5 | 2023
31. August I 124. Ausgabe
AUTOMATISIERUNG.AT
DAS FACHMAGAZIN

Österreichs fortschrittliches Magazin für Fertigungs- und Prozessautomatisierung | Österr. Post AG – MZ09Z038211M I Retouren an Postfach 555, 1008 Wien AlexanderVerlag.at GmbH, Hauptplatz 11, A-3712 Maissau I 7€ (Ausl.: 9€)
Entgeltliche Themenplatzierung am Titelbild (Promotion); Fotos: Adobe Stock;

Ethernet-APL
auch für die Fertigung?

Warum sich die Zwei-Draht-Ethernet-Lösung für die Prozessautomation unter der Ägide des im Etablieren von Kommunikationsstandards erfahrenen Dachverbands PI ebenso für die Fabrikautomation weiterentwickeln könnte

Warum künftig für die CE-Kennzeichnung Security-Aspekte in der Operational Technology berücksichtigt werden müssen

Kein Safety ohne Security

Am 29. Juni 2023 wurde die EU-Verordnung über Maschinen (2023/1230) veröffentlicht. Diese wird künftig die bisherige Maschinenrichtlinie 2006/42/EG und deren nationale Umsetzung, die Maschinen-Sicherheitsverordnung MSV2010, ablösen. Die neue Maschinenverordnung beinhaltet nun erstmals Security-Anforderungen. Konkret fordert sie Schutz gegen Korrumpierung durch in negativer Absicht handelnde Dritte. Das heißt, Security-Maßnahmen werden für Maschinen- und Anlagenhersteller künftig zur unmittelbaren Pflicht, denn die neue EU-Verordnung trägt nun direkten Gesetzescharakter innerhalb der gesamten europäischen Union und muss nicht erst durch einzelstaatliche Behörden in deren lokale Gesetzgebungen umformuliert werden. Von Andreas Willert

Das internationale Normenwerk IEC 62443 betrachtet die Security von »Industrial Automation and Control Systems« (»IACS«). Die Norm entspringt der Automatisierung der Prozessindustrie und hat sich zum horizontalen Standard der wertschöpfenden Industrie, inklusive der diskreten Fertigung, entwickelt. Diese Normenreihe ist ein umfassendes Konstrukt, das aus mehreren Teilen und Unterteilen besteht. Für den Anlagenbetreiber besteht Kompatibilität zur im Unternehmensbereich akzeptierten und etablierten Reihe ISO/IEC 27000. Ausfälle von Produktionen aufgrund von Security- Schwachstellen in vernetzten Industriesteuerungen oder Edge-Devices sowie nicht dem Stand der Technik entsprechende Implementierungen selbiger verursachen nicht nur wirtschaftlichen Schaden direkt beim betroffenen Produktionsunternehmen, sondern auch Bullwhip-Effekte (Peitscheneffekte) in der Supply-Chain. Die Normenreihe IEC 62443 setzt es sich daher zum Ziel, alle Anforderungen der Industrial-Security durch ein holistisches Schutzkonzept abzudecken.

Die Teile der IEC 62443

Das vielfach genannte Defense-In-Depth-Prinzip bedeutet angewandt, dass Schutzmaßnahmen sowohl von Produktherstellern und Systemintegratoren als auch Betreibern getroffen werden müssen – durch die ganze Lieferkette hindurch. Je nachdem, welche Rolle man einnimmt – also Hersteller, Integrator oder Betreiber – sind unterschiedliche Teile anzuwenden. Teil 2-1 der IEC 62443 kann ergänzend zur ISO 27001 in OT-Umgebungen eingesetzt werden und spezifiziert organisatorische Maßnahmen und Prozesse des Betreibers. Generell beschreibt Teil 2 Prozesse, die vom Systemintegrator (Teil 2-4) und vom Betreiber (Teil 2-1) umgesetzt werden. Teil 4 richtet sich an Hersteller von Komponenten, die in Automatisierungslösungen eingesetzt werden. Hierbei soll schon im Entwicklungsprozess die IT-Sicherheit ein integraler Bestandteil sein, um das Entstehen von Schwachstellen nicht nur zu vermeiden, sondern auch den Umgang mit Schwachstellen zu regeln. Beispielsweise ist der Entwicklungsprozess (Product-Development-Lifecycle) aller neuen Komponenten von Pilz, inklusive der Industrie-Firewall »Securitybridge« nach der IEC 62443-4-1 zertifiziert. Mit dedizierten Security-Produkten sowie mit vernetzungsfähigen Komponenten steht Pilz in der (Security-)Verantwortung gegenüber den nachfolgenden Abnehmern in der Lieferkette. Teil 3 der IEC 62443 richtet sich an das System selbst. Darin werden IT-sicherheitsrelevante Anforde-

Die Industrie-Firewall »Securitybridge« von Pilz ist nach der IEC 62443-4-1 zertifiziert und erfüllt damit die Anforderungen der Industrial-Security.

rungen an die funktionalen Fähigkeiten der Automatisierungssysteme spezifiziert. Im Detail wird in Teil 3-2 das Security-Risk-Assessment für das Systemdesign der Maschine/Anlage beschrieben. Darauf basiert übrigens auch die neue Pilz-Dienstleistung »Industrial Security Risk Assessment«. Durch diverse Maßnahmen, wie z.B. Netzwerksegmentierungen, werden Risiken gemildert. Das System muss spezifizierte Security-Anforderungen erfüllen, die entweder durch die Komponenten selbst oder durch zusätzliche Security-Maßnahmen erreicht werden, beispielsweise durch industrielle Firewalls oder Zugangskontrollen mit Authentifizierungen. Risikoreduzierungen können generell organisatorische Maßnahmen durch den Betreiber selbst sowie zugekaufte Security-Komponenten durch den Integrator sein. Damit ist Security in der Lieferkette ein wesentlicher Bestandteil.

Die Analogie der Kennwerte in Functional Saftey und Cybersecurity

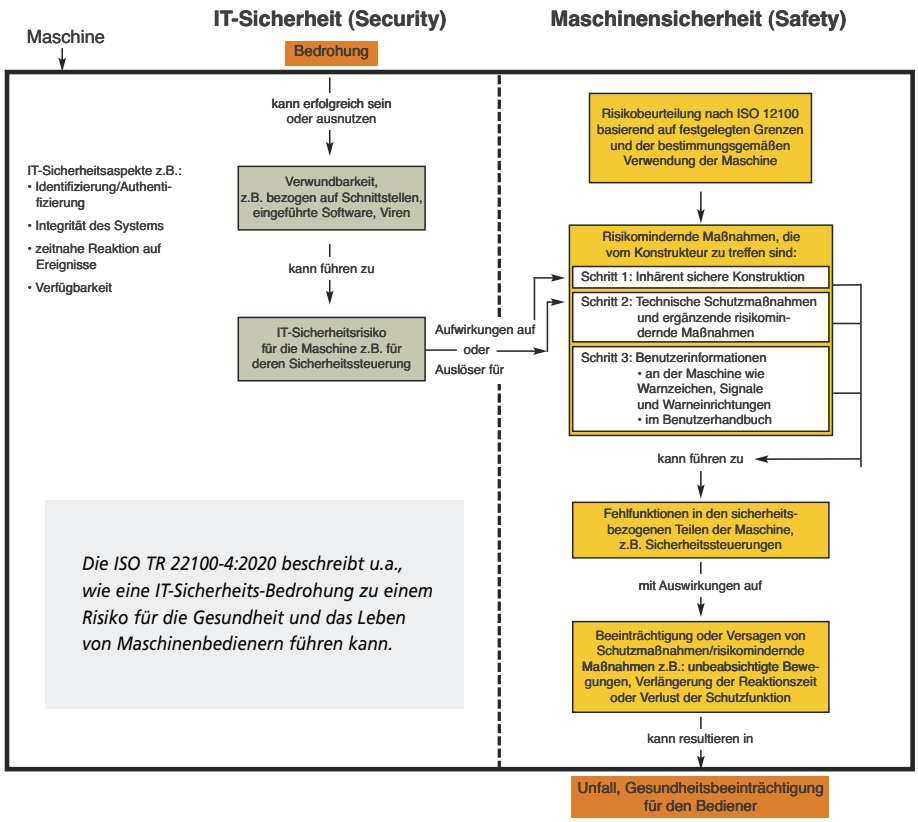
Die funktionale Sicherheit nach EN ISO 13849-1 und EN IEC 62061 ist für die Konstruktion und Bewertung von sicherheitsrelevanten Steuerungssystemen essenziell – also für die Auslegung von Steuerungen und Einrichtungen, die Menschen und Maschinen vor Gefahren schützen, beispielsweise Funktionen zum Stillsetzen im Notfall durch das Betätigen eines Not-Halt-Tasters oder Durchschreiten eines Sicherheits-Lichtgitters. Das Risiko wird durch Kennzahlen wie das Performance-Level (PL) oder Safety-Integrity-Level (SIL) quantifiziert. Das Security-Level (SL) spezifiziert, gegen welche Motivation von Angriff das System geschützt werden soll. Daraus werden die Anforderungen an die Zuverlässigkeit der Schutzmaßnahmen abgeleitet.

Risikobeurteilung von Maschinen

Cyberangriffe auf Industrieanlagen können nicht nur Produktionsausfälle verursachen, sondern auch Menschenleben gefährden. Im ISO TR 22100-4: »Sicherheit von Maschinen – Zusammenhang mit ISO 12100 – Teil 4: Leitlinien für Maschinenhersteller zur Berücksichtigung der damit verbundenen IT-Cybersicherheits-Aspekte« wird beschrieben, wie eine IT-Sicherheitsbedrohung zu einem Risiko für die Gesundheit und das Leben von Maschinenbedienern führen kann. Wenn Security-Bedrohungen eine Auswirkung auf die funktionale Sicherheit haben können, erfordert dies eine Risikobeurteilung und ist für den CE-Kennzeichnungsprozess relevant. Hierbei ist mit der 2023 in der Edition 1.0 erstmalig erschienenen »IEC TS 63074 Safety of machinery – Security aspects related to functional safety of safety-related control systems« eine Empfehlung zur Umsetzung der IEC 62443 für den Schutz der Safety von Maschinen gegen Cyberangriff veröffentlicht worden.

Zusammenhang mit der NIS2-Richtlinie

Die EU-Richtlinie 2022/2555 (NIS 2) Kapitel IV, Artikel 21 besagt:
1.) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen geeignete »



Die ISO TR 22100-4:2020 beschreibt u.a., wie eine IT-Sicherheits-Bedrohung zu einem Risiko für die Gesundheit und das Leben von Maschinenbedienern führen kann.

Der Weg zur CE-Kennzeichnung führt künftig auch über die Cybesecurity.

und verhältnismäßige technische, operative und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen und die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten. Die in Unterabsatz 1 genannten Maßnahmen müssen unter Berücksichtigung des Stands der Technik und gegebenenfalls der einschlägigen europäischen und internationalen Normen sowie der Kosten der Umsetzung ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist. Bei der Bewertung der Verhältnismäßigkeit dieser Maßnahmen sind das Ausmaß der Risikoexposition der Einrichtung, die Größe der Einrichtung und die Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen und deren Schwere, einschließlich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen, gebührend zu berücksichtigen (Anm.: Ist Bestandteil des »High-Level-Risk-Assessments« nach der IEC 62443-3-2).

2.) Die in Absatz 1 genannten Maßnahmen müssen auf einem gefahrenübergreifenden Ansatz beruhen, der darauf abzielt, die Netz- und Informationssysteme und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen, und zumindest Folgendes umfassen:
a) Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;
[…]
i) Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;
[…]

Der Artikel kongruiert also in weiten Bereichen mit der IEC 62443! Die NIS 2 erfordert ein Informationssicherheits-Managementsystem (ISMS). Für ein Unternehmen wird die ISO/IEC 27001/27002 für die Unternehmensebene herangezogen und die IEC 62443-2-1 für den Shopfloor.

Fazit

Wenn ein Anlagenbetreiber in den Wirkbereich der NIS 2 fällt, ist er mit einer Risikoanalyse der Anlage/des Systems nach IEC 62443-3-2 zur Erfüllung der Anforderungen der NIS 2 auf der sicheren Seite – zumindest im Bereich der OT im Shopfloor. Security in der Maschinenverordnung als Pflicht für die CE-Konformität und die NIS 2 – das alles passiert gerade fast gleichzeitig. Durch diese Gesetze werden neue Anforderungen an österreichische Maschinen- und Anlagenbauer sowie -betreiber entstehen. Aktuell ist oft schon alleine die Security-Verantwortung für Industrieanlagen im Shopfloor nicht geklärt. All diese Gesetze und Normen sind längst überfällige Maßnahmen, um eine Resilienz der europäischen Industrie vor Cyberangriffen aufzubauen. In den 1990er- und frühen 2000er-Jahren war es ein mehr oder weniger harmloses Vergnügen für Nerds, Security-Schwachstellen in Betriebssystemen zu finden oder mit simplen Programmen fremde Rechner zu manipulieren – »hacking for fun« sozusagen, ohne nennenswerten Schaden. Heutzutage werden ganze Unternehmen lahmgelegt und erpresst, was existenzbedrohend für Unternehmer und Angestellte sein kann. Security-software-Icons in der Taskleiste und regelmäßige Updates sind ein gewohnter Umstand in Office-Netzwerken. Die Security für vernetzungsfähige Geräte und Steuerungssysteme in der OT hinkt hingegen jener der IT stark hinterher. Daher kann der Appell nur lauten:

- Treffen Sie technische und organisatorische Maßnahmen,
- konsultieren Sie Spezialisten und
- beschäftigen Sie sich rechtzeitig mit dem Thema der OT-Security – nämlich jetzt!

Denn es wird künftig keine CE-Kennzeichnung geben, ohne Security-Aspekte in der Operational Technology berücksichtigt zu haben – insbesondere dann, wenn es um die funktionale Sicherheit geht. (TR)

„Es wird künftig keine CE-Kennzeichnung geben, ohne Security-Aspekte in der Operational Technology berücksichtigt zu haben – insbesondere wenn es um die funktionale Sicherheit geht."

Andreas Willert, CMSE ist Industrial-Security-Experte bei Pilz Österreich und Autor dieses Beitrages.

Zum Autor: *Andreas Willert, CMSE, ist Industrial-Security-Experte bei Pilz Österreich.*

INFOLINK: www.pilz.at

Fotos: Pilz, Adobe Stock;