

# WhitePaper

## Safety & Security in der Mensch-Roboter-Kollaboration

Einfluss der IT-Security

© ABB AG

Fotos

© Fotolia, Shutterstock, ABB AG

Impressum

© TÜV AUSTRIA HOLDING AG, TÜV Austria-Platz 1, 2345 Brunn am Gebirge  
FRAUNHOFER AUSTRIA RESEARCH GMBH, Theresianumgasse 7, 1040 Wien

# Mensch-Roboter- Kollaboration

*Einfluss der IT-Security*

*Dritte Ausgabe*

*Wien, 21.03.2018*



# Mensch-Roboter- Kollaboration

*Einfluss der IT-Security*

*Dritte Ausgabe*

*Wien, 21.03.2018*

TÜV AUSTRIA  
HOLDING AG  
TÜV AUSTRIA-Platz 1  
A-2345 Brunn am Gebirge

*Ing. Sabrina Steger, MSc*  
*DI Alexandra Markis*  
*DI Harald Montenegro, MSc*  
*Ing. Michael Neuhold*  
*Ing. Andreas Oberweger*  
*DI Christoph Schwald*

FRAUNHOFER AUSTRIA  
RESEARCH GMBH  
Theresianumgasse 27  
A-1040 Wien

*Prof. Dr.-Ing. Wilfried Sihn*  
*Fabian Ranz, MSc*  
*DI Thomas Edtmayr*  
*Dipl.-Wirtsch.-Ing. Philipp Hold*  
*DI Gerhard Reisinger*



# Mensch-Roboter- Kollaboration

## *Inhalt*

Abstract .....	9
1. Status-quo der IT-Security .....	10
2. Von der Information Technology zur Operational Technology .....	11
3. Angriffsflächen und Risiken industrieller Maschinen und Anlagen .....	12
4. Normen und Standards für die industrielle IT-Security .....	14
5. Praxisbeispiele zum vernetzten Einsatz von kollaborativer Robotik .....	16
5.1 Industrie 4.0 und Mensch-Roboter-Kollaboration bei ABB s.r.o. Elektro-Praga .....	16
5.2 Mensch-Roboter-Kollaboration in der TU Wien Pilotfabrik Industrie 4.0 .	18
6. Untersuchung von kollaborierenden Robotern aus Sicht der IT-Security .....	20
6.1 Allgemeiner Ablauf eines Sicherheitstests .....	20
6.2 Ergebnisse der Untersuchung bezogen auf das Produktionsnetzwerk .....	21
6.3 Ergebnisse der Sicherheitsüberprüfung bezogen auf kollaborierende Roboter .....	21
6.4 Zusammenhang der Gefährdungen der IT-Security mit der funktionalen Sicherheit .....	23
6.5 Gegenmaßnahmen (bezogen auf den Use Case TU Wien Pilotfabrik Industrie 4.0) .....	24
7. Integriertes Safety & Security-Konzept .....	25
7.1 Bestimmung der Maschinengrenzen und Vernetzung .....	26
7.2 Identifizierung der Gefährdungen .....	26
7.3 Risikoeinschätzung und -bewertung .....	26
7.4 Definition von Maßnahmen zur Risikominderung .....	27
8. Fazit und Ausblick .....	28
Quellen .....	30



## Abstract

Digitalisierung und Vernetzung machen auch vor Fabriken und Produktionsanlagen nicht halt: Anlagen werden bereits heute häufig aus der Ferne gesteuert oder gewartet, Mitarbeiter erhalten wichtige Informationen in Echtzeit auf Tablet oder Datenbrille, Prozesse werden Dank massenweise gesammelter Daten und entsprechender Datenanalysen transparenter und beherrschbarer. Immer mehr Geräte, Werkzeuge, Betriebsmittel und Maschinen in der Fabrik können, ganz der Idee und dem Paradigma von Industrie 4.0 folgend, Informationen über bekannte und weit verbreitete IP-basierte Protokolle empfangen, diese verarbeiten und andere Informationen an beliebige Stellen zurücksenden – das Internet der Dinge und die smarte Fabrik entstehen.

Für den effizienten Betrieb dieser smarten Fabrik ist es daher erforderlich, dass Maschinen und Anlagen jederzeit erreichbar sind und zur richtigen Zeit mit den richtigen Informationen versorgt werden, die sie für den reibungslosen Betrieb benötigen. Doch nicht nur die Effizienz, sondern auch die Sicherheit der Fabrik kann durch falsche, fehlerhafte oder fehlende Informationen gefährdet werden, indem Maschinen sich unvorhergesehen verhalten, Zustände einnehmen, die Beschädigungen oder gar Zerstörung hervorrufen – meist bewusst verursacht durch Schadsoftware oder Angreifer von außen.

Für Menschen bestehen hierdurch immer dann besonders große Risiken, wenn sie mit diesen Maschinen eng zusammenarbeiten – wie in der Mensch-Roboter-Kollaboration.

Eine wesentliche Erkenntnis aus der praktischen Arbeit des TÜV AUSTRIA ist, dass die funktionale Sicherheit von Maschinen und Anlagen durch Gefährdungen der Informationssicherheit kompromittiert werden kann – und insofern bei Risikobeurteilung und Zertifizierung von vernetzten Anlagen denselben Stellenwert wie die funktionale Sicherheit einnehmen muss.

In diesem dritten gemeinsamen White Paper zum Thema „Sicherheit in der Mensch-Roboter-Kollaboration“ von TÜV AUSTRIA und FRAUNHOFER AUSTRIA RESEARCH wird der wachsenden Rolle der Informationssicherheit in der modernen Fabrik Rechnung getragen und ihre Bedeutung am Beispiel Mensch-Roboter-Kollaboration herausgearbeitet.

Zu diesem Zweck geben die Autoren einen Überblick über den Stand des Themas industrieller IT-Security im Jahr 2018 und zeigen die Implikationen für den Anwendungsfall der Mensch-Roboter-Kollaboration anhand zweier praxisorientierter Anwendungsfälle auf.

Kernstück dieser Methoden ist die von TÜV AUSTRIA und FRAUNHOFER AUSTRIA RESEARCH entwickelte integrierte Beurteilung von funktionalen und informatorischen Gefährdungen innerhalb der Risikobeurteilung.

Insbesondere jedoch soll das Bewusstsein für die Abhängigkeit beider Welten im stark vernetzten und digitalisierten Szenario der Industrie 4.0 geschärft werden.



# 1. Status-quo der IT-Security

## Zahlen, Daten, Fakten

Beinahe täglich werden gezielte Cyberangriffe auf Unternehmen verübt. Cyber-Kriminalität gehört heute zu den bedeutendsten Bedrohungen für die weltweite Wirtschaft. Gleichzeitig wird die Abhängigkeit von Informationssystemen ständig größer, denn immer mehr Geschäftsabläufe funktionieren nur noch IT-gestützt.

Auch im Produktionskontext nimmt die Bedrohung durch Cyberangriffe zu: So konnten Angreifer 2014 durch Social Engineering Zugang zu einem Unternehmensnetzwerk innerhalb eines Stahlwerks in Deutschland bekommen, bis auf die Steuerungsebene der Anlagen vordringen und einen Schmelzofen in einen Zustand bringen, der zu seiner Beschädigung geführt hat, und gleichzeitig die Abschaltung des Ofens durch das lokale Personal unterbinden.

Bei einem Angriff über Fernzugriff auf ein amerikanisches Klärwerk 2011 wurde durch wiederholtes An- und Abschalten einer Pumpe deren Zerstörung herbeigeführt.

Doch auch in Österreich werden bereits seit 2013 jährlich deutlich über 10.000 IT-Sicherheitsvorfälle mit tatsächlichem Sicherheitsrisiko durch CERT, dem österreichischen nationalen Computer Emergency Response Team, registriert.

In Anbetracht der immensen Fallzahlen hat die EU-Kommission unlängst das Cybersicherheitsgesetz erlassen, welches Anbieter und Betreiber von Netzwerken und Diensten verpflichtet, Angriffe auf ihre Systeme behördlich zu melden.

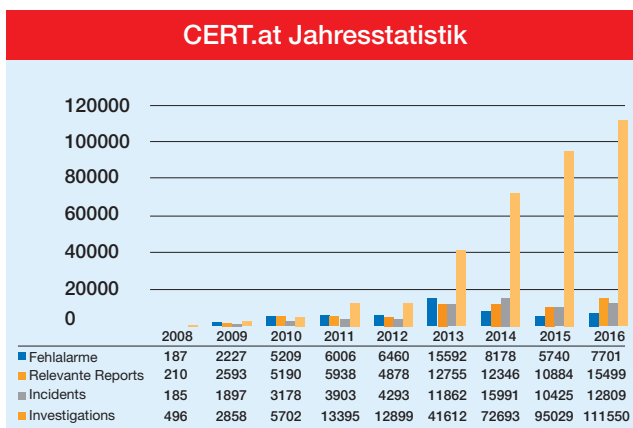


Abbildung 1: IT-Sicherheitsvorfälle in Österreich [2]

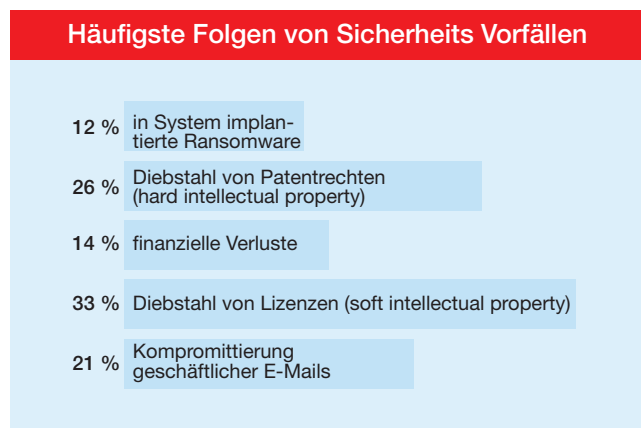


Abbildung 2: Folgen von IT- Angriffen [1]

Das Schlagwort Industrie 4.0 bezieht sich auf den Einzug des Internet der Dinge in die Fabrik: Maschinen, Anlagen und jegliche Art von Betriebsmitteln werden mittlerweile als cyber-physische Systeme (CPS) ausgeführt. Ein CPS stellt einen Verbund aus mechanischen und elektronischen Teilen sowie informativischen und softwarebasierten Komponenten dar. Durch die Verbindung von technischen und informationstechnischen Komponenten entstehen Maschinen, die sowohl im Hinblick auf ihre funktionale Sicherheit (Safety) als auch die informationstechnische Sicherheit (Security) kritisch sind.

Obwohl rund 40% der Unternehmen bereits mit externen Partnern zusammenarbeiten, um die Sicherheit ihrer IT-Systeme zu verbessern, und obwohl bereits einige Ansätze und Lösungen auch zur Sicherung von vernetzten Produktionssystemen existieren, sind diese nur vergleichsweise schwach oder häufig gar nicht abgesichert [1]. Grund dafür ist oftmals die strenge Trennung der Unternehmensbereiche, die für die klassische Unternehmens-IT und die Produktions-IT zuständig sind.



Abbildung 3: Cyber-Physisches System [4]

## 2. Von der Information Technology zur Operational Technology

In der klassischen unternehmerischen Organisation ist die Informationstechnologie (IT) gedanklich von der Operational Technology (OT), also der Produktions- und Betriebstechnik, getrennt – eine IT-Abteilung ist demnach zuständig für die gesamte zur Datenverarbeitung notwendige Technologie und ihre Sicherheit.

Sie beschäftigt sich aber üblicherweise nicht mit industriellen Systemen wie Robotern, Werkzeugmaschinen oder Förder-technik – und das war historisch betrachtet auch unproblematisch, denn üblicherweise waren industrielle Systeme nicht miteinander vernetzt, und schon gar nicht mit dem Internet verbunden. Bis 2025 sollen sich jedoch zwischen 25 und 50 Milliarden einzelne Geräte in Vernetzung befinden [3] – zu einem erheblichen Teil innerhalb von Fabriken.

Nutzen solche industriellen, cyber-physischen Systeme jedoch dieselben Kommunikationsmittel und -wege wie beispielsweise klassische Desktop-Computer in der Verwaltung, und beziehen sie Informationen beispielsweise aus denselben Unternehmenssystemen oder liefern sie Daten dorthin zurück, so entstehen Schnittstellen und Abstimmungsbedarf zwischen eben jener IT und OT.

	Office-IT=IT	Operational IT=OT
Lebensdauer	3-5 Jahre	5-20 Jahre
Patchmanagement	oft bis täglich	Selten, benötigt Freigabe oder Unterstützung des Maschinenherstellers
Zeitabhängigkeit	Verzögerungen akzeptiert	Kritisch
Verfügbarkeit	Kurze Ausfälle toleriert	Stände Verfügbarkeit vorausgesetzt

Abbildung 4: Unterschiede zwischen IT und OT [5]

Damit müssen OT-Systeme sicherheitstechnisch genauso betrachtet und geschützt werden, wie herkömmliche IT-Systeme und gleichwertig in die unternehmensweiten Überlegungen und Maßnahmen zu IT-Security einbezogen werden – oder sogar noch intensiver. Denn die Erwartungen an die Ausfallsicherheit, Zuverlässigkeit, Funktionstüchtigkeit und -sicherheit einer industriellen Anlage sind höher als in der Office Umgebung und können aufgrund ihrer Versorgungsfunktion, beispielsweise für die Bevölkerung, von immenser Bedeutung sein.

Aus diesem Grund ist eine ganzheitliche Betrachtung von funktionaler Sicherheit und IT-Security künftiger Infrastrukturen im Industrie 4.0-Umfeld unumgänglich, um das volle Potenzial der Technologien heben zu können.

### 3. Angriffsflächen und Risiken industrieller Maschinen und Anlagen

Die Möglichkeiten zum Eindringen in die IT-Infrastruktur einer industriellen Anlage sind für einen Angreifer vielfältig. Dies spiegelt sich auch bei einem Blick auf die wichtigsten Bedrohungen wider, welchen sich Industrie- und Fertigungsanlagen ausgesetzt sehen (vgl. Abb. 5). Bei diesen handelt es sich im Wesentlichen um Primärangriffe: Diese Methoden werden häufig von Angreifern genutzt, um in Industrieanlagen einzudringen, wodurch Sabotage und Manipulation in der Folge ermöglicht werden.

Nr.	Top 10 (2016)	Top 10 (2014)
1	Social Engineering and Pishing	Infektion mit Schadsoftware über Internet und Intranet
2	Einschleusen von Schadsoftware über Hardware (z.B. USB-Sticks)	Einschleusen von Schadsoftware über Hardware (z.B. USB-Sticks)
3	Infektion mit Schadsoftware über Inter- und Intranet	Social Engineering
4	Einbruch über Wartungsfernzugänge	Menschliches Fehlverhalten/Sabotage
5	Menschliches Fehlverhalten/Sabotage	Einbruch über Fernwartungszugänge
6	Internet verbundene Steuerungskomponenten	Internet verbundene Steuerungskomponenten
7	Technisches Fehlverhalten, höhere Gewalt	Technisches Fehlverhalten, höhere Gewalt
8	Kompromittierung von Extranet und Cloud-Komponenten	Kompromittierung von Smartphones im Produktionsbetrieb
9	(D) DoS Angriffe	Kompromittierung von Extranet und Cloud-Komponenten
10	Kompromittierung von Smartphones im Produktionsbetrieb	(D) DoS Angriffe

Abbildung 5: Häufigste Ursachen von Primärangriffen [6]

Durch diese Zugriffsgefährdungen ergeben sich potenziell Auswirkungen für die wesentlichen Schutzziele der Informationssicherheit, die genauso für industrielle Maschinen und Anlagen gelten, wie für herkömmliche IT-Systeme. Demnach dürfen Systemen nicht unautorisiert Informationen entnommen (Confidentiality) werden, Daten innerhalb der Systeme dürften nicht unautorisiert und unbemerkt manipuliert (Integrity) werden, und die (übliche, vorgesehene) Verfüg- und Nutzbarkeit des Systems darf nicht eingeschränkt werden (Availability). In der Fachsprache werden diese Schutzziele in der sogenannten **CIA Triade** zusammengefasst.

Werden diese Schutzziele verletzt, können sich hieraus Folgeschäden immensen Ausmaßes ergeben – von finanziellen Verlusten durch Anlagenstillstand oder -beschädigung, über Wettbewerbsnachteile durch Informationsverlust bis hin zu Verletzungen von Mitarbeitern durch außer Kontrolle geratene Maschinen. Insbesondere bei Maschinen und Anlagen, von denen im Falle der Manipulation eine Gefahr für Menschen im Sinne der funktionalen Sicherheit ausgehen kann, nimmt daher die Integrität eine herausragende Stellung ein.

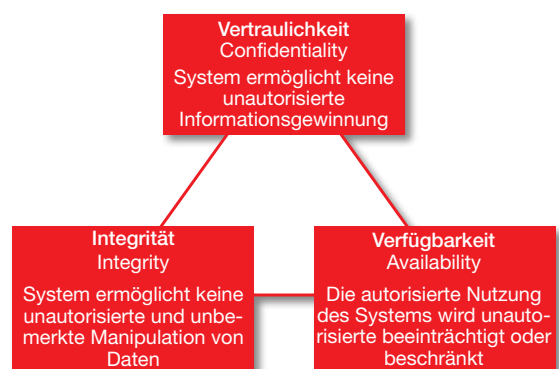


Abbildung 6: Schutzziele gemäß CIA-Triade

## 4. Normen und Standards für die industrielle IT-Security

Der Betreiber einer industriellen Anlage wird, analog der funktionalen Sicherheit, auch in Bezug auf IT-Security durch spezielle Normen und Richtlinien bei der Sicherstellung der Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität angeleitet und unterstützt. Praktisch existieren jedoch Hunderte nationale und internationale IT-Security-Standards, von denen sich immer noch mehr als ein Dutzend auf industrielle Automatisierungs- und Steuerungssysteme beziehen.

Analog zur ISO 27001, welche Anforderungen an allgemeine IT-Systeme stellt, befasst sich die **Standardfamilie IEC 62443** speziell mit industriellen Automatisierungs- und Steuerungssystemen und liefert eine konkrete Handlungsempfehlung für die drei wesentlichen mit der Erstellung und dem Betrieb befassten Zielgruppen: Anlagenbetreiber, Anlagenbauer und Komponentenhersteller.

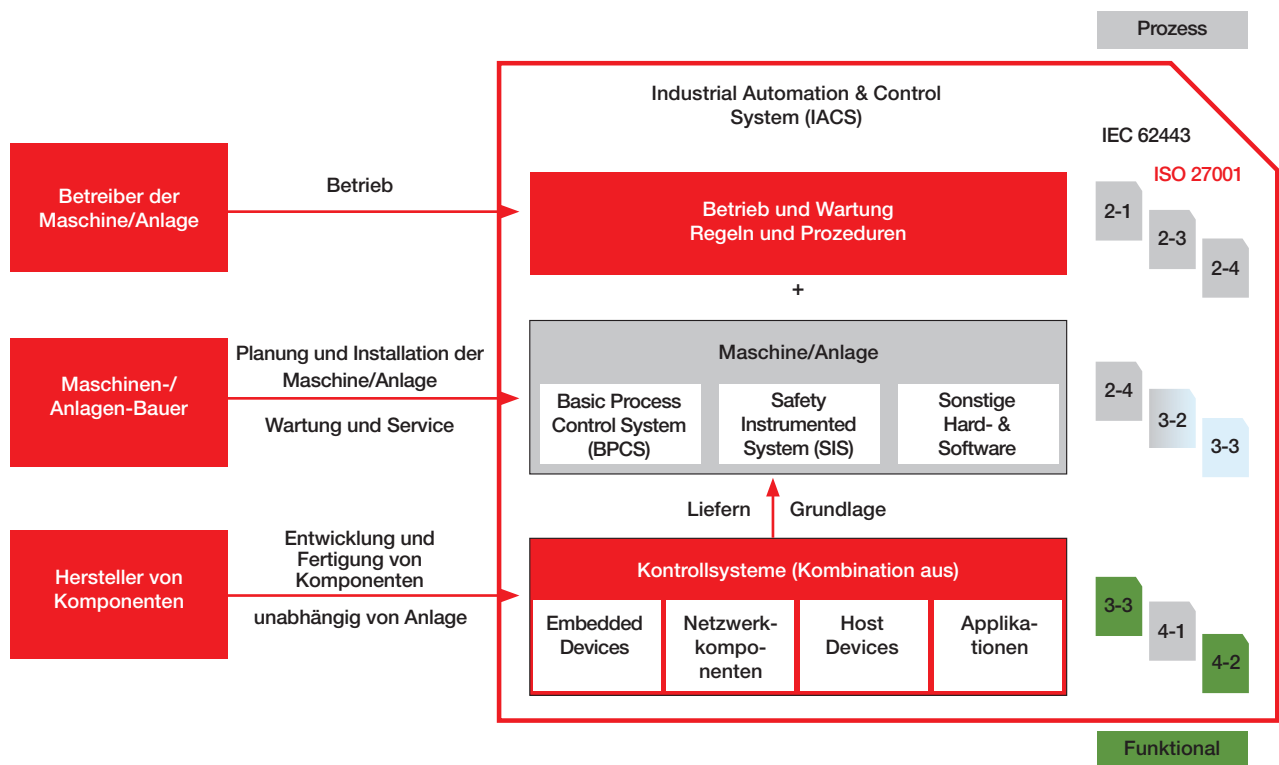


Abbildung 7: Zielgruppen und Struktur der Normenfamilie IEC 62443 [7]

Orientierung bei der Auslegung von Maschinen, Anlagen und anderen Geräten für das industrielle Internet der Dinge kann auch das **Open Web Application Security Project, kurz OWASP**, bieten. Bei OWASP handelt es sich um ein für jeden frei zugängliches Projekt, welches sich für die Erhöhung von IT-Sicherheitsstandards auch für Internet der Dinge-fähige Endgeräte einsetzt und hierzu zehn zu vermeidende Schwachstellen und jeweilige Gegenmaßnahmen formuliert hat.



Abbildung 8: Typische Schwachstellen von IoT-Devices [8]

Ein drittes Rahmenwerk mit Bezug zur IT-Security, welches insbesondere auch für industrielle Maschinen und Anlagen herangezogen werden kann, ist das Framework for Improving Critical Infrastructure Cybersecurity des **National Institute for Standards and Technology (NIST)**. Es formuliert weniger konkrete Anforderungen an das Design und die Auslegung von Maschinen und Anlagen, die auch vernetzt sicher betrieben werden können, als dass es ein methodisches Vorgehen für Anlagenbetreiber zur Risikoidentifizierung, -bewertung und -bekämpfung darlegt und Empfehlungen für dessen organisatorische Verankerung gibt.

Unter Berücksichtigung dieser verfügbaren Referenzwerke und der in ihnen enthaltenen Empfehlung wäre die Erwartung naheliegend, dass Hersteller moderner industrieller Anlagen diese bereits berücksichtigt haben und moderne Maschinen keine oder nur sehr wenige Angriffsflächen für Manipulation und Sabotage über den Informationsweg aufweisen – also auch in stark vernetzten Industrie 4.0-Szenarien bedenkenlos betrieben werden können.

In der „klassischen“ Fabrik werden Anlagen in der Regel lokal programmiert, und verfügen nur teilweise über Schnittstellen, um beispielsweise Programme zu laden oder Daten zu sichern. Findet die Vernetzung einzelner Maschinen miteinander auf Grundlage von kabelgebundener Automatisierungstechnik, wie mit Hilfe speicherprogrammierbarer Steuerungen, statt, so sind diese Netze häufig isoliert und haben keinen Kontakt zur Außenwelt. Die in der Industrie 4.0 verfolgte Flexibilitätssteigerung ergibt sich jedoch zu großen Teilen aus vertikaler und horizontaler Vernetzung von Teilsystemen, um beispielsweise Maschinen schneller mit ständig wechselnden Auftragsinformationen zu versorgen oder ihre Fernwartung zu ermöglichen, wie auch die folgenden Beispiele zeigen.

## 5. Praxisbeispiele zum vernetzten Einsatz von kollaborativer Robotik

Industrieroboter feierten 2017 mit einem weltweiten Absatz von knapp 350.000 Stück ein Rekordjahr, was einem Plus von 18% gegenüber 2016 entspricht.

Das weltweite Marktvolumen wurde 2017 auf 50 Milliarden Dollar geschätzt. Zwei Millionen Roboter sind weltweit im Einsatz, bis 2020 sollen es nach Prognosen des Branchenverbandes International Federation of Robotics (IFR) bereits drei Millionen sein. Weiteres Wachstum in der weltweiten Roboterpopulation erwartet die IFR vor allem durch das zunehmende Angebot an kollaborierenden Leichtbaurobotern und die verbesserten Möglichkeiten zur Vernetzung im Rahmen des Internets der Dinge und Industrie 4.0. Einblick in diese Entwicklung sollen die folgenden beiden Praxisbeispiele geben.

### 5.1 Industrie 4.0 und Mensch-Roboter-Kollaboration bei ABB s.r.o. Elektro-Praga



Abbildung 9: MRK-Applikation mit ABB YuMi

Ein industrielles Beispiel für die Zusammenarbeit von Menschen mit vernetzten Robotern findet sich bei Elektro-Praga, einer ABB-Tochter in Tschechien. An kollaborativen Arbeitsplätzen montieren Mensch und Roboter gemeinsam handelsübliche Steckdosen. Dabei werden die Aufgaben des Montageprozesses aufgrund der individuellen Fähigkeiten von Mensch und Maschine aufgeteilt.

**Kerninfos**     *Roboter:* IRB 14000-0.5/0.5 - YuMi®     *Reifegrad:* Industrieller Einsatz

*Art der Zusammenarbeit:* Kollaboration     *Prozessbereich:* Montage

---

**Anwendung**     Der Arbeitsplatz besteht aus einem menschlichen Bediener, einem Leichtbauroboter ABB YuMi, diversen Sensoren, Förderbändern, Vibrationsförderern und einem System zum Entwirren der Federn. Während des Prozesses montiert YuMi die Federn, die Kindersicherungen sowie deren Abdeckungen auf die Steckdosen. Der Montageprozess wird dabei vom Bediener ausgelöst, welcher zuvor zwei Deckel sowie zwei Abdeckungen für die Kindersicherungen vor dem Roboter auflegt. Anschließend nutzt YuMi seine Vakuumsauger um die Kindersicherungen aus dem Vibrationsförderer zu greifen und in die vorbereitenden Deckel der Steckdosen einzulegen. Danach nimmt YuMi die entsprechenden Federn aus der Zuführeinheit (zwei Teile pro Sockel) und legt diese in den Zwischenraum der Steckdosen. In die nun vorbereitete Baugruppe wird vom Roboter die Abdeckung für die Kindersicherung eingesetzt. Der Montagevorgang seitens YuMi wird beendet, indem dieser die Abdeckung in den Deckel einklippt. Abschließend setzt der Bediener noch eine Schraube in die Steckdose ein und legt diese in die entsprechende Verpackung. Zusätzlich zum Teilehandling ist der Bediener ebenfalls verantwortlich für die Überwachung des kompletten Prozesses und kann bei Bedarf eingreifen

- Ziele**
- ▶ Entlastung des Mitarbeiters durch Übertragung der nicht ergonomischen Tätigkeit an den Roboter
  - ▶ 20% höhere Ausbringungsmenge durch Arbeitsteilung zwischen Mensch und Maschine
- 

<b>Produkt</b>	<i>Produkt:</i> Steckdosen	<i>Abmessungen:</i> ca. 80x80x14 mm	<i>Gewicht:</i> ca. 10 g
----------------	-------------------------------	--	-----------------------------

---

### Sicherheitskonzept

- Umgebung:** ▶ Schutzbrille für Mitarbeiter, Vermeidung von scharfen Kanten und Ecken, Kennzeichnung durch Hinweisschilder
- 

- Werkzeug:** ▶ Ein Greifer verwendet nur Vakuumsauger, zweiter Greifer wurde für eine kollaborative Tätigkeit angepasst, keine scharfen Kanten und Ecken am Greifer
- 

- Programm:** ▶ Bewegungen des Roboters im Arbeitsbereich auf das Nötigste reduziert (keine „ausschweifenden Bewegungen“ der Arme), Vermeidung von Bewegungen welche zu Scherungen führen könnten
- 

**Zertifizierung:** ▶ Eigenzertifizierung

ABB bietet für YuMi digitale Dienstleistungen für die Zustandsüberwachung, Wartung und Anlagenoptimierung. Die Anbindung erfolgt kabellos oder per LAN. Die MyRobot-Homepage mit Alarm-Dashboard bildet die Schnittstelle zu Connected Services. Über das Alarm-Dashboard werden sowohl Kunden als auch das ABB-Serviceteam mit Informationen versorgt. Die Anwendung zeigt auftretende Störungen und Fehlermeldungen, die zu Ausfällen führen können und analysiert Trends und Warnungen, benachrichtigt und bietet Support im Falle von Problemen. Die ABB Ability™ Connected Services bestehen aus fünf Bausteinen: Condition Monitoring & Diagnostics (Zustandsüberwachung und Diagnose), Backup-Management, Remote Access (Fernzugriff), Fleet Assessment (Beurteilung des Roboter-Bestands) und Asset Optimization (Systemoptimierung).

Damit entspricht die illustrierte Anwendung stark der Idee von Industrie 4.0 – enge Zusammenarbeit von Mensch und Maschine, hoher Grad von Vernetzung und eine mehrwertstiftende Nutzung der dabei entstehenden Daten.

Dabei ergeben sich jedoch auch Fragen nach der IT-Security solcher vernetzter Roboterapplikationen. In Kapitel 7 wird im Forschungsumfeld der TU Wien Pilotfabrik Industrie 4.0 die IT-bezogene Sicherheit von standardmäßigen, artikulierte kollaborativen-Robotern untersucht.

## 5.2 Mensch-Roboter-Kollaboration in der TU Wien Pilotfabrik Industrie 4.0

In der Ausgangssituation bildet die TU Wien Pilotfabrik Industrie 4.0 ein typisches industrielles Montagesystem ab, dessen Infrastruktur durch einen hohen Vernetzungsgrad gekennzeichnet ist. Die Pilotfabrik Industrie 4.0 produziert 3D-Drucker in kundenspezifischen Ausführungen. Im Rahmen der Montage des Extruderschlittens des 3D-Druckers kommt ein Leichtbauroboter in direkter Mensch-Roboter-Kollaboration zum Einsatz, welcher den Mitarbeiter bei statischer Haltearbeit unterstützt bzw. entlastet.



- Werkzeug:**
- ▶ Abdeckkappen für Greiferkinematik und Flächenvergrößerung an Greiferspitzen
  - ▶ Absicherung der Werkzeugschnittstelle am Flansch durch Schutzring

- Programm:**
- ▶ Vermeidung von Scherstellen durch vertikale Pfadauslegung
  - ▶ Überwachung der Greifkraft zur Erkennung falscher Objekte (nicht sicherheitsgerichtet)

**Zertifizierung:** ▶ nicht zertifiziert, da Forschungs- und Versuchsaufbau

Ein ERP-System, welches Cloud-basiert bereitgestellt wird, steuert Produktionsaufträge in die Fabrik ein. Diese werden von der Montagesteuerung verarbeitet und an die einzelnen Montagestationen verteilt. Die Mitarbeiter erhalten Montageanweisungen über Tablet Computer. Betriebsmittel wie ein elektronisches Kanban-System oder intelligente Schraubsysteme sind ebenso über Ethernet angebunden und kommunizieren bi-direktional mit der Montagesteuerung. Auch der eingesetzte Roboter kommuniziert mit den übergeordneten Steuerungssystemen, er erhält unter anderem Startsignale für die Aufnahme des Extruderschlittens, die Koordinaten für dessen Positionierung über dem Werkstück und meldet die erfolgreiche Aufgabenausführung zurück.

Das Netzwerk innerhalb der Fabrik ist über einen zentralen Router mit dem Internet verbunden, über Access Points wird außerdem WLAN für Mitarbeiter und Besucher bereitgestellt.

Ein einfaches Netzwerkdiagramm, wie es auch die IEC 62443 zu erstellen empfiehlt, verschafft einen Überblick über die Einzelkomponenten und die Gesamtstruktur.

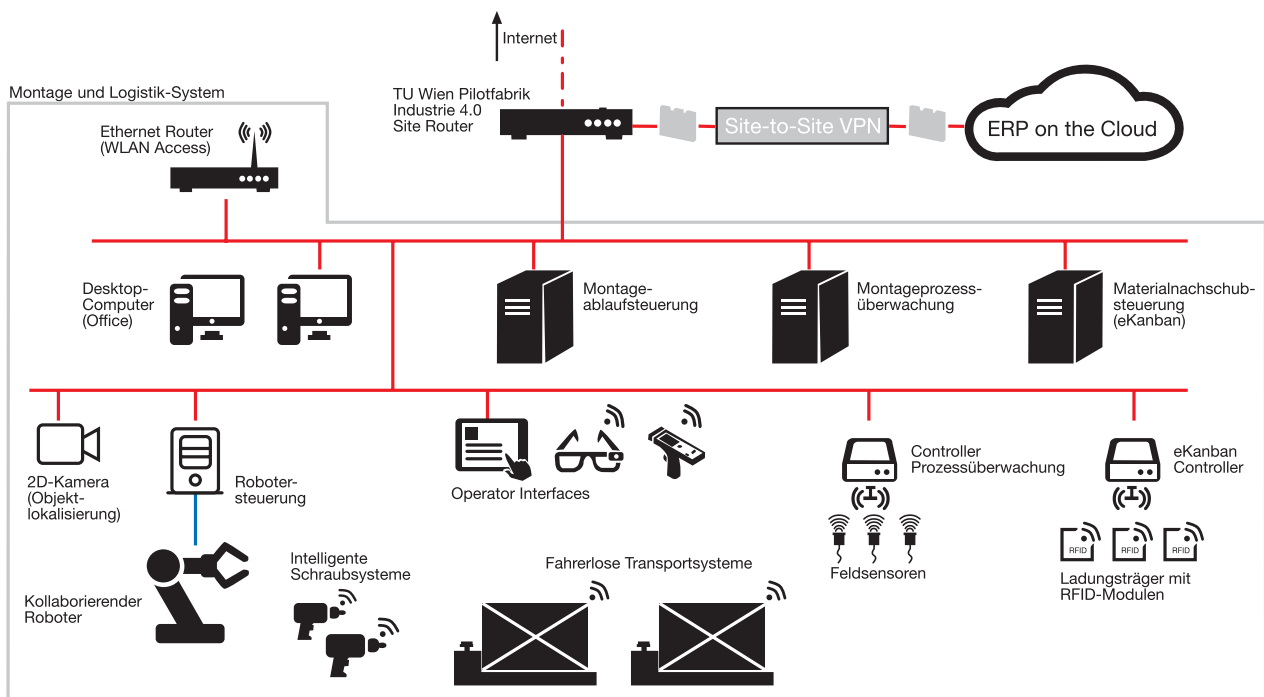


Abbildung 11: Ausgangssituation Netzwerkarchitektur TU Wien Pilotfabrik Industrie 4.0 (vor Optimierung)

An diesem Beispielszenario wird nachfolgend einerseits die Notwendigkeit einer ganzheitlichen Systembetrachtung zur Berücksichtigung von IT-Security in der vernetzten Fertigung und andererseits die Wichtigkeit einer integrativen Betrachtung von funktionaler Sicherheit und IT-Security auf der Basis einzelner Maschinen und Anlagen am Beispiel eines Leichtbau-roboters in der Mensch-Roboter-Kollaboration herausgearbeitet.

## 6. Untersuchung von kollaborierenden Robotern aus Sicht der IT-Security

### 6.1 Allgemeiner Ablauf eines Sicherheitstests

Nachfolgend wird der allgemeine Ablauf eines Sicherheitstests (Penetrationstests) beschrieben.

Im Rahmen der **Vorbereitung** werden die Ziele, der technische und zeitliche Scope und die Art der Sicherheitsüberprüfung erarbeitet und festgelegt. Im Industrieumfeld macht es Sinn ausführliche Informationen über die Geräte und Anlagen mitzuteilen um die Prüfung zielgerichtet darauf abzustimmen.

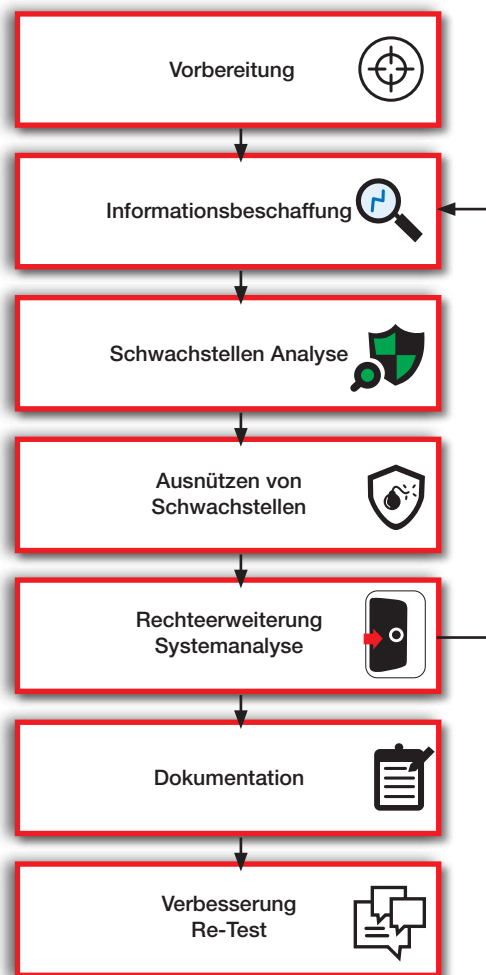


Abbildung 12: Testablauf IT-Security

In der Phase der **Informationsbeschaffung** wird die Angriffsfläche identifiziert, was als Grundlage für die Gestaltung von Angriffsszenarien dient.

In der dritten Phase eines Penetrationstests werden **Schwachstellen identifiziert und validiert**. Dabei werden Abfragen abgesetzt, welche in der normalen Benutzung nicht vorkommen um Sicherheitsdefizite aller Art zu identifizieren.

In den anschließenden Phasen werden die zuvor ermittelten **Schwachstellen ausgenutzt**. Dies kann das Ausnutzen einer bereits bekannten Schwachstelle sein oder auch das Selbsterstellen von Angriffsskripten. In der Fachsprache wird von Exploitation gesprochen.

Wurde einmal Zugriff zum System erreicht, ist der nächste Schritt seine **Rechte auf Administrationsrechte (root)** zu erweitern und die Systemanalyse fortzusetzen indem der Zugriff auf weitere Geräte getestet wird.

In diesen Phasen wird weiter versucht die Vertraulichkeit und Integrität zu gefährden. Ist die Verfügbarkeit in einer Form in Gefahr, wird dies im Bericht aufgezeigt, aber nicht aktiv ausgenutzt.

Abschließend werden die gefundenen Schwachstellen in Form von „**Findings**“ nachvollziehbar dokumentiert und einer Risikobewertung unterzogen. Es ist essentiell zu erläutern wie die Schwachstelle ausgenutzt wurde und Empfehlung, sowie mögliche kompensierende oder Härungsmaßnahmen abzugeben.

Nachdem der Bericht erstellt wurde, wird dieser ausführlich mit allen Beteiligten besprochen und Maßnahmen für die Umsetzung festgelegt. Nach der Umsetzung ist es sinnvoll einen Re-Test durchzuführen um die Wirksamkeit zu überprüfen.

### 6.2 Ergebnisse der Untersuchung bezogen auf das Produktionsnetzwerk

Die beschriebene Vorgehensweise zur Durchführung von Penetrationstests aus Kapitel 6.1 wurde von IT-Security Experten des TÜV AUSTRIA auf das skizzierte Produktionsnetzwerk der TU Wien Pilotfabrik Industrie 4.0 allgemein und unterschiedliche kollaborative Leichtbauroboter im Speziellen angewendet. Im Ausgangszustand wurden bei der Gestaltung und Einrichtung des Produktionsnetzes keine Sicherheitsmaßnahmen explizit bedacht und umgesetzt.

Als Eintrittspunkt in das Netzwerk diente das von den Access Points bereitgestellte Wireless LAN um das Passwort über einen Brute Force Angriff zu knacken.

Da die IT-Infrastruktur nicht in einzelne Zonen oder Bereiche unterteilt war, sondern das gesamte Produktionssystem in lediglich einem großen Netz betrieben wurde, konnten durch Einsatz eines Netzwerk-Scanners alle in diesem Netzwerk befindlichen Geräte und Maschinen lokalisiert werden – darunter klassische IT-Komponenten wie Rechner, Netzwerkdrucker und Server, aber auch die Komponenten der OT-Infrastruktur, welche unter anderem kollaborierende Roboter, Schraubsysteme und Transportsysteme beinhalten.

Der Zugriff auf und die Konfiguration und Programmierung einzelner Geräte und Maschinen war teilweise über Web-Oberflächen möglich. Die in der TU Wien Pilotfabrik Industrie 4.0 eingesetzten Geräte und Maschinen verfügten in Einzelfällen über keinen Passwortschutz, teilweise über werkseitig voreingestellte oder nur sehr schwache Passwörter und konnten rasch angesteuert und manipuliert werden.

War der Datenverkehr nicht verschlüsselt, was bei den eingesetzten und getesteten Geräte und Maschinen der Fall war, konnte dieser im Klartext mitgelesen werden.

Dies betraf nicht nur Zugangsdaten und Passwörter, sondern auch die reguläre Kommunikation zwischen den Geräten. So hätte ein Angreifer die Logik des Informationsaustausches nachvollziehen und falsche bzw. manipulierte Informationen (z.B. Aufträge oder Konfigurationsparameter) versenden können, welche zu Fehlverhalten oder Ausfall von Maschinen und Anlagen führen können.

### *6.3 Ergebnisse der Sicherheitsüberprüfung bezogen auf kollaborierende Roboter*

Die Möglichkeiten des Angreifers zur Störung des Betriebs, insbesondere in Bezug auf die Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität auf Ebene einzelner Maschinen und Anlagen werden am Beispiel kollaborierender Roboter dargestellt und eine Auswahl der Ergebnisse (Findings) im folgenden Abschnitt präsentiert.

Es wurde davon ausgegangen, dass sich der Angreifer in der in Abb. 11 beschriebenen Netzwerkarchitektur im selben Netz wie der Roboter befindet. Im Regelbetrieb erhält der Roboter Befehle und Anfragen ausschließlich von der Montagesteuerung (Programme laden, Programme starten, Rückmeldungen senden).

In Kenntnis der IP-Adresse hätte ein Angreifer nun ebenfalls **Befehle an den Roboter** senden oder Statusinformationen von diesem können. Weiterhin konnte von den Experten des TÜV AUSTRIA der Programmablauf gestoppt oder der Roboter auch teilweise komplett abgeschaltet werden. Durch ein Abschalten des Roboters ist das Schutzziel Verfügbarkeit gefährdet und es kommt zu einem Stillstand der Produktionsanlage. Gerade in Industriebetrieben ist die Verfügbarkeit von Maschinen elementar und kann bei einem Stillstand zu einem hohen Kostenfaktor werden.

Darüber hinaus konnten teils **Quittierungen von Meldungen und Störungen** aus der Ferne durchgeführt werden. Dazu zählen auch Sicherheitsstopps nach einer Kollision mit einem Menschen oder einem Gegenstand. Dies kann zu einer Gefährdung der funktionalen Sicherheit führen, da der Roboterlauf fortgesetzt wird, ohne, dass der vor Ort befindliche Mitarbeiter darauf vorbereitet ist, sodass es zu einer erneuten Kollision kommen kann. Das bedeutet, dass der Mensch durch mangelhaft ausgeführte IT-Security direkt in seiner persönlichen Sicherheit gefährdet ist.

Deutlich erschwerend kommt hinzu, dass einzelne Roboter beim Versuch des Zugriffs **keinerlei Authentifizierung**, beispielsweise durch Nutzernamen und Passwort, verlangen, und auch keine Autorisierung durchführen, sondern jeden an sie gesendeten Befehl von beliebigen Absendern vollkommen bedingungslos ausführen – was auch für die erwähnten „kritische“ Befehle wie für das völlige Abschalten des Roboters oder die Lösung/Quittierung eines Sicherheitsstopps zutrifft.

Im Rahmen der weiteren Tests konnten die Auditoren Administrationsrechte erreichen, um gespeicherte **Roboterprogramme zu öffnen, einzusehen, zu verändern** und diese Änderungen zu speichern. Damit sind die Schutzziele der Integrität und Vertraulichkeit nicht mehr gegeben. Einerseits ergibt sich hieraus eine für den Betreiber unvorhergesehene Veränderung des Bewegungs- bzw. Programmablaufs des Roboters, andererseits kann hierdurch auch die Sicherheit von Unternehmensinformationen gefährdet werden, indem Programme, welchen spezifisches Know-how zu Produkten oder Prozessen innewohnt, kopiert und gestohlen werden können. Ebenso konnten **gesetzte Passwörter überschrieben** werden, womit die Betreiber des Roboters keine Möglichkeit mehr haben, die Einstellungen selbst zu verändern. In weiterer Folge wird dadurch die Verfügbarkeit der Anlage gefährdet.

Letztlich konnten teilweise auch neue Installationsdateien, welche auch die Safety-Konfiguration, darunter zulässige Kräfte, Geschwindigkeiten und Safety Grenzen, enthalten, geladen werden. Damit wird das Schutzziel der Integrität abermals verletzt und ein Angreifer kann Daten am Roboter für seine Zwecke verändern und wiederum die funktionale Sicherheit

kompromittieren, wenn der Roboter beispielsweise mit einer höheren als der vorgesehenen Geschwindigkeit in den Arbeitsbereich eindringt.

Problematisch ist auch, dass die Verbindlichkeit (non-repudiability) als weiteres Schutzziel nicht gegeben ist. Es wurde identifiziert, dass Zugriffe und Befehle von außen in den Log-Files des Roboters, die üblicherweise auch von jeder anderen Maschine geführt werden, kaum oder gar nicht dokumentiert wurden. Damit ist der Ursprung einer unerwarteten (oder sogar böswilligen) Verhaltensweise völlig unklar und es können keinerlei Rückschlüsse auf den Verursacher (Angreifer) getroffen werden.

Im Ergebnis zeigt sich, dass nicht alle kollaborierenden Roboter, welche aufgrund ihres geringen Eigengewichts und der verbauten Sensorik auch für die Zusammenarbeit mit Menschen geeignet sind, die wesentlichen Anforderungen an die IT-Sicherheit vernetzter Geräte aus der IEC 62443 oder anderer Rahmenwerke werksseitig erfüllen.

Gleichsam ist es für den Maschinenbetreiber, je nach Einzelfall, schwierig bis unmöglich, diese maschinenbezogenen Schwachstellen zu beheben. Aus diesem Grund ist die gestaffelte Verteidigung von großer Bedeutung: Bereits „vor“ der Maschine auf den Ebenen der Netzwerkhard- und -software Schutzmaßnahmen zu treffen, die einem Angreifer den Zugriff auf die Maschine verhindern.

In der Folge wird der Zusammenhang zwischen den identifizierten Defiziten in Bezug auf die IT-Security und die funktionale Sicherheit diskutiert.

## 6.4 Zusammenhang der Gefährdungen der IT-Security mit der funktionalen Sicherheit

Die funktionale Sicherheit von Maschinen verlangt, dass physische Restrisiken für Mitarbeiter, insbesondere Verletzungsrisiken, die von einer Maschine oder Anlage, wie beispielsweise einer MRK-Applikation, ausgehen, eine bestimmte Höhe nicht überschreiten.

In Bezug auf den dargelegten Anwendungsfall der Mensch-Roboter-Kollaboration können dazu technischen Maßnahmen, wie beispielsweise die Reduzierung der Verfahrensgeschwindigkeiten des Roboters gesetzt werden, um im Fall eines Kontaktes zwischen Mensch und Roboter nur geringe Kollisionskräfte freizusetzen.

Ein zweites Beispiel wäre die Auslegung des Fahrweges in einer solchen Weise, dass Abstände des Manipulators zu physischen Aufbauten des Arbeitsplatzes zu jeder Zeit so groß sind, dass keine Quetschstellen entstehen können.

Lokal kann die Programmierung dieser technischen Maßnahmen zur Erhöhung des funktionalen Sicherheitsniveaus vor bewusster oder unbewusster Veränderung und Manipulation geschützt werden – z.B. durch das Hinterlegen unterschiedlicher Nutzerberechtigungen für Maschinenführer und Programmierer oder Passwörter im Bedienteil des Roboters.

Wie die durchgeführten Versuche und Sicherheitstests jedoch gezeigt haben, können über die Netzwerkverbindung des Roboters Angreifer, abhängig vom spezifischen Robotermodell, teilweise eben jene technischen Sicherheitsmaßnahmen kompromittiert werden: Die Veränderung von Sicherheitskonfiguration und von Ablaufprogrammen oder auch das Quittieren von Sicherheitsstopps und das erneute Starten und Anfahren des Programms sind aus der Ferne und mit Hilfe einfacher, über Ethernet an den Roboter gesendete Befehle teilweise problemlos möglich.

Davon bekommt der Nutzer oder Bediener vor Ort, welcher mit dem Roboter interagiert, nichts mit. Dass die Maschine nun nicht mehr der ursprünglichen Spezifikation, welche auch risikobeurteilt wurde, entspricht, sich unerwartet verhalten könnte und größere als angenommene Risiken von ihr ausgehen, bleibt für ihn im Verborgenen.

Damit zeigt sich, dass eine isolierte Betrachtung funktionaler Sicherheit beim Betrieb von vernetzten Maschinen und Anlagen nicht zielführend ist, da diese Maschinen potenziell – und dies muss im Einzelfall geprüft werden – Defizite im Bereich der IT-Security aufweisen, durch welche technische Sicherheitsmaßnahmen kompromittiert werden können. Sicherheitskonzepte im Sinne von **Security for Safety** sind somit unumgänglich.



Abbildung 13: Zusammenhang Safety und Security

## 6.5 Gegenmaßnahmen

### (bezogen auf den Use Case TU Wien Pilotfabrik Industrie 4.0)

Um diese Maschinen dennoch vernetzt betreiben zu können, bietet das Produktionsnetzwerk Ansatzpunkte zur Absicherung: Im ersten und maßgeblichen Schritt müssen zunächst, wie in den Abschnitten zuvor skizziert und detailliert in Kapitel 7 beschrieben, die vorherrschenden Gefährdungen identifiziert und bewertet werden. Darauf basierenden werden dann entsprechende Maßnahmen zur Risikosenkung abgeleitet. Hilfestellung dazu liefert die IEC 62443. Die Befolgung dieser Maßgaben kann die Gesamtsicherheit eines Produktionssystems vor Angriffen, Sabotage und Manipulation massiv erhöhen und den vernetzten Betrieb von Maschinen und Anlagen, die für sich genommen ggf. deutliche Sicherheitslücken aufweisen, in einem stark geschützten Netzwerk ermöglichen.

Zur Umsetzung dieser abgeleiteten Maßnahmen wurde durch **Phoenix Contact**, einem spezialisierten Komponentenhersteller und Dienstleister im Bereich der Elektrotechnik, Elektronik und Automatisierung, das Netzwerk der TU Wien Pilotfabrik Industrie 4.0 „zoniert“, also in Abschnitte eingeteilt. Einzelne Zonen sind durch Barrieren voneinander getrennt, welche basierend auf ihrer jeweiligen Konfiguration die Kommunikation zwischen zwei Zonen regeln. Solche Barrieren können Router, Switches oder physische Firewalls sein. Innerhalb einer Zone sind jeweils Geräte und Anlagen gemeinsamen Risikoniveaus oder derselben Schutzbedürftigkeit zusammengefasst.

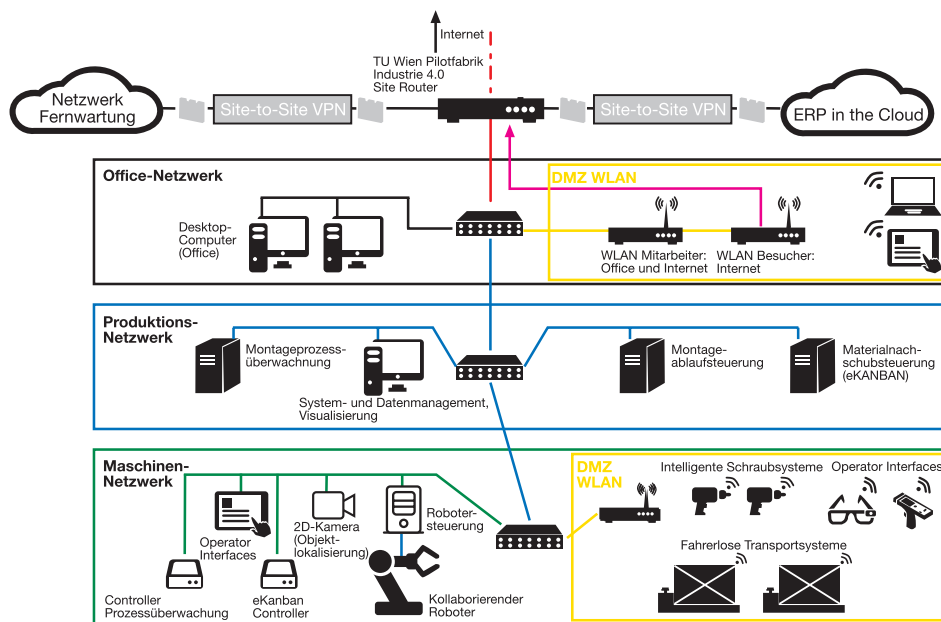


Abbildung 14: Netzwerkarchitektur TU Wien Pilotfabrik Industrie 4.0 (nach Optimierung)

Insbesondere die Kommunikation der Anlagen in das Maschinennetzwerk ist stark kanalisiert: Lediglich einzelne Steuerungssysteme aus dem Produktionsnetzwerk haben regulär die Möglichkeit, die Produktionsmaschinen mit Befehlen anzusprechen oder Informationen von Ihnen abzufragen. Dies wird durch eine entsprechend konfigurierte Firewall sichergestellt. Jene Geräte, welche mit Authentifizierung arbeiten, nutzen spezifische, komplexe Nutzernamen und Passwörter. Zugang zum Internet haben die Geräte innerhalb des Maschinennetzwerks nicht. Geräte im Office-Netzwerk wiederum haben keinerlei Zugriff auf das Maschinen-Netzwerk.

In einer solchen Strukturierung können auch Geräte, Maschinen oder Anlagen, welche Schwachstellen in Bezug auf die IT-Security aufweisen, betrieben werden.

Die IEC 62443 empfiehlt, Gegenmaßnahmen nach Risikoniveaus der Maschinen zu staffeln, wobei Authentifizierung über ein Zwei-Faktoren-System (z.B. Nutzernamen und Kennwort), Antivirusvorsorge, Systemhärtung und Netzwerksegmentierung in den allermeisten Fällen von industriellen Automatisierungs- und Steuerungssystemen indiziert sind.

## 7. Integriertes Safety & Security-Konzept

TÜV AUSTRIA und FRAUNHOFER AUSTRIA RESEARCH empfehlen in Anbetracht der identifizierten Schwächen von kollaborierenden Robotern in Bezug auf IT-Security ein integratives Vorgehen bei der Risikobeurteilung einer Applikation, welches in der Lage ist Gefährdungen der funktionalen Sicherheit und der IT-Security gleichzeitig zu erfassen und nach gleichem Schema, zu beurteilen. Die Gestaltung von Arbeitszellen und Produktionsstraßen muss somit nach dem **Security for Safety** Prinzip erfolgen.

Hierzu haben die Projektpartner das Integrierte Safety & Security-Konzept entwickelt. Seine Grundlage bilden die bewährte Vorgehensweise zur Beurteilung von Risiken der funktionalen Sicherheit gemäß ISO 12100 und die Anwendung von Best Practices zur Überprüfung und Sicherstellung der IT-Security in Anlehnung an IEC 62443. Ziel des Integrierten Safety & Security-Konzepts ist die Erklärung der CE-Konformität der Maschine in Bezug auf funktionale Sicherheit einerseits und die Sicherstellung der Erreichung der Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit andererseits.

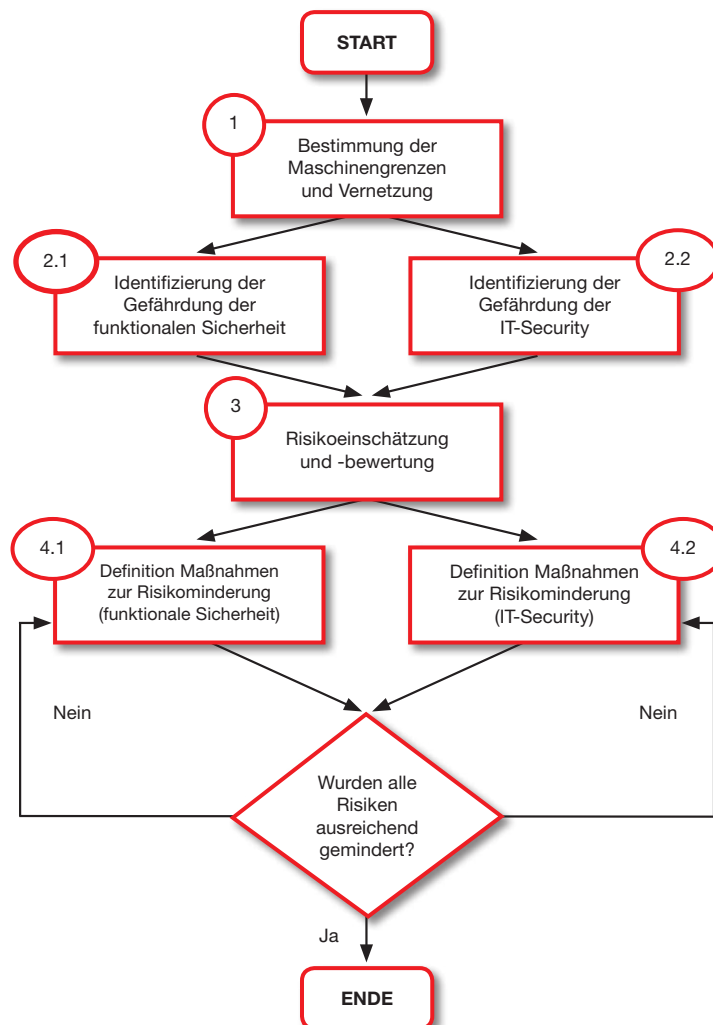


Abbildung 15: Strukturierter Ablauf der integrierten Beurteilung von Safety- und Security-Risiken

## 7.1 Bestimmung der Maschinengrenzen und Vernetzung

In einem ersten Schritt wird der Untersuchungsumfang festgelegt, welcher für die integrierte Beurteilung der Maschinen- und Informationssicherheit notwendig ist – was in Bezug auf die IT-Security insbesondere den Grad der Vernetzung der Maschine beinhaltet.

## 7.2 Identifizierung der Gefährdungen

Die Identifizierung der Gefährdungen für die funktionale Sicherheit erfolgt in interdisziplinärer Zusammenarbeit durch die Beurteilung von Konzeptbeschreibungen, Prozessdarstellungen oder bereits vorhandenen Prototypen bzw. Versuchsaufbauten der Maschine oder Anlage. Wie bereits in der zweiten Ausgabe dieser White Paper-Reihe ausführlich beschrieben, werden dabei unterschiedliche Betriebssituationen und Lebenszyklusphasen der Maschine sowie nicht nur die Gefahren berücksichtigt, die für den unmittelbaren Bediener der Maschine entstehen können, sondern auch für alle anderen Personengruppen, die ggf. auch nur selten mit der Maschine in Kontakt kommen.

Für die Identifizierung der Gefährdungen für die IT-Security kommt der in Kapitel 6.1 beschriebene, siebenstufige Prozess des Testablaufs für IT-Security zum Einsatz. Im Fokus stehen einerseits das Netzwerk, andererseits die vernetzte Maschine selbst. Der beurteilende Sicherheitsexperte nimmt hierbei gedanklich die Rolle eines Angreifers ein und versucht, netzwerk- und maschinenseitige Schwachstellen zu ermitteln, Zugriff zu erlangen und seine Möglichkeiten, Sabotage und Manipulation vorzunehmen, zu vergrößern – ohne den Schaden jedoch tatsächlich eintreten zu lassen.

Insbesondere im Rahmen einer Mensch-Roboter-Kollaboration werden unter Umständen mehrere Systemelemente unterschiedlicher Hersteller zu einer Gesamtanlage oder -applikation zusammengefasst: Diese Einzelelemente werden in der Schwachstellenanalyse einbezogen, da ihre Manipulation die Erreichung der Schutzziele genauso beeinträchtigen kann, wie die des Roboters selbst.

## 7.3 Risikoeinschätzung und -bewertung

Eine Entscheidungsgrundlage zur priorisierten Umsetzung von Maßnahmen zur Minderung der Risiken, die aus den identifizierten Gefährdungen entstehen, wird durch die ihre individuelle Quantifizierung erreicht.

Neuartig ist die Bewertung von Risiken für die IT-Security. Die Experten des TÜV AUSTRIA haben dazu eine Beurteilung in Anlehnung an die Bewertung von Risiken für die funktionale Sicherheit, unter Berücksichtigung der Faktoren Schadensausmaß (S) und Eintrittswahrscheinlichkeit (W), erarbeitet. Die Multiplikation beider Faktoren miteinander ergibt eine Risikoprioritätszahl (RPZ).

$$S \times W = RPZ$$

Dabei hat das **Schadensausmaß** eine Bandbreite von 0 bis 4. Hierbei entspricht die Bewertung 0 einem unerheblichen Schadensausmaß, welches die Aufgabenbewältigung eines Unternehmens kaum spürbar einschränkt. Ein Schadensausmaß, welches mit einer Wertung von 4 versehen wird, hat hingegen signifikante Auswirkungen, entweder im Sinne der Beeinträchtigung der körperlichen Unversehrtheit der Mitarbeiter oder für die Weiterentwicklung des Unternehmens. Während die Beurteilung von Gefährdungen für die funktionale Sicherheit einer Maschine oder Anlage vorrangig gesundheitliche Risiken involviert, werden bei der Quantifizierung von Gefährdungen der IT-Security auch ökonomische und unternehmerische Risiken in Betracht gezogen und zumindest grob beziffert bzw. kategorisiert.

Neben der Schwere der Folgen des Risikoeintritts muss dessen **Eintrittswahrscheinlichkeit** bestimmt werden, welche zwischen Werten von 1 und 5 schwankt. Dabei korreliert der Wert 1 mit einer extrem geringen Eintrittswahrscheinlichkeit, während 5 eine ständige Eintrittsmöglichkeit mit hoher Wahrscheinlichkeit indiziert. Hierbei liegt die Annahme zu Grunde, dass ein hundertprozentiger Ausschluss der Eintrittsmöglichkeit, also ein Wert entsprechend 0, nicht erreicht werden kann.

Die Ermittlung und Beachtung der sich aus Schadensausmaß und Eintrittswahrscheinlichkeit ergebenden Risikoprioritätszahl (RPZ) stellt sicher, dass höhere Risiken auch vorrangig behandelt und durch entsprechende Gegenmaßnahmen gesenkt werden. Eine wirkliche Aussagekraft erhält die RPZ jedoch erst durch Festlegung eines akzeptablen Restrisikos durch das die Risikobeurteilung erstellende Team – indem durch die Differenz zwischen angestrebtem Restrisiko und aktuell bestehendem Risiko der Handlungsbedarf ermittelt wird.

### 7.4 Definition von Maßnahmen zur Risikominderung

Risikosenkende Maßnahmen werden solange iterativ auf die Gefährdung implementiert, bis das gewünschte Risikoniveau, ausgedrückt durch die die Gefährdung betreffende RPZ, erreicht wurde. Ein Beispiel für den Zusammenhang zwischen funktionaler Sicherheit und IT-Security in der Mensch-Roboter-Kollaboration und den möglichen kompromittierenden gegenseitigen Einfluss zeigt das folgende Beispiel: Das identifizierte Verletzungsrisiko durch eine Quetschung zwischen Roboter und Arbeitsumgebung wird durch die Begrenzung von Verfahrgeschwindigkeit, Leistung und Kräften des Roboters in der Sicherheitsprogrammierung des Roboters auf ein akzeptables Maß reduziert – die RPZ sinkt von einem Wert 30 auf eine 10. Existiert im Gegenzug eine Gefährdung der IT-Security, welche es einem Angreifer ermöglicht, die Sicherheitskonfiguration unbemerkt – sei es aus der Ferne oder lokal – zu verändern, wird das ursprüngliche, inakzeptable Verletzungsrisiko wieder erreicht. Erst durch die zusätzliche Ergreifung von Gegenmaßnahmen gegen die unbefugte Kompromittierung der Sicherheitskonfiguration kann die originäre Gefährdung der funktionalen Sicherheit wirksam reduziert werden (Security for Safety).

Maschine		Erstellungsdatum										Akzeptiertes Restrisiko											
Ifd. Nr.	Gefährdung Beschreibung der Gefährdung / Gefahrenstelle an der Maschine	Risiko vorher										Risiko nachher											
		S(0, 1-4)	F(1-5)	W(1-5)	P(1, 3,5)	Risikoklasse	Risikoprioritätszahl RPZ	PLR	SIL	Konstruktiv	Technisch	Organisatorisch	IT	S(0, 1-4)	F(1-5)	W(1-5)	P(1, 3,5)	Risikoklasse	Risikoprioritätszahl RPZ				
Mechanische Gefährdung																							
102	Annäherung eines sich bewegenden an ein feststehendes Teil und daraus resultierende Quetschungen eines Körperoberteils, insb. Hände und Arme (quasi-statischer Kontakt mit Robotergehäuse)	3	5	2	3	10	30	c	1	<b>Maßnahme(n)</b> Beschreibung der getroffenen und noch zu treffenden Maßnahmen einschließlich Begründung von Maßnahmen				x				1	5	2	3	10	10
Mechanische Gefährdung																							
Ifd. Nr.	Gefährdung Beschreibung der Gefährdung / Gefahrenstelle an der Maschine	Risiko vorher										Risiko nachher											
		S(0, 1-4)	W(1-5)	Risikoprioritätszahl RPZ									Konstruktiv	Technisch	Organisatorisch	IT	S(0, 1-4)	W(1-5)	Risikoprioritätszahl RPZ				
Gefährdung der IT-Security																							
1211	Sabotage: Veränderung der Installationsdatei, insb. der Sicherheitskonfiguration (Kraft-, Leistungs-, Geschwindigkeitsgrenzen sowie räumliche Grenzen)	3	3	9			Für physisches Einspielen einer neuen Installationsdatei über USB-Schnittstelle: Rechtemanagement, Passwortschutz, ggf. Versiegelung der physischen Schnittstellen.								x		3	1	3				
		3	3	9			Für Veränderungen über Ethernet Socket: Authentifizierung, Autorisierung, Netzwerkzoning								x		3	1	3				

Abbildung 16: Zusammenhang zwischen Safety & Security unter Nutzung der Risikoprioritätszahl

## 8. Fazit und Ausblick

Die smarte Fabrik ist keine Zukunftsvision, sondern kann dank marktverfügbarer vernetzungsfähiger Maschinen und Anlagen bereits heute realisiert werden. Die durchgeführten Untersuchungen am Beispiel von kollaborativen Leichtbaurobotern haben jedoch gezeigt, dass selbst wenn die Maschinen über ein hohes Niveau an funktionaler Sicherheit verfügen, die IT-Security derselben Maschine Schwachstellen aufweisen kann, welche nicht nur die funktionale Sicherheit einschränken, sondern auch den reibungslosen Produktionsbetrieb stören oder die Sicherheit der Unternehmensdaten reduzieren können.

Eine gute Kenntnis der relevanten Normen und Richtlinien in Bezug auf industrielle IT-Security und eine gleichzeitige Betrachtung von funktionaler Sicherheit und IT-Security im Rahmen der Risikobeurteilung, wie sie das Integrierte Safety&Security-Konzept des TÜV AUSTRIA propagiert, ermöglicht eine strukturierte Identifizierung, Bewertung und Bearbeitung von Schwachstellen in den beiden wesentlichen Risikodimensionen – und befähigen produzierende Unternehmen damit zur nachhaltigen und sicheren Umsetzung der Vision Industrie 4.0 unter Berücksichtigung von Verfügbarkeit, Vertraulichkeit und Integrität.

In diesem Kontext ist die zunehmende Flexibilisierung der digitalen Fabrik eine noch offene Herausforderung für Safety und Security. Wechselnde Produkte und veränderbare Fabrikkonfigurationen erfordern Sicherheitskonzepte, welche sicherstellen, dass auch bei häufigen Anpassungen von Arbeitsumgebungen, Maschinen und Prozessen funktional und informativ neue Gefahren und Risiken abgedeckt sind – ohne dies ständig und aufwändig neu beurteilen zu müssen. Die zukünftige Arbeit der Partner wird sich an dieser Maßgabe orientieren und Methoden zur Risikobeurteilung industrieller Systeme entwickeln, um auch den flexiblen Einsatz bei wechselnden Aufgaben unter Aufrechterhaltung der funktionalen und informativischen Sicherheit zu ermöglichen.

### **Über den TÜV AUSTRIA:**

TÜV AUSTRIA ist ein unabhängiges österreichisches Unternehmen mit Niederlassungen in mehr als 40 Ländern der Welt. TÜV AUSTRIA beschäftigt über 1.500 Mitarbeiterinnen und Mitarbeiter.

Das Leistungsspektrum der TÜV AUSTRIA Group reicht von Personen-, System- und Produktzertifizierung über Prüfungen von Aufzügen und Druckgeräten, Anlagensicherheit, Aus- und Weiterbildung, Medizintechnik, Elektrotechnik, Umweltschutz, Industrie 4.0, Schallschutzgutachten, Carbon Footprint-Evaluierungen, IT-Security, Internet of Things, E-Mobility, AppChecks, Kalibrierungen, Produktprüfungen, Robotik, technischer Due Diligence und Legal Compliance Checks bis zu Prüfungen von Bühnen-, Photovoltaik- und Windkraftanlagen.

Ansprechpartnerin zum Thema Mensch-Roboter-Kollaboration:

**Dipl.-Ing. Alexandra Markis - alexandra.markis@tuv.at**

### **Über FRAUNHOFER AUSTRIA RESEARCH GMBH:**

Fraunhofer ist die größte Forschungsorganisation für anwendungsorientierte Forschung in Europa. Unsere Forschungsfelder richten sich nach den Bedürfnissen der Menschen: Gesundheit, Sicherheit, Kommunikation, Mobilität, Energie und Umwelt. Und deswegen hat die Arbeit unserer Forscher und Entwickler großen Einfluss auf das zukünftige Leben der Menschen. Wir sind kreativ, wir gestalten Technik, wir entwerfen Produkte, wir verbessern Verfahren, wir eröffnen neue Wege. Wir erfinden Zukunft.

Fraunhofer Austria Research wurde Ende 2008 als erste europäische Tochtergesellschaft der Fraunhofer-Gesellschaft gegründet. An den Standorten Wien, Graz und Wattens forschen aktuell mehr als 50 Wissenschaftler in den Bereichen Produktions- und Logistikmanagement, Visual Computing und Industrial Data Science an anwendungsorientierten Lösungen zum Nutzen der Wirtschaft und zum Vorteil der Gesellschaft.

Ansprechpartner zum Thema Mensch-Roboter-Kollaboration:

**Fabian Ranz, M.Sc. - fabian.ranz@fraunhofer.at**

### **Quellen:**

- [1] Global State of Information Security® Survey 2017, PWC.
- [2] Bericht Internet-Sicherheit Österreich 2016, Computer Emergency Response Team Austria
- [3] The Internet of Things – Mapping the Value beyond the Hype, Juni 2015, McKinsey & Company.
- [4] VierNull Blog (<https://viernull.blog/>), ISAP AG.
- [5] Orientierungsleitfaden für Hersteller zur IEC 62443, April 2017, Zentralverband Elektrotechnik und Elektronikindustrie e.V. (ZVEI).
- [6] Industrial Control System Security - Top 10 Bedrohungen und Gegenmaßnahmen 2016, Version 1.20, August 2016, Bundesamt für Sicherheit in der Informationstechnik.
- [7] Leitfaden Security für den Maschinen- und Anlagenbau - Der Weg durch die IEC 62443, 2016, HiSolutions AG.
- [8] OWASP Top 10 -2017 The Ten Most Critical Web Application Security Risks (<https://owasp.org>), The OWASP Foundation

# WhitePaper

TÜV AUSTRIA Group  
DI Alexandra Markis  
TÜV-Austria Platz 1  
2345 Brunn am Gebirge  
Mail: [i4.0@tuv.at](mailto:i4.0@tuv.at)

[www.tuv.at/i40](http://www.tuv.at/i40)

Fraunhofer Austria  
Research GmbH  
Fabian Ranz M.Sc.  
Theresianumgasse 27  
1040 Wien  
Mail: [fabian.ranz@fraunhofer.at](mailto:fabian.ranz@fraunhofer.at)

[www.fraunhofer.at](http://www.fraunhofer.at)