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

Safety och security för (framtids)säker automation

ASi-5 Safety och ASi Safety at Work – båda även med möjlighet att överföra standardsignaler på samma linje – plus ett brett utbud av gateways och moduler för att förverkliga en mängd olika säkerhetslösningar oavsett bransch och styrsystem, samt Safe Link för PLC-fri, säker koppling och nätverkande av ASi-nätverk: Den omfattande portföljen understryker Bihl+Wiedemanns expertis inom funktionell säkerhetsteknik. I och med digitaliseringen av maskin- och anläggningskonstruktion är det dock nästan otänkbart med Safety utan Security – dvs. utan skydd mot cyberattacker. Inte ens för automationsspecialisterna från Mannheim.

Funktionssäkerheten – Safety – syftar till att skydda människor och miljö från olycksrisker som kan orsakas av maskiner. Data- och kommunikationssäkerhet – Security – står för övervakning av OT-strukturer och IT-nätverk samt potentiella inkörsportar för att på ett tillförlitligt sätt eliminera riskerna för manipulation eller stöld av data. Eftersom den funktionella säkerheten blir alltmer digital kan Safety-lösningar – utan att ta hänsyn till data- och kommunikationssäkerhet – utsättas för faran med externa förändringar, förändringar som kan försämra eller till och med eliminera deras skyddsfunktion.

Vid ett eventuellt byte kan den maskinvaru- och Safety-konfiguration som finns lagrad på SD-kortet samt parameterdata för de anslutna enheterna överföras till en ny gateway av samma typ.

Säkerhet: Ny status i lagstiftningen

Det är därför ingen tillfällighet att t.ex. EU:s maskindirektiv 2023/1230, som kommer att ersätta maskindirektivet 2006/42/EG den 20 januari 2027, föreskriver att maskiner ska vara konstruerade och tillverkade på ett sådant sätt att varken en ansluten enhet i sig eller en fjärransluten enhet som kommunicerar med maskinen kan leda till en farlig situation. Detta gäller både maskinvara och programvara, både när maskinen används på avsett sätt och vid eventuell manipulering. Anslutning till eller kommunikation via enheter för fjärråtkomst, t.ex. routrar, får inte heller leda till farliga situationer. EU:s Cyber Resilience Act (CRA), som kommer att standardisera reglerna om cybersäkerhet för produkter med digitala element i hela EU och som också ska träda i kraft 2027, har samma inriktning. Även den senaste revideringen av TRBS (Technical Rules for Operational Safety) från Federal Institute for Occupational Safety and Health illustrerar den grundläggande kopplingen mellan Safety och Security. Säker automation innebär därför att man beaktar och kombinerar båda aspekterna av begreppet „säkerhet“.

Safety & Security: Två integrationsmetoder ...

I princip kan varje enhet i ett nätverk som är ansluten till IT-världen via TCP/IP bli ett verktyg för attacker mot andra enheter – och därmed äventyra produktionsstabiliteten och processäkerheten.

En möjlig lösning – som var vanlig förr, och som ibland fortfarande förekommer – skulle därför kunna vara att implementera en säkerhetslösning utan en länk mellan den externa fältbuss- och IT-världen och maskinens datanätverksstruktur. Förutom att en sådan frikoppling inte längre möjliggör automatiserad diagnos av t.ex. säkerhetstekniken, går den också stick i stäv med nuvarande tekniska och framtida trender inom automation – dvs. digitaliseringen och implementeringen av Industri 4.0. Separat kabeldragning av standard- och Safety-komponenter är inte heller längre aktuellt – inte minst på grund av den arbetsinsats som krävs.

Eftersom innovativa maskinkoncept i enlighet med Industri 4.0 och affärsmodeller som bygger på dessa knappast kan implementeras utan ytterligare diagnos- och sekundärdata från säkerhetsteknikområdet, skulle användningen av Ethernet-baserad Safety-teknik inom området också vara ett alternativ. Standardiserade och certifierade kommunikationsprotokoll såsom PROFIsafe, FSoE eller CIP Safety möjliggör överföring av säkerhetsrelevanta data i automationsapplikationer med funktionell säkerhet.

Var och en av dessa nätverkskomponenter måste dock ha sin egen Ethernet-anslutning och IP-adress, vilka måste skyddas individuellt med avseende på cybersäkerhet. En stor ansträngning och en hög risk – särskilt när öppna Ethernet-portar är fritt tillgängliga på fältet. Till råga på allt transporteras den data som samlas in för Industri 4.0 ofta inte via ett separat IT-gränssnitt utan även den via OT-gränssnittet, t.ex. till ett moln. Detta innebär att det inte längre finns någon barriär mellan OT- och IT-världen och de internetanslutningar som ofta följer med dem.

... och en enkel lösning: ASi-5 Safety

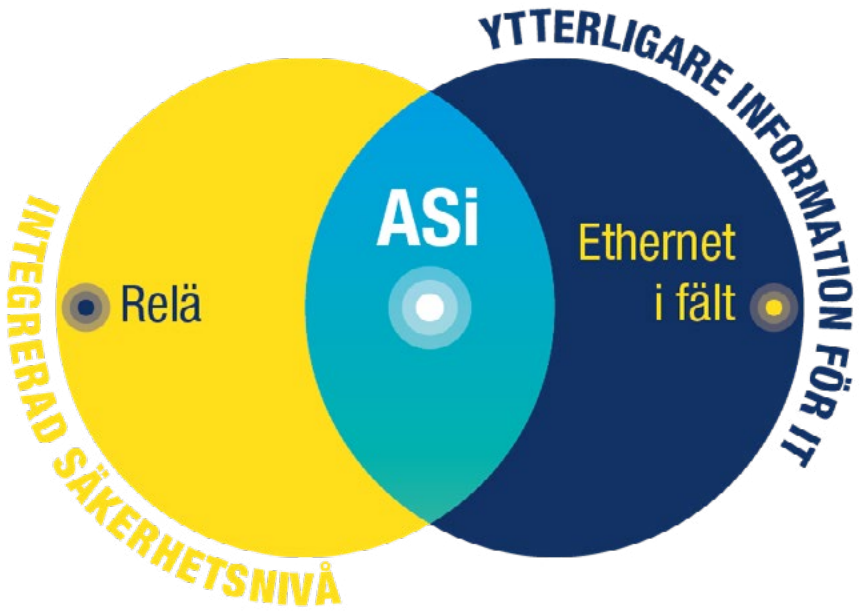
Inga kontakter, en kabel för standard- och säkerhetsteknik av olika generationer, bästa anslutning från varje punkt i nätverket – AS-Interface som det etablerade ledningssystemet på lägsta fältnivå ger möjlighet att förverkliga maskinsäkerhet enklare, mer kostnadseffektivt och mer kundanpassat än någonsin tidigare. Och förmodligen mer effektivt än någonsin tidigare. Till skillnad från säker Ethernet-baserad kommunikation, där varje komponent har sin egen IP-adress, erbjuder ASi-5 Safetyen mycket högre I/O-densitet per IP-adress. Med en kabellängd på upp till 2 x 200 meter kan en gateway med en ASi-5/ASi-3 säkerhetsmonitor från Bihl+Wiedemann enkelt hantera långt över 100 säkra I/O under en enda IP-adress i två ASi-kretsar och med I/O-moduler som nya BWU4277 med 14 säkra ingångar och två elektroniskt säkra utgångar. Dessa kan i sin tur enkelt skapas och övervakas i företagets konfigurationsmjukvara ASIMON360.

De säkra signalerna, som vid behov kompletteras med standardsignaler, samlas uteslutande in via en enda kabel – gula ASi-profilkabeln. I bildlig bemärkelse fungerar den som det centrala nervsystemet i OT-nätverket i en maskin eller ett system, och som en matarbuss för säkra signaler till ASi-5 Safety-gatewayen. Den integrerade säkerhetsmonitorn kan konfigureras som en säkerhetsstyrenhet och ger därmed möjlighet att realisera en Safety-applikation som en fristående lösning.

Men eftersom gateways alltid har ett integrerat fältbussgränssnitt, t.ex. PROFINET, EtherNet/IP, EtherCAT eller POWERLINK, kan omfattande diagnostisk information om säkerhetsfunktionerna göras tillgänglig för det överordnade styrsystemet. Om en gateway med ett säkert fältbussprotokoll används, t.ex. PROFIsafe, CIP Safety eller Safety over EtherCAT (FSoE), kan inte bara diagnosdata utan även själva säkerhetsdatan överföras till ett säkert styrsystem.

Gatewayen öppnar inte bara dörren till ASi:s värld av smarta kablage, med dess breda portfölj av Safety- och standard-I/O-moduler för fältet, utan bidrar också till att minska antalet Ethernet-gränssnitt och därmed till en betydligt lägre säkerhetsrisk inom ett system. För att göra den extra informationen användbar på ett meningsfullt sätt har alla gateways med ASi-5 Safety också ett separat diagnostikgränssnitt som är optimerat för IT-världen.

Detta stöder nuvarande IT-kommunikationsstandarder såsom OPC UA, REST API och i framtiden även MQTT. Tack vare möjligheten att utföra certifikatbaserade, säkra firmwareuppdateringar på fältet kan nya standarder och även nya säkerhetskrav – även på fältet – enkelt eftermonteras och därmed uppfyllas. För att säkerställa hög tillgänglighet och minimala driftstopp vid byte lagras maskinvaru- och Safety-konfigurationen samt parameterdata för de anslutna enheterna på ett SD-kort och överförs i sin helhet till en ny gateway av samma typ när den installeras.



Den kommunikativa brytningen mellan TCP/IP och fältnivå i gatewayen säkerställer att ASi kan förse IT med en hög nivå av tillgänglig tilläggsinformation, till exempel diagnosdata, samtidigt som det ger bästa möjliga skydd mot cyberattacker.

ASi-5 Safety har säkerheten ombord och i fokus

På grund av den omfattande uppkopplingen av Industri 4.0-enheter och risken för att dessa blir ett verktyg för attacker mot andra enheter, ökar säkerhetskraven för nätverksdeltagare mycket snabbt. Här imponerar Bihl+Wiedemanns produkter med ett helt paket av funktioner och åtgärder som garanterar produktionsstabilitet och processäkerhet i ett säkert nätverk.

Även om ASi Gateway med sin anslutning till TCP/IP är länken mellan den externa fältbuss- och IT-världen och en maskins datanätverksstruktur kan den inte bli en gateway eller en attackplattform för cyberattacker, detta eftersom den fysiskt frikopplar.

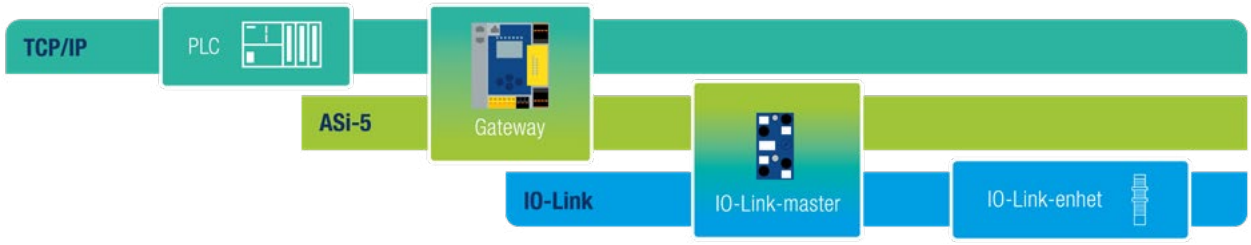
Medan modulerna och deltagarna i ASi-nätverket alltså måste uppfylla betydligt lägre säkerhetskrav – detta eftersom de inte kan kommunicera i TCP/IP-nätverk – är gatewayen i princip den enda komponenten av någon större betydelse för cybersäkerheten. För att skydda ASi-gateways vidtar Bihl+Wiedemann säkerhetsåtgärder omfattande tester med ett brett utbud av verktyg för cybersäkerhet redan under utveckling och driftsättning.

Exempelvis utsätts gatewayernas Ethernet-fältbussgränssnitt och Ethernet-diagnostikgränssnitt för stränga motståndskraftstester med hjälp av GE Digitals branschbeprövade Achilles® Robustness Test-programvara för att säkerställa att de är immuna mot cyberattacker.

Säkerhet: Heltäckande och framtidssäkrat

På grund av den långa livslängden på ASi-produkterna måste det också vara möjligt att åtgärda erkända svagheter i enhetens programvara långt efter att enheterna har tagits i drift. Dessutom kan hackare och cyberbrottslingar när som helst komma med nya hot som syftar till att kringgå befintliga säkerhetsåtgärder. I enlighet med mottot „Framtiden ombord och i fokus“ erbjuder Bihl+Wiedemann därför möjligheten att uppdatera säkra delar av gateways under pågående systemdrift med hjälp av firmwareuppdateringar i systemet samt signerad säkerhetsprogramvara som måste autentiseras av enheten i förväg som en del av certifikatbaserad end-to-end-kryptering. Det innebär att företagets ASi-5-moduler alltid kan utrustas med de senaste säkerhetsstandarderna, vilket gör dem investeringssäkra på nästan obestämd tid.

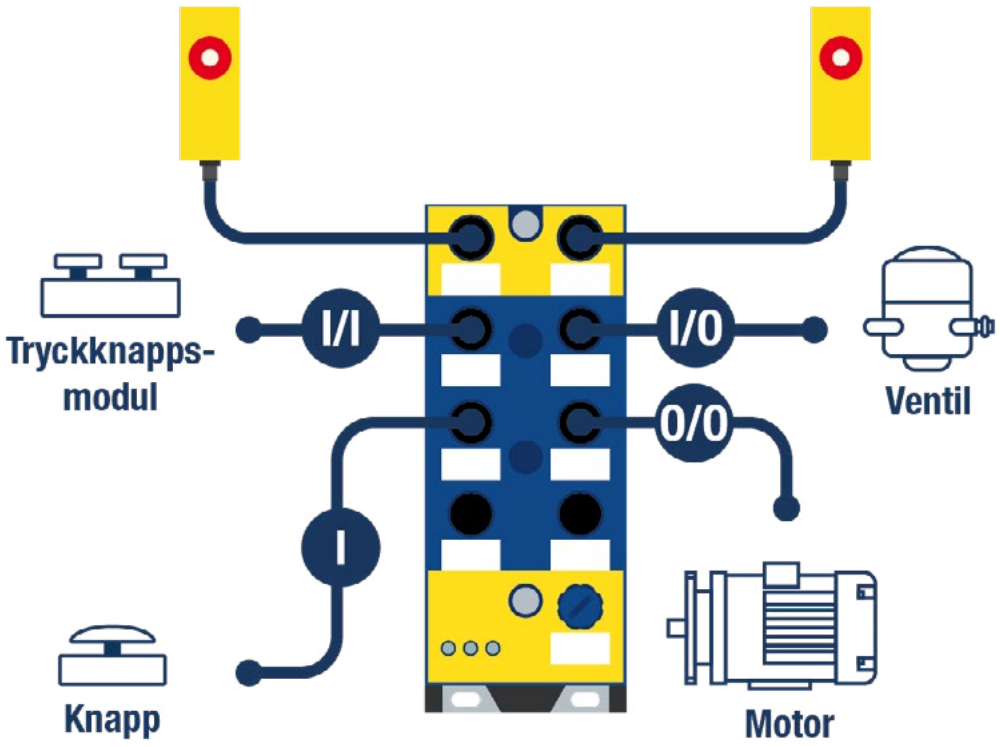
Andra anledningar till att ASi-5 och ASi-5 Safety erbjuder den högsta nivån av cybersäkerhet är användningen av kryptografiska och autentiserade krypterings- och verifieringsalgoritmer såsom AES-256 med SHA eller RSA i Bihl+Wiedemanns OPC UA-kompatibla produkter, samt stöd för kundspecifika certifikat som TLS. För det andra använder ASi-5 OFDM (Orthogonal Frequency Division Multiplexing) för att överföra data. På grund av denna dynamiska frekvenstilldelning är det mycket tidskrävande att registrera de utväxlade meddelandena, och det är dessutom endast möjligt om hela sammanhanget för anslutningsuppsättningen, inklusive frekvensändringarna mellan ASi-master och ASi-subscriber, är känt.



Fältbussgatewayen ASi-5/ASi-3 från Bihl+Wiedemann frikopplar TCP/IP fysiskt från ASi-5 och ASi-5 Safety, dvs. fältbussen och fältnivån.

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.



Tack vare kombinationen av säkra signaler och standardsignaler i en modul kan ASi-5 Safety täcka nästan alla branschrelevanta integrations- och applikationsscenarier.