Juni 2021
computer-automation.de

Computer & AUTOMATION

Sonderheft **SAFETY & SECURITY**

genua.

Künstliche Intelligenz

KI-Klassifikation für Safety

Seite 4

Kollaborative Robotik

Die Evaluierung der physischen Sicherheit

Seite 6

Verschlüsselung

Schutz für geistiges Eigentum

Seite 18

OT Security ist kein Feenstaub

KI-Klassifizierung nach Anwendungslevel

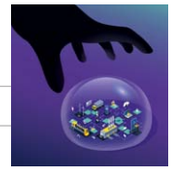
Künstliche Intelligenz in Sicherheitsapplikationen

Das eigene Know-how schützen

Quellcode sicher verschlüsseln

6 Sichere Mensch-Roboter-Kollaboration

Gefahrensituationen erfolgreich vorbeugen



SAFETY

SECURITY

RUBRIKEN

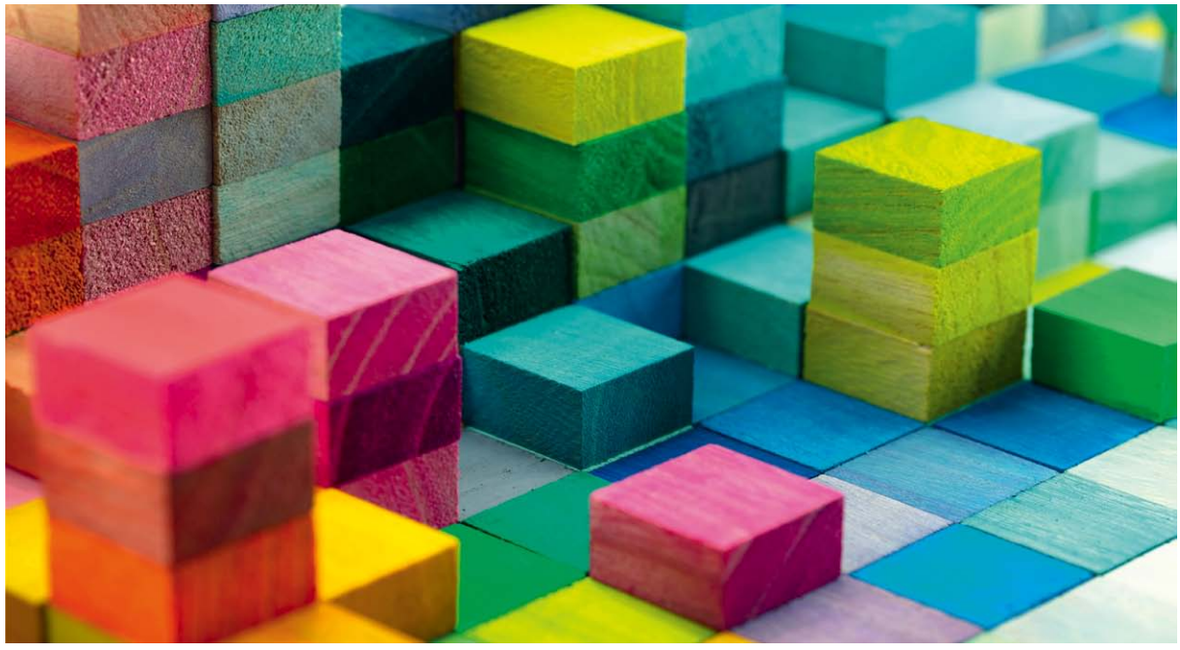
KI und Sicherheit

Künstliche Intelligenz dringt immer mehr in unseren Alltag ein, sei es in Form einer Bedienschnittstelle wie Alexa oder eines intelligenten Chatbots. Im industriellen Umfeld gilt die Technologie als interessanter Lösungsansatz für verschiedenste Problemstellungen. Doch welche Auswirkungen auf die Sicherheit von Mensch, Maschine oder Anlage hat der Einzug von KI in Produktion und Intralogistik?
Bereits einfache KI-Applikationen stellen eine Herausforderung bei der Nachweisführung zur Sicherheit dar. Daher werden mögliche Vorgehensweisen in den Normungsgremien diskutiert. Ganz am Anfang aber steht die Klassifikation von KI für Sicherheitsaufgaben. Ab *Seite 4* fasst Holger Laible die aktuelle Situation zusammen und stellt ein Klassifikationsschema für KI in Sicherheitsanwendungen vor.
Durch den Einzug von KI in Safety-Applikationen ist der Schutz der Algorithmen von höchster Bedeutung. Häufig nutzen Entwicklerinnen und Entwickler zum Programmieren der ML- und KI-Algorithmen die Programmiersprache Python. Da dieser Quellcode in KI-Applikationen aber als einfache Text-Datei ausgeliefert wird und daher im Klartext gelesen werden kann, ist er nicht vor Änderungen, Manipulation oder Kopie geschützt. Das geistige Eigentum liegt offen für jedermann da. Wie sich die Software mittels Vorkompilierung und Verschlüsselung sichern lässt, erfahren Sie ab *Seite 18*.

Andrea Gillhuber
Chefredakteurin

PS: Sie sind auf der Suche nach passenden Safety- oder Security-Lösungen? Dann empfehle ich Ihnen unsere interaktiven Marktübersichten. Diese bieten Ihnen den schnellen Überblick über Produkte und Systeme sowie deren Anbieter unter
https://www.computer-automation.de/marktuebersicht/

KI-Klassifikation für Safety



Künstliche Intelligenz wird in vielen Bereichen bereits verwendet und gilt als Lösungsansatz für aktuelle Herausforderungen in den verschiedensten Lebensbereichen. Die Politik fördert KI, möchte aber gleichzeitig die Technikfolgen abschätzen und gegebenenfalls regulieren. Nachfolgend wird der Einsatz von KI für Sicherheitsaufgaben betrachtet.

Der Begriff der KI hat sich über die Jahrzehnte seit dem Erstauftreten sehr gewandelt. Wo früher eine geschickte Verschachtelung von ‚if-then-else'-Statements bereits als KI galt, werden heute Mechanismen wie Machine Learning (ML) oder Knowledge-Graphen verstanden. Verschiedene Gremien haben sich mit dem Thema einer KI-Definition auseinandergesetzt, doch mit einer praktischen Beschreibung überrascht die Wikipedia mit einem interessanten Ansatz: „Meist bezeichnet künstliche Intelligenz den Versuch, bestimmte Entscheidungsstrukturen des Menschen nachzubilden, indem zum Beispiel ein Computer so gebaut und programmiert wird, dass er relativ eigenständig Probleme bearbeiten kann. Oftmals wird damit aber auch eine nachgeahmte Intelligenz bezeichnet, wobei durch meist einfache Algorithmen ein ‚intelligentes Verhalten' simuliert werden soll."

Festzustellen ist, dass es sich im Jahre 2021 bei angewandter Künstlicher Intelligenz immer noch um einen Versuch handelt, bestimmte Entscheidungsstrukturen nachzubilden, und im konkreten Anwendungsfall sogar nur eine Nachahmung von intelligentem Verhalten sein könnte. Diese Vorzeichen sind für einen Einsatz im sicherheitstechnischen Umfeld (Sicherheit steht in der Folge für das englische Safety und nicht für Security, also Informationssicherheit) eher ungünstig, da dort evidenzbasiert die risikominimierenden Eigenschaften zu bewerten sind. Somit stellt sich beim erstmaligen Einsatz von KI in Sicherheitsapplikationen – wie in anderen Bereichen bei Verwendung neuer Technologie auch – zuerst die Frage nach der Verhältnismäßigkeit.

Diese Überlegungen bedeuten zunächst Stabilität für bestehende Lösungen. Damit erhöht sich allerdings der Druck auf Lösungsansätze mit KI für aktuelle komplexere Problemstellungen (siehe *Bild 1*).

Während es für Sicherheitsfunktionen bisher in der Regel ausreichend war, Schaltzustände, Ströme oder Spannungen auszuwerten, stehen nun Fragen zur Erkennung von verschiedenen Hindernissen im Raum oder gar deren Charakterisierung. Die Zunahme dieser systematischen Komplexität geht einher mit der Verwendung von Sensoren, wie CCD-Kameras, die bisher nicht sicherheitsgerichtet eingesetzt wurden. Diese erschwerte Aufgabenstellung soll mit KI bewältigt werden, wobei selbst einfache KI-Applikationen eine Herausforderung bei der Nachweisführung zur Sicherheit darstellen. Der Einsatz von KI für einfache Anwendungen, etwa einer Auswertung von sicheren elektronischen Signalen, ist aber hinsichtlich des Marktes und der Forschung weniger attraktiv, auch wenn dies zur Erarbeitung von geeigneten Methoden anfangs angezeigt wäre.

Im Rahmen der Normung werden daher mögliche Vorgehensweisen diskutiert und sollen im technischen Bericht (ISO/IEC TR 5469 der JTC 1/SC 42/WG 3) beschrieben werden.

Klassifikation von KI für Sicherheitsaufgaben

Ausgangpunkt der Betrachtungen bleibt die Risikoanalyse, welche angemessen auf die Gegebenheiten in verschiedenen Einsatzbereichen angewandt werden kann. Zusam-

Bild: Shutterstock

men mit der vorgeschlagenen Klassifizierung (nach *Bild 2*) zum sicherheitstechnischen Kontext der KI können gezielt Empfehlungen hinsichtlich der Evaluation zugeordnet werden.

Die KI-Klassifizierung stellt den Kontext des Einsatzes von KI-Methoden/Techniken bezogen auf das E/E/PE-System (electrical and/or electronic and/or programmable electronic system; nach IEC 61508) dar, und zeigt die Bereiche auf, für welche KI nach bestehenden Regeln der Technik begutachtungsfähig ist, oder in denen noch Kriterien und Anforderungen zu erarbeiten sind.

Die Anwendungslevel A bis D sollen bei der Zuordnung von Anforderungen zum jeweiligen Einsatzzweck helfen:

- Die Anwendungslevel C und D verwenden bestehende Sicherheitskonzepte zur Risikoreduktion. Künstliche Intelligenz spielt hier noch keine Rolle.
- Der Anwendungslevel B bezeichnet den Einsatz von KI im Rahmen der Entwicklung von Safety-Systemen.
- Anwendungslevel A steht für den direkten Einsatz von KI in einer Sicherheitsfunktion. Die angefügten Kennzahlen ‚1' und ‚2' bezeichnen die Entscheidungshoheit der KI, wobei zum Beispiel ‚A1' für den direkten Einsatz im sicherheitsrelevanten Hauptkanal und ‚A2' für einen indirekten Einsatz, etwa im Rahmen von Diagnosen, steht.

Die KI-Klassen sind nicht technologiebezogen zu sehen, das heißt, bestimmte Techniken wie neuronale Netze oder Machine Learning gehören nicht automatisch in eine bestimmte Klasse:

KI Klasse I bezieht sich beispielsweise auf bestehende klassische Verfahren, ein sicheres ‚intelligentes System' zu entwickeln, zum Beispiel nach IEC 61508. Dabei ist der zugrundeliegende Code und dessen Wirkung vollständig nachvollziehbar und für den Entwickler verständlich.

Bei KI Klasse II handelt es sich nun um ein System, welches sich KI-Methoden/Techniken bedient, die nicht in allen Punkten zu vom Menschen nachvollziehbaren Ergebnissen führt, aber es trotzdem durch erweiterte Maßnahmen möglich ist, angemessene Kriterien und Anforderungen zu erfüllen. Diese Kriterien sind noch zu erarbeiten.

Bild 1. Bekannte strukturierte Szenarien für Sicherheitsapplikationen mit KI zu erschließen, wäre der nächste logische Schritt im Rahmen der evolutionären Entwicklung von Technologie. Als Beispiel ist die Objekterkennung bei Fahrzeugen zu nennen.

	KI Klasse I Begutachtung möglich	KI Klasse II Begutachtung teilweise nicht möglich, aber mit zusätzlichen Maßnahmen anwendbar	KI Klasse III Begutachtung nicht ausreichend möglich, zusätzlich Maßnahmen nicht ausreichend
Anwendungslevel A KI im E/E/PE-System zur Diagnose (A2) oder sogar Steuerung (A1)	Bestehende Normen zu risikominimierende Maßnahmen der Funktionalen Sicherheit können angewandt werden.	***Bereich der zu erarbeitenden Kriterien und Anforderungen***	Nicht empfohlener Einsatz
Anwendungslevel B1 oder B2 KI in der Entwicklung eines E/E/PE-System als Support Tool (B2) oder sogar Validierungs-Tool (B1)			
Anwendungslevel C KI nicht sicherheitsrelevant, aber mit Rückwirkung			
Anwendungslevel D KI nicht sicherheitsrelevant, ohne Rückwirkung	Bestehende risikominimierende Maßnahmen der Funktionalen Sicherheit können angewandt werden.		

Bild 2. KI-Klassifizierung entsprechend den derzeitigen Normungsprojekten.

Die KI Klasse III liegt außerhalb der Möglichkeiten der Klasse II und ist letztlich nur bei Systemen des Anwendungslevel D einsetzbar, die sich hinsichtlich der Sicherheit nicht auf die KI verlassen müssen.

Der Mensch als intelligente Instanz

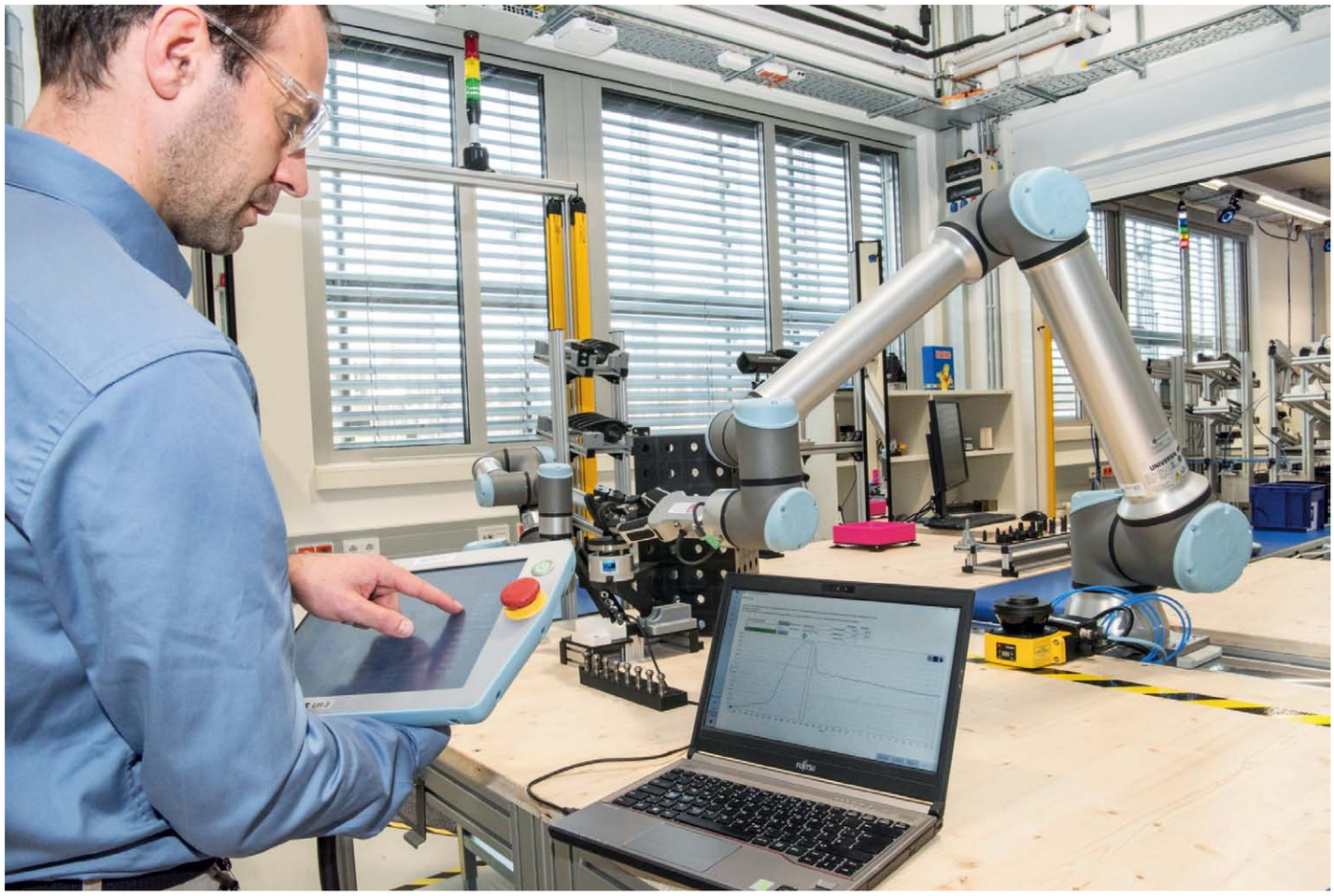
Die Tabelle zeigt, dass es durchaus angemessen sein kann, zur Bewertung bestimmter Applikationen bestehende Normen wie die IEC 61508 zu verwenden. Und zwar immer dann, wenn es sich um eher klassische Verfahren von simulierter Intelligenz (KI Klasse I) handelt. Denn was ein Mensch als intelligentes Verhalten eines Systems ansieht, unterliegt ohnehin der Subjektivität und stellt auch die anfangs diskutierte Schwierigkeit bei der Definition von KI dar.

Diese Klassifizierung der KI-Applikationen kann im Rahmen der Risikoanalyse helfen geeignete Räume für den KI-Einsatz, auch im sicherheitstechnischen Zusammenhang, zu eröffnen, wobei der bestehende Stand der Technik berücksichtigt wird. Herausfordernd wird die Erarbeitung konkreter Anforderungen sein, um die KI Klasse II mit geeigneten Methoden für bestimmte KI-Technologien ausreichend sicherheitstechnisch bewerten zu können.

Abschließend bleibt festzuhalten, dass bei allen Betrachtungen zu KI der Mensch als intelligente Instanz relevant ist, sowohl bei der Definition des Einsatzes und der Auswahl der zugrundeliegenden Daten, als auch bei der Ausarbeitung des KI-Algorithmus selbst. Wäre dies nicht mehr der Fall, wäre der Mensch auch für die weitere Evolution irrelevant geworden. Soweit ist die Entwicklung der KI allerdings noch nicht absehbar, jedoch sind die Auswirkungen der menschlichen Entscheidungen im Rahmen der Entwicklung und des Betriebs der KI deutlich weitreichender, als dies in der Breite wahrgenommen wird. *ag*

HOLGER LAIBLE
ist Senior Safety Expert bei Siemens.

Bilder: Siemens



Die Evaluierung der physischen Sicherheit

Kommen Roboter als kollaborative Assistenzsysteme in einer modernen Produktion zum Einsatz, werden sie ohne Schutzzaun betrieben. Beim Fehlen einer solchen trennenden Schutzeinrichtung spielt die physische Sicherheit für die beteiligten Arbeiterinnen und Arbeiter eine sehr wichtige Rolle.

Für die Digitalisierung und Automatisierung in der Produktion benötigt es moderne Robotersysteme, die ihre Aufgaben nicht nur richtig, sondern auch für den Menschen gefahrenfrei ausführen. Besonders wichtig wird die Sicherheitsfrage, wenn diese Systeme nicht nur in speziell für Roboter vorgesehenen Produktionsbereichen zum Einsatz kommen, sondern als sogenannte ‚Cobots' operieren. Anders als klassische Industrieroboter operieren diese speziell für die Zusammenarbeit mit Menschen entwickelten Roboter mit ebendiesen in einem Arbeitsbereich, um auch gemeinsam Produktionsschritte erledigen zu können. Aufgrund der engen Zusammenarbeit kann nicht ausgeschlossen werden, dass es zu ungewollten physischen Kontakten zwischen Roboter und Mensch kommt.

Um die Sicherheit einer Mensch-Roboter-Kollaboration zu definieren, braucht es klar strukturierte Regeln. Neben der EG-Maschinenrichtlinie 2006/42/EG definieren harmonisierte Normen und Vorschriften für Robotersicherheit den regulativen Rahmen für ein sicheres Zusammenarbeiten von Menschen und Roboter im industriellen Anwendungskontext – insbesondere die ISO 10218:2011 (Industrieroboter-Sicherheitsanforderungen) und die ISO/TS 15066:2016 (Roboter und Robotikgeräte – Kollaborierende Roboter). Das Besondere bei Cobots sind deren erweiterte Ausstattung mittels zusätzlicher, hochzuverlässiger Sensorik sowie ihre Fähigkeit, sicherheitsbewertete Funktionen realisieren zu können, die über den verpflichtenden Not-Halt hinausgehen. Beispielsweise kann der

Bilder: Joanneum Research

Roboter mit einer erhöhten Zuverlässigkeit seine Position und Geschwindigkeit überwachen und begrenzen.

Teil 2 der ISO 10218, der sich mit der Sicherheit von Robotersystemen beschäftigt, beschreibt die relevanten sicherheitstechnischen Maßnahmen für einen kollaborativen Roboterbetrieb. Hierfür werden vier klar umrissene Szenarien für die physische Kollaboration zwischen Menschen und Roboter definiert. Eine vorab festgelegte Aufgabenausführung, die Aktivierung aller erforderlichen Schutzmaßnahmen sowie die Verwendung eines für den kollaborierenden Betrieb konstruierten Roboters (Cobot) stellen die Ausgangsbasis für diese Interaktionsszenarien dar. Die vier Möglichkeiten sind:

- Sicherheitsbewerteter überwachter Halt (und Wiederanlauf)
- Handführung
- Geschwindigkeits- und Abstandsüberwachung
- Leistungs- und Kraftbegrenzung

Für moderne Roboteranwendungen sind vor allem die letzteren zwei Betriebsarten von großem Interesse.

Physische Robotersicherheit und deren Evaluierung

In klassischen Robotersystemen werden bauliche und funktionale Sicherheitsmaßnahmen genutzt, um ein ungewolltes Aufeinandertreffen von Mensch und Roboter zu verhindern. Diese Vorkehrungen sind vor allem dann notwendig, wenn bewegte Teile des Roboters sowie die Roboterumgebung nicht sicherheitsbewertet überwacht werden und diese Objekterfassung zur Kollisionsvermeidung herangezogen wird. Aufgrund der unzureichend verfügbaren sicherheitsbewerteten Sensorik zur validen Umgebungserfassung stößt die Betriebsform ‚Geschwindigkeits- und Abstandsüberwachung' momentan noch an ihre Grenzen in der Anwendbarkeit. Dies ist auch einer der Hauptfaktoren, weshalb diese Kollaborationsform meist noch im Laborumfeld im Zuge von Forschungsarbeiten untersucht wird und nur vereinzelt im industriellen Kontext Einsatz findet.

Im Gegensatz dazu stellt die Betriebsart ‚Leistungs- und Kraftbegrenzung' aktuell die am weitesten verbreitete kollaborative Betriebsform dar. Wie die Bezeichnung schon gut beschreibt, werden dabei die Leistungsparameter der elektrischen Antriebe in den Robotergelenken sowie die Sensitivität der Regelung in Form einer Kraftbegrenzung derart eingestellt, dass im Fall einer Mensch-Roboter-Kontaktsituation die vom Roboter zum Mensch übertragene Stoßenergie unterhalb der normativen Vorgaben liegt.

Identifikation potenzieller Gefahrensituationen

Als erster Schritt müssen also potenziell gefahrbringende Kontaktsituationen im Rahmen der bestimmungsgemäßen Verwendung des Robotersystems sowie bei vorhersehbarer Fehlanwendung in einer entsprechenden Risikobeurteilung identifiziert werden. Dabei sind die Mindestvorga-

Das Prüflabor

Das Robotics Evaluation Lab (REL) – https://rel.joanneum.at/ – ist ein speziell eingerichtetes Mess- und Prüflabor der Joanneum Research Forschungsgesellschaft am Institut Robotics mit Standort Klagenfurt am Wörthersee. In diesem Labor können biofidele Belastungen bei Kontaktsituationen in Roboterapplikationen rückführbar und valide gemessen und bewertet werden. Hierfür werden kalibrierte Messmittel am neuesten Stand der Technik verwendet und der gesamte Prüfprozess unter qualitätssichernden Maßnahmen nach ISO/IEC-17025 durchgeführt. Als erste und einzige Prüfstelle in Europa konnte das Robotics Evaluation Lab die Akkreditierung zur Messung der potenziellen Krafteinwirkung in der Mensch-Roboter Kollaboration erlangen. Die Prüfungen werden je nach Kundenspezifikation in den Räumlichkeiten des REL oder direkt vor Ort an der Anlage des Kunden durchgeführt.
Zudem unterstützt das Prüflabor die Wirtschaft und Industrie mit Dienstleistungen und Services rund um die Themen projektbegleitende Beratungsleistungen, eigenständig durchgeführte Sicherheits- und Risikobeurteilungen sowie kompetenzsteigernde Weiterbildungen im Bereich der Robotersicherheit. Durch die Mitarbeit in nationalen und internationalen Normungsgremien sind die Expertinnen und Experten des Prüfteams über die Entwicklung dieses Themenkomplexes stets am neuesten Stand und können auf Basis ihres praxisrelevanten Know-hows Trends aktiv mitgestalten. Unter dem Motto ‚Safety as a Service' werden maßgeschneiderte und praxisorientierte Dienstleistungspakete für den gesamten Entwurfs- und Lebenszyklus von Roboteranlagen angeboten.

Die Robotics Hands-on Area ist eine modular aufgebaute Test- und Verifikationsplattform, in der unterschiedlichste industrielle Anwendungsfälle nachgestellt sowie deren physische Sicherheit nachgewiesen werden kann.

ben der Maschinenrichtline sowie die Grundsätze der Normen ISO 12100 und ISO 10218 einzuhalten. Identifizierte mechanische Gefährdungen können in Form von Quetsch- oder freien Stoßsituationen auftreten. Bei Quetschsituationen – sogenanntem quasistatischen Kontakt – wird ein Körperteil (zum Beispiel Hand oder Arm) zwischen einem bewegten Roboterteil und einem starren Umgebungsobjekt eingeklemmt. Bei freien Stoßsituationen – dem sogenannten transienten Kontakt – ist die Belastung nur von kurzer Dauer, da das am Stoß beteiligte menschliche Körperteil (zum Beispiel Schulter) zurückweichen kann.

Laut den Anforderungen der Sicherheitsnorm für kollaborative Robotik ISO/TS 15066 müssen genau diese beiden Belastungsarten – also ein quasistatischer Belastungswert für den Fall einer Klemmung und ein transienter Belastungswert für den Fall einer Stoßbelastung – für die laut Risikobeurteilung gefahrbringenden physischen Kontaktsituationen evaluiert werden.

Für die Evaluierung einer Mensch-Roboter-Kontaktbelastung müssen sowohl die Kontaktkraft als auch der zugehörige Kontaktdruckwert erfasst werden. Die Norm ISO/TS 15066 enthält für eine Konformitätsbewertung eine Vergleichstabelle mit aus entsprechenden Studien ermittelten Grenzwerten für den menschlichen Schmerzeintritt bei Kraft- und Druckbelastung an unterschiedlichen Körperstellen. Die gemessenen quasistatischen beziehungsweise transienten Kraft- und Druckwerte werden unter Berücksichtigung der Messunsicherheit mit diesen Vorgaben verglichen. Werden die Grenzwerte überschritten, müssen risikomindernde Maßnahmen getroffen werden. Im Fall einer zu hohen Kraftbelastung sind dies typischerweise eine Reduktion der Bewegungsgeschwindigkeit oder eine Erhöhung der Robotersensitivität bezüglich des Abschaltverhaltens bei zu hoher Drehmomentbelastung der Gelenkantriebe. Bei zu hoher Druckbelastung führt meist eine bauliche Modifikation des Roboterwerkzeuges oder einer Werkstückhalterung zur Erhöhung der Kontaktfläche zum Erreichen der geforderten Grenzwerte – etwa durch das Abrunden oder Polstern von scharfen Kanten.

Messtechnische Verifikation

Während der Entwurfsphase können für den Nachweis der physischen Robotersicherheit, also der Konformität von potenziellen transienten und quasistatischen Kontaktbelastungen, rechnergestützte Werkzeuge wie Simulation, virtuelle Inbetriebnahme und digitale Abbilder der Anlage einen wertvollen Beitrag leisten. Aber: Derzeit kann noch keine Simulationssoftware eine messtechnische Evaluierung direkt an der realisierten kollaborativen Roboteranlage ersetzen. Zudem ist diese messtechnische Untersuchung unerlässlich, um die Gewissheit zu liefern, ob es sich um ein zuverlässiges und somit sicheres Verhalten des Robotersystems handelt.

Bei der messtechnischen Verifikation werden potenzielle Kollisionen von Mensch und Roboter im Sinne eines zerstörungsfreien Crash-Tests mittels einer sogenannten biofidelen Messanordnung untersucht. Biofidel bedeutet, dass die Messgeräte (Kraft- und Druckmessinstrument) so ausgestattet werden, dass die Nachgiebigkeits-Eigenschaften der am Kontakt beteiligten Körperstelle technisch nachgebildet werden. Realisiert wird dies über eine Kombination aus Stahlfedern und Dämpfungselementen aus Kunststoff. Anschließend wird die Messanordnung entsprechend im Arbeitsraum des Roboters positioniert und die zu evaluierende Kontaktsituation durch die Ausführung des entsprechenden Steuerprogramms herbeigeführt. Dabei werden Kraft- und Druckbelastungen ermittelt sowie deren Konformitätsbewertung gegenüber normativen Vorgaben, wie oben beschrieben, duchgeführt. Um die Validität der Ergebnisse zu garantieren, sollen qualitätssichernde Maßnahmen nach ISO 17025 (Allgemeine Anforderungen an die Kompetenz von Prüf- und Kalibrierlaboratorien) eingehalten werden. Dies umfasst zyklische und akkreditierte Kalibrierungen von Messmittel, Eignungsprüfungen und Teilnahme an Ringversuchen, adäquate Dokumentation von Mess-Ergebnissen in Prüfberichten und die Abhandlung von Prüfprojekten durch ein geeignetes QM-System. *ik*

MICHAEL RATHMAIR
ist Leiter der Kompetenzgruppe Robotics Evaluation Lab bei der Joanneum Research Forschungsgesellschaft in Klagenfurt, Österreich.

Sicherheit für den Einrichtbetrieb

Für den Einrichtbetrieb oder die Störungsbeseitigung an Maschinen ist die Sicherheitsfunktion ‚Sicher begrenzte Geschwindigkeit bei geöffneter Schutztür' relevant. Nachfolgend eine exemplarische Sicherheitslösung mit redundantem Drehgeber und Sicherheitssteuerung.

Bei größeren Maschinen oder Anlagen – zum Beispiel in der Verpackungsindustrie – ist der Bediener in der Regel durch einen Schutzzaun oder eine Umhausung vor gefährlichen Bewegungen geschützt. Ein Zugang zum Gefahrenbereich ist über eine Tür möglich. Unter dem Gesichtspunkt der Maschinensicherheit muss dabei neben den Sicherheitsfunktionen ‚Schutz vor unerwartetem Anlauf' und ‚Stillsetzen über Not-Halt-Einrichtung' oft eine weitere Sicherheitsfunktion gewährleistet sein: die ‚sicher begrenzte Geschwindigkeit (SLS) bei geöffneter Schutztür'. Die SLS-Funktion vereinfacht es für den Bediener, eine Fertigungsanlage einzurichten oder eine Störungsbeseitigung durchzuführen.

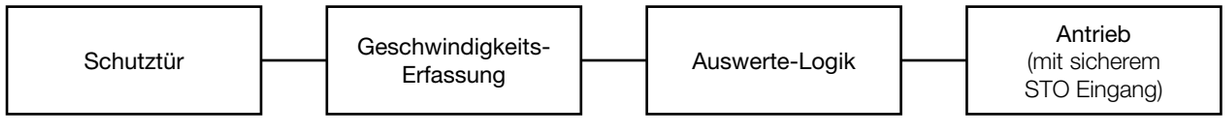
Ein aktuelles Whitepaper von Schmersal und Wachendorff stellt eine exemplarische Sicherheitslösung für eine solche Anlage vor, zu der unter anderem ein redundanter Drehgeber sowie eine Sicherheitskleinsteuerung gehören, und gibt eine Hilfestellung für die Bewertung der sicherheitstechnischen Tauglichkeit dieser Lösung. Um das geforderte Sicherheitsniveau zu bestimmen und zu belegen, wird bei diesem Beispiel die Normenreihe EN ISO 13849 angewendet. Für die betrachtete Maschine hat die Risikobewertung einen Performance Level (PLr) von d ergeben. Dieser lässt sich auf verschiedene Arten umsetzen. Für die technische Realisierung bietet sich zumeist die Kategorie 3 an. Sie fordert eine Einfehlersicherheit, die typischerweise durch eine konsequent zweikanalige Auslegung erreicht wird.

Zur Messung der Geschwindigkeit bietet sich die Verwendung eines Drehgebers an. Neben dem Drehgeber, der Auswertelogik – etwa der Sicherheitssteuerung ‚PSC1' von Schmersal – und dem Antrieb selbst muss meistens die Überwachung der Schutztür in die Betrachtung einfließen, da die SLS-Funktion im Allgemeinen mit dieser Schutztür aktiviert wird.

In dieser Struktur ist insbesondere die Betrachtung des Drehgebers zur Geschwindigkeitserfassung relevant.

Am einfachsten ließe sich die geforderte Zweikanaligkeit durch zwei separate Geber realisieren, die an verschiedenen Stellen montiert sein müssten, um auch mechanisch zweikanalig zu sein. ‚Allerdings gestaltet sich dies in der Praxis oft aufwendig und schwierig. Praktikabler ist es, nur eine Montageposition verwenden zu müssen. Der Drehgeber der Firma Wachendorff vereint diese beiden Eigenschaften: Er besteht aus zwei voneinander vollständig unabhängigen Gebern unterschiedlicher Technologien in einem Gehäuse. Neben der dadurch vereinfachten Montage erlaubt es die interne Redundanz zudem, die Anforderungen der Kategorie 3 zu erfüllen.

Bilder: Schmersal



Eine exemplarische Struktur der Sicherheitsfunktion: Neben dem Drehgeber zur Erfassung der Geschwindigkeit, der Auswertelogik, wie zum Beispiel der Sicherheitssteuerung ‚PSC1' von Schmersal, und dem Antrieb selbst muss zumeist auch die Überwachung der Schutztür mit in die Betrachtung einfließen, da die SLS-Funktion im Allgemeinen mit dieser aktiviert wird.

Der redundante Drehgeber

Ein redundanter Drehgeber besteht im Grundsatz aus zwei komplett autarken Standard-Drehgebern, wodurch der gesamte elektronische Teil des Drehgebers als zweikanaliges System zu betrachten ist. Einzig der mechanische Aufbau, bestehend aus Welle und Lagerpaket, ist einkanalig ausgeführt. Die Norm für elektrische Antriebe EN 61800-5-2 sieht die Betrachtung des Fehlerfalls durch das Lösen der mechanischen Verbindung zwischen Drehgeber und Antrieb vor. In vielen Fällen wird ein Fehlerausschluss benötigt, da die Steuerung einen derartigen Fehler nicht zwingend aufdecken kann. Dieser Fehlerausschluss lässt sich erreichen, indem die Anbauelemente entsprechend stark dimensioniert ausgelegt werden und eine 100 % zuverlässige mechanische Verbindung genutzt wird.

Die Drehgeber von Wachendorff setzen auf das Prinzip der Diversität. Dies bedeutet, dass gezielt die Ausfallsicherheit erhöht wird, indem verschiedene Messprinzipien eingesetzt und dadurch so wenig baugleiche Komponenten verwendet werden wie möglich. Grundgedanke dabei ist, dass die unterschiedlichen Sensorik-Plattformen auch verschieden empfindlich beziehungsweise unempfindlich auf Störungen jeglicher Art reagieren und dadurch nicht zeitgleich ausfallen, sodass die nachgeschaltete Elektronik diesen möglichen Ausfall sicher erkennen kann.

Der redundante Standarddrehgeber stellt diversitäre (magnetisch und optisch) Signale zur Verfügung, die vollständig unabhängig voneinander erzeugt werden, aber dennoch in Korrelation zueinander gebracht werden können. Selbst die Versorgungsspannung ist für jede Sensoreinheit separat vorhanden.

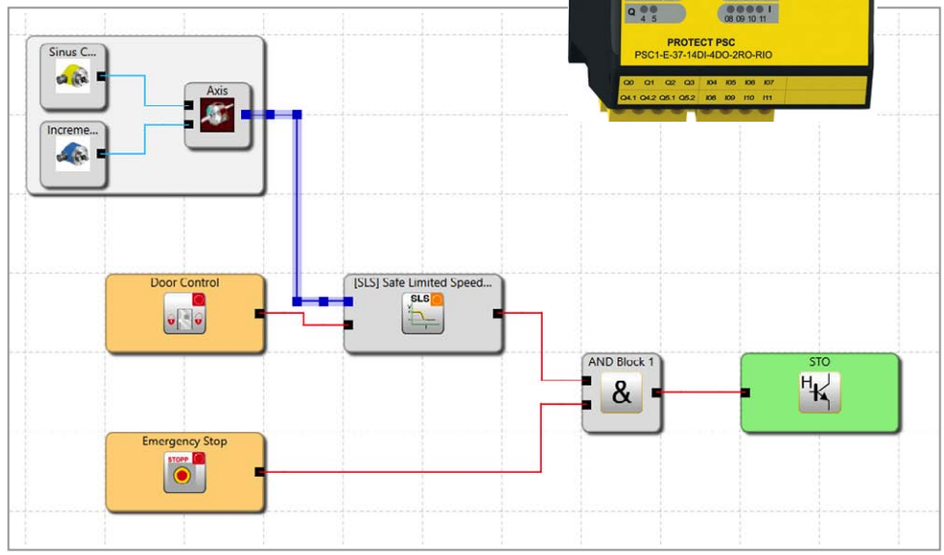
Subsystem ‚Geschwindigkeitserfassung'

Die von Kategorie 3 geforderte Einfehlersicherheit ist durch die durchgängige Zweikanaligkeit der Geschwindigkeits-/Richtungserfassung im Drehgeber gegeben. Die ebenso geforderte Fehleraufdeckung (DC) ist nicht in den Geber integriert, muss also in der Auswertelogik erfolgen.

Exemplarisch steht hier die Sicherheitssteuerungs-Reihe ‚PSC1' von Schmersal. Mit ihr können – wenn es die Applikation erfordert – bis zu zwölf Achsen sicher überwacht werden. Hierbei lassen sich die Drehgeber einfach über D-Sub-Schnittstellen anschließen. Durch Kreuzvergleich der beiden Gebersignale oder im Fall von sin-cos-Gebern durch Auswertung der Relation $\sin^2+\cos^2=1$ werden auftretende Fehler erkannt und eine Fehlerreaktion eingeleitet. Zudem sind im Programmiertool ‚SafePLC2' der ‚PSC1' bereits Funktionsblöcke für die wichtigsten Überwachungsfunktionen entsprechend der DIN EN 61800-5-2 vorhanden, beispielsweise SLS, SOS (Safe Operating Stop) oder SCA (Safe Cam, sichere Positionsüberwachung). Diese lassen sich einfach in das Programm der Sicherheitslogik integrieren.

Fehlerausschluss

Besondere Aufmerksamkeit gilt der mechanischen Kopplung zwischen Geber und Antrieb, die prinzipbedingt nur einkanalig ausgeführt ist. Dies macht einen Fehlerausschluss auf Versagen dieser Verbindung notwendig, da hier bereits der einzelne Fehler eine gefährliche Situation herbeiführen würde.



Die Sicherheitsteuerung PSC1 und die Programmierung der Anwendung in SafePLC2. Die Kategorie 3 fordert unter anderem Fehleraufdeckung (DC). Diese erfolgt in dem beschriebenen Beispiel über die Sicherheitsteuerung ‚PSC1'. Im Programmiertool ‚SafePLC2' der ‚PSC1' sind bereits Funktionsblöcke für die wichtigsten Überwachungsfunktionen integriert und aufgrund der einfachen Programmierung wird die Wahrscheinlichkeit von Fehlern minimiert.

Neben einem Nachweis der maximalen Belastbarkeit der Verbindung fordert die Norm EN ISO 13849, dass für diesen Fehlerausschluss eine FMEA (Fehlermöglichkeits- und -Einflussanalyse) durchgeführt wird.

Zu den weiteren Aspekten, die gemäß EN ISO 13849 zur Erfüllung der Kategorie 3 notwendig sind, zählen Maßnahmen zur Vermeidung von Ausfällen gemeinsamer Ursache (CCF Common Cause Failure), die Vermeidung systematischer Ausfälle in der Software der Sicherheitskleinsteuerung, die Berechnung einer Ausfallwahrscheinlichkeit der Steuerungslösung auf Basis von MTTFD-Werten (Mean time to failure dangerous) und/oder eine höherwertige Diagnose (DC – Diagnostic Coverage). Unter Einbeziehung dieser Aspekte wird im Whitepaper schließlich der Performance Level für diese exemplarische Sicherheitslösung berechnet. Siehe dazu auch:
https://bit.ly/2R7hqiN

Mit der beschriebenen Struktur lässt sich ein Performance Level von d erreichen. Begrenzt wird der mögliche PL in der Beispielrechnung im Wesentlichen durch den PL des Frequenzumrichters. Trotz des teilweisen Einsatzes von Standardkomponenten ist es also möglich, ein hohes Sicherheitsniveau zu erzielen. Die Verwendung des redundanten Gebers erleichtert die Montage. Und in Verbindung mit der Sicherheitskleinsteuerung ‚PSC1' ist auch die Realisierung weiterer Sicherheitsfunktionen wie Not-Halt oder die Überwachung weiterer Sicherheitskreise mit nur einem Gerät möglich. *ik*

CHRISTIAN LUMPE
ist Produktmanager Steuerungen bei der Schmersal Gruppe in Wuppertal.

STEFFEN NEGELI
ist Produktmanager und Mitarbeiter im technischen Vertrieb bei Wachendorff Automation in Geisenheim.

STORMSHIELD

Konrad-Zuse-Platz 8
D-81829 München
Germany
Tel. +49 89 8091 3578 – 0
dach@stormshield.eu

Firmenprofil / Firmenausrichtung

Stormshield ist ein europäisches, auf Cybersicherheit für kritische Infrastrukturen und Daten spezialisiertes Unternehmen des Airbus-Konzerns. Mit den über zwanzig Jahren Erfahrung in der Entwicklung von einander ergänzenden Lösungen zur Absicherung von Unternehmens- und Industrienetzwerken (Stormshield Network Security), Arbeitsplätzen und Servern (Stormshield Endpoint Security) und Daten (Stormshield Data Security) verfolgt der Hersteller einen ganzheitlichen, kollaborativen Security-Ansatz zum erfolgreichen Schutz von sensiblen IT- und OT-Infrastrukturen auch gegen unbekannte Bedrohungen.

Die Cybersicherheitslösungen von Stormshield sind nach den höchsten europäischen Standards zertifiziert (EU RESTRICTED, NATO, ANSSI EAL3+/EAL4+) und werden über ein solides Partnernetz in über 40 Ländern weltweit vertrieben. Die innovativen, verhaltensbasierten Stormshield-Technologien sind die richtige Antwort auf IT- und OT-Risiken und sichern strategische Informationen von Unternehmen aller Größen, sowie Behörden und militärischen Organisationen weltweit ab. Die Netzwerksicherheitslösungen für die Industrie sind speziell darauf ausgelegt, die IT/OT-Konvergenz zu fördern und beide Umgebungen zu schützen. Die Industrie-Firewalls sind in der Lage, in Echtzeit die Legitimität von Informationen und Befehlen zu überprüfen, die von Steuerungssystemen direkt an Maschinen gesendet und sowohl über IT- als auch Industrieprotokolle übertragen werden. Jedes abnormale Verhalten im Datenfluss, das auf eine mögliche Manipulation der Befehle oder auf einen Cyberangriff hinweist, wird in Echtzeit signalisiert und/oder blockiert.

Impressum

Anschrift des Verlages
WEKA FACHMEDIEN GmbH
Richard-Reitzner-Allee 2
85540 Haar
Telefon: 089.255 56 – 10 00
Telefax: 089.255 56 – 16 70
www.weka-fachmedien.de

Redaktion
redaktion@computer-automation.de

Assistenz
Simone Schiller
Telefon: 089.255 56 – 10 84
E-Mail: SSchiller@weka-fachmedien.de
www.weka-fachmedien.de

Chefredakteurin
Dipl.-Ing. (FH) Andrea Gillhuber (ag) verantw.
Telefon: 089.255 56 – 10 39
E-Mail: AGillhuber@weka-fachmedien.de

Senior Advisory Editor
Dipl-Ing. (FH) Meinrad Happacher (hap)
Telefon: 089.255 56 – 10 85
E-Mail: MHappacher@weka-fachmedien.de

Chefin vom Dienst
Elisabeth Skowronek
Telefon: 089.255 56 – 13 34
E-Mail: ESkowronek@weka-fachmedien.de

Redaktion
Inka Krischke M.A. (ik)
Telefon: 089.255 56 – 13 73
E-Mail: IKrischke@weka-fachmedien.de

Herstellungsleitung
Marion Stephan, 089.255 56 – 14 42

Herstellung/Sonderdrucke
Andreas Hofner
Telefon: 089.255 56 – 14 50
E-Mail: AHofner@wekanet.de

Verlagsleitung
Peter Eberhard

Sales Director
Tiffany Dinges verantw. 089.255 56 – 13 63
E-Mail: tdinges@weka-fachmedien.de

Key Account Manager
Christine Gässler 089.255 56 – 13 08
E-Mail: cgaessler@weka-fachmedien.de

Mediaberatung
Andreas Zepf 089.255 56 –13 64
E-Mail: azepf@weka-fachmedien.de

Disposition
Nadine Ziegler 089.255 56 –14 73
DISPO.ComputerundAutomation@wekanet.de

Anzeigenpreise nach Preisliste vom 1. 1. 2021
Media-Information auf Anforderung

Druck L.N. Schaffrath GmbH & Co. KG
Marktweg 42-50, 47608 Geldern

Vertriebsleitung
Marc Schneider (089.255 56 – 15 09)
E-Mail: mschneider@weka-fachmedien.de

Bestell- und Abonnement-Service
WEKA FACHMEDIEN GmbH
c/o Zenit Pressevertrieb GmbH
Postfach 810640, 70523 Stuttgart, Tel. 0711.7252.210
E-Mail: abo@weka-fachmedien.de

Erscheinungsweise: 12 Ausgaben

Jahresabonnement Print Inland
78,40 €, davon 49,00 € Heft, 29,40 € Versand
Jahresabonnement Print Ausland
88,60 €, davon 49,00 € Heft, 39,60 € Versand
Einzelausgabe Print
7,50 €, zzgl. 3,00 € Versand
Preise jeweils inkl. der aktuellen MwSt.

Jahresbezug digitales E-Paper
(Inland/Ausland) 24,99 €
inkl. der aktuellen MwSt., ohne Versandkosten
Einzelausgabe digitales E-Paper
(Inland/Ausland) 2,99 €
inkl. der aktuellen MwSt. ohne Versandkosten

shop.weka-fachmedien.de

Geschäftsführung
Kurt Skupin, Matthäus Hose

ISSN 1615-8512

VERLAGSVERTRETUNGEN
Benelux, Skandinavien, Frankreich:
Huson International Media, Kingsfordweg 151,
1043 GR Amsterdam, The Netherlands
Tel. +31.20 491 77 44, Fax +31.20 491 77 45
Great Britain: Huson European Media, Mr. Gerald Rhoades-Brown, Cambridge House,
8 Gogmore Lane, Chertsey, Surrey, KT16 9AP,
phone: +44 (0) 1932.564 999,
fax: +44 (0) 1932.564 998
USA: Huson European Media, Mr. Ralph Lockwood,
Pruneyard Towers, 1999 South Bascom Avenue,
Suite 510, Campbell, CA 95008,
Tel. 1.408.879 66 66, Fax 1.408.879 66 69

AI015

Abonnementbestellung

Bitte ausschneiden und einsenden an: WEKA FACHMEDIEN GmbH, c/o Zenit Pressevertrieb GmbH, Postfach 81 06 40, 70523 Stuttgart, Tel. 0711.7252.210 oder per Fax an: 0711.7252.333
Ich bestelle Computer&AUTOMATION mit 12 Ausgaben jährlich zum Preis von z. Zt. 78,40 Euro inkl. 7 % MwSt. im Inland. Auslandspreis 88,60 Euro. Ich kann jederzeit kündigen.
Geld für bezahlte, aber noch nicht gelieferte Ausgaben erhalte ich zurück.

Firma _____ PLZ, Ort _____

Name, Vorname _____ Telefon* _____

Abteilung _____ Beruf _____ Fax* _____

Straße, Nr. _____ E-Mail* _____

❍ Ich bin damit einverstanden, dass die zu entrichtenden Abonnementgebühren
❍ vierteljährlich ❍ halbjährlich ❍ jährlich von meinem Konto abgebucht werden.

Kontonummer BLZ _____ Kreditinstitut _____

Datum, _____ Unterschrift _____

Ein gesetzliches Widerrufsrecht besteht nicht (§§ 505, 491 Abs. 2 Nr. 1 BGB).
WEKA FACHMEDIEN GmbH, Richard-Reitzner-Allee 2, 85540 Haar, HRB 119806 Amtsgericht München
Hinweis: Ihre Daten werden von uns zur Durchführung des Vertrages und für Direktmarketingzwecke verarbeitet und genutzt. Mit dem Ausfüllen stimme ich dem Erhalt von Serviceangeboten zu.
Die Zustimmung kann jederzeit durch Löschung der Kommunikationsdaten widerrufen werden.
* (Diese Angaben sind freiwillig.)

Seilzugschalter

Sicherer Halt fürs laufende Band

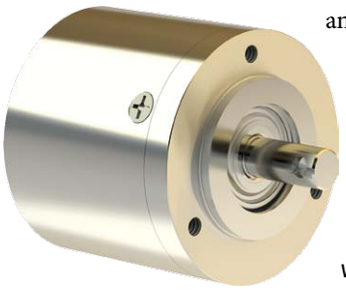
Für die Absicherung von Förderanlagen und Maschinen erweitert Pilz die Produktfamilie der Positions- und Näherungsschalter um den kompakten Seilzugschalter *PSENrope mini*. Die platzsparende Variante des Seilzugschalters ‚PSENrope' ermöglicht die Abschaltung von Funktionsprozessen per manueller Betätigung. Die mechanische Not-Halt-Funktion bei ‚PSENrope mini' lässt sich sowohl am integrierten Not-Halt-Taster als auch an jedem Punkt durch Ziehen des Seiles auslösen. Durch die Seillänge von bis zu 30 m können auch ausgedehnte Anwendungen mit nur einem Seilzugschalter bedient und abgesichert werden. Die Varianten des Seilzugschalters mit geradem oder gewinkelten Kopf tragen zu einer flexiblen Montage bei. Muss aufgrund des Maschinendesigns verdeckt eingebaut werden, kommt die Variante mit integriertem Reset-Taster zum Einsatz.
Das robuste Metall- oder Kunststoffgehäuse nach IP67 macht den Seilzugschalter sowohl für Indoor- als auch Outdoor-Anwendungen mit Umgebungstemperaturen von –30 bis +75 °C geeignet.

www.pilz.com

Sicherheits-Drehgeber

Erfüllen SIL 2 und PL d

Der *TRK38* von TWK ist ein Singleturn-Magnet-Drehgeber, der mit Blick auf sicherheitsgerichtete Anwendungen entwickelt wurde. Mit einem Durchmesser von nur 38 mm und einer Länge von ebenfalls 38 mm eignet sich der Sensor für die Montage in beengten Bauräumen; er wiegt circa 60 g. Der Safety-Drehgeber erfasst Position und Geschwindigkeit und erfüllt dabei die Anforderungen von SIL 2 (IEC 61508) und PL d (EN 13849). Die sicherheitsgerichteten Signale werden über eine zertifizierte Ethercat-FSoE-Schnittstelle übertragen. Die Positionsauflösung beträgt 16 Bit pro Umdrehung. Über die Ethercat-FSoE-Schnittstelle erfolgt die Übertragung der sicherheitsgerichteten Signale an die übergeordnete Steuerung beziehungsweise an ein Sicherheitsrelais sowie die Programmierung des Sensors.



Dank dem Aluminiumgehäuse sowie dem gesamten Design arbeitet der Sensor selbst unter ungünstigen Bedingungen wie Vibrations- und Stoßbelastungen.

www.twk.de

Servoantriebe

TÜV-zertifizierte Sicherheit

Synapticon bietet hochkompakte Servo Drives, deren Sicherheit vom TÜV Süd zertifiziert ist. Das jüngste TÜV-Zertifikat bestätigt die funktionelle Sicherheit hinsichtlich STO (Safe Torque Off) und SBC (Safe Brake Control) der *Circulo*-Serie. ‚Circulo' ist die aktuellste Klasse der ‚Somanet'-Reihe. Bei diesen ‚Integrated Motion Devices' handelt es sich um komplette Servo-Drive-Lösungen für die Integration am ‚Point of Motion'. Mit ihrer kreisrunden Form und großen Hohlwellen-Durchmessern von 20 bis 40 mm eignet sich die ‚Somanet Circulo'-Serie insbesondere für vollintegrierte Achsen, wie sie zum Beispiel bei Cobots, Servicerobotern oder Radnabenantrieben von AGVs zum Einsatz kommen.
Zunächst sind zwei Varianten verfügbar: ‚Circulo 7' und ‚Circulo 9', die sich durch Größe und Leistung unterscheiden. Beide sind für den Spannungsbereich bis 60 V ausgelegt. Die Servoantriebe verfügen über integrierte Encoder (19 bis 20 Bit) mit einer Multiturn-Option und besonderen Kalibrierungsfunktionen, die die Genauigkeit erhöhen.

www.synapticon.com

OT Security ist kein Feenstaub

Für die Cybersecurity von vernetzten Produktionsumgebungen besteht angesichts der volatilen Bedrohungslage dringender Handlungsbedarf. Eine zeitgemäße Strategie für OT Security kombiniert Regeln, Verfahren und Maßnahmen mit dem Defense-in-Depth-Prinzip und KI-gestützter Angriffserkennung – und berücksichtigt die wichtigsten OT-Security-Schutzziele von Anfang an.

Die zunehmende Vernetzung von Maschinen, Anlagen, industriellen Steuerungssystemen sowie Automatisierungslösungen hebt die bisherige physische Trennung der OT (Operational Technology) von anderen IT-Systemen auf. Für den Schutz der jetzt potenziell auch von außen angreifbaren OT-Netze sind klassische IT-Security-Lösungen oft nicht anwendbar. Häufig wird ein wirksamer Schutz durch veraltete Betriebssysteme, nicht erwünschte Eingriffe in laufende Prozesse, nicht umsetzbare Sicherheits-Updates oder nachträgliche Härtungsmaßnahmen verhindert. Jeder zweite erfolgreiche Angriff führte in der Vergangenheit zu Produktions- beziehungsweise Betriebsausfällen, so das Bundesamt für Sicherheit in der Informationstechnik (BSI).

Das Defense-in-Depth-Prinzip

Ein wirksamer Schutz für die Vertraulichkeit, Integrität und Verfügbarkeit von OT-Netzen ergibt sich aus dem Zusammenspiel

Bilder: Genua

von Regeln, Verfahren, Maßnahmen und Tools, wie sie unter anderem im Informations-Sicherheits-Management-System (ISMS gemäß ISO/IEC 27000) und der Norm für ‚Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme' (IEC 62443) definiert sind sowie unter dem Stichwort ‚Cyberresilienz' aktuell diskutiert werden (*siehe Kasten:* Cyberresilienz: Das neue IT-Security-Paradigma).

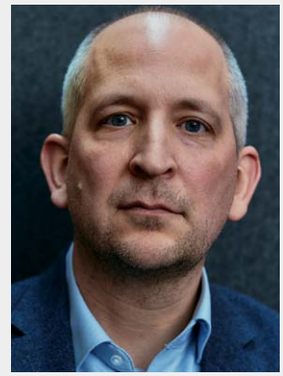
In der Norm IEC 62443 definiert das Defense-in-Depth-Prinzip (gestaffelte Verteidigung) den Schutz gegen Cyberangriffe in mehreren Schichten ähnlich einer Zwiebel: Auch wenn eine Sicherheitsschicht überwunden wurde, ist nur ein Teil des Netzes betroffen. Das Gesamtsystem ist durch weitere Sicherheitsebenen geschützt. Diesem Konzept folgend ist es sinnvoll, interne Netzwerke in unterschiedliche Sicherheitszonen aufzuteilen und gestaffelte Schutzlevel zu vergeben. So können besonders sensible Segmente von anderen Bereichen strikt getrennt werden. Die Zonenübergänge und die Kommunikation zwischen den Zonen können durch Industrial Firewalls und entsprechende Filterregeln restriktiv begrenzt werden.

Das Verhalten von Netzkomponenten überwachen

Das Netzmonitoring ist auch für OT-Netze eine geeignete Schutzmaßnahme, um die Anlagenkommunikation zu überwachen und auf Auffälligkeiten zu untersuchen. Hier setzt die KI-gestützte (KI –Künstliche Intelligenz) Anomalie-Erkennung an. „Sie ermöglicht die Erkennung untypischen Verhaltens und somit neben technischen Fehlerzuständen und Fehlkonfigurationen auch die Detektion bisher unbekannter Angriffsformen auf solche Netze", so die Cyber-Sicherheits-Empfehlung des BSI (BSI-CS 134).

Cyberresilienz: Das neue IT-Security-Paradigma

Interview mit Matthias Ochs, Geschäftsführer des Security-Spezialisten Genua.



Welche Voraussetzungen müssen für eine nachhaltige Cyberresilienz geschaffen werden?

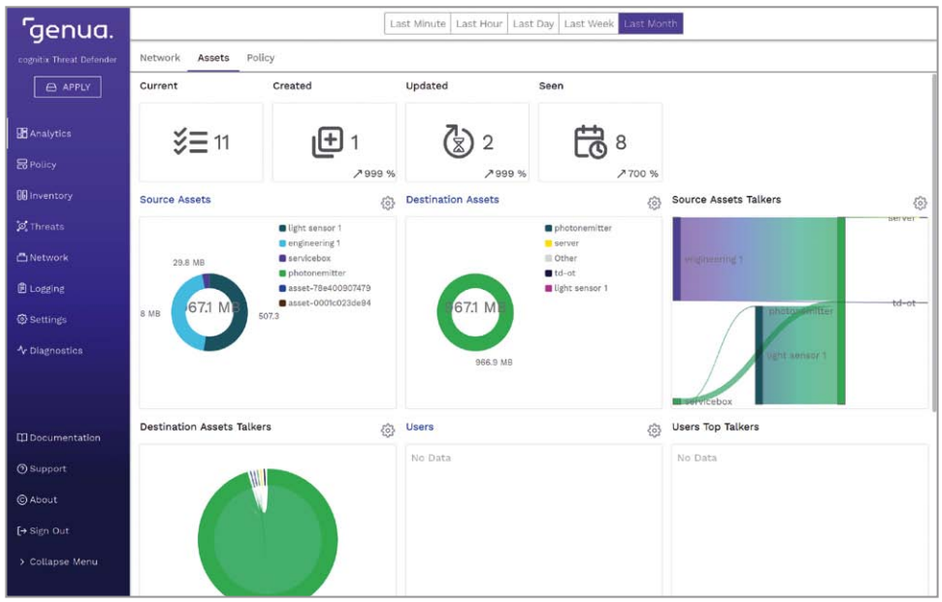
Matthias Ochs: Der Ausgangspunkt auf dem Weg zur Cyberresilienz ist eine fundierte Risikoanalyse der kritischen Geschäftsprozesse und die Definition möglicher Bedrohungen. Darauf aufbauend werden wirksame Maßnahmen zur Minimierung von Bedrohungslagen definiert. Der Fokus liegt dabei nicht auf hundertprozentiger, sondern adäquater Sicherheit. Für Risiken, die mit akzeptablem Aufwand nicht ausreichend zu reduzieren sind, müssen tragfähige Notfallpläne beschrieben werden. Verantwortlichkeiten, Führungsstrukturen und Kommunikationsprozesse werden auf Notsituationen ausgerichtet.

Wie kann dabei die hohe Komplexität beherrscht werden?

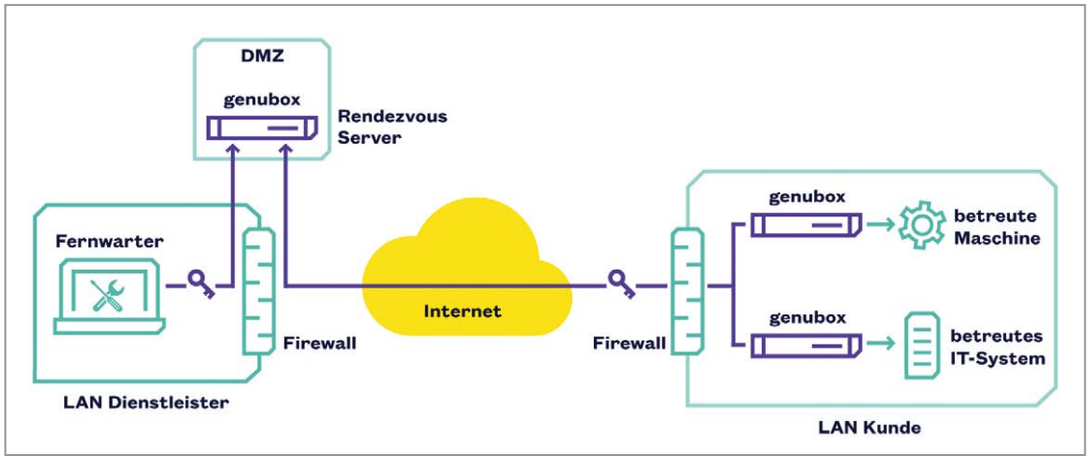
Der Schlüssel sind Prävention und frühe Detektion. Die hohe Komplexität macht Prävention zu einer anspruchsvollen Aufgabe, bei der klassische Firewall-Regeln und -Policies an ihre Grenzen kommen. KI-basierte Threat Defender bauen mittels Data-Analytics und Threat-Intelligence eine zweite Verteidigungslinie auf und ergänzen existierende Firewall-Lösungen. Industrie-Firewalls wie unsere genuwall schützen Produktionsnetze hochwirksam gegen Angriffe. Gleichzeitig sollte die Komplexität etwa durch klar definierte, minimale Schnittstellen weiter reduziert werden.

Welche organisatorischen Maßnahmen sind dabei wichtig?

Basierend auf Aufgaben und Verantwortlichkeiten müssen vor allem Sicherheitspolicies definiert werden. Ein Schwerpunkt liegt auf Identitäts- und dienstebasierten Zugriffskontrollen. Und schließlich bedarf es einer auf Cyberresilienz ausgerichteten IT-Sicherheitsorganisation. Ihre Initiierung hat tiefgreifende transformative Auswirkungen auf die gesamte Organisation und ist der Weg zu einem neuen IT-Security-Paradigma.



Wer spricht im OT-Netzwerk mit wem? Der KI-gestützte cognitix Threat Defender zeigt aufsummiert, welche Assets in der letzten Stunde oder in den letzten 30 Tagen wie viel Datenverkehr initiiert (Source Assets) beziehungsweise beantwortet (Destination Assets) haben, sowie den Datenverkehr zwischen den Assets. Basierend auf diesen Analysen können Policies festgelegt, überwacht und durchgesetzt werden.



Das Rendezvous-Konzept einer sicheren Fernwartung. Sichere Fernwartungslösungen erlauben den Zugang nur von innen nach außen und auch nur zu einer Sicherheitszone.

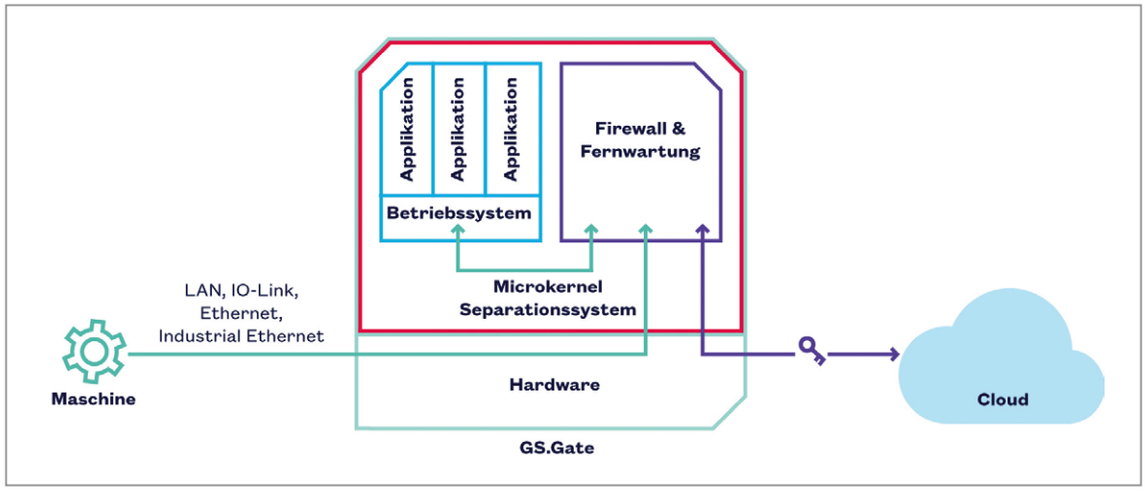


Schaubild zur Datenvorverarbeitung an der Edge. Sichere Edge-Gateways schotten Sicherheits-Gateway und Edge-Computing, also die Applikation, strikt ab.

Mit einem System zur Anomalie-Erkennung kann nicht nur der gesamte Netzwerk-Verkehr überwacht, sondern auch das Verhalten der Netzkomponenten (Assets) analysiert werden. Threat Defender richten hierfür ein überwachtes sicheres Netzwerk ein. Verhaltensmuster von Netzwerk-Geräten werden erkannt, klassifiziert und Regeln entsprechend der Klassifikation angewendet. Dabei werden bisher getrennte Funktionen wie Netzwerk-Analyse, Intrusion Detection, Asset Tracking und eine dynamische Policy Engine in einem System zusammengeführt.

Durch eine Bestandsaufnahme (Asset Tracking) des Netzwerks werden zunächst alle Devices und der gesamte Netzwerk-Verkehr im ‚Grundzustand' erfasst. Dabei wird die Kommunikation der Geräte untereinander analysiert und für die zulässige Kommunikation werden nach und nach Regeln angelegt. Wird jetzt eine unbekannte Kommunikation erfasst, muss gegebenenfalls die Policy nachjustiert werden. Anderenfalls stellt der neuartige Netzwerk-Verkehr eine Anomalie dar, die auf ein Problem oder gar eine Störung beziehungsweise einen Eindringling hinweist.

Netzwerk-Segmentierung sinnvoll

Darüber hinaus ist es sinnvoll, eine dynamische und transparente Segmentierung des Netzwerkes vorzunehmen. Welche Sicherheitsvorgaben für ein Gerät gelten, bestimmt sich dann nicht mehr nach dem Netzwerk-Port oder dem Switch, an dem das Gerät eingesteckt ist. Wie ein Gerät mit den anderen Teilnehmern des gleichen Netzwerkes oder anderer Netzwerke kommunizieren darf, entscheidet sich nun anhand der Funktion und des Verhaltens. Durch diese Zuordnung der Netzwerk-Komponenten können deren Security-Eigenschaften einzeln festgelegt und das Kommunikationsverhalten eingeschränkt werden.

Geschäftskritische Systeme und Prozesse lassen sich jetzt stärker abschotten. So kann beispielsweise der Datenverkehr von Produktionsanlagen mit dem SAP-System als besonders schützenswerter Prozess festgelegt werden. Um das zu erreichen, werden die Produktionsanlagen und Arbeitsstationen als SAP-Devices markiert und für diese Assets Regeln definiert. Darin können beispielsweise Priorisierungen im Datenverkehr, eine maximal Anzahl von Anfragen oder zugelassene Kommunikations-Protokolle festgelegt werden. So werden unerwünschte und problematische Zugriffe auf das SAP-System wirksam blockiert.

Fernwartungszugriffe zuverlässig absichern

Ein besonders sensibler Eingriff in das OT-Netz erfolgt durch die Fernwartung von Maschinen und Anlagen. Eine vertrauenswürdige Fernwartungslösung sorgt deshalb

Bilder: Genua

dafür, dass der Anlagenbetreiber über jeden Zugriff die Kontrolle behält. Sichere Fernwartungslösungen erlauben den Zugang nur von innen nach außen und auch nur zu einer Sicherheitszone. Dies kann mit einem sogenannten Rendezvous-Server mit integrierter Firewall umgesetzt werden, der in der demilitarisierten Zone (DMZ) installiert wird. Durch diese neutrale Zwischenebene wird eine direkte Verbindung mit dem Internet ausgeschlossen. In der DMZ bauen sowohl der Wartungsservice als auch der Maschinenbetreiber zum vereinbarten Zeitpunkt verschlüsselte Verbindungen auf. Erst mit deren Rendezvous auf dem Server in der DMZ und der Hoheit des Empfängers über die Verbindung, zum Beispiel beim initialen Aufbau, entsteht die durchgängige Wartungsverbindung zur betreuten Maschine.

Security für Edge-Computing

Mit Hilfe des Edge-Computing können immer größere Datenmengen beispielsweise von Sensoren maschinennah sofort verarbeitet werden. Zeitkritische Daten müssen nicht mehr komplett über das Netzwerk übertragen werden und sensible Daten können im eigenen Unternehmensnetz verbleiben. Das verkürzt die Reaktionszeit zum Beispiel im Vergleich mit der Datenverarbeitung in einer Big Data Cloud. Für die Absicherung der Daten sorgt ein Edge-Gateway. Sichere Gateways sollten zwei getrennte Bereiche in einer industrietauglichen Hardware bieten, die strikt voneinander abgeschottet sind: eine Computing-Plattform für individuelle Anwendungscontainer und ein Sicherheits-Gateway. Die separierten Bereiche verfügen über jeweils eigene Betriebssysteme sowie fest zugewiesene Hardware-Ressourcen.

Im Bereich der Anwendungsplattform können Maschinenhersteller oder -betreiber mittels Container-Technologie ihre individuelle Anwendung installieren. Die Anwendung ruft über gängige Schnittstellen die Zustands- und Leistungsdaten von der Maschine ab und führt eine Vorverarbeitung der Daten durch. Die Einsatzszenarien sind vielfältig. Beispielsweise können Informationen für die sofortige Auswertungen genutzt werden, während andere in die Cloud übertragen werden. Die Informationen werden also gefiltert und nur diejenigen Daten in die Cloud übertragen, die für die Data-Analytics-Auswertungen benötigt werden.

OPC UA verstärkt die Cybersecurity

Der Kommunikationsstandard OPC UA ermöglicht eine starke und abgesicherte Vernetzung. Bisher überwiegend proprietäre herstellerspezifische Protokolle müssen an den Netzgrenzen nicht mehr umgewandelt werden. Mit OPC UA kann vom Sensor bis in die Cloud ein einziges Protokoll verwendet werden. Das Thema Sicherheit spielt im OPC-UA-Standard von Anfang an eine wichtige Rolle. Dazu wurde ein eigener Security-Layer mitspezifiziert. Dieser legt Mechanismen fest, wie sich Dienste oder Geräte authentifizieren lassen, wie Daten verschlüsselt werden und wie deren Authentifizierung gewährleistet ist.

In der Praxis ist der Anwender allerdings von der Qualität der Implementierung des jeweiligen Herstellers abhängig. Für sensible Anlagen und Netzsegmente können daher ergänzende Sicherheitslösungen wie Datendioden sinnvoll sein. Sie lassen nur eine unidirektionale Kommunikation zu, um beispielsweise Daten aus sensiblen Industrieanlagen risikolos in ‚unsichere Umgebungen' wie das Internet oder eine Cloud auszuleiten. Ohne Rückkanal haben Angreifer dann in keinem Fall Zugriff auf die Maschinen oder Anlagen.

Geringer Aufwand, hoher Schutz

In der OT-Security kann mit heutigen Technologien eine hoher Schutzlevel gegen Cyberrisiken mit überschaubarem Aufwand erreicht werden. Dabei sollte der Fokus auf einer adäquaten Sicherheit liegen. Cybersicherheit ist allerdings kein Feenstaub, der zum Projektabschluss kurz einmal aufgetragen wird. OT Security ist von Anfang an und in allen relevanten Dimensionen zu berücksichtigen. Und wenn man nachrüsten möchte, sollte dies möglichst herstellerunabhängig geschehen, um einen Vendor Lock-in zu vermeiden. Das Ziel besteht darin, durch technische und organisatorische Maßnahmen gestaffelte Schutzlevel zu schaffen und die wichtigsten Daten und Systeme des Unternehmens besonders zu schützen. Durch diese Cyberresilienz wird darüber hinaus sichergestellt, dass Kernprozesse und Kerninfrastrukturen auch bei Cyberangriffen aufrechterhalten oder zumindest schnell wieder auf die volle Leistung hochgefahren werden können. *ag*

Sichere Datenausleitung

Die Interessengemeinschaft Automatisierungstechnik der Prozessindustrie (NAMUR) hat sich mit der ‚NAMUR Open Architecture' (NOA) zum Ziel gesetzt, Produktionsdaten einfach und sicher für eine Anlagen- und Geräteüberwachung (Monitoring) und für Optimierungen nutzbar zu machen – auch für bestehende Anlagen. Die NAMUR-Initiative schlägt zur direkten Ausleitung von Prozessdaten zusätzlich zu den vorhandenen Automatisierungsstrukturen einen sicheren One-Way-Kanal vor. Auf diesem zweiten Kanal können die Daten rückwirkungsfrei übertragen werden. Für die Sicherheit des Datentransfers soll eine Diode sorgen, die ungewollte und unkontrollierte Datenströme in Richtung des Senders verhindert. So ermöglicht die ‚cyber-diode' von Genua einen solchen sicheren Einbahn-Datentransfer, indem sie per Produkt-Design keine Kommunikation zulässt. Im Sinne des Defense-in-Depth-Prinzips schützt sie mit ihrem hohen Sicherheitsstandard als ergänzende Sicherheitsmaßnahme besonders sensible Netzwerk-Segmente. Diese sind dann de facto von außen nicht mehr angreifbar.

Für sensible Anlagenbereichen eignen sich Datendioden. Durch ihre One-Way-Architektur erlauben sie eine risikolose Ausleitung von Daten.

STEVE SCHONER
ist Strategic Product Marketing Manager für industrielle Cybersicherheit bei Genua.

Schutz für geistiges Eigentum

Im industriellen Umfeld entsteht umfangreicher Daten-Input aus den unterschiedlichsten Quellen, der oft mit Hilfe von Anwendungen mit Künstlicher Intelligenz verarbeitet wird. Wie lassen sich die guten Ideen hinter diesem Prozess wirksam schützen?

Arbeiten Maschinen, Anlagen, Roboter und Menschen im industriellen Umfeld, sorgen verschiedene Quellen für umfangreichen Daten-Input. Dieser wird oft mit Hilfe von Anwendungen mit Künstlicher Intelligenz (KI) verarbeitet. Zudem können Maschinen – Stichwort Machine Learning (ML) – anhand dieser Daten lernen und ihren Algorithmus dadurch selbst optimieren. So wird beispielsweise über Kameras die Qualität eines Produkts geprüft und mittels KI sowie ML lassen sich Abweichungen präzise und schnell entdecken. Um die Ideen der Entwickler hinter diesem Prozess zu schützen, benötigen Hersteller von Anwendungen für KI und ML, die oft mit der Programmiersprache Python geschrieben sind, einen wirkungsvollen technischen Schutz.

Die Beliebtheit der unterschiedlichen Programmiersprachen hat der Analyst Slash Data in einer Umfrage ‚State of the developer nation' untersucht. Im ersten Quartal 2021 wurden dazu über 19.000 Entwickler befragt. Eines der Ergebnisse: Am zweithäufigsten arbeiten die Software-Entwickler mit Python, wobei die Haupteinsatzzwecke Data Science, Machine Learning und Anwendungen für IoT sind.

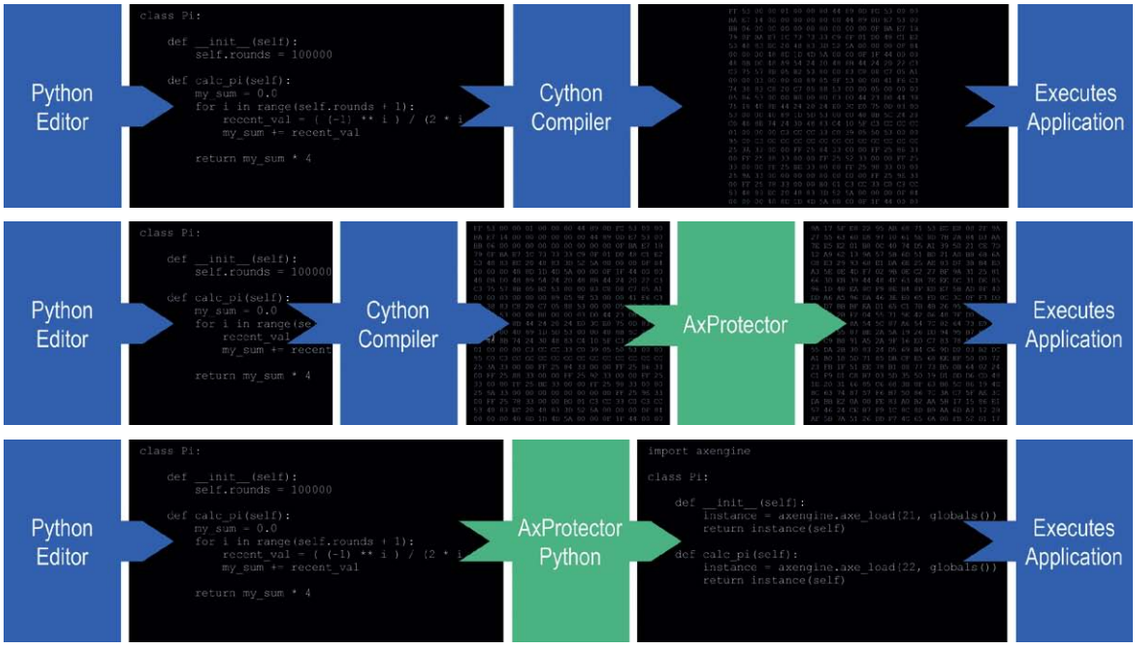
Angriff auf die Programmiersprache

Aufgrund der wachsenden Bedeutung von KI und ML werden Angreifer verstärkt versuchen, an die guten Ideen der Hersteller zu gelangen und mit geringem Aufwand davon zu profitieren. Typischerweise liegt in Python ein Angriffspunkt, da der Python-Quellcode als einfache Text-Datei ausgeliefert wird und im Klartext gelesen werden kann, was bei Skriptsprachen üblich ist. So können Anwender – absichtlich oder unabsichtlich – den Quellcode ändern, manipulieren, kopieren und die Idee dahinter, beispielsweise einen KI-Lernalgorithmus, analysieren und unberechtigt nutzen (Reverse Engineering).

Wibu-Systems kennt als Schutz- und Lizenzierungsexperte die Bedeutung der Programmiersprache Python für Hersteller von KI- und ML-Anwendungen. Aus diesem Grund hat das Unternehmen die Verschlüsselungsmöglichkeit ‚AxProtector Python' auf den Markt gebracht.

Die ‚CodeMeter'-Technologie des Anbieters konnte bereits Python-Software über Vorkompilierung der EXE-Dateien mittels Cython-Compiler schützen. Neu ist

Bild: Wibu-Systems / iStock, Serhii Yakovliev



Kompilierung des Python-Quellcodes in eine ausführbare Datei. Das Ergebnis ist plattformabhängig und unverschlüsselt. Die Anwendung kann weiterhin von einem Experten mit einem Disassembler analysiert werden.

Kompilierung des Python-Quellcodes in eine ausführbare Datei und anschließende Verschlüsselung mit AxProtector. Das Ergebnis ist plattformabhängig und verschlüsselt. Die Anwendung kann nicht mehr mit einem Disassembler analysiert werden.

Verschlüsselung des Python-Quellcodes mit AxProtector Python ohne vorherige Kompilierung in eine ausführbare Datei. Das Ergebnis ist plattformunabhängig und verschlüsselt. Die Anwendung kann nicht mehr mit einem Disassember analysiert werden.

nun die direkte und automatische Verschlüsselung der Python-Software über ‚AxProtector Python', was die vorhandenen Tools der CodeMeter Protection Suite erweitert.

Das Grundprinzip aller CodeMeter-Tools ist: Zuerst verschlüsseln die Hersteller ihre Software und danach liefern sie den passenden Lizenzschlüssel an die Anwender. Anschließend können die Anwender die verschlüsselte Software den Berechtigungen gemäß nutzen. Als Träger der Lizenzschlüssel dienen die Schutzhardware ‚CmDongle', die softwarebasierte Aktivierungsdatei ‚CmActLicense' oder der ‚CmCloudContainer', der in der Cloud liegt.

Über Vorkompilierung zur geschützten Software

Der klassische Weg besteht aus zwei Schritten: Vorkompilierung und Verschlüsselung. Über den Cython-Compiler wird die Python-Software in eine ausführbare, in C geschriebene Datei (EXE) umgewandelt, damit dann diese ausführbare Datei über das Standardtool ‚AxProtector' verschlüsselt wird. So können Hersteller ihr geistiges Eigentum, das in der Software steckt, verschlüsseln und auch lizenzieren und somit unter dem Stichwort ‚Softwaremonetarisierung' zusätzlichen Umsatz generieren. Hersteller können automatisiert verschiedene Lizenzmodelle umsetzen – beispielsweise Einzelplatzlizenz, Floating-Lizenz innerhalb eines Netzwerkes oder ein zeitbasiertes Modell. Für die Python-Software wichtige Daten lassen sich über das CodeMeter Core API ebenfalls verschlüsseln sowie signieren. Bei diesem Weg muss der Hersteller für jede einzelne Plattform je eine dafür bestimmte ausführbare Datei erzeugen und ausliefern, was technische Kenntnisse voraussetzt.

Direkte Verschlüsselung

Die Mindestvoraussetzungen zum Einsatz von ‚AxProtector Python' sind ‚Python 3' und ‚CodeMeter 7.30'. Das Tool verschlüsselt direkt, ohne die Umwandlung durch ‚Cython', und es wird kein nativer Code erzeugt. Da die Python-Software nur einmal verschlüsselt wird, gibt es nur eine einzige ausführbare Datei, die auf den verschiedenen Plattformen Windows, Linux oder macOS läuft. Nur der gerade benötigte Teil wird zur Laufzeit in den Hauptspeicher geladen und dann entschlüsselt, sodass der große Teil der Software immer noch verschlüsselt bleibt. Jede Funktion der ‚Python'-Software wird einzeln verschlüsselt, sodass Hersteller modulare Lizenzen erzeugen können. Anwender bekommen nur die Lizenzschlüssel für das, was sie gekauft haben. Auch spätere Käufe werden auf diese Weise behandelt.

Will der Hersteller Funktionen und Dateien unverschlüsselt lassen, kann er Annotationen setzen sowie dies über Einträge in der Schutzdefinition steuern. Die Integration des Schutzes ist mit ‚AxProtector Python' viel einfacher, da der Schritt der Vorkompilierung entfällt.

Unterschiedliche Verschlüsselungstools

Ähnlich einem Werkzeugkasten können Hersteller verschiedene Verschlüsselungstools nutzen, um die komplette Software oder nur bestimmte Teile zu verschlüsseln. Zur Auswahl stehen verschiedene ‚AxProtector'-Varianten, die für unterschiedliche Programmiersprachen optimiert sind und für den automatischen Schutz einer ausführbaren Datei sorgen, ‚IxProtector' zur Verschlüsselung einzelner Funktionen und ‚IP Protection', um Software vor Reverse Engineering zu schützen, jedoch werden keine Lizenzschlüssel benötigt. ‚AxProtector Python' ergänzt die vorhandenen Varianten: den Standard-‚AxProtector', ‚AxProtector Java', ‚AxProtector .NET' und ‚AxProtector CmE' für Embedded-Software. *ik*

RÜDIGER KÜGLER
ist VP Sales & Security Expert bei Wibu-Systems in Karlsruhe.

Bilder: Wibu Systems

Cloud Security

Mit kontextbezogener KI-Technologie

Check Point Software erweitert die Funktionen der Plattform ‚CloudGuard Cloud Native Security' um *CloudGuard Application Security (AppSec)*, eine automatisierte Lösung zum Schutz von Web-Anwendungen und APIs. CloudGuard AppSec beseitigt die Notwendigkeit der manuellen Abstimmung und senkt die hohe Rate von Fehlalarmen, die mit herkömmlichen Web Application Firewalls (WAFs) verbunden sind. Die Lösung nutzt kontextbezogene Künstliche Intelligenz, um Angriffe auf Cloud-Anwendungen zu verhindern. Sie blockiert Angriffe gegen Anwendungen, wie Site Defacing, Information Leakage, User Session Hijacking und alle der OWASP Top 10 Sicherheitsrisiken für Webanwendungen. Dabei passt sich die KI-Engine der Lösung permanent an Anwendungsänderungen an und aktualisiert sich selbst, um kontinuierliche Sicherheit zu gewährleisten.
Zudem nutzt die Lösung Verhaltensanalysen, um zwischen menschlichen und maschinellen Interaktionen mit Anwendungen zu unterscheiden. So werden Credential Stuffing, Brute-Force-Angriffe und Site Scraping verhindert.

www.checkpoint.com/de

Switches

Bis zu 24 Ports

Belden bringt mit dem High-Port Switch *Bobcat* von Hirschmann ein neues Mitglied der ‚Bobcat'-Produktfamilie auf den Markt. Der Managed Switch mit bis zu 24 Ports ist eine kompakte Netzwerklösung für das Industrial Internet of Things (IIoT). Zu den wichtigsten Merkmalen der Switches gehören eine hohe Port-Dichte für den Anschluss von Netzwerkgeräten, TSN-Technologie zur gleichzeitigen Unterstützung mehrerer Dienste im Netzwerk und zur Gewährleistung deterministischer Kommunikation, erweiterte Sicherheitsfunktionen wie Wire-Speed Access Control Lists (ACL) und automatischer Denial-of-Service (DoS)-Schutz sowie maximale Ausgangsleistung durch Power-over-Ethernet-Ports (PoE/PoE+), die keine Lastverteilung erfordern.

www.belden.com

Cybersecurity

Tansparenz auf die Cloud ausweiten

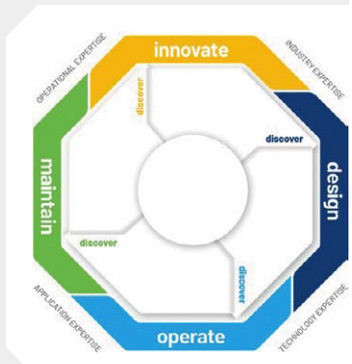
Netscout Systems gibt die Bereitstellung von *Netscout Cyber Investigator (NCI)* für AWS bekannt. Er steigert die Effizienz bei der Verwaltung zunehmender Komplexität aufgrund der Verlagerung von Anwendungen in die Cloud. Da sich die Bedrohungsoberfläche vergrößert, nutzt ‚NCI' Paketdaten, um schnell eine ganzheitliche Sichtbarkeit zu gewährleisten, die zur Ursachenfindung von Problemen erforderlich ist. Netscout hat bei der Einführung von ‚VPC Traffic Mirroring', ‚VPC Ingress Routing' und dem Gateway ‚Load Balancer' (GWLB) zusammen mit AWS an Lösungen für den Zugang zu Paketdaten gearbeitet. GWLB bietet einen skalierbaren Zugriff auf den Paketverkehr für Sicherheits- und Leistungsmanagement. So können Kunden den Datenverkehr von jeder Virtual Private Cloud (VPC) zu beliebigen Sicherheits- und Überwachungstools leiten, ohne die Cloud zu verlassen. NCI ist in AWS Security Hub integriert.

www.netscout.com

Lebenszyklus

Service-Portfolio erweitert

Die Firma Rockwell Automation hat ihre Service- und Lösungskompetenzen weiterentwickelt und führt die Marke *LifecycleIQ Services* ein. Bei ‚LifecycleIQ Services' werden digitale Technologien mit menschlichem Know-how kombiniert. Dadurch helfen die Services Unternehmen dem Anbieter zufolge an jedem Punkt ihres Geschäftszyklus, schneller, intelligenter und flexibler zu arbeiten. Die Services unterstützen Unternehmen während der Entwurfs-, Betriebs- und Wartungsphasen. Produzierende Unternehmen können die Services nutzen, um folgende Ergebnisse zu erzielen: Erfolgreiche Gestaltung der Digitalen Transformation, Stärkung der Cybersicherheit, optimale Unterstützung der Belegschaft.



www.rockwellautomation.com

nachgehakt

bei **Marcus Eibach**
Senior Vice President der Deutschen Messe AG

5G in der Halle 9

Siemens wird die Halle 9 auf dem Hannover Messegelände bis September mit einem 5G-Campus-Netz ausstatten, soweit die gemeinsame Mitteilung von Siemens und der Deutschen Messe Mitte Februar. Was dies konkret bedeutet, erläutert Marcus Eibach, Senior Vice President, Deutsche Messe AG im Interview.

In der Mitteilung vom Februar heißt es: „Das Besondere an der Siemens-Infrastruktur: Sie verbleibt dauerhaft in der Messehalle und wird der Deutschen Messe zur kommerziellen Nutzung überlassen." Bedeutet dies, dass die Deutsche Messe die Hoheit über die Siemens-Infrastruktur haben wird oder wird das 5G-Netz in Halle 9 ganzjährig von Siemens betreut und betrieben?
Marcus Eibach: Das 5G-Campus-Netz von Siemens in der Messehalle 9 wird nach seiner Fertigstellung ganzjährig gemeinsam mit Siemens betreut und betrieben. In enger Partnerschaft bieten wir als Deutsche Messe zusammen mit Siemens die Nutzung des Campus-Netzes für Test- und Demonstrationszwecke von 5G-Produkten, -Lösungen und -Anwendungen an. Der Fokus dabei liegt auf Industrie Use Cases.
Der Basisbetrieb des Netzes erfolgt dabei durch die Deutsche Messe. Hierzu zählen das Schreiben von SIM-Karten, Anmeldung von Geräten, Ein- und Ausschalten der Anlage. Darüber hinausgehende Themen wie Ausbau hinsichtlich Erweiterung und Upgrades, aber auch die Diagnose bei möglichen Problemen erfolgen dann durch Siemens.

Aussteller können das Netz während laufender Messen für Tests und Feldversuche nutzen. Damit haben Aussteller in Halle 9 zukünftig ein maßgebliches Alleinstellungsmerkmal gegenüber Ausstellern in den anderen Messehallen. Erzeugen Sie damit explizit auf die Hannover Messe bezogen einen Run auf Halle 9? Anders gefragt: Sind die Aussteller in anderen Hallen dann nicht benachteiligt?
Keineswegs. Neben dem Auf- und Ausbau des Industrial-5G-Campus-Netzes von Siemens in der Halle 9 erfolgt auf dem Messegelände die flächendeckende Ausstattung mit dem Mobilfunkstandard 5G. Technologiepartner für diesen Ausbau ist an der Stelle die Telekom. Dieses Campus-Netz realisiert die Telekom als ein hybrides Netz. Wir verfügen somit zukünftig über ein privates Netz, welches es unseren Ausstellern und Gastveranstaltern aller Messen in Hannover ermöglicht, ihre 5G-fähigen Produkte, Lösungen und Anwendungen live zu präsentieren. Gleichzeitig haben Besucher der Messen eine hervorragende Versorgung mit dem öffentlichen 5G-Netz der Telekom auf dem Gelände.

Wird es so etwas wie ein Testbed in der Halle 9 geben, mit dessen Hilfe Firmen Tests und Erprobungen im Zusammenspiel mit Produkten anderer Firmen durchführen können?
Genau derartige Szenarien wollen wir realisieren, denn das wird die Realität im Produktionsumfeld sein. Diese Notwendigkeiten wurden uns in einigen Vorgesprächen signalisiert und nun sind wir gespannt auf die ersten konkreten Anfragen. Die Größe der Halle ermöglicht es industriellen Anwendern, Applikationen in allen Formaten schon jetzt mit 5G zu testen. So können nicht nur große Unternehmen sondern auch kleine und mittelständische Unternehmen schon sehr früh in der Entwicklung 5G-Technologie testen, ohne in ein eigenes Campus-Netzwerk investieren zu müssen.

Ab September soll es mit dem Betrieb des Campus-Netzes losgehen. Können beziehungsweise haben sich interessierte Firmen schon für die Nutzung des Netzes angemeldet?
Wir konnten im Bereich Smart Mobility bereits einen ersten Kunden für unser 5G Smart Venue gewinnen: Die Firma SMEV hat eine patentierte Innovationstechnologie entwickelt, die zukünftig Einsatzfahrzeugen den schnellstmöglichen Weg zum Einsatzort garantieren soll. SMEV nutzt die 5G-Infrastruktur unseres Smart Venues, um ihre Technologie weiterzuentwickeln und auf den Echteinsatz vorzubereiten.
Durch die Einbindung der Deutschen Messe und des Messegeländes in das Konsortium Testfeld Niedersachsen ermöglichen sich für uns spannende neue Kooperationsmöglichkeiten mit Unternehmen und Forschungseinrichtungen in den Bereichen autonomes Fahren und vernetzte Mobilität. Darüber hinaus sind wir mit Unternehmen unterschiedlichster Branchen in Gesprächen. *hap*

Bild: Deutsche Messe AG

Die Königsklasse

der Motoren

Zukunft spüren

ECblue – intelligente Hightech-IE5-Motorentechnologie mit einzigartiger Performance.
Klimafreundlich, höchste Effizienz, größtes Energiesparpotential und integrierte MODBUS-Kommunikation. Hochintelligente Sensoren und optionale Bluetooth-Verbindung eröffnen den Weg in die Hochsicherheits-Datenräume unserer **ZAbluegalaxy** – der cloudbasierten IoT Plattform – und damit u.a. die Möglichkeit vorausschauender Wartung (Predictive Maintenance). **www.ziehl-abegg.de**

ZAset –
mobile App

ZAbluegalaxy
Cloudbasierte IoT-Plattform für Produktverwaltung der Zukunft

Die Königsklasse in Lufttechnik, Regeltechnik und Antriebstechnik

Bewegung durch Perfektion

110 Jahre | 110 Years
ZIEHL-ABEGG