Industrielle Robotertechnik und Cybersecurity.

www.tuv.com/fscs-de

TÜVRheinland®
Genau. Richtig.

Inhalt

INDUSTRIELLE ROBOTERTECHNIK UND CYBERSECURITY

Zusammenfassung.

Industrieroboter werden im Hinblick auf ihre Fähigkeiten und Leistung immer besser. Nicht zuletzt deshalb kommen sie immer häufiger in der Fertigungsbranche und verwandten Industrien zum Einsatz, in denen es bei sich wiederholenden Arbeitsabläufen auf Schnelligkeit und Präzision ankommt.

Das Sicherheitsbedürfnis innerhalb solcher Systeme wurde schon vor Jahren erkannt. Und durch die zunehmende Nähe von Robotern und menschlichen Arbeitskräften gewinnt das Thema Arbeitssicherheit mehr und mehr an Bedeutung. Industrieroboter werden zunehmend intelligenter, sind besser vernetzt und immer häufiger mit dem Internet verbunden. Das erhöht natürlich das Bedrohungspotenzial im Hinblick auf Cybersecurity, was sich wiederum negativ auf die sichere Nutzung und Implementierung von Robotern auswirkt. Hinzu kommen der mögliche Verlust von geistigem Eigentum, Produktionsverzögerungen und im schlimmsten Fall physische Schäden.

Die gute Nachricht: Unternehmen können mit einer gezielten Analyse der Cybersecurity-Risiken sowie Produkttests und der Implementierung angemessener Kontrollmechanismen einen sicheren und schadenfreien Betrieb ihrer Industrieroboter sicherstellen.

EINLEITUNG

Roboter haben die Welt der Fertigung verändert und werden auch für einen Wandel bei der Bereitstellung von Services und medizinischen Dienstleistungen sorgen. In der Industrie 4.0 wird der Einsatz von Robotern in der Fertigung noch weiter verstärkt. Serviceroboter werden vermehrt im privaten Bereich als Unterstützung für eine alternde Bevölkerung zum Einsatz kommen. Roboter für die Telemedizin werden komplexe chirurgische Eingriffe in weit entfernten und möglicherweise auch feindlichen Umgebungen durchführen.

Wie jedes elektromechanische System unterliegen auch Roboter potenziellen Cybersecurity-Bedrohungen, die den sicheren Betrieb gefährden können. Ein Roboter kann heute nicht als sicher angesehen werden, solange seine Cybersecurity-Risiken nicht untersucht und bei Bedarf Gegenmaßnahmen eingeleitet wurden. Vernetzte Roboter, die gängige aber ungeschützte Internet-Protokolle verwenden und mit anfälligen ungepatchten Betriebssystemen arbeiten, bergen Gefahren. Sie bieten eine große Angriffsfläche für bösartige Attacken und stellen eine signifikante Herausforderung für den Schutz und die Sicherheit dar.

In diesem Dokument werden die Cybersecurity-Aspekte von Industrierobotern erläutert und Herstellern, System-Implementierern und Benutzern Wege für die Zukunft aufgezeigt. Es vereint bewährte Verfahren aus anderen Branchen sowie umfassende Erfahrungen von TÜV Rheinland.

WAS IST EIN ROBOTER?

Der Begriff Roboter wurde zu Beginn des 20. Jahrhunderts vom tschechischen Wort *robota* abgeleitet, was so viel bedeutet wie Leibeigener oder Arbeiter. Drückte der Begriff in seiner ursprünglichen Bedeutung noch eine Ablehnung der Technologie aus, bezeichnet er heute alles von einem Science-Fiction-Roboter wie dem Terminator bis zu den unzähligen Maschinen, die Routinearbeiten an einer Fertigungslinie durchführen. Durch den weltweiten Einsatz von Robotern in Fabriken und anderen Einrichtungen haben sich die Menschen vieler alltäglicher und oftmals gefährlicher Aufgaben entledigt.

In diesem Dokument wird ein Roboter folgendermaßen definiert: „reprogrammierbares, multifunktionales Handhabungsgerät zum Bewegen von Materialien, Teilen, Werkzeugen oder Geräten anhand von variabel programmierten Bewegungen zur Ausführung verschiedener Aufgaben" (Mark W. Spong, 2004).

Definitionen und eine Standardklassifizierung von Robotern wird derzeit erarbeitet. Die Internationale Organisation für Normung (ISO) (ISO-Standard 8373:2012) unterteilt die Roboter in folgende Klassen:

- Industrieroboter, die als automatisch gesteuertes, reprogrammierbares, multifunktionales Handhabungsgerät, das in drei oder mehr Achsen programmiert und entweder stationär oder mobil für industrielle Anwendungen eingesetzt werden können.
- Serviceroboter, die als Roboter, nützliche Aufgaben für Menschen oder Ausrüstung mit Ausnahme von industriellen Automatisierungsanwendungen ausführen können. Dazu gehören persönliche Pflegeroboter wie mobile Diener, physische Assistenten und Personenbeförderer (European Robotics Association, 2017).
- Medizinische Roboter, die als „Roboter oder Roboter-Vorrichtungen für den Einsatz als medizinisches, elektrisches Gerät“ definiert werden (VIRK, 2017).

Die Terminologie wird derzeit noch angepasst und verfeinert; so hat beispielsweise ein Roboter im Gegensatz zu einem Robotiksystem keinen Endeffektor. Diese Problematik ist jedoch nicht Gegenstand dieses Dokuments.

Einer der ersten Einsätze von Robotern in der Fertigung geht auf den Anfang der 1960-iger Jahre zurück, als General Motors die Fahrzeugproduktion mit dem Unimate-Roboter unterstützte. Seitdem wurden Roboter immer häufiger in verschiedensten Bereichen der Gesellschaft abseits von Industrie und Fertigung eingesetzt. Laut Schätzungen gibt es derzeit weltweit fast 2 Millionen aktive Industrieroboter (Hagerty, 2015).

ROBOTERTECHNIK UND CYBERSECURITY

Wie bei vielen Produkten spielt das Thema Cybersecurity für Roboterhersteller oftmals nur eine untergeordnete Rolle. Cybersecurity steht häufig erst am Ende einer Liste mit wichtigen Aspekten und wird unweigerlich durch neue Funktionen, reduzierte Kosten und Sicherheitsfragen in den Hintergrund gedrängt. Der Gedanke, Cybersecurity zu Beginn der Entwicklung eines Roboters in das Produkt „einzubauen“, hat sich vielerorts noch nicht durchgesetzt. Tatsächlich interessieren sich viele Anwender und Verbraucher mehr für die Eigenschaften, Kosten und Funktionen eines Produkts, als für Cybersecurity.

Leider lassen sich viele von der anthropomorphen Natur einiger Robotiksysteme dazu verleiten, die Natur von roboterspezifischen Cybersecurity-Risiken falsch zu interpretieren. Roboter sind eine Kombination aus mechanischen Strukturen, Sensoren, Aktoren und Computer-Software, mit der diese Geräte wie jede andere Maschine gesteuert werden (Morante, 2015) - eine Tatsache, die bei der Bewertung von Cybersecurity-Risiken berücksichtigt werden muss.

Bei der Betrachtung von Robotik und Cybersecurity wird die Triade der Informationssicherheit - also Vertraulichkeit, Integrität und Verfügbarkeit - allzu oft durch einen verstärkten Fokus auf Verfügbarkeit und Maschinensicherheit verdrängt. Wenn Systeme für die Installation von Patches und Updates (auch wenn sie direkt vom Hersteller kommen) heruntergefahren werden müssen, ist dies mit Planungs-, Zeit- und Arbeitsaufwand verbunden. Hierbei sollte man insbesondere bedenken, dass auch Industrieroboter jederzeit voll ausgelastet sein sollten.

Die Vertraulichkeit sollte natürlich nicht ignoriert werden. Der Robotik-Prozess, der in einer Fabrik eingesetzt wird, oder die komplexe Steuerungssoftware, die für die Kontrolle eines autonomen oder teilautonomen Roboters verwendet wird, hat einen Wert – sowohl für Hacker als auch für Mitbewerber – und sollte daher entsprechend geschützt werden.

BEDROHUNGEN UND RISIKEN FÜR ROBOTER

Roboter und ihre Software und Firmware können wie jedes andere System auch zum Ziel von Angreifern werden. Leider kann sich ein solcher Angriff in vielen Fällen und besonders im industriellen Kontext negativ auf den sicheren Betrieb des betroffenen Roboters auswirken.

Während Hersteller immer mehr innovative Funktionen in ihre Produkte implementierten, wie z.B. die Möglichkeit der Steuerung eines Industrieroboters mit einem Smartphone an Stelle des üblichen Handbediengeräts (Handgerät für die Programmierung eines Roboters) (Control Engineering Europe, 2011), wird es immer wichtiger, Cybersecurity schon in der Design- und Entwicklungsphase eines Roboters zu berücksichtigen.

Für einen motivierten und gut ausgestatteten Angreifer, wie z.B. eine staatliche Institution, ist der Zugang zu Hardware und Software für Industrieroboter zu Forschungszwecken relativ einfach. Es ist unwahrscheinlich, dass ein Hobby-Hacker Zugriff auf die Hardware eines Industrieroboters erlangt, sofern er nicht Zutritt zu einer Fertigungseinrichtung oder zu den Räumen eines Händlers hat oder sich Remote Access per WLAN verschaffen kann. Gebrauchte Industrieroboter sind zwar am Markt erhältlich, jedoch fallen dafür Kosten an. Sie sind zwar nicht extrem teuer, für einen Hobby-Hacker ist der Preis aber trotzdem recht hoch. Und auch die Größe und das Gewicht vieler Industrieroboter sind nicht zu unterschätzen.

Einige Hersteller bieten die Controller-Firmware ihrer Industrieroboter kostenlos auf ihren Websites an (andere wiederum stellen Begleitsoftware nur bekannten Kunden zur Verfügung). Potenzielle Hacker haben damit die Möglichkeit, den Softwarecode zu untersuchen und auf Schwachstellen zu prüfen, ohne Zugang zur entsprechenden Hardware zu haben.

Medizinische Roboter in klinischen Umgebungen sind oftmals schlecht geschützt, da viele Krankenhäuser öffentliche Gebäude sind, zu denen Besucher rund um die Uhr Zutritt haben. Und auch Serviceroboter, die an Privatpersonen verkauft werden, sind ein Hauptangriffsziel, da der physische Zugriff relativ einfach ist.

ANGRIFFE AUF FIRMWARE UND SOFTWARE

Die Firmware und Begleitsoftware von Industrierobotern können auf ein lokales Flashlaufwerk, eine Festplatte oder ein Festspeichermedium geladen werden. Sie sind wie jede andere Software anfällig gegen Malware und Mängel bei der Programmierung, die zu unvorhersehbaren Problemen führen können.

Die Software und Firmware auf Robotern bieten häufig Zugriffsmöglichkeiten für die technische Wartung und den Support. Das kann ein offener USB- oder RJ-45-Port sein oder auch eine drahtlose Verbindung, die oft lediglich durch das Standardkennwort des Herstellers geschützt ist. Der Zugriff kann dann ganz einfach über die Fabrikräume oder die bereitgestellte Umgebung erfolgen, da physische Sicherheit häufig mangelhaft oder gar nicht vorhanden ist. Wartungstechniker verwenden in der Regel einen Laptop für den Zugriff auf einen Roboter und die Durchführung von Diagnosen oder Software-Updates. Diese Laptops könnten nicht mit der erforderlichen Sicherheit konfiguriert sein und auf andere Websites oder Ressourcen zugreifen und so ein Einfallstor für Malware oder Hacker-Angriffe bereitstellen.

ENTWICKLUNG VON ROBOTER-SOFTWARE

Für die Programmierung eines Roboters können viele Programmiersprachen verwendet werden. Diese reichen von proprietären Sprachen, die viele Hersteller von Industrierobotern nutzen, bis hin zu C#, .NET (wird im Microsoft Robotics Developer Studio verwendet), Python (wird in den Bibliotheken des Haupt-Clients des Robot Operating System (ROS) verwendet) und C++.

ROS bietet darüber hinaus Open-Source-Software, die in der kommerziellen und privaten Roboter-Community ausgetauscht und verbreitet werden kann. Der Austausch und die Wiederverwendung des Software-Codes ist einerseits ein wahrer Segen für die Entwickler. Andererseits bedeutet das aber, dass sicherheitsrelevante Mängel und Probleme kopiert und ungewollt über das gesamte Ökosystem hinweg verbreitet werden. Da ROS standardmäßig keine Sicherheitsfunktionen bietet, müssen die auf der Plattform basierenden Lösungen auf andere Art und Weise geschützt werden. Diese Tatsache wurde bereits erkannt, weshalb derzeit SROS, eine sichere Variante von ROS, entwickelt wird.

ROBOTER-KOMMUNIKATION

Viele Roboter sind für die Kommunikation mit externen Ressourcen konfiguriert, wie z.B. mit einem Fabriksteuerungssystem, mit einem lokalen Ökosystem eines anderen Roboters, mit Smartphones oder mit einer cloudbasierten Monitoring-Lösung des Herstellers.

Der Remote Access über eine Servicebox des Herstellers erfolgt oft drahtlos, wie z.B. über das Mobilfunknetz, und ermöglicht dem Händler den Remote Access auf den Roboter. In manchen Fällen wird dieser Zugriff ohne Wissen des Bedieners vorgenommen. Solche verborgenen Hintergrundverbindungen sind natürlich dafür gedacht, das Kundenerlebnis zu verbessern. Sie stellen aber auch ein Risiko dar, dessen sich die Betreiber der Fertigungsanlage oftmals gar nicht bewusst sind.

Wie wir festgestellt haben, spielt die Vertraulichkeit von Daten bei der Entwicklung eines Roboters keine oder nur eine untergeordnete Rolle. Die Folge ist, dass die Kommunikation zwischen Systemen in Klartext, schlecht verschlüsselt oder ungeschützt erfolgt. Datensicherheit ist unter Umständen bei einer kurzzeitigen Aufgabe nicht unbedingt ein großes Anliegen. In manchen Fällen kann es egal sein, dass sich ein Industrieroboter nur um 27 Grad und nicht um 30 Grad gedreht hat. Was zählt ist, dass der Kommunikationskanal unsicher ist und damit als Pfad für Angriffe auf andere Systeme oder die Störung der Produktionslogik dienen kann.

Auf der anderen Seite kann eine Manipulation von Regelungsmechanismen oder Parametern, die bewirkt, dass sich ein Roboterarm von 27 Grad zu 30 Grad bewegt, große Auswirkungen auf die Fertigungsqualität haben oder sogar einen Arbeiter verletzen.

ROBOTER UND IDENTITY & ACCESS MANAGEMENT

Identity & Access Management (IAM) sorgt dafür, dass dem richtigen Benutzer der richtige Systemzugriff zum richtigen Zeitpunkt gewährt wird – was eine entscheidende Grundlage für Cybersecurity ist. Bei guter Implementierung wird dadurch die Möglichkeit für Auditing und Accountability für Benutzer, Prozesse und andere Systeme geschaffen. Eine schlechte Implementierung vom IAM kann dagegen dazu führen, dass ungeschulte und unerfahrene Bediener Änderungen an einem Industrieroboter vornehmen, die Fertigungs- oder Sicherheitsprobleme auslösen können. Das ist in Umgebungen mit mangelhaften Abläufen der Fall, bei denen beispielsweise Zugangsdaten (Benutzername und Kennwort) für jeden sichtbar auf einer Haftnotiz an den Roboter geklebt werden oder wo komplett auf eine Anmeldung verzichtet wird. Und natürlich trägt auch eine schlechte Implementierung von grundlegender Access Control durch die Hersteller nicht zu einer Verbesserung dieser Situation bei.

Wenn nach der Installation eines Roboters die Standardkennwörter des Herstellers nicht geändert werden, haben Angreifer leichtes Spiel.

Mit der zunehmenden Verbreitung des Internets der Dinge (die unzähligen Geräte und Hardware-Komponenten, die sich mit dem Internet verbinden) ermöglicht Angreifern Geräte in ein "Botnetz" zu integrieren. Genau das hätte weitestgehend verhindert werden können, wenn Benutzer gezwungen würden, das Standard-Administrationskennwort beim Setup zu ändern (Newman, 2016).

DATENSCHUTZ UND ROBOTER

Auf Industrierobotern befinden sich im Normalfall keine persönlichen Daten. Dagegen ist es bei Robotern für die medizinische und chirurgische Versorgung unbedingt erforderlich, dass diese Geräte persönliche und sensible Daten, wie z.B. gesundheitsbezogene Angaben, speichern.

In den meisten Ländern werden persönliche und gesundheitsbezogene Daten aufgrund ihrer sensiblen Natur durch lokales, nationales oder branchenspezifisches Recht geschützt. Die Hersteller und die Benutzer dieses Equipments müssen daher besonders darauf achten, dass die Anforderungen im Hinblick auf die Patientenvertraulichkeit jederzeit eingehalten werden. In manchen Ländern können solche Roboterhersteller nur dann in Gesundheitsnetzwerken aktiv werden, Patientendaten austauschen oder Services bereitstellen, wenn sie strikte Anforderungen an die Informationssicherheit erfüllen.

SICHERE ENTSORGUNG UND WIEDERVERWERTUNG

Die Entsorgung von Industrierobotern oder Steuerungsgeräten, die sensible Daten enthalten, muss gut durchdacht und geplant werden. Bei der Außerbetriebnahme eines Roboters müssen alle residenten, nicht flüchtigen Speicher zerstört oder forensisch überschrieben werden, wenn solche sensiblen Daten vorhanden sind und das bestehende Risiko diese Maßnahme erforderlich macht. Das einfache Löschen dieser Daten bietet keinen wirkungsvollen Schutz, da Kriminelle diese Daten ganz leicht wiederherstellen und für ihre Zwecke nutzen können. Wenn ein G-Code (eine NC-Programmiersprache (numerische Steuerungen)) auf einem ausrangierten Roboter verbleibt, kann ein Mitbewerber daraus Schlüsse über die vom Vorbesitzer genutzten Prozesse ziehen.

FUNKTIONALE SICHERHEIT UND ROBOTERTECHNIK

Die Welten von funktionaler Sicherheit, Robotern und Cybersecurity sind jetzt untrennbar miteinander verbunden, da ein Industrieroboter nicht mehr als sicher angesehen werden kann, wenn er nicht geschützt wird. Doch in welchem Verhältnis stehen funktionale Sicherheit und Cybersecurity?

- Funktionale Sicherheit bezeichnet Maßnahmen zur Vermeidung von zufälligen und systematischen technischen Ausfällen zum Schutz des Lebens und der Umwelt.
- Cybersecurity bezeichnet Maßnahmen zur Vermeidung von fahrlässigen und vorsätzlichen Aktionen, um so Geräte, Einrichtungen und Daten zu schützen.

Industrieroboter sind oftmals physisch von ihren humanen Kollegen getrennt und in einem Käfig oder in einer Arbeitszelle untergebracht. Mit Hilfe verschiedener Sicherheitssperren stellen solche Käfige eine physische oder per Lichtschranke realisierte Sicherheitsbarriere zwischen Menschen und Maschinen bereit. Die Entwicklung von kollaborativen Industrierobotern (Co-Bots) hat eine Aufweichung dieser Trennung mit sich gebracht. Dadurch erhöht sich aber die Gefahr von Sicherheitsvorfällen, die direkt zu Arbeitsunfällen führen. Wenn eine Roboter-Arbeitszelle beispielweise Software für die Implementierung einer Käfig-Sicherheitszone nutzt, könnte diese manipuliert werden, um den Betrieb des Roboters zu stören. Im Jahr 2015 betrat ein Arbeiter einen Roboter-Sicherheitskäfig in einer Automobilfabrik und kam dabei ums Leben (Byrant, 2015).

Service- und Medizinroboter befinden sich im Normalfall im direktem Umfeld ihrer menschlichen Benutzer oder der menschlichen Kunden und Patienten. Funktionale Sicherheit ist in diesem Umfeld von zentraler Bedeutung.

Ein Roboter, der dank professionell geplanter und strikt umgesetzter funktionaler Sicherheit ein angemessenes Sicherheits-Integritätslevel (SIL) einhält, kann trotzdem durch einen Cyber-Angriff oder durch fahrlässige Aktionen gefährdet werden. Auch wenn Industrieroboter-Steuerungssysteme gut konzipiert und implementiert wurden - wenn der Controller nicht durch grundlegende Sicherheitsmaßnahmen geschützt wird, kann es vorkommen, dass er manipuliert wird oder dass die Parameter des Runtime-Regelkreises geändert werden. Das hat zur Folge, dass die Sicherheitsmaßnahmen einfach umgangen werden können.

ANALYSE VON CYBERSECURITY-BEDROHUNGEN

Im Gegensatz zu Sicherheitsbedrohungen entwickeln und wandeln sich Cybersecurity-Bedrohungen kontinuierlich. In diesem Kontext kann eine Bedrohung alles sein, was die Verfügbarkeit und Sicherheit eines industriellen Robotersystems beeinträchtigt. Dabei spielt es keine Rolle, ob die Bedrohung von einem technischen Softwarefehler herrührt oder durch kriminelle Handlungen hervorgerufen wird. Da Hacker jeglicher Art ein erhöhtes Interesse an Roboter-

technik haben, müssen diese Bedrohungen erkannt, verstanden und so verarbeitet werden, dass die wichtigsten Probleme basierend auf ihrem Risikopotenzial für das Geschäft identifiziert werden.

Die Analyse von Cybersecurity-Bedrohungen kann für diejenigen, die in der Welt der Industrierobotik als Anbieter oder Nutzer unterwegs sind, einen grundlegenden Wandel bei der Art und Weise des Umgangs mit geschäftsspezifischen Risiken bedeuten.

Die meisten Prozesse für die Analyse von Cybersecurity-Bedrohungen umfassen viele Schritte. Zu Beginn wird definiert, welche Informationen benötigt werden, um das Verständnis über Bedrohungen zu verbessern. Es muss sich zum Beispiel die Frage gestellt werden, ob in der Roboteranlage einer bestimmten Marke implementiert sind. Wenn das der Fall ist, wären die spezifischen Bedrohungen für diese Robotermarke von Interesse. Anschließend können Daten aus verschiedensten Quellen zusammengetragen werden, einschließlich öffentlich zugänglicher Informationen aus branchenspezifischen und staatlichen Sicherheitsforen. Diese Daten müssen dann analysiert werden, um Informationen zu gewinnen, die für geschäftliche Risiken relevant sind.

Die Zusammenführung von verschiedensten Informationsschnipseln zu nützlichen Bedrohungsinformationen kann eine komplexe Aufgabe sein. Doch diese Aufgabe hilft bei der Identifizierung der Bereiche, in denen für das Unternehmen Handlungsbedarf besteht. Nur durch die effektive Verarbeitung von Bedrohungsdaten können kosteneffiziente und angemessene Maßnahmen zum Schutz eines Industrieroboters ergriffen werden.

Das NIST Cybersecurity Framework (CSF) basiert auf 5 Funktionalitätsbereichen: Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen. Dieses Regelwerk wurde ursprünglich für industrielle Steuerungssysteme und kritische nationale Infrastrukturen entwickelt, liefert aber ein Modell für das Verständnis der kontextuellen Risiken bei der Nutzung eines Prozesses oder eines Systems wie z.B. eines Roboters. Es ermöglicht die Betrachtung des Modells für Risk, Governance and Compliance (also der Gesamtsituation im Hinblick auf die Sicherheit in der Fabrik/im Unternehmen) sowie die Adressierung von konkreten Problemen wie z.B. der richtige Umgang mit einem Sicherheitsvorfall beispielsweise bei einem IP-Diebstahl.

Hersteller sollten darüber nachdenken, den Kunden und Integratoren eine Risiko-Abbildbarkeitsmatrix zur Verfügung zu stellen, um Transparenz im Hinblick auf die Bedrohungen zu schaffen, die berücksichtigt (und nicht berücksichtigt) wurden. Der Integrator oder Nutzer kann dann zusätzliche mehrschichtige Kontrollen implementieren, die sich an Bedrohungen im Anwendungskontext des Industrieroboters richten.

SICHERHEITSTESTS FÜR INDUSTRIEROBOTER

Wie bereits erwähnt, kann ein komplexes elektromechanisches System nicht mehr als sicher angesehen werden, wenn keine angemessenen Kontrollmechanismen implementiert wurden, um den zuverlässigen Schutz vor Cyber-Risiken zu gewährleisten.

Die Grundnorm für funktionale Sicherheit, IEC 61508:2010, besagt:

- „Wenn eine Gefahrenanalyse eine böswillige oder unerlaubte Handlung feststellt, die eine Sicherheitsbedrohung als vorhersehbar einstuft, sollte eine Sicherheitsbedrohungsanalyse durchgeführt werden" (7.4.2.3).

Im weiteren Text heißt es:

- „Wenn Sicherheitsbedrohungen identifiziert wurden, muss eine Schwachstellenanalyse durchgeführt werden, um Sicherheitsanforderungen zu bestimmen" (7.5.2.2).

In der Norm wird außerdem empfohlen, die in der IEC 62443-Serie angegebenen Leitlinien zu verwenden.

IEC 62443 (ehemals ANSI/ISA-99) ist eine Normenreihe für Verfahren und Abläufe zum Schutz industrieller Steuerungssysteme und kann auch auf Industrieroboter angewandt werden. Die Leitlinie gilt für alle, die relevante Produkte entwickeln, Systeme integrieren und industrielle Steuerungs- und Robotik-Systeme betreiben.

Innerhalb von IEC 62443 sind sieben Grundanforderungen (Foundational Requirements; FR) definiert:

- FR 1 Identifizierungs- und Authentifizierungskontrolle (Identification and Authentication Control; IAC): Schutz des Geräts durch die Verifizierung der Identität und die Authentifizierung jedes Benutzers, der einen Zugriff anfordert.
- FR 2 Benutzerkontrolle: Schutz vor unerlaubten Handlungen durch die Überprüfung, ob die erforderlichen Rechte gewährt wurden, bevor ein Benutzer diese Handlungen ausführen darf.
- FR 3 Systemintegrität: Gewährleistung der Integrität der Anwendung, um unberechtigte Manipulationen zu verhindern.
- FR 4 Vertraulichkeit von Daten: Sicherstellung der Vertraulichkeit von Informationen auf Kommunikationskanälen und in Datenablagen, um die unberechtigte Weiterverbreitung zu verhindern.
- FR 5 Eingeschränkter Datenfluss: Segmentierung des Steuerungssystems in Zonen und Kanäle, um unnötigen Datenverkehr einzuschränken.
- FR 6 Zeitnahe Reaktion auf Vorfälle: Reaktion auf Sicherheitsverletzungen durch die Benachrichtigung der zuständigen Stellen, die Bereitstellung des erforderlichen Nachweises über die Verletzung und die zeitnahe Einleitung von Behebungsmaßnahmen bei der Erkennung von Vorfällen.

- FR 7 Ressourcenverfügbarkeit: Gewährleistung der Verfügbarkeit der Anwendung oder des Geräts zur Vermeidung einer Verschlechterung oder Verweigerung essenzieller Services.

Wenn diese Anforderungen sorgfältig berücksichtigt werden, können viele Cybersecurity-Risiken innerhalb eines Industrierobotersystems reduziert werden.
Ein Industrieroboter kann auf die Erfüllung der Grundanforderungen von IEC 62443-3-3 getestet werden. Anschließend kann dem System ein Security Level (SL) basierend auf den folgenden Definitionen zugewiesen werden:

- SL 1 - Schutz vor einer beiläufigen oder zufälligen Verletzung
- SL 2 - Schutz vor vorsätzlicher Verletzung mit einfachen Mitteln
- SL 3 - Schutz vor vorsätzlicher Verletzung mit komplexen Mitteln
- SL4 - Schutz vor vorsätzlicher Verletzung mit komplexen Mitteln und erweiterten Ressourcen

Level 4 verlangt signifikante Investitionen, um einen Angriff seitens einer staatlichen Institution zu verhindern. Das ist etwas, das in den meisten Industrieroboter-Umgebungen möglicherweise nicht als verhältnismäßig angesehen wird.

TÜV Rheinland empfiehlt, die Sicherheit bereits zu Beginn der Entwicklung eines Industrieroboters in dessen Design „einzubauen". Im Hinblick auf die Produkttestes deckt eine Kombination aus traditionellen Schwachstellen- und Penetrationstests und den Tests für IEC 62443-3-3 die wohl größte Bandbreite ab. Diese Tests richten sich auch an Probleme wie veraltete Softwarekomponenten, Nutzung von schwachen Authentifizierungsdaten oder Standard-Zugangsdaten, mangelhafte Transport-Verschlüsselung mit veralteten kryptographischen Methoden, unsichere Web-Schnittstellen und mangelhafter Softwareschutz.

IHRE MASSNAHMEN

Hersteller und Nutzer von Industrierobotern müssen die Cybersecurity-Risiken ihrer Produkte basierend auf der Funktion, der Leistung und dem Kontext, in dem sie eingesetzt werden, untersuchen.

Nach dieser Untersuchung müssen angemessene Kontrollmechanismen implementiert werden, um die Risiken auf ein akzeptables Maß reduzieren zu können. Auf diese Weise können die Hersteller ihre Produktforschung, Entwicklung und Innovationen in dem Wissen fortsetzen, dass diese Risiken angemessen behandelt werden.

Die Hersteller sollten folgende Maßnahmen durchführen:
- Untersuchung des Konzepts für die Robotersicherheit
- Gefahrenanalyse und Erstellung eines Bedrohungsmodells
- Erstellung einer Risiko-Abbildbarkeitsmatrix
- Untersuchung auf einen sicheren Code
- Durchführung von Eindringungstests und dynamischen Tests zur Identifizierung von Schwachstellen
- Untersuchung von Komponenten auf potenzielle Schwächen im Hinblick auf Cybersecurity
- Untersuchung der wichtigsten Sicherheitskontrollmechanismen
- Untersuchung des Reaktionsplans für Sicherheitsvorfälle
- Rechtliche und regulatorische Untersuchung
- Untersuchung des Software-Update- und Patch-Prozesses
- Untersuchung von anfälligen Design-Schnittpunkten innerhalb der Gerätearchitektur

Integratoren von Industrierobotersystemen stehen vor der schwierigen Aufgabe der Integration von komplexen Robotersystemen in einer Produktions-, Fertigungs- oder Prozessanlage. Wenn ein Systemintegrator unsichere Industrieroboter miteinander verknüpft, vervielfacht er die Cybersecurity-Probleme, da sich die Risiken über mehrere Plattformen multiplizieren. Systemintegratoren müssen die Sicherheitsrisiken ihrer Produkte verstehen und diese gemeinsam mit den Herstellern in einer implementierten Anlage reduzieren.

Integratoren sollten folgende Maßnahmen durchführen:
- Untersuchung von anfälligen Design-Schnittpunkten innerhalb der Systemarchitektur
- Untersuchung des Quellcodes des Geräts innerhalb des Systems
- Entwicklung einer Risiko-Abbildbarkeitsmatrix
- Untersuchung auf einen sicheren Code in anderen verbundenen Systemen
- Durchführung von Eindringungstests und dynamischen Tests zur Identifizierung von Software-Schwachstellen
- Untersuchung anderer Komponenten auf potenzielle Schwächen im Hinblick auf Cybersecurity
- Untersuchung und Empfehlung von angemessenen Sicherheitskontrollmechanismen

Nutzer müssen sicherstellen, dass die Roboter in ihrer Produktionsanlage unter Berücksichtigung der potenziellen Cyber-Risiken konfiguriert wurden. Andere Systeme müssen mit einer Produktions- oder Prozessanlage interagieren, weshalb ein ganzheitliches Konzept verfolgt werden sollte. Jede Implementierung wird möglicherweise stark individualisiert und daher gelten jeweils ganz spezielle Cybersecurity-Risiken. Es sollte regelmäßig eine Untersuchung der Cybersecurity-Risiken der Anlage und aller Robotersysteme in Abhängigkeit von der Natur und dem Typ der durchgeführten Arbeiten vorgenommen werden.

Die Nutzer sollten folgende Maßnahmen durchführen:
- Entwicklung eines Reaktionsplans für Sicherheitsvorfälle
- Untersuchung der Software-Update- und Patch-Management-Prozesse

- Untersuchung der Cybersecurity-Risiken für die Anlage und der anfälligen Design-Schnittpunkte

FAZIT

Wir haben gesehen, dass Industrieroboter signifikante Produktivitätssteigerungen und Kostensenkungen ermöglichen. Neue und entstehende Cyber-Bedrohungen bringen neue Herausforderungen für Hersteller, Integratoren und Roboterbediener mit sich. Mit einem an Cyber-Bedrohungen orientierten und risikobasierten Konzept für die Bewältigung dieser Probleme kann das erfolgreiche Wachstum eines Unternehmens, das sicher und profitabel ist, gewährleistet werden.

LITERATURVERZEICHNIS

Byrant, C. (2015, July 1st). Worker at Volkswagen plant killed in robot accident. Retrieved from Financial Times: https://www.ft.com/content/0c8034a6-200f-11e5-aa5a-398b2169cf79

Control Engineering Europe. (2011, September 11th). iPhone used to programme and control industrial robot. Retrieved from Control Engineering Europe: http://www.controlengeurope.com/article/44966/iPhone-used-to-programme-and-control-industrial-robot.aspx

European Robotics Association. (2017, April 26th). Definition of Robot (industrial and service) according to ISO-Standard 8373:2012. Retrieved from Eu-nited.net: http://www.eu-nited.net/robotics/market/introduction/index.html

Hagerty, J. R. (2015, June 2nd). Meet the New Generation of Robots for Manufacturing. Retrieved from Wall Street Journal: https://www.wsj.com/articles/meet-the-new-generation-of-robots-for-manufacturing-1433300884

Mark W. Spong, S. H. (2004). Robot Dynamics and Control. In S. H. Mark W. Spong, Robot Dynamics and Control. smpp.northwestern.edu/savedLiterature/Spong_Textbook.pdf.

Morante, S. (2015, September 29th). Cryptobotics: why robots need cyber safety. Retrieved from Frontiers in Robotics and AI: http://journal.frontiersin.org/article/10.3389/frobt.2015.00023/full

Newman, L. H. (2016, December 9th). The Botnet That Broke the Internet Isn't Going Away. Retrieved from Wired.com: https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/

Virk, G. S. (2017, April 26th). CHALLENGES OF THE CHANGING ROBOT MARKETS. Retrieved from Nist.gov: http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=913708

Anlage 1 Bedrohungsaktoren

Bedrohungsaktoren (Threat Actors) haben verschiedene Beweggründe für Angriffe auf einen Roboter oder eine Roboterinstallation. Viele dieser Beweggründe decken sich mit den Beweggründen derjenigen, die andere Systeme angreifen, also Unternehmens-IT oder operative Technologien/industrielles Internet der Dinge.

BEDROHUNGSGRUPPE	BEWEGGRUND	ZIEL
Unzufriedene Mitarbeiter	▪ Rache am Arbeitgeber ▪ Arbeitgeber in ein schlechtes Licht rücken ▪ Daten für die Verwendung in einem neuen Job stehlen	▪ Ruf des Arbeitsgebers schädigen ▪ Einem Arbeitgeber „zeigen, was er verdient hat“ ▪ Verzögerungen auf einer Produktionslinie auslösen
Kriminelle	▪ Finanzielle Vorteile	▪ Ransomware einschleusen, um die Produktion zu stören ▪ Finanz- und Transaktionsdaten stehlen
Opportunisten und Möchtegern-Cyber-Hacker	▪ Die Herausforderung ▪ „Spaß” an einem Angriff	▪ Beweisen, dass sie auf eine „sichere“ Seite kommen ▪ Angeberei
Staatliche Institutionen	▪ Politischer Nutzen ▪ Nationale technologische Fähigkeiten voranbringen ▪ Spionage ▪ Vorbereitung des „intelligenten Schlachtfelds“ für potenzielle künftige Konflikte	▪ Erlangung von geistigem Eigentum (Pläne, Prozesse, Methoden…) ▪ Material für Erpressungszwecke suchen ▪ Prozess oder Fertigungsanlage stoppen oder stören ▪ Lieferkette infiltrieren

Daneben besteht immer das Potenzial für versehentliche Datenverluste durch unsachgemäße/nicht böswillige Aktionen wie z.B. verlorene oder gestohlene Laptops oder Speichersticks von Mitarbeitern.

Anlage 2 Ausgewählte Schlüsselnormen in der industriellen Robotertechnik

NORMEN REFERENZ	NAME DER NORM	GELTUNGS-BEREICH	ANMERKUNGEN
ISO 10218-1:2011	Roboter und Robotikgeräte -- Sicherheitsanforderungen für Industrieroboter -- Teil 1: Roboter	Industrieroboter	Enthält Anforderungen und Leitlinien für die eigensichere Konstruktion, Schutzmaßnahmen und Informationen für die Verwendung von Industrierobotern. Es werden die grundlegenden Gefahren in Verbindung mit Robotern und die Anforderungen für die Eliminierung oder angemessene Reduzierung der Risiken in Verbindung mit diesen Gefahren beschrieben.
ISO 10218-2:2011	Roboter und Robotikgeräte -- Sicherheitsanforderungen für Industrieroboter -- Teil 2: Robotersysteme und Integration	Industrieroboter	Enthält Sicherheitsanforderungen für die Integration von Industrierobotern und Industrierobotersystemen gemäß Definition in ISO 10218-1 und Industrieroboterzellen.
ISO/TS 15066	Roboter und Robotikgeräte -- Kollaborative Roboter	Kollaborative Industrieroboter	Enthält Sicherheitsanforderungen für kollaborative Industrierobotersysteme und die Arbeitsumgebung und ergänzt die Anforderungen und Leitlinien für den Betrieb von kollaborativen Industrierobotern in ISO 102181 und ISO 102182.
ISO/NP TR 20218-1	Roboter und Robotikgeräte -- Sicherheitsanforderungen für Industrieroboter -- Teil 1: Industrieroboter-Greifsysteme (Endeffektor)	Industrieroboter	In Entwicklung
ISO 8373:2012	Roboter und Robotikgeräte -- Wörterbuch	Industrielle und nicht-industrielle Roboter	Definiert Begriffe, die in Verbindung mit Robotern und Robotikgeräten in industriellen und nicht-industriellen Umgebungen verwendet werden.
ANSI/RIA R15. 06-2012		Industrieroboter	Annahme von ISO 10218:2011 Teil 1 und 2, stellt für die Industrie einen Leitfaden für die ordnungsgemäße Nutzung der in diese Roboter eingebetteten Sicherheitsfunktionen sowie für die sichere Integration von Robotern in Fabriken und Arbeitsbereichen bereit.

Anlage 3 Andere relevante Normen

NORMEN REFERENZ	NAME DER NORM	GELTUNGS-BEREICH	ANMERKUNGEN
IEC 61508	Funktionale Sicherheit von elektrischen, elektronischen und programmierbaren elektronischen Systemen, die eine Sicherheitsfunktion ausführen	Funktionale Sicherheit	Grundlegende funktionale Sicherheitsnorm für alle Industriesegmente
IEC 62443	Sicherheit von industriellen Netzwerken und Systemen	Industrielle Systeme, einschl. Roboter	Beschreibt verschiedene grundlegende Anforderungen für die Bekämpfung von Cyber Security-Risiken

Über TÜV Rheinland.

TÜV Rheinland ist ein weltweit führender unabhängiger Prüfdienstleister, der vor 140 Jahren gegründet wurde. Der Konzern beschäftigt weltweit 19.600 Mitarbeiter; der Jahresumsatz beträgt knapp 1,9 Milliarden Euro. Seit mehr als 15 Jahren unterstützt TÜV Rheinland den privaten und öffentlichen Sektor mit umfassender Beratungs- und Lösungskompetenz in den Bereichen IT, Cybersecurity und Telekommunikation bis hin zu digitalen Transformationsprozessen.

Unterstützt durch mehr als 600 Spezialisten rund um den Globus bietet TÜV Rheinland vielfältige Services wie strategisches Consulting, Design- und Prozessoptimierung sowie Implementierung, Betrieb oder Zertifizierung von Systemen. Dank umfassenden technologischen Kompetenzen, langjähriger Erfahrung in Schlüsselbranchen und strategischen Partnerschaften mit Marktführern sind die Spezialisten von TÜV Rheinland in der Lage, innovative und zukunftssichere ICT-Lösungen zu entwickeln.

TÜV Rheinland bietet ausgeprägte Kompetenzen bei Informationstechnologien und kann Unternehmen bei der Optimierung von IT-Plattformen, dem Schutz von Informationsressourcen und der beschleunigten Einführung von strategischen Technologien unterstützen. Wir sind auf transformationale IT-Infrastrukturen, Sicherheit und Risiko-Consulting spezialisiert.

Wir unterstützen Unternehmen in verschiedensten Bereichen:

- Management von Cybersecurity-Risiken.
- Planung von Initiativen für die IT-Optimierung.
- Verlagerung der Computing-Abläufe zu virtuellen und cloudbasierten Infrastrukturen.
- Entwicklung von Anwendungen der nächsten Generation und von Rechenzentren, in denen es auf Sicherheit und Application Security der nächsten Generation ankommt.
- Koordinierung und Sicherstellung der Verbreitung des BYOD-Modells und von mobilen Endgeräten.
- Risikominimierung und Compliance im gesamten Unternehmen.
- Entwicklung von gut funktionierenden IT-Unternehmen bei gleichzeitiger Reduzierung der Kosten.

Ausführliche Informationen über TÜV Rheinland finden Sie unter www.tuv.com

TÜV Rheinland i-sec GmbH
Am Grauen Stein
51105 Köln
service@i-sec.tuv.com

www.tuv.com/fscs-de

TÜVRheinland®
Genau. Richtig.