 som en alternativ eller supplerende tilgang til sikkerhedsforanstaltninger. Tilsammen udgør disse standarder den normative kerne i Security for Safety: De kræver, at en maskines

digitale integritet betragtes som en forudsætning for Functional Safety og beskyttes i overensstemmelse hermed.

Hvorfor "Zones and Conduits" øger sikkerheden for maskinerne

Tilbage til billedet af huset: Fyrrummet repræsenterer en zone, mens forbindelsen til Smart Home-gatewayen repræsenterer den tilhørende forbindelsesvej. Hvis denne forbindelse manipuleres, kan det påvirke hele anlægget – selvom rummet er perfekt beskyttet. Det afgørende er derfor ikke kun sikkerheden i de enkelte områder, men også sikkerheden på de veje, der danner forbindelsen mellem dem. Det er netop her, princippet om "zoner og kanaler" kommer ind i billedet. Områderne adskilles tydeligt fra hinanden, og overgangene mellem dem udformes på en kontrolleret måde. Ligesom i et hus, hvor døre og tildelte nøgler bestemmer, hvem der har adgang hvorhen, går indre sikkerhed (safety) og ydre beskyttelse mod manipulation (security) i et industrialanlæg struktureret hånd i hånd.

Dette skaber et sikkerhedskoncept, der følger princippet om "Defence-in-Depth": Sikkerheden opnås ikke gennem en enkelt barriere, men gennem flere beskyttelseslag, der er placeret efter hinanden. Når et niveau er overvundet, holder det næste stand. Zoner udgør disse trinvis opdelte rum, mens kanaler udgør de kontrollerede gennemgange mellem dem. På denne måde undgår man, at et enkelt svagt punkt udgør en risiko for hele systemet – især når det drejer sig om safety og dermed beskyttelse af mennesker.

Pilz følger konsekvent denne tilgang under betegnelsen "Security for Safety", hvor safety er det overordnede mål for security. I centrum står beskyttelsen af safety, som igen beskytter mennesker. Derfor adskiller Pilz' safety sig fra den generelle maskinstyring, den såkaldte standardautomatisering, og mindsker dermed risikoen for

sikkerhedsrelevante funktioner. Jo tydeligere disse "skatte" adskilles funktionelt, desto færre ekstra sikkerhedsforanstaltninger er der behov for at beskytte dem pålideligt.

Fordelene ved denne tilgang kommer til udtryk gennem hele maskinernes levetid. Hvis safety og standardfunktioner adskilles, er det ikke nødvendigt at recertificere eller tilpasse safety-funktionerne sideløbende med en opdatering af standardfunktionerne, hvilket reducerer vedligeholdelses- og servicearbejdet betydeligt. Klassiske sikkerhedscontrollere kræver desuden langt sjældnere sikkerhedskritiske opdateringer end standardcontrollere, hvilket betyder, at adskillelsen eliminerer mange unødvendige indgreb. Også teknologisk set giver adskillelsen fordele: Et selvstændigt safety-system som den sikre lille styring PNOZmulti 2 kan frit kombineres med forskellige styresystemproducenter, mens integrerede systemer ofte er bunde til specifikke teknologier. Samtidigt gør separate safety-løsninger det sværere for angribere, da separate systemer skal kompromitteres hver for sig, hvilket gør manipulation betydeligt vanskeligere. Derudover kan et standardsystem være online, når det er nødvendigt, mens de egentlige safety-funktioner forbliver isolerede, hvilket reducerer dets angrebsflader drastisk.

Desuden øger denne adskillelse af safety- og security-automation – med optimalt tilpassede Security-niveauer – effektiviteten takket være bedre planlægning af sikkerheds-, vedligeholdelses- og udvidelsesforanstaltninger. Ændringer i standardprogrammet kræver således ingen indgreb i den sikkerhedsrelevante del, hvilket reducerer omfanget af programmerings- og tilpasningsarbejdet betydeligt. Samtidigt har opdelingen en positiv virkning på udgifterne til software og support, da der ofte er lavere licens- og servicegebyrer i separate systemer.

Beskyttelse gennem adskillelse – kompetence gennem oplæring

Den klare adskillelse mellem safety og standardautomatisering sikrer ikke blot teknisk robusthed, men også færre betjeningsfejl og mindre behov for oplæring. Da sikkerhedsrelevante funktioner kører på egen hardware og er klart afgrænset organisatorisk, forbliver de beskyttede, selv hvis der foretages ændringer i standardprogrammet. Fejl i den daglige drift udgør derfor ikke en safety-risiko, og ansvarsfordelingen bliver mere overskuelig.

For at hjælpe virksomheder med at implementere denne arkitektur tilbyder Pilz et omfattende uddannelses- og serviceprogram. Dette omfatter kurserne "Grundlag for Industrial Security" og "CESA – Certified Expert for Security in Automation" samt Industrial Security Services. De viser ikke blot, hvordan man ud fra de enkelte moduler kan udvikle robuste Security for Safety-koncepter, men går langt videre end det: De viser, hvordan security-risici kan styres systematisk, og hvordan helhedsorienterede sikkerhedskoncepter udvikles, hvordan kravene i IEC 62443 kan indordnes, hvordan arkitekturen i et sikkert maskinnetværk opbygges, og hvordan effektiviteten af de trufne foranstaltninger kan vurderes og løbende forbedres.

En afgørende fordel ved denne tilgang er, at slutbrugerens driftspersonale ikke behøver at sætte sig ind i security-spørgsmål i dybden, da der er en garanti for, at safety-funktionerne bliver beskyttet gennem den arkitektoniske udformning. Kurserne henvender sig derfor primært til dem, der træffer beslutninger om security eller udformer systemer – samtidig med at operatørerne fortsat kan arbejde sikkert uden behov for yderligere uddannelse inden for området Industrial Security. Dette resulterer i en praktisk

rollefordeling, der forenkler driften af anlægget og samtidig øger sikkerhedsniveauet på lang sigt.

Større sikkerhed takket være en klar struktur – og den rette ekspertise

En effektiv "Security for Safety"-strategi opstår ikke gennem enkeltstående tiltag, men gennem en gennemtænkt arkitektur, klare ansvarsforhold og målrettet kompetenceudvikling. Det er netop her, Pilz kommer ind i billedet. Med et konsekvent fokus på "Defence in Depth" og en klar adskillelse mellem safety og standardautomatisering skaber Pilz grundlaget for robuste maskiner – og supplerer dette med praktisk orienteret uddannelse og rådgivning, så virksomhederne trygt kan følge denne vej. På den måde opnås et sikkerhedsniveau, der ikke blot opfylder standardkravene, men også giver en mærkbar merværdi i den daglige drift: enklere, mere robust og med varig effekt.

((Tegn: 9.640))

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