FH University of Applied Sciences TECHNIKUM WIEN

TÜV AUSTRIA

WhitePaper

Figure: FH Technikum Wien

Sichere mobile Robotik

in modernen Produktionsumgebungen

Funded by

City of Vienna | Economic Affairs, Labour and Statistics

Sichere mobile Robotik in modernen Produktionsumgebungen

Maßnahmen für Entwicklung, Integration und Betrieb

Forschungsprojekt SIP 4.0

Wien, Jänner 2022

FH Technikum Wien
Höchstädtplatz 6
A-1200 Wien

Clemens Ambros, MSc
Isabella Reithner, MSc
Maximilian Papa, MSc
Cecilia Perroni, MSc
Dipl.-Ing. Dr. techn. Kemajl Stuja
Dr. techn. Mohamed Aburaia, MSc

TÜV AUSTRIA Group
TÜV-Austria-Platz 1
A-2345 Brunn am Gebirge

DI Merim Cato
Martin Steiner, MSc
DI Alexandra Markis

Geschätzte Leserinnen und Leser!

Die hohe Marktdynamik und steigender Konkurrenzdruck im Bereich der produzierenden Industrie führen zu neuen Herausforderungen, denen sich alle Stakeholder stellen müssen. Mehr denn je stehen Flexibilität und rasche Anpassungsfähigkeit im Zentrum der Anforderungen an industrielle Systeme, wobei vor allem kleinen und mittelgroßen Betrieben (KMU) wenig niederschwellige Optionen zum Einsatz innovativer Technologien zur Verfügung stehen. Gleichzeitig steigt der Bedarf an flexiblen Sicherheitslösungen, die eine geeignete Einbindung jener neuen Methoden unter Einhaltung eines hohen Niveaus an Betriebssicherheit erlauben. Der Wandel von starren Fertigungsprozessen und -hierarchien hin zu flexiblen, modularen Fabrikskonzepten unter dem Sammelbegriff „Industrie 4.0“, verleiht beiden Aspekten noch zusätzliches Gewicht.

Eine der zukunftsträchtigen Technologien der „Fabrik von Morgen“ ist die mobile Robotik. Intralogistische, autonome Prozesse im realen Einsatz sicher und vor allem norm- und gesetzesgerecht zu gestalten, ist für österreichische KMU jedoch eine ambitionierte Aufgabe, die während dem Tagesgeschäft oftmals nicht durchführbar ist. Das durch die MA23 der Stadt Wien geförderte Forschungsprojekt „Sicherheit in intelligenten Produktionsumgebungen (SIP 4.0)“ setzt genau hier an und liefert greifbare und effektive Methoden zur sicheren Gestaltung von intelligenten und dynamischen Betriebsumgebungen und der Integration von Sicherheitskonzepten im Kontext der mobilen Robotik.

FH-Prof. Dipl.-Ing. Dr. Erich Markl
Leitung Fakultät Industrial Engineering
FH Technikum Wien

In der Welt der Industrie 4.0 haben Cyber-Physische-Systeme eine zentrale Funktion. Durch ihre Flexibilität und Modularität sind sie ein wesentlicher Bestandteil von modernen Produktionsanlagen. Mobile Robotik stellt eines dieser Systeme dar und manifestiert sich zunehmend als Zukunftstechnologie in diesem Bereich.

Aufgrund ihrer Fähigkeit kollaborativ zu verfahren, müssen mobile Roboter und Manipulatoren nicht hinter Schutzzäunen betrieben werden, da sie auf physische Kontakte reagieren können. Dies unterscheidet kollaborative Roboter wesentlich von klassischen industriellen Robotern. Die Nähe zum Benutzer birgt allerdings das Risiko, dass es bei unzureichenden Vorkehrungen - organisatorisch oder technisch, zur Gefährdung der persönlichen Sicherheit des Menschen durch den Roboter kommen kann. Eine unsichere Normenlage für mobile Manipulatoren erschwert die sichere Integration und Betrieb für Produktionsunternehmen zusätzlich.

TÜV AUSTRIA nimmt hier seine Rolle als Wegbereiter für neue Technologien wahr und hat daher mit großer Freude die Fachhochschule Technikum Wien bei der Umsetzung des Projekts SIP4.0 unterstützt. Als akkreditierte Stelle für die IEC 62443 war es uns besonders wichtig, dass neben der funktionalen Sicherheit auch das Thema Security for Safety eingehend betrachtet wird, um sicherzustellen, dass gesetzte Schutzmaßnahmen nicht durch Cyber Security Schwachstellen beeinträchtigt werden.

Das vorliegende White Paper wird speziell für KMUs eine wertvolle Unterstützung beim sicheren Einsatz mobiler Roboter darstellen und so die Akzeptanz dieser neuen Technologie weiter steigern.

DI Dr. Reinhard Preiss
Geschäftsfeldleiter Industry & Energy
TÜV AUSTRIA SERVICES GMBH

Der stetig steigende Digitalisierungsgrad von industriellen Anlagen bietet großes Potenzial zur Verbesserung von Produktivität und Flexibilität, führt aber auch zu deutlich höheren Anforderungen an die Cyber Sicherheit von Arbeitssystemen und industriellen Netzwerken. Höhere Interkonnektivität und die Möglichkeit eine Vielzahl an Systemen in einer Produktionsanlage zu überwachen, zu steuern und zu messen, führt auch zu immer neuen Risiken für Cyber-Angriffe. Ohne entsprechende OT-Sicherheitsmaßnahmen kann ein Angriff zu gravierenden Ausfallzeiten einer Anlage führen oder gar Menschenleben gefährden.

TÜV AUSTRIA hat in den letzten Jahren massiv in den Aufbau von Know-how im Bereich Industrial Cyber Security investiert und setzt hierbei auf die gezielte Verschränkung mit Anforderungen der physischen/ funktionalen Sicherheit, um Industriebetriebe mit holistischen und harmonisierten Sicherheitskonzepten zu unterstützen.

Im Projekt SIP4.0 begleiteten die Experten der TÜV TRUST IT die Fachhochschule Technikum Wien bei der Analyse wesentlicher Security-Aspekte von mobilen Robotern. Besonders erfreulich ist, dass die dabei entwickelten Konzepte auch mittels Penetrationstests in der Digital Factory der Fachhochschule praktisch evaluiert werden konnten.

Die Zusammenarbeit zwischen TÜV AUSTRIA und FH Technikum Wien zeigt den erfolgreichen Brückenschlag zwischen angewandter Forschung und industrieller Praxis – und einen daraus direkt entstehenden Mehrwert für den heimischen Wirtschaftsstandort.

Ing. Mag. Andreas Köberl
Geschäftsführer
TÜV TRUST IT TÜV AUSTRIA GMBH
SPP Handelsges.m.b.H.
Unternehmensgruppe TÜV AUSTRIA

Inhaltsverzeichnis

1 Einleitung

Die vierte industrielle Revolution stellt Unternehmen und Produktionsprozesse vor neue technische Herausforderungen, die bewältigt werden müssen, um die Anforderungen des internationalen Marktes erfüllen zu können und die Konkurrenzfähigkeit aufrecht zu erhalten. In diesem Kontext halten Vernetzung und Echtzeit-Anbindung von Systemen Einzug in die Produktion. Das Konzept Industrial Internet of Things (IIoT) ermöglicht, durch einen erhöhten Anteil an Elektronik und Software in den Maschinen, eine hochflexible Fertigung und schnellere Reaktion auf sich ändernde Anforderungen - Stichwort: Cyber-Physische Systeme (CPS).

Diese Art der Vernetzung bringt eine nicht mehr trennbare Verbindung zwischen „Safety“ und „Security“ mit sich, die besonders für eine der zentralen Schlüsseltechnologien der zukünftigen Produktion - die mobile Robotik - hohe Relevanz hat. Jedoch haben bisher erst wenige Unternehmen den Umstieg auf ein - in Bezug auf Security - sicheres System durchgeführt.

In vielen Fällen stellen finanzielle Aufwände das größte Hindernis für die Weiterentwicklung der eigenen Produktionsumgebung dar. Zusätzliche Unkenntnis über die zahlreichen regulatorischen Rahmenbedingungen (Gesetze, Normen, Richtlinien etc.) beeinträchtigt den Überblick von Betreibern über die komplexe Thematik. Das führt dazu, dass Unternehmen nicht ausreichend über die weitreichenden Gefahren und Risiken vernetzter Produktionssysteme und mobiler Robotik, sowie über das damit einhergehende Potential, informiert sind.

Dieses Whitepaper des Forschungsprojekts SIP 4.0 soll einen Überblick über allgemeine Anforderungen, regulatorische Rahmenbedingungen sowie daraus abgeleiteten Maßnahmen und Empfehlungen für Entwicklung, Integration und Betrieb von mobilen Robotern (je nach Quelle auch „autonomer mobiler Roboter, AMR“ oder „fahrerloses Transportsystem, FTS“ genannt) ermöglichen. Der Fokus wird hierbei auf Betriebs- (Safety) und Informationssicherheit (Security) gelegt und um Methoden zur Risikobeurteilung und -vermeidung ergänzt.

Definition: Maschinensicherheit („Safety“)
Der Begriff „Safety“ wird im Allgemeinen als Betriebssicherheit und Unfallvermeidung der jeweiligen Maschine verstanden. Der Schutz von Mensch und Umwelt vor physischem Schaden steht dabei im Vordergrund. Durch die österreichische Gesetzgebung wird jene Sicherheit einer Maschine zwingend vorgeschrieben. Darüber hinaus wird sie als statische Eigenschaft angesehen, die sich - unter der Voraussetzung ausbleibender Veränderungen - bis zum Lebensende einer Anlage nicht verändert.

Definition: Informationssicherheit („Security“)
Der Begriff „Security“ wird im Allgemeinen als Informationssicherheit und Manipulationsprävention des jeweiligen Systems verstanden. Der Schutz der Daten im System sowie die daraus folgende Aufrechterhaltung der Betriebssicherheit einer Maschine stehen dabei im Vordergrund. Im Gegensatz zu „Safety“ wird „Security“ als schnelllebig bezeichnet. Maßnahmen und Sicherheitssysteme können innerhalb kürzester Zeit obsolet werden, weshalb eine durchgehende Überprüfung auf Aktualität und insbesondere der Integrität, Verfügbarkeit und Vertraulichkeit des Systems sowie der Daten notwendig ist.

Die Einhaltung eines hohen Levels an IT-Security geht mit der Wahrung der drei CIA-Schutzziele einher: Vertraulichkeit (engl. Confidentiality), Integrität (engl. Integrity) und Verfügbarkeit (engl. Availability). Im IT-Sektor hat Vertraulichkeit die höchste Priorität, um Daten vor unbefugtem Zugriff zu schützen. Bei industriellen Anwendungen hingegen ist die Verfügbarkeit von zentraler Bedeutung, da das Nicht-Vorhandensein von Daten zu beträchtlichen Gefährdungslagen führen kann und die Personensicherheit einschränkt [1].

Die Vorgehensweise dieses Dokuments ist an das in der VDI 2206 [2] vorgestellte V-Modell angelehnt (siehe Abbildung 1). Diese Methodik erlaubt es, den Entwicklungszyklus in drei Abschnitte zu unterteilen, welche jeweils separat oder aufeinanderfolgend ausgeführt werden können. Jene Abschnitte stehen hierbei für die drei Rollen, die von Maschinen- bzw. AnlagenbauerInnen eingenommen werden können und lauten - in Übereinstimmung mit VDI 2206 [2], VDI 2182-1 [3] und ÖVE/ÖNORM EN 61508-1:2010 [4] - wie folgt:

- **Hersteller:** Personen oder Unternehmen, die einen mobilen Roboter und dessen Systeme entwickeln
- **Integrator:** Personen oder Unternehmen, die einen (zugekauften) mobilen Roboter und dessen Systeme modifizieren oder kombinieren
- **Betreiber:** Personen oder Unternehmen, die ein Komplettsystem (mobiler Roboter und dessen Implementierung) zukaufen und betreiben

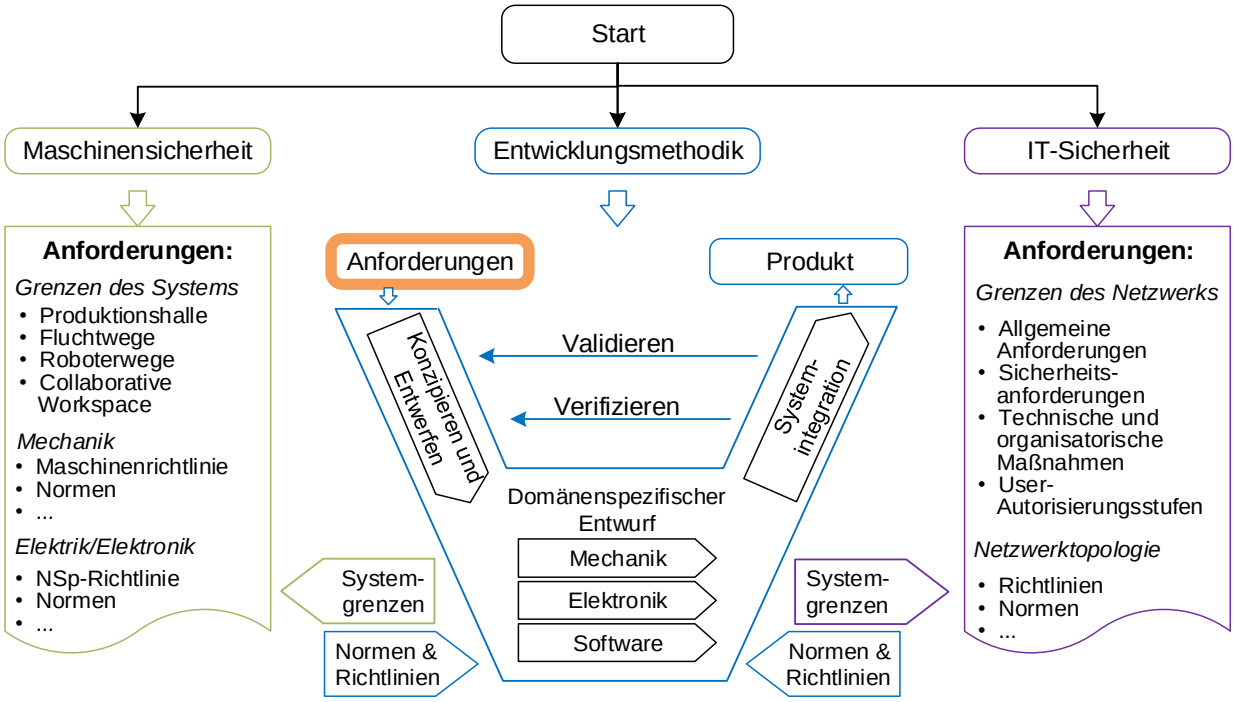


Abbildung 1: Anforderungsbezogene Entwicklungsmethodik auf Basis des V-Modells

In den folgenden Kapiteln werden die einzelnen Rollen beschrieben, um zu fällende Entscheidungen und sinnvolle Einordnungen des geplanten Projektes zu vereinfachen.

Daraufhin wird auf die mit den einzelnen Rollen zusammenhängenden Prozesse und Aufgaben eingegangen, die zur Implementierung von mobiler Robotik in eine intelligente Produktionsumgebung notwendig sind.

Darüber hinaus soll dieses Whitepaper einen Überblick über zentrale Faktoren der Entwicklung, der Integration und des Betriebs mobiler Robotik bieten und soll als Einstieg in die Thematik dienen. Dabei werden, mit Verweis auf die geltende Rechtslage, Richtlinien, Normen und Standards, sowohl die sichere Konstruktion mobiler Robotik, als auch der weiterführende Betrieb im Gesamtsystem behandelt. Des Weiteren werden Maßnahmen und Vorgehensweisen aus den hier betrachteten drei Lebensphasen um Erfahrungswerte ergänzt und angereichert.

Im Kontext der mit Industrie 4.0 assoziierten Produktionsparadigmen, spielt der autonome Waren- und Materialtransport eine entscheidende Rolle. Mobile Robotersysteme tragen zur Erreichung der damit einhergehenden Ziele bei und werden zukünftige Produktionsumgebungen prägen. Dies zeigt sich auch im World Robotics Report der International Federation of Robotics (IFR), worin eine jährliche Steigerung des Absatzvolumens von rund 30 Prozent prognostiziert wird [5].

Der Einsatz mobiler Robotik bietet zahlreiche Vorteile:

- flexible Auslegung des Produktionslayouts und schnellere Anpassung an veränderte Anforderungen
- damit einhergehende hohe Skalierbarkeit über Prozessteilnehmer, Schnittstellen und Auslastung
- Steigerung der Verfügbarkeit im Vergleich zu manueller Ausführung
- erhöhte Transparenz des betrieblichen Materialflusses
- hoher Automatisierungsgrad möglich
- effizientere Nutzung vorhandener interner Logistikwege und Ressourcen (im Vergleich zu linearen und ortsgebundenen Transportsystemen)
- hohe Flexibilität in Bezug auf Transportgut und Ladungsträger
- vergleichsweise simple Anbindung an vorhandene Produktions- und Logistiksysteme
- Einsatz in für den Menschen widrigen Verhältnissen
- Möglichkeit zur Erweiterung um Manipulatoren und Durchführung komplexer Tätigkeiten

Abbildung 2: Beispiel eines mobilen Roboters[1]

[1] https://www.mobile-industrial-robots.com/solutions/robots/mir1350/

2 Allgemeine Anforderungen

Der erste Schritt zur Automatisierung mit mobiler Robotik besteht aus einer detaillierten Anforderungsanalyse des durchführenden Unternehmens, womit auch der erste Schritt des hier vorgestellten V-Modells adressiert wird. Hierbei sollte ebenfalls darüber beraten werden, ob der Einsatz eines solchen Systems für die vorliegende Anwendung überhaupt sinnvoll und nutzbringend ist. Fällt diese Entscheidung positiv aus, müssen konkrete Anforderungen an das gewünschte System definiert werden, wobei besonderes Augenmerk auf das gewünschte Endergebnis gelegt werden sollte. Spätere Änderungen von Anforderungen sind, besonders, wenn sie nach der Konzept- und Entwurfsphase auftreten, nur mit erheblichem Mehraufwand möglich. Dementsprechend sollte die Ausgestaltung jener in Bezug auf Safety und Security des Systems von Beginn an berücksichtigt werden.

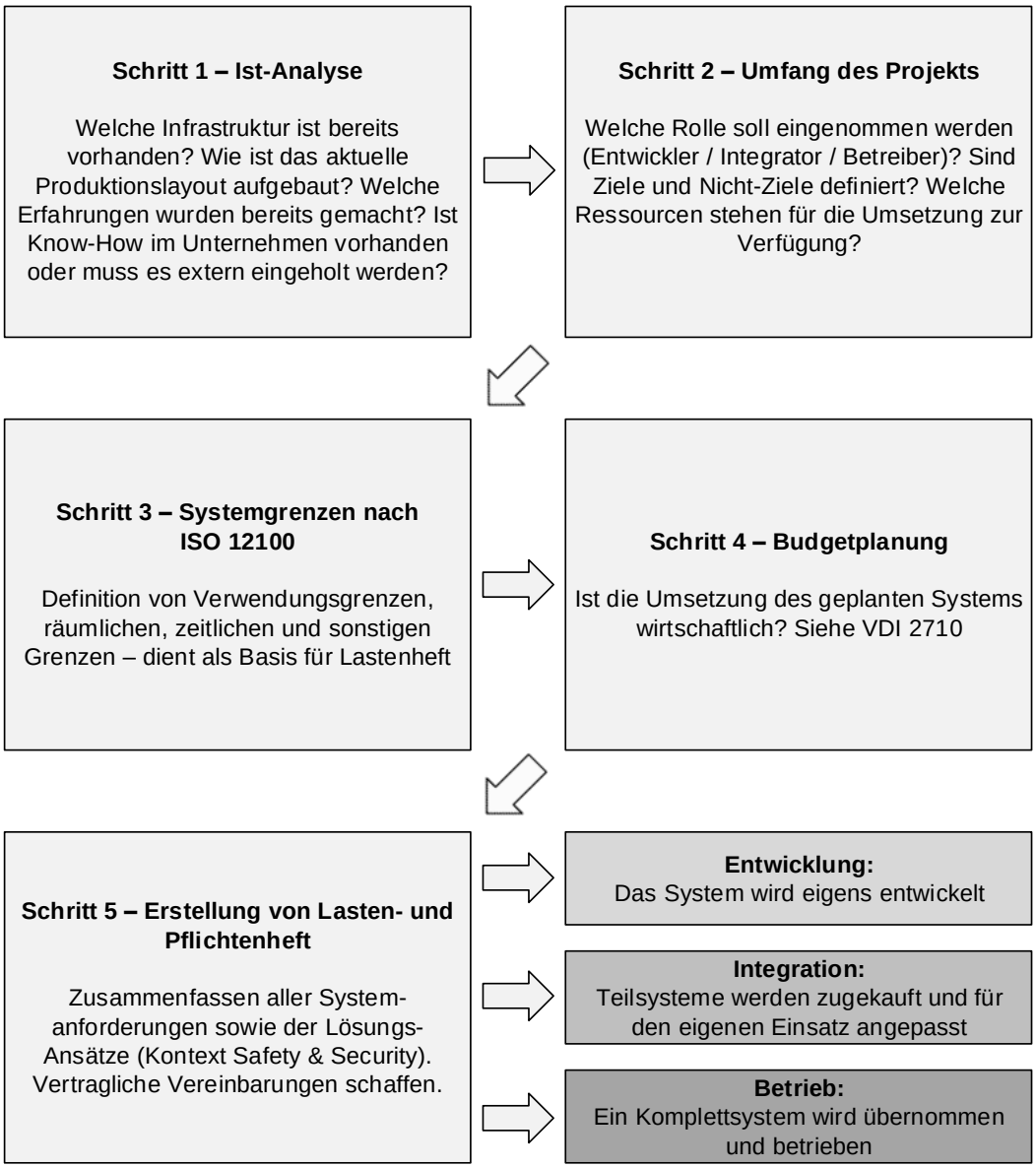


Abbildung 3: Ablauf der Anforderungsdefinitonen

2.1 Ist-Zustand und Festlegen der Systemgrenzen

Bevor mit der Auslegung von Systemen und Anlagen begonnen wird, sollte im ersten Schritt der Ist-Stand erhoben werden. Hierzu zählen Angaben zur Neuplanung oder Modernisierung der Anlage, zu vorhandenem Know-How im Unternehmen, sowie zu bereits eingenommenen Rollen und inwiefern diese im weiteren Verlauf berücksichtigt werden. Zusätzlich sollten bestehende Prozesse evaluiert und gegebenenfalls erneuert werden. In diesem Schritt wird auch festgelegt, welche (obligatorischen) Vorgaben bzw. EG- und EU-Richtlinien (Maschinenrichtlinie, EMV-Richtlinie etc.) für die Applikation Gültigkeit haben und welche Normen angewandt werden sollten, um die Anforderungen erfüllen zu können. Sobald die Rahmenbedingungen für die Implementierung von mobilen Robotern in die Produktion fixiert wurden, kann mit der Definition des eigentlichen Projektumfangs begonnen werden (Schritt 2). Hier wird eine Liste an Zielen und Nicht-Zielen (Scope) erstellt und erste konkrete Details zu Arbeitsschritten und der Zeitspanne spezifiziert. Weiters sollte eine erste grobe Budget-Überschlagsrechnung durchgeführt und die Ressourcenverfügbarkeit geprüft werden. Die Spezifikation der Systemgrenzen (Schritt 3) ist notwendig, um im Hinblick auf die Erstellung von Lasten- und Pflichtenheft eine klare Ausgangsbasis für notwendige Anforderungen und unerwünschte Bedingungen des Systems und dessen Umgebung zu schaffen.

Festlegen der Grenzen der Maschine nach ÖNORM EN ISO 12100:2013 [6]:

- **Verwendungsgrenzen:** bestimmungsgemäße Verwendung, Betriebsarten, Eingriffsmöglichkeiten der BenutzerInnen, vorhersehbare Fehlanwendungen
- **Räumliche Grenzen:** Systemlayout (Fahrwege, Fluchtwege, Arbeitsstationen etc.), Systemumgebungsbedingungen (Bodenbeschaffenheit, Fluchtwegkonzepte etc.), Infrastruktur (Anzahl der Stationen, Lademöglichkeiten, Leitsystem etc.)
- **Zeitliche Grenzen:** Lebensdauer, Wartungs- und Prüfintervalle
- **Weitere Grenzen:** Eigenschaften des Transportguts (Material, Flüssigkeiten, Last, Übergabeschnittstelle etc.), Umweltbedingungen (Indoor, Outdoor, Reinraum, explosionsgefährdete Umgebungen etc.)

2.2 Budgetplanung

Bei allen Investitionsprojekten legt das zur Verfügung stehende Budget den Umfang und die Reichweite der Umsetzung fest. Bereits vorhandene Infrastruktur, zu transportierende Güter und angestrebte Produktivitäts- und Effizienzkennwerte nehmen starken Einfluss auf die benötigte Anzahl an mobilen Robotern und damit auf die anfallenden Kosten. Eine detaillierte Kalkulation in Form einer Wirtschaftlichkeitsanalyse (Schritt 4) ist somit notwendig und eine Simulation der Produktionsprozesse, des Materialflusses und der logistischen Abläufe ein guter Anhaltspunkt, um eine optimale Lösung für die individuellen Bedürfnisse des Unternehmens zu finden. Zusätzliche Aufwände für eingesetzte Sensorik, das übergeordnete Leitsystem, sowie Wartungs- und Reparatur-dienstleistungen müssen frühzeitig in die Budgetplanung mit einfließen [7]. Neben klassischen Planungskennzahlen wie Return on Investment (ROI) und Total Cost of Ownership (TCO), stellt das Blatt 4 der VDI 2710 zur Durchführung einer Analyse der Wirtschaftlichkeit von FTS einen sinnvollen Ausgangspunkt dar.

2.3 Miteinbeziehen der Stakeholder

Eine zentrale Voraussetzung für die erfolgreiche Abwicklung von komplexen Projekten ist die frühzeitige Abstimmung mit allen Projektbeteiligten. Rahmenbedingungen, Grenzen und Ziele des Systems sollten von Anfang an klar dargelegt und abgestimmt werden, um eine niederschwellige Durchführung späterer Projektphasen zu gewährleisten. Es empfiehlt sich die Erstellung eines Lasten- (Betreiber, Integrator) bzw. Pflichtenhefts (Hersteller, Integrator) zur vertraglichen Festlegung von Anforderungen und Abhängigkeiten (siehe Abbildung 3 Schritt 5). Besonders für die Festlegung der funktionalen Anforderungen werden die bereits erarbeiteten Punkte der Ist-Analyse, der Beschreibung der Aufgabenstellung und der Systemgrenzenanalyse benötigt. Hinzu kommen noch die von dem/der ErstellerIn erwarteten Abnahmekriterien.

Schon bei der Anforderungsdefinition im Lastenheft sollte das Zusammenspiel von Safety und Security berücksichtigt werden, da (zu) späte Änderungen in erhöhtem finanziellen Aufwand resultieren können. Besonders im Hinblick auf Security sollte von Beginn an ein Ansatz verfolgt werden, der eine im Verhältnis zum ermittelten Risiko akzeptable Gesamtsicherheit zum Ziel hat.

Letztendlich sind auch organisatorische Rahmenbedingungen und etwaige Zuständigkeiten und Verantwortungen zu klären. Einerseits sind die terminlichen Ziele festzulegen, andererseits ist die Abnahme des Systems klar zu definieren (Validierungsprozess). Der Hersteller definiert während des Entwicklungsprozesses etwaige organisatorische Maßnahmen um Umgang mit dem System (Tragen von Schutzausrüstung, optische bzw. akustische Signale etc.). Der Betreiber ist in der Regel jedoch für die Umsetzung und Kontrolle jener Maßnahmen verantwortlich [8].

Derartige Verantwortungsverhältnisse (inkl. aller Servicevereinbarungen wie Wartungsintervalle etc.) sollten ebenfalls frühzeitig vertraglich festgehalten und abgegrenzt werden. Im Falle der Abnahme des Systems durch eine notifizierte Stelle[1], sollte bereits ab der Planungsphase laufender Kontakt zu jener Institution gehalten werden.

Basierend auf der Ausarbeitung der Anforderungen kann im nächsten Schritt ein mobiler Roboter - je nach Rolle - entwickelt, integriert oder betrieben werden. Die Abschnitte 3 bis 5 geben hier einen Überblick.

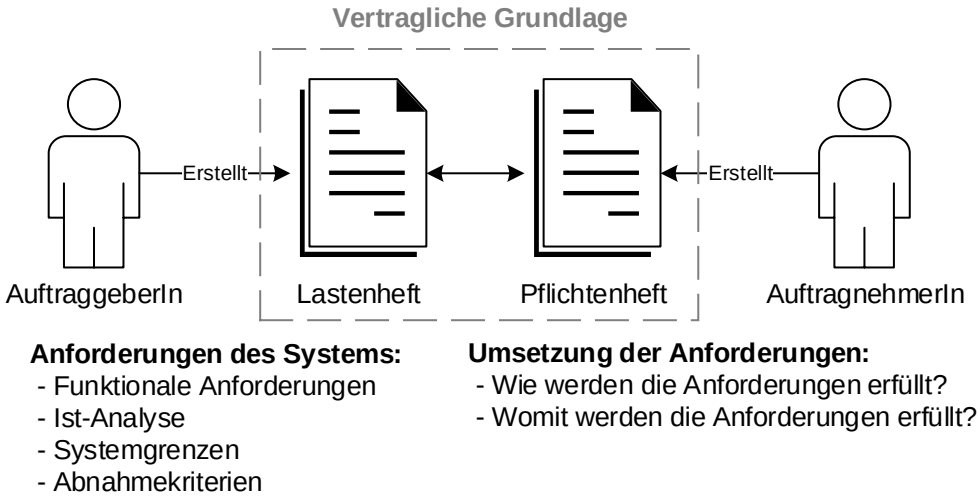


Abbildung 4: Erstellung von Lasten- und Pflichtenheft

[1] https://ec.europa.eu/growth/tools-databases/nando/

3 Entwicklung

Basierend auf der beschriebenen Entwicklungsmethodik aus Abbildung 5, thematisiert dieses Kapitel in erster Linie die Schritte des domänenübergreifenden Systementwurfs und des domänenspezifischen Entwurfs (Mechanik, Elektronik und Informatik). Anschließend wird die Integration der einzelnen Domänen in ein Gesamtprodukt behandelt, wobei kontinuierliche Schritte wie eine Risikoanalyse und die daraus resultierende Schnittstelle zwischen Safety und Security begleitend behandelt werden.

Um ein System sicher in Bezug auf Safety und Security auszulegen, ist es notwendig, ein funktionierendes Zusammenspiel beider aufrechtzuerhalten, ohne Konflikte zu erzeugen (z.B. hat Integrität im Hinblick auf Safety die höchste Priorität - Security priorisiert hingegen Vertraulichkeit [1]). Daher muss bei der Entwicklung besonderes Augenmerk auf die zentralen Bereiche der Industrie (Automatisierungstechnik, funktionale Sicherheit, Informations- und Kommunikationstechnik sowie Informationssicherheit) gelegt werden.

3.1 Systementwurf

Ein mobiler Roboter innerhalb einer automatisierten Fabrik beinhaltet komplexe Funktionen und eine Vielzahl an Systemelementen.

Für die Entwicklung eines solchen Systems müssen nun die verschiedenen Komponenten definiert und konzipiert werden, wobei hier eine Unterscheidung zwischen Funktion und Struktur getroffen werden kann. Auf der einen Seite werden durch die Funktionsgrößen alle wichtigen Elemente des Systems festgelegt und diese üblicherweise im Pflichtenheft definiert - sie dienen der späteren Verifizierung des Systems. Auf der anderen Seite werden Strukturelemente basierend auf jenen Funktionsgrößen entwickelt und konstruiert.

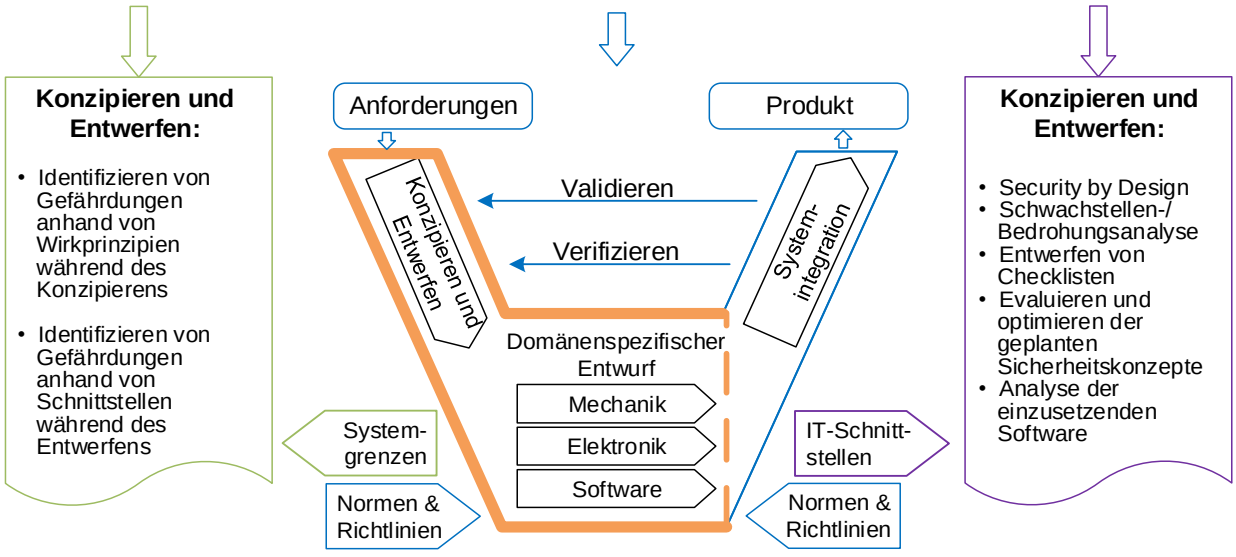


Abbildung 5: Konzeptbezogene Entwicklungsmethodik auf Basis des V-Modells

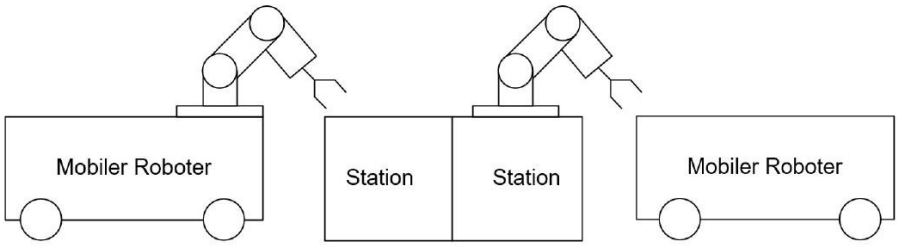
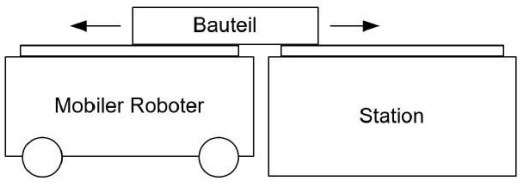
Die bereits festgelegten Funktionen sind hierbei häufig nur grob definiert und sollten durch verschiedene Teilfunktionen genauer spezifiziert werden. Eine Liste möglicher Teilfunktionen und Anforderungen für ein FTS findet sich in der ÖNORM EN ISO 3691-4:2020 [9] und kann als Anhaltspunkt für die Entwicklung eines mobilen Roboters herangezogen werden. Zusätzlich ist eine sinngemäße Anwendung der EN ISO 10218 [10, 11] die Sicherheitsanforderungen von Industrierobotern behandelt, zu empfehlen.

Da die hier erwähnten verschiedenen Normen unterschiedliche Eingrenzungen und Anwendungsbereiche aufweisen, muss im Zuge der Risikobeurteilung eine vollumfängliche Erkennung aller Gefahren sichergestellt werden. Als Beispiel für mangelnde Anwendbarkeit: In der ISO 3691-4:2020 werden keine Gefahren im Zusammenhang mit dem Betrieb mobiler Robotik in öffentlichen Bereichen behandelt [9].

Im Zuge des Systementwurfs ist ebenfalls bereits die Integration in die finale Betriebsumgebung zu berücksichtigen. Im Fall eines mobilen Roboters bzw. Transportsystems haben die physischen Schnittstellen und die Methode der Lasthandhabung zentrale Bedeutung. Ein System zur Manipulation von Bauteilen (z.B. Knickarmroboter) kann unterschiedlich genutzt werden, woraus wiederum unterschiedliche Anforderungen an die Schnittstellen entstehen. Wird bspw. ein Leichtbauroboter auf einem mobilen Transportfahrzeug integriert, spricht man von einem mobilen Manipulator (siehe Abbildung 12).

Auf Basis der zu transportierenden Güter müssen frühzeitig alle relevanten (Sub-)Prozesse sowohl am mobilen Roboter als auch an der angefahrenen Station, an der das Transportgut auf- bzw. abgeladen wird, berücksichtigt und entsprechende Entscheidungen getroffen werden. Tabelle 1 veranschaulicht unterschiedliche Varianten der Lasthandhabung.

Tabelle 1: Übliche Lasthandhabungen

Manipulator am mobilen Roboter:	**Manipulator an der Station:**
	
+ Flexibilität - erhöhte Sicherheitsanforderungen	- Flexibilität + einfachere Auslegung des Systems
Bauteilübergabe ohne Manipulator:	
	
- Flexibilität + Wirtschaftlichkeit	

3.2 Domänenspezifischer und -übergreifender Entwurf

Nachdem die Systemfunktionen nun im vorherigen Kapitel in diverse Teilfunktionen unterteilt und physikalischen Prinzipien (mechanisch, elektrisch, magnetisch, thermisch, optisch etc.) zugeteilt wurden, können sie in einer der drei Domänen (Mechanik, Elektronik, Informatik) entwickelt werden. Dies hat den Vorteil, dass sich ExpertInnen der einzelnen Domänen auf konkrete Teilfunktionen fokussieren und detailliertere sowie hochwertigere Auslegungen durchführen können.

Interdisziplinäre Absprache und regelmäßiger Austausch sind zentraler Bestandteil einer erfolgreichen und effizienten Projektdurchführung und sollten durch alle Phasen hinweg durchgezogen werden. Die Schnittstellen zwischen den einzelnen Domänen müssen nun exakt definiert werden, um in der späteren Kombination und Zusammensetzung des Endprodukts auf eine klare Verantwortungsstruktur und Aufgabenverteilung zurückgreifen zu können.

Bei der Definition der Eigenschaften blieb im Zuge der domänenspezifischen Entwicklung noch Interpretationsspielraum offen, der jetzt im domänenübergreifenden Entwurf geschlossen wird, indem finale Systemwerte und anzuschaffende Bauteile definiert werden. Dies ermöglicht eine optimale Abstimmung der Schnittstellen beim Zusammenführen der einzelnen Domänen. Welche Komponenten hier miteinander kombiniert werden, wurde beim Festlegen der Funktionsweise definiert, jedoch wird erst in dieser Phase die endgültige Gestaltung abgeschlossen und die Kombination der einzelnen Teilsysteme (mechanische Konstruktion, Sensorsystem etc.) durchgeführt. Für die darauffolgende Validierung der funktionalen Sicherheit wird innerhalb der EN ISO 13849-2 ein Validierungsprozess vorgegeben, der so früh wie möglich gestartet und auch parallel zum Entwurfsprozess von einer unabhängigen Person durchgeführt werden soll [12].

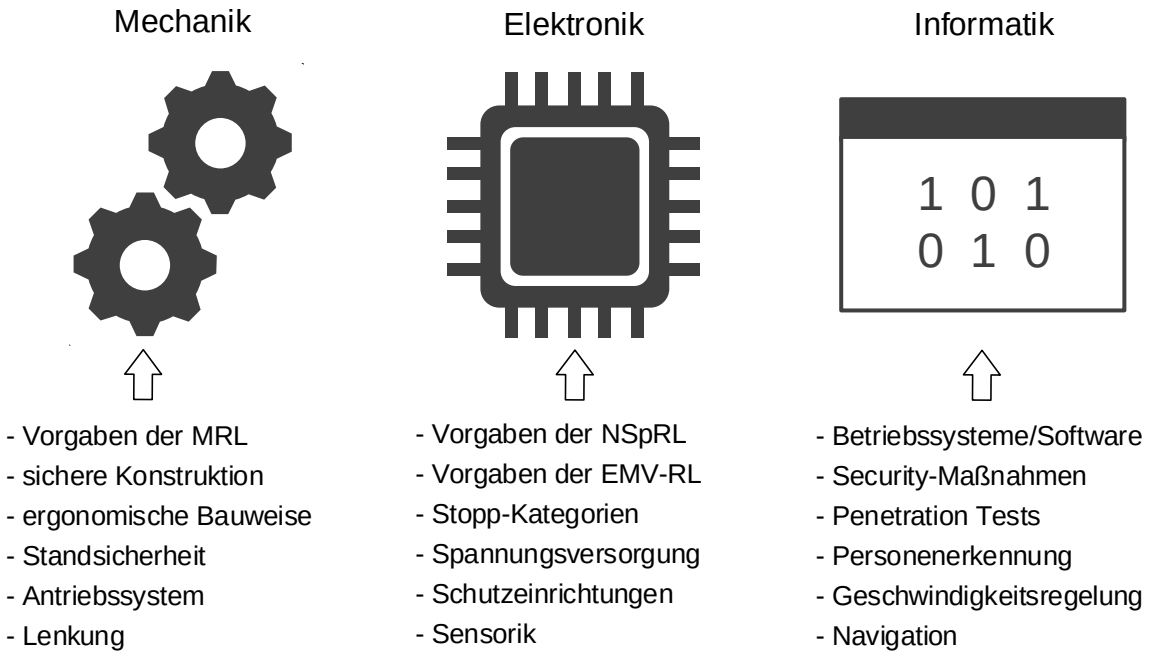


Abbildung 6: Auswahl an für domänenübergreifenden Entwurf relevanten Aspekten

3.3 Normenlage und regulatorische Rahmenbedingungen

Neben Anforderungen, die sich aus Lasten- und Pflichtenheft ergeben, kommen auch regulatorische Rahmenbedingungen zur Anwendung. EU- bzw. EG-Richtlinien, die auf Basis des Art. 14 des Vertrags über die Arbeitsweise der EU entstanden sind und als Produktvorschriften dienen, müssen von allen EU-Mitgliedstaaten in nationale Gesetze umgesetzt werden. Primär relevant für die Entwicklung eines mobilen Roboters in Österreich sind hierbei die Maschinen-Sicherheitsverordnung [13], die Niederspannungsgeräteverordnung [14], die elektromagnetische Verträglichkeitsverordnung [15], sowie das Funkanlagen-Marktüberwachungs-Gesetz [16]. Zu beachten gilt, dass weitere Verordnungen je nach Anwendungsfall ebenfalls zutreffend sein können. Hierfür steht ein Online-Tool[1] der Wirtschaftskammer Österreich zur Verfügung.

Die Einhaltung von Normen ist nicht verpflichtend, jedoch bietet sie eine Möglichkeit die Entwicklung nach einigermaßen aktuellen technischen Vorgehensweisen durchzuführen. Harmonisierte Normen dienen der Erfüllung der grundlegenden durch die EU- bzw. EG-Richtlinie gestellten Anforderungen und haben besonderen Stellenwert, da deren Einhaltung die Konformität mit der zugrundeliegenden Richtlinie vermuten lässt. Im Fall der Maschinenrichtlinie (2006/42/EG) gilt dies nur, wenn die zu entwickelnde Maschine vollständig im Anwendungsbereich der Norm(en) liegt und alle grundlegenden Sicherheits- und Gesundheitsschutzanforderungen behandelt werden [17]. Zu den harmonisierten und für mobile Roboter anwendbaren Normen zählen unter anderem die ÖNORM EN ISO 12100:2013 [6], die ÖNORM EN ISO 13849-1:2016 [18] sowie die OVE EN 62061:2016 [19].

Eine Auflistung aller harmonisierten Normen, die EU- und EG-Richtlinien selbst, sowie etwaige Änderungen und Aktualisierungen von Durchführungsbeschlüssen, sind im Rechtsinformationssystem der EU[2] abrufbar. Darauf aufbauend finden sich im deutschsprachigen Raum sogenannte Richtlinien (nicht zu verwechseln mit indirekt obligatorischen EU- bzw. EG-Richtlinien) vom Verein Deutscher Ingenieure (VDI). Diese müssen für die Abnahme eines Systems ebenfalls nicht zwingend eingehalten werden, liefern jedoch ausführliche Hilfestellung und Vorschläge für zusätzliche Maßnahmen.

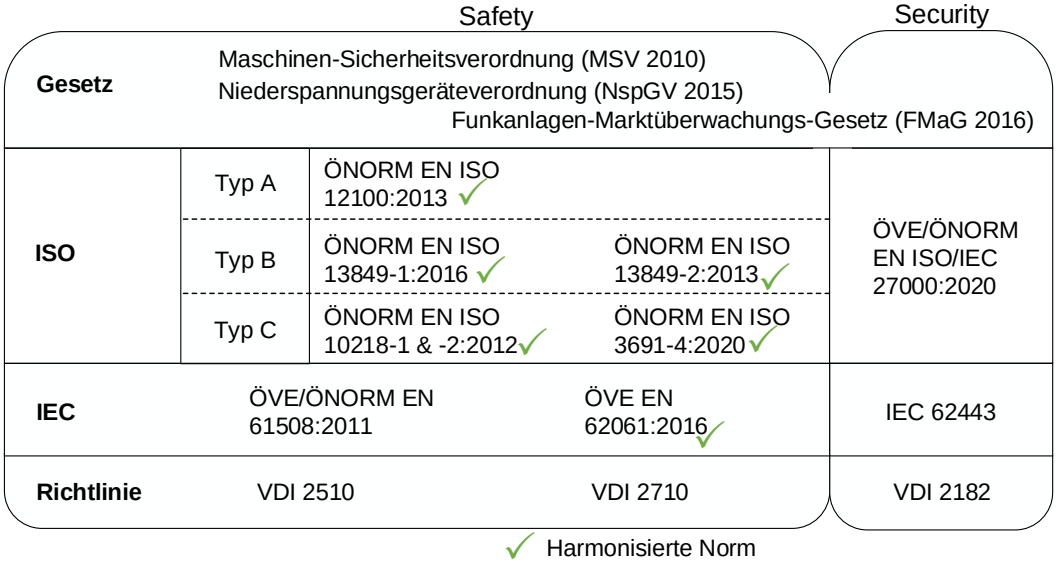


Abbildung 7: Auswahl aktuell (in Österreich) relevanter Gesetze, Normen und Richtlinien zur Entwicklung eines mobilen Roboters (in Anlehnung an [20])

[1] https://eur-lex.europa.eu/

[2] https://www.wko.at/service/innovation-technologie-digitalisierung/ist-ihr-produkt-ce-kennzeichnungspflichtig.html

Mobile Roboter können sehr unterschiedlich ausgelegt werden. Daher sind nicht immer alle hier angeführten regulatorischen Rahmenbedingungen relevant. Die Prüfung auf anzuwendende Gesetze, Normen oder Richtlinien muss für jedes System bzw. Implementierung individuell durchgeführt werden. Die harmonisierte ÖNORM EN ISO 3691-4:2020 [9] wird an dieser Stelle für die Entwicklung besonders hervorgehoben, da sie spezielle Anforderungen an ein FTS bzw. einen AMR stellt.

Zur Maschinenrichtlinie harmonisierte Normen lassen sich in drei Kategorien unterteilen: Fachnormen bzw. Maschinensicherheitsnormen (Typ-C) legen konkrete Sicherheitsanforderungen für eine bestimmte Maschine bzw. Maschinengruppe dar und verweisen üblicherweise häufig auf übergeordnete Sicherheits-Grundnormen (Typ-A) und Sicherheits-Gruppennormen (Typ-B). Weichen Festlegungen einer Typ-C-Norm von anderen Anforderungen ab, ist immer die Anwendung der Typ-C-Norm, aufgrund ihres spezifischen Anwendungsgebiets, zu bevorzugen [21].

Dementsprechend kann ebenfalls nur bei anwendbaren Typ-C-Normen die Konformität (bezogen auf die Maschinenrichtlinie) uneingeschränkt vermutet werden. Abbildung 8 zeigt die empfohlene Vorgehensweise zur Anwendung von Typ-B- und Typ-C-Normen auf Basis der ISO TR 22100.

Neben den grundlegenden Gestaltungsregeln, dem Zusammenbau angepasster Bauteile mit detaillierten Fertigungsparametern, sowie der Validierung, umfasst der letzte Schritt der Entwicklung auch die umfassende Dokumentation unter anderem in Form von Schaltplänen und Benutzungshandbüchern. Diese Dokumente werden für den Systemintegrator und Betreiber erstellt, sodass die sichere Benutzung und Wartung des Systems gewährleistet ist und auf die eventuell vorhandenen Restrisiken hingewiesen werden kann. Kennzeichnungen von Systemkomponenten, die ein potenzielles Risiko für den Betrieb darstellen, müssen sicht- und wahrnehmbar angebracht sein [6, 13]. Darüber hinaus ist die Durchführung regelmäßiger Bedrohungsanalysen sowie die Bereitstellung von Updates und proaktiven Informationen zu Sicherheitslücken empfehlenswert.

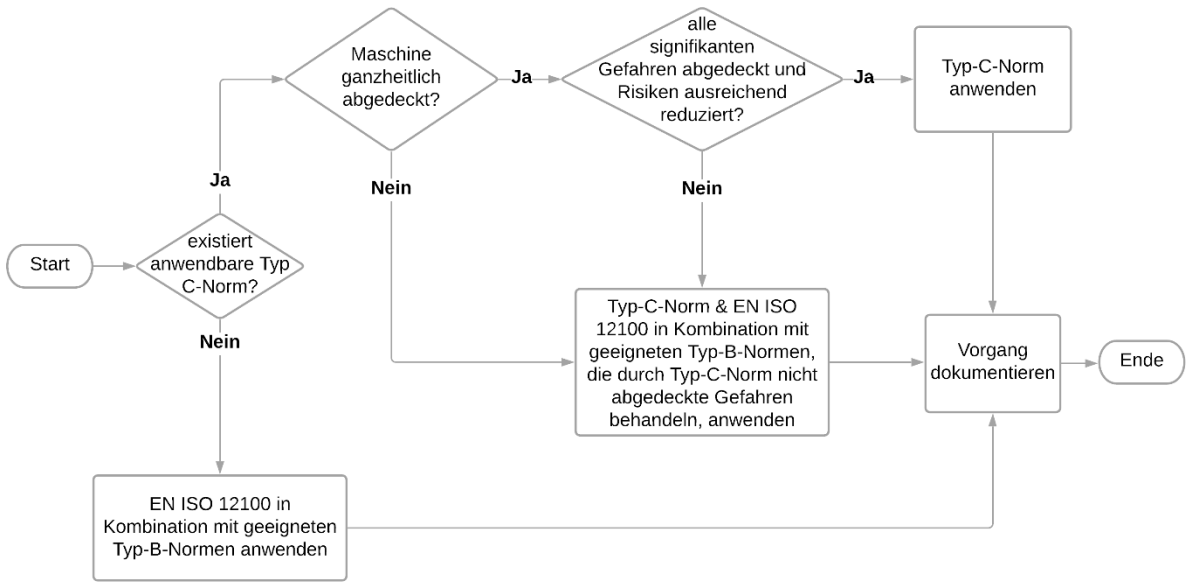


Abbildung 8: Empfohlene Schritte bei der praktischen Anwendung der ISO 12100 und bestehender Typ-B- und Typ-C-Normen innerhalb des Systems (modifiziert übernommen aus [21])

3.4 Risikoanalyse als begleitender Prozess

Für den Betrieb von Maschinen und Anlagen ist die Durchführung einer Risikoanalyse laut Maschinenrichtlinie 2006/42/EG verpflichtend [13].

Das Hauptaugenmerk einer Risikoanalyse in der Entwicklungsphase liegt vorrangig auf Safety, da damit einhergehende (physische) Sicherheitsaspekte mit Entwicklungsende vollständig bekannt und festgelegt sind. Sicherheitsaspekte in Bezug auf Security, unterliegen hingegen laufenden Veränderungen und müssen dementsprechend bis zur Außerbetriebsetzung des Systems regelmäßig und iterativ behandelt werden.

In einem Whitepaper des TÜV AUSTRIA in Kooperation mit Fraunhofer Austria Research [22] wurde ein strukturierter Ablauf der integrierten Beurteilung von Safety- und Security-Risiken vorgestellt (siehe Abbildung 9).

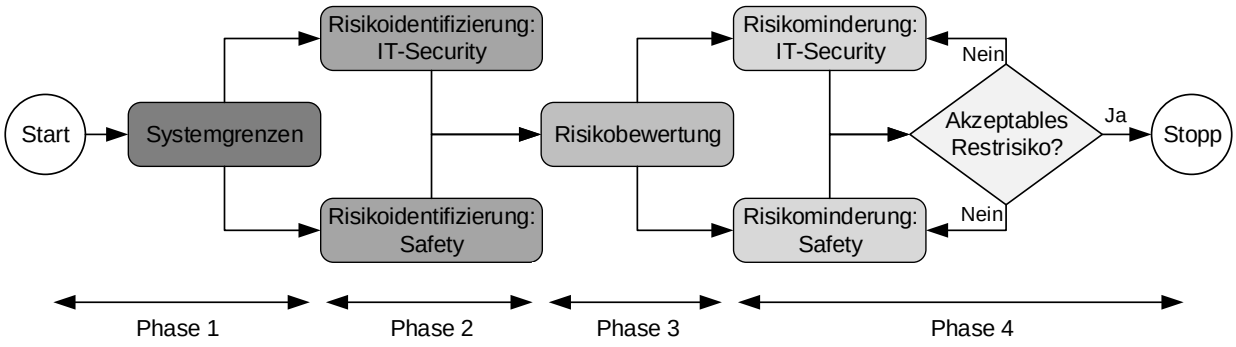


Abbildung 9: Strukturierter Ablauf der integrierten Beurteilung von Safety- und Security-Risiken (in Anlehnung an [22])

Im Zuge der Risikoanalyse werden, aufbauend auf den bereits im Lasten- und Pflichtenheft festgelegten Systemgrenzen, alle Risiken und potentiellen Gefahrenquellen identifiziert und anschließend mit einer übergreifenden Methodik bewertet. Für steuerungsbezogene Maßnahmen eignet sich die Anwendung des Performance Level (PL) der ISO 13849 sowie des Safety Integrity Level (SIL) der IEC 61508. Innerhalb der ISO 3691-4 wird unter anderem auf besondere Anforderungen im Zuge der Risikobeurteilung (z.B. erforderliche PL, Spaltmaße) eingegangen.

Alle Risiken über einem akzeptablen Schwellwert müssen grundsätzlich nach folgender Hierarchie gemindert werden [6]:

1. Konstruktive Maßnahmen
2. Technische Maßnahmen
3. Organisatorische Maßnahmen

Für **konstruktive Maßnahmen** an einem mobilen Roboter bietet sich vor allem die Reduktion von spitzen und scharfen Ecken bzw. Kanten sowie potenziellen Quetsch- und Einzugsstellen zwischen Rädern und Bodenfläche, in denen sich bspw. Kleidung verfangen könnte, an.

Technische Maßnahmen umfassen bspw. die Ausstattung und Erweiterung zusätzlicher Sicherheitssensorik (z.B. Laserscanner, haptische Bumper) und Kombinationen daraus.

Unter **organisatorische Maßnahmen** fallen u.a. Schulung und Weiterbildung von Personal, Arbeitsanweisungen (z.B. Tragen von Helm oder Sicherheitsschuhen), umfassende Nutzungsinformationen (Betriebsanleitung inkl. Restrisiken, Warnhinweise etc.), sowie den Betriebsablauf betreffende Maßnahmen (z.B. optische oder akustische Warnsignale).

3.5 Frühzeitige Betrachtung von Security-Aspekten

Die verknüpfende Betrachtung von Safety- und Security-Aspekten in der Planungsphase und Systementwicklung ist essenziell, da ein einseitiger Fokus in späteren Projektphasen in drastisch gesteigerten finanziellen und zeitlichen Aufwänden resultieren kann. Nachfolgend wird eine Auswahl an Security-Konzepten und Nachschlagewerken beschrieben, die sich für eine übergreifende Betrachtung eignen.

Vorgehensmodell der VDI 2182 [3]:
Dieses Modell sieht einen zyklischen Ablauf (Identifizieren, Bewerten, Auswählen und Umsetzen von Schutzmaßnahmen) vor, welcher über den gesamten Lebenszyklus der Anlage aufrechterhalten werden sollte. Das Modell kann sowohl auf bereits bestehende als auch in der Planung befindliche Anlagen sowie auf unterschiedliche Rollen angewandt werden.

ISO/TR 22100-4 [23]:
Diese technische Regel beschäftigt sich mit dem Zusammenhang von Maschinensicherheit aus Hersteller-Perspektive und der zentralen Norm der Risikoanalyse: die ISO 12100:2013. In Teil 4 wird speziell auf IT-Security-Aspekte eingegangen, die sich auf die physische Sicherheit von Maschinen auswirken können.

IEC 62443:
Die IEC/TS 62443-1-1:2009 [1] definiert Sicherheitsanforderungen an Produkte oder Systeme und teilt sie in vier Ebenen, den sog. Security Level (siehe Abbildung 10), ein. Insbesondere die Teile 4-1:2018 [24] und 4-2:2019 [25] richten sich an Hersteller bzw. Entwickler von Komponenten und Systemen. Für die eigene Anwendung muss spezifiziert werden, mit welchen Angriffen gerechnet werden muss, um dementsprechend das System auszulegen. Die Einstufung des SL hängt von der Komplexität der Bedrohung bzw. von der Kritikalität des Systems, der Zone, oder der Komponente ab. Des Weiteren wird das SL in seiner Betrachtungsweise unterteilt: Während der Hersteller das maximal zu erreichende Level angibt - Security Level-Capability (SL-C) - definiert der Betreiber ein notwendiges Ziellevel - Security Level-Target (SL-T). Das tatsächlich erreichte SL - Security Level-Achieved (SL-A) - kann durch den Integrator definiert werden, nachdem ein System feststeht und konfiguriert wurde. Der vom Hersteller angegebene SL-C setzt sich aus spezifischen technischen Anforderungen der IEC 62443-4-2:2019 zusammen und ist nur gültig unter der Voraussetzung, dass das System richtig eingesetzt und konfiguriert wird [26].

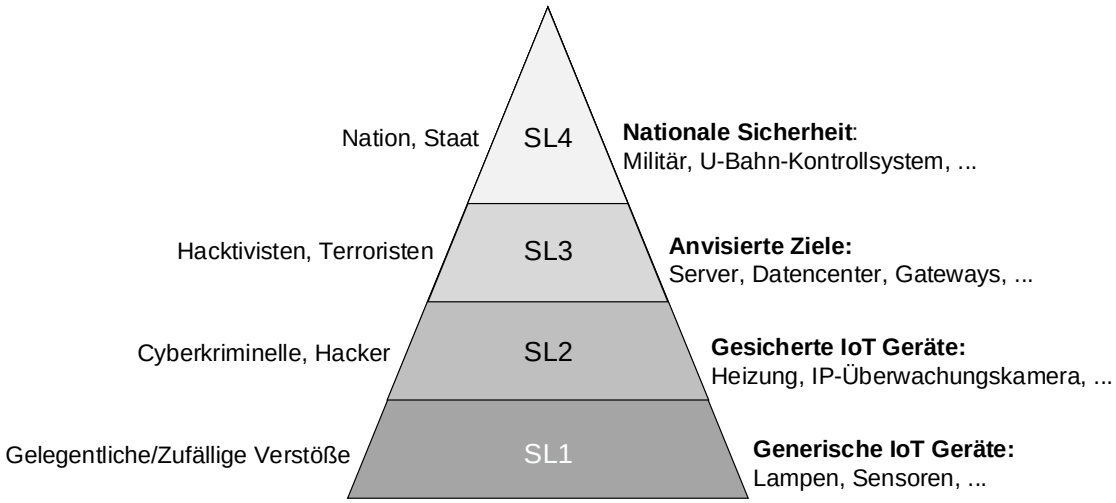


Abbildung 10: Hierarchie der Security-Levels nach IEC 62443

3.6 Ausstellen einer CE-Kennzeichnung

Die Kennzeichnung eines Produktes gemäß Verordnung (EG) Nr. 765/2008 ermöglicht Herstellern, die Einhaltung aller geltenden Anforderungen, Richtlinien und Verordnungen der Europäischen Union nach außen und leicht erkenntlich zu visualisieren. Unterstützung bei der Erstellung jener Konformitätserklärung bietet der „Blue Guide“ der Europäischen Kommission [27].

Wird ein mobiler Roboter bereits als vollständige Maschine angekauft und bestimmungsgemäß verwendet, ist keine erneute CE-Kennzeichnung notwendig. Wird jedoch jene Maschine z.B. über ihre bestimmungsgemäße Verwendung hinaus verändert oder erweitert - etwa durch einen Manipulator, der als unvollständige Maschine gilt - entsteht eine neue Maschine, die in ihrer Gesamtheit erneut auf die Erfüllung geltender Anforderungen geprüft und mit einem CE-Kennzeichen ausgestattet werden muss [28].

Wenn ein mobiler Roboter in eine Produktion und den Materialfluss einer Anlage eingebunden wird, liegt eine Verkettung von Maschinen vor. Hierbei ist zwischen einer geringfügigen und einer tiefgreifenden Verkettung zu unterscheiden:

Bei einer **geringfügigen Verkettung** werden Maschinen z.B. über den Materialfluss miteinander verbunden, verrichten jedoch selbständig und unabhängig voneinander ihre Arbeit.

Im Vergleich dazu spricht man von einer **tiefgreifenden Verkettung**, wenn mehrere Maschinen einen Gesamtkomplex bilden, worin Einzelmaschinen z.B. aufgrund einer gemeinsamen Logik nicht mehr separiert voneinander arbeiten und keine Einzelsteuerung der Instanzen vorgesehen bzw. möglich ist.

Weiterführende Informationen zu Austausch und Umbau von Maschinen im Kontext des ArbeitnehmerInnenschutzgesetzes sind unter [28] zu finden.

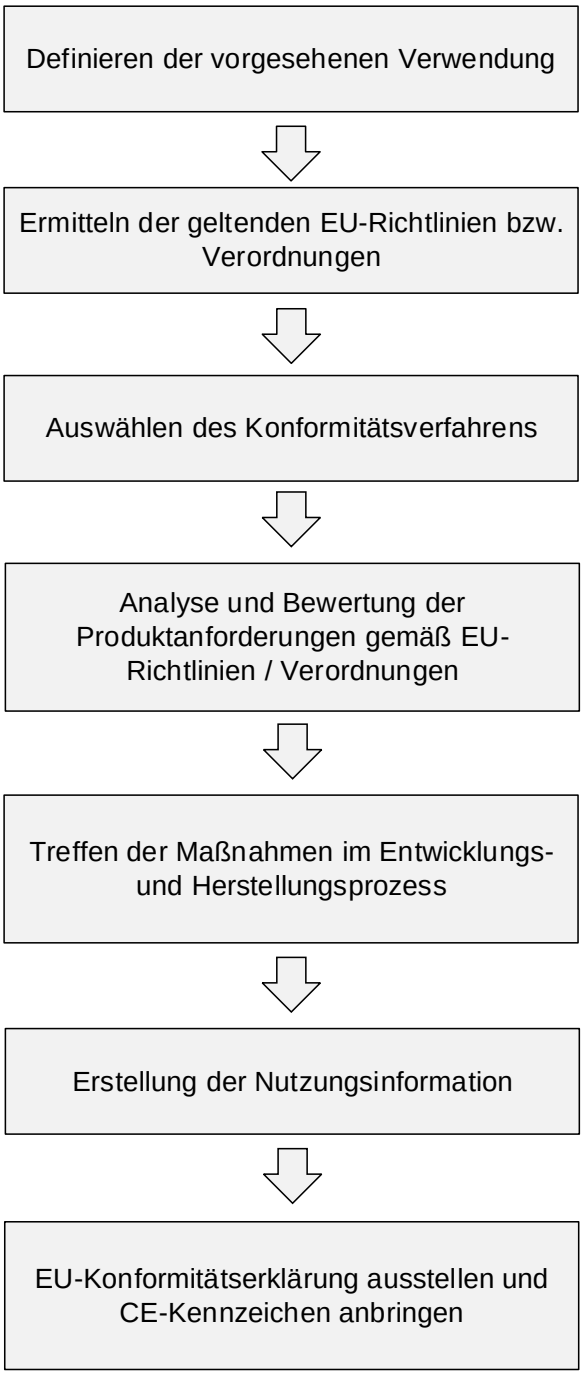


Abbildung 11: Die 7 Schritte zur CE-Kennzeichnung nach [29]

4 Integration

Die Integration behandelt die Eingliederung eines entweder im vorherigen Schritt entwickelten oder extern zugekauften Systems in die jeweilige Produktionsumgebung.

In diesem Schritt findet zumeist eine Verkettung fertig entwickelter und CE-zertifizierter Systeme statt, um spezielle Anforderungen der Produktionsumgebung erfüllen zu können. Wie in Abschnitt 3.6 beschrieben, kann eine solche Integration eine erneute CE-Kennzeichnung notwendig machen.

Die Ausstellung jener wandelt den Integrator zum Hersteller, da durch den Verbund ein neues Produkt in Verkehr gebracht wird. Darüber hinaus muss die bestimmungsgemäße und sichere Verwendung des Zusammenspiels aus mobilem Robotersystem und sonstigen Produktionsanlagen ebenfalls durch eine Risikoanalyse überprüft und ggf. aufbauende Maßnahmen getroffen werden. Es besteht die Möglichkeit, dass der ursprüngliche Hersteller die Einbindung des Produkts auf diese Weise bereits vorgesehen hat - somit wäre keine neue Prüfung und CE-Kennzeichnung notwendig.

4.1 Anpassungen an Umgebung oder mobilem Roboter

Der mobile Roboter selbst ist schon einer Risikoanalyse unterzogen und sicher entwickelt worden. Dessen Betriebsanleitung sollte ausreichend Information zu Anforderungen und Grenzen des sicheren Betriebs beinhalten und in jedem Fall berücksichtigt werden. Wird eine neuerliche Risikoanalyse und damit zusätzliche Maßnahmen aufgrund der eingangs beschriebenen Faktoren notwendig, können diese ebenfalls auf die Produktionsumgebung angewandt werden.

Konnte das ermittelte Risiko durch konstruktive Maßnahmen nicht ausreichend gemindert werden, stehen eine Reihe an technischen Maßnahmen zur Verfügung, die auch an die Betriebsumgebung angewandt werden können. Tabelle 2 und Tabelle 3 beinhalten einen Auszug gängiger Einrichtungen, mit denen die Betriebsumgebung erweitert bzw. ausgestattet werden kann.

Bei Sensorik wird seitens des Herstellers ein PL angegeben, das für die Steuerungsqualität der damit realisierten Sicherheitsfunktion ausschlaggebend ist. Zusätzliche Maßnahmen umfassen alle sonstigen Bestreben zur Gefahrenminimierung, Erhöhung der Produktivität oder Steigerung der MitarbeiterInnenakzeptanz.

Tabelle 2: typische Schutzeinrichtungen

Taktile Sensorik:
• drucksensitive Roboterhaut • Bumper • Türkontaktschalter • Druckempfindliche Matten
Optische Sensorik:
• Einstrahlsensor • Lichtvorhang • Laserscanner (LiDAR) • Kamerasystem

Sichere mobile Robotik durch sichere Umgebung
In diesem Zusammenhang kann es unter bestimmten Voraussetzungen wirtschaftlich und organisatorisch vorteilhaft sein, sich primär auf die sichere Gestaltung der Produktionsumgebung zu fokussieren. Komplexe Fertigungsprozesse mit einer Vielzahl an autonomen mobilen Robotern bzw. fahrerlosen Transportsystemen, können durch diese Herangehensweise effizienter gestaltet und erweitert werden.

Tabelle 3: Ergänzende Schutzeinrichtungen

Zusätzliche Maßnahmen:	
• Bodenmarkierungen • Spiegel • Kollisionswarnungen • Ultraschallsensoren	• Ampelsysteme • Tore • Sicherheitswesten • akustische Warnsignale

Stellt der Produktionsprozess spezielle Anforderungen, die von einem zugekauften mobilen Robotersystem nicht „out of the box“ erfüllt werden können, besteht die Möglichkeit der Erweiterung der Maschine (siehe Abschnitt 3.6). Ein gängiges Beispiel hierfür wäre die Kombination aus AMR und Manipulator (siehe Abbildung 12).

Ist eine derartige Kombination nicht bereits durch den Hersteller des mobilen Transportsystems vorgesehen, ist eine neue Risikobeurteilung und CE-Kennzeichnung der daraus resultierenden Maschine (ein Roboterarm gilt als unvollständige Maschine und hat dementsprechend keine CE-Kennzeichnung [13]) notwendig, wobei die individuellen Umgebungseigenschaften für den Einsatz berücksichtigt werden müssen.

Die Verantwortung für die sichere Integration liegt in diesem Fall somit beim Integrator. Besonders zu beachten sind in diesem Zusammenhang die Lastverteilung, Standsicherheit, Spannungsversorgung, sowie die Verkettung des Safety-Systems und der Steuerungen.

Häufige Gefährdungen, die während der Integrationsphase zu beachten sind, resultieren erfahrungsgemäß aus der Lastverteilung, der Standsicherheit und der Spannungsversorgung.

Weiters müssen die zusammengefügten Systeme, unter Berücksichtigung der funktionalen und Security-relevanten Anforderungen, sicherheitsrelevante Daten austauschen.

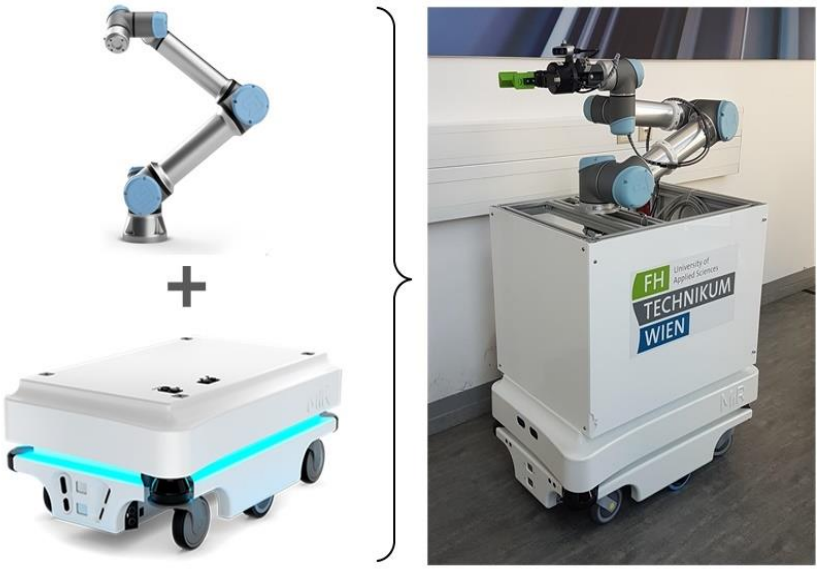


Abbildung 12: Kombination aus (kollaborativem) Industrieroboter[1] und mobilem Roboter[2] innerhalb der Technikum Digital Factory[3]

[1] https://www.universal-robots.com/de/produkte/ur5-roboter/
[2] https://www.mobile-industrial-robots.com/de/products/mir100/
[3] https://digitalfactory.technikum-wien.at/

4.2 Integration von Security-Funktionen

Sobald ein neues System integriert wird, sollte für dieses und die damit in Zusammenhang stehenden Systeme eine Security-bezogene Risikobeurteilung durchgeführt werden. Hier sind vor allem die Schnittstellen des Roboters und der bereits vorhandenen Produktionsanlage von Bedeutung. Während der Integrationsphase ist die begleitende Durchführung von Security-Audits, Penetration-Tests und Simulation von Angriffen empfehlenswert, um Sicherheitslücken frühzeitig zu erkennen und mit entsprechenden Maßnahmen entgegenwirken zu können.

Die Normenreihe IEC 62443 bzw. deren Teile 3-2 und 3-3 stellen unter anderem das Modell „**Zones and Conduits**“ vor, das auf dem Defense-in-Depth-Grundsatz beruht (siehe Abbildung 13). Hierbei wird das Netzwerk in verschiedene Zonen mit gleichen Sicherheitsanforderungen, Funktionen oder Standorten unterteilt, wobei sich anhand der bereits erstellten Risikoanalyse orientiert werden sollte. Des Weiteren empfiehlt sich die Separierung von sicherheitsrelevanten, temporär verbundenen, kabellosen und via externem Netzwerk verbundenen Komponenten gemäß IEC 62443-3-2:2020 [30].

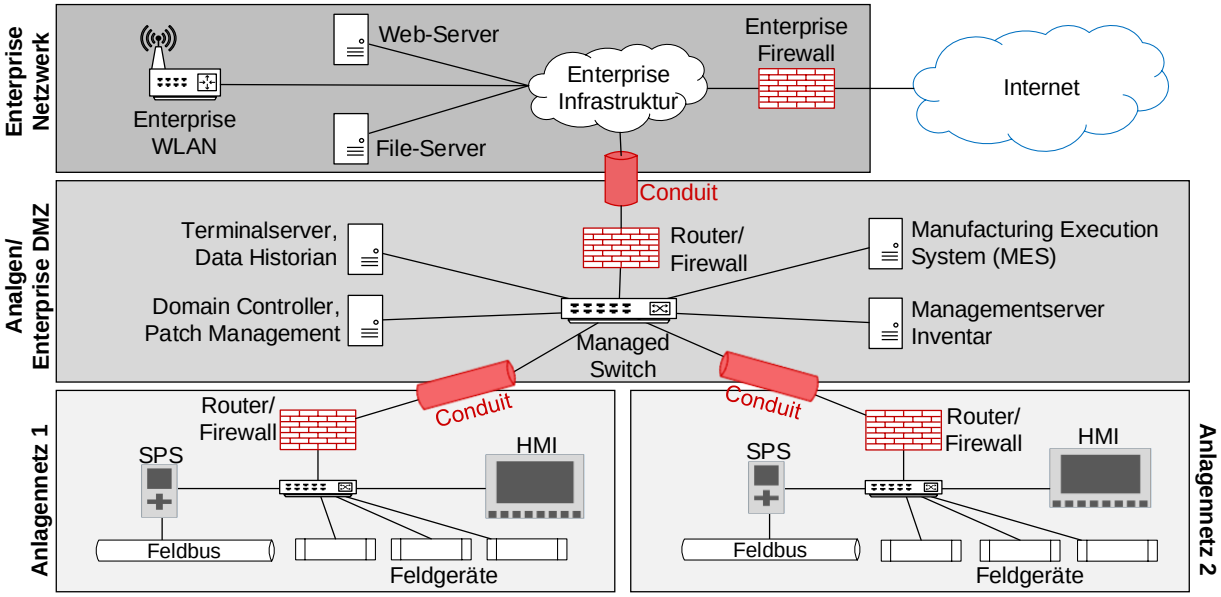


Abbildung 13: Beispielhafte Netzwerksegmentierung mit dem Zones-and-Conduits-Modell (modifiziert übernommen aus [31])

Grundlegende Anforderungen der IEC/TS 62443-1-1:2009 [1]:

- **Zugriffskontrolle:** Regelung der Nutzung und des Informationszugriffs
- **Nutzungskontrolle:** Überwachung der Nutzung und des Informationszugriffs zum Schutz vor unautorisiertem Betrieb bzw. Informationsverwendung
- **Datenintegrität:** Korrektheit und Unmodifiziertheit von Daten gewährleisten, um vor unautorisiertem Datenaustausch zu schützen
- **Datenvertraulichkeit:** Daten vor unautorisierten Personen oder Geräten schützen
- **eingeschränkter Datenfluss:** die Datenübertragung in Kanälen soweit einschränken, dass keine Informationen an unautorisierte Personen oder Geräte gelangen
- **schnelle Reaktion auf Ereignisse:** rechtzeitige Reaktion auf Verletzungen der IT-Security durch Benachrichtigung der zuständigen Stellen
- **Verfügbarkeit der Mittel und Ressourcen:** Sicherstellung der Verfügbarkeit (Vorbeugung gegen DoS-Attacken)

5 Betrieb

Mit der Inverkehrbringung, also der Ausstellung der Konformitätserklärung und Anbringung des CE-Kennzeichens bzw. des Typenschilds, kann mit dem tatsächlichen Betrieb begonnen werden. Jene Phase stellt einen durchgehenden Prozess bis zur Ausmusterung des Systems dar und weist somit im Normalfall die längste Dauer auf. Ungeachtet dessen, ob der mobile Roboter (ggf. samt Integrationsdienstleistung) extern zugekauft oder vom geplanten Betreiber selbst entwickelt wurde, sollte durch (Vor-)Abnahmen sichergestellt werden, dass alle Anforderungen erfüllt und Schnittstellen mit der vorhandenen Produktionsumgebung kompatibel sind.

Vor der Inbetriebnahme sollten insbesondere folgende Aspekte beachtet werden:

- Einhaltung formaler Voraussetzungen für die Inbetriebnahme (EG-Konformitätserklärung, Betriebsanleitung)
- Berücksichtigung des Standes der Technik (z.B. durch Einhaltung der aktuellen Normenlage)
- Ausreichendes Sicherheitskonzept (z.B. Arbeitsplatzevaluierung durch den Betreiber)
- Prüfung der Funktionsfähigkeit von Bedienelementen, Steuerungen, Schutzeinrichtungen, elektrischen/pneumatischen/hydraulischen Ausrüstungen entsprechend der Herstellerangaben
- Vorhandensein von Betriebsanweisungen (in allen relevanten Themenbereichen)

5.1 Anpassungen am abgenommenen System

Nachdem das System abgenommen und in Verkehr gebracht worden ist, dürfen keine Änderungen mehr an den domänenspezifischen Komponenten (Mechanik, Elektronik, Informatik), sowie dem Zusammenspiel jener und der Prozesse in der Produktionsumgebung vorgenommen werden. Sollten dennoch Anpassungen notwendig sein, ist zu evaluieren, ob ein Umbau nach ArbeitnehmerInnenschutzgesetz (§ 35 ASchG) oder lediglich ein simpler Austausch erforderlich ist. (siehe Abschnitt 3.6).

Bei einem Umbau gemäß § 35 ASchG handelt es sich um vom Hersteller nicht vorgesehene Änderungen am System bzw. um einen Austausch mit Komponenten anderer Hersteller - auch, wenn es sich hierbei z.B. um (in Bezug auf Sicherheit) höherwertigere handelt.

Dementsprechend wird eine neuerliche Gefahrenanalyse inkl. Setzung geeigneter Maßnahmen notwendig. Eine erneute CE-Kennzeichnung wird dann erforderlich, wenn z.B. eine tiefgreifende Verkettung vorliegt, wobei beteiligte Systeme ihren Einzelmaschinen-Charakter verlieren (siehe Abschnitt 2.1) [28].

Beispiele für Umbauten, die ein neuerliches Inverkehrbringen bedingen:

- der Einbau einer SPS mit erweiterter Funktionalität, die über die bestimmungs-gemäße Verwendung hinausgeht
- der Einbau eines anderen Antriebssystems z.B. mit mehr Leistung

Achtung: wird die Anlage oder der mobile Roboter dennoch durch den Betreiber umgebaut, wird ein Konformitätsbewertungsverfahren und ggf. eine neue Inverkehrbringung notwendig.

5.2 Safety im laufenden Betrieb

Aus Safety-Sicht wurden im Zuge der Entwicklung und Integration bereits alle Gefahren erkannt und behandelt, wobei konstruktive und technische Maßnahmen möglicherweise nicht alleinig ausreichen. Vorhandene Restrisiken müssen in der Betriebsanleitung angeführt und vom Betreiber adressiert werden. Hierfür eignen sich organisatorische Sicherheitsmaßnahmen, die zwar primär von Hersteller und Integrator erarbeitet wurden, jedoch vom Betreiber aktiv und laufend durchgesetzt werden müssen. Dazu zählen beispielsweise Schulung von Mitarbeitenden, ausreichende Kennzeichnung der Fahrwege des mobilen Roboters, Einrichtung von „Sperrzonen“ für Personen, Erstellung von Lage- und Übersichtsplänen oder die Anbringung diverser optischer oder akustischer Warnsignale. Darüber hinaus fällt die gesamte Instandhaltung und Reinigung laut Betriebsanleitung für den dauerhaften und einwandfreien Betrieb in die Verantwortung des Betreibers.

Für laufende Überprüfungen eignet sich die Abarbeitung und Protokollierung einer einheitlichen Checkliste. Anhang B kann hierbei als Ausgangspunkt dienen.

Ist ein Safety-Managementsystem vorhanden, können eigens auf die Anlage zugeschnittene Checklisten erstellt und Prüfaufträge verwaltet werden. Hierfür empfiehlt sich der Einsatz eines/einer Sicherheitsbeauftragten bzw. Sicherheitsvertrauensperson mit Verantwortlichkeit zur Umsetzung und Kontrolle von Maßnahmen bzw. Aufgaben sowie zur Schulung der Mitarbeitenden.

Typische Aufgabenbereiche umfassen:

- Information, Beratung und Unterstützung von Beschäftigten
- Vertretung der Interessen von ArbeitnehmerInnen im Safety-Kontext gegenüber Betrieb, Behörden oder sonstigen Stellen
- Beratung von Führungskräften zum Thema ArbeitnehmerInnenschutz
- Kontrolle von Schutzeinrichtungen und -vorkehrungen sowie Information des Betriebs bei bestehenden Mängeln
- Zusammenarbeit mit Sicherheits- und Arbeitsmedizin-Fachkräften

5.3 Security im laufenden Betrieb

Mit steigender Vernetzung von Produktionsanlagen und -umgebungen, dem zunehmenden Einsatz von IIoT-Lösungen und Internetanbindungen sowie der Aufrüstung klassischer Industriesteuerungen zu CPS, entsteht eine Flut an neuen Gefährdungslagen. Produktionsanlagen geraten somit zunehmend aus unterschiedlichen Motiven in den Fokus krimineller und illegitimer Vorhaben.

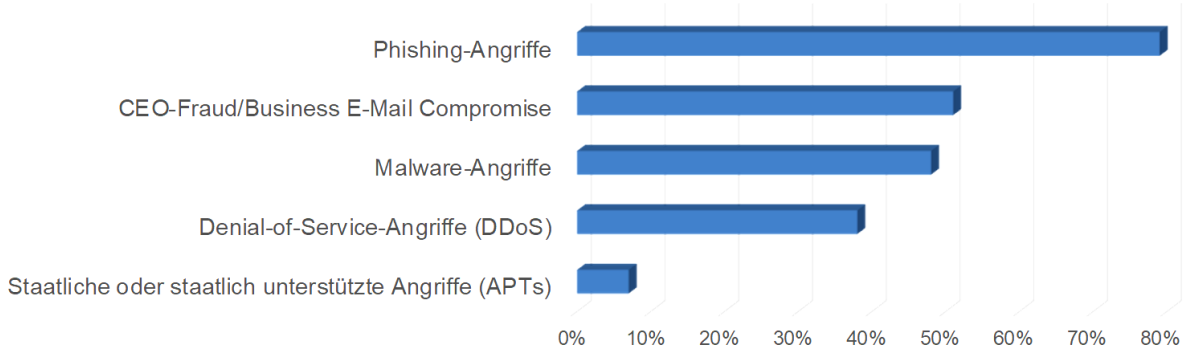


Abbildung 14: Häufigkeit von Cyberangriffen auf österreichische Unternehmen nach Art (2020) (modifiziert übernommen aus [32])

Abbildung 14 gibt einen Überblick über die häufigsten Angriffsarten auf österreichische Unternehmen. Durch den Einsatz grundlegender IT-Security-Maßnahmen (aktuelle Virenschutz-Software, Firewalls etc.), aufbauender Maßnahmen (Intrusion Detection & Alerting Systeme etc.) sowie die regelmäßige Schulung von Mitarbeitenden, kann ein Großteil der Angriffe abgewehrt werden.

Abbildung 15 zeigt das 5-stufige Security-Modell nach Robert M. Lee [33] zur strukturierten Einteilung von Maßnahmen, Kompetenzen und Ressourcen, wobei letzterer Punkt (Angriff) nur in den seltensten Fällen (kritische Infrastruktur, nationale Verteidigung etc.) zur Anwendung kommt.

- **Architektur:** Sicherheit ist durch die horizontale und vertikale Struktur des Unternehmensnetzwerks gegeben
- **passive Verteidigung**: Statische Systeme erkennen Angriffe und wehren diese ab
- **aktive Verteidigung**: Auf Security-Incidents wird mittels kontinuierlicher Analyse der Angriffsvektoren reagiert, um erneute Sicherheitsverletzungen zu vermeiden
- **Intelligence:** Protokollierung der Prozess- und Kommunikationsdaten mit kontinuierlicher Auswertung, um auftretende Anomalien zu erkennen
- **Angriff:** Legale (Gegen)Maßnahmen zur aktiven Selbstverteidigung

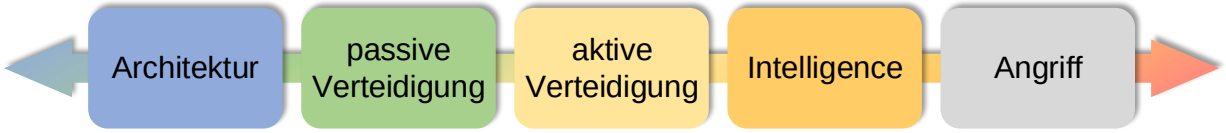


Abbildung 15: Sliding Scale of Cyber-Security (modifiziert übernommen aus [33])

Für die dauerhafte Aufrechterhaltung eines angebrachten Maßes an IT-Security und damit einhergehender Maßnahmen, existiert eine Reihe an nützlicher weiterführender Literatur. Das ICS-Security-Kompendium des deutschen Bundesamts für Sicherheit in der Informationstechnik liefert diverse Best Practice Guides zur Absicherung und sicheren Gestaltung von (Produktions)Netzwerken[1]. Zusätzlich sind Informationen zum Aufbau von Security Management Systemen sowie zur Vorgehensweise bei der Erstellung von diverser Dokumentation abrufbar.

Der Verein Industrie 4.0 Österreich bietet einen Leitfaden über den Schutz vor Cyberattacken in Produktionsbetrieben[2], der auch die gegenseitige Wechselwirkung zwischen Informations- und Maschinensicherheit berücksichtigt. Durch Praxisbeispiele soll ein Überblick über das Gefahrenpotential von unzureichendem Verständnis über Cyber-Security geschaffen werden.

Aus industrieller Sicht sollten die Vorgehensweisen aus den Teilen 2-1:2010 und 3-2:2020 der IEC 62443 berücksichtigt werden. Auf Unternehmensebene empfiehlt sich die Umsetzung eines Information Security Management System (ISMS) nach ISO/IEC 27000er Reihe. Hierbei handelt es sich um ein System zur Verwaltung von Politik, Verfahren, Richtlinien und damit verbundenen Ressourcen und Tätigkeiten zum Schutz der Informationswerte eines Unternehmens. Innerhalb der ISO/IEC 27001:2017 werden Anforderungen für Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufender Verbesserung eines ISMS unter Berücksichtigung organisationsspezifischer Rahmenbedingungen dargelegt. Weiters kann auch eine Zertifizierung des Unternehmens erfolgen, die folgende Vorteile bietet [34]:

- Erhöhung der Datensicherheit
- rechtzeitiges Erkennen von Bedrohungen
- Einhaltung externer Anforderungen
- kontinuierliche Verbesserung der internen Abläufe durch wiederholte Evaluierung

[1] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.html
[2] https://plattformindustrie40.at/security-safety/

6 Best Practices

Dieser Abschnitt beinhaltet Erfahrungswerte und Best-Practice-Vorgehensweisen, die im Zuge der Forschungstätigkeiten innerhalb der Technikum Digital Factory[1] im Kontext von Safety & Security gesammelt wurden. Neben bewährten Methoden wird unter anderem auf Herausforderungen bei der Umsetzung einer sicheren Umgebung und dem Betrieb mobiler Robotik in flexiblen und intelligenten Produktionsumgebungen eingegangen. Dieses Whitepaper stellt eine theoretische Hilfestellung bei der Entwicklung, Integration und dem Betrieb eines mobilen Roboters in einer intelligenten Produktionsumgebung dar. Damit die Ergebnisse dieses Dokuments validiert und verifiziert werden können, wurden zwischen 2018 und 2021 verschiedene Szenarien begleitend als praktische Anwendung des Whitepapers geplant und umgesetzt. Eine Auswahl der Erkenntnisse wird hier zusammengefasst vorgestellt.

Zusammenarbeit mit TÜV AUSTRIA und Arbeitsinspektorat empfohlen

Die Zusammenarbeit mit notifizierten Stellen bzw. Dienstleistungsunternehmen mit entsprechender Expertise und dem Arbeitsinspektorat wird an dieser Stelle explizit empfohlen. Je früher jene Institutionen in den Entwicklungs- bzw. Integrationsprozess eingebunden werden, desto geringer ist die Wahrscheinlichkeit, dass aufwendige Änderungen in späten Projektphasen durchgeführt werden müssen. Die TÜV AUSTRIA SERVICES GmbH[2] ist eine nach österr. Recht notifizierte Stelle zur Durchführung von Prüfverfahren unter anderem gemäß „Maschinenrichtlinie“ (2006/42/EG), „EMV-Richtlinie“ (2014/30/EU), „Funkanlagenrichtlinie“ (2014/53/EU), sowie Prüf- und Zertifizierungsverfahren gemäß IEC 62443. Weitere Informationen zu notifizierten Stellen sind im Nando (New Approach Notified and Designated Organisations) Information System[3] abrufbar.

Offenes Stationskonzept für Laborbetrieb

Speziell um weg von traditionellen, starren Absicherungssystemen hin zu innovativer, dynamischer Arbeitsraumüberwachung zu gelangen, verfolgt die Technikum Digital Factory ein offenes Stationskonzept für mobile Robotik und Mensch-Roboter-Kollaboration (MRK). Dies ermöglicht niederschwelligen Zugang für Mitarbeitende und fördert Weiterentwicklungen. Obwohl die Maschinen-Sicherheitsverordnung 2010 gemäß §1 Buchstabe h in diesem Fall nicht anzuwenden ist, werden dennoch hohe Ansprüche an Safety gestellt, um den sicheren Betrieb bestmöglich zu gewährleisten. Dementsprechend wurde bei allen kollaborativen Robotersystemen eine Geschwindigkeits- und Kraftbegrenzung umgesetzt, die im Laborbetrieb eine Maximalgeschwindigkeit von 250mm/s erlaubt. Für mobile Roboter wurden Geschwindigkeitsgrenzen ebenfalls entsprechend angepasst.

Beeinträchtigung durch Sonneneinstrahlung

Konstante Lichtbedingungen sind essentiell für den zuverlässigen Einsatz von optischen oder laserbasierten (Sicherheits)Systemen. Nichtsdestotrotz ist die zur Verfügung stehende Umgebung nicht immer optimal gestaltet und z.B. durch Fenster oder große Glasfronten veränderlichen Bedingungen ausgesetzt. In der Technikum Digital Factory haben Spiegelungen im Glas und einfallendes Sonnenlicht unter bestimmten Umständen zu Fehldetektionen oder Versagen von diversen Sensoren (z.B. Laserscanner am mobilen Roboter, ToF-Kamerasystem zur Arbeitsraumüberwachung) geführt. Um die Zuverlässigkeit der einzelnen Systeme zu verbessern, wurde deshalb intensiv auf eine diverse Kombination aus Sensorik mit unterschiedlichen Wirkprinzipien gesetzt (z.B. Ergänzung um Ultraschallsensoren).

[1] https://digitalfactory.technikum-wien.at/
[2] https://www.tuv.at/home
[3] https://ec.europa.eu/growth/tools-databases/nando/

Schulung von Mitarbeitenden, Studierenden und BesucherInnen

Durch ein offenes Stationskonzept bleibt in jedem Fall ein gewisses Gefahrenpotential vorhanden. Der Zutritt zur Technikum Digital Factory für Mitarbeitende, Studierende sowie BesucherInnen ist dementsprechend erst nach erfolgter Einschulung und Unterweisung möglich. Die Weiterbildung von Personal sollte in allen Betriebsumgebungen - auch abseits von Forschungslaboratorien - eine zentrale Rolle bei der Reduktion von Restrisiken einnehmen. Die Verfügbarkeit und Sichtbarkeit von Information (z.B. durch Warnhinweise, Schilder) trägt darüber hinaus maßgeblich zur Aufrechterhaltung der Betriebssicherheit bei.

Messung biomechanischer Grenzwerte

Um ein detailliertes Bild über das real vorhandene Gefahrenpotenzial und wirkende Kräfte des eingesetzten mobilen Manipulators zu erlangen, wurde eine Messung biomechanischer Grenzwerte durchgeführt. Die hieraus ermittelten Kräfte für eine kontaktbetätigte Erkennungseinrichtung werden innerhalb der Risikobeurteilung der Applikation entsprechend ISO/TS 15066:2016 [35] weiter bewertet. Eine zertifizierte Messung biomechanischer Grenzwerte kann aufschlussreiche Erkenntnisse über das tatsächliche Verletzungsrisiko liefern und die Erarbeitung weiterer Maßnahmen unterstützen. Besonders Umbauten oder Erweiterungen des AMR können differente Kraft- und Druckwerte sowie neues Gefahrenpotential hervorrufen. Abbildung 16 zeigt, dass der Grenzwert von 130 N (Unterschenkel - quasistatisch) knapp überschritten wurde und weitere Maßnahmen erforderlich sind. In der korrespondierenden Druckmessung (Abbildung 17) lag die Messung mit 93 N/cm² deutlich unter dem Grenzwert (210 N/cm²). Ein umgekehrtes Bild zeigt sich bei Messung 4 (fünfter Lendenwirbel). Kraftwerte (Abbildung 18) befinden sich unterhalb der Grenze, während der Druck (Abbildung 19) aufgrund der Kontur außerhalb des zulässigen Bereichs liegt, was in weiterer Folge die Umsetzung konstruktiver Maßnahmen bedingt.

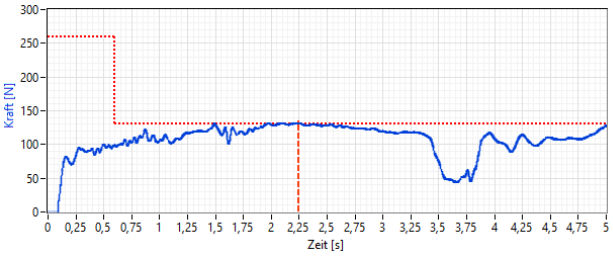


Abbildung 16: Messung 1: Kraft im zeitlichen Verlauf

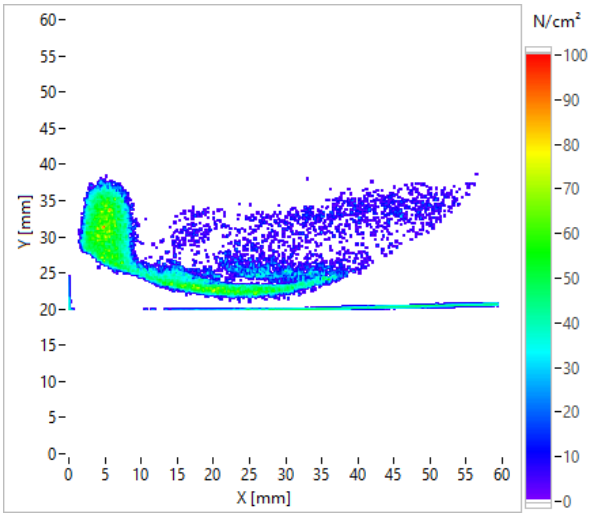


Abbildung 17: Messung 1: Druck

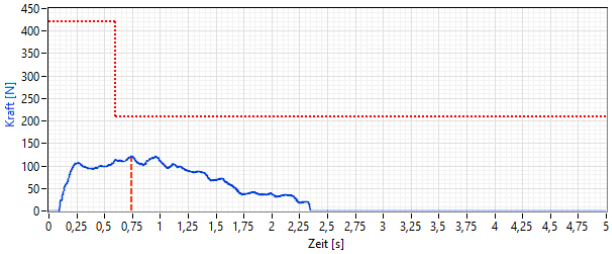


Abbildung 18: Messung 4: Kraft im zeitlichen Verlauf

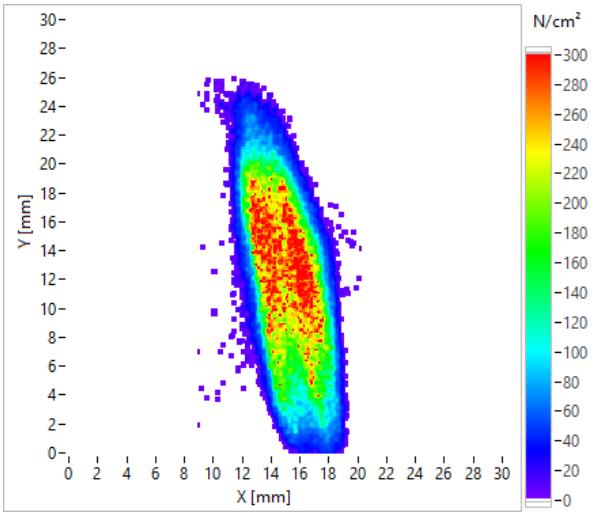


Abbildung 19: Messung 4: Druck

Risikoidentifikation, -bewertung & -minderung

Auf Basis der Ergebnisse der biomechanischen Grenzwertmessung sowie einer umfassenden Risikoanalyse zur Bewertung des Gefahrenpotentials der neu geschaffenen Kombination aus MiR100 und UR5, wurde eine Reihe an Maßnahmen zur Risikominimierung abgeleitet. Ausgangspunkt für die systematische Analyse und Ermittlung von Ursprung und möglichen Folgen von Gefährdungen in allen Prozessphasen bildete die ÖNORM EN ISO 12100:2013. Die nachfolgende Liste beinhaltet eine Auswahl an ermittelten Gefahrenstellen des AMR sowie zugehöriger Risiko-minderungsmaßnahmen (siehe Abbildung 20):

1. Einklemmen von Gliedmaßen zwischen den Achsen des UR5
   - Achsenbewegungen während Fahrt verhindern
   - Senkung der Auslösekraft für kollaborativen Stopp
2. Quetschen von Gliedmaßen zwischen den Greiferbacken
   - konstruktive Anpassung des Greifers
   - optische und akustische Warnhinweise
   - Leistungsreduzierung des Greifvorgangs
3. Schnittgefahr durch scharfe Kanten am Gehäuse des AMR
   - Anpassung der Außenkontur
   - Abrundung scharfer Kanten
4. Verletzungsgefahr durch Umkippen
   - konstruktive Anpassung des Aufbaus und Senkung des Schwerpunkts
5. Verletzungsgefahr durch unsichere Konstruktion des Bauteilträgers
   - konstruktive Änderung der Produktaufnahmevorrichtung
6. Security-Risiko durch freiliegende Ethernet- und USB-Ports
   - konstruktive Anpassung der Verkleidung, um Zugang zu erschweren
   - Access Control nach IEEE 802.1X

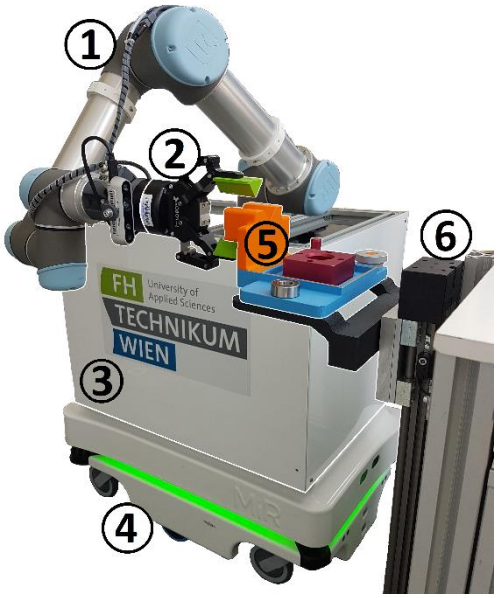


Abbildung 20: Identifizierte Gefahrenstellen am mobilen Manipulator [36]

Penetration Testing

Ein Testnetzwerk, das für die (Produktions)-Prozesse innerhalb der Technikum Digital Factory erstellt wurde, wurde in einem Penetration-Test auf Schwachstellen in der Struktur und den eingesetzten Geräten untersucht. Jene Art des Testens liefert aufschlussreiche Informationen über die Gesamtsicherheit von Netzwerken und Softwaresystemen in Angriffsszenarien. Die Ergebnisse zeigten teilweise schwerwiegende Sicherheitslücken (z.B. unzureichende Netzwerksegmentierung), woraus u.a. folgende IT-Security-Maßnahmen abgeleitet wurden:

- Zugang über verschlüsselte Kommunikationskanäle (VPN)
- Monitoring & Protokollierung von Zugriffsanforderungen (extern/intern)
- aktueller Virenschutz auf Produktionssystemen und Endgeräten
- regelmäßige Datenbackups der Systeme inkl. Wiederherstellungs- und Integritätstests
- Verschlüsselung des Datentransfers
- Netzwerksegmentierung (IEC 62443)
- Richtlinien für den Einsatz von Wechseldatenträgern
- Security-Schulung des Personals
- proaktiver Umgang mit potentiellen Bedrohungen
- Einführung eines Information Security Management System (ISMS)

7 Literaturverzeichnis

[1] *IEC/TS 62443-1-1:2009 - Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models*

[2] VDI/VDE-FACHBEREICH AUTONOME SYSTEME & MECHATRONIK: *VDI/VDE 2206 - Entwicklung mechatronischer und cyber-physischer Systeme*. 2021

[3] FACHBEREICH INDUSTRIELLE INFORMATIONSTECHNIK: *VDI/VDE 2182 Blatt 1 - Informationssicherheit in der industriellen Automatisierung - Allgemeines Vorgehensmodell*. 2020

[4] *ÖVE/ÖNORM EN 61508-1:2011 - Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 1: Allgemeine Anforderungen*

[5] INTERNATIONAL FEDERATION OF ROBOTICS: *World Robotics Report 2020*. URL http://reparti.free.fr/robotics2000.pdf

[6] *ÖNORM EN ISO 12100:2013 - Sicherheit von Maschinen – Allgemeine Gestaltungsleitsätze – Risikobeurteilung und Risikominderung*

[7] GÜNTER ULLRICH ; THOMAS ALBRECHT: *Fahrerlose Transportsysteme* : *Eine Fibel – mit Praxisanwendungen – zur Technik – für die Planung*, 2019

[8] *Bundesgesetz über Sicherheit und Gesundheitsschutz bei der Arbeit (ArbeitnehmerInnenschutzgesetz – ASchG), BGBl. Nr. 450/1994 idF I Nr. 100/2018*

[9] *ÖNORM EN ISO 3691-4:2020 - Flurförderzeuge – Sicherheitstechnische Anforderungen und Verifizierung – Teil 4: Fahrerlose Flurförderzeuge und ihre Systeme*

[10] *ÖNORM EN ISO 10218-1:2020 - Robotik - Sicherheitsanforderungen für Industrieroboter - Teil 1: Roboter*

[11] *ÖNORM EN ISO 10218-2:2012 - Industrieroboter – Sicherheitsanforderungen – Teil 2: Robotersysteme und Integration*

[12] *ÖNORM EN ISO 13849-2:2013 - Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 2: Validierung*

[13] *Verordnung des Bundesministers für Wirtschaft und Arbeit über die Sicherheit von Maschinen und von Sicherheitsbauteilen für Maschinen (Maschinen-Sicherheitsverordnung 2010 - MSV 2010), BGBl. II Nr. 282/2008 idF II Nr. 204/2018*

[14] *Verordnung des Bundesministers für Wissenschaft, Forschung und Wirtschaft über elektrische Betriebsmittel zur Verwendung innerhalb bestimmter Spannungsgrenzen (Niederspannungsgeräteverordnung 2015 – NspGV 2015), BGBl. II Nr. 21/2016*

[15] *Verordnung des Bundesministers für Wissenschaft, Forschung und Wirtschaft über elektromagnetische Verträglichkeit (Elektromagnetische Verträglichkeitsverordnung 2015 – EMVV 2015), BGBl. II Nr. 22/2016*

[16] *Bundesgesetz über die Marktüberwachung von Funkanlagen (Funkanlagen-Marktüberwachungs-Gesetz – FMaG 2016), BGBl. I Nr. 57/2017 idF I Nr. 190/2021*

[17] EUROPÄISCHE KOMMISSION - GENERALDIREKTION BINNENMARKT, INDUSTRIE, UNTERNEHMERTUM UND KMU: *Leitfaden für die Anwendung der Maschinenrichtlinie 2006/42/EG, Ausgabe 2.2*. URL https://ec.europa.eu/docsroom/documents/38022

[18] *ÖNORM EN ISO 13849-1:2016 - Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze*

[19] *OVE EN 62061:2016 - Sicherheit von Maschinen - Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme*

[20] ALEXANDRA MARKIS ; MAXIMILIAN PAPA ; DAVID KASELAUTZKE ; MICHAEL RATHMAIR ; VINZENZ SATTINGER ; MATHIAS BRANDSTÖTTER: *Safety of Mobile Robot Systems in Industrial Applications*

[21] *ONR CEN ISO/TR 22100-1:2021 - Sicherheit von Maschinen - Beziehung zu ISO 12100 - Teil 1: Wie ISO 12100 und Typ-B- und Typ-C-Normen zusammenhängen*

[22] SABRINA STEGER ; ALEXANDRA MARKIS ; HARALD MONTENEGRO ; MICHAEL NEUHOLD ; ANDREAS OBERWEGER ; CHRISTOPH SCHWALD ; WILFRIED SIHN ; FABIAN RANZ ; THOMAS EDTMAYR ; PHILIPP HOLD ; GERHARD REISINGER: *White Paper III - Safety und Security in der Mensch-Roboter-Kollaboration - Einfluss der IT-Security*. URL https://www.tuv.at/next-generation/white-paper/

[23] *ONR CEN ISO/TR 22100-4:2021 - Sicherheit von Maschinen - Zusammenhang mit ISO 12100 - Teil 4: Leitlinien für Maschinenhersteller zur Berücksichtigung der damit verbundenen IT-Sicherheits-(Cybersicherheits-) Aspekte*

[24] *OVE EN IEC 62443-4-1:2018 - IT-Sicherheit für industrielle Automatisierungssysteme - Teil 4-1: Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung*

[25] *OVE EN IEC 62443-4-2:2020 - IT-Sicherheit für industrielle Automatisierungssysteme - Teil 4-2: Technische Sicherheitsanforderungen an Komponenten industrieller Automatisierungssysteme*

[26] GUNTHER KOSCHNICK: *Orientierungsleitfaden für Hersteller zur IEC 62443*. URL https://www.zvei.org/presse-medien/publikationen/orientierungsleitfaden-fuer-hersteller-zur-iec-62443/

[27] EUROPÄISCHE KOMMISSION: *Bekanntmachung der Kommission - Leitfaden für die Umsetzung der Produktvorschriften der EU 2016 („Blue Guide“)*. URL https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52016XC0726(02)

[28] ALLGEMEINE UNFALLVERSICHERUNGSANSTALT: *Folder: Umbau von Maschinen*. URL https://www.auva.at/cdscontent/?contentid=10007.672901&portal=auvaportal&viewmode=content

[29] WIRTSCHAFTSKAMMER ÖSTERREICH: *CE-Kennzeichnung und Normen*. URL https://www.wko.at/service/innovation-technologie-digitalisierung/ce-kennzeichnung-normen.html

[30] *IEC 62443-3-2:2020 - Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design*

[31] BARRACUDA NETWORKS INC.: *Whitepaper - Implementierung der IEC 62443 mit Barracuda CloudGen Firewall*. URL https://assets.barracuda.com/assets/docs/dms/CloudGen_Firewall_WP_IEC62443_DE.pdf

[32] ROBERT LAMPRECHT: *Cyber Security in Österreich 2021*

[33] ROBERT M. LEE: *The Sliding Scale of Cyber Security*. URL https://sansorg.egnyte.com/dl/GJEumszLQX/?

[34] TÜV AUSTRIA: *ISO 27001 - Informationssicherheit*. URL https://www.tuv.at/loesungen/business-assurance/managementsystemzertifizierung/iso-27001-informationssicherheit

[35] *DIN ISO/TS 15066:2017 - Roboter und Robotikgeräte - Kollaborierende Roboter*

[36] VINZENZ SATTINGER ; MAXIMILIAN PAPA ; KEMAJL STUJA ; WILFRIED KUBINGER: Methodik zur Entwicklung sicherer kollaborativer Produktionssysteme im Rahmen von Industrie 4.0. In: *e & i Elektrotechnik und Informationstechnik*, S. 318–325

Abkürzungsverzeichnis

AMR	autonomer mobiler Roboter
CE	Conformité Européenne
CPS	Cyber-Physische Systeme
FTS	fahrerloses Transportsystem
IIoT	Industrial Internet of Things
IT	Information Technology
PL	Performance Level
SIL	Safety Integrity Level
SL	Security Level
DoS	Denial of Service
ISMS	Information Security Management System

Begriffsbestimmungen

Betreiber

Personen oder Unternehmen mit organisatorischer und technischer Verantwortung für die gesamte Produktionsanlage
[VDI 2182-1]

Betrieb

Aufrechterhalten des wertschöpfenden Produktionsablaufs nach der Inbetriebnahme eines Systems, inklusive regelmäßiger Wartung und regelmäßiger Sicherheitsüberprüfungen

Conduit

logische Gruppierung von Kommunikationskanälen, die zwei oder mehr Zonen verbindet, für die gemeinsame IT-Sicherheitsanforderungen gelten
Anmerkung: Ein Conduit (ein Leitungsschutzrohr) darf eine Zone durchqueren, solange die IT-Sicherheit der im Conduit verlaufenden Kanäle durch die Zone nicht beeinträchtigt wird.
[OVE EN IEC 62443-3-3:2020]

Entwickler

(siehe auch Hersteller)
Personen oder Unternehmen, die ein Gesamtsystem von Grund auf designen, auslegen und nach gegebener Gesetzes- und Normenlage umsetzen

Entwicklung

Prozess, bei dem der mobile Roboter oder Teile dessen und/oder die Lastübergabestation von Grund auf neu konzipiert, entworfen und umgesetzt werden und schließlich laut gegebener Gesetzes- und Normenlage in einer Produktionsumgebung eingesetzt werden können

fahrerloses Transportsystem (FTS)

innerbetriebliche, flurgebundene Fördersysteme mit automatisch gesteuerten Fahrzeugen, deren primäre Aufgabe der Materialtransport, nicht aber der Personentransport ist
Sie werden innerhalb und außerhalb von Gebäuden eingesetzt und bestehen im Wesentlichen aus:

- einem oder mehreren Fahrerlosen Transportfahrzeugen,
- einer Leitsteuerung,
- Einrichtungen zur Standortbestimmung und Lageerfassung,
- Einrichtungen zur Datenübertragung, sowie
- Infrastruktur und peripheren Einrichtungen.

[VDI 2510]
Anm. d. Verf.: Innerhalb der ÖNORM EN ISO 3691-4 wird dieser Begriff synonym mit "autonomer mobiler Roboter" verwendet.

Hersteller

(siehe auch Entwickler)
verantwortliches Unternehmen für Entwurf, Design, Konstruktion, Produktion, Vertrieb und Service von Automatisierungslösungen und Automatisierungssystemen
[VDI 2182-1]

Integration

Vorgang des Zusammenführens eines Roboters mit einem Endeffektor und anderer Ausrüstung oder Maschine (einschließlich weiterer Robotersysteme) zur Bildung einer vollständigen Maschine, die nützliche Arbeit ausführen kann [...]
[ÖNORM EN ISO 10218-1:2012]
Anm. d. Verf.: Im weiteren Sinne ist auch das Zusammenführen und Miteinbeziehen einzelner Subsysteme zu einem Gesamtsystem, welches eine bestimmte Funktion erfüllt, gemeint.

Integrator

Personen oder Unternehmen mit Verantwortung für die Kombination einzelner oder verschiedener Automatisierungsgeräte zu Automatisierungssystemen und Integration dieser in Produktionsanlagen
[VDI 2182-1]

Integrität

(engl.: integrity)
Bedingung für den Schutz vor unsachgemäßer Änderung oder Zerstörung von Informationen
[ONR CEN ISO/TR 22100-4:2021]

intelligente Produktion

(auch intelligente Fertigung)
(engl.: Smart Manufacturing)
Fertigung, die ihre Leistungsaspekte durch den integrierten und intelligenten Einsatz von Prozessen und Ressourcen im Cyber-, physischen und menschlichen Bereich verbessert, um Produkte und Dienstleistungen zu erzeugen und bereitzustellen, die auch mit anderen Bereichen innerhalb der Wertschöpfungsketten von Unternehmen zusammenarbeitet
Anmerkung 1: Zu den Leistungsaspekten gehören Agilität, Effizienz, Sicherheit, Nachhaltigkeit oder andere vom Unternehmen identifizierte Leistungsindikatoren.
Anmerkung 2: Zusätzlich zur Fertigung können andere Unternehmensbereiche wie Engineering, Logistik, Marketing, Beschaffung, Vertrieb oder andere vom Unternehmen identifizierte Bereiche einbezogen sein.
[ONR CEN ISO/TR 22100-4:2021]

Manipulator

Im Kontext der Robotik wird der bewegliche Teil des Robotersystems (bzw. Roboterarm) zur physischen Umgebungsinteraktion als Manipulator bezeichnet.

Maschine

- eine mit einem anderen Antriebssystem als der unmittelbar eingesetzten menschlichen oder tierischen Kraft ausgestattete oder dafür vorgesehene Gesamtheit miteinander verbundener Teile oder Vorrichtungen, von denen mindestens eines bzw. eine beweglich ist und die für eine bestimmte Anwendung zusammengefügt sind;
- eine Gesamtheit im Sinne des ersten Gedankenstrichs, der lediglich die Teile fehlen, die sie mit ihrem Einsatzort oder mit ihren Energie- und Antriebsquellen verbinden;
- eine einbaufertige Gesamtheit im Sinne des ersten und zweiten Gedankenstrichs, die erst nach Anbringung auf einem Beförderungsmittel oder Installation in einem Gebäude oder Bauwerk funktionsfähig ist;
- eine Gesamtheit von Maschinen im Sinne des ersten, zweiten und dritten Gedankenstrichs oder von unvollständigen Maschinen [...], die, damit sie zusammenwirken, so angeordnet sind und betätigt werden, dass sie als Gesamtheit funktionieren;
  [BGBl. II Nr. 282/2008 (Maschinen-Sicherheitsverordnung 2010)]

Performance Level (PL)

diskrete Stufe, welche die Fähigkeit von sicherheitsbezogenen Teilen einer Steuerung spezifiziert, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen
[ÖNORM EN ISO 13849-1:2016]

Risiko

Kombination der Wahrscheinlichkeit des Eintritts eines Schadens und seines Schadensausmaßes
[ÖNORM EN ISO 12100:2013]

Risikoanalyse

Kombination aus Festlegung der Grenzen der Maschine, Identifizierung der Gefährdungen und Risikoeinschätzung
[ÖNORM EN ISO 12100:2013]

Risikobeurteilung

Gesamtheit des Verfahrens, das eine Risikoanalyse und Risikobewertung umfasst
[ÖNORM EN ISO 12100:2013]

Risikobewertung

auf der Risikoanalyse beruhende Beurteilung, ob die Ziele zur Risikominderung erreicht wurden
[ÖNORM EN ISO 12100:2013]

Roboter

Industrieroboter

Automatisch gesteuerter, frei programmierbarer Mehrzweck-Manipulator, der in drei oder mehr Achsen programmierbar ist und zur Verwendung in der industriellen Automatisierungstechnik entweder an einem festen Ort oder beweglich angeordnet sein kann
[ÖNORM EN ISO 10218-1:2012]

(autonomer) mobiler Roboter (AMR)

mobile Plattform, die mit Hilfe von Hindernisvermeidung und Bahnplanung navigiert, statt einem vordefinierten Pfad zu folgen
[in Anlehnung an ANSI/RIA R15.08-1-2020]
Anm. d. Verf.: Gemäß ANSI/RIA R15.08-1:2020 liegt der entscheidende Unterschied zu einem fahrerlosen Transportsystem (FTS) in der Spurgebundenheit und Fähigkeit der Hindernisumgehung. Innerhalb der ÖNORM EN ISO 3691-4:2020 werden diese Begriffe synonym verwendet. Die Kombination aus industrietauglichem mobilen Roboter und Roboterarm wird als mobiler Manipulator (IMR Type C) bezeichnet.

Safety

(dt.: Maschinensicherheit)
Abwesenheit inakzeptabler Risiken für die (körperliche) Unversehrtheit von Menschen oder Schaden an Eigentum oder Umwelt
[in Anlehnung an IEC 80001-1:2010]

Safety Integrity Level (SIL)

(dt.: Sicherheits-Integritätslevel)

diskrete Stufe zur Festlegung der Anforderungen an die Sicherheitsintegrität der Sicherheitsfunktionen, die den sicherheitsbezogenen elektrischen/elektronischen/ programmierbar elektronischen Systemen zugeordnet werden [...]

[ÖVE/ÖNORM EN 61508-4:2011]

Security

(auch Informationssicherheit)

Bewahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Information

Anmerkung: Zusätzlich können auch andere Eigenschaften wie Authentizität, Zurechenbarkeit, Nichtabstreitbarkeit und Verlässlichkeit einbezogen werden.

[in Anlehnung an ÖVE/ÖNORM EN ISO/IEC 27000:2020]

Anm. d. Verf.: Auf Informationstechnik bezogene Security (IT-Security) adressiert hingegen die Informationssicherheit eines konkreten informationstechnischen Systems. Beide Begriffe umfassen jedoch die physische Zugangsbeschränkung zur Aufrechterhaltung der Sicherheit (siehe Integrität).

Verfügbarkeit

(engl.: availability)

Eigenschaft zugänglich und Nutzbar zu sein, wenn eine befugte Entität Bedarf hat

[ÖVE/ÖNORM EN ISO/IEC 27000:2020]

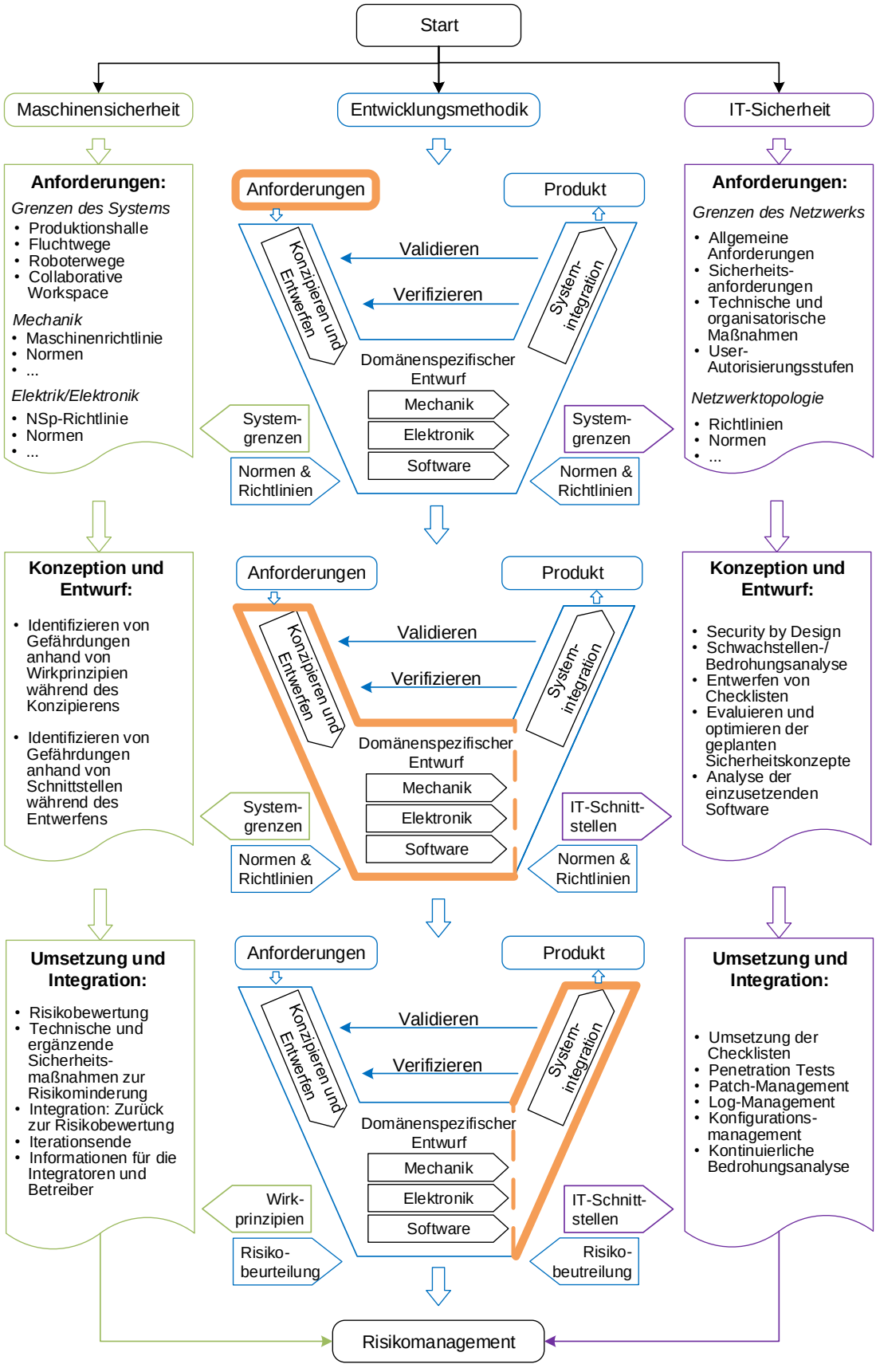
Vertraulichkeit

(engl. confidentiality)

Aufrechterhaltung autorisierter Beschränkungen und Verhinderung des unbefugten Zugriffs auf Informationen

[ONR CEN ISO/TR 22100-4:2021]

Anhang A: Erweitertes SIP4.0-Entwicklungsmodell



Anhang B: Checkliste für Betriebsüberprüfungen

Beurteilungspunkte		Ordnungs-gemäß	Problem	Maßnahmen
A	**Arbeitsumgebung/Verkehr**			
A1	Persönliche Schutzausrüstung			
A2	Sicherheitskennzeichnung			
A3	Verkehrswege, Fluchtwege, Notausgänge, Gehwege (frei?)			
A4	Unterweisungsnachweise			
B	**Arbeitsmittel, Maschinenschutz**			
B1	Betriebsbeschreibung vorhanden			
B2	Geräte & Werkzeuge überprüft			
B3	Wartung/Instandsetzung			
C	**Ergonomie**			
C1	Arbeitsmittel			
D	**Notfallorganisation**			
D1	Erste Hilfe vorhanden			
D2	Brandschutz vorhanden			
E	**Gefahrstoffe**			
E1	Gefahrstoffe überprüfen			
E2	Sicherheitsdatenblätter vorhanden			
F	**Lagerung/Transport**			
F1	Material, Lagerung/Lagerflächen			
F2	Ladungssicherung durchgeführt			
F3	Flurförderfahrzeuge einwandfrei			

Diese beispielhafte Checkliste soll als Orientierungspunkt dienen und für die jeweiligen Bedürfnisse des Betriebs angepasst werden.

Anhang C: Liste relevanter Normen und Richtlinien

Jene Auflistung umfasst zum Veröffentlichungszeitpunkt (Q1 2022) in Österreich gültige EU- bzw. EG-Richtlinien sowie normative Dokumente im Kontext mobiler Robotik und stellt keinen Anspruch auf Vollständigkeit. Die tatsächlich anzuwendenden regulatorischen Rahmenbedingungen sind spezifisch im Einzelfall für das geplante Vorhaben zu ermitteln.

- **EU-/EG-Richtlinien:**
  - 2006/42/EG (Maschinenrichtlinie)
    in Österreich durch Maschinen-Sicherheitsverordnung 2010 umgesetzt
  - 2014/30/EU (EMV-Richtlinie)
    in Österreich durch Elektromagnetische Verträglichkeitsverordnung 2015 umgesetzt
  - 2014/35/EU (Niederspannungsrichtlinie)
    in Österreich durch Niederspannungsgeräteverordnung 2015 umgesetzt
  - 2014/53/EU (RED-Richtlinie)
    in Österreich durch Funkanlagen-Marktüberwachungs-Gesetz umgesetzt

- **Normen:**
  - ISO 12100:2010 (ÖNORM EN ISO 12100:2013)
  - ISO 3691-4:2020 (ÖNORM EN ISO 3691-4:2020)
  - ISO 10218-1:2011 (ÖNORM EN ISO 10218-1:2012)
  - ISO 10218-2:2011 (ÖNORM EN ISO 10218-2:2012)
  - ISO 13849-1:2015 (ÖNORM EN ISO 13849-1:2016)
  - ISO 13849-2:2012 (ÖNORM EN ISO 13849-2:2013)
  - ISO 13850:2015 (ÖNORM EN ISO 13850:2016)
  - ISO 13855:2010 (ÖNORM EN ISO 13855:2010)
  - ISO 13856-3:2013 (ÖNORM EN ISO 13856-3:2013)
  - ISO 14118:2017 (ÖNORM EN ISO 14118:2018)
  - ISO/IEC 27000:2018 (ÖVE/ÖNORM EN ISO/IEC 27000:2020)
  - ISO/IEC 27001:2013 + Cor 1:2014 + Cor 2:2015 (ÖVE/ÖNORM EN ISO/IEC 27001:2017)
  - IEC 61508:2010 Parts 1 - 7 (ÖVE/ÖNORM EN 61508:2011 Teile 1 - 7)
  - IEC 62061:2005 + A1:2012 + A2:2015 (OVE EN 62061:2016)
  - IEC 62443-2-4:2015 + Cor.:1:2015 + A1:2017 (OVE EN IEC 62443-2-4:2020)
  - IEC 62443-3-2:2020
  - IEC 62443-3-3:2013 + COR1:2014 (OVE EN IEC 62443-3-3:2020)
  - IEC 62443-4-1:2018 (OVE EN IEC 62443-4-1:2018)
  - IEC 62443-4-2:2019 (OVE EN IEC 62443-4-2:2020)
  - IEC 60204-1:2016 (OVE EN 60204-1:2019)
  - IEC 61496-1:2020 (OVE EN IEC 61496-1:2021)
  - IEC 61310-1:2007 (ÖVE/ÖNORM EN 61310-1:2008)
  - IEC 62046:2018 (OVE EN IEC 62046:2019)
  - EN 1175:2020 (ÖNORM EN 1175:2021)

- **Technische Regeln und Spezifikationen:**
  - IEC/TS 62443-1-1:2009
  - ISO/TS 15066:2016

WhitePaper

TÜV AUSTRIA HOLDING AG

TÜV AUSTRIA-Platz 1
A-2345 Brunn am Gebirge
E-Mail: *nexthorizon@tuv.at*

tuvaustria.com

Stadt Wien
Wirtschaft, Arbeit und Statistik

Rathaus
A-1010 Wien
E-Mail: *wien@gv.at*

wien.gv.at

Fachhochschule
Technikum Wien

Höchstädtplatz 6
A-1200 Wien
E-Mail: *office@technikum-wien.at*

technikum-wien.at

Figure: FH Technikum Wien