25.05.2023

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern
Deutschland
http://www.pilz.com

Pressemitteilung

Thomas Pilz: Die Zukunft der sicheren Automation

Ostfildern , 25.05.2023 - **(Es gilt das gesprochene Wort)**

Thomas Pilz

Security: Das kommt gesetzlich auf Industrie und Maschinenbau zu

Bei den Normen und Gesetzen für die Sicherheit im industriellen Umfeld findet derzeit ein Umbruch statt. Getrieben wird dieser durch die Themen Security und Künstliche Intelligenz (KI). Für die Industrie im Allgemeinen und für den Maschinen- und Anlagenbau sind beim Thema Security drei neue bzw. kommende gesetzliche Vorgaben relevant: Die EU-Richtlinie NIS 2, die neue Maschinenverordnung und der Cyber Resilience Act.

Wie beim letzten Jahrespressegespräch fokussiere ich mich auf das Thema Security und möchte Ihnen heute darstellen, wie umfangreich die Auswirkungen für die gesamte Industrie sein werden.

NIS 2: Mehr Pflichten und mehr Sanktionen für mehr Unternehmen

NIS (Netz- und Informationssicherheit) ist eine Richtlinie der Europäischen Union zur Stärkung der Cybersicherheit. Diese Richtlinie gibt es bereits seit 2016 und sie galt bislang für Anbieter im Bereich kritische Infrastrukturen, darunter Energie, Verkehr, Banken und Finanzen, Gesundheit, Trinkwasserversorgung und -verteilung sowie digitale Infrastruktur. Anbieter in diesen Sektoren mussten mit Blick auf die Security „angemessene Sicherheitsvorkehrungen“ treffen und gravierende Cybersicherheitsvorfälle melden. Der Nachfolger ist NIS 2, die Anfang 2023 in Kraft trat und bis Herbst 2024 von den EU-Mitgliedsstaaten in nationales Recht umgesetzt werden muss. Die Richtlinie gilt jetzt unter anderem auch innerhalb der Sektoren Maschinenbau sowie Automotive und hier für Unternehmen mit mehr als 50 Mitarbeitern oder einem Jahresumsatz von mehr als 10 Millionen Euro. Europaweit betrifft dies nach Angaben des VDMA rund 9.000 Unternehmen. Diese Unternehmen müssen künftig nachweisen, dass sie technische, operative und organisatorische Maßnahmen zum Schutz vor Security-Vorfällen ergreifen. Dazu gehört zunächst die Risikoanalyse von bestehenden Systemen auch in Produktionsumgebungen, also der OT (Operations Technology). Dann folgen die Ausarbeitung und Umsetzung spezifischer Prozesse und Maßnahmen wie Passwortschutz oder Verschlüsselung sowie, Weiterbildung und Schulung von Mitarbeitern. Cybersicherheitsvorfälle müssen innerhalb von 24 Stunden den zuständigen Behörden gemeldet werden. Neu ist auch die ausdrückliche Einbeziehung von Lieferketten. Zusammengefasst betrifft NIS 2 nun mehr Unternehmen, erweitert die Pflichten und sieht strengere Sanktionen vor. Unternehmen, die keine Maßnahmen ergreifen, drohen empfindliche Strafen.

Cyber Resilience Act – Security für den gesamten Produktlebenzyklus

Im September 2022 hat die Europäische Kommission einen Entwurf für eine Verordnung vorgelegt, die die Cybersicherheit von Produkten erhöhen soll. Dieser Cyber Resilience Act richtet sich an Hersteller von Produkten mit digitalen Elementen. Damit ist sowohl Hard- als auch Software (wie z.B. Firmware) gemeint. Die Verordnung bezieht sich hierbei sowohl auf Consumer-Produkte, als auch auf Produkte für industrielle Anwendungen, wie zum Beispiel Maschinensteuerungen. Laut Cyber Resilience Act dürfen nur noch Produkte in Verkehr gebracht werden, die ein angemessenes Cybersicherheitsniveau gewährleisten. Des Weiteren werden Hersteller verpflichtet, Kunden über Sicherheitslücken so schnell wie möglich zu informieren und diese zu schließen. Die Verordnung betrifft also den gesamten Lebenszyklus eines Produktes. Das bedeutet, dass Hersteller nun auch über den üblichen Gewährleistungszeitraum hinaus Softwareupdates anbieten müssen, um auch zukünftige Bedrohungen abzuwehren. Wir gehen davon aus, dass die Verordnung Ende 2024 verabschiedet wird.

Die neue Maschinenverordnung – Cybersecurity als Pflicht

Die dritte neue gesetzliche Security-Vorgabe ist die Maschinenverordnung der EU. Ihre Veröffentlichung steht kurz bevor. Da sie eine Verordnung ist, muss sie nicht erst in nationales Recht übertragen werden.
Maschinenhersteller haben 42 Monate Zeit, die neuen Anforderungen zu erfüllen. Die Maschinenverordnung ersetzt die bisherige Maschinenrichtlinie und macht, im Unterschied zur Vorgängerin, Cybersecurity verpflichtend. War die Maschinenrichtlinie eine reine Betrachtung der Safety, wurde in der Verordnung das Schutzziel Security unter „Protection against corruption“ in die „Essential health and safety requirements EHSR” mit aufgenommen: Die Sicherheitsfunktionen der Maschine dürfen durch unbeabsichtigte oder vorsätzliche Verfälschung nicht beeinträchtigt werden. Bisher ist bekannt, dass ein Erfüllen der Vorgaben aus dem Cyber Resilliance Act zu einer Konformitätsvermutung für die Maschinenverordnung führt.

Und jetzt: Wer muss sich um was kümmern?
Welche Bedeutung haben die gesetzlichen Vorgaben nun? Anhand des Sektors Stromerzeugung möchte ich die Zusammenhänge darstellen:
Bislang war nur der Stromversorger von der NIS-Richtlinie zur betroffen. Mit NIS 2 müssen künftig auch Maschinenbauer, wie etwa der Hersteller von Anlagen zur Stromerzeugung (z.B. Windkraftanlagen), die Vorgaben erfüllen. Der Hersteller der Windkraftanlage wiederum benötigt etwa Automatisierungslösungen, Steuerungen oder Sensoren z.B. von Pilz. Ab einer bestimmten Größe fallen auch Hersteller von elektrischen Komponenten unter NIS 2. Und da NIS 2 auch die Berücksichtigung der Lieferanten vorschreibt, muss sich auch ein Unternehmen wie Pilz um sichere Lieferketten kümmern und Anforderungen an ihre Lieferanten stellen. NIS 2 deckt also die komplette Lieferkette ab.

Seit jeher müssen Maschinenbauer, um Maschinen in Europa einführen zu können, das Konformitätsbewertungsverfahren durchlaufen an dessen Ende die CE-Kennzeichnung steht.
Jetzt, mit der neuen Maschinenverordnung, müssen Maschinenbauer nachweisen, dass ihre Maschinen auch gegen Manipulationen geschützt sind. Und schließlich unterliegt der Hersteller der elektrischen Komponenten den künftigen Vorgaben des geplanten Cyber Resilience Acts.

Zusammenfassend ist zu sagen: Ob und in welcher Tiefe sich ein Unternehmen mit Security auseinandersetzen will, ist nicht länger Ermessenssache des Unternehmens. Nein, es ist eine gesetzliche Vorgabe! Unternehmen tun gut daran, sich baldmöglichst mit NIS 2 zu beschäftigen und eine ganzheitliche Security-Betrachtung für das Unternehmen durchzuführen. Dazu gehört beispielsweise der Aufbau eines Managementsystems für Informationssicherheit (ISMS) mit Zertifizierung nach der Informationssicherheits-Norm ISO 27001.

Im Maschinenbau ist Security in Form von Industrial Security nicht allein Aufgabe der IT, sondern integraler Bestandteil der Konzeption und Konstruktion. Security im Nachhinein zu implementieren ist immer aufwändig und bedeutet meist Einbußen bei Anwenderfreundlichkeit, Funktionalität und Produktivität. Bei der Risikobeurteilung kommt zur Safety jetzt auch die Security hinzu. Ohne Security keine CE-Kennzeichnung!

Und für Hersteller von Produkten mit digitalen Elementen steht mit der Normenreihe IEC 62443 eine gute Orientierung bereit. In der untergeordneten Norm IEC 62443-4-1 werden beispielsweise Anforderungen an einen sogenannten „Security Development Lifecycle Prozess“ beschrieben.

Die EU ist bei der Security-Gesetzgebung vorgeprescht und in Europa werden die weltweit schärfsten Vorgaben gelten. Aber es laufen bereits Abstimmungen mit anderen Ländern, und auch dort werden solche Gesetze kommen. Aktuell ist z.B. Australien in Austausch mit der EU und wird sich vermutlich an die europäischen Normen anlehnen. Es ist also eine weltweite Harmonisierung bei Industrial Security zu erwarten.

Thomas Pilz

Offene Kommunikationsstandards als historische Aufgabe

Bei Pilz sind Offenheit und Anwenderfreundlichkeit wesentliche Kennzeichen des Portfolios. Wir wollen den Kunden Produkte anbieten, die immer auf dem Stand der Technik sind, einfach in der Handhabung bleiben und sich in jede Automatisierungsarchitektur einfügen.

Wir haben mit SafetyBUS p, dem ersten sichere Feldbussystem, und mit dem sicheren Echtzeit-Ethernet SafetyNET p die Entwicklung der sicheren industriellen Kommunikation geprägt. Doch die Zeit der proprietären Unternehmens-Lösungen ist vorbei. Wir setzen uns mit aller Kraft für die Schaffung von Industrie-Standards ein. Das ist eine historische Aufgabe!

OPC UA
Für die sichere, herstellerübergreifende Vernetzung für industrielle Anlagen hat sich die Industrie auf OPC UA (Open Platform Communications Unified Architecture) geeinigt. Dieses Kommunikationsprotokoll stellt eine standardisierte (IEC 62541) Schnittstelle für die Kommunikation zwischen verschiedenen Datenquellen in der Industrie bereit. Als Mitglied der OPC Foundation sind Mitarbeiter von Pilz sowohl im Lenkungskomitee als auch in Technischen Arbeitskreisen der Field Level Communication (FLC) Gruppe aktiv. Das Augenmerk von Pilz liegt dabei auf der Arbeitsgruppe, in der es um das Thema Safety geht (Safety over OPC UA).

Besonders wertvoll ist unser Know-how über den Einsatz der Publisher/Subscriber-Technologie (Pub/Sub) in Verbindung mit den Anforderungen von funktional sicheren Feldbusprotokollen. Im Vergleich zur klassischen Master/Slave-Architektur können bei Pub/Sub Daten direkt zwischen Teilnehmern ausgetauscht werden. Das erlaubt es, OPC UA auch für anspruchsvolle, verteilte Automatisierungsaufgaben einzusetzen. Pilz besitzt hier besondere Expertise, da unser SafetyNET p das einzige sichere, auf Ethernet basierende Feldbussystem ist, das von Beginn an Pub/Sub unterstützt.

Bei der Arbeit rund um die Themen der funktionalen Sicherheit kommen wir gut voran. Hand in Hand mit Prüfbehörden arbeitet die Gruppe an Testspezifikation und Testsystemen sowie die Zertifizierung von Kommunikations-Stacks für OPC UA Safety Die Version 1.05 ist bereits frei gegeben.

IO-Link Safety
Auf Sensorebene ist die Automatisierung bereits einen großen Schritt weiter in Sachen Offenheit. Hier steht das Kommunikationsprotokoll IO-Link Safety kurz vor der kommerziellen Verfügbarkeit. Die Punkt-zu-Punkt Kommunikation bietet viele Vorteile wie etwa Vereinfachungen bei der Installation (z.B. durch standardisierte Verkabelung und den Wegfall von Parallel-Verdrahtungen), eine automatisierte und toolunterstützte Parametrierung sowie erweiterte Diagnosemöglichkeiten.

Um IO-Link auch für sicherheitsrelevante Automatisierungsaufgaben einsetzen zu können, hat Pilz im Rahmen der IO-Link Community intensiv an der entsprechenden Extension mit den dazugehörigen Tests und Zertifizierungen gearbeitet. Experten von Pilz leiten die beiden IO-Link Safety Arbeitsgruppen (für Marketing und Technik).

Die ersten marktreifen Sensoren werden wir auf der SPS im November vorstellen. Der Ansatz von Pilz ist es, ein komplettes System, also Sensoren, Aktoren plus Master-Module, anzubieten. Das vereinfacht die Anwendung für den Kunden und erhöht die Leistungsfähigkeit.

Wir sind davon überzeugt, dass sich Automatisierungslösungen künftig noch stärker über ihre Funktionalitäten differenzieren: Wie gut sind die Benutzeroberflächen, wie einfach die Bedienung, welchen Zusatznutzen bieten sie? Hier liegt eine starke Innovationskraft und es entsteht großes Potenzial für neue Anwendungen.

Thomas Pilz

Die Zukunft der Sicherheit ist dynamisch

Was bedeutet die weitere Digitalisierung für den Schutz von Mensch und Maschine? Welche Technologien halten den Anforderungen an die Sicherheit Stand? Welche Rolle spielt der Mensch? Wir wollen heute auch einen Blick in die Zukunft werfen. Die gute Nachricht voraus: Der Mensch steht im Mittelpunkt. Seine Rolle wird sogar gestärkt.

Der Mensch als aktiver Gestalter

So zum Beispiel im Projekt „Fluide Produktion“ der Arena 2036. Pilz arbeitet mit Partnern an Entwicklung und Implementierung eines menschzentrierten, cyberphysischen Produktionskonzeptes insbesondere für die Automobilproduktion. Die Idee im Projekt ist, Produktionsanlagen in ortsflexible Module zu zerlegen, um ganz nach Bedarf dynamische Einheiten bilden und wieder auflösen zu können. Die Module sind mit einem zentralen Fokus auf die Rolle des Menschen als aktiver Gestalter seiner Produktionsumgebung konzipiert.

Aus diesen Anforderungen erwächst der Wunsch nach dynamischer Sicherheit, also einer flexibleren Anpassung der Sicherheitsfunktionen an die sich verändernden Produktionsprozesse und die damit verbundenen Schutzanforderungen. Die erlauben es beispielsweise, dass Roboter oder mobile Plattformen nicht gleich hart gestoppt werden müssen, wenn sich ein Mensch in den Arbeitsbereich hinein bewegt, sondern mit reduzierter (und damit weniger gefährlicher) Geschwindigkeit weiter arbeiten können oder besser noch sichere Ausweichstrategien beherrschen. Intelligente Sensoren und Aktoren in verteilten Systemen werden dabei immer mehr die Funktionen von Steuerungen übernehmen und zu einer besseren Interaktion von Maschinenmodulen untereinander und von Mensch und Maschine führen.

Sicherheit zur Echtzeit

Die dynamischen Situationen in den künftigen Produktionsumgebungen müssen mit Blick auf die Sicherheit in Echtzeit geprüft und freigegeben werden, damit der Schutz von Mensch und Maschine jederzeit gewährleistet bleibt. Das Schlagwort hier ist „Sicherheit zur Echtzeit“. Denkbar ist, dass sich verschiedene Maschinen – oder allgemein Assets – künftig Sicherheitseinrichtungen teilen. Das ist die „Shared Safety“, die wir in der SmartFactory KL erproben. Eine klassische CE-Kennzeichnung als Ergebnis eines analogen Konformitätsbewertungsverfahrens scheidet bei einem solchen Verständnis von Sicherheit aus. Informationen zu allen beteiligten Assets müssen zur Laufzeit aktuell verfügbar sein, Stichworte dazu sind Digitales Typenschild und Verwaltungsschale.

Im bereits erwähnten Projekt "Fluide Produktion" arbeiten wir an weiteren Zukunftsthemen wie die Identifikation (und damit Unterscheidung) von Menschen und Gegenständen. Hier bietet sich der Einsatz von Künstlicher Intelligenz an. Risiken können dann von lernfähigen KI-Algorithmen erkannt und beurteilt werden. Die „analoge“ CE-Kennzeichnung ist dabei der Basis-Schutz. Aber es lassen sich weitere Maßnahmen zur Risiko-Minimierung einleiten, die Sicherheit nochmals flexibler machen und zu mehr Produktivität beitragen.

Bildunterschrift:

Texte und Bilder finden Sie auch unter www.pilz.com zum Download. Um direkt auf die relevanten Internetseiten im Pressezentrum zu gelangen, geben Sie in der Suche auf der Homepage den folgenden Webcode ein.: **237512**

Pilz Gruppe

75 Jahre Pilz: Werte. Schaffen. Zukunft.

Als globaler Anbieter von Produkten, Systemen und Dienstleistungen für die Automatisierungstechnik blickt Pilz 2023 auf eine 75jährige Erfolgsgeschichte zurück: Gegründet 1948, beschäftigt die Pilz Gruppe heute rund 2.500 Mitarbeiter in 42 Tochtergesellschaften und Niederlassungen. Der Pionier der sicheren Automation mit Stammsitz in Ostfildern schafft weltweit mit seinen kompletten Automatisierungslösungen Sicherheit für Mensch, Maschine und Umwelt.
Das Portfolio des Technologieführers umfasst die Sensorik, Steuerungs- und Antriebstechnik genauso wie Systeme für die industrielle Kommunikation, Diagnose und Visualisierung. Ein internationales Dienstleistungsangebot mit Beratung, Engineering und Schulungen rundet das Angebot ab. Die Lösungen für Safety und Security kommen über den Maschinen- und Anlagenbau hinaus in zahlreichen Branchen, wie etwa der Intralogistik, der Bahntechnik oder im Bereich Robotik zum Einsatz.

www.pilz.com

Pilz in sozialen Netzwerken

In unseren Social Media Kanälen geben wir Hintergrundinformationen über das Unternehmen und den Menschen bei Pilz. Wir berichten über aktuelle Entwicklungen und Trends in der Automatisierungstechnik.

https://www.facebook.com/pilzINT

https://twitter.com/Pilz_INT

https://www.youtube.com/user/PilzINT

https://www.linkedin.com/company/pilz

Kontakt für Presse

Martin Kurth
Unternehmens- und Fachpresse
+49 711 3409 -158
publicrelations@pilz.com

Sabine Karrer
Fach- und Unternehmenspresse
+49 711 3409 - 7009
s.skaletz-karrer@pilz.de