



TECHNISCHE
UNIVERSITÄT
WIEN
Vienna University of Technology

Institut für
Fertigungstechnik und
Photonische Technologien



Diplomarbeit

Konzept, Planung und Umsetzung der funktionalen Sicherheitstechnik für eine flexible Fertigungszelle mit Roboterbeschickung

ausgeführt zum Zwecke der Erlangung des akademischen Grades eines

Diplom-Ingenieurs (Master of Science) unter der Leitung von

Ao.Univ.Prof. Dipl.-Ing. Dr.techn. Burkhard Kittl

(Institut für Fertigungstechnik und Photonische Technologien)

Univ.Ass. Dipl.-Ing. Thomas Trautner

(Institut für Fertigungstechnik und Photonische Technologien)

eingereicht an der Technischen Universität Wien

Fakultät für Maschinenwesen und Betriebswissenschaften

von

Lukas Seisenbacher, BSc

01425314 (066 445)

Wien, im August 2019

Lukas Seisenbacher

Ich habe zur Kenntnis genommen, dass ich zur Drucklegung meiner Arbeit unter der Bezeichnung

Diplomarbeit

nur mit Bewilligung der Prüfungskommission berechtigt bin.

Ich erkläre weiters Eides statt, dass ich meine Diplomarbeit nach den anerkannten Grundsätzen für wissenschaftliche Abhandlungen selbstständig ausgeführt habe und alle verwendeten Hilfsmittel, insbesondere die zugrunde gelegte Literatur, genannt habe.

Weiters erkläre ich, dass ich dieses Diplomarbeitsthema bisher weder im In- noch Ausland (einer Beurteilerin/einen Beurteiler zur Begutachtung) in irgendeiner Form als Prüfungsarbeit vorgelegt habe und dass diese Arbeit mit der vom Begutachter beurteilten Arbeit übereinstimmt.

Wien, im August 2019

Lukas Seisenbacher

Danksagung

An dieser Stelle möchte ich mich bei einigen Personen bedanken, die mich bei meiner Arbeit unterstützt und motiviert haben.

Einen ganz besonderen Dank möchte ich Thomas Trautner dafür aussprechen, dass er mich als Mitbetreuer stets unterstützt und sich für mich Zeit genommen hat.

Ebenfalls möchte ich mich bei Dr. Burkhard Kittl bedanken, der es mir überhaupt erst ermöglichte, dieses interessante Thema für meine Diplomarbeit zu nutzen.

Ebenso möchte ich mich bei meinen Kollegen vom IFT bedanken, die bei der praktischen Umsetzung wie etwa bei der Deckenmontage der Laserscanner behilflich waren.

Kurzfassung

In dieser Arbeit wird ein Sicherheitskonzept für eine flexible Fertigungszelle mit Roboterbeschickung erarbeitet. Es werden Methoden und Maßnahmen beschrieben, die zur Erreichung eines ausreichend hohen Sicherheitsniveaus für Personen im Umfeld von verketteten und automatisierten Anlagen notwendig sind. Für das Sicherheitskonzept werden Laserscanner, Sicherheitslichtvorhänge und ein sicheres Kamerasystem eingesetzt, um Gefahrenbereiche abzusichern. Um dem Prozessleitsystem sämtliche relevanten Informationen bereitzustellen, wird der aktuelle Zustand der Sicherheitseinrichtungen dabei über OPC UA nach außen dargestellt. Für ein Fahrerloses Transportsystem (FTS) wird eine Schleuse über das sichere Kamerasystem eingerichtet, deren Raumüberwachungszustände ebenfalls über OPC UA aktiv manipuliert werden können, damit eine flexible Nutzung der Zelle ermöglicht wird.

Einen zentralen Teil der Arbeit stellt die Risikobeurteilung und anschließende Risikominderung dar. Der Fokus liegt dabei auf der ordnungsgemäßen Umsetzung der vorhandenen Sicherheitsnormen, wobei auf die wesentlichen Punkte der entsprechenden Normen eingegangen wird. Darüber hinaus werden auch die Anforderungen an die Sicherheitstechnik in Beziehung zur Industrie 4.0 Thematik behandelt und es wird betrachtet, in wie weit es mit den derzeit verfügbaren Mitteln möglich und sinnvoll ist, ein Sicherheitskonzept Industrie 4.0 tauglich zu gestalten.

Abstract

This thesis is about the development of a safety concept for a flexible manufacturing cell that uses robots for the loading and unloading process of the machines. It includes a description of the methods and measures that are necessary to achieve an adequate safety level for persons in the vicinity of linked and automated systems. The employed safety concept that separates the hazard area from its surroundings includes devices such as laser scanners, safety light curtains and a safe camera system. In order to provide the process control system with all the relevant information, the current state of the safety devices is transmitted to the outside via OPC UA. Moreover, a security gate for an automated guided vehicle (AGV) is set up via the safe camera system. To ensure a flexible use of the cell, the area monitoring state of the gate can also be manipulated via OPC UA.

A key point is the risk assessment and subsequent risk reduction. With a focus on the proper implementation of the existing safety standards, the main aspects of the corresponding standards are also summarised and discussed. Additionally, the requirements for safety technology are considered in an Industry 4.0 context. It is determined to what extent it is possible and reasonable with the means currently available to design a safety concept suitable for Industry 4.0 applications.

Inhaltsverzeichnis

1	Einleitung	7
1.1	Problemstellung	7
1.2	Vorgehensweise	9
2	Theoretische Grundlagen	10
2.1	Gesetze, Normen und Richtlinien	10
2.2	Strategie zur Risikobeurteilung	11
2.2.1	Risikoanalyse	13
2.2.2	Risikobewertung	15
2.3	Strategie zur Risikominderung	16
2.3.1	Schritt 1: Inhärent sichere Konstruktion	16
2.3.2	Schritt 2: Technische und ergänzende Schutzmaßnahmen	17
2.3.3	Schritt 3: Benutzerinformation	20
2.4	Dokumentation zur Risikobeurteilung und Risikominderung	21
2.5	Festsetzung eines Sicherheits-Integritätslevels zur Risikominderung	22
2.5.1	Klassifikation der Schwere S	23
2.5.2	Klassifikation der Wahrscheinlichkeit des Auftretens des Schadens K	23
2.6	Bestimmung des erforderlichen Performance-Levels für eine Sicherheitsfunktion	26
2.7	Gesamtvalidierung	27
2.8	CE-Zertifizierung	28
3	Risikobeurteilung in der Pilotfabrik	29
3.1	Klassifikation des Fertigungsbereichs	29
3.2	Anordnung der verketteten Maschinen	30
3.3	Grenzen der Maschine (Fertigungsbereich)	30
3.3.1	Identifikation der verketteten Maschinen der Drehzelle	31
3.3.2	Identifikation der verketteten Maschinen der Hybridbearbeitungszelle	34
3.3.3	Daten der vollständigen Maschine NEOBOTIX MP-400	39
3.3.4	Definition der Schnittstellen zwischen den einzelnen Teilen des IMS	39
3.3.5	Arbeitsaufgaben im bestimmungsgemäßen Betrieb	43
3.3.6	Verwendungsgrenzen	44
3.3.7	Lärmemission	45
3.3.8	Zeitliche Grenzen	45
3.3.9	Räumliche Grenzen	45

3.3.10	Weitere Grenzen	46
3.3.11	Tätigkeiten in sämtlichen relevanten Lebensphasen und Betriebsarten	46
3.4	Identifizierung der Gefährdungen, Risikoabschätzung und Risikobewertung	48
3.4.1	Ermittlung des erforderlichen Sicherheits-Integritätslevel.....	51
3.4.2	Ermittlung des erforderlichen Performance Level	52
4	Risikomindernde Maßnahmen in der Pilotfabrik	53
4.1	Risikominderung durch Konstruktive Maßnahmen.....	53
4.2	Risikominderung durch technische Schutzmaßnahmen.....	54
4.2.1	Auswahl von Schutzeinrichtungen	55
4.2.2	Anordnung und Verschaltung der Sicherheitsgeräte	62
4.2.3	Erforderliche Abstände von Sicherheitseinrichtungen	69
4.2.4	Verifizierung der funktionalen Sicherheit.....	77
4.3	Risikominderung durch Hinweisende Maßnahmen und Benutzerinformation.....	79
4.3.1	Persönliche Schutzausrüstung	79
4.3.2	Besondere Schulung des Personals	79
5	Industrie 4.0-Anforderungen an die funktionale Sicherheit	80
6	Resümee und Ausblick	84
	Literaturverzeichnis.....	88
	Abbildungsverzeichnis	92
	Formelverzeichnis.....	94
	Tabellenverzeichnis	95
	Abkürzungsverzeichnis	96

1 Einleitung

Die Sicherheitstechnik befasst sich damit, Risiken mittels verschiedenster technischer Maßnahmen zu reduzieren. Im Maschinen- und Anlagenbau werden Gefährdungssituationen durch Einsatz von physischen Barrieren wie Schutzgittern, optoelektronischen Schutzeinrichtungen wie Laserscannern, usw. vermieden und somit Personen geschützt und Unfälle vermieden. Als erster Schritt ist es dabei notwendig, alle möglichen Risiken herauszufinden und anschließend abzuschätzen, ob diese vertretbar sind oder ob geeignete Maßnahmen eingeleitet werden müssen, um das jeweilige Risiko zu mindern. Im Europäischen Raum gibt es dafür gesetzliche Vorgaben in Form von EU-Richtlinien, an die sich die Hersteller von Maschinen halten müssen, damit diese als sicher gelten. Weiters sind Hersteller von Maschinen rechtlich abgesichert, sofern sie sich an die vorgegebenen Richtlinien halten.

Der Begriff Sicherheit beschreibt einen Zustand frei von Risiken, Gefahren oder Schäden. In der Praxis wird es jedoch nie möglich sein alle Risiken oder Gefahren komplett zu eliminieren. Es wird immer ein Restrisiko geben, das als vertretbar oder aber auch als nichtvertretbar angesehen wird. Dabei gibt es in den meisten Fällen keine genau definierte Grenze, da die Abschätzung häufig auf rein subjektiven Faktoren beruht.

1.1 Problemstellung

Die Pilotfabrik teilt sich in verschiedene Bereiche, für die unterschiedliche Institute der TU Wien zuständig sind. Für diese Arbeit wird der Bereich des Instituts für Fertigungstechnik und Photonische Technologien (IFT) der TU Wien betrachtet. Dieser besteht aus mehreren Fertigungszellen und ist für die Demonstration von vollautomatischen Systemen und Industrie 4.0-Kommunikation der Maschinen bei einer Losgröße von eins gedacht. Dabei werden verschiedene Technologien eingesetzt, wie z. B. die Zerspannung von Metallen und technischen Kunststoffen sowie die additive Fertigung mittels Auftragschweißen. Der Materialtransport im automatisierten Betrieb ohne Bediener wird durch zwei Industrieroboter, ein Linear-Portal und ein fahrerloses Transportsystem (FTS) realisiert. In Abbildung 1.1 ist die Anordnung dargestellt. Die Demonstrationen von Fertigungs- und Entwicklungsideen zielen auf Personen mit unterschiedlichem fachlichem Hintergrund ab. Darüber hinaus werden neuartige Konzepte in Pilotversuchen erprobt sowie Workshops für externe Personen angeboten und die Pilotfabrik somit auch als Lernfabrik verwendet.

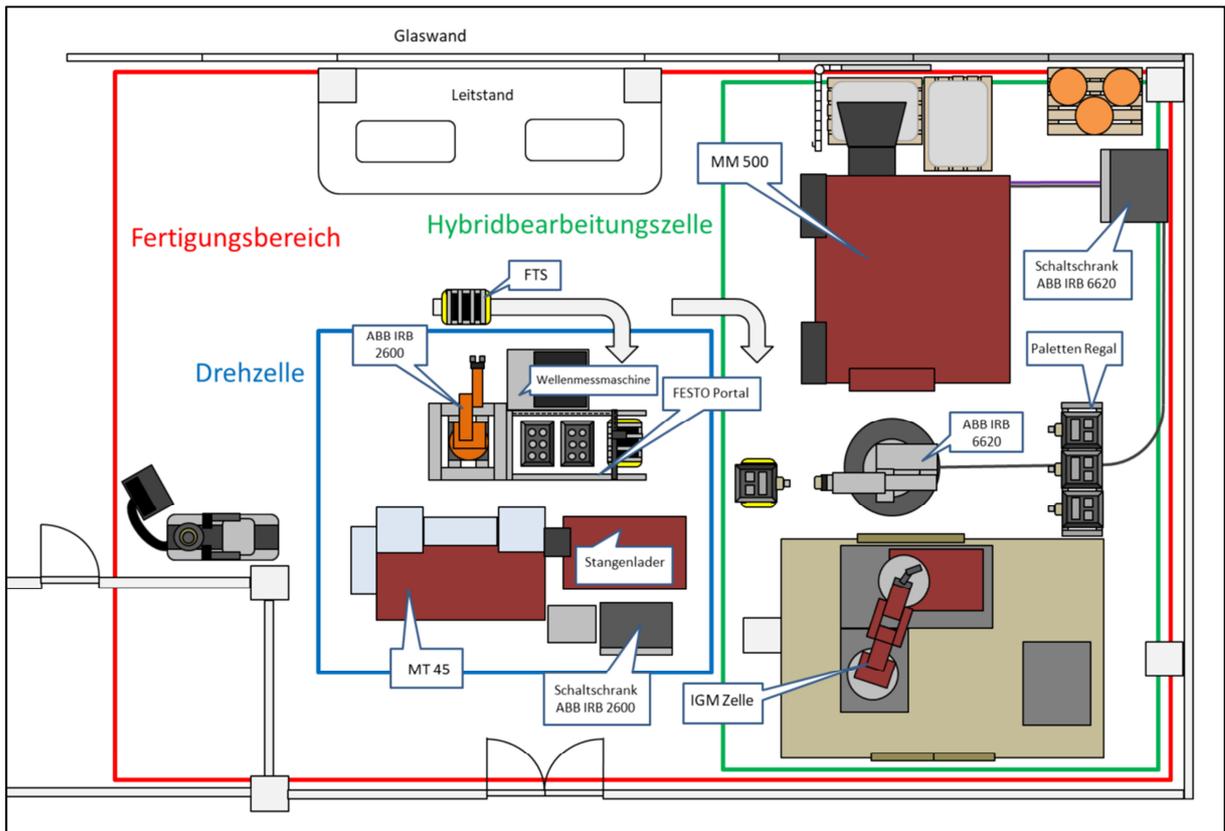


Abbildung 1.1: Anordnung der Maschinen

Aufgrund der zahlreichen Personen mit unterschiedlichstem fachlichem Hintergrund und Wissen, die sich in dem Bereich aufhalten könnten, ist ein entsprechendes Sicherheitskonzept umzusetzen. Dieses muss sämtliche Personen ausreichend vor den möglicherweise auftretenden Gefährdungen schützen und damit das Risiko eines Personenschadens hinreichend vermindern. Gleichzeitig soll die Sicht auf die verschiedenen Vorgänge und die Zugänglichkeit der Maschinen möglichst nicht eingeschränkt werden. Aufgrund der besseren Einsehbarkeit, was besonders für die Demonstration wichtig ist, werden berührungslos wirkende Sicherheitseinrichtungen verwendet. Für diese ist jeweils ein bestimmter Mindestabstand zu den Gefährdungsbereichen erforderlich. Die beiden in der Pilotfabrik befindlichen Fertigungszellen sind aus Platzgründen so nahe beieinander angeordnet, dass sie hinsichtlich der berührungslos wirkenden Sicherheitseinrichtungen praktisch wie eine einzige große Zelle betrachtet werden, weiters als Fertigungsbereich bezeichnet (in Abbildung 1.1 rot markiert). Andernfalls könnten die erforderlichen Mindestabstände nicht eingehalten werden, ohne gleichzeitig zumindest auch einen Teilbereich der jeweils anderen Fertigungszelle zu betreffen und deren Nutzbarkeit einzuschränken. Zusätzlich wäre eine größere Anzahl von Sensoren usw. notwendig, wodurch sich höhere Kosten ergeben würden. In dieser Arbeit wird die Ausarbeitung und Umsetzung des Sicherheitskonzepts dokumentiert, da es zum einen in den entsprechenden Richtlinien gefordert wird und zum anderen für eine mögliche zukünftige Erweiterung hilfreich ist.

1.2 Vorgehensweise

Zuerst werden eine Risikobeurteilung und eine Risikobewertung durchgeführt, in der alle potentiell auftretenden Gefährdungen identifiziert und bewertet werden. Im Anschluss folgt, falls erforderlich, eine Risikominderung. Dies erfolgt durch Auswahl von entsprechenden konstruktiven, technischen oder hinweisenden Schutzmaßnahmen. Zuletzt werden die Dokumentation und Verifizierung der Sicherheitseinrichtungen erläutert.

2 Theoretische Grundlagen

2.1 Gesetze, Normen und Richtlinien

Die Maschinenrichtlinie 2006/42/EG legt Aufgaben zur Erfüllung von Sicherheitsanforderungen und Gesundheitsanforderungen für Maschinen und Sicherheitsbauteile fest, die im europäischen Wirtschaftsraum in Verkehr gebracht werden sollen. Sie gilt somit sowohl für neue Maschinen als auch für gebrauchte Maschinen, die aus Drittländern wie z. B. den USA oder China importiert und erstmals im europäischen Wirtschaftsraum in den Verkehr gebracht werden. In Österreich wurde die Maschinenrichtlinie mit der Maschinen-Sicherheitsverordnung 2010 und dem Produktsicherheitsgesetz 2004 umgesetzt. Die Mitgliedstaaten dürfen keine höheren Anforderungen an die Maschinen durch nationale Gesetze stellen. [1, S. 2]

Die Anwendung von Normen wird von der Maschinenrichtlinie nicht verlangt, werden jedoch harmonisierte Normen angewendet, so gilt die Konformitätsvermutung und es kann davon ausgegangen werden, dass die Maschinenrichtlinie erfüllt wird. [1, S. 10]

Unter harmonisierten Normen werden jene Normen verstanden, die sämtliche Anforderungen der europäischen Richtlinien präzise ausformulieren, sodass bei Einhaltung dieser Normen die Konformität mit den europäischen Richtlinien sichergestellt werden kann. Eine harmonisierte Norm entsteht auf folgendem Weg: Die EU-Kommission erlässt ein Mandat zur Erarbeitung einer europäischen Norm, um die Anforderungen einer EU-Richtlinie genau festzulegen. Internationale Gremien erarbeiten diese Norm und legen technische Spezifikationen fest, um die Sicherheitsanforderungen der EU-Richtlinie zu erfüllen. Wird die Norm angenommen, so wird sie im EU-Amtsblatt veröffentlicht. Außerdem muss die Norm zusätzlich in mindestens einem EU-Mitgliedstaat veröffentlicht werden. [1, S. 10]

Internationale Sicherheitsnormen können in drei Normentypen eingeteilt werden. Typ-A Normen, sind Sicherheitsgrundnormen und behandeln Grundbegriffe, Gestaltungsleitsätze und allgemeine Aspekte, die auf Maschinen angewendet werden können. Typ-B Normen, Sicherheitsfachgrundnormen, behandeln einen Sicherheitsaspekt oder eine Art von Schutzeinrichtungen, die für eine große Reihe von Maschinen eingesetzt werden können. Diese Normen werden nochmal unterteilt in Typ-B1-Normen, diese beschreiben bestimmte Sicherheitsaspekte wie z. B. Berechnung von Sicherheitsabständen, Lärm, maximale Oberflächentemperaturen oder Anforderungen an Steuerungssysteme. Typ-B2-Normen beschreiben die Anforderungen an Schutzeinrichtungen wie z. B. trennende Schutzeinrichtungen, berührungslose Schutzeinrichtungen oder Zweihandschaltungen. Typ-C-Normen, Maschinensicherheitsnormen, beschreiben detaillierte Sicherheitsanforderungen an

einen bestimmten Maschinentyp. Existiert eine Typ-C-Norm zu einem bestimmten Maschinentyp, so hat diese Vorrang gegenüber einer Typ-A oder Typ-B Norm. [2, S. 5], [1, S. 7]

2.2 Strategie zur Risikobeurteilung

Eine Risikobeurteilung besteht aus einer Risikoanalyse und einer Risikobewertung. Die Risikoanalyse liefert benötigte Informationen für die anschließende Risikobewertung. Mit Hilfe der Risikobewertung können Entscheidungen dahingehend getroffen werden, ob eine Risikominderung erforderlich ist. Die Entscheidung, ob eine Risikominderung notwendig ist, muss durch qualitative oder quantitative Einschätzungen des Risikos, welches mit den durch die Maschine verursachten Gefährdungen verbunden ist, gestützt werden. [2, S. 18]

Der Prozess einer Risikobeurteilung mit seinen Schritten ist in Abbildung 2.1 durch den orange markierten Bereich im Flussdiagramm dargestellt. Die Schritte zur Risikobeurteilung sind durch die harmonisierte Typ-A-Norm DIN EN ISO 12100 festgelegt. Dabei wird zuerst eine Risikoanalyse durchgeführt zur Ermittlung der möglichen auftretenden Gefährdungen. Anschließend erfolgt eine Risikobewertung aller zuvor identifizierten Gefährdungen und danach erfolgt die Risikominderung, die in Abbildung 2.1 durch den blau markierten Bereich dargestellt ist. Auf die Risikominderung mit ihren Schritten wird in Abschnitt 2.3 genauer eingegangen.

Die Typ-A-Norm DIN EN ISO 12100 stellt Leitsätze zur Risikobeurteilung und Risikominderung auf, um sichere Maschinen zu konstruieren. [2, S. 6] Für integrierte Fertigungssysteme (IMS bzw. Integrated Manufacturing Systems) legt die Typ-B1-Norm DIN EN ISO 11161 ergänzende Sicherheitsanforderungen fest. Integrierte Fertigungssysteme sind zwei oder mehrere zusammenwirkende Maschinen, die mit einer Handhabeinrichtung verbunden sind und somit zu einer Gesamtheit verkettet sind. Beim Konstruieren einer Maschine oder bei der Einrichtung von integrierten Fertigungssystemen müssen die möglichen Risiken analysiert und gegebenenfalls Maßnahmen ergriffen werden, um die Personen im Anwenderkreis vor Gefährdungen zu schützen. Im Anschluss an eine Risikobeurteilung erfolgt daher bei Bedarf eine Risikominderung, indem geeignete Schutzmaßnahmen ausgewählt und umgesetzt werden. Durch die Anwendung von Schutzmaßnahmen soll jedoch kein neues Risiko entstehen. [1, 1–1]

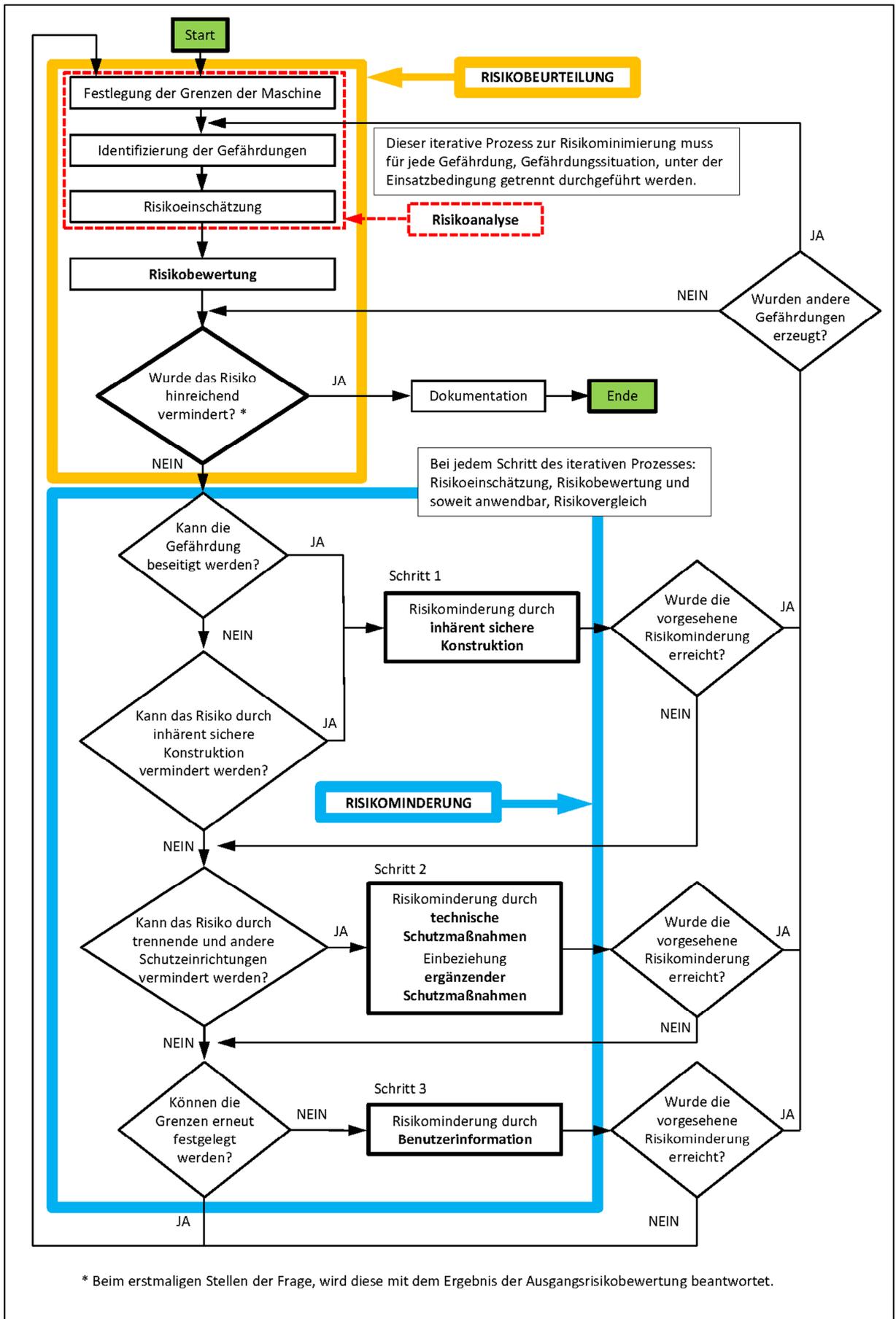


Abbildung 2.1: Prozess der Risikobeurteilung und Risikominderung [2, S. 16]

2.2.1 Risikoanalyse

2.2.1.1 Festlegung der Grenzen der Maschine

Eine Risikobeurteilung beginnt stets mit der Festlegung der Grenzen der Maschine, wobei sämtliche Phasen der Lebensdauer der Maschine berücksichtigt werden. Dies bedeutet, dass die Merkmale und die Leistung der jeweiligen Maschine bzw. der im Prozess verwendeten Maschinen genau bestimmt werden sollten. Zusätzlich sind die im Maschinenumfeld beteiligten Personen, die Umgebung und die mit der Maschine in Zusammenhang stehenden Produkte im Hinblick auf die Grenzen der Maschine zu bestimmen. [2, S. 19]

Zusätzlich zu diesen Parametern sind für integrierte Fertigungssysteme folgende weitere Parameter festzulegen: Funktionalität, Grenzen und Schnittstellen zwischen den verschiedenen Teilen des IMS. [3, S. 13]

• **Verwendungsgrenzen**

Hier sind zusätzlich zu den bestimmungsgemäßen Verwendungsgrenzen auch die vernünftigerweise vorhersehbaren Fehlanwendungen miteinzubeziehen. Um die Verwendungsgrenzen vollständig festzulegen, sollten folgende Aspekte berücksichtigt werden:

- die verschiedenen Betriebsarten der Maschine und unterschiedlichen Eingriffsmöglichkeiten durch den Benutzer, einschließlich solcher Eingriffe, die durch Fehlfunktionen der Maschine erforderlich werden
- ob die Maschine beispielsweise in der Industrie oder im Haushalt eingesetzt wird
- die Benutzung durch mehrere Personen mit verschiedenen physischen Voraussetzungen wie Links- oder Rechtshänder, unterschiedliches Alter und Geschlecht, insbesondere bezogen auf Körpergröße und Kraft, sowie Beeinträchtigungen wie Seh- oder Hörschwäche
- Ausbildung, Fähigkeiten, Erfahrung bezüglich der spezifischen Gefährdungen und Kenntnisse der standortbezogenen Sicherheitsverfahren sämtlicher Benutzer von Bedien- und Instandhaltungspersonal über in Schulung befindliche Personen bis zur allgemeinen Öffentlichkeit wie Besuchern einschließlich Kindern [2, S. 19 f]

• **Räumliche Grenzen**

Hier sind zu berücksichtigende Aspekte der Bewegungsraum, der Platzbedarf von Personen, die die Maschine bedienen, Schnittstelle Mensch-Maschine sowie Schnittstelle Maschine-Energieversorgung. [2, S. 20]

- **Zeitliche Grenzen**

Zeitliche Grenzen beinhalten Aspekte wie die sogenannte „Grenze der Lebensdauer“ der Maschine bzw. derer Bauteile wie z. B. Werkzeuge, elektrische Komponenten und Verschleißteile. Zu berücksichtigen sind dabei sowohl die bestimmungsgemäße Verwendung, als auch die vernünftigerweise vorhersehbare Fehlanwendung sowie vorgeschriebene Wartungsintervalle. [2, S. 20]

- **Weitere Grenzen**

Weitere Grenzen umfassen Eigenschaften des zu verarbeiteten Materials bzw. der zu verarbeitenden Materialien, den erforderlichen Reinlichkeitsgrad sowie die empfohlenen Mindest- und Höchsttemperaturen der Umgebung. Ebenfalls ist anzugeben ob der Betrieb im Innenraum oder im Freien, unter trockenen oder nassen Witterungsbedingungen, bei direkter Sonneneinstrahlung, staub- und nässeverträglich usw. stattfinden kann. [2, S. 20]

Bei verketteten Maschinen bzw. integrierten Fertigungssystemen sind zusätzlich die Schnittstellen zwischen den verschiedenen Teilen des integrierten Fertigungssystems festzulegen. [3, S. 13]

2.2.1.2 Identifizierung der Gefährdungen

Nach der Festlegung der Grenzen der Maschine erfolgt der wichtigste Schritt der Risikobeurteilung und zwar die systematische Identifizierung von vernünftigerweise vorhersehbaren Gefährdungen. Dies umfasst sowohl dauerhaft vorhandene Gefährdungen als auch Gefährdungen, die unerwartet auftreten können. Dabei sind alle möglichen Gefährdungssituationen und Gefährdungsereignisse in sämtlichen Phasen der Lebensdauer der Maschine zu identifizieren. Als Lebensdauer der Maschine zählen unter anderem Transport, Montage und Installation, Inbetriebnahme, Verwendung, Demontage, Außerbetriebnahme und Entsorgung. [2, S. 21]

Die Identifizierung der Gefährdungen erfolgt durch den Konstrukteur bzw. Integrator. Dieser muss insbesondere Eingriffe durch Personen während der gesamten Lebensdauer der Maschine, sämtliche mögliche Betriebszustände sowie unbeabsichtigtes Verhalten des Bedienpersonals und vernünftigerweise vorhersehbare Fehlanwendung der Maschine berücksichtigen. Wesentlich ist dabei auch die Unterscheidung, welche Arbeitsschritte von der Maschine durchgeführt werden und welche von Personen, die mit der Maschine umgehen. Erst im Anschluss an die Identifizierung sämtlicher Gefährdungen können risikomindernde bzw. gefährdungsbesetzende Maßnahmen durchgeführt werden. [2, S. 21 f]

2.2.1.3 Risikoeinschätzung

Anschließend an die Identifizierung der Gefährdungen erfolgt für jede Gefährdungssituation eine Risikoeinschätzung durch Bestimmung der Risikoelemente. [2, S. 23]

Zu den Aspekten, die während der Risikoeinschätzung zu berücksichtigen sind, zählen unter anderem: exponierte Personengruppe sowie Art, Häufigkeit und Dauer der Gefährdungsexposition, Zusammenhang zwischen Gefährdungsexposition und Auswirkungen, menschliche Faktoren, Tauglichkeit von Schutzmaßnahmen, Möglichkeit zur Ausschaltung oder Umgehung von Schutzmaßnahmen, Fähigkeit zur Aufrechterhaltung von Schutzmaßnahmen, Benutzerinformation. [2, S. 26 ff]

Das Risiko, das mit einer Gefährdungssituation verbunden ist, hängt von zwei Elementen ab. Bei diesen beiden Risikoelementen handelt es sich um das Schadensausmaß und die Eintrittswahrscheinlichkeit des Schadens. Letzteres ist dabei eine Funktion der Faktoren Gefährdungsexposition einer oder mehrerer Personen, Eintritt eines Gefährdungsereignisses sowie technische und menschliche Möglichkeiten zur Vermeidung oder Begrenzung des Schadens. Die Risikoelemente sind in Abbildung 2.2. dargestellt. [2, S. 23 f]

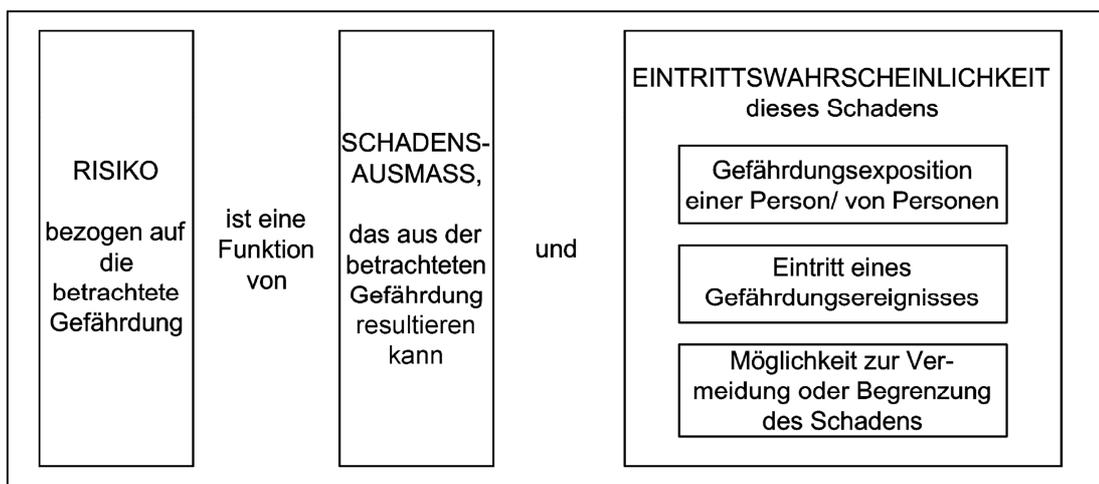


Abbildung 2.2: Risikoelemente [2, S. 24]

2.2.2 Risikobewertung

Nach der Risikoeinschätzung erfolgt die Risikobewertung. Wenn sich dabei herausstellt, dass das Risiko zu hoch ist, muss es durch Auswahl und Einsatz geeigneter Schutzmaßnahmen abgemindert werden. Entsprechend Abbildung 2.1 ist nach jeder einzelnen der drei Stufen zur Risikominderung (siehe 2.3) zu entscheiden, ob die Risikominderung ausreicht. Der Konstrukteur bzw. Integrator muss zusätzlich auch beachten, dass durch Anwendung von Schutzmaßnahmen neue Gefährdungen entstehen bzw. andere Risiken erhöht werden können. Derartige zusätzliche Risiken müssen dann entsprechend zu den bereits identifizierten Gefährdungen hinzugefügt

werden. Im Zuge dieses iterativen Prozesses werden dann gegebenenfalls weitere Schutzmaßnahmen notwendig. [2, S. 28]

DIN ISO/TR 14121-2 enthält einen praktischen Leitfaden zur Durchführung einer Risikobeurteilung in Übereinstimmung mit ISO 12100 und beschreibt verschiedene Verfahren und Instrumente für jeden Prozessschritt. [4, S. 6]

Bei integrierten Fertigungssystemen muss gewährleistet sein, dass manuelle Eingriffe im Betrieb, aber auch bei der Instandhaltung sicher durchgeführt werden können. Fallweise kann es dafür sinnvoll sein, das integrierte Fertigungssystem in mehrere Bereiche zu unterteilen, die einzeln angehalten werden können. So können im jeweiligen Bereich gefahrlos die beabsichtigten Eingriffe durchgeführt werden, ohne jedoch das gesamte System anhalten zu müssen. Die Risikobeurteilung beinhaltet dabei die Spezifikation des IMS, die Identifizierung von Gefährdungen und Gefährdungssituationen sowie die Risikoabschätzung und Risikobewertung. Zusätzlich schließt sie auch die Risikominderung mit ein, die wiederum sämtliche Schutzmaßnahmen sowie deren Validierung umfasst. [3, S. 13]

2.3 Strategie zur Risikominderung

Eine Risikominderung kann grundsätzlich entweder durch Entfernen der Gefährdungen oder aber durch Verringerung mindestens eines der beiden Risikoelemente, Schadensausmaß und Eintrittswahrscheinlichkeit, erzielt werden. Die dazu nötigen Schutzmaßnahmen sind in entsprechender Reihenfolge nach dem sogenannten „Drei-Stufen-Verfahren“ auszuwählen bzw. umzusetzen, dieses Verfahren setzt sich aus den drei Schritten zusammen, welche in Abbildung 2.1 blau markiert sind, in weiterer Folge werden diese Schritte noch genauer betrachtet. [2, S. 29]

2.3.1 Schritt 1: Inhärent sichere Konstruktion

Eine durch entsprechende Konstruktion der Maschine bzw. Auswahl geeigneter Interaktionen zwischen Mensch und Maschine erzielte Risikominderung bezeichnet man als inhärent sichere Konstruktion. In weiterer Folge wird dafür auch der Begriff konstruktive Maßnahme zur Reduktion von Risiken eingeführt. Nur in dieser Phase können Risiken nicht nur gemindert, sondern die Gefährdungen auch gänzlich beseitigt werden, wodurch sich weitere technische oder ergänzende Schutzmaßnahmen erübrigen. [2, S. 29]

Auch eine inhärent sichere Konstruktion für Steuerungen erfolgt durch entsprechende Auswahl der Konstruktionsmerkmale, sodass das Risiko durch deren sicherheitsrelevante Beiträge genügend stark abgemindert wird. Nähere

Informationen dazu finden sich in DIN EN ISO 13849-1 oder DIN EN 62061. [2, S. 35]

Bei verketteten Maschinen gestaltet es sich mitunter schwierig inhärent sichere Konstruktionen anzuwenden, da bereits fertige Maschinen oder fertige unvollständige Maschinen eingesetzt werden und diese nicht geändert werden.

2.3.2 Schritt 2: Technische und ergänzende Schutzmaßnahmen

Sollte durch inhärent sichere Konstruktion eine Beseitigung der Gefährdung bzw. eine ausreichende Risikominderung nicht erzielt werden können, so können entsprechende technische und ergänzende Schutzmaßnahmen eingesetzt werden, um die Ziele der Risikominderung zu erreichen. Dabei sind neben der bestimmungsgemäßen Verwendung auch die vernünftigerweise vorhersehbaren Fehlanwendungen zu berücksichtigen. [2, S. 29]

Für die Auslegung und Anwendung von sicherheitsbezogenen Steuerungen von Maschinen gibt es zwei relevante Normen, die sich zwar voneinander unterscheiden, allerdings bei ordnungsgemäßer Verwendung zu einer vergleichbaren Risikominderung führen. Nach DIN EN ISO 13849-1 werden Steuerungen, die Sicherheitsfunktionen beinhalten, einem von fünf Performance Levels (PL) a bis e zugeordnet. Die Zuteilung erfolgt dabei jeweils entsprechend der Wahrscheinlichkeit eines Ausfalls pro Stunde, der eine Gefährdung verursacht. In DIN EN 62061 werden hingegen anstelle der fünf Performance Level drei Sicherheits-Integritätslevel (SIL) 1 bis 3 eingesetzt. Für Produktnormen (Typ-C-Normen) wird empfohlen, dass Komitees sowohl die erforderlichen PLs als auch SILs einstufen, während Maschinenkonstrukteure je nach Anwendung zwischen Verwendung von ISO DIN EN ISO 13849-1 und DIN EN 62061 wählen können. [5, S. 6], [6, S. 10]

Werden bestimmte Risiken die sich aus den jeweiligen Gefährdungen ergeben, durch die Ausführung von sicherheitsbezogenen Steuerungsfunktionen reduziert, so ist der Sicherheits-Integritätslevel (SIL) für die jeweilige sicherheitsbezogene Steuerungsfunktion zu bestimmen. Der Sicherheits-Integritätslevel wird nach DIN EN 62061 abgeschätzt. Falls jedoch die Risikominderung nicht durch sicherheitsbezogene Steuerungsfunktionen erzielt wird, so ist auch kein Sicherheits-Integritätslevel zu bestimmen. [7, S. 73]

2.3.2.1 Trennende und nichttrennende Schutzeinrichtungen

Die Anforderungen an trennende und nichttrennende Schutzeinrichtungen sind folgende:

- Sie müssen stabil gebaut sein.
- Sie dürfen keine zusätzlichen Gefährdungen hervorrufen.

- Sie dürfen nicht auf einfache Art und Weise umgangen oder unwirksam gemacht werden können.
- Sie müssen in ausreichendem Abstand zum Gefährdungsbereich angebracht werden, genaueres dazu in ISO 13855 und ISO 13857.
- Sie dürfen den Arbeitsprozess nicht unnötig behindern.
- Sie müssen alle wesentlichen Arbeiten für den Einbau oder Wechsel von Werkzeugen und die für Instandhaltungsarbeiten notwendigen Eingriffe ermöglichen, indem ein Zugang nur zu dem Bereich zugelassen wird, in dem die Arbeiten durchzuführen sind, möglichst ohne dass die trennende Schutzeinrichtung entfernt wird oder die nichttrennende Schutzeinrichtung ausgeschaltet wird. [2, S. 49]

Bei nichttrennenden Schutzeinrichtungen muss durch geeignete Konstruktion und Verbindung mit der Steuerung gewährleistet sein, dass diese ordnungsgemäß funktionieren und nicht leicht umgangen werden können. Die Konstruktion der Schutzeinrichtung hat dabei entweder den Grundsätzen aus DIN EN ISO 13849-1 oder DIN EN 62061 zu folgen, oder aber die Auswahl der Schutzeinrichtung entspricht der jeweiligen Produktnorm wie beispielsweise IEC 61496 für aktive optoelektronische Schutzmaßnahmen. [2, S. 51 f]

In Abbildung 2.3 ist dargestellt wann trennende oder nichttrennende Schutzeinrichtungen verwendet werden dürfen. Dies hängt in erster Linie davon ab, wie die Gefährdungssituation entsteht, und ob die Stelle an der die Gefährdung auftritt unzugänglich gemacht werden kann.

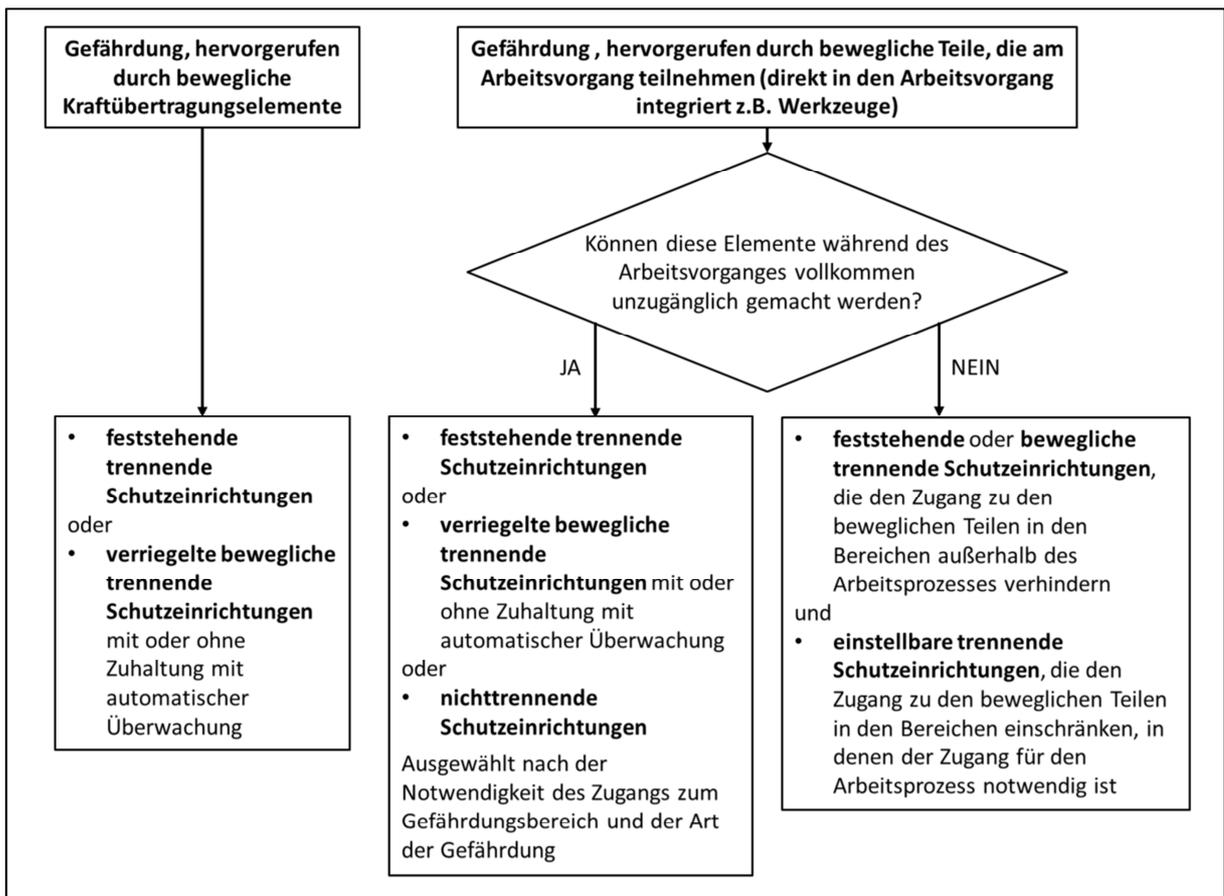


Abbildung 2.3: Auswahl von Schutzeinrichtungen gegen Gefährdungen, die von sich bewegenden Teilen ausgehen [2, S. 44]

2.3.2.2 Bauteile und Bauelemente zum Stillsetzen im Notfall

Ist es notwendig, dass die Maschine im Fall einer Notsituation zum Stillsetzen gebracht werden kann, so müssen die dafür erforderlichen Bauteile und Bauelemente bestimmte Anforderungen erfüllen. Zum einen müssen die Stellteile gut erkenn- und sichtbar sowie schnell zugänglich sein. Zusätzlich muss der Vorgang, der die Gefährdung bewirkt, möglichst rasch gestoppt werden können, ohne dadurch jedoch weitere Gefährdungen zu verursachen. Andernfalls sollte erneut überdacht werden, ob die Methode der Stillsetzung im Notfall die beste Möglichkeit zur Risikominderung darstellt. Dabei kann es unter Umständen notwendig sein, dass durch die Auslösung des Stillsetzens im Notfall zusätzliche Bewegungen, die die Maschine in einen sicheren Zustand führen, eingeleitet werden. Die Auswirkungen des Befehls der Stillsetzung müssen auch dann noch aufrechterhalten bleiben, wenn dadurch die Einrichtung, die die Stillsetzung durchführt, nicht mehr aktiv ist. Erst durch eine Rückstellung des Befehls darf ein erneuter Start der Maschine zugelassen werden. Die Rückstellung darf dabei ausschließlich an jener Stelle, an der der Befehl zur Stillsetzung erfolgt ist, durchgeführt werden können und nicht zu einem direkten Wiederanlaufen der Maschine führen. [2, S. 53]

2.3.2.3 Wiederanlauf nach einem Not-Halt

Der Stoppzustand muss nach Eingabe des Befehls so lange aufrechterhalten bleiben, bis ein sicherer Zustand für einen Wiederanlauf gewährleistet werden kann. Dabei wird der Stoppbefehl durch die Rückstellung der Schutzeinrichtung und die damit verbundene Wiederherstellung der Sicherheitsfunktion aufgehoben. Entsprechend der Risikobeurteilung kann es dafür notwendig sein, dass eine manuelle Rückstellung durchgeführt werden muss, die eine separate und beabsichtige manuelle Handlung darstellt. [6, S. 44], [8, S. 45]

Die manuelle Rückstellung hat dabei an einem getrennten, manuell zu bedienendem Gerät im sicherheitsbezogenen Teil der Steuerung zu erfolgen, wobei dies nur dann möglich sein darf, wenn sämtliche Sicherheitsfunktionen und Schutzeinrichtungen funktionsfähig sind. Dabei darf jedoch keine Bewegung oder Gefährdungssituationen verursacht werden. Zusätzlich muss es durch Ausführung der manuellen Rückstellfunktion für die Steuerung möglich sein, einen separaten Startbefehl anzunehmen. Die Ausführung der manuellen Rückstellung hat dabei erst durch Loslassen des Betätigungselements nach dessen Betätigung zu erfolgen. [6, S. 44], [8, S. 46]

Damit die Einbeziehung der manuellen Rückstellfunktion nicht zu einer Minderung der Sicherheit führt, muss der Performance Level sämtlicher zugehöriger sicherheitsrelevanter Teile entsprechend hoch gewählt werden. [6, S. 44]

Um sicherzustellen, dass sich keine Person im Gefahrenbereich befindet, hat sich das Betätigungselement für die manuelle Rückstellung an einer Position zu befinden, die zwar außerhalb des Gefahrenbereiches liegt, gleichzeitig aber einen guten Überblick über den gesamten Gefahrenbereich bietet. Ist dies nicht möglich, ist ein spezielles Rückstellverfahren notwendig. [6, S. 44]

2.3.3 Schritt 3: Benutzerinformation

Die Benutzerinformation muss auf sämtliche Restrisiken hinweisen, die trotz inhärent sicherer Konstruktion und Einsatz technischer und ergänzender Schutzmaßnahmen verbleiben. Darüber hinaus muss sie den Benutzer über das Risiko, welches durch vernünftigerweise vorhersehbare Fehlanwendungen entsteht, informieren und ihn davor warnen. Dabei müssen ausreichende Angaben inklusive Warnhinweise zu den in den jeweiligen Lebensphasen der Maschine verbleibenden Restrisiken gemacht werden. Außerdem muss die Benutzerinformation die Arbeitsverfahren und die empfohlenen Verfahren für ein sicheres Arbeiten mit der Maschine sowie die dazu nötigen Ausbildungsanforderungen für sämtliche Personen, einschließlich Bedienpersonal, die den von der Maschine ausgehenden Gefährdungen ausgesetzt sein könnten, enthalten. Darüber hinaus muss sie auch Informationen zur jeweils erforderlichen persönlichen Schutzausrüstung, deren Anwendung und der dazu

notwendigen Ausbildung enthalten. Gegebenenfalls muss die Benutzerinformation auch Informationen über trennende bzw. nichttrennende Schutzeinrichtungen, die benötigt werden, enthalten. Dabei stellt die Benutzerinformation jedoch keinen Ersatz für die inhärent sichere Konstruktion, technische sowie ergänzende Schutzmaßnahmen dar. [2, S. 29, 55]

Das Erstellen der Benutzerinformation stellt einen wichtigen Aspekt bei der Konstruktion einer Maschine dar. Mittels Texten, Wörtern, Zeichen, Signalen, Symbolen und Diagrammen werden die Informationen an gewerbliche und/oder private Benutzer übermittelt, wobei die genaue Strukturierung und Präsentation auch in IEC 62079 geregelt ist. [2, S. 55]

Die relevanten Lebensphasen, die in der Benutzerinformation behandelt werden müssen, sind Transport, Installation, in Betrieb nehmen und Verwendung der Maschine sowie unter Umständen Demontage, Außerbetriebnahme und Entsorgung. [2, S. 55]

Die Angabe der Informationen kann dabei jeweils in Abhängigkeit vom Risiko, wann die Information vom Benutzer benötigt wird, und der Maschinenkonstruktion entweder auf bzw. in der Maschine selbst, in Begleitunterlagen wie der Betriebsanleitung, auf der Verpackung oder außerhalb der Maschine erfolgen. Letzteres beinhaltet dabei beispielsweise Signale und Warnhinweise, wobei für wichtige Mitteilungen auch Standardformulierungen entsprechend IEC 62079 gut geeignet sind. [2, S. 56]

2.4 Dokumentation zur Risikobeurteilung und Risikominderung

In der Dokumentation zur Risikobeurteilung bzw. Risikominderung müssen das eingesetzte Verfahren und die erzielten Ergebnisse festgehalten werden. Die Dokumentation erfolgt dabei entsprechend Abschnitt 7 der DIN EN ISO 12100. Sie beinhaltet für die Maschine, für die die Risikobeurteilung durchgeführt worden ist, sämtliche relevanten Annahmen, die dazu gemacht worden sind, alle identifizierten Gefährdungen und Gefährdungssituationen sowie die betrachteten Gefährdungsereignisse. Außerdem sind die verwendeten Daten inklusive deren Quellen und die damit verbundenen Unsicherheiten einschließlich ihrer Auswirkungen auf die Risikobeurteilung anzugeben. Darüber hinaus sind die angewendeten Schutzmaßnahmen einschließlich Verweise auf Normen oder andere Spezifikationen, die zu deren Auswahl verwendet worden sind, sowie die zu erreichenden Risikominderungsziele, die Restrisiken und das Ergebnis der Risikobeurteilung zu dokumentieren. Zusätzlich sollten sämtliche während der Risikobeurteilung ausgefüllten Formulare in der Dokumentation enthalten sein. Die

DIN EN ISO 12100 schreibt nicht vor, dass die Dokumentation zur Risikobeurteilung zusammen mit der Maschine zu übergeben ist. [2, S. 60 f]

2.5 Festsetzung eines Sicherheits-Integritätslevels zur Risikominderung

Wie in 2.3.2 bereits erwähnt, sind für jene Risiken, die mit einer sicherheitsbezogenen Steuerungsfunktion reduziert werden, Sicherheits-Integritätslevel für die entsprechende sicherheitsbezogene Steuerungsfunktion zu bestimmen. In Tabelle 2.1 ergibt sich eine entsprechende Zuweisung eines Sicherheits-Integritätslevels für eine bestimmte Gefährdung. Die in Tabelle 2.1 gelb gekennzeichneten Bereiche sollten als Empfehlung betrachtet werden, dass andere Maßnahmen (AM) angewendet werden sollten. Das mit der identifizierten Gefährdung verbundene Risiko wird dabei mit den Parametern S (schwere des möglichen Schadens) und K (Klasse der Wahrscheinlichkeit des Schadens) abgeschätzt. Die Klasse der Wahrscheinlichkeit des Schadens K setzt sich nach (Gl. 2.1) zusammen, die dabei verwendeten Parameter sind wie folgt definiert: [7, S. 74]

- F ... Häufigkeit und Dauer der Exposition von Personen zur Gefährdung
- W ... Wahrscheinlichkeit des Auftretens eines gefahrbringenden Ereignisses
- P ... Möglichkeit zur Vermeidung oder Begrenzung des Schadens

$$K = F + W + P \quad (\text{Gl. 2.1})$$

Wenn jedoch eine Produktnorm (Typ-C Norm) ein bestimmtes Sicherheits-Integritätslevel für eine Sicherheitsbezogene Steuerungsfunktion festlegt, dann muss diese Festlegung Vorrang gegenüber der oben beschriebenen Festlegung haben. [7, S. 28]

Schwere (S)	Klasse (K = F + W + P)				
	4	5 bis 7	8 bis 10	11 bis 13	14 bis 15
4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
3		(AM)	SIL 1	SIL 2	SIL 3
2			(AM)	SIL 1	SIL 2
1				(AM)	SIL 1

Tabelle 2.1: Matrix zur Festlegung des SIL [7, S. 78]

2.5.1 Klassifikation der Schwere S

Die Schwere von Verletzungen oder gesundheitlichen Schäden kann abgeschätzt werden, indem reversible Verletzungen, irreversible Verletzungen und Tod in Betracht gezogen werden. Es wird die passende Stufe der Schwere aus Tabelle 2.2, basierend auf den Folgen einer möglichen Verletzung ausgewählt. [7, S. 74]

Auswirkungen	Schwere (S)
irreversibel: Tod, Verlust eines Auges oder Arms	4
irreversibel: gebrochene Gliedmaßen, Verlust eines oder mehrerer Finger	3
reversibel: Behandlung durch einen Mediziner erforderlich	2
reversibel: Erste Hilfe erforderlich	1

Tabelle 2.2: Klassifikation der Schwere (S) [7, S. 74]

Wobei die einzelnen Stufen genauer beschrieben sind durch:

- 1 Eine kleinere Verletzung, einschließlich Schrammen und kleinere Quetschungen, sodass es der Behandlung im Rahmen Erster Hilfe bedarf.
- 2 Eine reversible Verletzung, einschließlich schwerer Fleischwunden, Stichwunden und schwerer Quetschungen, sodass es der Behandlung durch einen Mediziner bedarf.
- 3 Eine größere oder irreversible Verletzung, die derart ausfällt, dass es möglich ist, die gleiche Arbeit nach Heilung beizubehalten. Dies kann auch eine schwere größere, jedoch reversible Verletzung, wie z. B. gebrochene Gliedmaßen, einschließen.
- 4 Eine tödliche oder bedeutende irreversible Verletzung, sodass es schwierig sein wird, die gleiche Arbeit nach Heilung beizubehalten, wenn Heilung überhaupt möglich ist. [7, S. 74]

2.5.2 Klassifikation der Wahrscheinlichkeit des Auftretens des Schadens K

Die Wahrscheinlichkeit des Auftretens des Schadens setzt sich aus den drei Parametern Häufigkeit und Dauer der Exposition (F), Wahrscheinlichkeit des Auftretens des gefahrbringenden Ereignisses (W) und Wahrscheinlichkeit der Vermeidung oder Begrenzung des Schadens (P) zusammen. In (Gl. 2.1) ist der einfache Zusammenhang dargestellt. [7]

2.5.2.1 Häufigkeit und Dauer der Exposition F

Um den Grad der Exposition zu bestimmen sind zwei Aspekte zu betrachten, die im Folgenden beschrieben werden. Zum einen die Notwendigkeit des Zugangs zum Gefahrenbereich basierend auf allen Betriebsarten (z. B. Automatikbetrieb, Instandhaltung). Als zweiter Aspekt ist die Art des Zuganges zu betrachten, z. B.

manuelles Bestücken von Rohmaterial oder Durchführung von Einstellungen. Dadurch sollte es möglich sein, den mittleren Zeitabstand zwischen Expositionen und somit die mittlere Häufigkeit des Zugangs einzuschätzen. [7, S. 75]

Außerdem sollte es möglich sein, die Dauer vorherzusehen, wie lange die Exposition im Gefahrenbereich andauern wird. Falls die Dauer kleiner als 10 Minuten ist, so kann der Wert des Parameters in Tabelle 2.3 jeweils auf die Zahl eine Reihe darunter herabgestuft werden. Ist jedoch die Häufigkeit der Exposition ≥ 1 pro Stunde, so ist der Wert für die Häufigkeit und Dauer der Exposition (F) nie herabzustufen. [7, S. 75]

Häufigkeit und Dauer der Exposition (F)	
Häufigkeit der Exposition	Dauer > 10 min
≥ 1 pro h	5
< 1 pro h bis ≥ 1 pro Tag	5
< 1 pro Tag bis ≥ 1 pro 2 Wochen	4
< 1 pro 2 Wochen bis ≥ 1 pro Jahr	3
< 1 pro Jahr	2

Tabelle 2.3: Häufigkeit und Dauer der Exposition [7, S. 75]

2.5.2.2 Wahrscheinlichkeit des Auftretens des gefahrbringenden Ereignisses W

Die Wahrscheinlichkeit für das Auftreten eines gefahrbringenden Ereignisses W muss abgeschätzt werden, wobei dies unabhängig von den anderen beiden Parametern Häufigkeit und Dauer der Exposition (F) und Wahrscheinlichkeit der Vermeidung oder Begrenzung des Schadens (P) erfolgen sollte. Mittels Worst-Case-Annahmen für jeden Parameter kann dann sichergestellt werden, dass der Sicherheits-Integritätslevel (SIL) der sicherheitsbezogenen Steuerungsfunktionen ausreichend hoch ist. Dabei ist die Verwendung einer aufgabenorientierten Analyse empfehlenswert. [7, S. 75]

Bei der Abschätzung der Wahrscheinlichkeit des Auftretens eines gefährdenden Ereignisses (W) sind mehrere Faktoren zu berücksichtigen.

Zum einen spielt die Vorhersagbarkeit des Verhaltens der Maschine bzw. der relevanten Bauteile und des verarbeiteten Materials während verschiedener Formen der Nutzung wie beispielsweise Normalbetrieb, Instandhaltung und Fehlersuche eine wichtige Rolle. Insbesondere muss das Steuerungssystem in Bezug auf das Risiko eines unerwarteten Anlaufens berücksichtigt werden. Nicht zu berücksichtigen sind hingegen die Schutzwirkungen von sicherheitsbezogenen elektrischen Steuerungsteilen, damit auch das Risiko, das bei deren Ausfall entstehen würde, miteinbezogen wird. Die Vorhersehbarkeit der Maschine korreliert dabei häufig mit der Komplexität der Funktionen der Maschine, jedoch können unvorhersehbare

Ereignisse auch bei ansonsten sehr vorhersehbarem Verhalten der Maschine nicht vernachlässigt werden. [7, S. 76]

Zum anderen ist auch festgelegtes oder vorhersehbares menschliches Verhalten in Wechselwirkung mit Teilen der Maschine und mit Bezug auf die Gefährdung zu berücksichtigen. Die wesentlichen Faktoren sind dabei Stress und fehlende Kenntnis von Informationen in Bezug auf die Gefährdung, wobei diese Informationen der Gefährdung ausgesetzten Personen in der jeweiligen Situation bewusst sein müssen. Dabei stellen unter anderem Geschicklichkeit, Ausbildung, Erfahrung und Komplexität der Maschine bzw. des Prozesses entscheidende Einflussfaktoren dar. Sämtliche jeweils erforderlichen Kenntnisse und Fähigkeiten sind in der Benutzerinformation aufzulisten. Die Abschätzung, wann vernünftigerweise kein vollständiges Bewusstsein über alle Gefährdungen angenommen werden kann, erfolgt dabei mittels genauer Analyse der Aufgaben und Tätigkeiten. Eine sehr hohe Wahrscheinlichkeit für das Auftreten eines gefährdenden Ereignisses sollte für normale Produktionszwänge sowie für Worst-Case-Szenarien gewählt werden, wobei eine Verringerung des Wertes nur unter genauer Angabe von Gründen, wie beispielsweise detailliert beschriebene Anwendung und hohes Niveau der Kenntnisse über die Anwenderfähigkeiten, erfolgen darf. [7, S. 76]

Die Wahrscheinlichkeit des Auftretens des gefahrbringenden Ereignisses (W) wird dabei entsprechend Tabelle 2.4 von vernachlässigbar bis sehr hoch mit den Zahlenwerten 1 bis 5 bewertet. [7, S. 76]

Wahrscheinlichkeit des Auftretens	Wahrscheinlichkeit (W)
sehr hoch	5
wahrscheinlich	4
möglich	3
selten	2
vernachlässigbar	1

Tabelle 2.4: Klassifikation der Wahrscheinlichkeit W , [7, S. 76]

2.5.2.3 Wahrscheinlichkeit der Vermeidung oder Begrenzung des Schadens P

Die Wahrscheinlichkeit der Vermeidung oder Begrenzung des Schadens (P) ist abhängig von Aspekten der Maschinenkonstruktion und der geplanten Anwendung der Maschine, die zu einer Vermeidung oder Begrenzung des Schadens durch eine Gefährdung führen können. Wichtig ist dabei, ob das gefährdende Ereignis plötzlich, schnell oder langsam auftritt und aus räumlicher Sicht die Möglichkeit besteht, sich von der Gefährdung ausreichend wegzubewegen. Zusätzlich ist auch die Beschaffenheit des Bauteils oder Systems entscheidend und ob es möglich ist, die Gefährdungen zu erkennen oder nicht, weil diese beispielsweise durch gewisse

Umgebungsbedingungen wie Lärm überdeckt werden könnten oder aber bestimmte Instrumente wie z. B. Geräte zur Spannungsmessung dazu notwendig wären. [7, S. 76 f]

Die Wahrscheinlichkeit der Vermeidung oder Begrenzung des Schadens wird entsprechend Tabelle 2.5 mit den Zahlenwerten 1, 3 oder 5 bewertet. [7, S. 77]

Wahrscheinlichkeit der Vermeidung oder Begrenzung des Schadens (P)	
unmöglich	5
selten	3
wahrscheinlich	1

Tabelle 2.5: Klassifikation der Wahrscheinlichkeit der Vermeidung oder Begrenzung des Schadens P, [7, S. 77]

2.6 Bestimmung des erforderlichen Performance-Levels für eine Sicherheitsfunktion

Eine andere Möglichkeit zur Auswahl der entsprechenden Sicherheitsfunktion für die Gestaltung und Integration sicherheitsbezogener Teile von Steuerungen ist, den Performance-Level für die jeweilige Sicherheitsfunktion zu bestimmen. Der erforderliche Performance Level für die jeweilige sicherheitsbezogene elektrische Steuerfunktion, kann anhand eines Graphen, siehe Abbildung 2.4, bestimmt werden. Dies erfolgt anhand eines Entscheidungsbaumes und berücksichtigt alle notwendigen Risikoparameter auf einfache Weise. Im Gegensatz zum Sicherheits-Integritätslevel, der nur für sicherheitsbezogene elektrische, elektronische und programmierbare elektronische Steuerungssysteme für Maschinen gilt, ist der Performance-Level technologieunabhängig. [6, S. 11], [7, S. 10]

Der Performance-Level drückt die Fähigkeit von sicherheitsbezogenen Teilen, eine Sicherheitsfunktion auszuführen, aus. [6, S. 27]

Die Beziehung zwischen Performance-Level und Sicherheits-Integritätslevel ist in Tabelle 2.6 dargestellt.

PL	SIL
a	keine Entsprechung
b	1
c	1
d	2
e	3

Tabelle 2.6: Beziehung zwischen PL und SIL [6, S. 29]

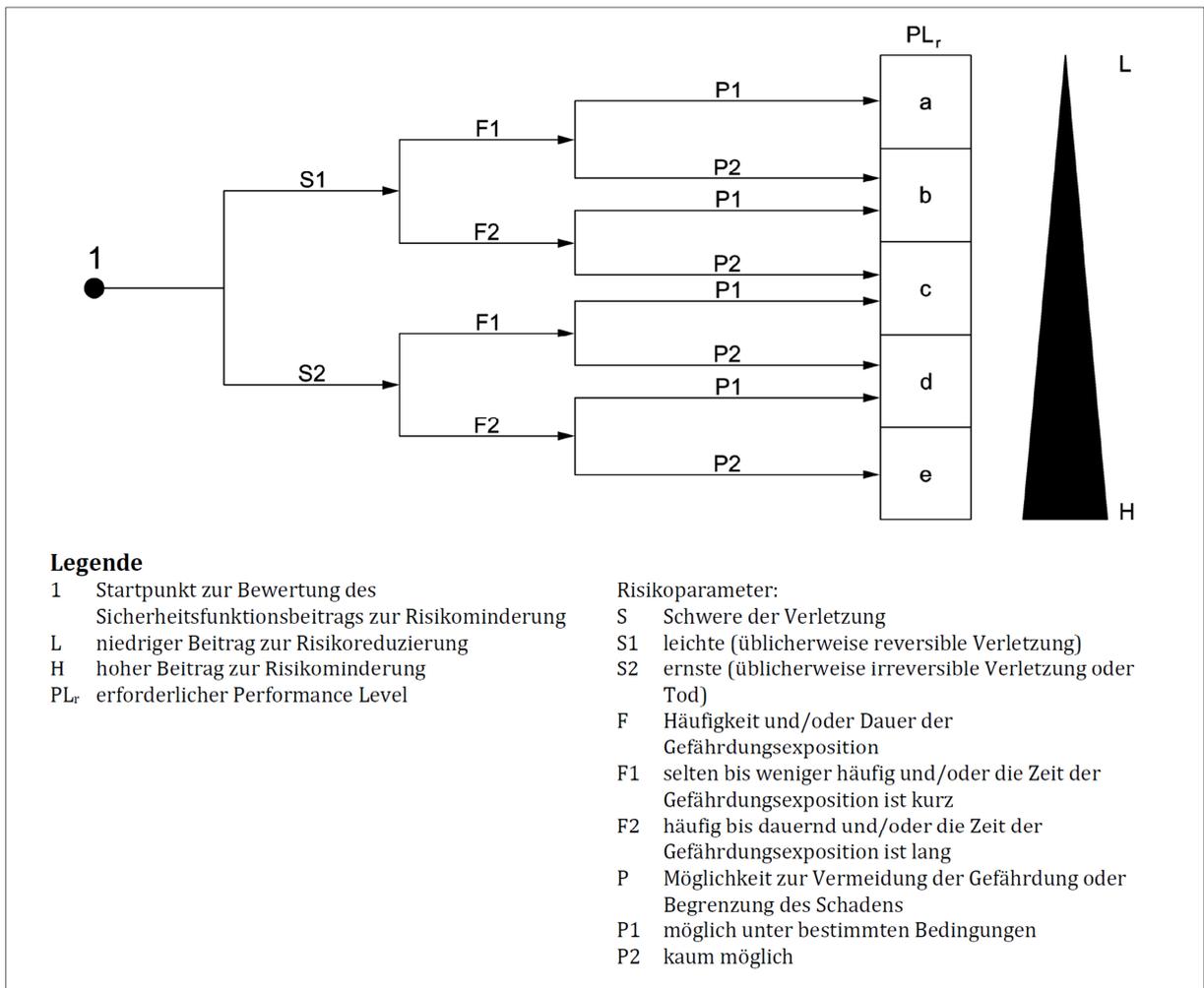


Abbildung 2.4: Graph zur Bestimmung des erforderlichen PL [6, S. 63]

2.7 Gesamtvalidierung

Als Gesamtvalidierung kann der Prozess nach der Umsetzung aller laut Risikobeurteilung erforderlichen Maßnahmen gesehen werden. Dabei wird das umgesetzte Sicherheitskonzept auf Vollständigkeit und Wirksamkeit geprüft. Es wird also kontrolliert, ob die Maßnahmen tatsächlich so umgesetzt wurden, wie geplant, und ob bei bestimmten Handlungen sämtliche geplante Ereignisse eintreten. [1, 5-1]

Zusätzlich sollte, falls nichttrennende Schutzeinrichtungen zur Risikominderung eingesetzt werden, eine Nachlaufzeitenmessung durchgeführt werden. Eine Nachlaufzeitenmessung stellt fest, ob die vorgesehenen Sicherheitsabstände für die nichttrennenden Schutzeinrichtungen für die reale Maschine ausreichend groß sind. Dies ist notwendig, um zu garantieren, dass die Maschine bei der Annäherung einer Person rechtzeitig abschaltet bzw. in einen sicheren Zustand übergeht und somit das Risiko für eine sich annähernde Person ausreichend reduziert ist. Diese Messungen und Kontrollen sollten in einem Protokoll festgehalten werden und den technischen Unterlagen für die Maschine beigelegt werden.

2.8 CE-Zertifizierung

Nachdem die Konformität, eventuell unter Einbeziehung einer externen Prüfstelle, im Rahmen einer Gesamtvalidierung festgestellt wurde, kann die EG-Konformitätserklärung ausgestellt und das CE-Zeichen an der Maschine angebracht werden. Die EG-Konformitätserklärung ist Teil der technischen Unterlagen, die für mindestens 10 Jahre ab dem Tag der Fertigstellung der ersten Maschine bzw. bei Serienfertigung 10 Jahre nach dem Tag der Fertigstellung der letzten Einheit aufbewahrt werden müssen. [1, 6-1], [9, Anhang VII]

Die Konformitätsbewertung durch eine interne Fertigungskontrolle bei der Herstellung von Maschinen erfolgt für alle Maschinen bis auf jene, die in der Maschinenrichtlinie unter Anhang IV gelistet sind. Dabei sind die Maschinen unter Anhang IV für automatisierte Fertigungszellen, in denen Metallwerkstoffe bearbeitet werden, eher nicht relevant. In Anhang IV sind beispielsweise Maschinen wie etwa Holzbearbeitungsmaschinen oder Maschinen für unter Tage gelistet. [9, Anhang VIII]

Um die Konformität bewerten zu können, ist es notwendig, dass alle technischen Unterlagen für die Maschine wie in Anhang VII der Maschinenrichtlinie beschrieben, vorhanden sind. Zusätzlich muss der Hersteller alle erforderlichen Maßnahmen ergreifen, damit durch den Herstellungsprozess gewährleistet ist, dass die hergestellten Maschinen den technischen Unterlagen entsprechen. Wird dies erfüllt, so stellt der Hersteller eine EG-Konformitätserklärung aus. Wie die EG-Konformitätserklärung aufgebaut sein muss, ist in Anhang II der Maschinenrichtlinie ausführlich beschrieben. [9]

Werden jedoch Maschinen speziell für Forschungszwecke konstruiert und gebaut und sind nur zur vorübergehenden Verwendung in Laboratorien bestimmt, so sind diese Maschinen vom Anwendungsbereich der Maschinenrichtlinie ausgenommen. Das bedeutet auch, dass alle Anforderungen an die Maschinenrichtlinie, wie etwa die CE-Zertifizierung, für solche Maschinen nicht erfüllt werden müssen. [9, Artikel 1 Absatz 2]

3 Risikobeurteilung in der Pilotfabrik

Die Risikobeurteilung für den entsprechenden Bereich der Pilotfabrik wird wie in Abschnitt 2 beschrieben durchgeführt. Durch Anwendung der in Abschnitt 2 beschriebenen Normen werden alle Sicherheitsanforderungen und Gesundheitsanforderungen der Maschinenrichtlinie 2006/42/EG betrachtet. Im Anschluss an die Risikobeurteilung erfolgt die Risikominderung aller Gefährdungen nach dem in Abschnitt 2 beschriebenen „Drei-Stufen-Verfahren“. Für die gewählten Sicherheitsfunktionen, sofern diese durch sicherheitsbezogene Steuerungsfunktionen realisiert werden, wird der erforderliche Sicherheits-Integritätslevel nach DIN EN 62061 bzw. der erforderliche Performance Level nach DIN EN ISO 13849-1 bestimmt. Auf Basis der erforderlichen Sicherheits-Integritätslevel bzw. Performance Level werden die Sicherheitsbauteile ausgewählt.

3.1 Klassifikation des Fertigungsbereichs

Die Pilotfabrik der TU Wien in der Seestadtstraße 27, 1220 Wien teilt sich in unterschiedliche Bereiche, für die unterschiedliche Institute der TU Wien zuständig sind. Für diese Arbeit wird nur der Bereich in der Pilotfabrik des Instituts für Fertigungstechnik und Photonische Technologien der TU Wien betrachtet.

Der Bereich des Instituts für Fertigungstechnik und Photonische Technologien (IFT) in der Pilotfabrik besteht aus einer Drehzelle und einer Hybridbearbeitungszelle. Die räumliche Anordnung für den Bereich des IFT kann in Abbildung 3.1 betrachtet werden und stellt somit auch den Ausgangszustand ohne jegliche Risikomindernde Maßnahmen dar.

Die Hybridbearbeitungszelle besteht aus einem 5-Achs Bearbeitungszentrum, einer IGM-Schweißzelle mit 6-Achs Schweißroboter plus Dreh- und Schwenktisch und einem ABB IRB 6620 Industrieroboter, der zur Handhabung von Nullpunktspannsystem-Paletten, auf denen die Werkstücke aufgespannt sind, dient. Somit kann die additive Fertigung (Auftragsschweißen) mit der Fräsbearbeitung kombiniert werden. Durch Verwendung eines Nullpunktspannsystems ist ein Wechsel zwischen den beiden Verfahren jederzeit möglich.

Die Drehzelle besteht aus einer CNC-Drehmaschine, einer Wellenmessmaschine, einem ABB IRB 2600 Industrieroboter zur Handhabung von einzelnen Drehteilen und einem Portal, das zur Handhabung von Paletten dient. Die Paletten dienen zur Lagerung von fertigen Drehteilen bzw. Rohmaterial.

Der Materialtransport im Fertigungsbereich erfolgt durch ein fahrerloses Transportsystem (FTS), auf dem sowohl die Nullpunktspannsystem-Paletten, der

Hybridbearbeitungszelle als auch die Materialpaletten der Drehbearbeitungszelle transportiert werden können.

Zusätzlich ist ein Rüstplatz außerhalb der Fertigungszelle vorgesehen und wird daher in sämtlichen Abbildungen dieser Arbeit nicht dargestellt. An diesem Rüstplatz kann das FTS durch einen Bediener be- und entladen werden.

3.2 Anordnung der verketteten Maschinen

In Abbildung 3.1 ist die Anordnung der Maschinen und unvollständigen Maschinen schematisch dargestellt. Dabei wird der gesamte Fertigungsbereich (in Abbildung 3.1 rot markiert) dargestellt, der sich aus zwei Fertigungszellen, einer Drehzelle (blau markiert) und einem Hybridbearbeitungszentrum (grün markiert) zusammensetzt. Das FTS ist in der Abbildung dreimal eingezeichnet, um die möglichen Endpositionen besser zu erkennen, dies bedeutet jedoch nicht, dass mehrere FTS im Einsatz sind.

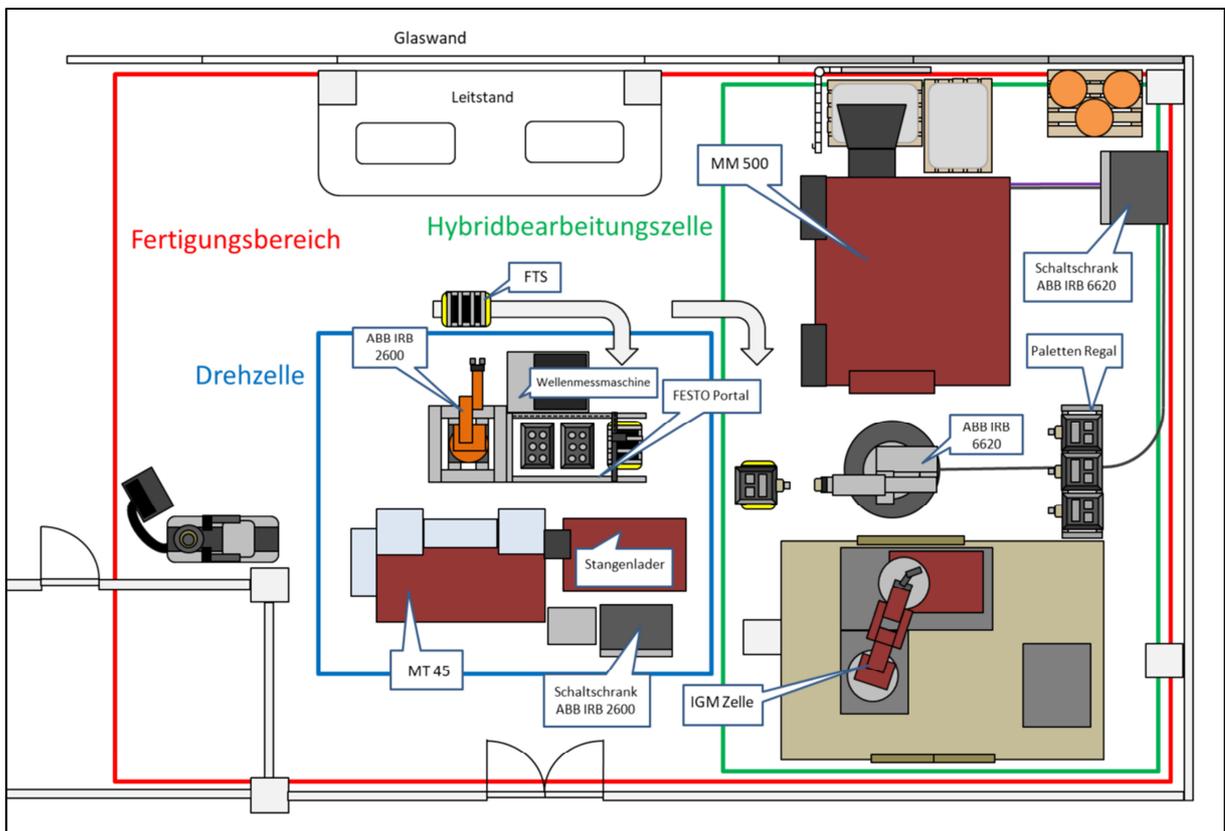


Abbildung 3.1: Anordnung der verketteten Maschinen

3.3 Grenzen der Maschine (Fertigungsbereich)

In diesem Kapitel erfolgt die Beschreibung sämtlicher Maschinen bzw. unvollständigen Maschinen, sowie deren Grenzen im Rahmen der Betrachtung als Gesamtheit in weiterer Folge Fertigungsbereich genannt. Alle Maschinen bzw.

unvollständigen Maschinen sind in Kapitel 3.3.1 bis Kapitel 3.3.3 aufgelistet und beschrieben.

Es werden außerdem alle Lebensphasen und Arbeitsgänge in den jeweiligen Lebensphasen des Fertigungsbereichs beschrieben und aufgeführt, sofern diese nicht in den einzelnen Dokumenten der Maschinen bzw. unvollständigen Maschinen beschrieben sind.

3.3.1 Identifikation der verketteten Maschinen der Drehzelle

Die Drehzelle dient zur Herstellung und Vermessung von Drehteilen. Die Ablage der fertig bearbeiteten Drehteile erfolgt in einem flexibel anpassbarem Palettenmagazin. Das Festo-Portal kann die Paletten von dem FTS aufnehmen bzw. diese auf das FTS ablegen und für die zwischenzeitliche Lagerung der Paletten genutzt werden. Die Paletten für die fertigen Drehteile bzw. das Rohmaterial sind nach DIN 24602 ausgeführt. In Abbildung 3.2 ist der Aufbau der Drehzelle dargestellt, jedoch noch ohne Wellenmessmaschine. In weiterer Folge sind alle zur Drehzelle zugehörigen Maschinen bzw. unvollständigen Maschinen aufgeführt und beschrieben.



Abbildung 3.2: Drehzelle ohne Wellenmessmaschine

3.3.1.1 Daten der Maschine MAXXTURN 45

Die MT 45 ist ein CNC-Drehzentrum mit Gegenspindel, angetriebenen Werkzeugplätzen und C-Achse.

Hersteller:	EMCO MAIER Ges.m.b.H.
Typ:	MAXXTURN 45
Maschinen-Nr.:	S4C124001
Baujahr:	2012

Tabelle 3.1: Daten der Maschine MT 45

3.3.1.2 Daten der Maschine LM 1200 Stangenlader

Mit dem EMCO LM 1200 Stangenlader kann der MT 45 Stangenmaterial bis zu 1200 mm Länge vollautomatisch zugeführt werden.

Hersteller:	MKE Metall & Kunststoffwaren Erzeugung Ges.m.b.H.
Typ:	EMCO LM1200
Geräte-Nr.:	E 0732
Baujahr:	2012

Tabelle 3.2: Daten der Maschine Stangenlader

3.3.1.3 Daten der unvollständigen Maschine ABB IRB 2600

Der ABB IRB 2600 besitzt eine Armreichweite von 1,65 m und kann eine maximale Masse von 20 kg bewegen.

Zusätzlich besitzt er eine Anhaltezeit von 250 ms für einen Not Halt der Kategorie 0. Diese Zeit ist bei maximaler Geschwindigkeit, maximaler Beladung und maximal ausgestreckten Arm gültig. [10, S. 182]

Der ABB IRB 2600, der in der Pilotfabrik steht, ist mit einer älteren Version von SafeMove ausgestattet, das über I/O Signale an die Sicherheitssteuerung angebunden ist und nicht über PROFIsafe wie beim ABB IRB 6620.

SafeMove erfüllt in Kombination mit der Robotersteuerung den Performance-Level PL d bzw. den Sicherheits-Integritätslevel SIL 2. [11, S. 219]

Die Stopp-Kategorie 0 entspricht einem Stillsetzen durch sofortiges Unterbrechen der Energiezufuhr zu den Antriebselementen der Maschinen. Ein zusätzliches Bremsen der Antriebselemente kann erforderlich sein. [12, S. 12]

Im Gegensatz dazu entspricht die Stopp-Kategorie 1 einem Stillsetzen von Bewegungen und Funktionen mit beibehaltener Energiezufuhr zu den Maschinen Antriebselementen und anschließender Unterbrechung der Energiezufuhr. [12, S. 13]

Hersteller:	ABB Robotics
Typ:	IRB 2600
Maschinen-Nr.:	26M-64744
Baujahr:	2012

Tabelle 3.3: Daten der unvollständigen Maschine IRB2600

3.3.1.4 Daten des Greifer-Schnellwechselsystems

Auf dem Roboterflansch des ABB IRB 2600 wird ein Schnellwechselsystem der Fa. Schunk verwendet. Dadurch wird ein automatisierter Greiferwechsel ermöglicht. Das Schnellwechselsystem wird pneumatisch entriegelt. Durch einen selbsthemmenden Verriegelungsmechanismus ist für das Halten des Greifers keine Druckluft erforderlich.

Hersteller:	Schunk
Typ:	SWS 020
Maschinen-Nr.:	SWK 20 302322; SWA 20 302323

Tabelle 3.4: Daten des Schnellwechselsystems

3.3.1.5 Daten der unvollständigen Maschine FESTO-Portal

Das Festo-Portal dient zum Handhaben von Paletten für die Drehzelle und zum Be- und Entladen des FTS. Dabei werden Paletten die an die DIN 24602 angelehnt sind verwendet. Die Paletten dienen zum geordneten Speichern von fertigen Drehteilen bzw. von Rohmaterial.

Das Festo-Portal wurde teilmontiert geliefert und entspricht einer unvollständigen Maschine. Die Steuerung für das Portal wird vom IFT entwickelt. Da es im Betrieb nicht notwendig ist, hohe Verfahrgeschwindigkeiten des Portals zu realisieren, wird die maximale Geschwindigkeit des Festo-Portals durch die Steuerung auf einen Bruchteil der theoretisch möglichen Geschwindigkeit reduziert. Somit besitzt das Portal im Vergleich zum benachbarten ABB IRB 2600 vernachlässigbar geringe Anhaltezeiten. Aus diesem Grund wird die Anhaltezeit des Festo-Portals für die weiterfolgenden Berechnungen der minimal erforderlichen Sicherheitsabstände nicht berücksichtigt.

Hersteller:	FESTO (IFT)
Typ:	Linear-Portal
Baujahr:	2018

Tabelle 3.5: Daten der unvollständigen Maschine Festo Portal

3.3.1.6 Daten der Wellenmessmaschine Opticline C 308

Die Opticline C 308 Wellenmessmaschine ist eine optische Messmaschine zur Messung von rotationssymmetrischen Werkstücken und für den Einsatz in der Fertigung geeignet. Mit dieser Messmaschine sind Werkstücke mit einem maximalen Durchmesser von 80 mm und einer Länge von bis zu 300 mm messbar.



Abbildung 3.3: Wellenmessmaschine Opticline C 308

Hersteller:	JENOPTIK Industrial Metrology Germany GmbH
Typ:	Wellenmesssystem Opticline C 308
Mat.-No.:	636013
Ser.-No.:	10 3764 19
Baujahr:	2019

Tabelle 3.6: Daten der Maschine Wellenmessmaschine

3.3.2 Identifikation der verketteten Maschinen der Hybridbearbeitungszelle

Die Hybridbearbeitungszelle vereint die additive Fertigung mittels robotergestütztem CMT-Auftragsschweißen und dem Fräsen in einer 5-Achs CNC-Fräsmaschine. Der Wechsel der Bauteile von einer Station zur nächsten wird durch einen ABB IRB 6620 ausgeführt. Um die Bauteile nach dem Schweißprozess auskühlen zu lassen oder

um Paletten zwischenspeichern zu können, ist hinter dem ABB IRB 6620 ein Palettenregal, welches bis zu 9 Paletten aufnehmen kann, angebracht. Für einen vollautomatischen Werkstückwechsel wird ein Nullpunktspannsystem der Firma Schunk verwendet. Der Roboter ist ebenfalls mit einem pneumatisch betätigten Greifer NSR 160 von der Firma Schunk ausgestattet um die Nullpunktspannsystem-Paletten zu greifen. Die MAXXMILL 500 (MM 500) besitzt an der Seite zum Roboter eine automatische Tür für die Beladung durch den Roboter. Die IGM-Schweißzelle besitzt ebenfalls eine automatische Tür zur Roboterseite. In Abbildung 3.4 sind die beteiligten Maschinen zu sehen, der ABB IRB 6620 hält dabei eine Nullpunktspannsystem-Palette mit einem fertigen Frästeil. Im hinteren Bereich von Abbildung 3.4 ist die IGM-Schweißzelle zu erkennen.



Abbildung 3.4: Hybrid Bearbeitungszelle

3.3.2.1 Daten der Maschine MAXXMILL 500

Die MM 500 ist eine vertikale 5-Achs CNC-Fräsmaschine mit Werkzeugmagazin, welches bis zu 40 Werkzeuge fasst. Die CNC-Fräsmaschine ist für die automatisierte Be- und Entladung der Werkstücke durch einen Roboter ausgelegt.



Abbildung 3.5: EMCO MT 500 [13]

Hersteller:	EMCO FAMUP s.r.l.
Typ:	MM 500
Maschinen-Nr.:	M-06520017
Baujahr:	2017

Tabelle 3.7: Daten der Maschine 3, MM500

3.3.2.2 Daten der Maschine IGM-Schweißzelle

Die IGM-Schweißzelle besteht aus einem 6-Achs Roboter und aus einem Dreh- und Schwenktisch, auf dem eine Spannstation für Nullpunktspannsystem-Paletten montiert ist. Die Schweißzelle ist mit einem Schweißgerät vom Typ TPS 500i der Firma Fronius ausgestattet. In Abbildung 3.6 ist der montierte Schweißbrenner am Roboter zu sehen.

Hersteller:	IGM Robotersysteme AG
Typ:	Roboteranlage
Maschinen-Nr.:	101712/301950
Baujahr:	2017

Tabelle 3.8: Daten der Maschine IGM-Schweißzelle



Abbildung 3.6: Inneres der Schweißzelle

3.3.2.3 Daten der unvollständigen Maschine ABB IRB 6620

Der ABB IRB 6620 besitzt eine Armreichweite von 2,20 m und kann eine maximale Masse von 150 kg bewegen.

Die Robotersteuerung des ABB IRB 6620 erfüllt gemeinsam mit SafeMove den Performance-Level PL d bzw. den Sicherheits-Integritätslevel SIL 2. [14, S. 20]

Der ABB IRB 6620 besitzt eine Anhaltezeit von 490 ms für einen Not Halt der Kategorie 0. Diese Zeit ist bei maximaler Geschwindigkeit, maximaler Beladung und maximal ausgestreckten Arm gültig. [10, S. 283]

Hersteller:	ABB Robotics
Typ:	IRB 6620
Maschinen-Nr.:	6620-101699
Baujahr:	2017

Tabelle 3.9: Daten der unvollständigen Maschine IRB6620

3.3.2.4 Daten der unvollständigen Maschine Palettenkupplung NSR 160

Die Palettenkupplung zum Greifen der Nullpunktspannsystem-Paletten ist fix auf dem Handgelenk des ABB IRB 6620 über eine Adapterplatte montiert, und dient dem Roboter als Greifer. Dadurch kann der Roboter die Nullpunktspannsystem-Paletten aufnehmen und transportieren. Die Palettenkupplung wird pneumatisch betätigt.

Hersteller:	Schunk
Typ:	NSR 160
Maschinen-Nr.:	0471915

Tabelle 3.10: Daten der unvollständigen Maschine Palettenkupplung

3.3.2.5 Daten der Nullpunktspannstation in der MM 500

In der MM 500 ist auf dem Maschinentisch eine Spannstation für das Nullpunktspannsystem montiert. Die Spannstation ist für die in der Hybridbearbeitungszelle verwendeten Paletten ausgelegt und wird pneumatisch geöffnet.

Hersteller:	Schunk
Bezeichnung:	Spannstation Nullpunktspannsystem Standard
Typ:	VERO-S NSL PLUS 400
Maschinen-Nr.:	0471048

Tabelle 3.11: Daten der Nullpunktspannstation in der MM 500

3.3.2.6 Daten der Nullpunktspannstation in der IGM-Schweißzelle

Die Spannstation, welche in der IGM-Schweißzelle verwendet wird, ist baugleich zu der in der MM 500.

Hersteller:	Schunk
Bezeichnung:	Spannstation Nullpunktspannsystem Standard
Typ:	VERO-S NSL PLUS 400
Maschinen-Nr.:	0471048

Tabelle 3.12: Daten der Nullpunktspannstation in der IGM-Schweißzelle

3.3.2.7 Daten der Cognex Kamera

Da das Kamerasystem mit keinem Antriebssystem ausgestattet ist und auch keine beweglichen Teile besitzt, fällt die Kamera nicht unter den Begriff einer Maschine, wie er in der DIN EN ISO 12100 definiert ist. [2, S. 6]

Um jedoch die Abläufe in der Fertigungszelle besser nachvollziehen zu können, wird die Kamera hier der Vollständigkeit halber erwähnt.

Vorne am Roboterflansch wird ein Kamerasystem montiert (siehe auch Abbildung 3.4), um die genaue Position des FTS zu erkennen, da die Positioniergenauigkeit des FTS nicht ausreicht. Dies ist notwendig um mit dem ABB IRB 6620 Paletten vom FTS aufzunehmen bzw. abzulegen.

Hersteller:	COGNEX
Product ID:	IS7802M-373-50-LAB

Tabelle 3.13: Daten der Cognex Kamera

3.3.3 Daten der vollständigen Maschine NEOBOTIX MP-400

Es wird nur ein FTS Neobotix MP-400 den gesamten Fertigungsbereich versorgen bzw. es wird sich nur ein FTS innerhalb der Schutzeinrichtungen befinden. Somit ist das FTS weder der Drehzelle noch der Hybridbearbeitungszelle zugeordnet. Das FTS ist mit einem Aufbau bestückt, auf den sowohl die Paletten der Hybridbearbeitungszelle als auch die Paletten der Drehzelle passen.

Um das FTS ohne Unterbrechung der Schutzeinrichtungen aus dem geschützten Bereich zu bringen, wird durch das Safety Eye eine Art Schleuse errichtet. Die genaue Beschreibung des Ablaufs zur Einfahrt in den geschützten Bereich bzw. Ausfahrt aus dem geschützten Bereich folgt in Abschnitt 4.2.2.4.

Hersteller:	Neobotix GmbH
Typ:	Mobiler Roboter MP-400 V1.0
Maschinen-Nr.:	20140715-1
Baujahr:	2014

Tabelle 3.14: Daten der vollständigen Maschine FTS

3.3.4 Definition der Schnittstellen zwischen den einzelnen Teilen des IMS

In diesem Abschnitt werden die Verkettungsschnittstellen zwischen den verwendeten Maschinen bzw. unvollständigen Maschinen beschrieben. Dabei wird der Arbeitsablauf im vorhergesehenen Betrieb betrachtet. Die Verkettungsschnittstellen sind in Abbildung 3.7 dargestellt. Ab Verkettungsschnittstelle Nr. 10 sind die einzelnen Schnittstellen der Übersichtlichkeit halber nicht mehr in Abbildung 3.7 dargestellt, die Beschreibung der Schnittstellen reicht jedoch zu deren Identifikation aus.

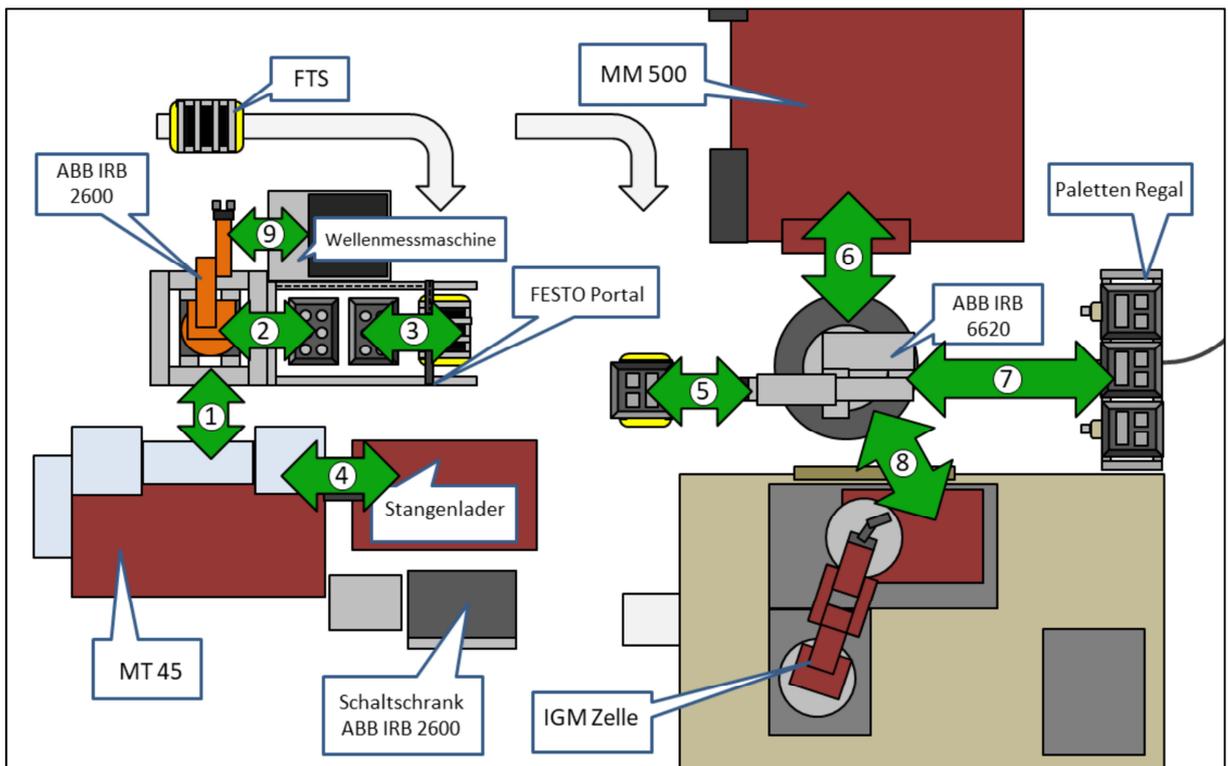


Abbildung 3.7: Schnittstellen zwischen den Maschinen

3.3.4.1 Verkettungsschnittstelle 1

Betroffene Maschinen: MT 45, ABB IRB 2600

Beschreibung: Der Roboter belädt das Drehzentrum mit einzelnen Rohteilen von einer Palette bzw. entnimmt das fertige Bauteil und legt es auf eine Palette.

3.3.4.2 Verkettungsschnittstelle 2

Betroffene Maschinen: ABB IRB 2600, FESTO Portal

Beschreibung: Das Portal befördert die entsprechende Palette mit Rohmaterial bzw. fertigen Bauteilen zu einer Ablageposition, bei der der Roboter die Bauteile bzw. das Rohmaterial entnimmt bzw. ablegt.

3.3.4.3 Verkettungsschnittstelle 3

Betroffene Maschinen: FESTO Portal, FTS

Beschreibung: Das FTS bewegt sich zu einer Parkposition, wo das FESTO-Portal eine Palette ablegt bzw. aufnimmt. Die Position des FTS wird durch drei Sensoren erfasst und durch die Steuerung des FESTO-Portals ausgewertet. Dadurch kann das FESTO-Portal trotz ungenauer Positionierbarkeit des FTS die Palette ablegen bzw. aufnehmen.

3.3.4.4 Verkettungsschnittstelle 4

Betroffene Maschinen: MT 45, Stangenlader

Beschreibung: Der Stangenlader belädt die MT 45 mit Rohmaterial in Stangenform. Ein Bediener muss den Stangenlader manuell bestücken.

3.3.4.5 Verkettungsschnittstelle 5

Betroffene Maschinen: ABB IRB 6620, FTS, Schunk Palettenkupplung NSR-A 160, Cognex Kamera

Beschreibung: Der Roboter entnimmt oder belädt das FTS mit einer Nullpunktspannsystem-Palette. Die Position des FTS wird mittels Vision System (Cognex Kamera auf Roboterflansch) ermittelt, da das FTS sich nicht präzise genug positionieren kann.

3.3.4.6 Verkettungsschnittstelle 6

Betroffene Maschinen: ABB IRB 6620, MM 500, Schunk Palettenkupplung NSR-A 160, Nullpunktspannstation

Beschreibung: Der Roboter entnimmt oder belädt die MM 500 mit einer Nullpunktspannsystem-Palette, auf der Rohmaterial bzw. fertige Bauteile gespannt sind.

3.3.4.7 Verkettungsschnittstelle 7

Betroffene Maschinen: ABB IRB 6620, Paletten Regal, Schunk Palettenkupplung NSR-A 160

Beschreibung: Der Roboter entnimmt dem Regal eine Palette oder legt eine Palette ins Regal. Das Regal dient als Zwischenspeicher von Paletten bzw. zum Auskühlen von geschweißten Bauteilen.

3.3.4.8 Verkettungsschnittstelle 8

Betroffene Maschinen: ABB IRB 6620, IGM-Schweißzelle, Schunk Palettenkupplung NSR-A 160, Nullpunktspannstation

Beschreibung: Der Roboter entnimmt oder belädt die IGM-Schweißzelle mit Nullpunktspannsystem-Paletten, auf denen sich fertig geschweißte Bauteile oder noch zu schweißende Bauteile befinden.

3.3.4.9 Verkettungsschnittstelle 9

Betroffene Maschinen: ABB IRB 6620, Wellenmessmaschine

Beschreibung: Der Roboter entnimmt oder belädt die Wellenmessmaschine mit einzelnen fertig bearbeiteten Werkstücken, die gemessen werden sollen.

3.3.4.10 Verkettungsschnittstelle 10

Betroffene Maschinen: ABB IRB 6620, Schunk Palettenkupplung NSR-A 160, Cognex Kamera

Beschreibung: Verkettungsschnittstelle 10 betrifft das Werkzeug bzw. die Zubehörteile, die vorne am Roboterflansch des ABB IRB 6620 montiert sind. Die Palettenkupplung ist fest und entsprechend den Vorgaben aus der Bedienungsanleitung mit einer Adapterplatte auf dem Roboterflansch montiert. Die Kupplung öffnet und schließt pneumatisch. Mittels Kupplung werden Schunk-Nullpunktspannsystem-Paletten mit aufgespannten Werkstücken am Roboter gehalten. Die Cognex Kamera wird mittels Winkel auf der Adapterplatte des Roboterflansches montiert. Das Kamerasystem dient zur Positionserkennung des FTS, welches die Hybridbearbeitungszelle mit Rohmaterial versorgt bzw. fertige Werkstücke wegtransportiert.

3.3.4.11 Verkettungsschnittstelle 11

Betroffene Maschinen: ABB IRB 1200, Schnellwechselsystem SWS 020, unterschiedliche Greifertypen

Beschreibung: Verkettungsschnittstelle 11 umfasst den Roboterflansch des ABB IRB 2600 und die darauf montierten Werkzeuge und Zubehörteile. Auf dem Roboterflansch werden die entsprechenden Werkzeuge bzw. Greifer entweder fest montiert oder mittels Schnellwechselsystem befestigt. Dabei ist das Anzugsdrehmoment der Schrauben zu beachten und gegebenenfalls eine Klebesicherung der Schrauben zu verwenden. Der Greifer wird pneumatisch betätigt. Das Schnellwechselsystem wird pneumatisch entriegelt. Die Pneumatik Leitung wird durch am Roboterarm angebrachte Kabelkanäle zum Roboterhandgelenk geführt.

3.3.4.12 Verkettungsschnittstelle 12

Betroffene Maschinen: MM 500, Nullpunktspannstation

Beschreibung: Verkettungsschnittstelle 12 definiert die Schnittstelle zwischen Nullpunktspannstation und der MM 500. Die Spannstation für das Nullpunktspannsystem wird fest auf dem Maschinentisch der MM 500 montiert. Die Betätigung der Spannstation erfolgt pneumatisch und wird durch die MM 500 realisiert.

3.3.4.13 Verkettungsschnittstelle 13

Betroffene Maschinen: IGM-Schweißzelle, Nullpunktspannstation

Beschreibung: Verkettungsschnittstelle 13 definiert die Schnittstelle zwischen Nullpunktspannstation und der IGM-Schweißzelle. Die Spannstation für das Nullpunktspannsystem wird fest auf dem Dreh- und Schwenktisch der IGM-

Schweißzelle montiert. Die Betätigung der Spannstation erfolgt pneumatisch und wird durch die IGM-Schweißzelle realisiert.

3.3.5 Arbeitsaufgaben im bestimmungsgemäßen Betrieb

In diesem Abschnitt werden die Arbeitsaufgaben für Personen, die Aufgaben an der Fertigungszelle erfüllen müssen, bei bestimmungsgemäßem Betrieb definiert und die dabei betroffenen Maschinen angegeben.

3.3.5.1 Arbeitsaufgabe 1

Betroffene Maschine: FTS

Beschreibung: An einem Rüstplatz außerhalb der Fertigungszelle wird das FTS durch einen Bediener mit einer Nullpunktspannsystem-Palette für das Hybridbearbeitungszentrum oder mit einer Palette für die Drehzelle bestückt bzw. eine dieser Paletten mit fertigen Bauteilen wird dem FTS abgenommen und am Rüstplatz abgestellt.

3.3.5.2 Arbeitsaufgabe 2

Betroffene Maschine: MT 45

Beschreibung: Rüsten der CNC-Drehmaschine, Programmierung eines CNC-Programms manuelle Be- und Entladung, Reinigung und Wartung der Maschine durch einen Bediener.

3.3.5.3 Arbeitsaufgabe 3

Betroffene Maschine: Stangenlader

Beschreibung: Bestücken des Stangenladers mit Stangenmaterial durch einen Bediener.

3.3.5.4 Arbeitsaufgabe 4

Betroffene Maschine: IGM-Schweißzelle

Beschreibung: Rüsten der Schweißzelle, Programmierung des Schweißroboters, manuelle Be- und Entladung, Reinigung und Wartung der Maschine durch einen Bediener.

3.3.5.5 Arbeitsaufgabe 5

Betroffene Maschine: MM 500

Beschreibung: Rüsten des Fräszentrums, Programmierung eines CNC-Programms manuelle Be- und Entladung, Reinigung und Wartung der Maschine durch einen Bediener.

3.3.5.6 Arbeitsaufgabe 6

Betroffene Maschine: Wellenmessmaschine

Beschreibung: Rüsten der Wellenmessmaschine und Programmierung der Maschine durch einen Bediener.

3.3.6 Verwendungsgrenzen

3.3.6.1 Bestimmungsgemäße Verwendung

Der Bereich des Instituts für Fertigungstechnik in der Pilotfabrik ist gedacht für die Demonstration von vollautomatischen Systemen und Industrie 4.0-Kommunikation der Maschinen bei einer Losgröße von eins. Dabei werden verschiedene Technologien eingesetzt wie z. B. die Zerspannung von Metallen und technischen Kunststoffen sowie die additive Fertigung mittels Auftragschweißen. Weitere Einsatzbereiche sind die Demonstration von Fertigungs- und Entwicklungsideen für Personen mit unterschiedlichem fachlichem Hintergrund, die Pilotierung von neuartigen Konzepten und die Verwendung als Lernfabrik in Form von Workshops für externe Personen.

3.3.6.2 Einschränkungen bei der Verwendung

Maximal ist ein Einschichtbetrieb vorgesehen. Falls bei Demonstrationen die Fertigungszelle länger in Betrieb sein sollte, so relativiert sich dies mit Tagen, an denen die Zelle nicht verwendet wird bzw. eingerichtet wird.

3.3.6.3 Einsatzbereich der verketteten Maschinen

Haupteinsatzbereich der Fertigungszelle ist der Forschungs- und Demonstrationsbetrieb. Die Fertigungszelle soll jedoch auch zumindest teilweise für die Lohnfertigung dienen.

3.3.6.4 Vernünftigerweise vorhersehbare Fehlanwendungen

Eine mögliche Fehlanwendung ist das Mitfahren von Personen (Besucher, Kinder) auf dem FTS.

3.3.6.5 Anwenderkreis

Dieser Abschnitt beschreibt den Personenkreis, welcher den Gefährdungen ausgesetzt sein könnte und teilt die Personen, je nach Einschulung und fachlichem Hintergrund, der entsprechenden Gruppe zu.

- **Nicht unterwiesene Personen**

Eine nicht unterwiesene Person ist eine Person, die keine besondere Einschulung erhalten hat wie z. B. Besucher, Reinigungspersonal, Wachdienst, Kinder bei Besuchergruppen unter Aufsicht von Lehrern oder ähnlichen Aufsichtspersonen.

- **Unterwiesene Personen**

Eine unterwiesene Person ist eine Person, die durch den Hersteller oder Betreiber in der Handhabung des Systems und über die damit verbundenen Restrisiken geschult und unterwiesen wurde. Beispiele dafür sind unter anderem Maschinenbediener, Auszubildende, Praktikanten, wissenschaftliche und studentische Mitarbeiter.

- **Fachkräfte**

Eine Fachkraft ist eine Person, die aufgrund ihrer fachlichen Ausbildung, Kenntnisse und Erfahrungen sowie Kenntnis der einschlägigen Normen und Bestimmungen die ihr übertragenen Arbeiten beurteilen und mögliche tätigkeitsbezogene Gefahren erkennen können sollte. Diese Personen sollten sich der spezifischen Gefährdungen sehr genau bewusst sein. Beispiele dafür sind: Elektrofachkraft, Instandhalter, Maschinist, vom Hersteller der Einzelmaschine geschultes Personal, Transporteur.

3.3.7 Lärmemission

Laut Arbeitnehmerschutzgesetz muss in Bereichen, in denen der Wert von 80 dB(A) überschritten wird, Gehörschutz zur Verfügung gestellt werden. Wird der Wert von 85 dB(A) überschritten, so muss der Gehörschutz in jedem Fall getragen werden. [15]

3.3.8 Zeitliche Grenzen

Ein Betrieb der Fertigungszelle ist für 10 Jahre vorgesehen.

3.3.8.1 Empfohlene Wartungsintervalle

Sämtliche Maschinen und unvollständige Maschinen sind entsprechend der jeweiligen mitgelieferten Betriebsanleitung zu warten.

3.3.9 Räumliche Grenzen

Alle Maschinen und unvollständigen Maschinen (einzige Ausnahme: FTS) sind fest am Boden verankert und können somit nicht verschoben werden.

Der ABB IRB 2600 und der ABB IRB 6620 werden zusätzlich durch virtuelle räumliche Zonen, welche in der Roboterprogrammierung zu berücksichtigen sind, im Bewegungsraum eingeschränkt. Somit ergeben sich zusätzliche räumliche Grenzen, welche die Gefährdungsbereiche genau definieren. In Abbildung 3.8 sind die eingeschränkten Bewegungsbereiche der Roboter bzw. des Festo-Portals durch rote Linien markiert.

Für Personen, die Arbeiten an den Maschinen durchführen, ist ausreichend Platz vorhanden. Dieser Platz soll freigehalten werden.

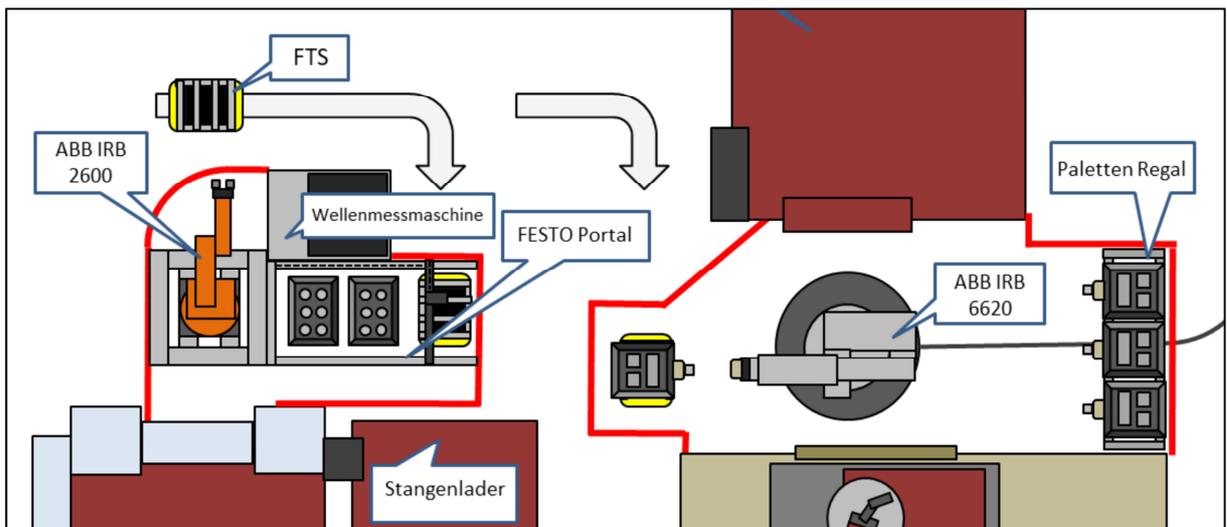


Abbildung 3.8: Räumliche Grenzen der Gefährdungsbereiche

3.3.10 Weitere Grenzen

Als weitere Grenzen werden der Temperaturbereich der Umgebung, der Grad an Sauberkeit und der Luftdruck am Aufstellort betrachtet. Die Parameter für die Pilotfabrik der TU Wien entsprechen den normalen Industriebedingungen, aus diesem Grund sind diesbezüglich keine weiteren Daten angegeben.

3.3.11 Tätigkeiten in sämtlichen relevanten Lebensphasen und Betriebsarten

Die in Tabelle 3.15 beschriebenen Tätigkeiten dienen als Grundlage der Identifizierung von Gefährdungen und den Gefährdungssituationen in den einzelnen Lebensphasen und Betriebsarten der Maschine. Somit können Gefährdungssituationen und der betroffene Personenkreis in allen Lebensphasen besser identifiziert werden. Dabei werden jedoch nur jene Tätigkeiten gelistet, die örtlich in Verbindung mit der Pilotfabrik der TU Wien stehen. Jene Tätigkeiten, die z. B. beim Hersteller durchgeführt werden, werden in dieser Betrachtung nicht angeführt.

Die Maßnahmen zur Risikominderung bzw. zur Beseitigung der Gefährdungen können erst dann eingeleitet werden, wenn sämtliche Gefährdungen identifiziert wurden. Dazu muss festgestellt werden, welche Arbeitsgänge die Maschine ausführt und welche Aufgaben die Personen, die mit der Maschine umgehen, erfüllen müssen. Dabei sind sämtliche Mechanismen und Funktionen der Maschine, das zu verarbeitende Material und das Umfeld in dem die Maschine eingesetzt wird, zu berücksichtigen. [2, S. 21]

Lebensphase/ Arbeitsgänge der Maschine	Tätigkeiten, Arbeitsabläufe, Eingriffe, Situationen	betroffener Personenkreis
Transport, Montage und Installation		
Bau und Herstellung	Zusammenbau	Fachkraft
	Probelaufe, Tests	Fachkraft
Transport	Verpacken, Be- und Entladen, Auspacken entsprechend den Anleitungen der jeweiligen Maschine	Fachkraft
	Transport entsprechend den Anleitungen der jeweiligen Maschine	Fachkraft
Montage, Installation, in Betrieb nehmen	Installation beim Betreiber	Fachkraft
	Montage von teilmontierten Maschinen	Fachkraft
	Probelaufe	Fachkraft
	Testen, Prüfen	Fachkraft
In Betrieb nehmen		
Einrichten	Einrichten der Maschine	Fachkraft
Einlernen, Programmieren	Einlernen (z. B. von Roboterpositionen)	Fachkraft, unterwiesene Person
	Programmieren	Fachkraft, unterwiesene Person
	Testen von Programmabläufen	Fachkraft, unterwiesene Person
Verwendung		
Einschalten der Maschinen	Anlaufen der Maschinen, Hochfahren	Fachkraft, unterwiesene Person
Automatikbetrieb	Automatischer Maschinenbetrieb	Fachkraft, unterwiesene Person, nichtunterwiesene Person
	Wiederanlauf nach einem Not-Halt	Fachkraft, unterwiesene Person
Manueller Betrieb	Manueller Betrieb der einzelnen Maschinen als eigenständige nicht zusammenhängende Maschine	Fachkraft, unterwiesene Person
	Manuelle Entnahme von schweren Werkstücken	Fachkraft, unterwiesene Person
Maschinenbeschickung	Zuführen von Rohmaterial	Fachkraft, unterwiesene Person
	Öffnen der Maschine	Fachkraft, unterwiesene Person
Prozessbeobachtung	Beobachtung beim ersten Zyklus ob alle Parameter stimmen	Fachkraft, unterwiesene Person
	Beobachtung um Daten zu analysieren	Fachkraft, unterwiesene Person, nichtunterwiesene Person

Lebensphase/ Arbeitsgänge der Maschine	Tätigkeiten, Arbeitsabläufe, Eingriffe, Situationen	betroffener Personenkreis
Stillsetzen der Maschine	Stillsetzen im Notfall	Fachkraft, unterwiesene Person, nichtunterwiesene Person
Reinigung / Wartung	Putzen im Zuge von allgemeinen Reinigungstätigkeiten	nichtunterwiesene Person
	Reinigung des Innenraums der Maschine	unterwiesene Person
	Schmierern	unterwiesene Person
	Wechsel des Kühlschmiermittels	unterwiesene Person
Umrüsten	Werkzeugwechsel	unterwiesene Person
	Umstellen auf andere Werkstücke	Fachkraft, unterwiesene Person
Instandhaltung	Präventive Instandhaltung	Fachkraft
	Fehlerbehebende Instandhaltung	Fachkraft
Fehlersuche und Fehlerbeseitigung	Arbeiten an der offenen Maschine mit direktem Zugang zur Gefahrenquelle	Fachkraft
	Wechsel von gebrochenen Schneiden	Fachkraft, unterwiesene Person
	Verklemmte Werkstücke lösen	Fachkraft, unterwiesene Person
	Wiederanlauf nach einer Blockierung	Fachkraft, unterwiesene Person
Demontage, Außerbetriebnahme und Entsorgung		
Außerbetriebnahme, Demontage	Außerbetriebnahme	Fachkraft
	Abtrennen der Energieversorgung	Fachkraft
	Entnahme von Gefahrenstoffen	Fachkraft
	Demontage schwerer Teile	Fachkraft
	Abtransport	Fachkraft
Entsorgung	Entsorgung von Gefahrenstoffen wie z. B. KSS	Fachkraft
	Entsorgung von defekten Teilen	Fachkraft
	Entsorgung der Anlage	Fachkraft

Tabelle 3.15: Tätigkeiten in den Lebensphasen der Maschinen nach [2]

3.4 Identifizierung der Gefährdungen, Risikoabschätzung und Risikobewertung

Bei der Identifizierung der Gefährdungen werden systematisch alle vernünftigerweise vorhersehbaren Gefährdungen (dauerhaft auftretende Gefährdungen und solche, die unerwartet auftreten) in sämtlichen relevanten Lebensphasen, der Maschine bzw. Maschinen betrachtet, siehe dazu auch Abschnitt 3.3.11. [2, S. 21]

Sämtliche möglicherweise auftretenden Gefährdungen werden für die Drehzelle in Tabelle 3.16 und die Hybridbearbeitungszelle in Tabelle 3.17 aufgelistet.

Gefährdungsnummer	Gefährdungsbeschreibung für die Drehzelle
1	Ein Werkzeug (z. B. eine Greiferbacke) löst sich während der Bewegung bzw. beim Abbremsen (z. B. Not-Halt) des Roboters. Dadurch können Personen am Kopf getroffen werden.
2	Ein Werkstück löst sich während der Bewegung bzw. beim Abbremsen (z. B. Not-Halt) des Roboters. Dadurch können Personen am Kopf getroffen werden.
3	Eine Person wird vom sich bewegenden Roboter erfasst. Es können tödliche Verletzungen entstehen.
4	Die Messspitze des Roboters (nur während Einrichtungsphase verwendet) kann eine Person am Auge verletzen.
5	Eine Person wird zwischen Roboterwerkzeug oder Teilen des Roboters und feststehenden Teilen der Zelle eingeklemmt. Es kann zu Quetschungen oder Scherungen der Finger, der Hände oder des Kopfs kommen.
6	Eine Person wird zwischen Roboterrückseite bzw. Roboterarm und feststehenden Teilen der Zelle eingeklemmt. Es kann zu Quetschungen oder Scherungen der Finger, der Hände oder des Kopfs kommen.
7	Finger können beim Schließen der Greiferbacken eingeklemmt werden.
8	Eine Person wird vom FESTO-Portal gequetscht. Es kann zu Verletzungen an Oberkörper und Kopf kommen.
9	Eine Person wird bei der Maschinentür der MT 45 eingeklemmt. Es kann zu Quetschungen des Kopfes oder Oberkörpers kommen.
10	Beim Ausschalten der Druckluft können vom Roboter gehaltene Teile herabfallen. Die Teile können Personen treffen.
11	Der Roboter kann umkippen. Dadurch können Personen eingequetscht werden.
12	Auf den Werkstücken kann sich Kühlschmierstoff (KSS) sammeln. Der Roboter bewegt die Werkstücke aus der Maschine. Dabei kann KSS auch auf den Hallenboden gelangen, wodurch Personen ausrutschen können.
13	Fertige Werkstücke können einen Grat aufweisen. Personen können sich daran schneiden.
14	Personen können beim Zugang zum Stangenlader stolpern. Es können Kopfverletzungen entstehen.

Tabelle 3.16: Identifizierung der Gefährdungen für die Drehzelle nach [2]

Gefährdungsnummer	Gefährdungsbeschreibung für die Hybridbearbeitungszelle
15	Der Roboter kann durch starke Beschleunigung/Abbremsung umkippen, wenn er nicht der Vorgabe entsprechend verankert wurde.
16	Palettenadapter oder andere Anbauteile lösen sich vom Roboter und können dadurch Personen am Kopf verletzen.
17	Palette löst sich während der Bewegung und kann dadurch Personen am Kopf verletzen.
18	Werkstück bzw. Palettenaufbau löst sich während der Roboterbewegung bzw. bei einem Not-Halt des Roboters. Dadurch können Personen am Kopf bzw. Auge verletzt werden.
19	Der Aufbau des Roboters, wie z. B. Ventilinsel, kann sich während der Bewegung lösen und weggeschleudert werden. Dadurch können Personen am Kopf verletzt werden.
20	Eine Person wird vom sich bewegenden Roboter erfasst. Es können tödliche Verletzungen entstehen.
21	Die Messspitze des Roboters (nur während Einrichtungsphase verwendet) kann eine Person am Auge verletzen.
22	Person wird zwischen Roboterwerkzeug und feststehenden Teilen der Zelle eingeklemmt. Es kann zu Quetschungen oder Scherungen der Finger, der Hände oder des Kopfs kommen.
23	Eine Person wird zwischen Roboterrückseite bzw. Roboterarm und feststehenden Teilen der Zelle eingeklemmt. Es kann zu Quetschungen oder Scherungen der Finger, der Hände oder des Kopfs kommen.
24	Bei geöffneter Seitentür der MM 500 kann eine Person den Oberkörper hineinstecken und durch Schließen der Tür kann diese eingeklemmt werden. Es kann zu Quetschungen an Kopf und Oberkörper kommen.
25	Bei geöffneter Tür der IGM-Schweißzelle kann eine Person durch automatisches Schließen eingeklemmt werden. Dadurch kann der Oberkörper oder Kopf gequetscht werden.
26	Beim Vorbeigehen am Palettenregal können Teile einer Palette oder die Palette selbst herabfallen. Dadurch können Zehen gequetscht werden.
27	Das Palettenregal kann umkippen. Dadurch können Personen eingequetscht werden.

Gefährdungsnummer	Gefährdungsbeschreibung für die Hybridbearbeitungszelle
28	Gasflaschen der IGM-Schweißzelle können umfallen. Dadurch kann das Ventil abschlagen und die Gasflasche fliegt durch den ganzen Raum. Dadurch können Personen tödlich verletzt werden.
29	Auf der Palette kann sich KSS sammeln. Das FTS transportiert die Palette weg. Dabei kann KSS auch auf den Hallenboden gelangen, wodurch Personen ausrutschen können.
30	Durch scharfe Kanten am fertigen Werkstück, welches durch das FTS transportiert wird, können sich Personen verletzen. Schnittwunden an der Hand können entstehen.
31	Heiße Werkstücke können die IGM-Schweißzelle verlassen. Dadurch können sich Personen verbrennen.
32	Bei der Bearbeitung in der MM 500 kommt es zu erheblichem Lärm. Dadurch kann die Hörfähigkeit beeinträchtigt werden.
33	Bei der IGM-Schweißzelle kann an der Automatiktür Laserstrahlung entweichen.
34	KSS kann bei Hautkontakt zu Hautreizungen und Allergien führen.
35	Rauch und Gase können im Bereich der IGM-Schweißzelle zu Benommenheit führen.
36	Personen können über den Schlauch zwischen IGM-Schweißzelle und Gasflasche stolpern.
37	Es können Personen mit dem FTS mitfahren und somit in den Gefahrenbereich kommen.

Tabelle 3.17: Identifizierung der Gefährdungen für die Hybridbearbeitungszelle nach [2]

3.4.1 Ermittlung des erforderlichen Sicherheits-Integritätslevel

In weiterer Folge wird für jede Gefährdung aus Tabelle 3.16 und Tabelle 3.17 eine Risikobewertung durchgeführt. Da für einige Gefährdungen technische Maßnahmen getroffen werden, die sicherheitsbezogene Steuerungsfunktionen beinhalten, ist es notwendig für diese technischen Maßnahmen den erforderlichen SIL oder den PL zu ermitteln. Dabei ist es dem Systemintegrator überlassen welches System verwendet wird. In Tabelle 3.18 ist der erforderliche SIL beispielhaft für die Gefährdung Nr. 5 aus Tabelle 3.16 ermittelt. Für die anderen Gefährdungen erfolgt ebenfalls die Bestimmung des erforderlichen SIL analog dazu, wird jedoch aus Platzgründen und da es sich bei Gefährdung Nr. 5 um eine der Gefährdungen, aus denen der höchste erforderliche SIL resultiert, handelt, in dieser Arbeit nicht festgehalten. Somit ist für die technische Maßnahme zur Minimierung von Gefährdung Nr. 5 mindestens SIL 2

erforderlich. Da bei Greifen der technischen Maßnahme die Schwere der möglichen Verletzung auf null reduziert wird, ist in Tabelle 3.18 bei der Bewertung der Schwere S dies eingetragen und die verwendete technische Maßnahme stellt somit eine ausreichende Reduzierung des Risikos dar.

Nr.	Identifizierung der Gefährdungen mit risikomindernden Maßnahmen	Risikoeinschätzung					Akzeptabel	SIL
		S	F	W	P	K		
5	Beschreibung der Gefährdung: Person wird zwischen Roboterwerkzeug und feststehenden Teilen der Zelle eingeklemmt. Es kommt zu Quetschungen, Scherungen der Finger, Hände oder Kopf.	4	5	4	1	10	NEIN	SIL 2
	Risikominderung durch inhärent sichere Konstruktion: keine	4	5	4	1	10	NEIN	
	Risikominderung durch technische Schutzmaßnahme: Zutrittsüberwachung des Fertigungsbereichs durch Laserscanner, Lichtgitter etc.	0	-	-	-	-	JA	
	Risikominderung durch Benutzerinformation: keine							

Tabelle 3.18: Beispiel zur Ermittlung des erforderlichen SIL nach [7]

3.4.2 Ermittlung des erforderlichen Performance Level

Um für die gleiche Gefährdungsnummer (Nr. 5) aus Tabelle 3.16 den erforderlichen PL zu ermitteln ist in Abbildung 3.9 der Pfad im Graphen zur Ermittlung des PL rot eingezeichnet. Es ist zu erkennen, dass der zum SIL 2 äquivalente PL d ermittelt wird. Der verwendete Graph wird in Abbildung 2.4 genauer beschrieben.

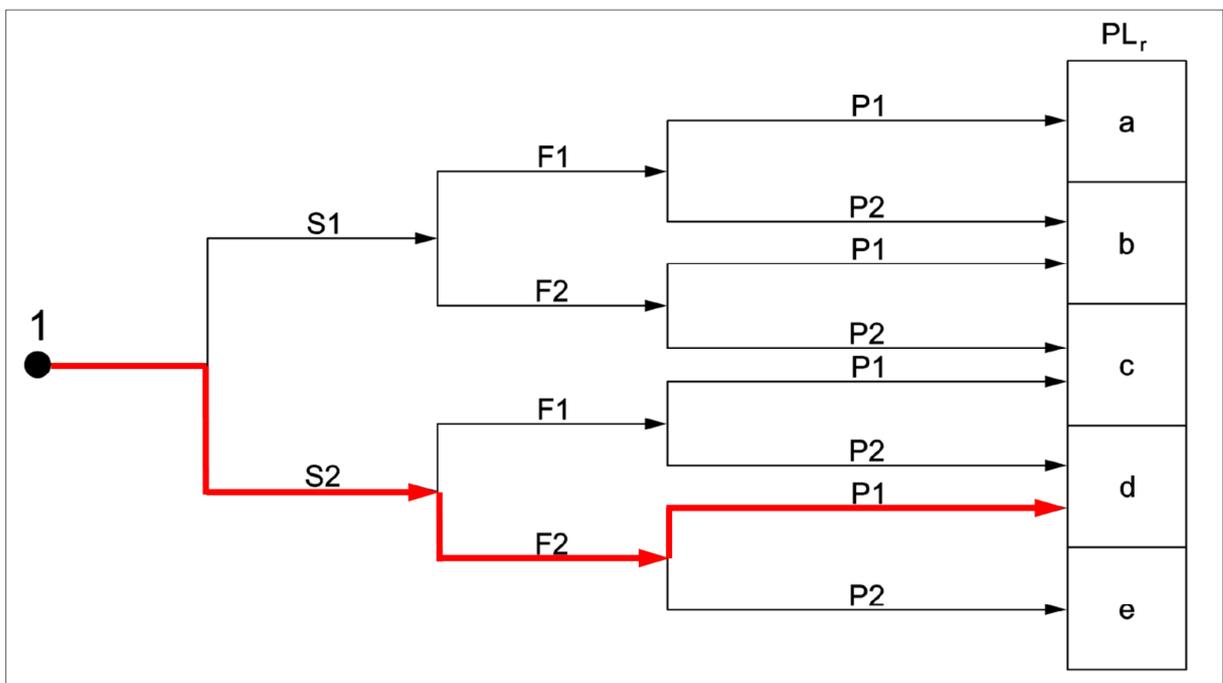


Abbildung 3.9: Beispiel zur Ermittlung des erforderlichen PL nach [6]

4 Risikomindernde Maßnahmen in der Pilotfabrik

4.1 Risikominderung durch Konstruktive Maßnahmen

Als erste risikomindernde Maßnahme sind konstruktive Maßnahmen anzuwenden, sofern dies möglich ist. In Tabelle 4.1 sind sämtliche konstruktiven Maßnahmen für die Fertigungszelle in Bezug zur jeweiligen Gefährdung aus Tabelle 3.16 und Tabelle 3.17 aufgelistet.

Nr.	Beschreibung der Konstruktiven Maßnahme	zugehörige Gefährdungs Nr.
1	Ordnungsgemäße Montage des Werkzeugs am Roboterflansch. Kontrolle des Anzugdrehmoments der Schrauben.	1
2	Die Schließkraft des Greifers muss ausreichend hoch sein.	2
3	Montage des Roboters ABB IRB 2600 ordnungsgemäß auf dem Gestell bzw. Sockel. Konstruktion eines ausreichend steifen Gestells bzw. Sockels. Verankerung des Gestells bzw. Sockels am Hallenboden.	11
4	Verankerung des Roboters ABB IRB 6620 ordnungsgemäß am Hallenboden.	15
5	Montage des Palettenadapters laut Bedienungshandbuch am Roboterhandgelenk und Anziehen der Schrauben mit dem vorgeschriebenen Anzugsdrehmoment. Zusätzliches Sichern der Befestigungsschrauben mit Klebstoff-Gewindesicherung um ein Lösen zu verhindern.	16
6	Nachrechnung der Palettenkupplung laut Bedienungshandbuch.	17
7	Nachrechnung der Befestigungsart des Palettenaufbaus und der Spannkraft des Werkzeugs, welches die Werkstücke hält.	18
8	Ordnungsgemäße Montage des Palettenaufbaus und zusätzliche Sicherung von Schraubverbindungen mit Klebstoff-Gewindesicherung.	19
9	Auf dem Regal sind Ablageelemente anzubringen, welche die Paletten in der Position festlegen und ein hin und her Rutschen verhindern. Somit ist einem unbeabsichtigten Herabfallen der Paletten vorgebeugt.	26
10	Ordnungsgemäße Verankerung des Palettenregals am Hallenboden.	27
11	Sicherung der Gasflaschen durch an der Wand befestigte Ketten, um ein Umkippen zu vermeiden.	28
12	Montage einer Kunststoffdichtlippe, die den Austritt von Laserstrahlung verhindert.	33
13	Installation einer Absaugung für die IGM-Schweißzelle	35

Tabelle 4.1: Konstruktive Maßnahmen

4.2 Risikominderung durch technische Schutzmaßnahmen

Da es nicht möglich ist, sämtliche Risiken durch konstruktive Maßnahmen ausreichend zu reduzieren, sind technische Schutzmaßnahmen notwendig. Für die entsprechenden Gefährdungen wird als technische Schutzmaßnahme eine Zutrittsüberwachung des Fertigungsbereichs durch Laserscanner, Lichtgitter, Türsensor an der IGM-Schweißzelle und Safety Eye realisiert. Dadurch wird der Fertigungsbereich so überwacht, dass keine Person den Gefahrenbereich betreten kann, ohne einen Not-Halt auszulösen. Die Gefährdungsnummern aus Tabelle 3.16 und Tabelle 3.17, welche zur Risikominderung diese zusätzlichen technischen Schutzmaßnahmen erfordern sind folgende: 1, 2, 3, 5, 6, 7, 8, 9, 17, 18, 19, 20, 22, 23, 24 und 25.

Damit die sich der ABB IRB 6620 nur in dem definierten Arbeitsbereich bewegt, werden mittels SafeMove bestimmte Bereiche definiert, in denen sich der Roboter nicht bewegen darf oder in denen dessen Geschwindigkeit überwacht wird. Diese Bereiche werden in der Einrichtephase durch eine dazu befugte Person definiert und danach für alle notwendigen Betriebsarten aktiviert. Durch ein Passwort kann die SafeMove Konfiguration geschützt werden, somit kann sichergestellt werden, dass durch den Standard-Benutzer keine sicherheitsrelevanten Konfigurationen geändert werden können. Konkret bedeutet dies, dass der Roboter einen Stopp der Kategorie 1 ausführt sobald er sich in eine dieser „verbotenen“ Zonen bewegt. Der zulässige Bereich ist in Abbildung 3.8 durch rote Linien markiert. In Abbildung 4.10 und Abbildung 4.11 sind die SafeMove Zonen für die MM 500 und die IGM-Zelle dargestellt, die Kollisionen zwischen Roboter und Maschine verhindern sollen.

Der ABB IRB 2600 wird im Arbeitsbereich durch sogenannte Weltzonen gehalten, dies funktioniert ähnlich wie beim ABB IRB 6620, jedoch direkt in der Steuerung des Roboters. Da die SafeMove-Version des ABB IRB 2600 eine ältere ist als beim ABB IRB 6620, kann die Raumüberwachung des Roboters nicht über SafeMove programmiert werden.

Für die Leistungsanforderung von sicherheitsbezogenen Teilen von Robotersteuerungen gilt, dass diese zumindest Performance Level PL d oder den Sicherheits-Integritätslevel SIL 2 erfüllen müssen. Da diese Anforderung einer Typ-C Norm, wie in Abschnitt 2.5 beschrieben, Vorrang gegenüber der Auswahl des entsprechenden PL bzw. SIL hat, ist die entsprechende Schutzeinrichtung mit mindestens SIL 2 bzw. PL d zu wählen. [16, S. 14]

Dies hat zur Folge, dass die Sicherheitssteuerung und die zugehörige Sensorik als Gesamtheit zumindest SIL 2 bzw. PL d erreichen muss.

4.2.1 Auswahl von Schutzeinrichtungen

Da die Pilotfabrik in erster Linie zu Demonstrationszwecken dient, sind nichttrennende Schutzeinrichtungen besser geeignet, da sie die Sicht auf die Maschinen nicht beeinträchtigen. Aus diesem Grund werden Laserscanner, Lichtgitter und Safety-Eye als Schutzeinrichtungen gewählt.

4.2.1.1 Horizontaler Laserscanner im Bereich des Palettenregals

Im Bereich des Palettenregals wird ein horizontaler Laserscanner in Bodennähe (200 mm Abstand vom Boden) eingesetzt, der den Bereich überwacht und somit vor unbemerktem Zutritt schützt. Dazu wird ein Sicherheits-Laserscanner microScan3 Core I/O mit einer Schutzfeldreichweite von 5,5 m der Firma SICK verwendet, siehe Abbildung 4.1.

Dieser Laserscanner besitzt einen Sicherheits-Integritätslevel (SIL) von 2, dies entspricht dem Performance-Level (PL) d. [17, S. 137]

Die Ansprechzeit (die maximale Zeit zwischen dem Auftreten des Ereignisses, das zum Ansprechen des Sensors führt, und der Bereitstellung des Abschaltsignals) des Laserscanners ist abhängig von Scanzzykluszeit, eingestelltem Beeinflussungsschutz und eingestellter Mehrfachauswertung. [17, S. 141]

Die Ansprechzeit für die verwendeten Einstellungen beträgt 90 ms. Die eingestellte Auflösung entspricht einer sogenannten Beinauflösung und beträgt 50 mm.



Abbildung 4.1: Sicherheits-Laserscanner microScan3 Core I/O [18]

4.2.1.2 Vertikale Laserscanner parallel zum Leitstand

Parallel zum Leitstand werden drei vertikale Sicherheits-Laserscanner eingesetzt, die den Zutritt zu den Gefährdungsbereichen verhindern. Diese Aufgabe erledigen drei Sicherheits-Laserscanner S3000 Advanced ebenfalls von der Firma SICK, siehe dazu Abbildung 4.2. Diese Laserscanner sind an der Decke montiert, als Befestigung dient ein Gestell aus Alu Profilen, dass bei der Montage ein Nachjustieren in zwei Richtungen ermöglicht, siehe Abbildung 4.14.

Diese Laserscanner besitzen einen SIL 2 und einen PL d. [19, S. 148]

Die Ansprechzeit für den Laserscanner ist abhängig von der Basisansprechzeit bei der jeweiligen Auflösung und der maximalen Schutzfeldreichweite, der eingestellten Mehrfachauswertung und den verwendeten OSSDs. [19, S. 145]

Die Ansprechzeit des Laserscanners in der verwendeten Konfiguration beträgt 120 ms. Die eingestellte Auflösung entspricht einer sogenannten Handauflösung und beträgt 40 mm.



Abbildung 4.2: Sicherheits-Laserscanner S3000 Advanced [20]

4.2.1.3 Safety Eye

Um den Bereich in Verlängerung zum Leitstand abzusichern, dient ein Safety Eye von der Firma PILZ, siehe Abbildung 4.3. Das Safety Eye kann durch drei Kameras einen dreidimensionalen Bereich überwachen und Personen bzw. Objekte in dem Bereich erkennen.

Um ein durchschleusen des FTS zu gewährleisten, ohne dass dabei versehentlich Personen in den Gefahrenbereich gelangen können, werden mehrere Raumordnungen programmiert, welche auf Anforderung umgeschaltet werden können und somit kann eine virtuelle Schleuse erzeugt werden.

Das Safety Eye erreicht einen SIL 2 bzw. einen PL d. [21]

Die Raumordnungen können mit der zugehörigen Software parametrierbar werden. Die eingestellte Auflösung für die verwendeten Räume ist eine sogenannte Körperaflösung mit 200 mm. Die Ansprechzeit für die eingestellte Konfiguration beträgt 265 ms.

Das Safety Eye ist so konfiguriert, dass es zwischen zwei Bereichsarten unterscheidet. Zum einen gibt es einen gelben Bereich bzw. Warnraum, der weiter von der Gefährdungsstelle entfernt ist. Wird dieser Bereich verletzt, so wird die Geschwindigkeit der Roboter reduziert. Der zweite, rote Bereich ist ein Not-Halt-Raum bzw. ein Schutzraum. Wird dieser Raum verletzt so löst es einen Not-Halt für den gesamten Fertigungsbereich aus. Die Räume sind in Abbildung 4.13 entsprechend durch einen roten und gelben Bereich dargestellt.



Abbildung 4.3: Safety Eye [22]

4.2.1.4 Sicherheits - Lichtvorhang

Der Bereich zwischen IGM-Schweißzelle und Stangenlader wird durch einen Sicherheits-Lichtvorhang deTec / Typ 4 von der Firma SICK abgesichert. In Abbildung 4.4 ist der Sicherheits-Lichtvorhang dargestellt. Der verwendete Lichtvorhang besitzt eine Auflösung von 14 mm und eine Schutzfeldhöhe von 1800 mm. Der Lichtvorhang wird so angebracht, dass die Unterseite 200 mm vom Boden entfernt ist, somit kann ein Unterkriechen vermieden werden.

Der Lichtvorhang besitzt ein SIL 3 und ein PL e [23, S. 56] sowie eine Ansprechzeit von 20 ms [23, S. 58].



Abbildung 4.4: Sicherheits-Lichtvorhang deTec / Typ 4 [24]

4.2.1.5 Türüberwachung der IGM-Schweißzelle

Zur Überwachung der manuell betätigten Tür der IGM-Schweißzelle, wird ein Berührungsloser Sicherheitsschalter STR1 der Firma SICK verwendet, siehe Abbildung 4.5.

Der berührungslose Sicherheitsschalter besitzt ein SIL 3, ein PL e und eine Ansprechzeit von 40 ms. [25, S. 36]



Abbildung 4.5: Berührungsloser Sicherheitsschalter STR1 [26]

4.2.1.6 Sicherheitssteuerung

Um die größtenteils I/O basierten Sicherheitsüberwachungsgeräte auszuwerten und in den Fertigungsbereich zu integrieren, ist eine Sicherheitssteuerung erforderlich. Für diesen Zweck sind zwei Sicherheitssteuerungen Flexi-Soft, siehe Abbildung 4.6, mit je mehreren I/O-Modulen verbaut. Die beiden Module sind mit einem sicherheitsfähigen Bus von SICK dem sogenannten Flexi Line miteinander verbunden. Die Hauptsteuerung (in weiterer Folge CPU 1 genannt) befindet sich auf der IGM-Schweißzelle und die zweite Steuerung (CPU 2) ist im Schaltschrank des ABB IRB 2600 verbaut.

Das Hauptmodul und das I/O Modul FX3-XTIO84002 besitzen beide einen SIL 3 und einen Performace Level PL e. [27, S. 137, 139]

Da die beiden Hauptmodule über Flexi-Line miteinander verbunden sind, hängt die Ansprechzeit von dem jeweiligen Signalpfad ab.

Die Logikausführungszeit der CPU ist von der Programmgröße abhängig. Bei den verwendeten Programmen besitzt die CPU 1 eine Logikausführungszeit von 8 ms und die CPU 2 eine Logikausführungszeit von 4 ms.

Die Ansprechzeiten für die Ein- und Ausgänge und die zusätzliche Reaktionszeit, falls die Kommunikation über Flexi Line läuft, sind in Tabelle 4.2 eingetragen.

Logikausführungszeit CPU 1	8 ms
Logikausführungszeit CPU 2	4 ms
Ansprechzeit der Eingänge	6,5 ms
Ansprechzeit der Ausgänge	4,5 ms
Zusätzliche Reaktionszeit für Kommunikation über Flexi Line	14 ms

Tabelle 4.2: Ansprechzeiten für Flexi-Soft Steuerung, [27]



Abbildung 4.6: Flexi Soft Sicherheitssteuerung mit unterschiedlichen Modulen [28]

4.2.1.7 PROFIsafe Kommunikationsmodul

Um die SafeMove Funktion des ABB IRB 6620 nutzen zu können und damit beispielsweise die Geschwindigkeitsüberwachung mittels SafeMove zu aktivieren, ist eine PROFIsafe Kommunikation erforderlich. Das UE4740 Modul von der Firma SICK leitet die Signale der Sicherheitssteuerung über PROFIsafe weiter.

Das Kommunikationsmodul besitzt einen SIL 3 bzw. einen PL e. [29, S. 32]

Die interne Verarbeitungszeit des Kommunikationsmoduls beträgt 6 ms. [29, S. 34]



Abbildung 4.7: SICK PROFIsafe Gateway UE4740-22H0000 [30]

4.2.1.8 Sicherheitsrelais

Um das Not-Halt Signal an die IGM-Schweißzelle sowie an das Festo Portal, an die Automatik-Sicherheitskreise der beiden Robotersteuerungen, an die MM 500, an die MT 45 und an die Wellenmessmaschine weiterzuleiten, werden Sicherheitsrelais UE10-3OS der Firma SICK verwendet, siehe dazu Abbildung 4.8.

Das Sicherheitsrelais besitzt einen SIL 3 und einen PL e. Die Ansprechzeit ergibt sich mit einer Einschaltzeit von 40 ms am Eingangskreis und einer Ansprechzeit der Schutzfunktion von 20 ms am Ausgangskreis zu einer gesamten Ansprechzeit von 60 ms. [31]



Abbildung 4.8: Sicherheitsschaltgerät UE10-3OS [32]

4.2.1.9 Siemens SIMATIC S7-1500F

Da der Zellenaufbau mit der Zeit gewachsen ist und bei den Industrierobotern die SafeMove Funktion implementiert wurde, ist zusätzlich ein PROFIsafe fähiger Master notwendig, da die IRC5 Steuerung des ABB Roboters keinen PROFIsafe Master bereitstellt. Dazu wird eine Siemens SIMATIC S7-1500F CPU 1511F-1 PN verwendet. Die Sicherheits-SPS von Siemens dient zur Weitergabe der Sicherheitssignale des PROFIsafe Gateways zur SafeMove Eingangskarte des IRB 6620 und wird über PROFIsafe realisiert.

Die fehlersichere CPU von Siemens erreicht maximal einen SIL 3 bzw. einen PL e. [33]



Abbildung 4.9: Siemens SIMATIC S7-1500F [34]

4.2.1.10 ABB SafeMove

SafeMove mit den funktionalen Sicherheitsoptionen dient dazu, im Robotersystem eine robuste und einfach zu bedienende Sicherheitssteuerung zu bieten. Das SafeMove Paket von ABB ist eine Software und Hardware Lösung, die vollständig in die IRC5-Robotersteuerung und in die Programmierumgebung von RobotStudio integriert ist. Mit SafeMove können Überwachungsfunktionen wie z. B. eine Geschwindigkeitsüberwachung verwendet werden, die den Roboter stoppen können. Zusätzlich können externe Not-Halt Anforderungen von einer Sicherheits-SPS über die sichere Feldbus-Kommunikation PROFIsafe kommuniziert werden. [14, S. 15]

Mit ABB SafeMove werden Zonen definiert, die Kollisionen mit anderen Maschinen verhindern sollen. Die SafeMove Zonen für die MM 500 und für die IGM-Zelle sind in Abbildung 4.10 und Abbildung 4.11 dargestellt.

SafeMove erfüllt in Kombination mit der Robotersteuerung einen SIL 2 bzw. einen PL d. [14, S. 20]

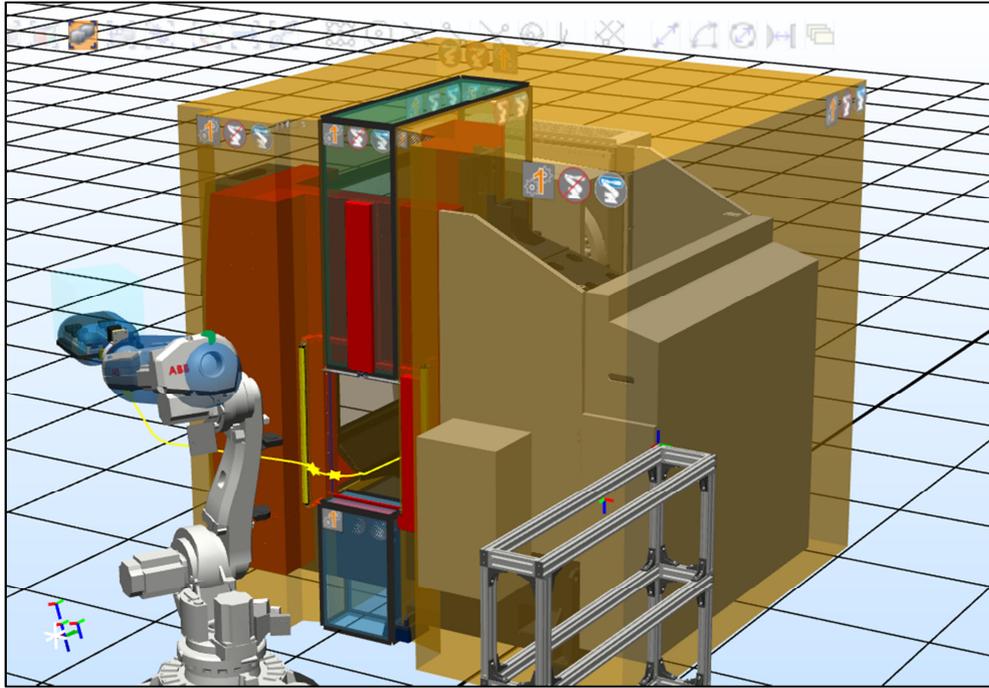


Abbildung 4.10: SafeMove Zonen für die MM 500

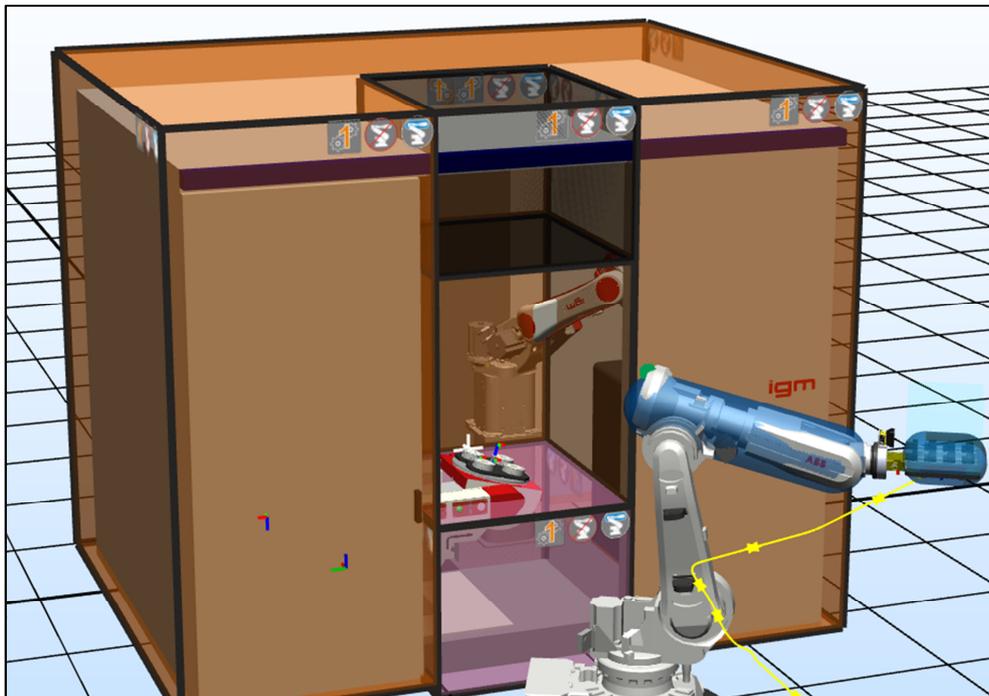


Abbildung 4.11: SafeMove Zonen für die IGM-Zelle

4.2.1.1 Bedienmodul am Leitstand

Beim Leitstand ist ein Bedienmodul für den gesamten Fertigungsbereich an einer Säule angebracht, siehe Abbildung 4.12. Dieses Bedienmodul beinhaltet einen Not-Halt Taster für den gesamten Fertigungsbereich, einen Schlüsselschalter zum Quittieren des Not-Halts, einen Start-Taster zum Starten der Zelle, einen Stopp Taster zum Stoppen, einen Betriebsartenschalter, der zwischen Automatikbetrieb und manuellem Betrieb umschaltet, und einer Meldeleuchte, die einen Stöorzustand anzeigt bzw. bei einem aktiven Not-Halt blinkt.



Abbildung 4.12: Bedienmodul am Leitstand

4.2.2 Anordnung und Verschaltung der Sicherheitsgeräte

Um den gesamten Fertigungsbereich zu überwachen werden die in Abschnitt 4.2.1 angeführten Sicherheitseinrichtungen verwendet. Deren räumliche Anordnung ist in Abbildung 4.13 dargestellt. Der weiße Bereich in Abbildung 4.13 definiert den geschützten Bereich. Dabei handelt es sich um jenen Bereich, der so von Schutzmaßnahmen umgeben ist, dass die Gefährdungen nicht von Personen erreicht werden können [3, S. 12]. In diesem Bereich dürfen sich während des Automatik-Betriebs keine Personen aufhalten. Der Wiederanlauf nach einem Not-Halt muss am Bedienmodul am Leitstand durch einen Schlüsselschalter quittiert werden, erst danach kann der Start Taster am Leitstand betätigt werden, um die

Maschinen wieder zu starten. Durch den Not-Halt Taster am Bedienmodul des Leitstands kann für den gesamten Fertigungsbereich, der alle darin enthaltenen Maschinen umfasst, ein Not-Halt ausgelöst werden. Die berührungslos-wirkenden Schutzeinrichtungen lösen hingegen nur für die Roboter und das Festo-Portal einen Not-Halt aus. Dies wird so gelöst, da sich häufig Besucher in der Pilotfabrik aufhalten, denen diverse Vorgänge an den Maschinen näher demonstriert werden sollen. Daher müssen sich Personen den Maschinen auch während des Bearbeitungsvorgangs ausreichend nähern können. Da es sich bei den verwendeten Maschinen um eigenständige Maschinen handelt, die werkseitig bereits mit entsprechenden Sicherheitseinrichtungen, wie z. B. mit Sicherheitsschalter mit Zuhaltung ausgestatteten Türen, können sich Personen auch während des Betriebs gefahrlos in unmittelbarer Nähe aufhalten. Einerseits können Besucher die Bearbeitungsvorgänge so genau beobachten, zusätzlich wird auch die Bearbeitungszeit nicht unnötigerweise verlängert.

Da es in weiterer Folge zur Ermittlung der Mindestabstände notwendig ist, die gesamte Nachlaufzeit des Systems zu kennen und diese von den Signalpfaden abhängig ist, wird in Abbildung 4.15 dargestellt, wie die einzelnen Sicherheitsgeräte zusammenhängen. Weiters ist in Abbildung 4.15 die sichere Kommunikation der Maschinen zum Einleiten eines Not-Halts schematisch dargestellt.

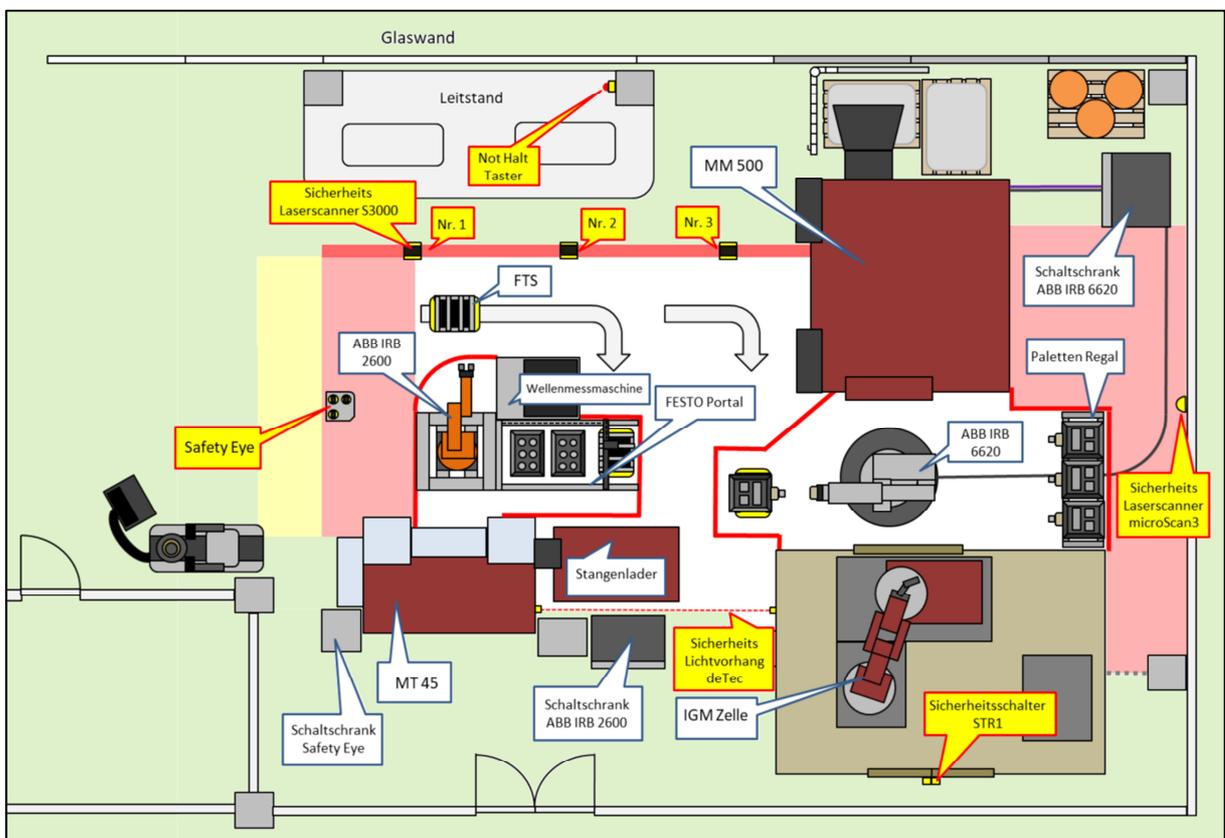


Abbildung 4.13: Räumliche Anordnung der Sicherheitsgeräte



Abbildung 4.14: Laserscanner S3000 Advanced und Safety Eye an der Decke

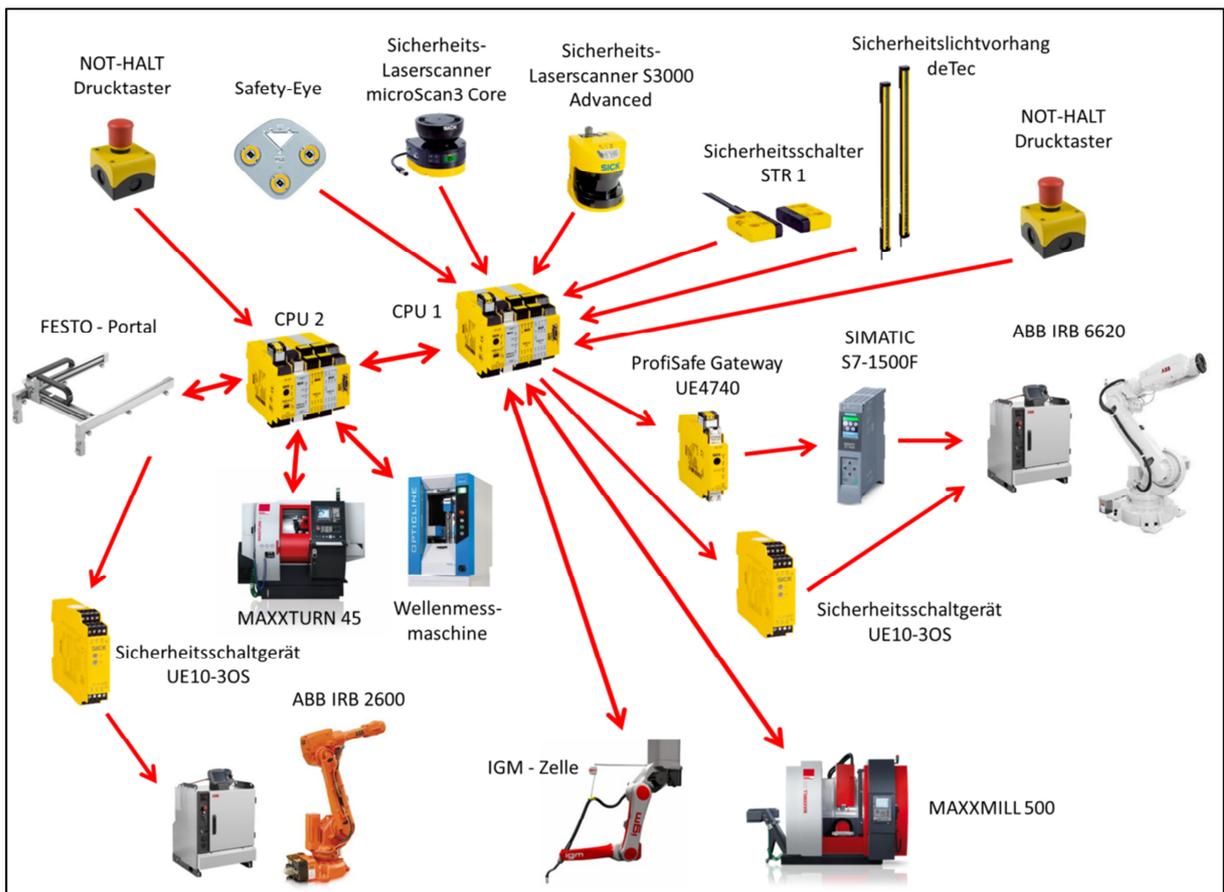


Abbildung 4.15: Einbindung der Sicherheitseinrichtungen [13], [22], [35]–[42]

4.2.2.1 Manueller Betrieb des Fertigungsbereichs

Am Bedienmodul, welches am Leitstand angebracht ist, kann die Betriebsart des Fertigungsbereichs eingestellt werden. Dabei gibt es einen Automatik-Modus und einen manuellen-Betriebsmodus. Im manuellen-Modus können die einzelnen Maschinen auch bei einer Verletzung der berührungslos-wirkenden Schutzeinrichtungen betrieben werden, jedoch nur als eigenständige Maschinen. Die Roboter können allerdings nur durch die ständige Betätigung der Zustimmungseinrichtung am Teach-Pendant im Hand-Betrieb mit reduzierter Geschwindigkeit bewegt werden. Das Festo-Portal kann ebenfalls durch die Bedieneinrichtung, die sich direkt auf diesem befindet, bewegt werden.

4.2.2.2 Automatik Betrieb des Fertigungsbereichs

Der Automatik-Betrieb des Fertigungsbereichs muss am Bedienmodul, welches am Leitstand angebracht ist, durch den Wahlschalter eingestellt werden. Der Not-Halt am Bedienmodul löst für alle Maschinen im Fertigungsbereich einen Not-Halt aus, auch für die MM 500, MT 45 und die IGM-Zelle.

Sowohl für die Drehzelle als auch für die Hybridbearbeitungszelle gilt, dass alle darin beteiligten Maschinen an die Sicherheitssteuerung angebunden sind. Wird nun die Drehzelle betrachtet, so ist der Betrieb dieser im Automatik-Modus nur dann möglich,

wenn sich keine Maschine der Drehzelle im Not-Halt-Zustand befindet. Befindet sich die MT 45 in einem Not-Halt-Zustand oder löst diese einen Not-Halt aus, so wird durch die Sicherheitssteuerung am ABB IRB 2600 und am Festo-Portal ein Not-Halt ausgelöst. Die Drehzelle kann unabhängig davon betrieben werden, ob sich die Hybridbearbeitungszelle beispielsweise im Not-Halt- bzw. ausgeschalteten Zustand befindet. Umgekehrt gilt dies auch für die Hybridbearbeitungszelle, die sich auch ansonsten ähnlich wie die Drehzelle verhält. Befindet sich die MM 500 oder die IGM-Zelle in einem Not-Halt Zustand oder lösen diese einen Not-Halt aus, so wird am ABB IRB 6620 ein Not-Halt durch die Sicherheitssteuerung ausgelöst.

4.2.2.3 Warnbereich

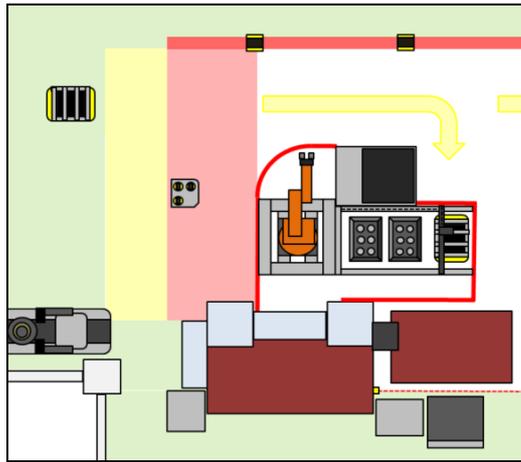
Der Warnbereich wird durch das Safety-Eye festgelegt. In Abbildung 4.13 ist der Warnbereich durch den gelben Bereich gekennzeichnet. Betritt eine Person diesen Warnbereich, dann reduzieren beide Roboter und das Festo-Portal ihre Bewegungsgeschwindigkeit und ein Signalton wird ausgegeben. Der Sinn des Signaltons besteht darin, dass nichteingewiesene Personen vorab gewarnt werden, bevor sie einen Not-Halt auslösen könnten und somit die Anlage nicht unnötigerweise gestoppt wird. Verlässt diese Person diesen Warnbereich wieder, dann bewegen sich die Roboter und das Festo-Portal wieder mit der normalen Geschwindigkeit und der Signalton erlischt.

4.2.2.4 Durchschleuse Vorgang des FTS

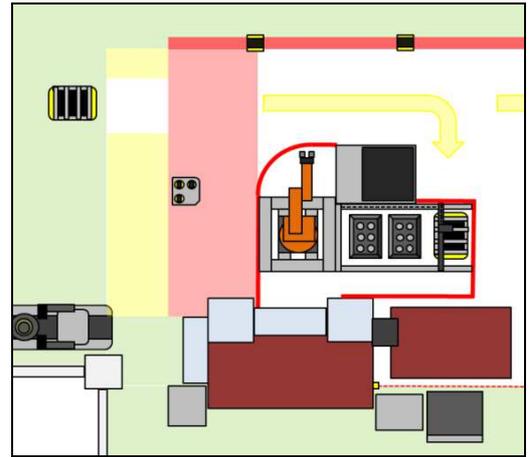
Damit das FTS den geschützten Bereich verlassen kann, um zu einer außerhalb liegenden Rüststation zu fahren, dabei jedoch keine Personen in die Gefahrenbereiche kommen können, schaltet das Safety-Eye eine virtuelle Schleuse. Dabei werden die Raumanordnungen des Safety-Eyes in einer bestimmten Reihenfolge geändert. Somit ist es möglich, dass das FTS den geschützten Bereich verlassen und einfahren kann, ohne dass ein Not-Halt (rot markierter Bereich) oder der Warnbereich (gelbe Zone = reduzierte Geschwindigkeit der Roboter) ausgelöst wird. Die Schleuse wird dabei so eingerichtet, dass eine mitfahrende Person einen Not-Halt auslösen würde. Dabei wird die Höhe in der Schleuse so eingestellt, dass das FTS mit Palette, die mit Werkstücken oder Rohmaterial beladen ist, gerade noch keine Verletzung der Raumordnung verursacht. Die Reihenfolge beim Einfahren in den geschützten Bereich ist in Abbildung 4.16 a) bis f) schematisch dargestellt. Die Ansteuerung der einzelnen Raumordnungen wird durch ein Transportleitsystem initiiert. Dabei kommuniziert das Transportleitsystem ebenfalls mit dem FTS und lotst es somit durch die Schleuse. Da das FTS eine eigenständige Maschine ist und sich auch außerhalb des geschützten Bereichs bewegen darf, wird das FTS bei einem Not-Halt des Fertigungsbereichs nicht angehalten. Dies wird ermöglicht, da das FTS einen eingebauten Laserscanner besitzt und somit Personen erkennt und rechtzeitig stoppt. Falls das FTS durch Positionierungsfehler oder irgendwelche anderen Fehler

einen Not-Halt auslöst, so gibt das Transportleitsystem dem FTS den Befehl, dass der Durchschleusevorgang nicht mehr notwendig ist, und leitet es direkt zum gewünschten Zielort. Nach dem Not-Halt ist ein manuelles quittieren erforderlich.

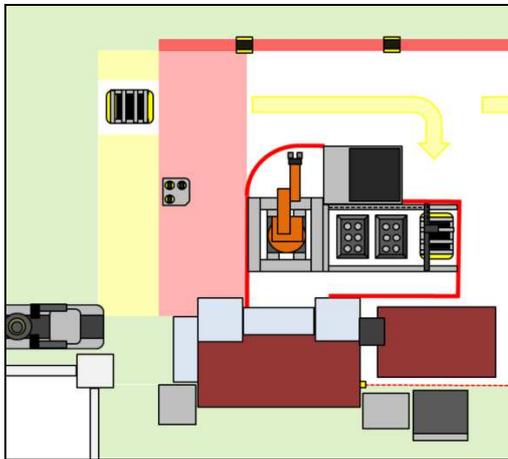
Der Vorgang zum Einfahren des FTS in den geschützten Bereich läuft so ab, dass sich das FTS wie in Abbildung 4.16 a) vor dem gelben Bereich positioniert und dann dem Transportleitsystem meldet, dass es bereit ist. Das Transportleitsystem schaltet die Raumordnung wie in Abbildung 4.16 b) und teilt dem FTS mit, dass es eine Position weiter fahren soll. Hat das FTS die Position nach Abbildung 4.16 c) erreicht, so meldet es dem Transportleitsystem dies. Das Transportleitsystem schaltet auf die nächste Raumordnung um und schließt somit den roten Bereich hinter dem FTS und meldet dies wieder dem FTS. Dieser Raumzustand ist so knapp bemessen, dass sich unmittelbar vor, hinter oder neben dem FTS keine Person aufhalten kann, ohne einen Not-Halt auszulösen. Danach kann das FTS in den geschützten Bereich einfahren. Sobald es sich in dem Bereich befindet, meldet es dem Transportleitsystem dies, und das Transportleitsystem schaltet wieder auf die Ausgangsraumordnung um. Beim Ausfahren des FTS aus dem geschützten Bereich werden die Raumordnungen in der umgekehrten Reihenfolge durchgeschaltet.



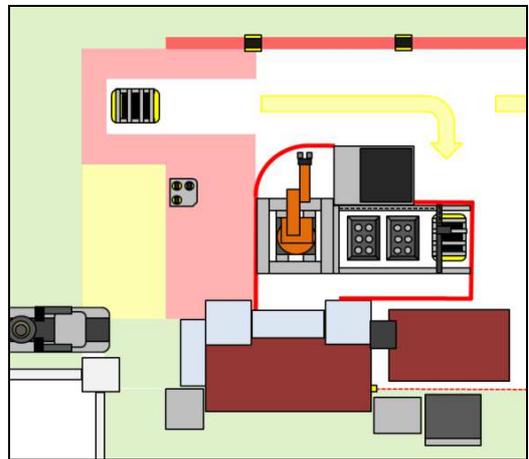
a)



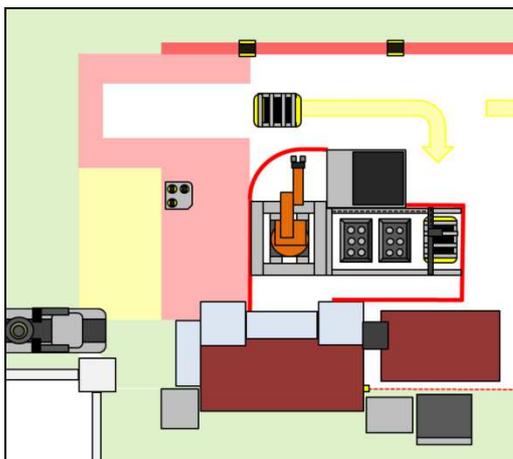
b)



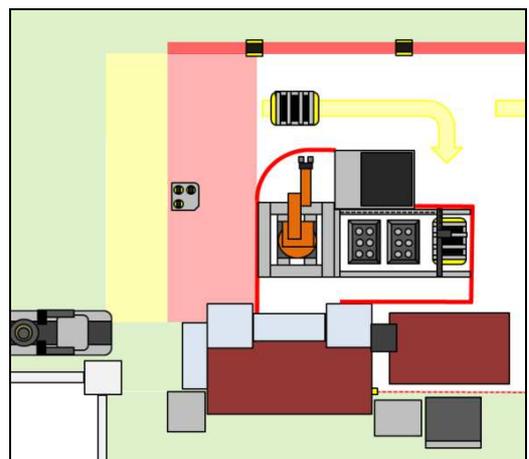
c)



d)



e)



f)

Abbildung 4.16 a) bis f): Raumzustände des Safety Eyes als Schleuse für das FTS

4.2.3 Erforderliche Abstände von Sicherheitseinrichtungen

Um Mindestabstände zu ermitteln ist es notwendig, die gesamte Nachlaufzeit (T) des Systems zu ermitteln. Dazu werden die einzelnen Signalpfade der entsprechenden Sicherheitsgeräte zu den jeweiligen Maschinen abstrahiert und die gesamte Nachlaufzeit für den jeweiligen Signalpfad aufgrund der Herstellerdaten für die entsprechenden Ansprechzeiten gebildet. Wie die Sicherheitseinrichtungen miteinander verknüpft sind ist in Abbildung 4.15 dargestellt.

Um die notwendigen Mindestabstände der berührungslos wirkenden Schutzeinrichtungen festzulegen, wird die Typ B-Norm DIN EN ISO 13855 herangezogen.

Die DIN EN ISO 13855 legt für die Annäherung mit Schrittgeschwindigkeit und für die Annäherung durch Bewegung der oberen Gliedmaßen an den Gefährdungsbereich Parameter fest und stellt somit ein bewährtes Verfahren zur Verfügung, um Mindestabstände zu ermitteln. Andere Annäherungsarten wie Laufen, Springen oder Fallen werden in dieser Norm nicht behandelt. Weiters wird ein Schutz gegen Risiken, welche durch das Herausschleudern von Teilen entstehen, in dieser Norm nicht berücksichtigt. Spezielle Daten für die Annäherung von Kindern gibt es in dieser Norm ebenfalls nicht. Falls Kinder sich dem Gefahrenbereich annähern könnten, liegt es in der Verantwortlichkeit des Konstrukteurs bei der Berechnung der Mindestabstände zu berücksichtigen, dass sich Kinder schneller bewegen könnten bzw. dass Kinder erst später von der berührungslos wirkenden Schutzeinrichtung erkannt werden könnten. [43, S. 9]

Die DIN EN ISO 13855 schreibt vor, dass Schutzeinrichtungen so konfiguriert werden müssen, dass ein unerkannter Zugang zum Gefährdungsbereich nicht möglich ist.

Der Mindestabstand, als S bezeichnet, ist in der DIN EN ISO 13855 definiert als notwendiger Abstand zwischen der Schutzeinrichtung und dem Gefährdungsbereich, der verhindern soll, dass eine Person oder ein Körperteil einer Person den Gefährdungsbereich vor Beendigung der gefahrbringenden Maschinenfunktion erreicht. [43, S. 7]

$$S = (K \cdot T) + C \quad (\text{Gl. 4.1})$$

Der Mindestabstand errechnet sich nach (Gl. 4.1), wobei in der Formel S der Mindestabstand in Millimeter und K ein Parameter in mm/s, der sich aus Daten über Annäherungsgeschwindigkeit von Körperteilen ableitet, ist. T beschreibt die gesamte Nachlaufzeit des Systems in Sekunden, die jener Zeit entspricht, die von Auslösen der Schutzrüstung bis zum Stillstand der gefahrbringenden Maschinenfunktion vergeht. C beschreibt den Eindringabstand in Millimeter, bei dem es sich um jenen

Abstand handelt, um den sich ein Körperteil, meistens eine Hand, vorbei an der Schutzeinrichtung in Richtung der Gefährdungsstelle bewegen kann, ohne dabei die Schutzeinrichtung auszulösen. [43]

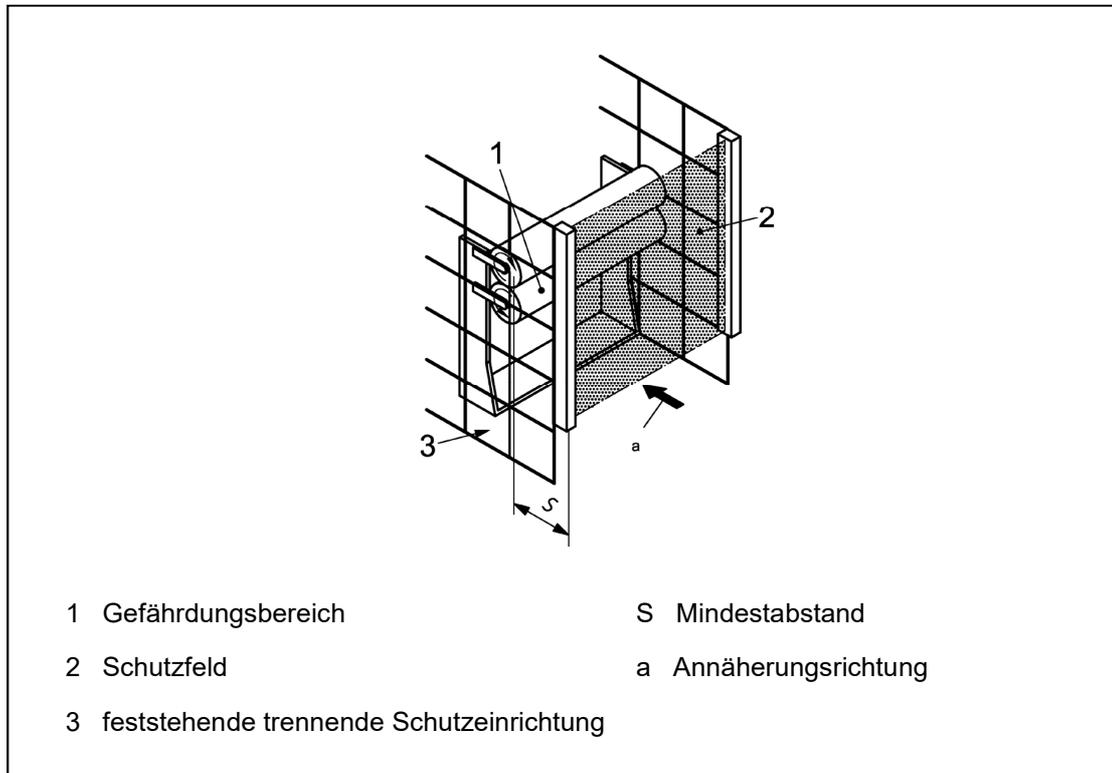


Abbildung 4.17: orthogonale Annäherung [43, S. 14]

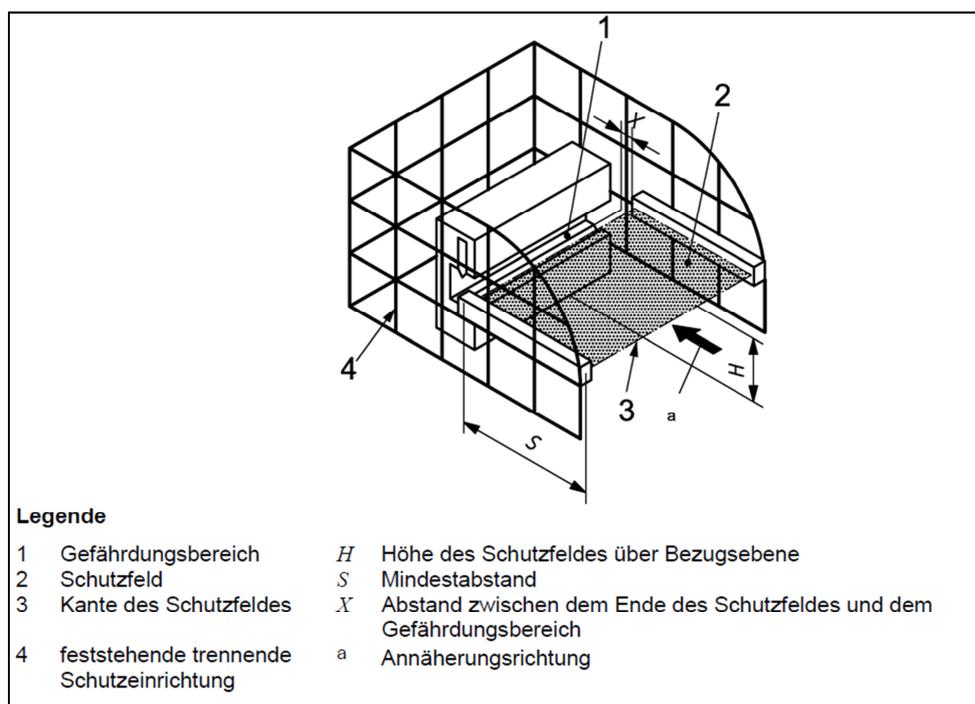


Abbildung 4.18: Annäherung parallel zur Schutzeinrichtung [43, S. 18]

Für eine Annäherung an die Gefährdungsstelle, bei der sich das Schutzfeld, wie in Abbildung 4.17 dargestellt, orthogonal zur Annäherungsrichtung befindet und einen Mindestabstand $S = 500$ mm, ist für den Wert $K = 1600$ mm/s und für C die Formel aus (Gl. 4.2) zu verwenden. Dabei beschreibt d das Sensordetektionsvermögen der Schutzeinrichtung in Millimeter und C kann nicht kleiner als null werden. Somit ergibt sich eine Formel für die Berechnung des Mindestabstandes nach (Gl. 4.3). [43, S. 19]

$$C = 8 \cdot (d - 14) \quad (\text{Gl. 4.2})$$

$$S = (1600 \cdot T) + 8 \cdot (d - 14) \quad (\text{Gl. 4.3})$$

Ist es jedoch vorhersehbar, dass berührungslos wirkende Schutzeinrichtungen in nichtindustriellen Bereichen, beispielsweise bei Demonstrationsbetrieb und möglicher Anwesenheit von Kindern, eingesetzt werden, so darf (Gl. 4.3) nicht mehr verwendet werden und es muss (Gl. 4.4) zur Berechnung des Mindestabstandes verwendet werden. [43]

$$S = (2000 \cdot T) + 8 \cdot (d - 14) + 75 \quad (\text{Gl. 4.4})$$

Je nach Sensordetektionsvermögen, kann es sein, dass für C andere Formeln angewendet werden müssen bzw. dass zusätzlichen Anforderungen für die Anordnung der Schutzeinrichtung gelten, dies kann jedoch in der DIN EN ISO 13855 nachgelesen werden.

Wird das Schutzfeld zur Erkennung des gesamten Körpers verwendet, muss die niedrigste Höhe des Schutzfeldes bei möglicher Anwesenheit von Kindern, kleiner als 200 mm sein, um ein Unterkriechen zu verhindern. Weiters muss die oberste Höhe H des Schutzfeldes größer als 900 mm sein um ein Überschreiten zu verhindern. [43, S. 14]

Erfolgt die Annäherung an die Gefährdungsstelle parallel zur Schutzeinrichtung, wie in Abbildung 4.18 dargestellt, so sind folgende Dinge zu berücksichtigen. Die niedrigste zulässige Höhe H_{\min} des Schutzfeldes berechnet sich abhängig vom Sensordetektionsvermögen nach (Gl. 4.5). Ist die Höhe H des Schutzfeldes gegeben, dann kann mit (Gl. 4.6) ein maximales Sensordetektionsvermögen (d_{\max}) in mm berechnet werden. Es muss ebenfalls sichergestellt werden, dass ein Unterkriechen nicht möglich ist. Dann errechnet sich der Mindestabstand nach (Gl. 4.7). [43]

$$H_{\min} = 15 \cdot (d - 50) \quad (\text{Gl. 4.5})$$

$$d_{max} = \left(\frac{H}{15}\right) + 50 \quad (\text{Gl. 4.6})$$

$$S = (1600 \cdot T) + (1200 - 0,4 \cdot H) \quad (\text{Gl. 4.7})$$

4.2.3.1 Mindestabstände für horizontalen Laserscanner im Bereich des Palettenregals

Da der Sicherheits-Laserscanner microScan3 Core den Bereich in der Nähe des ABB IRB 6620 überwacht, ist nur der Signalpfad bis zu diesem Roboter relevant. Die gesamte Nachlaufzeit dieses Signalpfades wird in (Gl. 4.8) und in Abbildung 4.19 dargestellt.

Um die niedrigste zulässige Höhe des horizontalen Schutzfeldes zu bestimmen, wird (Gl. 4.9) verwendet. Da das Schutzfeld auf einer Höhe von 200 mm wirkt und somit größer als die geforderte minimale Höhe ist, ist diese Anordnung zulässig.

Da hier das Schutzfeld parallel zum Gefährdungsbereich angeordnet ist, sind (Gl. 4.10) und (Gl. 4.11) anzuwenden. Somit ergibt sich nach (Gl. 4.11) ein Mindestabstand zum Gefährdungsbereich von $S = 2174$ mm. Da der eingestellte Abstand 2200 mm beträgt, ist diese Bedingung erfüllt.

$$T = 90 \text{ ms} + 19 \text{ ms} + 60 \text{ ms} + 490 \text{ ms} = 659 \text{ ms} \quad (\text{Gl. 4.8})$$

$$H_{min} = 15 \cdot (d - 50 \text{ mm}) = 15 \cdot (60 \text{ mm} - 50 \text{ mm}) = 150 \text{ mm} \quad (\text{Gl. 4.9})$$

$$C = 1200 \text{ mm} - 0,4 \cdot H = 1200 \text{ mm} - 0,4 \cdot 200 \text{ mm} = 1120 \text{ mm} \quad (\text{Gl. 4.10})$$

$$S = \left(1600 \frac{\text{mm}}{\text{s}} \cdot T\right) + C = \left(1600 \frac{\text{mm}}{\text{s}} \cdot 0,659 \text{ s}\right) + 1120 \text{ mm} = 2174 \text{ mm} \quad (\text{Gl. 4.11})$$

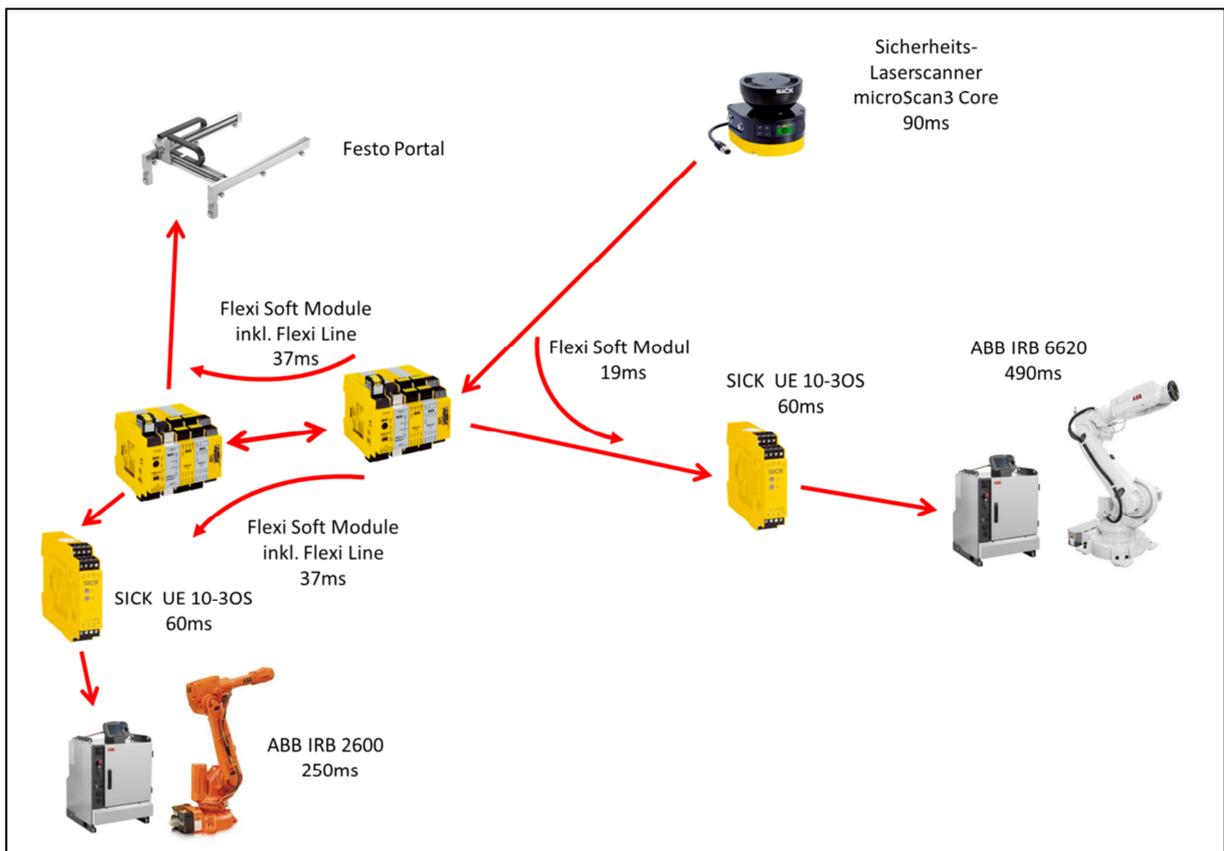


Abbildung 4.19: Signalpfade für den microScan3 [18], [28], [32], [35]–[37], [42]

4.2.3.2 Mindestabstände für vertikale Laserscanner parallel zum Leitstand

Um für die drei vertikal angeordneten Laserscanner S3000 die Mindestabstände zu ermitteln, ist zuerst die gesamte Nachlaufzeit des Systems zu bestimmen. Die Nachlaufzeit, die sich aus der Summe der Ansprechzeiten der in Reihe geschalteten Geräte ergibt, ist aber je nach Signalpfad unterschiedlich. In Abbildung 4.20 sind die unterschiedlichen Signalpfade inklusive der Verzögerungszeit der einzelnen Geräte dargestellt.

Da für die Anwendung in der Pilotfabrik davon ausgegangen wird, dass bei Führungen für Besucher möglicherweise Kinder anwesend sind, werden die Gleichungen (Gl. 4.12), (Gl. 4.14) und (Gl. 4.16) zur Berechnung des Minimalabstandes verwendet. Wie bereits in Abschnitt 3.3.1.5 beschrieben, wird die Nachlaufzeit des Festo-Portals nicht für die Berechnung der Mindestabstände verwendet, da die Geschwindigkeiten und Verzögerungszeiten des Festo-Portals verglichen mit denen des benachbarten ABB IRB 2600 verschwindend gering sind und somit der ABB IRB 2600 ausschlaggebend ist für den erforderlichen Mindestabstand der nichttrennenden Schutzeinrichtungen.

$$C = 8 \cdot (d - 14 \text{ mm}) = 8 \cdot (40 \text{ mm} - 14 \text{ mm}) = 208 \text{ mm} \quad (\text{Gl. 4.12})$$

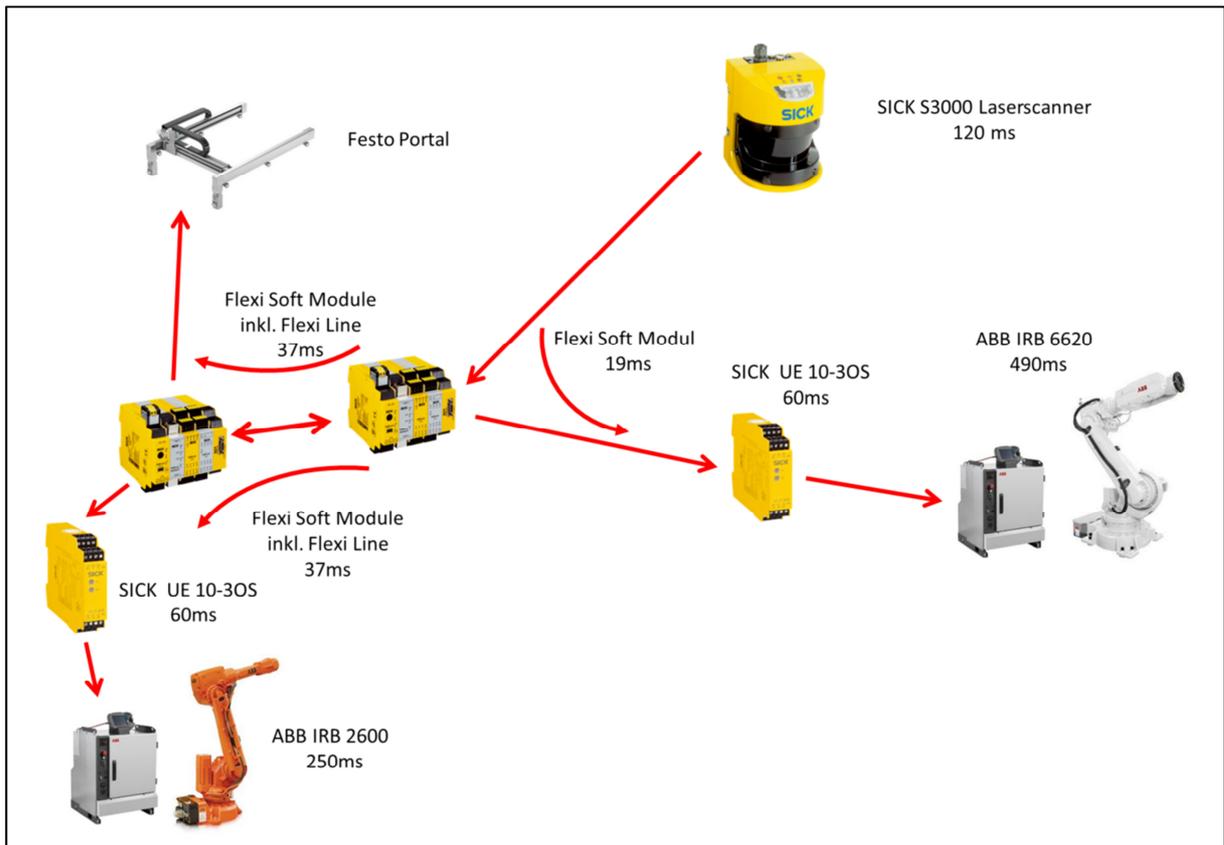


Abbildung 4.20: Signalpfade für die vertikalen Laserscanner [20], [28], [32], [35]–[37], [42]

• **Mindestabstand zum ABB IRB 6620**

Die gesamte Nachlaufzeit des Systems T über den Signalpfad bis zum ABB IRB 6620 ist in (Gl. 4.13) und in Abbildung 4.20 dargestellt. Der erforderliche Mindestabstand des betrachteten Laserscanners bis zum ABB IRB 6620 ist in (Gl. 4.14) berechnet.

$$T = 120 \text{ ms} + 19 \text{ ms} + 60 \text{ ms} + 490 \text{ ms} = 689 \text{ ms} \tag{Gl. 4.13}$$

$$S = \left(2000 \frac{\text{mm}}{\text{s}} \cdot T \right) + C + 75 \text{ mm} \\ = \left(2000 \frac{\text{mm}}{\text{s}} \cdot 0,689 \text{ s} \right) + 208 \text{ mm} + 75 \text{ mm} = 1661 \text{ mm} \tag{Gl. 4.14}$$

• **Mindestabstand zum ABB IRB 2600**

Wird der Signalpfad bis zum ABB IRB 2600 betrachtet, so ergibt sich eine andere Nachlaufzeit. Diese ist in Abbildung 4.20 und in (Gl. 4.15) dargestellt. Der erforderliche Mindestabstand des betrachteten Laserscanners bis zum ABB IRB 2600 ist in (Gl. 4.16) berechnet.

$$T = 120 \text{ ms} + 37 \text{ ms} + 60 \text{ ms} + 250 \text{ ms} = 467 \text{ ms} \tag{Gl. 4.15}$$

$$\begin{aligned}
 S &= \left(2000 \frac{\text{mm}}{\text{s}} \cdot T\right) + C + 75 \text{ mm} \\
 &= \left(2000 \frac{\text{mm}}{\text{s}} \cdot 0,467 \text{ s}\right) + 208 \text{ mm} + 75 \text{ mm} = 1217 \text{ mm}
 \end{aligned}
 \tag{Gl. 4.16}$$

4.2.3.3 Mindestabstände für das Safety Eye

Für das Safety Eye werden die Mindestabstände mit der mitgelieferten Software ermittelt. Dabei ist lediglich die Eingabe der Nachlaufzeit der Geräte des nachgeschalteten Signalpfades notwendig. In Abbildung 4.21 ist das Ergebnis aus der mitgelieferten Software des Safety Eyes dargestellt. Die Nachlaufzeit der nachgeschalteten Geräte wird hier als Nachlaufzeit der Maschine t_2 bezeichnet. In dieser Software werden für jeden Raum der Mindestabstand und die Mindestbreite des jeweiligen Schutzraumes separat berechnet. Da jedoch die Daten für alle Raumzustände identisch sind, sind die Ergebnisse ebenfalls identisch. Aus diesem Grund ist das Ergebnis nur für einen Raum dargestellt. In Abbildung 4.22 sind die Nachlaufzeiten der relevanten Geräte für die Signalpfade dargestellt. Für den Signalpfad bis zum ABB IRB 6620 ist somit eine Ansprechzeit von $T = 569 \text{ ms}$ einzusetzen und für den Signalpfad zum ABB IRB 2600 ist eine Zeit von $T = 347 \text{ ms}$ zu verwenden. Bei beiden Ansprechzeiten handelt es sich dabei um die Nachlaufzeiten der Geräte des jeweils nachgeschalteten Signalpfades ohne Berücksichtigung des Safety Eyes. Durch die verwendete Konfigurationssoftware für das Safety Eye ergibt sich somit für den Signalpfad zum ABB IRB 2600 ein minimaler Sicherheitsabstand von $S = 1,98 \text{ m}$. Da der ABB IRB 6620 um einiges weiter von der Schutzzone des Safety Eyes entfernt ist, wird der Sicherheitsabstand des Safety Eyes zum ABB IRB 6620 nicht ermittelt.

Konfigurierter Raum: 3	
Name:	Schutzraum 3
Nummer:	3
Typ:	Schutzraum
Höhe:	2 [m]
Abstand zur Anwenderenebene:	0,2 [m]
Raumanordnungsnummer:	1,2,4,5,7
Auflösung:	Körperauflösung
Informationen zu den Sicherheitsabständen für Raum: 3	
Mindestabstand S:	1,98 [m]
Mindestbreite des Schutzraums s1:	0,31 [m]
Z:	3,55 [m]
Toleranzwerte (XY):	0,15 [m]
C:	0,85 [m]
Nachlaufzeit der Maschine t2:	347 [ms]
Höchste Mehrfachauswertung:	1
Zyklen pro Auswertung:	2
Größte Ansprechzeit:	265 [ms]

Abbildung 4.21: Mindestabstände für das Safety Eye

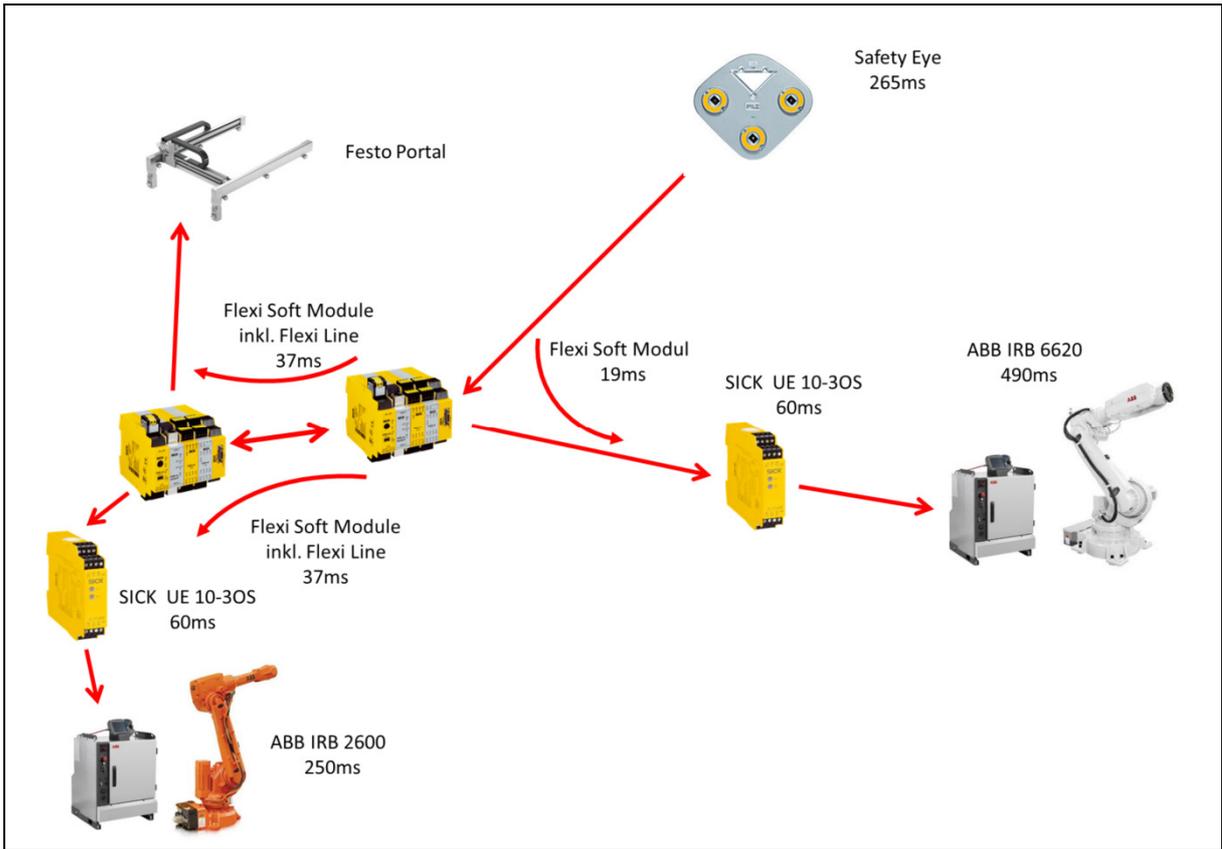


Abbildung 4.22: Signalpfade für das Safety Eye [22], [28], [32], [35]–[37], [42]

4.2.3.4 Mindestabstände für den Lichtvorhang

Werden die Mindestabstände für den Sicherheits-Lichtvorhang ermittelt, so ist der Abstand zum ABB IRB 6620 relevant, da dieser dem Sicherheits-Lichtvorhang näher liegt. Bei der Berechnung werden ebenfalls die Formeln für den Fall, dass Kinder anwesend sein könnten, verwendet. Die Signalpfade sind in Abbildung 4.23 dargestellt.

Somit ergibt sich für die Nachlaufzeit des Systems bis zum ABB IRB 6620 nach (Gl. 4.17). Der Mindestabstand zum ABB IRB 6620 ergibt sich nach (Gl. 4.18). Da C nicht kleiner als 0 sein kann, wird $C = 0$ gesetzt.

$$T = 20 \text{ ms} + 19 \text{ ms} + 60 \text{ ms} + 490 \text{ ms} = 589 \text{ ms} \quad (\text{Gl. 4.17})$$

$$S = \left(2000 \frac{\text{mm}}{\text{s}} \cdot T \right) + C + 75 \text{ mm} \\ = \left(2000 \frac{\text{mm}}{\text{s}} \cdot 0,589 \text{ s} \right) + 0 \text{ mm} + 75 \text{ mm} = 1253 \text{ mm} \quad (\text{Gl. 4.18})$$

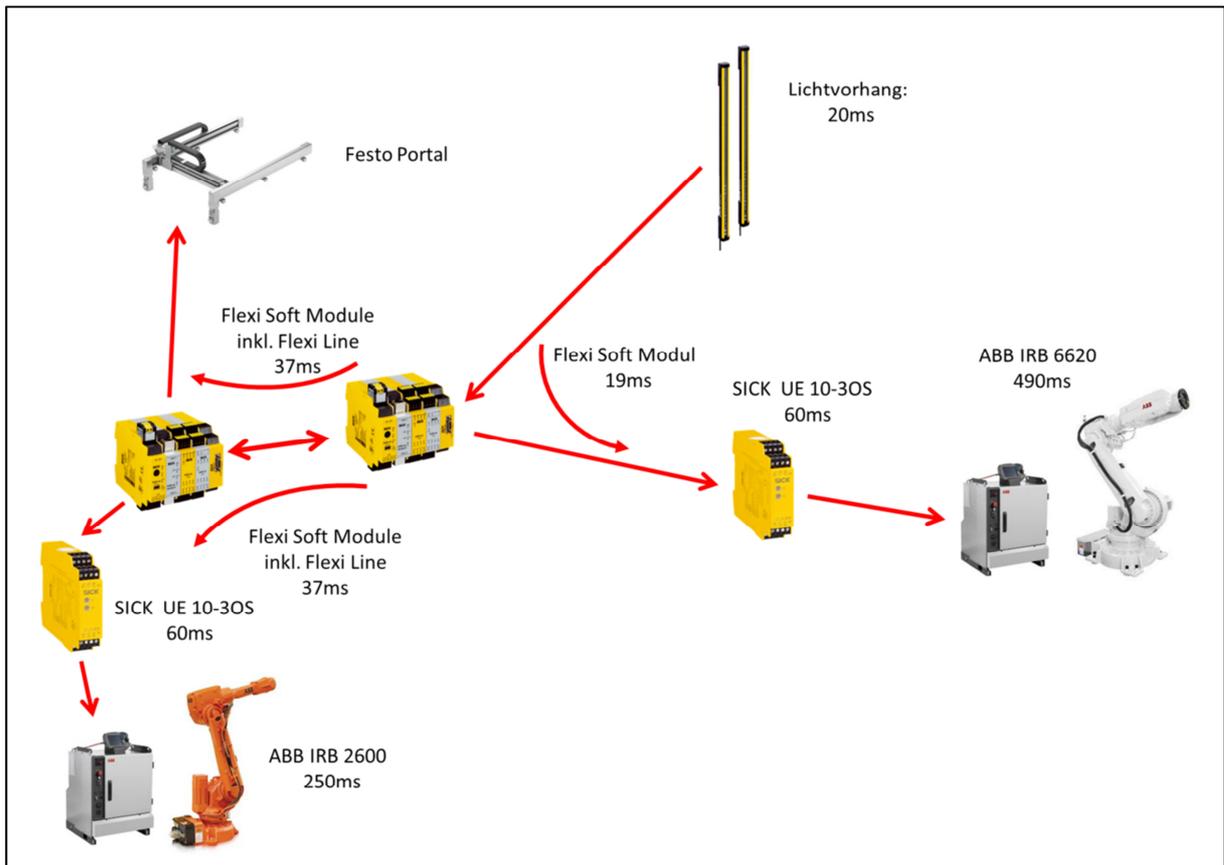


Abbildung 4.23: Signalpfade für den Sicherheits-Lichtvorhang [24], [28], [31], [35]–[37], [42]

4.2.4 Verifizierung der funktionalen Sicherheit

4.2.4.1 Bestimmung des erreichten Performance Levels

Für eine Sicherheitsfunktion werden meist mehrere Teilsysteme wie z. B. Sicherheitslaserscanner, Sicherheitssteuerungen oder Sicherheitsrelais miteinander kombiniert. Sind für die einzelnen Teilsysteme die Performance-Level bekannt, so kann das vereinfachte, tabellarische Verfahren zur Bestimmung eines gesamt Performance-Levels für eine Reihenschaltung von sicherheitsbezogenen Teilen einer Steuerung nach DIN EN ISO 13849-1 verwendet werden. Dazu muss zuerst jenes Teilsystem der Reihenschaltung mit dem niedrigsten Performance-Level ermittelt werden (PL_{niedrig}). Dann muss die Anzahl der Teilsysteme mit dem gleichen Performance-Level wie jenes Teilsystem mit dem niedrigsten Performance-Level, ermittelt werden (N_{niedrig}). Dann wird mit PL_{niedrig} und N_{niedrig} der Gesamt-PL aus Tabelle 4.3 ermittelt. [6, S. 55 f]

Um den erreichten Performance-Level zu bestimmen müssen die einzelnen Signalpfade mit den dabei verwendeten Geräten betrachtet werden. Da für die Anwendung in der Pilotfabrik ein Gesamt-Performance-Level d laut Risikobeurteilung erforderlich ist und die Sicherheitseinrichtungen mit dem niedrigsten PL die beiden Laserscannertypen mit je einem PL d sowie die SafeMove-Option der ABB Roboter

mit einem PL d sind, so dürfen in einer Reihe (entspricht einem Signalpfad) maximal drei Geräte (entspricht N_{niedrig}) mit einem PL d vorkommen, um einen Gesamt-PL d zu erreichen. Dies ist in Tabelle 4.3 durch die grün markierten Tabellen dargestellt. Da in einem Signalpfad jedoch nur zwei Geräte mit einem PL d eingesetzt werden, wird diese Bedingung erfüllt und ein Gesamt-Performance-Level von PL d wird erreicht.

PL_{niedrig}	N_{niedrig}	->	Gesamt-PL
a	> 3	->	keiner, nicht erlaubt
	≤ 3	->	a
b	> 2	->	a
	≤ 2	->	b
c	> 2	->	b
	≤ 2	->	c
d	> 3	->	c
	≤ 3	->	d
e	> 3	->	d
	≤ 3	->	e

Tabelle 4.3: Tabelle zur Ermittlung des Gesamt-PL [6, S. 56]

4.3 Risikominderung durch Hinweisende Maßnahmen und Benutzerinformation

Da es nicht möglich ist in bestimmten Lebensphasen der Maschinen die Risiken ausreichend zu minimieren, wie z. B. bei der Montage oder beim Einlernen der Roboterpositionen, sind diese Tätigkeiten nur durch Fachkräfte (Definition siehe 3.3.6.5) auszuführen. Diese Personen sind zusätzlich durch entsprechende Benutzerinformationen über die jeweils möglichen auftretenden Risiken zu informieren und haben auch dafür Sorge zu tragen, dass sich nicht unterwiesene Personen während der entsprechenden Tätigkeit nicht in den Gefährdungsbereichen aufhalten. Zusätzlich sind Fachkräfte dazu verpflichtet, eine geeignete persönliche Schutzausrüstung zu verwenden.

4.3.1 Persönliche Schutzausrüstung

Durch die TU GUT wurde eine Lärmmessung vor der MM 500 durchgeführt. Dabei wurde ein Spitzenwert von 87 dBa gemessen. Da jedoch keine Dauerbelastung durch den Lärm gegeben ist, ist Gehörschutz nicht andauernd zu tragen, sondern nur bei auftretendem Lärm.

Werden Paletten durch einen Bediener mit Werkstücken oder Spannmittel bestückt, so sind Sicherheitsschuhe zu tragen.

4.3.2 Besondere Schulung des Personals

All jene Personen, die einen Not-Halt an der Fertigungszelle quittieren dürfen, müssen zuvor ausreichend mit der Prozedur vertraut gemacht werden und müssen sich ihrer Handlung bewusst sein.

5 Industrie 4.0-Anforderungen an die funktionale Sicherheit

Da es sich bei der Umgebung Pilotfabrik, wo die sicherheitsrelevanten Themen dieser Arbeit umgesetzt werden, um eine Demonstrationsanlage für das Thema Industrie 4.0 handelt, ist dieses Thema soweit es derzeit technisch umsetzbar ist, auch in der Sicherheitstechnik zu berücksichtigen.

In der Welt der Industrie 4.0 sind Cyber-Physische Systeme (CPS) wesentliche Elemente. Diese Elemente umfassen eingebettete Systeme, Produktions-, Logistik-, Engineering-, Koordinations- und Managementprozesse sowie Internetdienste, die sowohl physikalische Daten erfassen, als auch auf physikalische Vorgänge einwirken. Besonders im Kontext von Industrie 4.0 geht es um die Anwendung von CPS in der produzierenden Industrie. Diese werden dann Cyber-Physische Produktions-Systeme (CPPS) genannt. [44]

Für die erfolgreiche Einführung von Industrie 4.0 ist ein herstellerunabhängiger Austausch von Daten und einheitlichere Schnittstellen in der Produktion notwendig. Im Maschinen- und Anlagenbau setzt sich dazu zunehmend der Standard OPC UA („Open Platform Communications Unified Architecture“) durch. OPC UA ist ein offener Schnittstellenstandard, welcher die Mechanismen der Zusammenarbeit in der industriellen Umgebung festlegt. Dadurch wird es möglich, dass die Produktion einfacher digital vernetzt werden kann. Folglich können Maschinen und Anlagen per Plug & Work nach Bedarf umgestaltet werden, unabhängig vom Hersteller der Maschinen. [45, S. 1]

OPC UA ist momentan als kein zusätzlicher Kommunikationsstandard für die Echtzeitkommunikation zu verstehen, sondern schafft einen zusätzlichen Kommunikationskanal zwischen ansonsten getrennten Kommunikationsinseln. [45, S. 2] OPC UA ist eine Service orientierte Architektur (SOA) und ermöglicht den standardisierten Datenaustausch von Maschinendaten auf Basis von Informationsmodellen und Companion Specifications. Dabei ersetzt OPC UA nicht die deterministische Kommunikation zwischen den einzelnen Maschinen, sondern ermöglicht eine Kommunikation zwischen Komponenten, Maschinen und Anlagen verschiedenster Hersteller. [45, S. 12] Hauptaufgabe von OPC UA ist die Übermittlung von Informationen für neue Industrie 4.0 Dienste. Darüber hinaus hat sich gezeigt, dass OPC UA skalierungsfähig ist, was bedeutet, dass einfache Sensoren oder Feldgeräte zukünftig mit einer entsprechenden Funktionalität ausgestattet werden können. [45, S. 2] Die Industrie 4.0-Kommunikation auf Basis von OPC UA fügt sich dem Referenzarchitekturmodell für Industrie 4.0 (RAMI 4.0) und ist auf dem Communication-Layer und Information-Layer verortet. [45, S. 5] Eine

Kommunikation auf Basis von OPC UA für eine Industrie 4.0 Kommunikation kann auf allen Ebenen der Hierarchieachse von RAMI 4.0 verwendet werden. Das bedeutet, dass OPC UA sowohl in kleinsten Sensoren als auch für die fabriksübergreifende Kommunikation verwendet werden kann. [45, S. 28] Damit eine Komponente als Industrie 4.0-Komponente gilt, muss sie zumindest als Entität verwaltet werden und mindestens passiv kommunikationsfähig sein, Näheres dazu siehe DIN SPEC 91345. [46, S. 17] Eine Entität bezeichnet einen eindeutig identifizierbaren Gegenstand, der in der Informationswelt verwaltet wird und dessen notwendige Daten durch eine Industrie 4.0-konforme Kommunikation der Außenwelt zur Verfügung gestellt werden. [46, S. 13]

Auf die umgesetzte Sicherheitssteuerung bezogen bedeutet dies, dass zumindest Daten bzw. Variablen der Sicherheitssteuerung über eine Industrie 4.0-konforme Kommunikation der Außenwelt zum Lesen bereitgestellt werden sollen, damit die Sicherheitseinrichtungen insgesamt als eine Industrie 4.0 Komponente gewertet werden können. Dabei ist besonders darauf zu achten, dass das Bereitstellen der Daten über eine Industrie 4.0-konforme Kommunikation die sicherheitskritische Verarbeitung nicht beeinträchtigt und keine zusätzliche Ansprechzeit für sicherheitsrelevante Signale verursacht. Zusätzlich darf es nicht möglich sein, über eine Industrie 4.0-konforme Kommunikation ein sicherheitsrelevantes Signal zu beeinflussen, da die Industrie 4.0-konforme Kommunikation derzeit noch nicht für sicherheitsrelevante Kommunikation zertifiziert ist. Das bedeutet weiters, dass ein externes Gerät, wie z. B. ein Not-Halt Taster, derzeit noch nicht wie ein eigenständiges Industrie 4.0 Gerät verwendet werden kann, sofern es sich dabei um ein sicherheitskritisches Signal handelt. Dies ist derzeit noch nicht möglich, da es noch keinen Kommunikationsstandard gibt, der sowohl die Anforderungen des Referenzarchitekturmodells für Industrie 4.0, als auch die Anforderungen für eine fehlersichere Kommunikation, die notwendig sind, um einen bestimmten Sicherheits-Integritätslevel bzw. Performance-Level zu erreichen, erfüllt. Somit erfolgt die Kommunikation für sicherheitsrelevante Signale immer noch I/O basiert bzw. über sichere Feldbusse.

Um der Sicherheitseinrichtung in der Pilotfabrik den Charakter einer Industrie 4.0-Komponente zu verleihen, wird die eingesetzte Siemens F-SPS dazu verwendet, Statusvariablen wie z. B. aktive Sicherheitseinrichtungen oder einen aktiven Not-Halt-Zustand nach außen nur zum Lesen zugänglich zu machen, und dabei die Industrie 4.0-konforme Kommunikation berücksichtigt. Dies ist möglich, da die F-SPS OPC UA unterstützt. Um die Funktionsfähigkeit etwas auszuweiten, wird die Raumumschaltung des Safety Eyes, damit das FTS die Fertigungszelle verlassen und hineinfahren kann, ebenso durch die F-SPS verwaltet. Diese Raumumschaltung stellt keinen sicherheitskritischen Prozess dar, da die Auswerteeinheit des Safety-Eyes erkennt, ob der gewünschte Raumzustand erlaubt ist, bzw. nur einen aktiven

Raumzustand erlaubt und im Fehlerfall einen Not-Halt des Safety-Eyes ausgibt. In der F-SPS wird eine OPC UA Methode zur Raumumschaltung implementiert, die es ermöglicht, den Raumzustand des Safety-Eyes über OPC UA zu ändern. Dadurch ist es möglich, dass das FTS den Schutzraum der Fertigungszelle verlassen und hineinfahren kann, ohne dabei einen Not-Halt auszulösen.

Um eine Verbindung über OPC UA mit der Sicherheits-SPS herzustellen, kann beispielsweise das Programm „Unified Automation UaExpert“ verwendet werden. Dieses Programm stellt einen einfachen OPC UA Client mit einer übersichtlichen Benutzeroberfläche zur Verfügung. Dadurch können beispielsweise OPC UA Variablen betrachtet oder Methoden manuell ausgeführt werden, um die Funktionalität vorab zu testen. Die Einstellungen, die notwendig sind, um die Sicherheits-SPS mit OPC UA zu erreichen, sind in Abbildung 5.1 dargestellt. Um die Sicherheits-SPS mit der Programmiersoftware TIA-Portal von Siemens zu erreichen, so kann diese mit „erweitert online verbinden“ und mit den Einstellungen aus Abbildung 5.2 erreicht werden.

Im fertigen Zustand der Zelle soll jedoch ein Transportleitsystem die Methoden zur Raumzustandsänderung des Safety-Eyes aufrufen und die Orchestrierung der einzelnen Maschinen übernehmen.

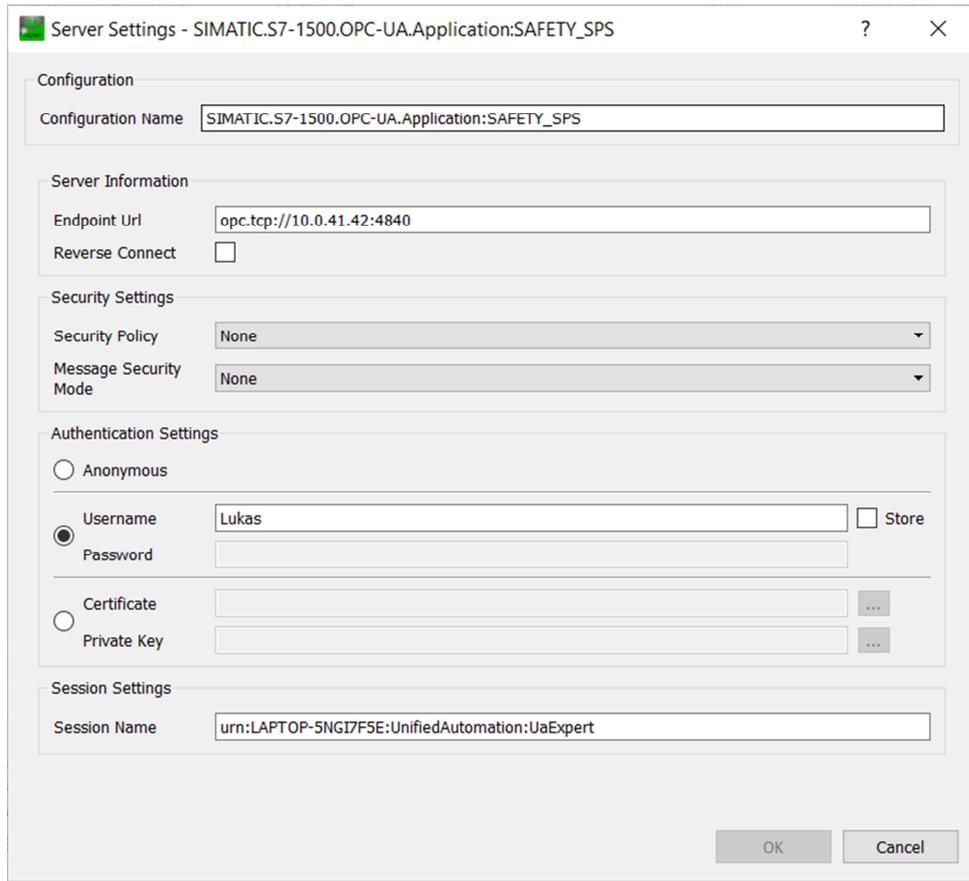


Abbildung 5.1: Erreichbarkeit der Sicherheitssteuerung über OPC UA

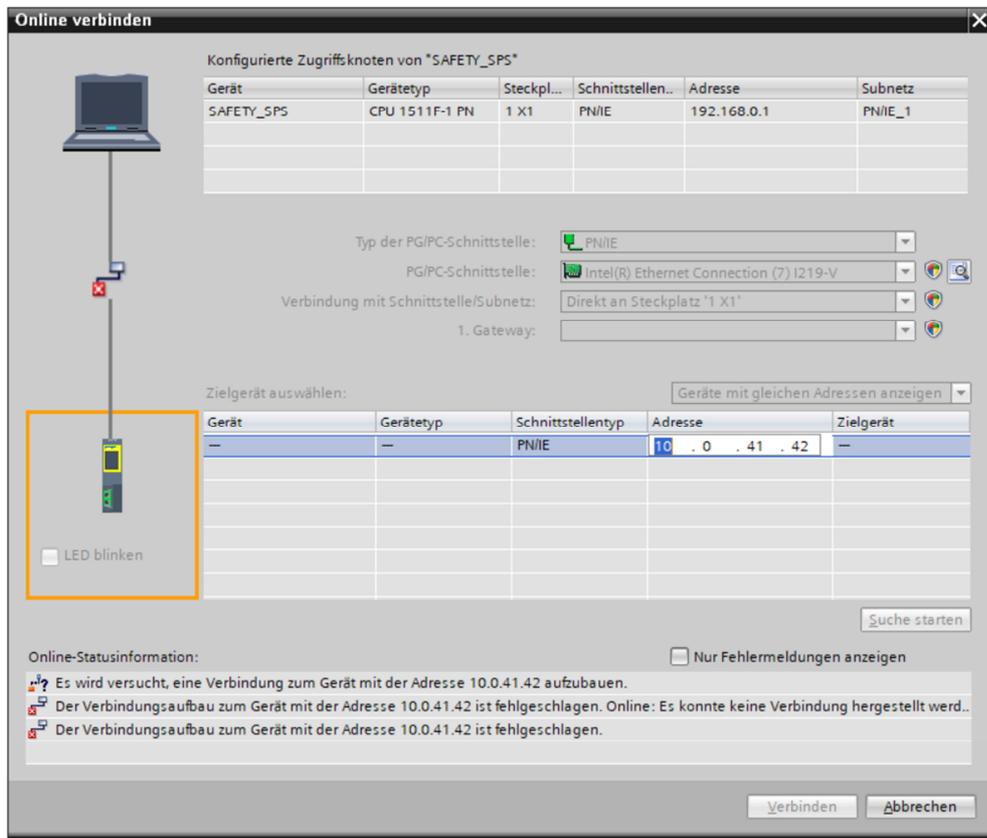


Abbildung 5.2: Online Verbindung zur Safety SPS über TIA-Portal

6 Resümee und Ausblick

Das umgesetzte Sicherheitskonzept ist in erster Linie für einen Demonstrationsbetrieb ausgelegt und berücksichtigt dabei auch Besucher und Kinder, die bei Industrieanwendungen keine Berücksichtigung finden würden. Selbst ohne der Berücksichtigung von Kindern und Besuchern ist ein komplexeres Sicherheitskonzept erforderlich, da sich in der Pilotfabrik der TU Wien viele unterschiedliche Mitarbeiter, Studenten, etc. mit unterschiedlichstem fachlichem Hintergrund aufhalten. Da diese häufig wechseln ist somit eine Einschulung aller Personen nur schwer möglich. Daher musste das Sicherheitskonzept so gestaltet werden, dass es erst durch einen eingesteckten Schlüsselschalter, der abgezogen werden kann, ermöglicht wird, die Fertigungszellen im Fertigungsbereich im Automatik-Betrieb zu starten.

Somit ist das umgesetzte Sicherheitskonzept nicht unbedingt das einfachste und kostengünstigste und würde in der Industrie für eine ähnliche Anwendung auf diese Art und Weise eher nicht umgesetzt werden. Es wurden viele unterschiedliche Typen von Sicherheitseinrichtungen wie etwa ein Safety Eye, Laserscanner und Lichtvorhänge eingesetzt. Dies war zum einen notwendig, da das FTS im Betrieb in den geschützten Bereich hineinfahren bzw. diesen verlassen muss und zum anderen, um die Sicht auf die Anlagen nicht einzuschränken. Ohne diese Gründe wäre es möglich ein kostengünstigeres Sicherheitskonzept z. B. mit fest montierten Schutzgittern zu realisieren.

Das Konzept von Industrie 4.0 sieht eine individuell und flexibel auf Kundenwünsche reagierende Produktion vor. Aus diesem Grund müssen sich die Maschinen und Anlagen in der Produktion selbsttätig und auftragsbezogen während der Laufzeit konfigurieren können, um eine entsprechende Individualisierung des Produktes zu erreichen. Die heutigen sicherheitstechnischen Konzepte gehen zwar von variablen aber vorab eindeutig definierten Prozessen aus, die jedoch keine einfache Rekonfiguration der Maschine oder Anlage während der Laufzeit zulassen. Diese sicherheitstechnischen Beurteilungsmethoden gehen davon aus, dass die Maschine oder Anlage nach der Inbetriebnahme nicht mehr verändert wird. Vor jeder Änderung ist eine erneute sicherheitstechnische Überprüfung bzw. Validierung notwendig. Dies wird auch ausdrücklich in den aktuellen Sicherheitsnormen beschrieben, die eine dynamische Rekonfiguration der Systeme während der Laufzeit explizit verbieten. [44]

Mit einer Rekonfiguration der Maschinen und Anlagen während der Laufzeit geht notwendigerweise auch eine Rekonfiguration der Sicherheitsfunktionen während der Laufzeit einher. Nach der Neuvernetzung muss die erforderliche Sicherheitsstufe (SIL bzw. PL), für die neue Kombination erreicht werden. Diese Validierung muss

zukünftig während der Laufzeit durchgeführt werden können. Dies erfordert jedoch, dass die heute weitgehend manuellen Abläufe zur Risikoanalyse und Risikobewertung automatisierbar und vernetzbar werden müssen. Nur auf diese Art und Weise kann das derzeitige Sicherheitsniveau aufrechterhalten werden. [44]

Für die Sicherheit von Maschinen sind heute zwei Punkte entscheidend. Zum einen die Produkt- und Betriebssicherheit bzw. funktionale Sicherheit (Safety), die auch in dieser Arbeit behandelt wurde, sowie die Daten-, Informations- und Kommunikationssicherheit (Security). Die massive zusätzliche Vernetzung schafft eine neue Art von Security-Gefährdungen für die industrielle Produktion mit potentiellen Auswirkungen auf Aspekte der funktionalen Sicherheit. Die beiden Punkte Safety und Security entstammen zwar unterschiedlichen Fachdisziplinen, sind jedoch unbedingt als Gesamtsystem zu betrachten, da sich die beiden Aspekte gegenseitig beeinflussen können. Beispielsweise kann bei mangelhafter Angriffssicherheit eine Manipulation an der Maschinensteuerung zum Ausfall von bestimmten Sicherheitsfunktionen führen. Dadurch steigt die Gefahr für die Beschäftigten. Bevor sich CPPS erfolgreich durchsetzen können, werden jedoch geeignete Sicherheitsarchitekturen, Schutzmaßnahmen und Validierungsmethoden benötigt. Die funktionale Sicherheit der Prozesse muss die heutigen Standards der Automation weiterhin erfüllen und daher unangetastet bleiben. [44], [47, S. 7]

Derzeit ist eine fehlersichere Kommunikation über Feldbus oder Industrial Ethernet nur auf reine Master-Slave bzw. Controller-Device Architektur begrenzt. Für die sichere Kommunikation zwischen den Maschinen (Controller-Controller-Kommunikation) sind entsprechende Koppler erforderlich, die jedoch keinen herstellerübergreifenden Standards entsprechen. [48]

PI (PROFIBUS & PROFINET International) hat sich daher entschieden, die Mechanismen von OPC UA auch auf PROFI-safe auszuweiten um somit eine fehlersichere Controller-Controller Kommunikation zu erreichen. [48] Die Spezifikation „PROFI-safe over OPC UA“, welche die bestehenden Mechanismen von PROFI-safe verwendet, befindet sich derzeit allerdings noch im Review. Somit gibt es wie bisher für PROFI-safe ein einziges Kabel sowohl für die Standard-Kommunikation als auch für die fehlersichere Kommunikation. Dabei wird wie bei PROFI-safe das Black Channel Prinzip verwendet, jedoch übernimmt das OPC UA Kommunikations-Protokoll die Rolle des Black Channels. Zusätzlich werden Protokoll-Sicherungsmechanismen, welche bereits für PROFI-safe existieren, übernommen. Durch „PROFI-safe over OPC UA“ wird es möglich Verbindungen auch zur Laufzeit zu verändern, wodurch ein dynamischer Verbindungsaufbau möglich wird. Daher müssen die an der sicheren Kommunikation teilnehmenden Geräte nicht schon bei der Projektierung bekannt sein, so wie es derzeit bei den verfügbaren sicheren Kommunikationsprotokollen üblich ist. Somit wird es möglich der Anlage eine neue

Maschine hinzuzufügen oder eine bestehende Maschine zu ersetzen, ohne dass alle anderen Maschinen neu konfiguriert werden müssen. Dies erleichtert es eine fehlersichere Kommunikation zwischen den Maschinen aufzubauen. [49]

Eine sichere Kommunikation basierend auf OPC UA würde eine wesentliche Vereinfachung der Inbetriebnahme von Sicherheitsgeräten für Hersteller bzw. Systemintegratoren bedeuten und einen guten Ausgangszustand für eine mögliche Rekonfiguration von Sicherheitsfunktionen der Maschine bzw. Anlage während der Laufzeit ermöglichen.

Die derzeit eingesetzten sicherheitszertifizierten Kommunikationsmodelle, wie etwa sichere Feldbusse für einen sicheren Datenaustausch von Maschine zu Maschine, sind derzeit noch wenig flexibel und stellen einen erheblichen Konfigurationsaufwand dar, sofern entsprechend dem grundlegenden Konzept von Industrie 4.0 an der Maschinenkonfiguration etwas geändert werden können soll. Ebenso ist bei Änderungen eine erneute Gesamtvalidierung erforderlich, die sicherstellt, dass die neue Konfiguration die erforderlichen Sicherheitsfunktionen ordnungsgemäß erfüllt.

Bei flexiblen automatisierten Fertigungszellen, bei denen die einzelnen Maschinen häufiger durch andere ersetzt werden sollen, um wechselnden Anforderungen optimal entgegenzuwirken, ist bei einer Änderung der Hardware jedes Mal eine neue Risikobeurteilung nach DIN EN ISO 12100 mit entsprechender Dokumentation durchzuführen. Dies ist notwendig, um die Anforderungen der Maschinenrichtlinie zu erfüllen und sämtliche sicherheitsrelevanten Anforderungen bereitzustellen. Da es sich dabei um einen Prozess handelt, der in der Industrie meist durch externe, spezialisierte Firmen durchgeführt wird, wäre es vorteilhaft, wenn die notwendigen Dokumentationen und Informationen, die für die weitere Risikominderung notwendig sind, ebenfalls automatisiert erstellt werden.

Ein flexibler Aufbau von Sicherheitskomponenten durch eine Plug & Work Methode, wäre wünschenswert, da somit einzelne Sicherheitseinrichtungen, wie z. B. ein Laserscanner, relativ problemlos durch ein anderes Modell, wie beispielsweise ein neueres Modell mit mehr Features, ersetzt werden könnte. Dies ist nach derzeitigem Stand nicht so ohne weiteres möglich, da zum einen die Industrie 4.0-Kommunikation noch nicht für eine fehlersichere Kommunikation geeignet ist und zum anderen der Prozess der Risikobeurteilung und Gefährdungsminderung erneut durchgegangen werden muss, um die Anforderungen an die Maschinenrichtlinie nach den jeweiligen harmonisierten Normen zu erfüllen. Ein wichtiges Ziel für die Zukunft ist es, diesen Prozess des Ersetzens von Sicherheitseinrichtungen zu vereinfachen und somit eine höhere Flexibilität in die bisher eher unflexiblen Lösungen für die funktionale Sicherheit zu bringen. Dazu wird es notwendig sein, geeignete Werkzeuge zu programmieren, die es erlauben, den Prozess der Risikobeurteilung und anschließenden Dokumentation für die jeweiligen verwendeten

Sicherheitseinrichtungen zu automatisieren. Damit eine entsprechende Dokumentation für die unterschiedlichsten Sicherheitseinrichtungen entsprechend automatisch generiert werden kann, wäre eine Datenbank mit Werten wie z. B. Ansprechzeiten, Sicherheitsintegritätslevel etc. von sämtlichen auf dem Markt verfügbaren Sicherheitseinrichtungen vorteilhaft. Erst wenn für die Validierung wenig menschliche Arbeit notwendig ist, ist ein flexibler Austausch von Sicherheitselementen mit entsprechender Erfüllung aller zu berücksichtigen Normen sinnvoll möglich. Ein weiterer Punkt, der noch einige Entwicklungsarbeit verlangt, ist die Kommunikation von Sicherheitseinrichtungen über einen Industrie 4.0 konformen Kommunikationskanal. Dies würde die Anbindung von Geräten wesentlich erleichtern und dazu beitragen, dass eine flexible Fabrik weniger Arbeitsaufwand erfordert.

Literaturverzeichnis

- [1] SICK AG, „Leitfaden Sichere Maschinen, In 6 Schritten zur sicheren Maschine“.
- [2] „DIN EN ISO 12100:2011-03, Sicherheit von Maschinen – Allgemeine Gestaltungsleitsätze – Risikobeurteilung und Risikominderung (ISO 12100:2010)“.
- [3] „DIN EN ISO 11161:2010-10 Sicherheit von Maschinen - Integrierte Fertigungssysteme - Grundlegende Anforderungen (ISO 11161:2007 + Amd 1:2010)“.
- [4] „DIN ISO/TR 14121-2 DIN SPEC 33885:2013-02, Sicherheit von Maschinen – Risikobeurteilung – Teil 2: Praktischer Leitfaden und Verfahrensbeispiele (ISO/TR 14121-2:2012)“.
- [5] „DIN ISO/TR 23849 DIN SPEC 33883:2014-12, Leitfaden zur Anwendung von ISO 13849-1 und IEC 62061 bei der Gestaltung von sicherheitsbezogenen Steuerungen für Maschinen (ISO/TR 23849:2010)“.
- [6] „DIN EN ISO 13849-1:2016-06, Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen – Teil 1: Allgemeine Gestaltungsleitsätze (ISO 13849-1:2015)“.
- [7] „DIN EN 62061 (VDE 0113-50):2016-05, Sicherheit von Maschinen – Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme (IEC 62061:2005 + A1:2012 + A2:2015)“.
- [8] „DIN EN 60204-1 (VDE 0113-1):2007-06 Sicherheit von Maschinen – Elektrische Ausrüstung von Maschinen – Teil 1: Allgemeine Anforderungen (IEC 60204-1:2005, modifiziert); Deutsche Fassung EN 60204-1:2006“.
- [9] Europäisches Parlament, „Richtlinie 2006/42/EG des europäischen Parlaments und des Rates vom 17. Mai 2006 über Maschinen und zur Änderung der Richtlinie 95/16/EG (Neufassung)“, *Amtsblatt der Eur. Union*, S. 24–86, 2006.
- [10] ABB, *Product specification Robot stopping distances according to ISO 10218-1*, Document ID: 3HAC048645-001 Revision: G. 2017.
- [11] ABB, *Anwendungshandbuch SafeMove DokumentNr: 3HAC050974-003*. 2016.
- [12] „DIN EN ISO 13850:2016-05 Sicherheit von Maschinen - Not-Halt-Funktionen - Gestaltungsleitsätze (ISO 13850:2015); Deutsche Fassung EN ISO 13850:2015“.
- [13] „EMCO MAXXMILL 500“. [Online]. Verfügbar unter: https://www.emco-world.com/fileadmin/_processed_/1/4/csm_pic_MM500_offen_1200x900px_web_67c0153d04.png. [Zugegriffen: 03-Mai-2019].
- [14] ABB, *Anwendungshandbuch Funktionssicherheit und SafeMove*. 2017.
- [15] RIS, „Verordnung über den Schutz der Arbeitnehmer/innen vor der Gefährdung

- durch Lärm und Vibrationen (Verordnung Lärm und Vibrationen – VOLV) StF: BGBl. II Nr. 22/2006 [CELEX-Nr.: 32002L0044, 32003L0010]“. [Online]. Verfügbar unter: www.ris.bka.gv.at/GeltendeFassung/Bundesnormen/20004576/VOLV%2CFassung_vom_18.03.2019.pdf. [Zugegriffen: 18-März-2019].
- [16] „DIN EN ISO 10218-1:2012-01, Industrieroboter - Sicherheitsanforderungen - Teil 1: Roboter (ISO 10218-1:2011)“.
- [17] SICK AG, *Betriebsanleitung microScan3 Sicherheits-Laserscanner 8016345/YSQ9/2016-04-25*. Waldkirch Deutschland.
- [18] „Sicherheits-Laserscanner microScan3 Core / microScan3 Core I/O“. [Online]. Verfügbar unter: <https://cdn.sick.com/media/ZOOM/7/57/257/IM0061257.png>. [Zugegriffen: 10-Feb-2019].
- [19] SICK AG, *Betriebsanleitung S3000 Sicherheits-Laserscanner 8009937/YY95/2016-02-10*. Waldkirch Deutschland.
- [20] „Sicherheits-Laserscanner S3000 Advanced“. [Online]. Verfügbar unter: <https://cdn.sick.com/media/ZOOM/5/55/555/IM0007555.png>. [Zugegriffen: 10-Feb-2019].
- [21] Pilz GmbH & Co. KG, „SafetyEYE - Sichere Kamerasysteme - Bedienungsanleitung - Nr. 21743-DE-14“.
- [22] PILZ, „Safety Eye“. [Online]. Verfügbar unter: https://www.pilz.com/imagecache/mam/pilz/images/uploads/f_safetyeye_f2_3c_2017_09_218x218-desktop-1507619338.jpg. [Zugegriffen: 01-März-2019].
- [23] SICK AG, *Betriebsanleitung deTec4 Core Sicherheits-Lichtvorhang 8014252/ZOH3/2017-08-04*. Waldkirch Deutschland.
- [24] „Sicherheits-Lichtvorhänge deTec / deTec4 Core / Typ 4“. [Online]. Verfügbar unter: <https://cdn.sick.com/media/ZOOM/6/76/076/IM0047076.png>. [Zugegriffen: 10-Feb-2019].
- [25] SICK AG, *Betriebsanleitung STR1 Sicherheitsschalter*. Waldkirch Deutschland.
- [26] „Berührungslose Sicherheitsschalter STR1 / Sensor und Betätiger“. [Online]. Verfügbar unter: <https://cdn.sick.com/media/ZOOM/3/43/143/IM0062143.png>. [Zugegriffen: 10-Feb-2019].
- [27] SICK AG, *Betriebsanleitung Flexi Soft Modulare Sicherheitssteuerung - Hardware 8012477/ZYK0/2018-10-22*. Waldkirch Deutschland.
- [28] „Sicherheitssteuerungen Flexi Soft“. [Online]. Verfügbar unter: <https://cdn.sick.com/media/895/5/05/605/IM0074605.png>. [Zugegriffen: 10-Feb-2019].
- [29] SICK AG, *Betriebsanleitung UE4740 PROFINET IO PROFIsafe EFI-Gateway 8020181/ZJN2/2017-04-20*. Waldkirch Deutschland.
- [30] „Zubehör Module und Gateways“. [Online]. Verfügbar unter: <https://cdn.sick.com/media/ZOOM/6/16/616/IM0045616.png>. [Zugegriffen: 10-

- Feb-2019].
- [31] SICK AG, *Betriebsanleitung UE10-3OS Erweiterungsgerät für Basisgeräte 8009656/YSS0/2016-03-17*. Waldkirch Deutschland.
- [32] „SICK Sicherheitsschaltgeräte UE10-3OS“. [Online]. Verfügbar unter: <https://cdn.sick.com/media/895/3/83/383/IM0045383.png>. [Zugegriffen: 10-Feb-2019].
- [33] Siemens, „Datenblatt 6ES7511-1FK02-0AB0 SIMATIC S7-1500F“, 2019.
- [34] „Siemens SIMATIC S7-1500F“. [Online]. Verfügbar unter: https://www.automation.siemens.com/bilddb/interfaces/InterfacelImageDB.asmx/GetImageVariant?objectkey=P_ST70_XX_07840&imagevariantid=16&lang=&interfaceuserid=MALL. [Zugegriffen: 10-Feb-2019].
- [35] ABB, „ABB IRB 6620“. [Online]. Verfügbar unter: <https://imageservice.abb.com/public/images/7416d241-c715-4e35-9ef4-bc96f11bedb6/presentation.jpg?target=https%253A%252F%252Fabbcloud.blob.core.windows.net%252Fpublic%252Fimages%252F7416d241-c715-4e35-9ef4-bc96f11bedb6%252Fpreview.jpg%253Fcrop%253D0%252C7%252C400%252C312%2526width%2525>. [Zugegriffen: 01-März-2019].
- [36] ABB, „ABB IRB 2600“. [Online]. Verfügbar unter: http://www.mfgnewsweb.com/archives/automation_assembly/jul11/ABB_IRB_2600_Robot_Family_pix_files/image003.jpg. [Zugegriffen: 01-März-2019].
- [37] ABB, „IRC5“. [Online]. Verfügbar unter: <https://imageservice.abb.com/public/images/831fa6d4-2ec7-40fe-808f-30ad62079a4e/preview.jpg?target=https%3A%2F%2Fabbcloud.blob.core.windows.net%2Fpublic%2Fimages%2F831fa6d4-2ec7-40fe-808f-30ad62079a4e%2Fpreview.jpg%3Fcrop%3D0%2C7%2C400%2C376%26width%3D400>. [Zugegriffen: 01-März-2019].
- [38] Automation24, „NOT-AUS Drucktaster“. [Online]. Verfügbar unter: https://media.automation24.com/Artikelbilder/Shop800px/100978_1.jpg. [Zugegriffen: 01-März-2019].
- [39] „EMCO MAXXTURN 45“. [Online]. Verfügbar unter: https://kapema.dk/wp-content/uploads/2017/11/MT_45.jpg. [Zugegriffen: 03-Mai-2019].
- [40] „Jenoptik - Wellenmessmaschine“. [Online]. Verfügbar unter: <https://www.jenoptik.de/-/media/websiteimages/metrology/optical/spc-measuring-station/opticline-hommel-etamic-c308.jpg>. [Zugegriffen: 03-Mai-2019].
- [41] „IGM Schweißroboter“. [Online]. Verfügbar unter: <https://yt3.ggpht.com/a-/ACSszfELB9-Twbjla1xDNo25H2AIX8NCGiNx4onKiw=s900-mo-c-c0xffffff-rj-k-no>. [Zugegriffen: 03-Mai-2019].
- [42] „FESTO - Portal“. [Online]. Verfügbar unter: https://www.festo.com/rep/de-at/assets/EXCH_17683mu_4_710px.jpg. [Zugegriffen: 10-Feb-2019].
- [43] „DIN EN ISO 13855:2010-10, Sicherheit von Maschinen - Anordnung von

- Schutzeinrichtungen im Hinblick auf Annäherungsgeschwindigkeiten von Körperteilen (ISO 13855:2010)“.
- [44] B. Kasper, *Weiterentwicklung sicherheitstechnischer Analyse- und Bewertungsmethoden für die Industrie 4.0*. Dresden: Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA).
- [45] F. Pethig u. a., „Industrie 4.0 Kommunikation mit OPC UA - Leitfaden zur Einführung in den Mittelstand“, *VDMA Verlag*, S. 28, 2017.
- [46] „DIN SPEC 91345:2016-04 Referenzarchitekturmodell Industrie 4.0 (RAMI4.0)“.
- [47] K. Bettenhausen und S. Kowalewski, „Cyber-Physical Systems : Chancen und Nutzen aus Sicht der Automation“, *VDI/VDE-Gesellschaft Mess- und Autom.*, Nr. April, S. 1–12, 2013.
- [48] PI (PROFIBUS & PROFINET International), „Pressemitteilung - PROFI-safe für OPC UA - Die Vernetzung von Maschinen wird fehlersicher“, Nürnberg, 29-Nov-2017.
- [49] M. Walter, „The ‘Safety over OPC UA’ Concept“, 2019. [Online]. Verfügbar unter: <http://profinews.com/2019/03/the-safety-over-opc-ua-concept/>. [Zugegriffen: 14-Juni-2019].

Abbildungsverzeichnis

Abbildung 1.1: Anordnung der Maschinen	8
Abbildung 2.1: Prozess der Risikobeurteilung und Risikominderung [2, S. 16]	12
Abbildung 2.2: Risikoelemente [2, S. 24].....	15
Abbildung 2.3: Auswahl von Schutzeinrichtungen gegen Gefährdungen, die von sich bewegenden Teilen ausgehen [2, S. 44]	19
Abbildung 2.4: Graph zur Bestimmung des erforderlichen PL [6, S. 63]	27
Abbildung 3.1: Anordnung der verketteten Maschinen.....	30
Abbildung 3.2: Drehzelle ohne Wellenmessmaschine.....	31
Abbildung 3.3: Wellenmessmaschine Opticline C 308	34
Abbildung 3.4: Hybrid Bearbeitungszelle.....	35
Abbildung 3.5: EMCO MT 500 [13].....	36
Abbildung 3.6: Inneres der Schweißzelle	37
Abbildung 3.7: Schnittstellen zwischen den Maschinen	40
Abbildung 3.8: Räumliche Grenzen der Gefährdungsbereiche	46
Abbildung 3.9: Beispiel zur Ermittlung des erforderlichen PL nach [6]	52
Abbildung 4.1: Sicherheits-Laserscanner microScan3 Core I/O [18].....	55
Abbildung 4.2: Sicherheits-Laserscanner S3000 Advanced [20].....	56
Abbildung 4.3: Safety Eye [22]	57
Abbildung 4.4: Sicherheits-Lichtvorhang deTec / Typ 4 [24]	57
Abbildung 4.5: Berührungsloser Sicherheitsschalter STR1 [26].....	58
Abbildung 4.6: Flexi Soft Sicherheitssteuerung mit unterschiedlichen Modulen [28].	59
Abbildung 4.7: SICK PROFIsafe Gateway UE4740-22H0000 [30].....	59
Abbildung 4.8: Sicherheitsschaltgerät UE10-3OS [32].....	60
Abbildung 4.9: Siemens SIMATIC S7-1500F [34]	60
Abbildung 4.10: SafeMove Zonen für die MM 500	61
Abbildung 4.11: SafeMove Zonen für die IGM-Zelle.....	61
Abbildung 4.12: Bedienmodul am Leitstand	62
Abbildung 4.13: Räumliche Anordnung der Sicherheitsgeräte	63
Abbildung 4.14: Laserscanner S3000 Advanced und Safety Eye an der Decke	64
Abbildung 4.15: Einbindung der Sicherheitseinrichtungen [13], [22], [35]–[42]	65
Abbildung 4.16 a) bis f): Raumzustände des Safety Eyes als Schleuse für das FTS68	
Abbildung 4.17: orthogonale Annäherung [43, S. 14].....	70
Abbildung 4.18: Annäherung parallel zur Schutzeinrichtung [43, S. 18].....	70
Abbildung 4.19: Signalpfade für den microScan3 [18], [28], [32], [35]–[37], [42].....	73
Abbildung 4.20: Signalpfade für die vertikalen Laserscanner [20], [28], [32], [35]–[37], [42]	74
Abbildung 4.21: Mindestabstände für das Safety Eye	75
Abbildung 4.22: Signalpfade für das Safety Eye [22], [28], [32], [35]–[37], [42].....	76

Abbildung 4.23: Signalpfade für den Sicherheits-Lichtvorhang [24], [28], [31], [35]– [37], [42]	77
Abbildung 5.1: Erreichbarkeit der Sicherheitssteuerung über OPC UA.....	83
Abbildung 5.2: Online Verbindung zur Safety SPS über TIA-Portal	83

Formelverzeichnis

(Gl. 2.1)	22
(Gl. 4.1)	69
(Gl. 4.2)	71
(Gl. 4.3)	71
(Gl. 4.4)	71
(Gl. 4.5)	71
(Gl. 4.6)	72
(Gl. 4.7)	72
(Gl. 4.8)	72
(Gl. 4.9)	72
(Gl. 4.10)	72
(Gl. 4.11)	72
(Gl. 4.12)	73
(Gl. 4.13)	74
(Gl. 4.14)	74
(Gl. 4.15)	74
(Gl. 4.16)	75
(Gl. 4.17)	76
(Gl. 4.18)	76

Tabellenverzeichnis

Tabelle 2.1: Matrix zur Festlegung des SIL [7, S. 78].....	22
Tabelle 2.2: Klassifikation der Schwere (S) [7, S. 74].....	23
Tabelle 2.3: Häufigkeit und Dauer der Exposition [7, S. 75]	24
Tabelle 2.4: Klassifikation der Wahrscheinlichkeit W, [7, S. 76]	25
Tabelle 2.5: Klassifikation der Wahrscheinlichkeit der Vermeidung oder Begrenzung des Schadens P, [7, S. 77]	26
Tabelle 2.6: Beziehung zwischen PL und SIL [6, S. 29]	26
Tabelle 3.1: Daten der Maschine MT 45	32
Tabelle 3.2: Daten der Maschine Stangenlader	32
Tabelle 3.3: Daten der unvollständigen Maschine IRB2600	33
Tabelle 3.4: Daten des Schnellwechselsystems.....	33
Tabelle 3.5: Daten der unvollständigen Maschine Festo Portal.....	34
Tabelle 3.6: Daten der Maschine Wellenmessmaschine	34
Tabelle 3.7: Daten der Maschine 3, MM500.....	36
Tabelle 3.8: Daten der Maschine IGM-Schweißzelle.....	36
Tabelle 3.9: Daten der unvollständigen Maschine IRB6620	37
Tabelle 3.10: Daten der unvollständigen Maschine Palettenkupplung	38
Tabelle 3.11: Daten der Nullpunktspannstation in der MM 500.....	38
Tabelle 3.12: Daten der Nullpunktspannstation in der IGM-Schweißzelle	38
Tabelle 3.13: Daten der Cognex Kamera	39
Tabelle 3.14: Daten der vollständigen Maschine FTS	39
Tabelle 3.15: Tätigkeiten in den Lebensphasen der Maschinen nach [2].....	48
Tabelle 3.16: Identifizierung der Gefährdungen für die Drehzelle nach [2].....	49
Tabelle 3.17: Identifizierung der Gefährdungen für die Hybridbearbeitungszelle nach [2]	51
Tabelle 3.18: Beispiel zur Ermittlung des erforderlichen SIL nach [7]	52
Tabelle 4.1: Konstruktive Maßnahmen	53
Tabelle 4.2: Ansprechzeiten für Flexi-Soft Steuerung, [27]	58
Tabelle 4.3: Tabelle zur Ermittlung des Gesamt-PL [6, S. 56].....	78

Abkürzungsverzeichnis

AGV	automated guided vehicle (englisch für FTS)
bzw.	beziehungsweise
CMT	cold metal transfer
CNC	computerized Numerical Control
CPPS	Cyber-Physische Produktions-Systeme
CPS	Cyber-Physische Systeme
CPU	central processing unit
EG	Europäische Gemeinschaft
F-SPS	Fehlersichere SPS
FTS	Fahrerloses Transportsystem
GUT	Gebäude und Technik
I/O	input/output
IFT	Institut für Fertigungstechnik und Photonische Technologien
IMS	integriertes Fertigungssystem
IRB	Industrieroboter
KSS	Kühlschmierstoff
MM 500	MAXXMILL 500
MT 45	MAXXTURN 45
OPC UA	Open Platform Communications Unified Architecture
PL	Performance Level
RAMI 4.0	Referenzarchitekturmodell Industrie 4.0
SIL	Sicherheits-Integritätslevel
SOA	service-oriented architecture
SPS	Speicherprogrammierbare Steuerung
TIA	Totally Integrated Automation
TU	Technische Universität
z. B.	zum Beispiel