

WhitePaper

Sicherheit in der
Mensch-Roboter-Kollaboration



Sicherheit in der Mensch-Roboter- Kollaboration

Grundlagen, Herausforderungen, Ausblick

Erste Ausgabe

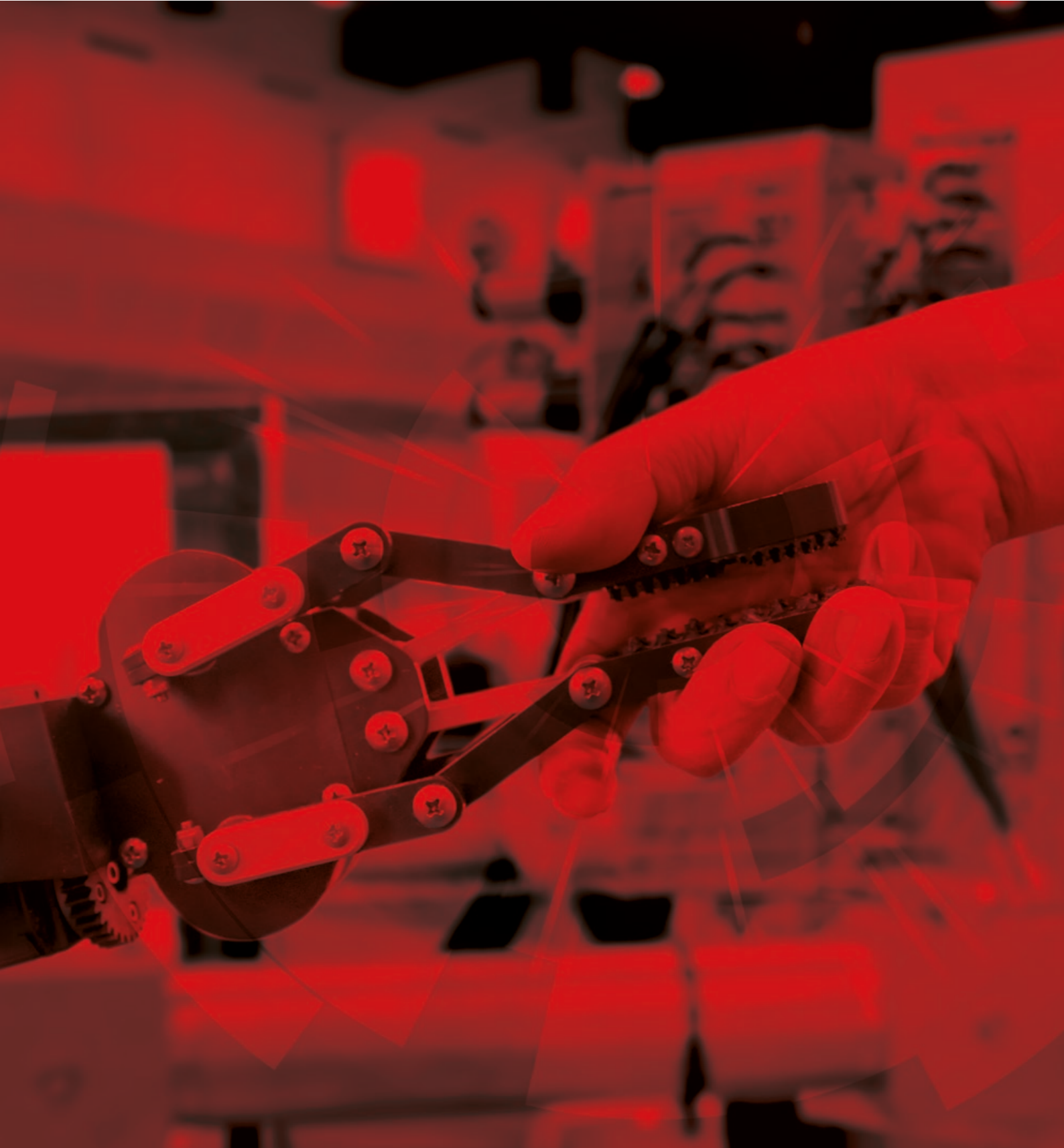
Wien, am 10.10.2016

TÜV AUSTRIA Holding AG
TÜV-Austria-Platz 1
A-2345 Brunn am Gebirge

Fraunhofer Austria Research GmbH
Theresianumgasse 27
A-1040 Wien

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

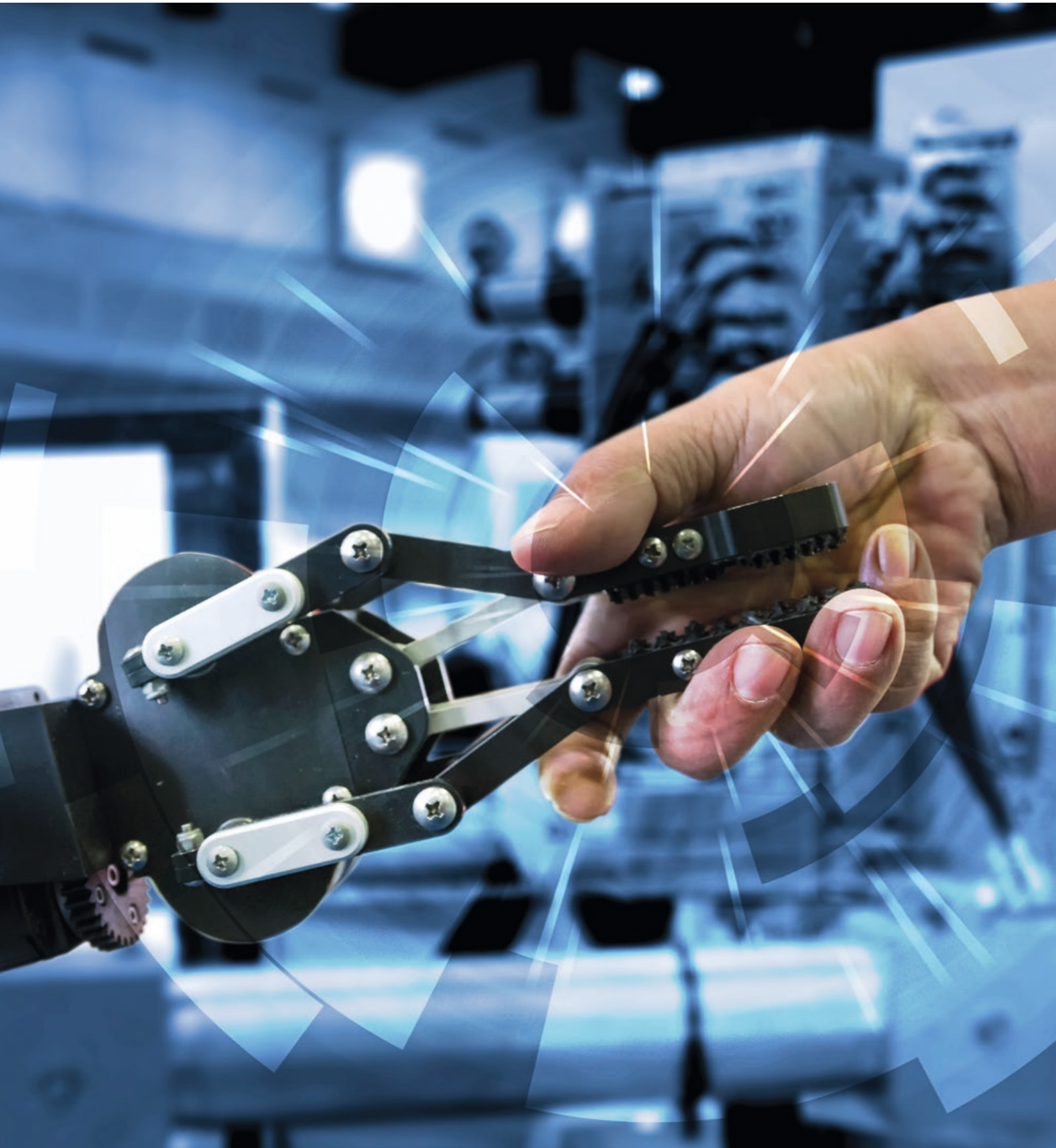
*Prof. Dr.-Ing. Wilfried Sihn
Fabian Ranz, M.Sc.
DI Thomas Edtmayr
Dipl.-Wirtsch.-Ing. Philipp Hold
DI Gerhard Reisinger*



Sicherheit in der Mensch-Roboter-Kollaboration

Inhalt

Abstract.....	7
Smart Factory.....	9
Gesetzliche Rahmenbedingungen	10
Integration der IT-Security.....	12
Viele Normen, viele Fragen bei der Umsetzung.....	13
Mehr Sicherheit bei der Implementierung.....	15
Safety & Security-Konzept.....	17
TÜV AUSTRIA und Fraunhofer Austria Research	19



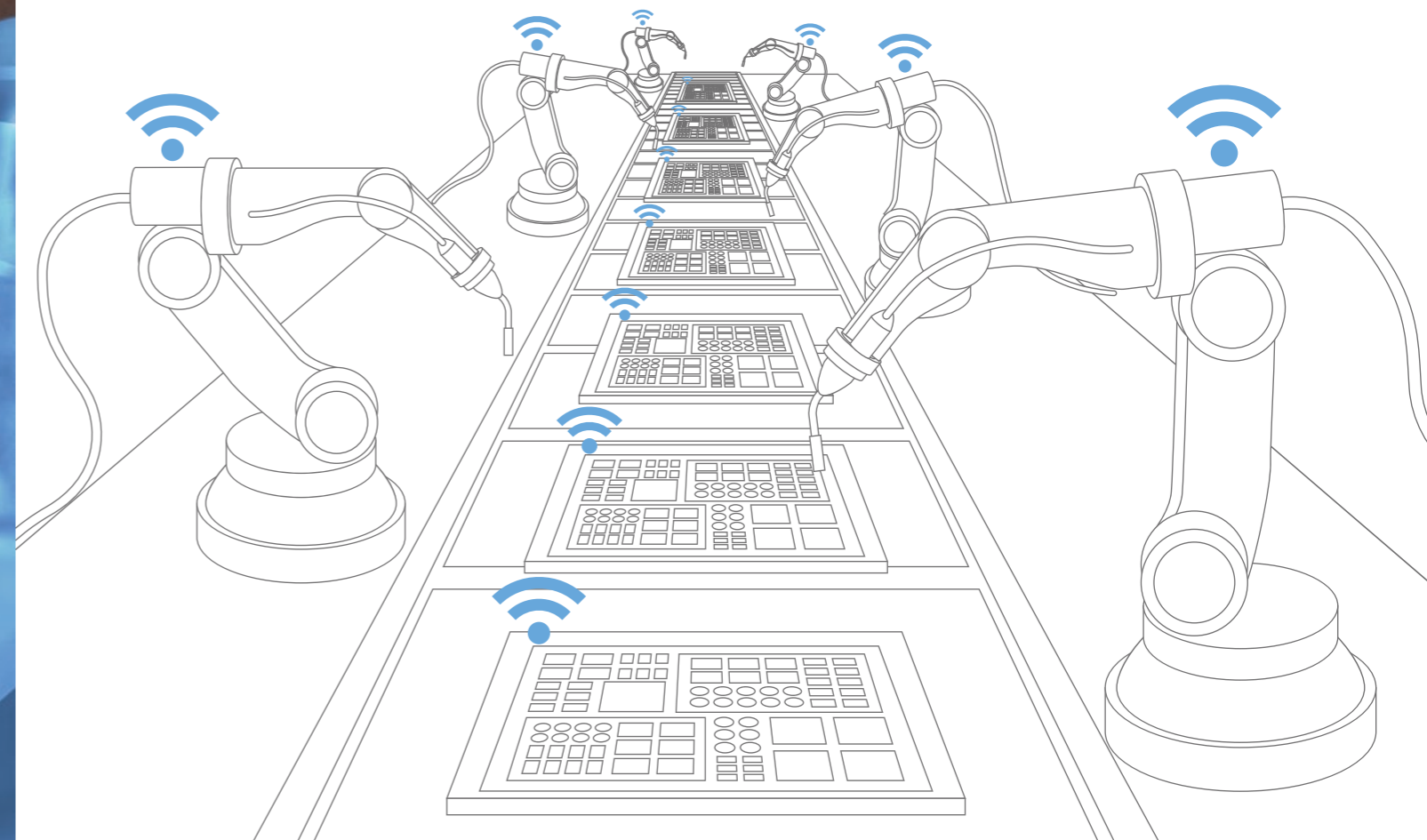
Abstract

Die vierte Industrielle Revolution

Dieses erste White Paper der White Paper Reihe „Sicherheit in der Mensch-Roboter-Kollaboration“ von TÜV AUSTRIA und Fraunhofer Austria gibt eine Einführung in das Konzept der Mensch-Roboter-Kollaborationen, einen Überblick über die aktuelle Normungslage im Themenfeld und einen Ausblick in ein gemeinsam zu entwickelndes, **integriertes Safety & Security-Konzept**, welches produzierenden **Unternehmen die Einführung von MRK-Anwendungen zukünftig erleichtern** wird.

Die Einführung der Mensch-Maschine-Kollaboration (MRK) gilt als einer der wichtigsten Trends im Rahmen der vierten industriellen Revolution. Durch MRK lassen sich Arbeitsqualität und -effizienz in industriellen Prozessen steigern, da die individuellen Eigenschaften von Mensch und Roboter in einem gemeinsamen Arbeitssystem kombiniert werden.

Die Sicherheit des Menschen in der Interaktion mit vernetzten Maschinen hat höchste Priorität – und ihre Sicherstellung wird von zahlreichen Normen und Richtlinien unterstützt. Aktuell fehlen aber gerade bei der direkten Kollaboration von Mensch und Maschine, sowie bei der Integration von IT-Security, noch Erfahrungswerte in der Praxisumsetzung der gesetzlich vorgeschriebenen Anforderungen. Dadurch ergeben sich für Unternehmen erhebliche Umsetzungsbarrieren bei der Einführung von kollaborativen Arbeitssystemen.



Smart Factory

Mensch und Maschine integriert und vernetzt

Das Konzept der intelligenten Fabrik (Smart Factory) verfolgt die Vision einer industriellen Produktionsumgebung, in der sich Fertigungsanlagen und Logistiksysteme weitgehend selbst organisieren und Menschen mit der sie umgebenden Technik integrativ kooperieren (1). Was zunächst abstrakt klingt, ist bereits heute möglich: Zwei der wesentlichen Ansätze zur Erreichung von Selbstorganisation und Mensch-Maschine-Kooperation sind die digitale Vernetzung aller Produktionsressourcen zum Austausch von Informationen in Echtzeit sowie die Mensch-Roboter-Kollaboration.

Mensch-Roboter-Kollaboration (MRK) bezeichnet die Zusammenarbeit von Menschen und Robotern in einem gemeinsamen Arbeitssystem - ohne das Vorhandensein von trennenden (bspw. Gitter und Zäune) und nichttrennenden Schutzeinrichtungen (bspw. Lichtgitter, Laserscanner). Dabei arbeiten Mensch und Roboter zur selben Zeit am selben Objekt, also in echter **Kollaboration**. Alternativ stehen sie in **Kooperation**, indem sie wechselseitig Aufgaben am selben Ort verrichten. In jedem Fall aber entsteht ein gemeinsamer Wirk- und Arbeitsraum.

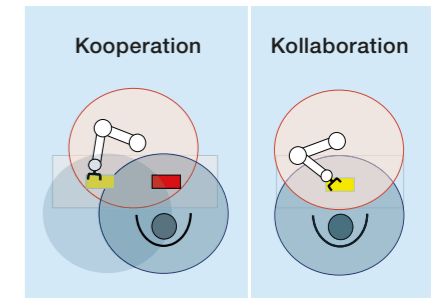


Abb. 1: MRK-Arten im Vergleich in Anlehnung an (7)

Der Mehrwert der Mensch-Roboter-Kollaboration besteht darin, dass die Stärken des Menschen, wie beispielsweise Auge-Hand-Koordination, Kraftdosierung und die Fähigkeit zur selbstständigen Problemlösung, mit den Stärken eines Roboters, wie Präzision, Bahntreue und Ermüdungsfreiheit, in einem Prozess genutzt werden können. Ziel ist es beide Ressourcen gemäß ihrer tatsächlichen Fähigkeiten einzusetzen und damit einen effizienteren Gesamtprozess zu erzielen.

Für den Anwender ergeben sich aus dem kombinierten Einsatz des Menschen und flexibler Roboter außerdem wirtschaftliche Automatisierungsmöglichkeiten auch für kleine bis mittlere Losgrößen und Stückzahlen, in denen eine starre Vollautomatisierung üblicherweise nicht rentabel ist (2). Damit können durch MRK auch jene Unternehmen von Automatisierungspotenzialen profitieren, denen dies durch höheren Individualisierungsgrad oder größere Variantenvielfalt ihrer Produkte bislang aus Kostengesichtspunkten verwehrt bleibt (vgl. Abbildung 2).

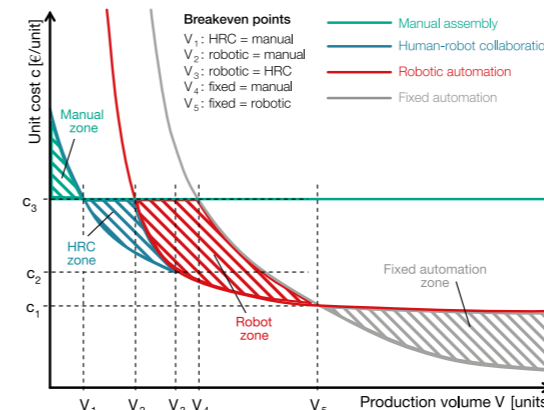


Abb. 2: Wirtschaftliche Anwendbarkeit von verschiedenen Produktionsparadigmen

Durch die üblicherweise von Maschinen und insbesondere Robotern ausgehenden Gefahren waren deren Arbeitsräume bislang physisch von denen des Menschen getrennt, sodass bis heute vor allem komplett automatisierte, oder eben im Gegensatz dazu, rein manuelle Arbeitssysteme in der Industrie zu finden sind. Roboter im Kollaborationseinsatz müssen daher über Sicherheitseinrichtungen verfügen, die in der Lage sind eine Annäherung mit dem Menschen noch vor einem echten Kontakt zu erkennen und dementsprechend zu reagieren oder mit so geringen Kräften arbeiten, dass auch im Falle eines Zusammenstoßes keine inakzeptable Verletzungsgefahr für den Menschen entsteht.

Speziell für den kollaborativen Betrieb bieten erste Hersteller sogenannte **kraft- und leistungsreduzierte Leichtbauroboter** an, häufig auch als **kollaborative Roboter** (siehe Tabelle 1) bezeichnet. Sie sind durch inhärente

Sicherheitsfunktionen, wie beispielsweise taktile oder kapazitive Sensorik zur Kollisionserkennung für die direkte Zusammenarbeit mit dem Menschen innerhalb des definierten Interaktionsraums konzipiert. Prinzipiell lassen sich auch herkömmliche Industrieroboter durch Erweiterungen erforderlicher Sicherheitseinrichtungen für den kollaborativen Betrieb einsetzen. Beispiele für solche Sicherheitseinrichtungen sind gepolsterte Softcover Ummantelungen und Sensorhäute.

Neben der funktionalen Sicherheit einer MRK-Applikation durch ihre sicherheitsgerichtete Überwachung und Steuerung spielt, bei zunehmender Vernetzung von Maschinen und Anlagen, auch die Informationssicherheit, *IT-Security*, eine neuerdings bedeutende Rolle. Durch Anbindung des kollaborativen Roboters, beispielsweise in ein industrielles Netzwerk, kann dieser Daten und Befehle von außerhalb des Arbeitssystems empfangen, speichern und verarbeiten. Insbesondere wenn diese Befehle direkten Einfluss auf die Konfiguration eines kollaborativen Roboters nehmen, sind diese vor der Ausführung zu prüfen, um zu vermeiden, dass die funktionale Sicherheit der Applikation durch korrupte Befehle beeinträchtigt wird.



Firma	Modell
ABB / Gomtec	Roberta
ABB Robotics	YuMi
Bionic Robots	BioRob
Bosch	Apas
F&P Robotics	P-Rob
Fanuc	CR-35iA OUR2
Kawada Industries	NEXTAGE
KUKA	iiwa7 R800 / 14 R820
Precise Automation	PAVP6
Precise Automation	PF400
Precise Automation	PP100
Rethink Robotics	Sawyer / Baxter
Smokie Robotics	OUR2
Stäubli	TX2-40
Universal Robots	UR3 / UR5 / UR10

Tabelle 1: Liste aktuell am Markt verfügbarer kollaborativer Roboter (Stand März 2016, kein Anspruch auf Vollständigkeit)

Gesetzliche Rahmenbedingungen

Einführung von MRK-Systemen

Nun hat ein solcher Roboter für sich allein aus Sicht des Betreibers noch keinen konkreten Nutzen. Erst durch Integration der richtigen Werkzeuge und Greifer, durch eine geeignete Anbringung des Roboters am Kollaborationsarbeitsplatz und letztlich die Einbindung des Roboters in das industrielle Kommunikationsnetz des Unternehmens wird er wirklich zu einer einsatzbereiten MRK-Applikation.

Wie jede Maschine (im industriellen Umfeld) ist auch die MRK-Applikation mit dem Roboter als deren zentrales Element gemäß der Maschinenrichtlinie 2006/42/EG (3) zu behandeln und in Verkehr zu bringen, damit sie vom Betreiber nicht nur sicher, sondern auch rechtskonform verwendet werden kann.

Je nach Umfang an Sicherheitseinrichtungen, die entweder bereits mit dem Roboter geliefert werden oder durch den Systemintegrator oder Betreiber als Hersteller noch zu implementieren sind, wird der kollaborative Roboter entweder als „Unvollständige Maschine“ oder als „Maschine“ mit den dazugehörigen Dokumenten in Verkehr gebracht.

Unabhängig davon ergibt sich durch die Applikation oftmals eine Verkettung des Roboters mit anderen (Teil-) Maschinen im kollaborativen Arbeitssystem, für das wiederum durch die nationalen ArbeitnehmerInnenschutzbestimmungen (ASchG und AM-VO in Österreich) die sichere Funktion durch den Betreiber nachgewiesen werden muss.

Dadurch ergibt sich, dass derjenige, welcher eine MRK-Applikation erstellt (das kann ein Systemintegrator, aber auch der Betreiber selbst sein) auch deren CE-Konformität untersuchen und bescheinigen muss.

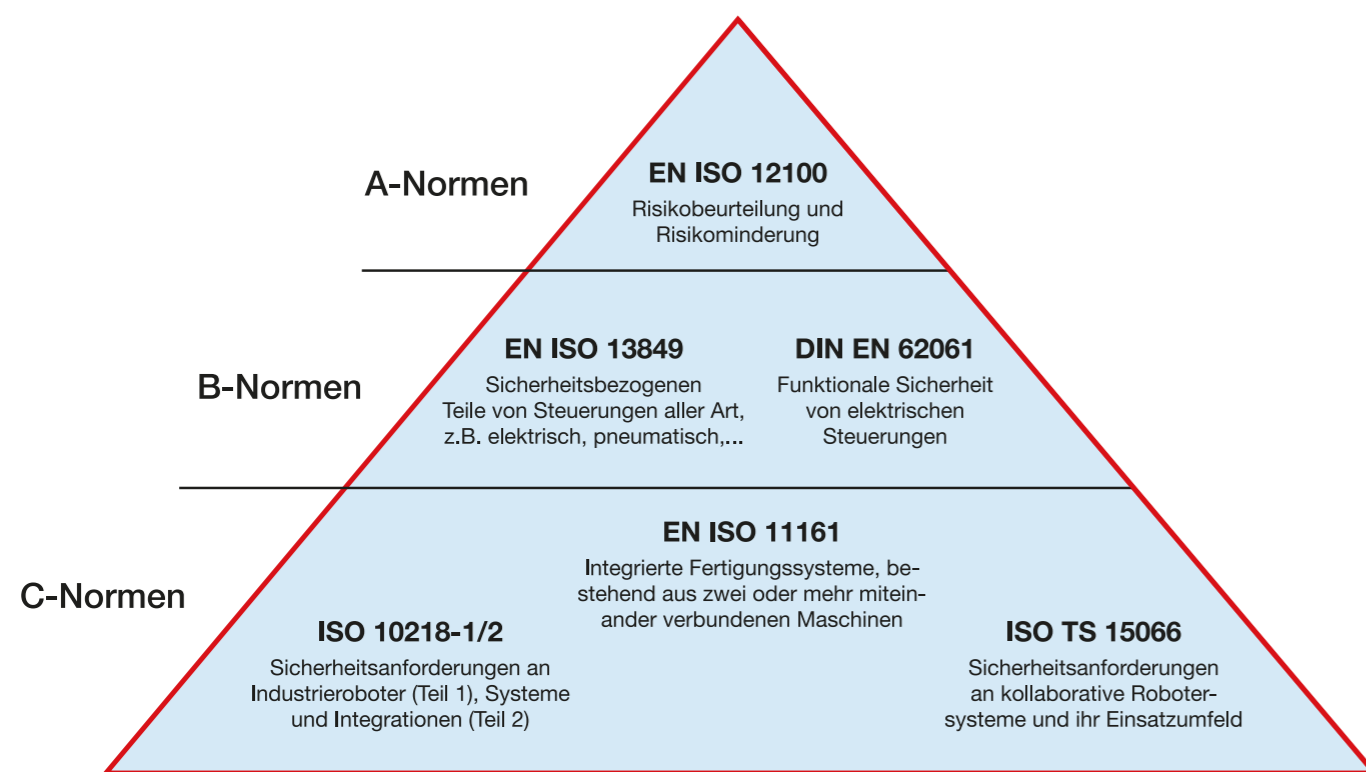


Abb. 3: Relevante Normen aus der Sicht einer MRK-Applikation (Auszug)

Das Kernstück einer Konformitätsuntersuchung ist die **Risikobeurteilung**. Sie stellt ein strukturiertes Prozedere dar, mit dem ermittelt wird, welche Sicherheitsanforderungen die MRK-Applikation zu erfüllen hat, um die von ihr ausgehenden Risiken für den Menschen auf ein akzeptables Niveau zu senken.

Die Anforderungen ergeben sich aus den nicht konkret formulierten Schutzziele der gesetzlichen Grundlage in Form der EU-Produkttrichtlinien (u.a. der Maschinenrichtlinie). Die in dazu harmonisierten Normen beschriebenen Lösungsansätze dienen zur Unterstützung bei der Erfüllung dieser Anforderungen.

Die in Europa verwendeten Normen werden in Gruppen klassifiziert. Die einzige existente *A-Norm*, ISO 12100, beschreibt neben bisher gültigen Gestaltungsgrundsätzen zur sicheren Konstruktion auch das Verfahren der Risikobeurteilung gemäß Maschinenrichtlinie und ist verbindlich für alle Maschinen. *B-Normen* beschreiben allgemeine Gestaltungsaspekte, die für zahlreiche Maschinen Relevanz haben. *C-Normen* sind stark maschinenspezifisch und behandeln Maßnahmen zur Senkung von Risiken, die mit eben diesen speziellen Maschinen und Anlagen zusammenhängen.

Von hoher Bedeutung für eine MRK-Applikation ist, neben den roboterspezifischen Normen wie ISO 11161 oder ISO 10218, die erst im Februar 2016 erschienene Technische Spezifikation ISO/TS 15066 – die erste Norm speziell für MRK überhaupt. Sie listet zunächst vier mögliche Kollaborationsformen zwischen Mensch und Roboter (4):

- *Sicherheitsüberwacher Halt*: Der Roboter hält vor Eintritt eines Menschen in den gemeinsamen Arbeitsraum an und fährt erst wieder an, wenn dieser den Arbeitsraum wieder verlassen hat.
- *Handführung*: Der Roboter bewegt sich nur bei direkter manueller Einwirkung durch den Bediener und stellt diesem seine Kraft passiv zur Verfügung. Dies kann bei handgeführten Hebehilfen oder beim Teaching durch direkte Bewegung des Roboterarms der Fall sein.
- *Geschwindigkeits- und Abstandsüberwachung*: Bei sinkender Distanz zwischen Mensch und Roboter wird die Geschwindigkeit des Roboters zunehmend und stufenweise reduziert, im Zweifelsfall bis zum Stillstand.
- *Leistungs- und Kraftbegrenzung*: Die vom Roboter ausgehenden Kräfte sind soweit begrenzt, dass auch im Falle einer Kollision keine bleibenden Verletzungen entstehen können. Dies wird durch vorab auf ein akzeptables Maß definierte Leistungen und Verfahrgeschwindigkeiten realisiert.

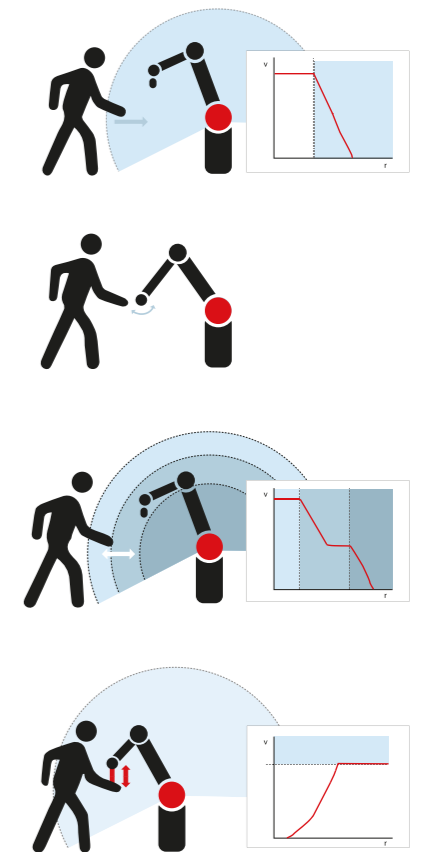


Abb. 4: Schutzprinzipien nach TS 15066

Nur in der letztgenannten Kollaborationsform, der **Leistungs- und Kraftbegrenzung**, ist eine tatsächlich unabhängige Bewegung mit dem Risiko einer unbeabsichtigten Berührung von Mensch und Roboter im gemeinsamen Arbeitsraum möglich. Hierzu sind die eingangs erwähnten leistungs- und kraftreduzierten Roboter mit entsprechender Sensorik zur Erkennung von Annäherung bzw. Berührung und variablen Sicherheitsparametern erforderlich.

Da eine dynamische Kollision zwischen Mensch und Roboter in dieser Kollaborationsform durchaus realistisch ist, schlägt die ISO/TS 15066 zusätzlich auch **Kraft- und Druckgrenzwerte** für verschiedene Körperregionen vor. Diese können dazu verwendet werden, die erforderlichen Limits für Roboterleistung und Verfahrgeschwindigkeit, unter gegebenen bewegten Massen und Geometrien und der potenziell in einer bestimmten Applikation gefährdeten Körperregionen, ableiten zu können.

In Umfeld der rechtlichen Rahmenbedingungen zur Einführung von MRK Systemen sind datenschutzrechtlichen Aspekte ergänzend anzuführen. Dies begründet sich insbesondere darin, dass für den Betrieb von MRK Systeme u.a. vermehrt biometrische Merkmale der MitarbeiterInnen zur Authentifizierung und Steuerung eingesetzt werden. Somit werden MRK Steuerungssysteme zu Datenanwendungen, die aktuell gemäß den Vorgaben des DSGVO 2000 und ab 28.5.2018 gemäß der Datenschutzgrundverordnung (DSGVO) zu betreiben sind. Dies bedeutet, dass angemessene Schutzmaßnahmen für die verarbeiteten Datensätze zu treffen sind.

Integration der IT-Security

Durchgängige Gewährleistung der Sicherheit

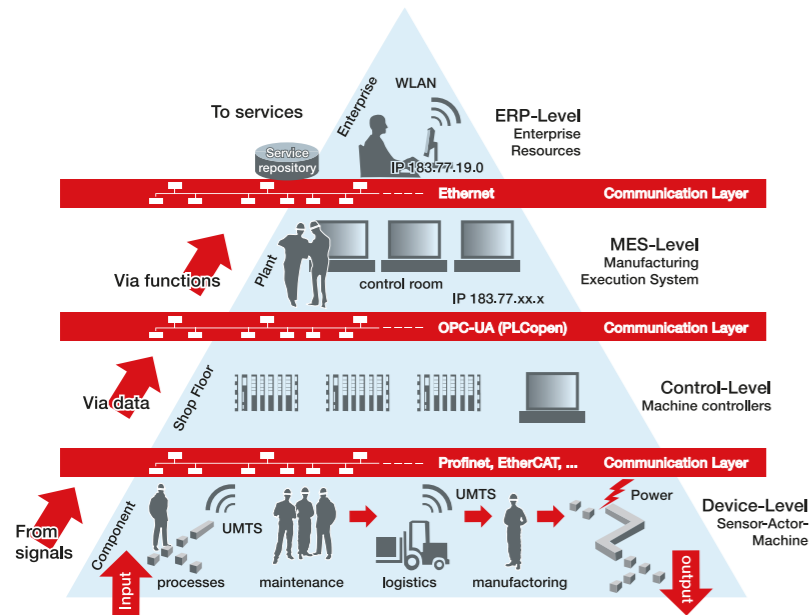


Abb. 5: Typische Kommunikationsinfrastruktur. Quelle: OPC Foundation (9)

bspw. Internet, Unternehmensnetz und dem Device, zum Beispiel also der MRK-Applikation. Hierdurch wird der Fernzugriff zu Informations- und Auswertezwecken ermöglicht, aber auch die Versorgung des Roboters mit einfachen Steuerungsbefehlen, Produktionsaufträgen oder ganzen Fertigungsprogrammen. Das bedeutet, dass das Verhalten des Roboters in der MRK-Anwendung von außen beeinflussbar ist. Dadurch ergeben sich einerseits Bedrohungspotenziale für die Mensch-Roboter-Kollaboration und andererseits Schutzziele, die, angelehnt an klassische IT-Systeme bzw. ISO 27001, auch für die MRK Relevanz haben, wie beispielsweise (5):

- **Integrität:** Daten und Funktionen des Systems können nicht unbemerkt durch Unberechtigte manipuliert werden
- **Vertraulichkeit:** Unberechtigte können nicht auf Daten und Funktionen des Systems lesend zugreifen
- **Verfügbarkeit:** benötigte Daten und Funktionen des Systems stehen im Bedarfszeitpunkt zur Verfügung

Wie auch für die funktionale Sicherheit formulieren für die Informationssicherheit zahlreiche Normen Empfehlungen, deren Einhaltung die Sicherheit des Systems erhöht. Die IEC 62443 zur IT-Sicherheit in industriellen Automatisierungssystemen ist aus Sicht eines Betreibers einer MRK-Applikation sicher von besonderer Relevanz: Sie beschreibt ein Vorgehen zur Risikobeurteilung einer Automatisierungsanlage - ähnlich wie ISO 12100, nur mit Fokus auf Informationssicherheit.

Fazit zur Integration rechtlicher Rahmenbedingungen und IT-Security

Die vorangestellten Ausführungen zeigen die aktuelle Praxis zur Behandlung der unterschiedlichen Themen. Unternehmen wickeln diese Herausforderungen oftmals weitestgehend getrennt ab. Spätestens jetzt wird deutlich, dass funktionale Sicherheit und Informationssicherheit integrativ zu behandeln sind, damit sowohl für den Hersteller, wie auch den Betreiber einer MRK-Applikation ein gesetzeskonformer sicherer (safe & secure) Betrieb möglich ist.

Die IEC 61508 bringt es auf den Punkt: „Wenn die Gefährdungsanalyse zeigt, dass eine böswillige oder nicht autorisierte Handlung, die eine Bedrohung der IT-Sicherheit darstellt, als vernünftigerweise vorhersehbar gilt, sollte eine Bedrohungsanalyse zur IT-Sicherheit durchgeführt werden. Für eine Anleitung zur Risikoanalyse im Rahmen der IT-Sicherheit siehe die Normenreihe IEC 62443 und ISO 27005.“

Ebenfalls referenzieren beide Normen, darauf, dass alle rechtlichen Rahmenbedingungen eingehalten werden und somit auch die datenschutzrechtlichen Aspekte bereits bei der Konzeptionierung eines MRK Systems zu berücksichtigen sind.

Die in Abbildung 4 beispielhaft gelisteten Normen adressieren die Anforderungen an MRK-Applikationen hinsichtlich der physischen Umsetzung von Steuerung und Aktorik, ihrer Programmierung sowie des Arbeitsumfeldes allgemein. Dabei bleibt die geschilderte Einbindung des Roboters bzw. der MRK-Applikation in das industrielle Kommunikationsnetzwerk völlig unbeachtet.

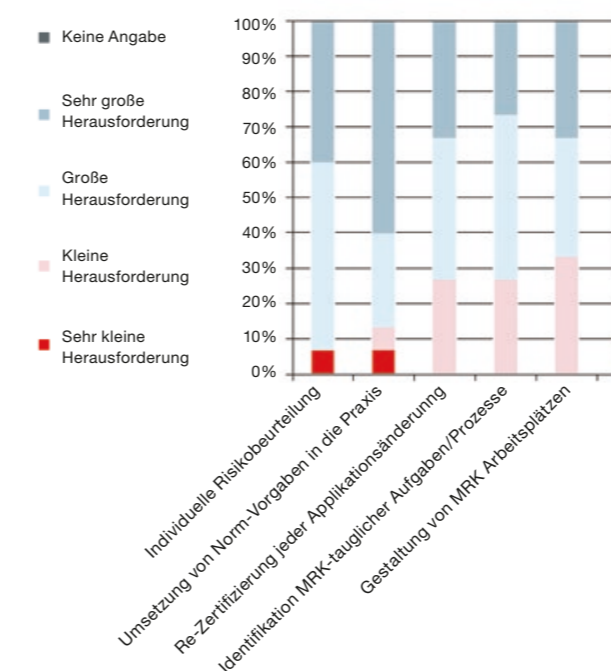
Die MRK-Applikation stellt innerhalb der Kommunikationsinfrastruktur in der Fabrik eine Ressource auf Device-Level dar (vgl. Abbildung 5) und kann über verschiedene Standards mit dem Umfeld kommunizieren – angefangen vom einfachen digitalen E/A-Signal bis zum Ethernet/IP-Protokoll.

Letzteres unterstützt aufgrund der TCP- und IP-Basierung die durchgängige Kommunikation zwischen

Viele Normen, viele Fragen bei der Umsetzung

Auch wenn funktionale Sicherheit und Informationssicherheit bislang nicht ganzheitlich betrachtet werden, so entsteht dem Beobachter der subjektive Eindruck, Vorgaben zur Risikobeurteilung sowie zahlreiche Normen und Richtlinien müssten eine gute Hilfestellung bei MRK-Einführungsvorhaben bieten. Doch eine 2016 durchgeführte Studie unter 15 Roboterherstellern,

Abb. 6: Top 5 Einführungshindernisse für MRK-Systeme (6)



14 Integratoren sowie fünf Anwenderfirmen aus Österreich und Deutschland, allesamt bereits mit MRK-Erfahrung, belegt, dass der vermeintlich bereits ausführlich normativ aufgearbeitete Aspekt der Sicherheit eigentlich das größte Umsetzungshindernis für Mensch-Roboter-Kollaboration darstellt (6). So beurteilen 97% der Studienteilnehmer das Zukunftspotenzial für MRK als „groß“ oder „sehr groß“ und sehen die insgesamt größten Einsatzmöglichkeiten im Rahmen von Montageprozessen – einem Prozessbereich, der auch in Europa nach wie vor stark von manueller Arbeit geprägt ist.

Dennoch sind MRK-Szenarien im industriellen Einsatz nach wie vor nur selten auszumachen. Aus Sicht der Roboterhersteller stellen die Komplexität der applikationsspezifischen Risikobeurteilung, Unklarheiten bei der Interpretation und Umsetzung der Vorgaben aus den einschlägigen Normen und die Notwendigkeit einer Neubeurteilung und -zertifizierung jeder Änderung und Anpassung der Applikation, die drei größten von insgesamt 16 abgefragten Hindernissen dar, die einer größeren Verbreitung des MRK-Konzepts im Weg stehen.

Die befragten Anwenderunternehmen bestätigen diese Sichtweise und führen die Schwierigkeiten einerseits auf fehlende unternehmensinterne Erfahrung mit MRK, andererseits auf die

mangelnde Verfügbarkeit von öffentlich zugänglichen Handlungsleitfäden und Empfehlungen für die normgerechte Applikationsgestaltung und Risikobewertung zurück – und belegen gleichzeitig den herrschenden Handlungsbedarf zur Unterstützung der Industrie bei der Planung und Umsetzung von sicheren MRK-Applikationen. Eine Untersuchung des Fraunhofer Instituts für Arbeitswirtschaft und Organisation (IAO) geht gar davon aus, dass 20% der in Produktion befindlichen MRK-Anwendungen überhaupt nicht CE-konform sind (7).

Eine weitere Perspektive bieten Statistiken und Daten zu Arbeitsunfällen mit Roboterbezug, beispielsweise der österreichischen AUVA oder der Deutschen Gesetzlichen Unfallversicherung. Auch hier würden die Vielfalt am Markt verfügbarer Schutz- und Sicherheitseinrichtungen für den Betrieb von Robotern und die Normungslage darauf schließen lassen, dass ein hohes Sicherheitsniveau im industriellen Roboterbetrieb herrscht. Tatsächlich jedoch sind mehr als 500 meldepflichtige Vorkommnisse im Zeitraum 2011 bis 2014 aufgetreten:

	2011	2012	2013	2014	tödlich
Österreich	10	17	12	15	0
Deutschland	107	72	119	151	2

Tabelle 2: Meldepflichtige Arbeitsunfälle mit Roboterbeteiligung (Quelle: AUVA – Abt. Statistik / DGUV – Referat Statistik)

Viele Normen, viele Fragen bei der Umsetzung

Insgesamt ist der Verlust der Maschinenkontrolle inklusive unerwartetem Anlauf der häufigste Grund für Unfälle mit Robotern, gefolgt von unkoordinierten, unpassenden Bewegungen des Menschen bei der Arbeit an und mit dem Roboter. Zwar spiegeln diese Daten keine Unfälle aus der noch verhältnismäßig neuen, direkten Mensch-Roboter-Kollaboration wider, sondern aus klassischen Automatisierungsszenarien, belegen aber dennoch das nach wie vor existente Gefährdungspotenzial von Industrierobotern im Allgemeinen.

Bei den bei Unfällen betroffenen Körperteilen sind am stärksten die Hände betroffen (37%), gefolgt vom Kopf (22%) und den oberen Extremitäten wie Schulter, Arme und Handgelenke (20%). Zumeist sind oberflächliche Wunden und Prellungen die aus dem Unfall resultierende Verletzung, in rund 15% der Fälle jedoch auch Quetschungen und bei immerhin jedem zehnten Unfall Frakturen.

Häufiger als im Regelbetrieb passieren Unfälle zwischen Menschen und Robotern in Ausnahmesituationen wie der Einrichtung, Wartung und beim Beheben von Störungen – eine Indikation dafür, dass auch bei der Gestaltung einer Mensch-Roboter-Kollaboration auf diese Betriebsphasen besonderes Augenmerk bei der Absicherung gelegt werden muss.



Mehr Sicherheit bei der Implementierung

In Anbetracht des Neuheitsgrades des Konzepts der Mensch-Roboter-Kollaboration und der vorherrschenden, geschilderten Schwierigkeiten der Unternehmen bei der Einführung von MRK-Systemen haben sich der TÜV AUSTRIA und Fraunhofer Austria Research zur Aufgabe gemacht, etwaige Schwachstellen der für MRK relevanten Normen und Richtlinien genauer zu identifizieren und dabei die Fragen zu beantworten:

- Welche zusätzlichen Anforderungen, die bislang nicht durch Normen und Richtlinien formuliert sind, können zur Risikominderung in der Mensch-Roboter-Kollaboration an die Applikation gestellt werden?
- Welche Anforderungen, die bereits durch Normen und Richtlinien formuliert sind, können weiter konkretisiert werden, um Unternehmen als Hilfestellung bei der Planung, Umsetzung und Zertifizierung von MRK-Anwendungen zu dienen? Beispielsweise: Welche Technologien und/oder Methoden stehen zur Verfügung, um die Erfüllung einer bestimmten Anforderung zu unterstützen?

Ziel von TÜV AUSTRIA und Fraunhofer Austria Research ist es, diesen Fragestellungen in einem integrierten Safety & Security Konzept zu begegnen, das Unternehmen bei der Einführung von MRK-Anwendungen zukünftig unterstützen zu können. Zur Identifikation des Handlungsbedarfs wurde eine zweistufige Vorgehensweise implementiert:

1. Identifikation und Formulierung von Anforderungen

Analyse u.a. von Robotermanuals und Use Cases, Durchführung von Expertenbefragungen, Analysen von Unfällen mit Roboterbeteiligung. In dieser Phase konnten rund 240 einzelne Anforderungen identifiziert werden, deren Erfüllung zur Sicherheit in der Mensch-Roboter-Kollaboration beiträgt.

2. Korrelationsanalyse und Identifikation von tatsächlichen Handlungsfeldern

Analyse der Abdeckung und des Konkretisierungsgrads der identifizierten Anforderungen durch die einschlägigen Normen und Richtlinien. Die nicht oder, aus Sicht von TÜV AUSTRIA und Fraunhofer Austria, nicht mit ausreichender Konkretisierung von Normen abgedeckten Anforderungen können in 18 Handlungsfelder gegliedert werden:

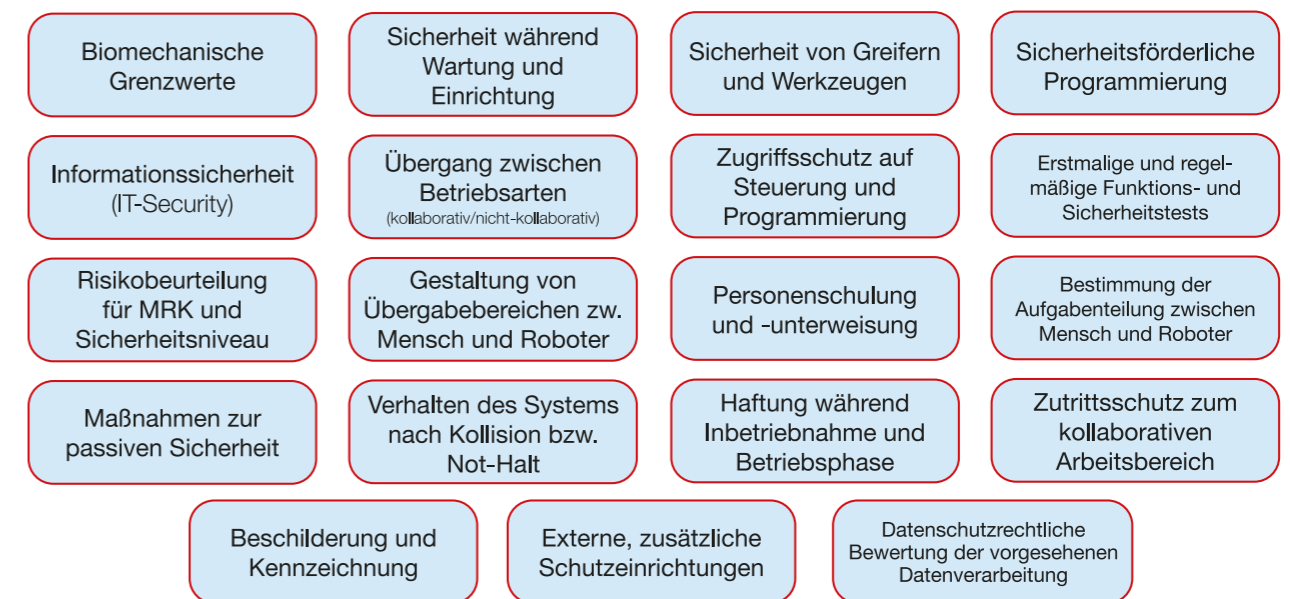


Abb. 7: Identifizierte Handlungsfelder zur Erhöhung der Sicherheit in MRK-Anwendungen

Mehr Sicherheit bei der Implementierung

Die im Rahmen der Untersuchung identifizierten Handlungsfelder decken ein breites thematisches Spektrum ab und tangieren die aktive Sicherheit, die passive Sicherheit, die Informationssicherheit, wie auch organisationsbezogene Aspekte, bspw. der Kennzeichnung und Mitarbeiterschulung.

Das Handlungsfeld der **biomechanischen Grenzwerte** zeigt anschaulich, mit welchen Schwierigkeiten sich Integratoren und Betreiber bei der Anwendung der Normvorgaben aktuell ausgesetzt sehen. Mit Erscheinen der ISO/TS 15066 wurden im März 2016 erstmals Grenzwerte für die Belastung des menschlichen Körpers im Rahmen einer Kollision mit einem Roboter veröffentlicht. Erarbeitet wurden diese durch empirische Kollisionsversuche zur Ermittlung der Schmerzempfindlichkeit an der Mensch-Maschine-Schnittstelle (8).

Die Daten erhalten Grenzen für Kraft und Druck, also Kraft je Fläche, für alle relevanten Körperbereiche (vgl. Abbildung 8).

Unter Kenntnis der bewegten Masse innerhalb einer MRK-Applikation (sich beispielsweise aus dem Gewicht des bewegten Teils des Roboterarms, des Endeffektors und des manipulierten Werkstücks ergebend) und der parametrisierten Robotergerwindigkeit lassen sich also wirkende Kräfte errechnen und, so die Idee, mit den Grenzwerten der ISO/TS 15066 vergleichen.

Nun sind die Druckgrenzwerte allerdings auf eine Kontaktfläche von einem Quadratzentimeter normalisiert. Auch wird von einem „flachen“ Kontakt mit gleichmäßiger Kraftverteilung ausgegangen. Natürlich ist ein derart idealisierter Kontaktfall in der Realität schwerlich zu finden, sodass nur Messungen der tatsächlich herrschenden Kräfte und Drucke unter Berücksichtigung von Werkstückgeometrien und tatsächlich möglicher Kollisionsszenarien auf die Einhaltung der biomechanischen Grenzwerte schließen lassen – und die Hilfestellung, welche die Norm bietet, endet.

Die Identifikation solcher realistischer Kollisionsszenarien, die Auswahl geeigneter Messverfahren und -mittel oder eben die Übertragung der biomechanischen Grenzwerte auf geometrisch komplexe Kollisionsfälle sowie die Überführung der Untersuchungsergebnisse in das Roboterprogramm, also beispielsweise die Definition von Geschwindigkeits- und Bereichsgrenzen, werden nicht von der Norm unterstützt sondern obliegen der Erfahrung des Beurteilenden, die häufig noch nicht vorhanden ist.

Als eines der identifizierten Handlungsfelder wird das Thema „Biomechanische Grenzwerte“ im Projekt von TÜV AUSTRIA und Fraunhofer Austria Research gemeinsam mit weiteren Partnern intensiv bearbeitet werden, sowohl theoretisch als auch experimentell. Die erlangten Erkenntnisse werden direkt in die Entwicklung eines integrierten Safety & Security Konzepts einfließen.

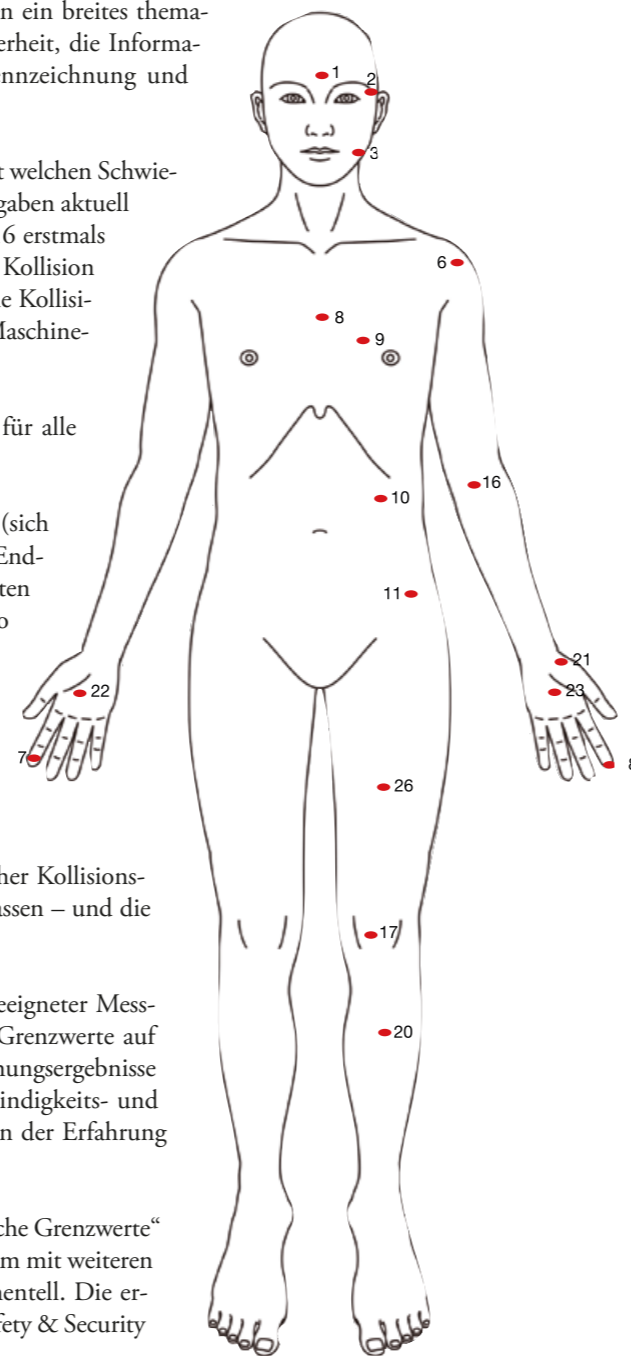


Abb. 8: Körpermodell nach ISO/TS 15066 (Frontseite) (4)

Entwicklung eines integrierten Safety & Security Konzepts für die Mensch-Roboter-Kollaboration

In Reaktion auf die identifizierten herrschenden Unsicherheiten der produzierenden Unternehmen in Österreich bei der Gestaltung, Beurteilung und Inbetriebnahme von MRK-Applikationen und angelehnt an die identifizierten Handlungsfelder haben der TÜV AUSTRIA und die Fraunhofer Austria Research GmbH per Mai 2016 ein zweijähriges, stark anwendungsorientiertes Forschungsprojekt initiiert.

Ziel des Vorhabens ist die Entwicklung eines **integrierten Safety- und Security-Konzepts**, welches ganzheitlich alle maschinensicherheitsbezogenen Aspekte der MRK, also die Safety, betrachtet und weiterhin der zukünftigen Relevanz der Daten- und Informationssicherheit sowie des Datenschutzes in einer hochvernetzten Fabrikumgebung, der Security, Rechnung trägt. Hierbei geht es weniger darum, grundsätzlich neue Vorgaben zu erarbeiten als vielmehr das vorhandene Spektrum regulatorischer Richtlinien und Empfehlungen aus den Welten der Anlagen- und der Informationssicherheit mit Bezug zur Mensch-Roboter-Kollaboration in ein integriertes Sicherheitskonzept zu überführen und auf Grundlage der Voruntersuchungen zu konkretisieren.

Damit wird der Industrie ein nachvollziehbarer Gestaltungsleitfaden in die Hand gegeben, der die wichtigsten, d.h. primär die sicherheitsrelevanten Gestaltungsparameter einer MRK-Applikation hinsichtlich einer von Beginn an optimalen Auslegung und Vernetzung der Anlage beschreibt und in der sich anschließenden und zwingend notwendigen Risikobeurteilung als klarer Fahrplan dient. Dadurch wird Unternehmen eine schnelle und einfachere Integration ermöglicht.



Abb. 9: Grobe Vorgehensweise bei der Erarbeitung des integrierten Safety & Security-Konzepts

Entwicklung eines integrierten Safety & Security Konzepts für die Mensch-Roboter-Kollaboration

Inhaltlich deckt das *integrierte Safety & Security-Konzept* alle im Rahmen der Recherchen, Studien und Unfallanalysen identifizierten Teilbereiche ab – von der Programmierung unter Berücksichtigung biomechanischer Kollisionsgrenzwerte bis zu organisatorischen Maßnahmen, wie der Zutrittsregelung zum Kollaborationsbereich, und hat allein aufgrund seiner Vollumfänglichkeit bereits Neuheitscharakter.

Über diese theoretische Erarbeitung hinaus wird das Konzept zur Sicherstellung seiner Richtigkeit, Vollständigkeit und Anwendbarkeit über den gesamten Projektzeitraum hinaus in eigens installierten MRK-Applikationen in der *TU Wien Pilotfabrik Industrie 4.0* in Wien-Aspern erprobt, validiert und aufgrund der dort erzielten Erkenntnisse angepasst. Die Pilotfabrik Industrie 4.0 stellt eine modellhafte, aber dennoch ganzheitliche Produktionsumgebung auf über 600 m² zur Verfügung und bietet die Möglichkeit, den ersten Versuchsträger, einen *Universal Robot UR5*, an verschiedenen Stellen innerhalb von Fertigungs-, Montage- und Logistikprozessen virtuell wie auch physisch zu integrieren und mit seiner Umgebung über unterschiedliche Kommunikationsprotokolle zu vernetzen.

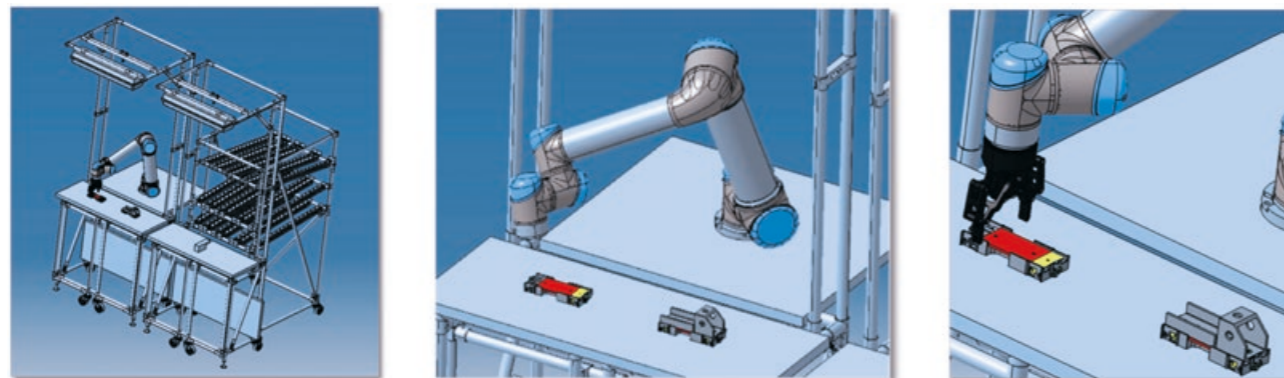
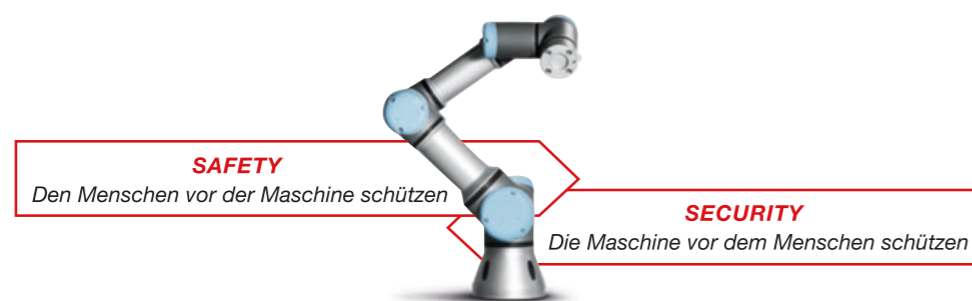


Abb. 10: Kollaborationsarbeitsplatz in der TU Wien Pilotfabrik Industrie 4.0

Im ersten Szenario ab Herbst 2016 wird die Montage eines Miniatur-LKWs an einem Kollaborationsarbeitsplatz umgesetzt, an welchem Mensch und Roboter einander gegenüberstehend gleichzeitig auf denselben Arbeitsbereich einwirken. Grundlage ist ein klassisches Montagesystem, wodurch häufig vorherrschende Rahmenbedingungen in der Fertigungsindustrie einerseits abgebildet und die Transferfähigkeit der Projektergebnisse andererseits gesichert werden.

Die Zwischenergebnisse aus der Erarbeitung des integrierten Safety & Security-Konzepts für die Mensch-Roboter-Kollaboration werden fortlaufend durch die Projektpartner publiziert, die Endergebnisse sind im Frühjahr 2018 zu erwarten. Industrieunternehmen mit Interesse an Erfahrungsaustausch und projektbasierter Zusammenarbeit zum Thema der Gestaltung, Umsetzung und Bewertung von MRK-Applikationen können sich jederzeit an die Projektleiter wenden.



Über TÜV AUSTRIA und Fraunhofer Austria Research

TÜV AUSTRIA Gruppe

Der österreichische TÜV ist ein internationales Unternehmen mit Niederlassungen in mehr als 40 Ländern der Welt und über 1400 Mitarbeitern. Das Leistungsspektrum reicht von der Maschinensicherheit und der IT – Security über Managementsystem-Zertifizierung, der Prüfungen von Aufzügen und Druckgeräten, Anlagensicherheit, Aus- und Weiterbildung, Medizintechnik, Elektrotechnik, umweltschutztechnische Gutachten, Schallschutzgutachten, Carbon Footprint-Evaluierungen, Loss Adjustments, AppChecks, alle Arten von Zertifizierungen und Kalibrierungen, Produktprüfungen, 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

Fraunhofer Austria Research

Fraunhofer ist die größte Forschungsorganisation für anwendungsorientierte Forschung in Europa mit über 24.000 Mitarbeitern. Die Forschungsfelder richten sich nach den Bedürfnissen der Menschen: Gesundheit, Sicherheit, Kommunikation, Mobilität, Energie und Umwelt. Und deswegen hat die Arbeit der Forscher und Entwickler bei Fraunhofer großen Einfluss auf das zukünftige Leben der Menschen. Sie sind kreativ, gestalten Technik, entwerfen Produkte, verbessern Verfahren und eröffnen neue Wege. In Österreich arbeiten 51 Mitarbeiter an Projekten insbesondere in den Bereichen Produktions- und Logistikmanagement sowie Visual Computing und insbesondere an der Innovierung von Wertschöpfungsprozessen durch emergierende Technologien.

Ansprechpartner zum Thema Mensch-Roboter-Kollaboration:

Fabian Ranz, M.Sc. – fabian.ranz@fraunhofer.at

Quellen

- (1) Acatech – Deutsche Akademie der Technikwissenschaften: *Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0*, April 2013.
- (2) Matthias Björn, Ding Hao: *Die Zukunft der Mensch-Roboter-Kollaboration*, 2013.
- (3) *Maschinenrichtlinie - Richtlinie 2006/42/EG des europäischen Parlaments und des Rates vom 17. Mai 2006 über Maschinen und zur Änderung der Richtlinie 95/16/EG (Neufassung)*.
- (4) ISO/TS 15066:2016(E): *Technical Specification: Robots and robotic devices – collaborative robots. Erste Edition*, 15.2.2016
- (5) Palmin, A., Kobes, P.: *Security-Management und Security-Transparenz in der industriellen Automatisierung*. ISBN 978-3-981406-2-1.
- (6) Gaede, C.; Ranz, F.; Hummel, V.; Echelmeyer, W.: *A Study on Challenges in the Implementation of Human-Robot-Collaboration*, (in Veröffentlichung).
- (7) Bauer, W. (Hrsg.): *Leichtbauroboter in der manuellen Montage – einfach EINFACH anfangen*. Fraunhofer-Institut für Arbeitswirtschaft und Organisation (IAO), 2016.
- (8) *Wissenschaftlicher Abschlussbericht zum Vorhaben FP-0317: „Kollaborierende Roboter – Ermittlung der Schmerzempfindlichkeit an der Mensch-Maschine-Schnittstelle“*. Universitätsmedizin – Institut für Arbeits-, Sozial- und Umweltmedizin, Mainz.
- (9) Sebastian Wallner, Karlbeinz Mayer: *Ein ganzheitliches IT-Sicherheitskonzept für Industrie 4.0*, 2016.

Abbildungen

KUKA AG (Coverfoto), Fraunhofer Austria Research (Abb. 3, 7, 9, 10), Shutterstock (S. 4, 6, 7, 14, 16), Fotolia (S. 8), „Safe Human-Robot Collaboration Combines Expertise and Precision in Manufacturing“ (Abb. 2), ATN Hölzel GmbH (Abb. 4), „Ein ganzheitliches IT-Sicherheitskonzept für Industrie 4.0 Infrastrukturen“ in Anlehnung an OPC Foundation (Abb. 5), ISO/TS 15066 (Abb. 8).

WhitePaper



TÜV AUSTRIA Gruppe
DI Alexandra Markis
TÜV-Austria-Platz 1
2345 Brunn am Gebirge
Mail: i4.0@tuv.at

www.tuv.at/i40

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

www.fraunhofer.at