HERAUSFORDERUNGEN BEI DER SICHEREN GESTALTUNG VON AUTONOMEN SERVICEROBOTERN FÜR ASSISTENZFUNKTIONEN

Dipl.-Ing. Theo Jacobs, theo.jacobs@ipa.fraunhofer.de

Fraunhofer-Institut für Produktionstechnik und Automatisierung IPA

DIN § § ISO § CE

Fraunhofer IPA

AGENDA
4.9.2018, 15:15 – 17:15 UHR

- Einführungsvortrag: Sicherheitsstandards für Roboter – Stand der Technik und aktuelle Entwicklungen
  - Europäische Richtlinien und harmonisierte europäische Standards
  - Sicherheitsstandards für Roboter
  - Auslegung von Sicherheitsfunktionen und sicherheitsgerichteter Software
  - Das Normungsgremium TC 299
- Diskussionsrunde: Herausforderungen bei autonomen Servicerobotern, z.B.
  - Redundanz durch die Kombination vieler einfacher Sensoren?
  - Vorhersehbare Fehlanwendungen
  - Tolerierbare Restrisiken

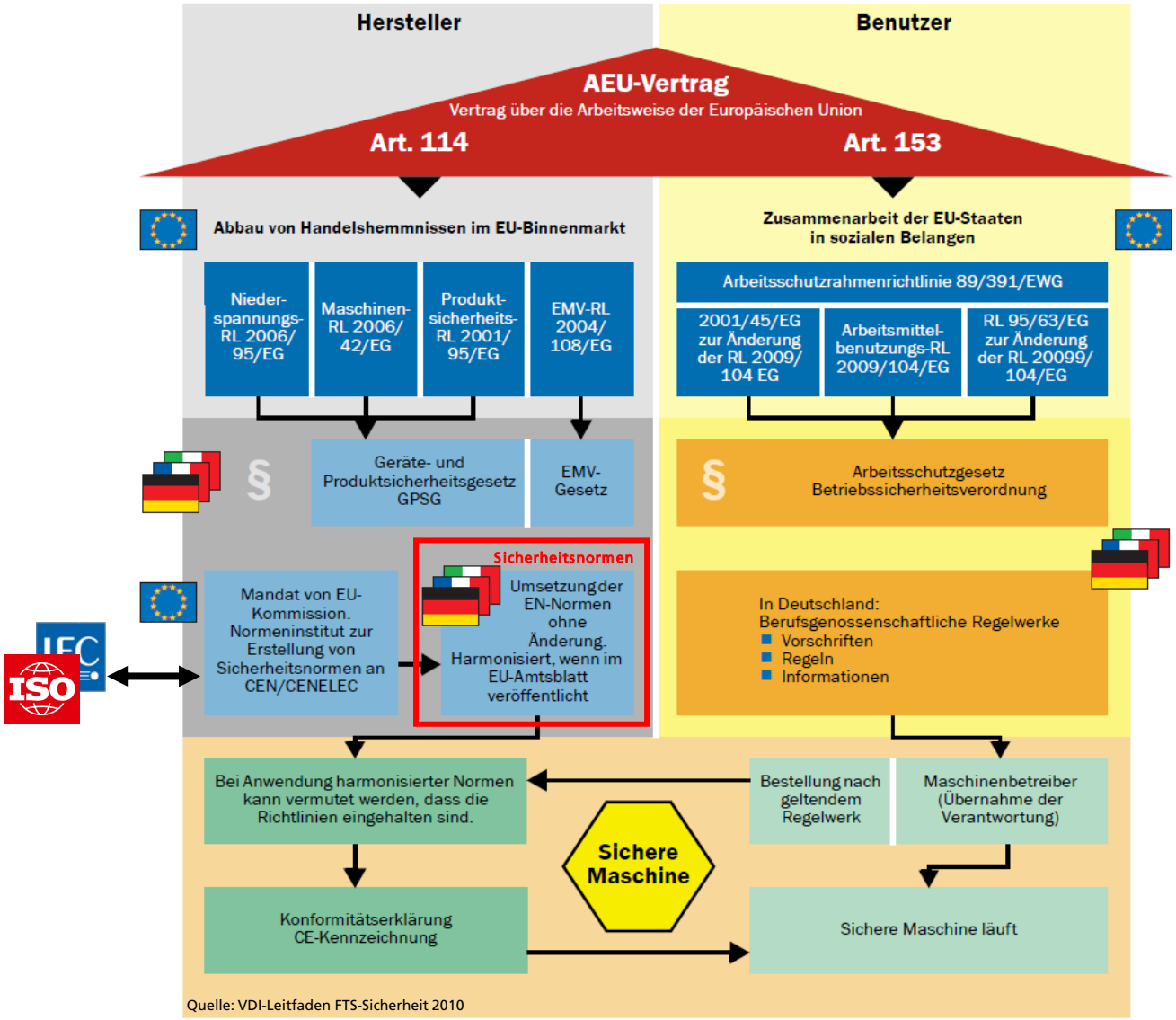
SICHERHEITSSTANDARDS FÜR ROBOTER – STAND DER TECHNIK UND AKTUELLE ENTWICKLUNGEN

Dipl.-Ing. Theo Jacobs

Fraunhofer IPA

Fraunhofer IPA

Europäische Richtlinien

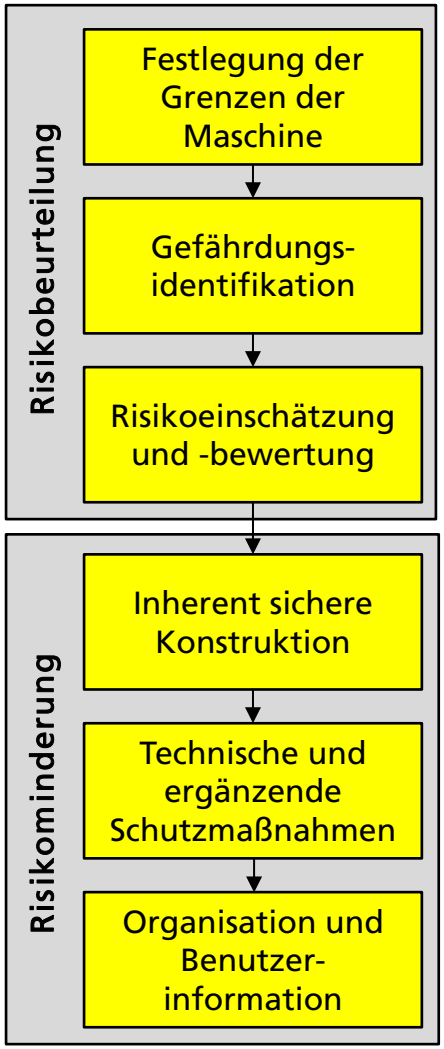


Quelle: VDI-Leitfaden FTS-Sicherheit 2010

Fraunhofer IPA

ISO 12100: Risikobeurteilung und Risikominderung

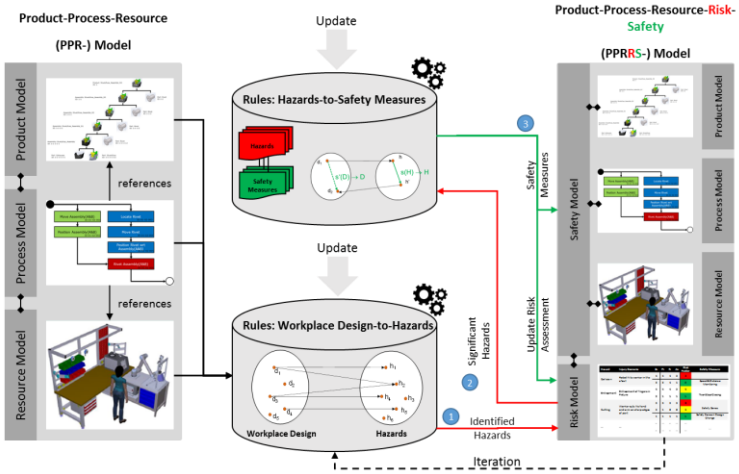
- ISO 12100 – Sicherheit von Maschinen – Allgemeine Gestaltungsleitsätze – Risikobeurteilung und Risikominderung
- Generelle Anforderungen für Maschinen (z.B. Notausknöpfe, Unerwarteter Anlauf, …)
  - Verpflichtung zur Durchführung einer Risikobeurteilung um nicht akzeptable Risiken zu identifizieren
  - Minderung nicht akzeptabler Risiken, bis das Restrisiko akzeptabel ist
- Der Hersteller muss entscheiden, was ein akzeptables Risiko ist
  - In Hinblick auf den aktuellen Stand der Technik (z.B. verfügbare Sicherheitseinrichtungen)
  - In Hinblick auf ähnliche Produkte auf dem Markt

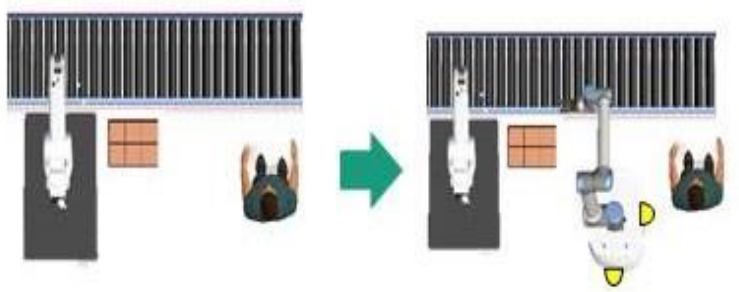


Fraunhofer IPA

Trend: Computer-Aided Risk Assessment

- CARA – Computer-Aided Risk Assessment
  - Automatischer Risikobeurteilung für (Industrie-) Roboterapplikationen basierend auf formalen Methoden und Modellverifikation
  - Workspace Design Tool zur Offline-Planung und zur Berechnung des Safety-Performance Tradeoffs
- Rekonfigurierbare Sicherheitslösungen – „Plug & Safe“
  - Rekonfiguration basierend auf Modellen von Sicherheitskomponenten, Kommuniktion und logischen Verknüpfungen





Fraunhofer IPA

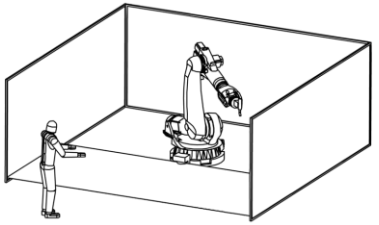
Sicherheitsnormen für Industrieroboter

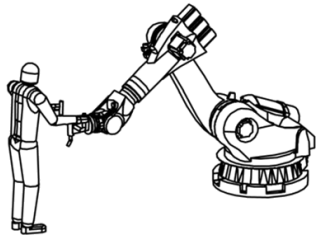
- ISO 10218-1 – Industrieroboter – Sicherheitsanforderungen – Teil 1: Roboter
  - Beispiele: mechanische und elektrische Auslegung, Bediengeräte, Betriebsmodi, sicherheitsgerichtete Komponenten im Inneren des Roboters, etc.
- ISO 10218-2 – Industrieroboter – Sicherheitsanforderungen – Teil 2: Robotersysteme und Integration
  - Anforderungen zur Integration eines Industrieroboters in ein Automatisierungssystem
  - Beispiele: Kollaboratives Arbeiten wie überwachter Halt, Handführung, Sicherheits- und Abstandsüberwachung
- ISO/TS 15066 – Roboter und Robotikgeräte – Kollaborierende Roboter
  - Festlegung tolerierbarer Kräfte und Drücke bei Kollisionen mit verschiedenen Körperteilen
  - Anleitung zur Messung von Kollisionskräften und zur Verifikation der Grenzwerte

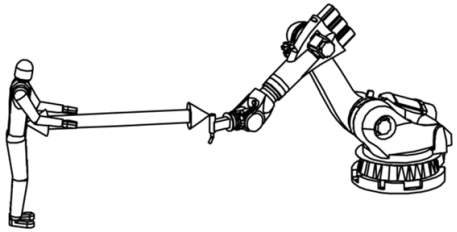
Fraunhofer IPA

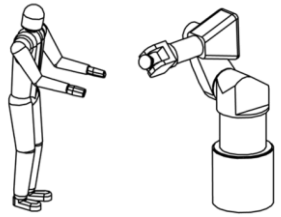
ISO 10218-2 – Arten der Mensch-Roboter-Kollaboration

1. Sicherheitsbewerteter überwachter Halt
   - Roboter im normalen automatischen Modus
   - Roboter hält beim Betreten des Arbeitsraums an und setzt die Bewegung nach dem Verlassen automatisch fort
2. Handführung
   - Roboter bewegt sich mit geringer Geschwindigkeit
   - Bewegung nur mit Zustimmeinrichtung
3. Geschwindgkeits- und Abstandsüberwachung
   - Roboter bewegt sich autonom mit geringer Geschwindigkeit
   - Roboter hält an, wenn der Abstand zum Menschen zu gering wird
4. Leistungs- und Kraftbegrenzung
   - Beschränkung der Kräfte und Leistung des Roboters
   - Kontakt zwischen Mensch und Roboter erlaubt





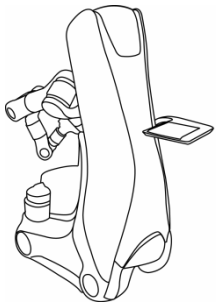


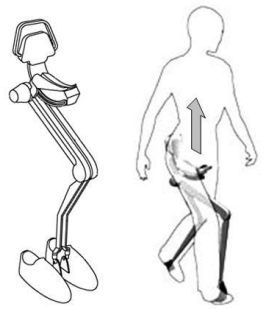


Fraunhofer IPA

Sicherheitsnorm für persönliche Assistenzroboter

- ISO 13482 – Roboter und Robotikgeräte – Sicherheitsanforderungen für persönliche Assistenzroboter
- Personal care robot: *“service robot that performs actions contributing directly towards improvement in the quality of life of humans, excluding medical applications.”*
  - Beispiele im Standard: “Mobile servant robot”, “Person carrier robot”, “Physical assistant robot”
  - Anforderungen an mechanisches und elektrisches Design
  - Anforderungen an die Auslegung und die Zuverlässigkeit des Steuerungssystems
- Neue Konzepte im Bereich der Servicerobotik
  - Gemeinsam genutzter Arbeitsraum als Standardfall
  - Beabsichtigter Kontakt zwischen Mensch und Roboter
  - Risiken basierend auf autonomen Aktionen und Entscheidungen



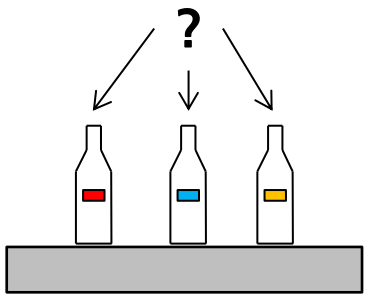


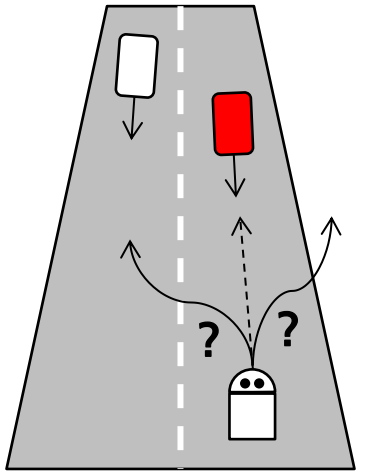
© ISO 13482

Fraunhofer IPA

Fehler bei autonomen Entscheidungen und Aktionen

- Autonome Entscheidungen können zu gefährlichen Situationen führen
  - Mobile servant robot greift das falsche Objekt (e.g. falsche Flasche um ein Getränk einzugießen)
  - Person carrier robot wählt einen ungeeigneten Pfad aus, um einem Hindernis auszuweichen
- Hersteller muss ermitteln, ob das Risiko aufgrund falscher Entscheidungen und Aktionen akzeptabel ist
- Möglichkeiten zur Risikominderung
  - Begrenzung der Komplexität von Entscheidungen (weniger Verantwortung für den Roboter)
  - Erhöhung der Zuverlässigkeit von Entscheidungen (z.B. bessere oder zusätzliche Sensoren, diversitäre Sensorprinzipe, etc.)



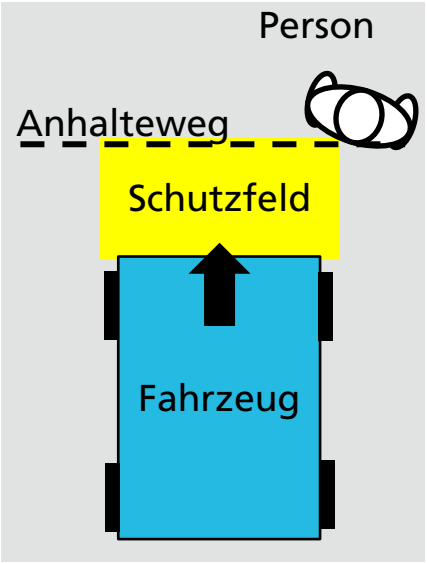


Fraunhofer IPA

Sicherheitsnormen für fahrerlose Flurförderzeuge

- Derzeit: DIN EN 1525 (1997)
  - Rein europäische Norm
  - Nicht unter aktueller Maschinenrichtlinie harmonisiert
  - Fokus: mechanische Gefährdungen, Elektrik , Steuerung
- Zukünftig: ISO 3691-4 (2019)
  - International einheitliche Norm
  - Erweitert u.a. bezüglich Betriebsarten, Betriebsanleitungen, Förderern auf FTF
- Anforderungen zu Personenerkennung:
  - Detektion einer Person im Fahrweg mittels Bumper oder Laserscanner
  - Fahrzeug muss innerhalb des Detektionsbereichs des Sensors anhalten können
  - Test der Personenerkennung mittels Prüfkörper (Zylinder, 200mm Durchmesser)

© MLR



Fraunhofer IPA

FTF oder mobiler Roboter?

Abgrenzung Industrieroboter – FTF

- ISO 10218 bezieht sich ausschließlich auf Manipulatoren und manipulierende Teile von mobilen Systemen
- Auslegung von mobilen Plattformen nach FTF-Normen
- Bei Fahrzeugen mit Manipulator Auslegung der Einzelteile nach jeweiliger Norm

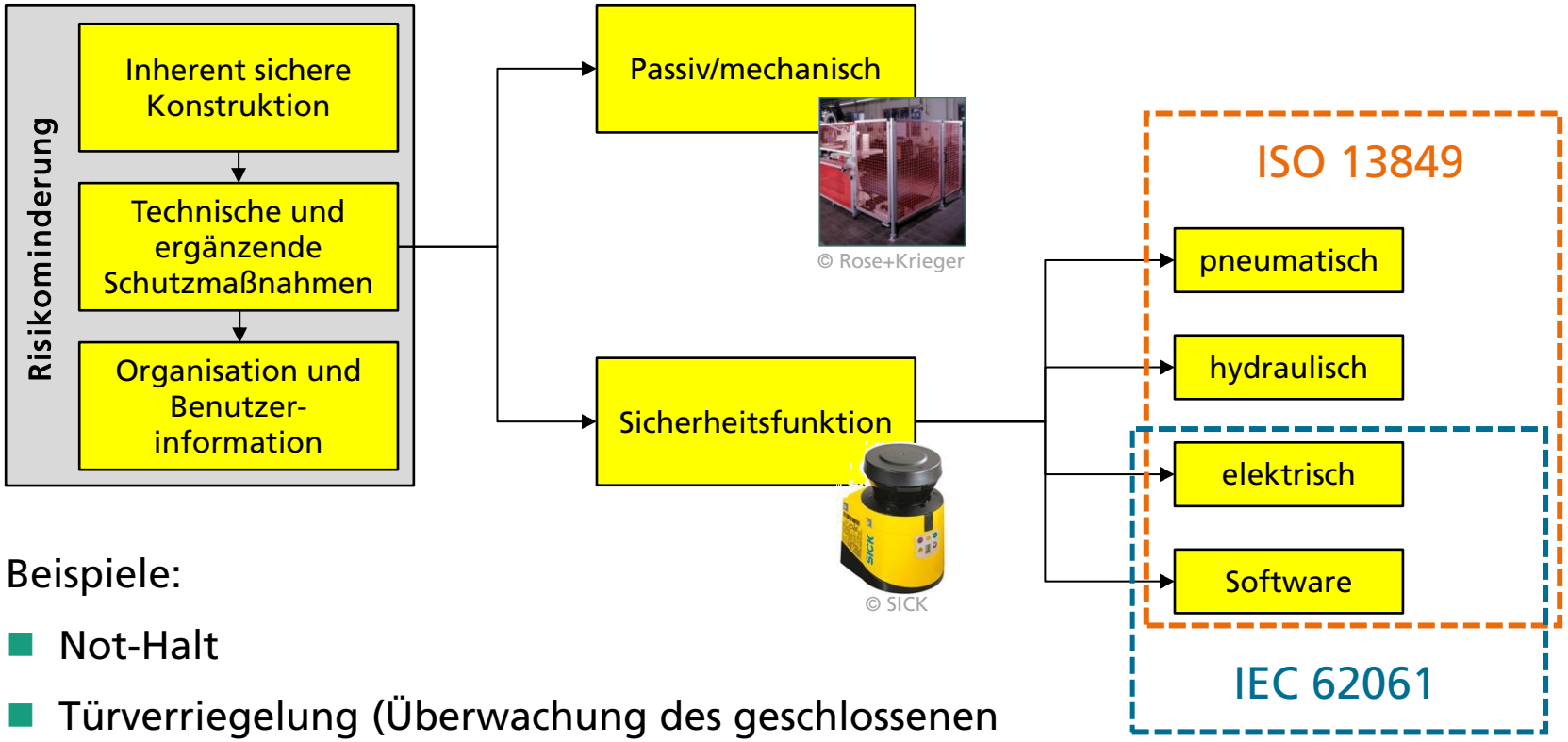
Quelle: KUKA AG

Abgrenzung Serviceroboter – FTF

- Serviceroboter existieren ausschließlich außerhalb der industriellen Automatisierung → FTF-Normen dort nicht gültig
- ISO 13482 umfasst auch sichere Auslegung von mobilen Plattformen
- ISO 13482 enthält Hinweise zu Kindern, Senioren, etc. als Nutzer

Fraunhofer IPA

Sicherheitsbezogene Teile von Steuerungen



Beispiele:

- Not-Halt
- Türverriegelung (Überwachung des geschlossenen Zustands einer Tür, wenn die Maschine läuft)
- Sicherheitsgerichtete Geschwindigkeits- und Positionsüberwachung
- Sicherheitsgerichtete Kraftüberwachung

Fraunhofer IPA

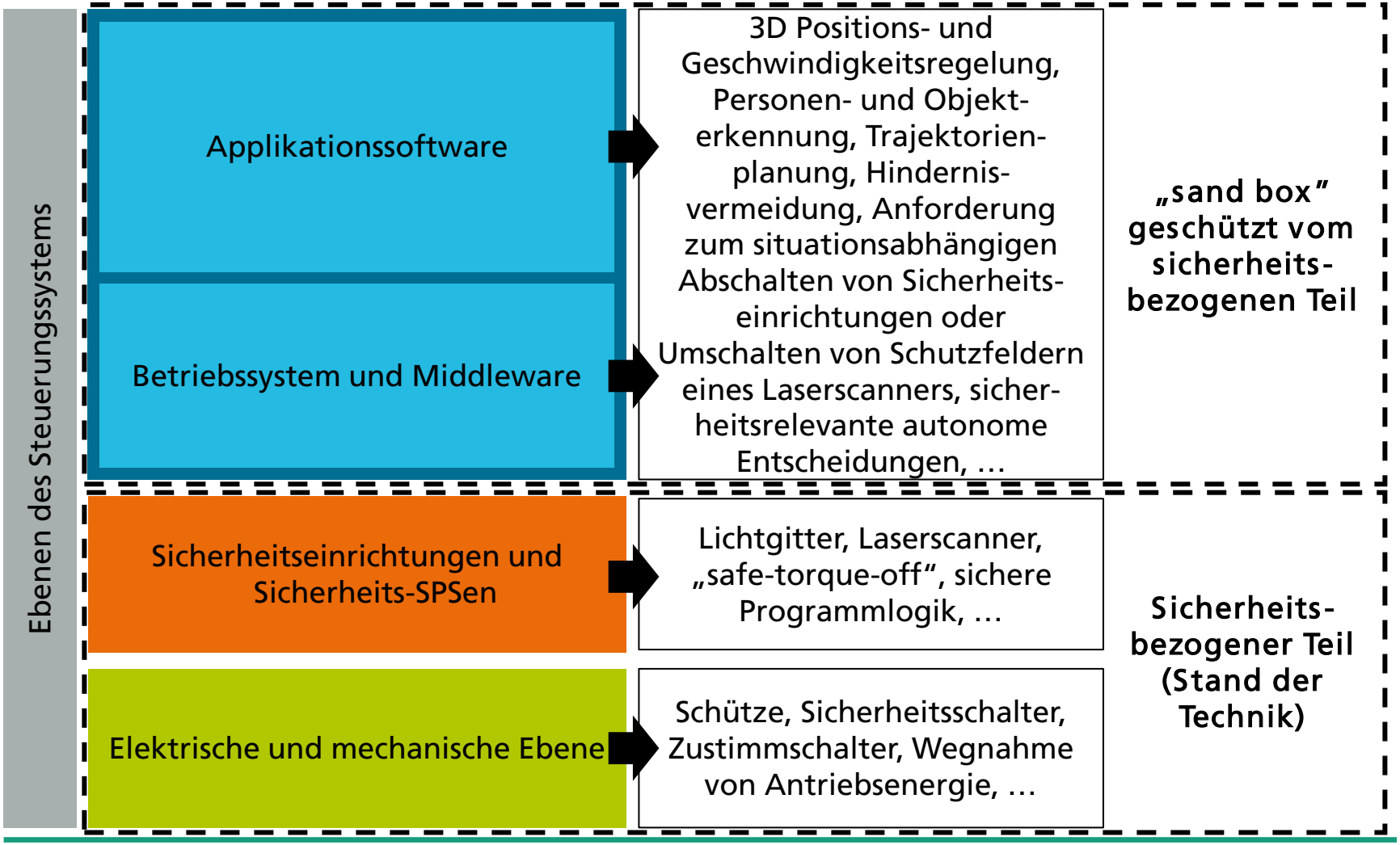
Anforderungen an eine sicheren Steuerung eines „Personal care robot“ (ISO 13482)

- Erforderlicher Performance Level gemäß ISO 13849-1:

Type of robot:	Mobile servant robot		Physical assistant robot				Person carrier robot	
Safety functions of personal care robots:	Type 1.1	Type 1.2	Type 2.1	Type 2.2	Type 2.3	Type 2.4	Type 3.1	Type 3.2
Protective stop	b	d	b	d	b	c	c	e
Emergency stop	d (no low risk option)		c	d	c	d	d	d
Limits to workspace (inc forbidden area avoidance)	b	d	b	d	a	d	n/a	e
Safety related speed control	b	d	b	b	b	d	c	e
Safety related force control	b	d	b	e	a	b	n/a	n/a
Hazardous collision avoidance	b	d	n/a	n/a	b	d	n/a	e
Stability control (inc overload protection)	b	d	n/a	c	b	d	b	d

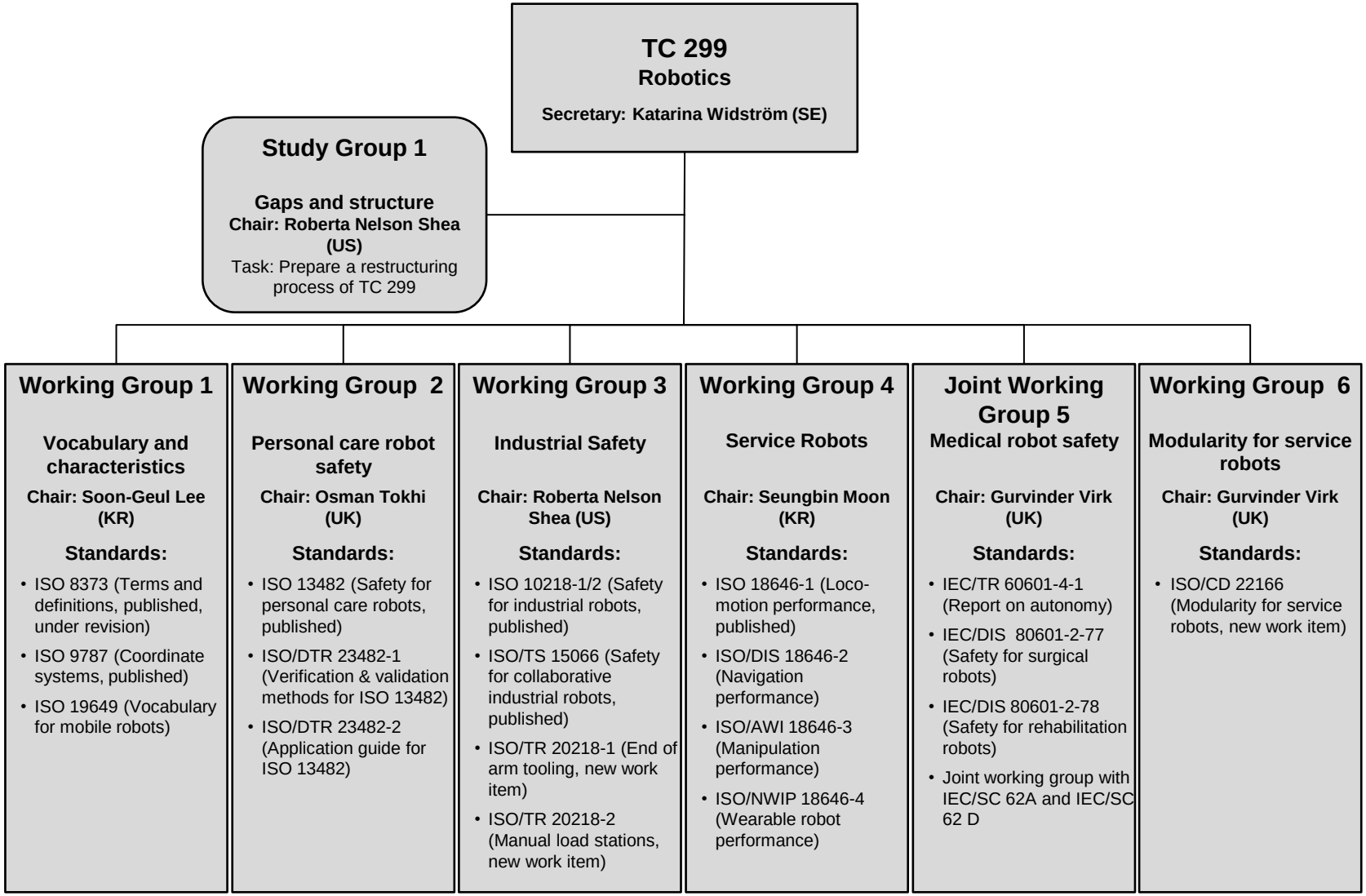
Fraunhofer IPA

Sichere Software: Grenzen des sicherheitsbezogenen Teils der Steuerung



Fraunhofer IPA

Das ISO-Normungsgremium TC 299



Fraunhofer IPA

Zusammenfassung

- Roboter fallen unter die Maschinenrichtlinie
  - CE-Kennzeichnung
  - Risikobeurteilung und Risikominderung nach ISO 12100
- Typ-C Sicherheitsstandards für Industrieroboter, Personal Care Robots und fahrerlose Flurförderzeuge
- Auslegung sicherheitsgerichteter Teile der Steuerung nach ISO 13849-1 oder IEC 62061
- Zukunftstrend: Implementierung komplexerer Funktionen in sicherer Software
- Entwicklung von Standards für Sicherheit und andere Aspekte im Normungsgremium ISO TC 299

Diskussion

Fraunhofer IPA

Themensammlung für die Diskussion

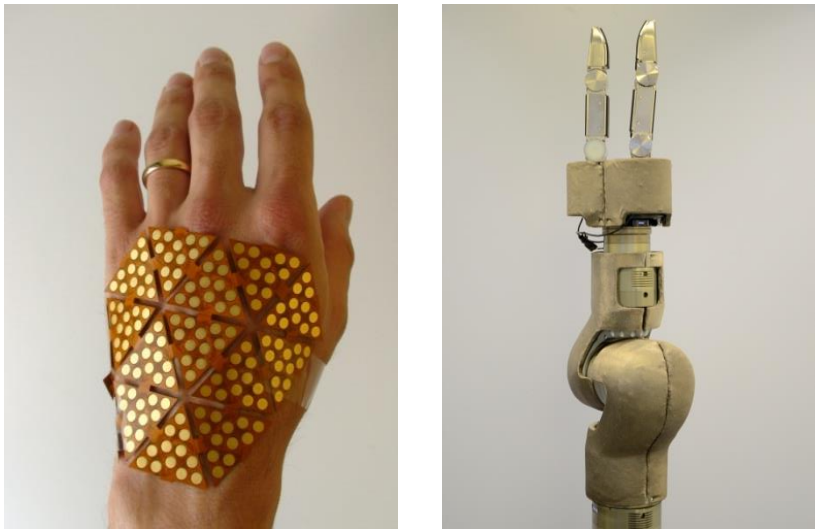
Themensammlung aus einem Safety-Workshop im Rahmen des Projektes ARAIG im Juli 2018 sowie zusätzliche Beiträge im Workshop. Priorisierung durch Abstimmung im Workshop. Diskussion bis Punkt 3.

1. Wie lässt sich Redundanz und damit Sicherheit durch die Kombination vieler einfacher Sensoren erreichen? (10 Stimmen)
2. Was sind vorhersehbare Fehlanwendungen und wie geht man damit um? (10 Stimmen)
3. Was ist ein tolerierbares Restrisiko? (9 Stimmen)
4. Verantwortung des Nutzers? (7 Stimmen)
5. Sicherheit vs. Forschungstätigkeit - Wie viel Aufwand muss man treiben? (4 Stimmen)
6. Herstellerverantwortung des Betreibers bei Modifikation des Roboters? (4 Stimmen)
7. Arbeitsraumbegrenzung: Stand der Technik (4 Stimmen)

1. Redundanz durch die Kombination vieler einfacher Sensoren?

- Beispiel: Viele günstige Kameras
  - z.B. 10 Kameras für je 150€

- Beispiel: Taktile Haut mit kapazitiven Elementen
  - Kondensator-Array erlaubt Ortsauflösung
  - Hierarchische Controller-Anordnung (Dreieck, Region, gesamte Haut)



© Roboskin

Fraunhofer IPA

1. Redundanz durch die Kombination vieler einfacher Sensoren?

- Anforderungen zur Nutzung nichtsicherer Elektronik finden sich in der Norm ISO 13849-1
  - Betrachtung von Fehlern gleicher Ursache (Common-Cause-Failures)
  - Es gelten spezielle EMV-Anwendungen an Steuerungen
- Für die Erstellung einer eigenen Sicherheitseinrichtung müssten Normen für Hersteller von Sicherheitseinrichtungen verwendet werden (z.B. IEC 61508)
- Wenn eine solche Sicherheitseinrichtung verkauft würde, müsste sie zusätzlich gemäß Maschinenrichtlinie von einer benannten Stelle zertifiziert werden (Baumusterprüfung). Eine Selbstzertifizierung ist nicht möglich.
- Der zusätzliche Aufwand (z.B. EMV-Prüfungen) erklärt, warum Sicherheitsbauteile auf dem Markt so viel teurer sind als andere Bauteile.
- Für die Erreichung von PL e ist zusätzlich zu beachten, dass diversitäre Sensorprinzipe gefordert werden.
- Oft sind relevante Daten für die Sicherheitsbewertung von Bauteilen gar nicht verfügbar (z.B. Lebensdauer von DC-Schützen beim Schalten induktiver Leistungen)

1. Redundanz durch die Kombination vieler einfacher Sensoren?

- Beispiel einer solchen Anwendung bei Daimler: die Anwesenheit einer Kiste, die von einem autonomen Fahrzeug bewegt wird, wird an der Station mit unsicheren Sensoren erfasst.
  - Für den Prozess sind zwei Sensoren notwendig → Zweikanaligkeit gegeben
  - Im Prozess muss jeder Sensor in jedem Zyklus einmal betätigt werden → 100% Diagnosedeckungsgrad
  - Sensoren werden mit einer sicheren Steuerung abgefragt → Alle Anforderungen erfüllt ohne sicherheitszertifizierte Sensoren
- Fazit: Die Kombination vieler einfacher Sensoren zur Erfüllung einer Sicherheitsfunktion ist – bis auf Ausnahmen – nicht zu empfehlen
- In öffentlichen Forschungsprojekten, bei den die Ressourcen eingeschränkt ist, ist so eine Lösung mit diversitären, unsicheren Sensoren an einer zuverlässigen Steuerung ggf. positiv zu bewerten, ehe gar keine Sicherheitseinrichtungen verwendet werden.

2. Wie umgehen mit vorhersehbaren Fehlanwendungen?

Beispiele:

Mitfahren verboten

Nicht für den Straßenverkehr zugelassen!

Nicht für medizinische Anwendungen!

3.24
vernünftigerweise vorhersehbare Fehlanwendung
Verwendung einer Maschine in einer Weise, die vom Konstrukteur nicht vorgesehen ist, sich jedoch aus dem leicht vorhersehbaren menschlichen Verhalten ergeben kann

aus der ISO 12100

Fraunhofer IPA

2. Wie umgehen mit vorhersehbaren Fehlanwendungen?

- Sicherheitshinweise können absurde Züge annehmen: Bei einem in Plastikfolie verpackten Küchenmesser wird vor Erstickungsgefahr in der Tüte (=Fehlanwendung) gewarnt, nicht aber vor dem scharfen Messer (=bestimmungsgemäße Anwendung)
- Die Maschinenrichtlinie bzw. ISO 12100 schreibt vor, dass auch bei Fehlanwendung die drei Schritte zur Risikominderung zur Anwendung kommen
  - Prüfung ob Konstruktion geändert werden kann oder ob Schutzmaßnahmen zum Einsatz kommen können. Beim Mitfahren auf FTF ist dies zum Beispiel nicht möglich, denn FTF sollen ja eine Last tragen können und es ist unmöglich zu unterscheiden, welche Last dies ist.
  - Erst dann Hinweise in der Bedienungsanleitung bzw. durch Piktogramme
- Frage: Ist es erlaubt, dass ein Hersteller die typische Nutzung (Hoverboard im Straßenverkehr) verbietet?
  - Antwort: In diesem Fall schon, weil nur Deutschland speziell diese Einschränkungen kennt. In anderen Ländern (z.B. Schweiz, Österreich), wäre die Nutzung erlaubt

2. Wie umgehen mit vorhersehbaren Fehlanwendungen?

- Frage: Ist es erlaubt, dass ein Hersteller die typische Nutzung (Hoverboard im Straßenverkehr) verbietet?
  - Das Problem betrifft nicht nur Hoverboards. Auch andere Geräte (z.B. Kinderfahrräder ohne Beleuchtung) sind für den Straßenverkehr in Deutschland nicht zugelassen.
  - Generell könnte so ein Gerät auch als Sportgerät genutzt werden. Damit stehen weitere Anwendungen offen.
- Exkurs: Straßenfahrzeuge
  - Die Europäische Kommission hat entschieden, dass Elektrofahrräder Maschinen darstellen und bei der Zertifizierung dementsprechend zu behandeln sind.
  - Elektrokleinfahrzeuge sind in der Schweiz und Österreich bereits zugelassen. Ein entsprechendes Gesetz für Deutschland ist in Arbeit
- Fazit: Der Hersteller kann in der Bedienungsanleitung viele Nutzungen ausschließen, wenn er vorhergehende Schritte (siehe oben) ausgeschöpft hat.

3. Was ist ein tolerierbares Restrisiko?

- Aus der ISO 12100:

> **5.6.2 Hinreichende Risikominderung**
>
> Die Anwendung des in 6.1 beschriebenen „Drei-Stufen-Verfahrens“ ist unverzichtbar, um eine hinreichende Risikominderung zu erreichen.
>
> Der Anwendung des „Drei-Stufen-Verfahrens“ entsprechend ist eine hinreichende Risikominderung erreicht, wenn
>
> — alle Betriebsbedingungen und alle Eingriffsmöglichkeiten berücksichtigt wurden,
>
> — die Gefährdungen beseitigt oder die Risiken vermindert wurden, soweit dies praktisch umsetzbar ist,
>
> — sämtliche neuen Gefährdungen, die aus ergriffenen Schutzmaßnahmen resultieren, in angemessener Weise berücksichtigt wurden,
>
> — die Benutzer über Restrisiken ausreichend informiert und gewarnt wurden (siehe 6.1, Schritt 3),
>
> — die durchgeführten Schutzmaßnahmen miteinander vereinbar sind,
>
> — die Folgen ausreichend berücksichtigt wurden, die sich durch den Gebrauch einer für den gewerblichen/industriellen Einsatz konstruierten Maschine im nicht gewerblichen/nicht industriellen Bereich ergeben können, und
>
> — die durchgeführten Schutzmaßnahmen die Arbeitsbedingungen der Bedienpersonen oder die Benutzerfreundlichkeit der Maschine nicht negativ beeinflussen.

- Offen:
  - Welches Restrisiko wird gesellschaftlich akzeptiert?
  - Unterscheidet sich das tolerierbare Restrisiko von Anwendung zu Anwendung?

3. Was ist ein tolerierbares Restrisiko?

- Es gibt definitiv unterschiedliche, von der Gesellschaft tolerierte Restrisiken. Diese können sich aber unterschiedlich auswirken. Zum Beispiel:
  - In der Industrie ist von eingewiesene Personen auszugehen. Diese können auch Maschinen bedienen, die ein höheres Risiko aufweisen.
  - Umgekehrt wird aber auch im Haushalt ein höheres Verletzungsrisiko akzeptiert (z.B. heiße Herdplatten, Kettensäge)
- Das hohe erwartete Sicherheitsniveau in der Industrie rührt auch daher, dass technisch inzwischen viel möglich ist.
  - Sicherheitseinrichtungen (z.B. Laserscanner, Lichtgitter) sind verfügbar
  - Gegenbeispiel Landmaschinen: Gängige Sensoren funktionieren im Outdoorbereich, insbesondere bei Regen und Nebel schlecht. Norm für Sicherheitskategorien fordert für die gleichen Performance Level geringere Zuverlässigkeiten.
- Grundsätzliches Kriterium für tolerierbare Restrisiken (auch vor Gericht): Was wäre technisch möglich? Machen andere Hersteller das auch so? Was würde ein Mehr an Sicherheit kosten? Wie stehen die Kosten im Verhältnis zum Gewinn?

3. Was ist ein tolerierbares Restrisiko?

- Juristische Anforderung: Es muss eine „verkehrsübliche Sorgfaltspflicht“ bei der Risikoanalyse wahrgenommen werden. → Risikoanalysen werden „nach bestem Wissen“ durchgeführt. Irrtümer sind „erlaubt“.
- Beispiel für ein als tolerabel eingestuftes Restrisiko, das nicht den Normen entspricht:
  - MRK-Roboter in beengter Umgebung. Der Werker muss „Schulter an Schulter“ mit dem Roboter arbeiten.
  - Roboter bewegt sich langsam und erfüllt fast alle Kriterien der ISO/TS 15066. Der Mensch könnte allerdings von sich aus mit nicht gepolsterten Teilen des Roboters zusammenstoßen
  - Beschluss: Wenn Kollisionen dadurch entstehen, dass sich der Mensch wesentlich schneller bewegt als der Roboter selbst, ist ein Überschreiten der Schmerzschwellen tolerierbar.