AS-INTERFACE MASTER **NEWS**
Digitales Magazin von Bihl+Wiedemann 02/2024

Safety und Security für die (zukunfts-)sichere Automation

ASi-5 Safety und ASi Safety at Work – beide mit der Möglichkeit, auf derselben Leitung auch Standardsignale zu übertragen – dazu eine Vielzahl an Gateways und Modulen für eine branchen- und steuerungsunabhängige Realisierung unterschiedlichster Sicherheitslösungen sowie Safe Link zur SPS-losen, sicheren Kopplung und Vernetzung von ASi Netzwerken: Das umfangreiche Portfolio untermauert die Expertise von Bihl+Wiedemann in der funktionalen Sicherheitstechnik. Mit der Digitalisierung im Maschinen- und Anlagenbau ist Safety jedoch ohne Security – also ohne Schutz vor Cyber-Angriffen – kaum mehr denkbar. Auch nicht für die Automatisierungsspezialisten aus Mannheim.

Funktionale Sicherheit – Safety – dient dem Schutz von Menschen und der Umwelt vor Unfallgefahren, die von Maschinen ausgehen können. Daten- und Kommunikationssicherheit – Security – steht für die Überwachung von OT-Strukturen und IT-Netzwerken sowie von möglichen Einfallstoren, um die Gefahren durch Manipulation oder Diebstahl von Daten zuverlässig zu eliminieren. Da die funktionale Sicherheit zunehmend digitaler wird, können Safety-Lösungen ohne die Berücksichtigung von Security-Risiken der Gefahr von Veränderungen von außen ausgesetzt sein – Veränderungen, die ihre Schutzfunktion beeinträchtigen oder sogar aufheben können.

Im Austauschfall können die auf der SD-Karte gespeicherte Hardware- und Safety-Konfiguration sowie die Parameterdaten der angeschlossenen Geräte komplett auf ein neues, typengleiches Gateway übertragen werden.

Security: Neuer Stellenwert in der Gesetzgebung

Nicht umsonst bestimmt daher beispielsweise die EU-Maschinenverordnung 2023/1230, die am 20. Januar 2027 die Maschinenrichtlinie 2006/42/EG ablösen wird, Maschinen so zu konstruieren und zu bauen, dass weder eine angeschlossene Einrichtung selbst noch eine entfernte, mit der Maschine kommunizierende Einrichtung zu einer gefährlichen Situation führen kann. Dies gilt für Hardware und für Software, sowohl beim bestimmungsgemäßen Gebrauch der Maschine als auch im Falle möglicher Manipulationen. Auch der Anschluss an oder die Kommunikation über Fernzugriffseinrichtungen wie z. B. Router darf nicht zu gefährlichen Situationen führen.

Die gleiche Stoßrichtung hat der Cyber Resilience Act (CRA) der Europäischen Union, der die Regeln zur Cybersecurity von Produkten mit digitalen Elementen EU-weit vereinheitlichen wird und ebenfalls ab 2027 gelten soll. Und auch die jüngste Revision der TRBS (Technische Regeln für Betriebssicherheit) der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin stellt den fundamentalen Zusammenhang zwischen Safety und Security dar. Sichere Automation bedeutet also, beide Aspekte des Begriffs „Sicherheit“ zu betrachten und zu verbinden.

Safety & Security: Zwei Integrationsansätze ...

Grundsätzlich kann in einem Netzwerk jedes Gerät mit einer Verbindung per TCP/IP in die IT-Welt zum Vehikel für Angriffe auf andere Geräte werden – und so die Produktionsstabilität und die Prozesssicherheit gefährden.

Ein möglicher Lösungsansatz – wie früher üblich und teilweise auch heute noch anzutreffen – wäre also, eine sicherheitstechnische Lösung ohne Bindeglied zwischen der äußeren Feldbus- und IT-Welt und der datentechnischen Netzwerkstruktur einer Maschine umzusetzen. Neben der Tatsache, dass eine solche Entkopplung beispielsweise keine automatisierte Diagnose der Sicherheitstechnik mehr ermöglicht, steht sie auch aktuellen Technologie- und Zukunftstrends in der Automatisierung – also der Digitalisierung und Umsetzung von Industrie 4.0 – entgegen. Und auch eine separate Verdrahtung von Standard- und von Safety-Komponenten ist – nicht zuletzt wegen des damit verbundenen Aufwands – nicht mehr Stand der Technik.

Ausgehend davon, dass ohne zusätzliche Diagnose- und Sekundärdaten auch aus dem Bereich der Sicherheitstechnik wohl kaum noch innovative Maschinenkonzepte im Sinne von Industrie 4.0 und darauf basierender Geschäftsmodelle umgesetzt werden können, würde sich alternativ auch die Nutzung von ethernetbasierter Safety-Technologie im Feld anbieten. Standardisierte und zertifizierte Kommunikationsprotokolle wie PROFIsafe, FSoE oder CIP Safety ermöglichen die Übertragung sicherheitsrelevanter Daten in Automatisierungsanwendungen mit funktionaler Sicherheit.

Dafür muss aber jede dieser Netzwerkkomponenten einen eigenen Ethernetanschluss und eine eigene IP-Adresse haben, die im Hinblick auf Cybersecurity jeweils individuell gesichert werden müssen. Ein hoher Aufwand und ein hohes Risiko – gerade dann, wenn offene Ethernet-Ports im Feld frei zugänglich sind. Erschwerend kommt hinzu, dass die für Industrie 4.0 gesammelten Daten häufig nicht über eine gesonderte IT-Schnittstelle, sondern ebenfalls über die OT-Schnittstelle z. B. in eine Cloud transportiert werden. Damit gibt es keine Barriere mehr zwischen der OT- und der IT-Welt und damit oft einhergehender Internetverbindungen.

... und eine einfache Lösung: ASi-5 Safety

Keine Stecker, ein Kabel für Standard- und Sicherheitstechnik verschiedener Generationen, beste Verbindung von jeder Stelle im Netzwerk – AS-Interface als das etablierte Verdrahtungssystem der untersten Feldebene bietet die Möglichkeit, Maschinensicherheit so einfach, kostengünstig und maßgeschneidert zu realisieren wie noch nie. Und wohl auch so effizient wie noch nie. Denn im Gegensatz zu einer sicheren ethernetbasierten Kommunikation, bei der jede Komponente ihre eigene IP-Adresse benötigt, bietet ASi-5 Safety eine weitaus höhere E/A-Dichte pro IP-Adresse. Verteilt über bis zu 2 x 200 m Leitungslänge kann ein Gateway mit ASi-5/ASi-3 Sicherheitsmonitor von Bihl+Wiedemann unter einer einzigen IP-Adresse in zwei ASi Kreisen und mit E/A-Modulen wie dem neuen BWU4277 mit 14 sicheren Eingängen und zwei elektronisch sicheren Ausgängen ohne Weiteres weit über 100 sichere E/As verwalten. Diese wiederum lassen sich in der Konfigurationssoftware ASIMON360 des Unternehmens ganz einfach anlegen und überwachen.

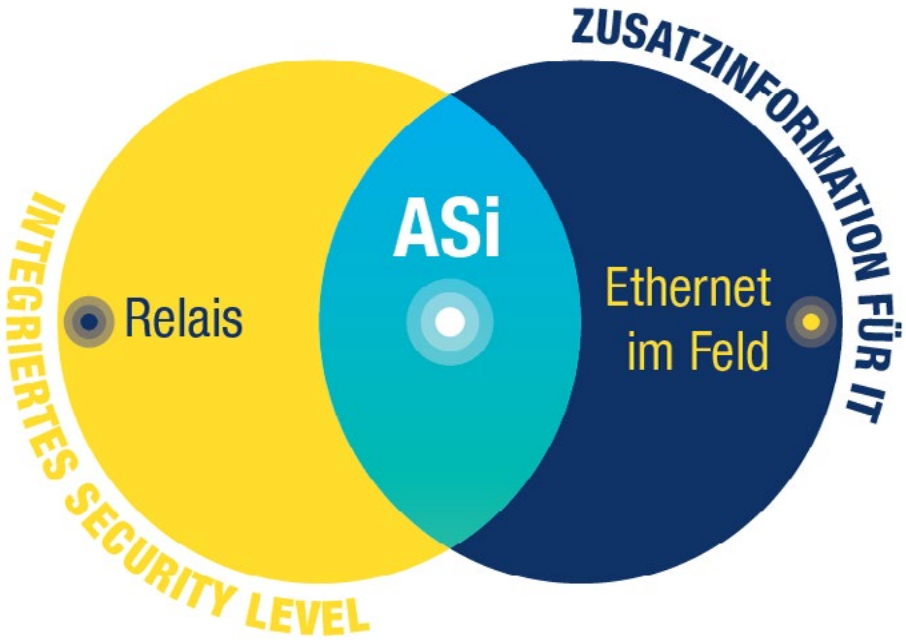
Die sicheren Signale werden, bei Bedarf ergänzt um Standardsignale, ausschließlich über eine einzige Leitung eingesammelt – das gelbe ASi Profilkabel. Dieses fungiert im übertragenen Sinn als zentrales Nervensystem im OT-Netzwerk einer Maschine oder Anlage und als

Zubringerbus für sichere Signale zum ASi-5 Safety Gateway. Der integrierte Sicherheitsmonitor kann als Sicherheitssteuerung konfiguriert werden und liefert so die Möglichkeit, eine Safety-Applikation als Stand-Alone-Lösung zu realisieren.

Da die Gateways aber immer über eine integrierte Feldbusschnittstelle wie PROFINET, EtherNet/IP, EtherCAT oder POWERLINK verfügen, können der übergeordneten Steuerung umfangreiche Diagnoseinformationen zu den Sicherheitsfunktionen zur Verfügung gestellt werden. Wenn ein Gateway mit einem sicheren Feldbusprotokoll wie PROFIsafe, CIP Safety oder Safety over EtherCAT (FSoE) zum Einsatz kommt, können nicht nur die Diagnosedaten, sondern auch die sicheren Daten selbst an eine sichere Steuerung übertragen werden.

Dabei dient das Gateway nicht nur als Türöffner in die Welt der intelligenten Verdrahtungstechnologie ASi mit seinem breiten Portfolio an Safety und Standard E/A Modulen fürs Feld, sondern trägt zur Reduktion der Ethernet-Schnittstellen und damit zu einem erheblich geringeren Security-Risiko innerhalb einer Anlage bei. Um die zusätzlichen Daten auch sinnvoll nutzbar zu machen, verfügen alle Gateways mit ASi-5 Safety zudem über eine separate Diagnoseschnittstelle, die für die IT-Welt optimiert ist.

Diese unterstützt aktuelle IT-Kommunikationsstandards wie OPC UA, REST API und zukünftig auch MQTT. Dank der Möglichkeit, zertifikatsbasierte, sichere Firmware-Updates im Feld durchzuführen, können neue Standards, aber eben auch neue Anforderungen an die Security – auch im Feld – einfach nachgerüstet und so erfüllt werden. Um einen hochverfügbaren Betrieb und minimale Downtime im Austauschfall zu gewährleisten, werden die Hardware- und die Safety-Konfiguration sowie die Parameterdaten der angeschlossenen Geräte auf einer SD-Karte gespeichert und beim Einsetzen in ein neues, typengleiches Gateway auf dieses komplett übertragen.



Der kommunikative Bruch zwischen TCP/IP- und Feldebene im Gateway sorgt dafür, dass ASi der IT ein hohes Maß an verfügbaren Zusatzinformationen wie z. B. Diagnosedaten zur Verfügung stellen kann und gleichzeitig bestmöglich vor Cyber-Attacken geschützt ist.

ASi-5 Safety hat Security an Bord und im Blick

Durch die starke Vernetzung von Industrie-4.0-Geräten und die Gefahr, dass diese zum Vehikel für Angriffe auf andere Geräte werden, steigen die Security-Anforderungen an Netzwerkteilnehmer sehr schnell an. Hier überzeugen die Produkte von Bihl+Wiedemann gleich mit einem ganzen Bündel an Merkmalen und Maßnahmen, die die Produktionsstabilität und die Prozesssicherheit im sicheren Netzwerk gewährleisten.

Selbst wenn das ASi Gateway mit seiner Verbindung zu TCP/IP das Bindeglied zwischen der äußeren Feldbus- und IT-Welt und der datentechnischen Netzwerkstruktur einer Maschine ist, kann es nicht zum Einfallstor oder zur Angriffsplattform für Cyber-Attacken werden, denn es entkoppelt physisch die TCP/IP-Ebene und die Feldebene mit ASi und ASi Safety. Dieser kommunikative Bruch zwischen ASi und TCP/IP isoliert die ASi Netzwerkteilnehmer nach außen und lässt so einen direkten TCP/IP-Durchgriff auf die Feldebene gar nicht erst zu.

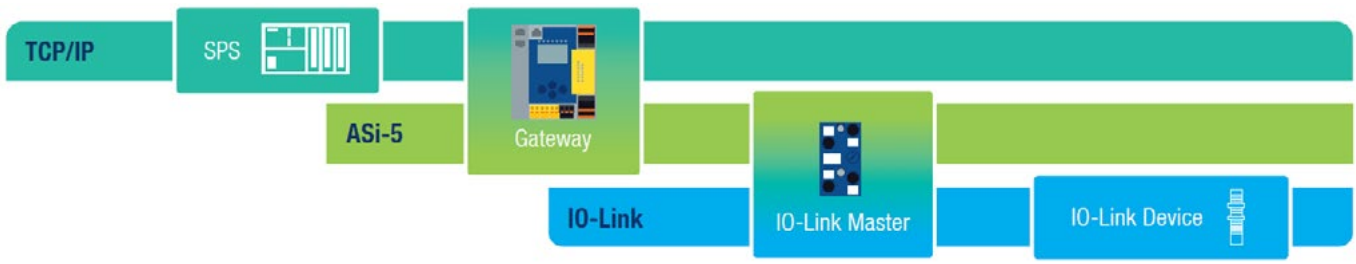
Während also an die Module und Teilnehmer im ASi Netzwerk weitaus geringere Security-Anforderungen gestellt werden müssen, da sie nicht in TCP/IP-Netzen kommunizieren können, ist das Gateway im Prinzip die einzige, maßgeblich Cybersecurity-relevante Komponente. Um ASi Gateways zu schützen, werden bereits in der Entwicklung und auch bei der Inbetriebnahme von Bihl+Wiedemann umfangreiche Tests mit einer breiten Palette an Werkzeugen aus dem Bereich der Cyber-Security durchgeführt.

So werden beispielsweise die Ethernet-Feldbusschnittstelle und die Ethernet-Diagnoseschnittstelle der Gateways durch die industriebewährte Testsoftware Achilles® Robustness Test von GE Digital strengen Belastbarkeitstests unterzogen, um die Unempfindlichkeit gegen Cyber-Angriffe sicherzustellen.

Security: Umfassend und zukunftssicher

Durch die lange Einsatzdauer von ASi Produkten muss es zudem möglich sein, erkannte Schwachstellen in der Gerätesoftware noch lange nach der Inbetriebnahme von Geräten zu beheben. Zudem können von Hackern und Cyber-Kriminellen jederzeit neue Gefahren ausgehen, mit denen bisherige Sicherheitsmaßnahmen umgangen werden sollen. Getreu der Devise „Die Zukunft an Bord und im Blick“ bietet Bihl+Wiedemann daher die Möglichkeit, im laufenden Anlagenbetrieb sichere Teile von Gateways durch In-System-Updates von Firmware und durch signierte, vom Gerät zuvor zu authentifizierende Sicherheitssoftware im Rahmen einer zertifikatsbasierten Ende-zu-Ende-Verschlüsselung zu aktualisieren. Dadurch ist es möglich, die ASi-5 Module des Unternehmens immer mit den neuesten Security-Standards auszustatten und sie so nahezu unbegrenzt investitionssicher zu machen.

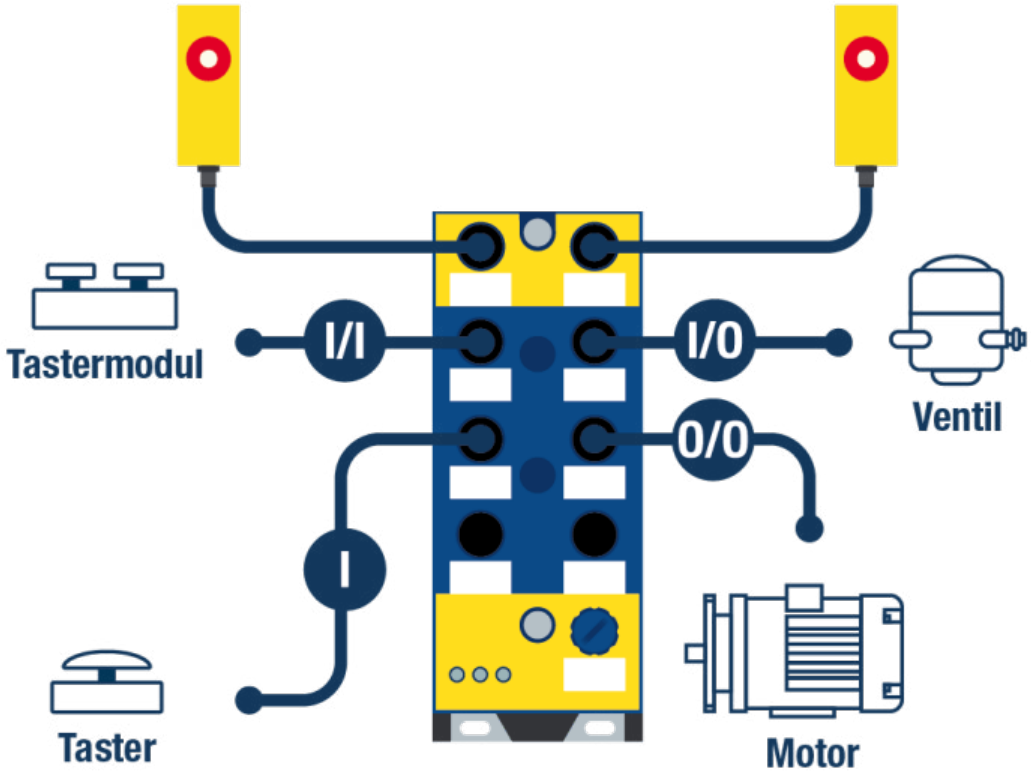
Weitere Gründe, weshalb ASi-5 und ASi-5 Safety ein Höchstmaß an Cybersecurity bieten, sind zum einen der Einsatz kryptografischer und authentisierter Verschlüsselungs- und Prüfalgorithmen wie AES-256 mit SHA oder RSA bei den OPC-UA-fähigen Produkten von Bihl+Wiedemann sowie die Unterstützung kundenspezifischer Zertifikate wie TLS. Zum anderen erfolgt bei ASi-5 die Übertragung der Daten per Orthogonalem Frequenzmultiplexverfahren (OFDM, Orthogonal Frequency-Division Multiplexing). Durch diese dynamische Frequenzzuweisung ist das Mitschneiden der ausgetauschten Nachrichten sehr aufwendig und nur möglich, wenn der gesamte Kontext des Verbindungsaufbaus inklusive der Frequenzwechsel zwischen ASi Master und ASi Teilnehmer bekannt ist.



Durch das ASi-5/ASi-3 Feldbus Gateway von Bihl+Wiedemann erfolgt eine physische Entkopplung zwischen TCP/IP und ASi-5 sowie ASi-5 Safety, sprich der Feldbus- und der Feldebene.

Safety & Security: Nur zusammen sind Maschinen wirklich sicher

Die digitale Transformation im Maschinen- und Anlagenbau bietet zugleich die Chance und die Notwendigkeit, Maschinensicherheit und industrielle Cybersecurity als gleichwertige Aspekte der Sicherheitstechnik zu verstehen und umzusetzen. Bei Bihl+Wiedemann bildet sich dies konsequent in den Produkten des Unternehmens ab. Wie bereits im Standardbereich mit ASi-5, wo sich seit der Einführung des neuen Standards dank seiner großen Leistungsfähigkeit viele neue Anwendungsgebiete – etwa in der Antriebstechnik oder bei der Integration von IO-Link Devices – mit vielen neuen Produkten eröffnet haben, bietet auch ASi-5 Safety viele neue Potenziale für eine noch smartere Sicherheitstechnik unter Berücksichtigung aller zukünftig geforderten Security-Aspekte. Denn nur durch ein solches Zusammenwirken von Safety und Security lässt sich Maschinensicherheit 4.0 erreichen – und damit neben einer funktionalen und Cyber-resilienten auch eine finanzielle Zukunftssicherheit.



Mit ASi-5 Safety können dank der Kombination von sicheren Signalen und Standardsignalen in einem Modul nahezu alle industrierelevanten Integrationsund Einsatzszenarien abgedeckt werden.