AS-INTERFACE MASTER **NEWS**
Digital magazine by Bihl+Wiedemann 02/2024

Safety og security for (fremtids-)sikker automatisering

ASi-5 Safety og ASi Safety at Work – begge med mulighed for at sende standardsignaler på samme linje – plus et bredt udvalg af gateways og moduler til realisering af en lang række sikkerhedsløsninger uanset branche og styresystem, samt Safe Link til PLC-fri, sikker kobling og netværksdannelse af ASi-netværk: Den omfattende portefølje dokumenterer Bihl+Wiedemanns ekspertise inden for funktionel sikkerhedsteknologi. Men med digitaliseringen af maskin- og anlægskonstruktion er safety uden security – dvs. uden beskyttelse mod cyberangreb – næsten utænkelig. Ikke engang for automationsspecialisterne fra Mannheim.

Funktionel sikkerhed – safety –har til formål at beskytte mennesker og miljø mod ulykker, der kan forårsages af maskiner. Data- og kommunikationssikkerhed – security – står for overvågning af OT-strukturer og IT-netværk samt potentielle gateways for pålideligt at eliminere farerne ved datamanipulation eller -tyveri. Da den funktionelle sikkerhed bliver mere og mere digital, kan safety-løsninger, der ikke tager højde for security-risici, blive udsat for eksterne ændringer – ændringer, der kan forringe eller endda eliminere deres beskyttende funktion.

I tilfælde af udskiftning kan den hardware- og safety-konfiguration, der er gemt på SD-kortet, samt de tilsluttede enheders parameterdata overføres fuldstændigt til en ny gateway af samme type.

Security: Skærpet betydning i lovgivningen

Det er derfor ikke tilfældigt, at f.eks. EU's maskinforordning 2023/1230, som erstatter maskindirektivet 2006/42/EF den 20. januar 2027, foreskriver, at maskiner skal konstrueres og fremstilles på en sådan måde, at hverken en tilsluttet enhed i sig selv eller en ekstern enhed, der kommunikerer med maskinen, kan føre til en farlig situation.

Det gælder både hardware og software, både når maskinen bruges efter hensigten og i tilfælde af mulig manipulation. Forbindelse til eller kommunikation via fjernadgangsenheder som f.eks. routere må heller ikke føre til farlige situationer. EU's Cyber Resilience Act (CRA), som vil standardisere reglerne om cybersikkerhed for produkter med digitale elementer i hele EU, og som også skal træde i kraft i 2027, har samme sigte. Og den seneste revision af TRBS (tekniske regler for driftsmæssig sikkerhed) fra det tyske Forbundsinstitut for Arbejdsbeskyttelse og Arbejdsmedicin understreger også den grundlæggende forbindelse mellem safety og security. Sikker automatisering betyder derfor, at man skal overveje og kombinere begge aspekter af begrebet "sikkerhed".

Safety og security: To integrationstilgange ...

I princippet kan enhver enhed i et netværk med forbindelse til IT-verdenen via TCP/IP blive et middel til angreb på andre enheder – og dermed bringe produktionsstabiliteten og processikkerheden i fare.

En mulig tilgang – som var almindelig før i tiden og stadig nogle gange forekommer i dag – ville derfor være at implementere en sikkerhedsløsning uden en forbindelse mellem den eksterne feltbus- og IT-verdenen og maskinens datanetværksstruktur. Ud over at en sådan afkobling ikke længere muliggør automatiseret diagnose af f.eks. sikkerhedsteknologi, er den også i modstrid med de nuværende teknologiske og fremtidige tendenser inden for automatisering – dvs. digitaliseringen og implementeringen af Industri 4.0. Separat ledningsføring af standard- og safety-komponenter er heller ikke længere state of the art – ikke mindst på grund af den indsats, det kræver.

Baseret på det faktum, at uden yderligere diagnostiske og sekundære data fra sikkerhedsteknologiområdet kan innovative maskinkoncepter i form af Industri 4.0 og forretningsmodeller baseret på dem næppe implementeres, ville brugen af Ethernet-baseret safety-teknologi i marken også være et alternativ. Standardiserede og certificerede kommunikationsprotokoller som PROFIsafe, FSoE eller CIP Safety muliggør overførsel af sikkerhedsrelevante data i automatiseringsapplikationer med funktionel sikkerhed.

Men hver af disse netværkskomponenter skal have sin egen Ethernet-forbindelse og IP-adresse, som skal sikres individuelt med hensyn til cybersikkerhed. En stor indsats og en høj risiko – især når der er fri adgang til åbne Ethernet-porte i marken. For at gøre ondt værre transporteres de data, der indsamles til Industri 4.0, ofte ikke via en separat IT-grænseflade, men også via OT-grænsefladen, f.eks. til en sky. Det betyder, at der ikke længere er en barriere mellem OT- og IT-verdenen og de internetforbindelser, der ofte er forbundet dermed.

... og en enkel løsning: ASi-5 Safety

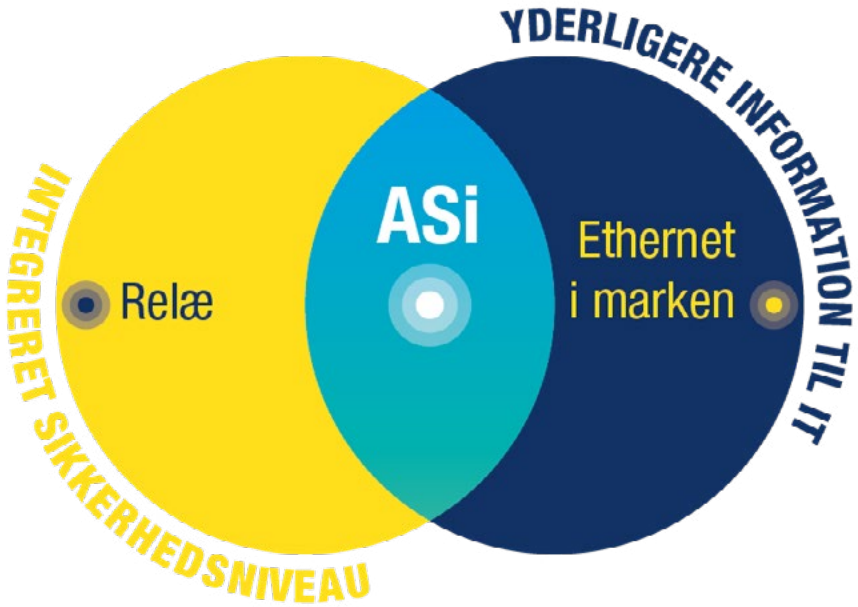
Ingen stik, ét kabel til standard- og sikkerhedsteknologi fra forskellige generationer, den bedste forbindelse fra ethvert punkt i netværket – AS-Interface som det etablerede ledningssystem på det laveste feltniveau giver mulighed for at realisere maskinsikkerhed mere enkelt, omkostningseffektivt og skræddersyet end nogensinde før. Og sandsynligvis mere effektivt end nogensinde før. Det skyldes, at i modsætning til sikker Ethernet-baseret kommunikation, hvor hver komponent har sin egen IP-adresse, tilbyder ASi-5 Safety en meget højere I/O-tæthed pr. IP-adresse. Fordelt over en kabellængde på op til 2 x 200 meter kan en gateway med en ASi-5/ASi-3-sikkerhedsmonitor fra Bihl+Wiedemann nemt håndtere langt over 100 sikre I/O'er under en enkelt IP-adresse i to ASi-kredsløb og med I/O-moduler som den nye BWU4277 med 14 sikre indgange og to elektronisk sikre udgange. Og disse kan nemt oprettes og overvåges i virksomhedens ASIMON360-konfigurationssoftware.

De sikre signaler, eventuelt suppleret med standardsignaler, opsamles udelukkende via et enkelt kabel – det gule ASi-profilkabel. I overført betydning fungerer det som centralnervesystemet i en maskines eller et systems OT-netværk og som en shuttlebus for sikre signaler til ASi-5 Safety Gateway. Den integrerede sikkerhedsmonitor kan konfigureres som en sikkerhedscontroller og giver dermed mulighed for at realisere en safety-applikation som en stand-alone-løsning.

Men da gateways altid har en integreret feltbusgrænseflade som PROFINET, EtherNet/IP, EtherCAT eller POWERLINK, kan omfattende diagnostiske oplysninger om sikkerhedsfunktionerne stilles til rådighed for det overordnede styresystem. Hvis der anvendes en gateway med en sikker feltbusprotokol som PROFIsafe, CIP Safety eller Safety over EtherCAT (FSoE), kan ikke kun diagnosedataene, men også selve de sikre data overføres til et sikkert styresystem.

Gatewayen åbner ikke kun døren til ASi's verden af intelligent kablingsteknologi med dens brede portefølje af safety- og standard-I/O-moduler til felten, men bidrager også til at reducere antallet af Ethernet-grænseflader og dermed til en betydeligt lavere security-risiko i et system. For at gøre de ekstra data anvendelige på en meningsfuld måde har alle gateways med ASi-5 Safety også en separat diagnostisk grænseflade, der er optimeret til IT-verdenen.

Denne understøtter aktuelle IT-kommunikationsstandarder som OPC UA, REST API og i fremtiden MQTT. Takket være muligheden for at udføre certifikatbaserede, sikre firmwareopdateringer i felten kan nye standarder og også nye security-krav – også i felten – nemt eftermonteres og dermed opfyldes. For at sikre høj tilgængelighed og minimal nedetid i tilfælde af udskiftning gemmes hardware- og safety-konfigurationen samt de tilsluttede enheders parameterdata på et SD-kort og overføres i sin helhed til en ny gateway af samme type, når de skal bruges.



et kommunikative brud mellem TCP/IP- og feltniveauet i gatewayen sikrer, at ASi kan give IT et højt niveau af tilgængelig ekstra information, som f.eks. diagnostiske data, samtidig med at der tilbydes den bedst mulige beskyttelse mod cyberangreb.

ASi-5 Safety har security om bord og i sigte

På grund af det stærke netværk af Industri 4.0-enheder og risikoen for, at disse bliver et middel til angreb på andre enheder, stiger security-kravene til netværksdeltagere meget hurtigt. Her imponerer Bihl+Wiedemanns produkter med en lang række funktioner og foranstaltninger, der garanterer produktionsstabilitet og processikkerhed i et sikkert netværk.

Selv om ASi-gatewayen med sin forbindelse til TCP/IP er bindeleddet mellem den eksterne feltbus- og IT-verden og maskinens datatekniske netværksstruktur, kan den ikke blive en gateway eller en angrebsplatform for cyberangreb, da den fysisk afkobler TCP/IP-niveauet og feltniveauet med ASi og ASi Safety. Dette kommunikative brud mellem ASi og TCP/IP isolerer ASi-netværksdeltagerne udadtil og forhindrer dermed direkte TCP/IP-adgang til feltniveauet i første omgang.

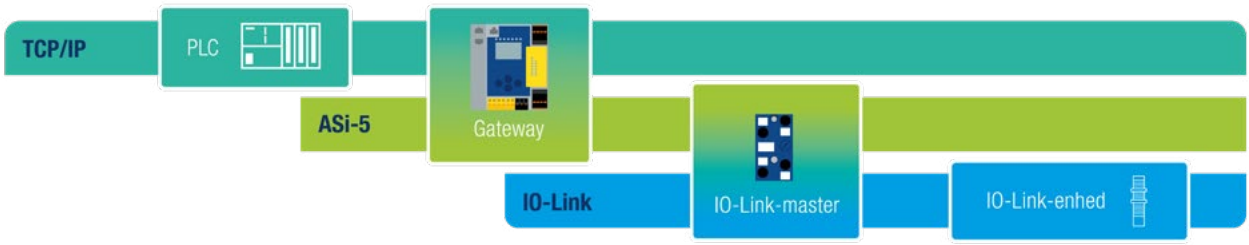
Mens modulerne og deltagerne i ASi-netværket skal opfylde langt lavere security-krav, da de ikke kan kommunikere i TCP/IP-netværk, er gatewayen i princippet den eneste komponent, der er væsentligt relevant for cybersikkerheden. For at beskytte ASi-gateways udfører Bihl+Wiedemann allerede i udviklingen og idriftsættelsen omfattende tests med en bred vifte af cybersikkerhedsværktøjer.

For eksempel udsættes gatewayernes Ethernet-feltbusgrænseflade og Ethernet-diagnosegrænseflade for strenge modstandsdygtigheds-tests ved hjælp af GE Digitals brancheafprøvede Achilles® Robustness Test-software for at sikre, at de er immune over for cyberangreb.

Security: Omfattende og fremtidssikret

På grund af ASi-produkternes lange levetid skal det også være muligt at udbedre erkendte svagheder i enhedens software længe efter, at enhederne er taget i brug. Desuden kan hackere og cyberkriminelle til enhver tid komme med nye trusler, som har til formål at omgå eksisterende sikkerhedsforanstaltninger. Under mottoet "Fremtiden om bord og i sigte" tilbyder Bihl+Wiedemann derfor muligheden for at opdatere sikre dele af gateways under løbende systemdrift ved hjælp af firmwareopdateringer i systemet og signeret sikkerhedssoftware, der skal godkendes af enheden på forhånd som en del af den certifikatbaserede end-to-end-kryptering. Det betyder, at virksomhedens ASi-5-moduler altid kan udstyres med de nyeste security-standarder og dermed gøre dem investeringssikre i nærmest ubegrænset tid.

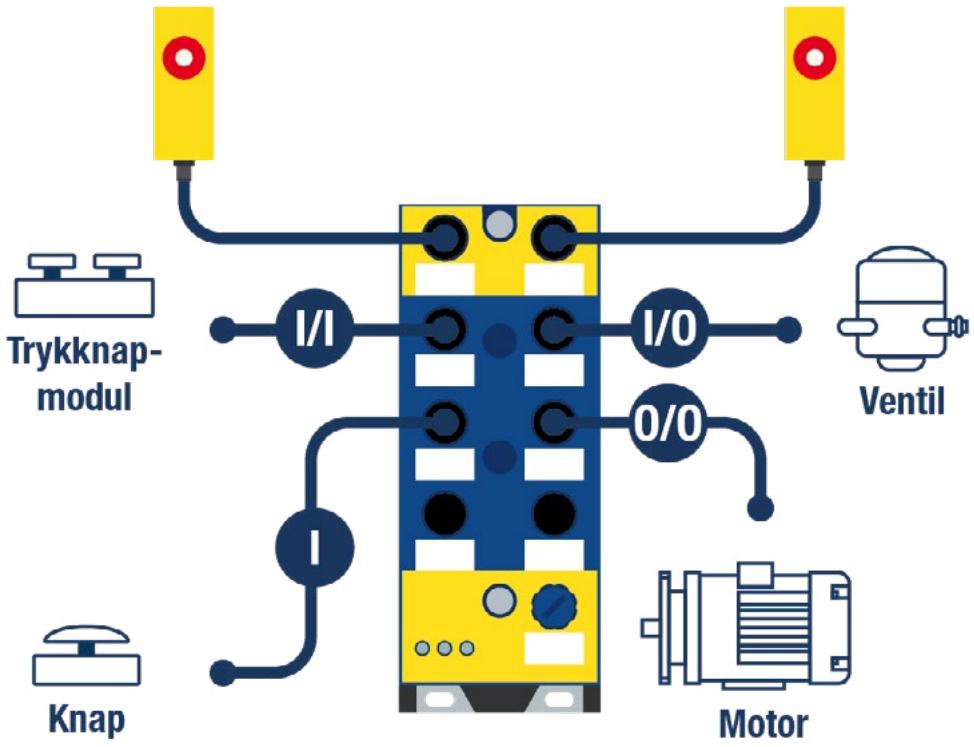
Andre grunde til, at ASi-5 og ASi-5 Safety tilbyder det højeste niveau af cybersikkerhed, er brugen af kryptografiske og autentificere-de krypterings- og verifikationsalgoritmer som AES-256 med SHA eller RSA i Bihl+Wiedemanns OPC UA-kompatible produkter samt understøttelse af kundespecifikke certifikater som TLS. For det andet bruger ASi-5 OFDM (orthogonal frequency-division multiplexing) til at transmittere data. På grund af denne dynamiske frekvenstildeling er det meget tidskrævende at registrere de udvekslede meddelelser, og det er kun muligt, hvis hele konteksten for forbindelsesopsætningen, herunder frekvensændringerne mellem ASi-masteren og ASi-del-tageren, er kendt.



Feltbusgatewayen ASi-5/ASi-3 fra Bihl+Wiedemann afkobler fysisk TCP/IP fra ASi-5 og ASi-5 Safety, dvs. feltbus- og feltniveauet.

Safety & Security: Maskiner är bara riktigt säkra tillsammans

Den digitala omvandlingen inom maskin- och anläggningsteknik innebär både en möjlighet och en nödvändighet att förstå och implementera maskinsäkerhet och industriell cybersäkerhet som lika viktiga aspekter av säkerhetstekniken. Hos Bihl+Wiedemann avspeglas detta konsekvent i företagets produkter. Som i standardområdet med ASi-5, där tack vare dess höga prestanda många nya användningsområden har öppnats upp sedan den nya standarden introducerades - förutom de många nya produkter som har öppnat upp nya möjligheter inom områden såsom drivteknik och integration av IO-Link-enheter erbjuder ASi-5 Safety också en omfattande ny potential för ännu smartare säkerhetsteknik, med hänsyn tagen till alla de säkerhetsaspekter som kommer att krävas i framtiden. Detta beror på att maskinsäkerhet 4.0 endast kan uppnås genom denna typ av interaktion mellan Safety och Security – och därför inte bara är funktionell och cyberresisistent, utan också ekonomiskt framtidssäker.



Med ASi-5 Safety kan man takket være kombinationen af sikre signaler og standardsignaler i ét modul dække næsten alle brancherelevante integrations- og anvendelsesscenarier.