

# **Hochschule Ostwestfalen-Lippe**

**Fachbereich Elektrotechnik und Technische Informatik**

## **Studienarbeit**

des Herrn  
Philip Kleen  
Matr.-Nr.: 1524 4088

gemäß Bachelorprüfungsordnung für den Studiengang Elektrotechnik  
in der Fassung der Bekanntmachung  
vom 26.Oktober 2011  
(Verkündungsblatt der Hochschule 2011/Nr.29).

**Thema:** Erstellung eines Konzepts für die funktionale Sicherheit (Safety) für ein wandlungsfähiges Montagesystem, Vergleich von Lösungsmöglichkeiten

**Prüfer:** Prof. Dr.-Ing. Jürgen Jasperneite

Der Bericht umfasst 85 Seiten.

## **Erklärung**

Ich erkläre, dass ich die vorliegende Studienarbeit selbstständig angefertigt habe. Zur Anfertigung benutzte ich keine anderen als die angegebenen Quellen und Hilfsmittel.

Die Ausfertigung als CD-ROM liegt bei.

Lemgo, den 13.05.2015

---

Philip Kleen

**Hochschule Ostwestfalen-Lippe**  
*University of Applied Sciences*

Fachbereich Elektrotechnik und Technische Informatik

**Erstellung eines Konzepts für die  
funktionale Sicherheit (Safety) für  
ein wandlungsfähiges  
Montagesystem, Vergleich von  
Lösungsmöglichkeiten**

von

**Philip Kleen**

Mai 2015

## **Zusammenfassung**

In der Vergangenheit wurden einzelne Maschinen zur Herstellung eines Produkts gebaut. Steigerung der Effizienz und Erhöhung der Stückzahlen gleicher Teile führte zu günstigeren Produkten. Die vierte industrielle Revolution erfordert neue Anlagen- und Maschinenkonzepte, sogenannte wandlungsfähige Produktionsanlagen oder dynamisch konfigurierbare Produktionssysteme. Diese können aus einzelnen Maschinenmodulen bedarfsgerecht zusammengestellt werden und ermöglichen eine Serienfertigung der Stückzahl eins.

Maschinen, die in Europa in den Verkehr gebracht werden, müssen die Richtlinien der Europäischen Union erfüllen. Dazu gehört die funktionale Sicherheit zum Schutz von Mensch, Umwelt und Maschine. Diese Studienarbeit überprüft, wie sich neue Maschinenkonzepte mit den aktuellen Regelwerken vereinen lassen. Bei der Erstellung der Risikobeurteilungen fällt bereits die Beschränkung auf Einzelmaschinen auf, da die aktuellen Regelwerke häufig nur einzelne Maschinen betrachten. Das aktuelle Regelwerk wird, durch aufeinander aufbauenden und iterativ zusammenhängenden Risikobeurteilungen der einzelnen Maschinenmodule, angewendet. Durch dieses Vorgehen werden die neuen Maschinenkonzepte eingeschränkt. Ein zukünftiger Lösungsansatz ist ein Konzept, welches eine modulare Zertifizierung ermöglicht. Als Beispielmaschine steht das wandlungsfähiges Montagesystem der [smartFactoryOWL](#) zur Verfügung.

Parallel wurde über eine Marktanalyse nach steuerungstechnischen Lösungsansätzen gesucht. Der Ansatz soll ein sicheres und einfaches Hinzufügen und Entfernen von vernetzten Maschinenmodulen ermöglichen. Auf diese und weitere Anforderungen wurde bei der Beschreibung der Lösungsansätze eingegangen. Abschließend sind die wichtigsten Anforderungen tabellarisch gegenübergestellt worden. Es stellte sich eine hohe Herstellerabhängigkeit, bei der Auswahl der Sicherheitssteuerungen, heraus und die gewünschten Funktionen sind nur mit hohen Implementierungsaufwand zu erreichen. Die Funktionsweise und die Durchführbarkeit der vorgestellten Lösungsansätze, konnte kein Unternehmen anhand einer dokumentierten Beispielanwendung verdeutlichen. Anhand der Anforderungen sind die Lösungsansätze zu bewerten. Ein Ansatz ist für die Beispielmaschine auszuwählen.

## Inhaltsverzeichnis

<b>Abbildungsverzeichnis</b>	<b>VII</b>
<b>Tabellenverzeichnis</b>	<b>VIII</b>
<b>Glossar</b>	<b>IX</b>
<b>Abkürzungsverzeichnis</b>	<b>XII</b>
<b>1 Zielstellung</b>	<b>1</b>
1.1 Motivation . . . . .	1
1.2 Das Ziel . . . . .	3
1.3 Gliederung . . . . .	4
<b>2 Stand der Technik</b>	<b>5</b>
2.1 Beschreibung des wandlungsfähigen Montagesystems . . . . .	5
2.1.1 Allgemeines Konzept der Anlage . . . . .	5
2.1.2 Stand der Anlage . . . . .	6
2.2 Allgemeines zur Normgebung in Deutschland . . . . .	10
2.3 Erlangung der CE-Kennzeichnung . . . . .	11
2.4 Normenrecherche . . . . .	11
2.5 ISO 13849 oder IEC 62061 – Ein Vergleich . . . . .	12
2.5.1 Die ISO 13849 . . . . .	13
2.5.2 Die IEC 62061 . . . . .	13
2.5.3 Der Vergleich . . . . .	14
2.6 Verkettete Maschine oder nicht? . . . . .	18
2.7 Risikobeurteilung . . . . .	22
2.8 Vorgehensweise der Risikobeurteilung . . . . .	22
2.8.1 Bestimmung der Maschinengrenzen . . . . .	24
2.8.2 Lebensphasen der Anlage . . . . .	24
2.8.3 Ermittlung von Gefährdungen . . . . .	25
2.8.4 Von der Gefährdung zum quantifizierten Risiko . . . . .	26
2.8.5 Risikobewertung . . . . .	27
2.9 Risikominderung . . . . .	27
2.10 Erstellung der Dokumentation . . . . .	29
2.11 Abschluss der Risikobeurteilung . . . . .	29

<b>3 Anforderungen</b>	<b>31</b>
3.1 Normen und Richtlinien . . . . .	31
3.2 An die Steuerung . . . . .	34
3.3 An die Wirtschaftlichkeit . . . . .	35
3.4 Aus der Risikobeurteilung . . . . .	35
3.4.1 Allgemein . . . . .	36
3.4.2 Montageroboter . . . . .	36
3.4.3 Smartes Transfersystem . . . . .	39
3.4.4 Gravurmaschine . . . . .	39
<b>4 Konzept</b>	<b>41</b>
4.1 Normativer Lösungsansatz - Konzept: Modulare Zertifizierung . . . . .	41
4.2 Steuerungstechnischer Lösungsansatz der Sicherheitsfunktionen . . . . .	43
4.2.1 Mit übergeordneter Steuerung . . . . .	43
4.2.2 Ohne übergeordnete Steuerung . . . . .	44
4.2.3 Einfach ohne Ethernet . . . . .	44
4.2.4 Der theoretische Lösungsansatz . . . . .	45
4.3 Der Vergleich spezifischer Lösungsansätze . . . . .	46
4.3.1 Auswahl der Firmen . . . . .	46
4.3.2 Vergleichskriterien . . . . .	47
4.4 ABB . . . . .	48
4.5 B&R . . . . .	50
4.6 Beckhoff . . . . .	53
4.7 HIMA . . . . .	57
4.8 Phoenix Contact . . . . .	61
4.9 SICK . . . . .	66
4.10 Siemens . . . . .	69
4.11 Tabellarischer Vergleich . . . . .	73
<b>5 Bewertung und Auswahl</b>	<b>75</b>
5.1 Bewertung . . . . .	75
5.2 Auswahl . . . . .	79
<b>Literaturverzeichnis</b>	<b>81</b>
<b>Anlage: Inhalt der CD-ROM</b>	<b>85</b>

## Abbildungsverzeichnis

1	Aufbau einer Anlage mit integrierbaren Maschinenmodulen an einem smarten Transfersystem (Backbone) . . . . .	6
2	Formalisierte Prozessbeschreibung des wandlungsfähigen Montagesystems . .	7
3	Formalisierte Prozessbeschreibung eines integrierbaren automatischen Montagemoduls . . . . .	8
4	Formalisierte Prozessbeschreibung der Integreationsumgebung . . . . .	9
5	Stichpunktartiger Vergleich zwischen der <i>IEC 62061</i> und <i>ISO 13849</i> in Bezug auf die <i>ISO 61508</i> . . . . .	16
6	Flussdiagramm zur Entscheidung, ob eine Maschinengesamtheit nach 2006/42/EG Artikel 2a vorliegt. Die Entscheidungssequenz lehnt sich an das Interpretationspapier vom Bundesministerium für Arbeit und Soziales (BMAS) an . . . . .	19
7	Heutige Situation der Zertifizierung bei einer konfigurierbaren Maschinen- system . . . . .	21
8	Risikobeurteilung und –minderung im Rahmen einer Sicherheitsstrategie von einer Einzelmaschine [14, S. 18] . . . . .	23
9	Anforderungen an ein Sicherheits- und Bedienkonzept [14, S. 31] . . . . .	28
10	Ablauf der Risikobeurteilung . . . . .	33
11	Räume des Roboters zur Ermittlung der risikomindernden Maßnahmen . .	38
12	V-Modell für eine intelligente Fertigungsanlage . . . . .	42
13	Entstehung dynamisch konfigurbarer Systeme durch Modulklassifizierung	42
14	Mögliche Konfiguration; Module 2, 4, 5, 7 und 8 sind deaktiviert . . . . .	48
15	Aufbau mit Powerlink, openSAFETY und Komponenten von B&R . . . . .	51
16	Möglicher Aufbau mit jeweils einem EtherCAT-Master in jedem Modul und einer Vernetzung über PROFINet . . . . .	55
17	Ablaufdiagramm zur Herstellung der dynamischen Verbindungen . . . . .	59
18	Beispiel für eine Berechnung der Worst-Case-Reaktionszeit . . . . .	61
19	SafetyBridge Topologie für das Anwendungsbeispiel, dezentrale Logik . . . .	63
20	Anschluss und Topologie eines Flexi-Line-Systems . . . . .	66
21	Verzögerungen im Signalfluss des FlexiLine-Systems . . . . .	68
22	Möglicher Aufbau der Hardware für drei Montagestationen und das smarte Transfersystem . . . . .	70
23	Sequendiagramm: Aufbau der Kommunikation . . . . .	71

## Tabellenverzeichnis

1	Vereinfachte sinnvolle Anwendung und Zuordnung von Kategorie zu PL und SIL [9, Tabelle 5.1] . . . . .	15
2	Gegenüberstellung von Begriffen aus den beiden Normen . . . . .	17
3	Listenpreise der Komponenten von ABB . . . . .	50
4	Listenpreise der Komponenten von B&R . . . . .	54
5	Listenpreise der Komponenten von Beckhoff . . . . .	57
6	Listenpreise der Komponenten von HIMA . . . . .	61
7	Reaktionszeiten der Hardware . . . . .	65
8	Listenpreise der Komponenten . . . . .	65
9	Listenpreise der Komponenten von SICK . . . . .	69
10	Listenpreise der Komponenten von Siemens . . . . .	72
11	Tabellarischer Vergleich der Lösungsansätze . . . . .	73
11	Tabellarischer Vergleich der Lösungsansätze (Fortsetzung) . . . . .	74
12	Bewertungsmatrix zur Auswahl . . . . .	79

## Glossar

### **CE-Kennzeichen**

Der Maschinenhersteller muss ein CE Kennzeichen an der Maschine anbringen, die in Verkehr gebracht wird. [1, S. 380]

### **CE-Kennzeichnung**

Notwendige Bescheinigung des Maschinenherstellers, dass die Maschine alle relevanten Vorschriften der Maschinenrichtlinie erfüllt und somit in den Verkehr gebracht werden darf. Mit dem **CE-Kennzeichen** wird dies gegenüber dem Anwender bescheinigt. [1, S. 380]

### **CE-Konformität, Konformitätserklärung**

Verfahren, mit dem erklärt wird, dass die in Verkehr gebrachte Maschine den grundlegenden Sicherheits- und Gesundheitsanforderungen der **MRL** entspricht. Erst mit der Konformitätserklärung kann die **CE-Kennzeichnung** erfolgen. [1, S. 390]

### **CEN**

Steht für Comité Européen de Normalisation und ist das europäische Komitee für Normung.

### **CENELEC**

Steht für Comité Européen de Normalisation Électrotechnique und ist das europäische Komitee für elektrotechnische Normung.

### **Europäische Norm (EN)**

Kennzeichnung einer Norm, dass diese unter einer EU-Richtlinien harmonisiert ist oder von **CENELEC** bzw. **CEN** erarbeitet wurde.

### **Failure Mode and Effects Analysis (FMEA)**

dt: Fehlermöglichkeits- und -einflussanalyse

Eine analytische Methode zur systematischen und vollständigen Erfassung potenzieller Fehler und von Ausfallzuständen der Komponenten eines Systems sowie deren Auswirkung. [1, S. 386]

**Integriertes Fertigungssystem (IMS)**

Gruppe von Maschinen, die in koordinierter Weise zusammenwirken, durch ein Materialfördersystem miteinander verbunden und durch Steuerungen (d. h. IMS-Steuerungen) zum Zwecke der Fertigung, Be- und Verarbeitung, Bewegung oder des Verpackens von Einzelteilen oder Baugruppen miteinander verbunden sind. [2]

**Limited Variability Language (LVL)**

dt: eingeschränkter Befehlssatz

Dieser schützt gemäß *DIN EN ISO 13849-1* den Anwender vor typischen Fehlern. Beispiele hierfür sind, dass keine Schleifen und Sprünge im Programmcode möglich sind und dass ein sicherer Ausgang beispielsweise nur einmalig im Programmcode geschrieben werden darf. Bei Abweichungen deckt der Compiler Fehlermeldungen auf und bricht die Code-Generierung ab.

**Maschinenrichtlinie (MRL)**

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). Die Richtlinie findet Anwendung auf Maschinen und legt u. a. in Anhang I die einschlägigen grundlegenden Sicherheits- und Gesundheitsanforderungen fest (Vereinbarung zwischen den EU-Mitgliedstaaten, die sich verpflichten, diese in ein nationales Recht zu überführen). [1]

**NAMUR**

Die NAMUR ist ein internationaler Verband der Anwender von Automatisierungs-technik der Prozessindustrie. [3]

**Performance Level (PL)**

Diskretes Level, das die Fähigkeit von sicherheitsbezogenen Teilen einer Steuerung spezifiziert, eine Sicherheitsfunktion unter vorhersehbaren Bedingungen auszuführen: von PL a (höchste Ausfallwahrscheinlichkeit) bis PL e (niedrigste Ausfallwahrscheinlichkeit). [4]

**Probability of Dangerous Failure per Hour ( $\text{PFH}_D$ )**

dt: mittlere Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde Von einem sicherheitsbezogenen System/Teilsystem, das die festgelegte Sicherheits-funktion über einen gegebenen Zeitraum ausführt. [5]

**Sicherheits-Integritätslevel (SIL)**

Diskrete Stufe (eine von drei möglichen) zur Festlegung der Anforderungen zur Sicherheitsintegrität der sicherheitsbezogenen Steuerungsfunktionen, die dem **SRECS** zugeordnet wird, wobei der Sicherheits-Integritätslevel 3 den höchsten und der Sicherheits-Integritätslevel 1 den niedrigsten Sicherheits-Integritätslevel darstellt. [5]

**Sicherheitsbezogene Steuerungsfunktion (SRCF)**

en: safety-related control function

Vom **SRECS** ausgeführte Steuerungsfunktion mit einem festgelegten Integritätslevel, die dazu vorgesehen ist, den sicheren Zustand der Maschine aufrechtzuerhalten oder einen unmittelbaren Anstieg des (der) Risikos (Risiken) zu verhindern. [5, S. 16]

**Sicherheitsbezogenes elektrisches Steuerungssystem (SRECS)**

en: safety-related electrical control systems

Sicherheitsbezoogenes elektrisches Steuerungssystem einer Maschine, dessen Ausfall zu einer unmittelbaren Erhöhung von Risiken führt. [5, S. 14]

**smartFactoryOWL**

In der SmartFactoryOWL werden die wichtigsten Handlungsfelder der intelligenten Fabrik, wie Wandlungsfähigkeit, Ressourceneffizienz und Mensch-Maschine-Interaktion adressiert. Hierbei spielen intelligente technische Systeme eine herausragende Rolle. Auf dem Campus der Hochschule OWL in Lemgo, inmitten eines der wichtigsten Maschinenbauregionen Deutschlands gelegen, ist die SmartFactoryOWL daher gleichzeitig praxisrelevante Versuchs- und Demonstrationsplattform für die Wissenschaftler und Ingenieure der beteiligten Forschungseinrichtungen und Industrieunternehmen sowie Lernumgebung für Studierende der ingenieurwissenschaftlichen Fachrichtungen. [6]

**Speicher Programmierbare Steuerung (SPS)**

en: Programmable Logic Controller (PLC)

Eine speicherprogrammierbare Steuerung ist ein Gerät, das zur Steuerung oder Regelung einer Maschine oder Anlage eingesetzt und auf digitaler Basis programmiert wird.

## Abkürzungsverzeichnis

BMAS	Bundesministerium für Arbeit und Soziales
CEN	Comité Européen de Normalisation
CENELEC	Comité Européen de Normalisation Électrotechnique
DIN	Deutsche Institut für Normung
E/E/PE	elektrische/elektronische/programmierbar elektronische Systeme
EAP	EtherCAT Automation Protocol
FBS	Funktionsbaustein-Sprache
FSOE	FailSafe over EtherCAT
GSDML	General Station Description Markup Language
HMI	Human Machine Interface
IEC	International Electrotechnical Commission
IMS	Integriertes Fertigungssystem
inIT	Institut für industrielle Informationstechnik der Hochschule Ostwestfalen-Lippe
ISO	International Organization for Standardization
LLDP	Link Layer Discovery Protocol
LVL	Limited Variability Language
MRL	Maschinenrichtline
PFH <sub>D</sub>	Probability of Dangerous Failure per Hour
PL	Performance Level

ProdSG Produktsicherheitsgesetz

SIL safety integrity level

SPS Speicher-Programmierbare-Steuerung

ST Strukturierter Text

VDE Verband der Elektrotechnik Elektronik Informations-technik e.V.

VDI Verein Deutscher Ingenieure

## 1 Zielstellung

### 1.1 Motivation

Heute in einem sich so rasant entwickelnden Umfeld, wo alles auf das Stichwort *Industrie 4.0* hört, verliert das folgende Zitat keine Bedeutung:

„Das Verhüten von Unfällen darf nicht als Vorschrift des Gesetztes aufgefasst werden, sondern als ein Gebot menschlicher Verpflichtung und wirtschaftlicher Vernunft!“ (Werner von Siemens im Jahr 1880). [1]

Dass der Mensch im Mittelpunkt steht, ist ein wesentlicher Gedanke der vierten industriellen Revolution. Bei diesem Schritt ist insbesondere der Schutz vor Gefahren, die von einer Maschine ausgehen, nicht zu vernachlässigen. Damit diese Ansicht bei jedem Gehör findet und gleich aufgefasst wird, wurden unter anderem Normen zur Standardisierung geschaffen. Eine negative oder lästige Einstellung gegenüber Normen ist zu überdenken, denn

„Normen fördern den weltweiten Handel und dienen der Rationalisierung, der Qualitätssicherung, dem Schutz der Gesellschaft sowie der Sicherheit und Verständigung. Das Wirtschaftswachstum wird durch Normen stärker beeinflusst als durch Patente oder Lizenzen.“ [7]

Im Rahmen dieser Studienarbeit wird diese Aussage überprüft, indem ein Sicherheitskonzept für ein dynamisch konfigurierbares Fertigungssystem erstellt wird. Die Normen aus dem heutigen Regelwerk sind stark auf die Sicherheit von Einzelmaschinen fokussiert. Die zukünftige industrielle Fertigung wird durch dynamische konfigurierbare Systeme mit Aktoren, Sensoren, Maschinenmodulen und autarken Maschinen bestimmt. Es muss ein Sicherheitskonzept gefunden werden, das es ermöglicht, neue oder modifizierte Maschinenmodule, die zum Zeitpunkt der Anlagenerstellung noch nicht entwickelt waren, in die Gesamtanlage einzufügen. So kann ein großer Vorteil von Industrie 4.0, mit funktionaler Sicherheit, umgesetzt werden. [8]

Ein Produkt (Maschine), das in Europa in Verkehr gebracht wird, muss ein **CE-Kennzeichen** tragen. Dieser Zwang erfordert eine Umsetzung der EG-Richtlinien für jedes Produkt (Maschine), auch wenn dieses über die europäische Grenze hinaus in Verkehr gebracht wird. Für Maschinen ist unter anderem die **Maschinenrichtlinie (MRL)** 2006/42/EG zu beachten, die in Deutschland mit dem **Produktsicherheitsgesetz (ProdSG)** in der 9. Verordnung national berücksichtigt wurde. Zur Präzisierung der grundlegenden Anforderungen können harmonisierte Normen herangezogen werden. [9]

Maschinenhersteller in Deutschland arbeiten in Hinblick auf funktionale Sicherheit mit den Anwendernormen **IEC 62061** und **ISO 13849**. Diese gehen unter anderem aus der

Sicherheits-Grundnorm [IEC 61508](#) hervor, in der die *Funktionale Sicherheit* bezüglich elektrischer/elektronischer und programmierbarer elektronischer Systeme bereits 1999 grundsätzlich festgelegt wurde. [1] Diese Normen gehen von einer zuvor durchgeföhrten Risikobeurteilung aus und verweisen dabei auf die Norm [ISO 12100](#) mit dem Titel „Sicherheit von Maschinen – Risikobeurteilung“. Bereits hier fällt auf, dass es nicht mit der Berücksichtigung einer Norm erledigt ist, sondern durch Verweise in andere Normen eine Reihe von Normen zu berücksichtigen sind. Dabei kommt es oft zu Vorwürfen wie „Ballast“ oder „Geldvernichtung“, gepaart mit Ratlosigkeit: Das bewegt den realen Industriemarkt und die Maschinenhersteller. [9]

Anhand des wandlungsfähigen Montagesystems vom [Institut für industrielle Informations-technik der Hochschule Ostwestfalen-Lippe \(inIT\)](#) und des Fraunhofer-Anwendungszentrums IOSB-INA soll ein Konzept zur funktionalen Sicherheit erstellt und umgesetzt werden. Zur Hannover Messe 2014 entstand das wandlungsfähige Montagesystem mit Blick auf die vierte industrielle Revolution. Es stellt ein dynamisches konfigurierbares System mit Maschinenmodulen dar. Mithilfe dieses modularen Anlagenaufbaus und steckbarer Verbindungen zu den einzelnen Montagemaschinen(-modulen) wurde ein wandlungsfähiges Montagesystem geschaffen.

In vielen Fällen wird unter modularem Aufbau von Steuerungen und Anlagen, das einmalige Erweitern/Ändern einer Anlage verstanden. Im Themengebiet der Maschinensteuerungen wird unter dem Begriff modularer Aufbau oftmals das Zusammenfügen von Baugruppen der Steuerung verstanden, damit sie durch diese steckbaren Baugruppen an die Anforderungen angepasst werden können. Eine weitere gängige Ansicht vom modularen Anlagenbau ist die dezentrale Organisation eines Steuerungssystems. Dabei ist in jedem Anlagenteil eine Teilsteuerung verbaut. Zum Informationsaustausch werden die Teilsteuerungen miteinander zu einer Gesamtsteuerung vernetzt. Der Einsatz einer übergeordneten Steuerung ist dabei gängig. Durch diese Ansätze ist die funktionale Sicherheit im Maschinen- und Anlagenbau ein Stück flexibler geworden. Ob diese für das wandlungsfähige Montagesystem flexibel genug sind und wie der Stand der Regelwerke ist, ist in dieser Studienarbeit festzustellen. Das Montagesystem ist durch den Einsatz integrierbarer Maschinenmodule so flexibel, dass es wandlungsfähig geworden ist. Der Aufbau entspricht der Modellvariante II der NAMUR-Empfehlung NE 148:2013-10 [10]. Die Normen [ISO 11161](#) bezeichnet dieses Anlagendesign als [integriertes Fertigungssystem \(IMS\)](#). Ein solcher Ansatz stellt vorhandene Steuerungskonzepte der funktionalen Sicherheit vor neue Herausforderungen. Einer sicheren Steuerung müssen die vorhandenen Sicherheitseinrichtungen bekannt sein, um ein sicheres Abschalten aller integrierten Module zu gewährleisten. Es wird somit eine gewisse Erwartungshaltung benötigt, die durch den Einsatz autonomer Maschinen allerdings nur schwer automatisch

aufgebaut werden kann. Ein Maschinenmodul, welches in das wandlungsfähige Montagesystem zu integrieren ist, ist zunächst nicht auf andere Steuerungskomponenten angewiesen. Es ist auf die Integrationsinfrastruktur angepasst, die hier das smarte Transfersystem darstellt. Das Verhalten der Maschinenmodule kann durch zuvor einheitlich definierte Statusmeldungen von anderen integrierten Modulen über das Transfersystem beeinflusst werden. Um weiterhin das Menschenleben zu sichern, ist ein Konzept der funktionalen Sicherheit zu finden, welches am Markt verfügbare Produkte berücksichtigt und mit den aktuellen Regelwerken umzusetzen ist.

## 1.2 Das Ziel

Zum besseren Verständnis des Ziels, wird zunächst der Begriff *Sicherheit* näher beschrieben. Die englische Sprache teilt den Begriff Sicherheit in *safety* und *security* mit folgender Bedeutung auf: Unter *security* wird die Sicherheit von Daten gegenüber einem unberechtigten Zugriff von außen verstanden – mit den Schutzzügen: Vertraulichkeit, Integrität und Authentizität. Dagegen wird unter *safety* die funktionale Sicherheit von Maschinen und Anlagen zum Schutz von Mensch, Maschine und Umwelt verstanden. Diese Art von Sicherheit, die funktionale Sicherheit, ist in der [IEC 61508-4](#) definiert. Genau das ist in dieser Studienarbeit mit dem Begriff *Sicherheit* gemeint.

Das Ziel dieser Studienarbeit ist die Erstellung eines funktionalen Sicherheitskonzepts zum Schutz von Mensch, Maschine und Umwelt, für ein konfigurierbares Fertigungssystem. Dabei sind folgende Punkte zu klären:

- Welche Richtlinien, Vorschriften, Verordnungen, Normen und Gesetze gibt es? Es ist von einer Vielzahl dieser auszugehen, daher ist eine begründete Auswahl auf einige entscheidende vorzunehmen. Die weiteren Punkte sind mit dieser Einschränkung durchzuführen.
- Welche Abschaltvorschriften gehen aus diesen hervor? Es ist ein geeignetes Instrument zur Bestimmung der Abschaltvorschriften auszuwählen.
- Wie können die resultierten Abschaltvorschriften realisiert werden? Es sind am Markt verfügbare sicherheitstechnische Konzepte zu vergleichen, davon ist eins für das wandlungsfähige Montagesystem auszuwählen.

Die Klärung dieser Punkte ist anhand des wandlungsfähigen Montagesystems der [smart-FactoryOWL](#) durchzuführen.

### 1.3 Gliederung

Nach der Beschreibung des Montagesystems wird im Rahmen der Normenrecherche ein Vergleich von zwei Normen vorgenommen. Des Weiteren wird der Frage nachgegangen, ob es sich bei dem wandlungsfähigen Montagesystem um eine verkettete Maschine im Sinne der [MRL](#) handelt. Im weiteren Verlauf wird als geeignetes Instrument zur Bestimmung von Abschaltvorschriften die Risikobeurteilung nach [ISO 12100](#) festgelegt und der Aufbau bzw. die Durchführung erläutert. Dies erfolgt anhand der in Kapitel [2.1.1](#) beschriebenen Anlage. Weitere Anforderungen ergeben sich aus der Normenrecherche und den Risikobeurteilungen der betrachteten Maschinen. Aus den gewonnenen Erkenntnissen werden in Kapitel [3 Anforderungen](#) mit messbaren Kriterien beschrieben. In Kapitel [4](#) werden verschiedene Konzepte der funktionalen Sicherheit und steuerungstechnische Lösungsansätze beschrieben. Den möglichen allgemeinen Lösungskonzepten schließen sich die am Markt verfügbaren Lösungsmöglichkeiten einiger Zuliefererfirmen an. Abschließend werden diese tabellarisch gegenübergestellt. Im Kapitel [5, Bewertung und Auswahl](#), werden diese mit Hilfe der Anforderungen aus Kapitel [3](#) bewertet. Daraus wird eine Entscheidung für das betrachtete wandlungsfähige Montagesystem abgeleitet.

## 2 Stand der Technik

In diesem Kapitel wird der Stand der Technik für alle Punkte erläutert, die für die Zielstellung von Relevanz sind. Zunächst wird das wandlungsfähige Montagesystem in der smartFactoryOWL beschrieben. Im nächsten Abschnitt wird Bezug auf die Normen und auf die Erlangung der CE-Konformität eingegangen. Nach der Normenrecherche und dem Vergleich der ISO 13849 und IEC 62061 wird das Vorgehen der Risikobeurteilung nach ISO 12100 mit entscheidenden Erkenntnissen beschreiben.

### 2.1 Beschreibung des wandlungsfähigen Montagesystems

#### 2.1.1 Allgemeines Konzept der Anlage

Im Folgenden wird das Konzept des wandlungsfähigen Montagesystems in Bezug auf die NAMUR-Empfehlung NE 148:2013-10 [10] erläutert. Mit dem wandlungsfähigen Montagesystem soll ein neues Anlagendesign entstehen, welches für mehr Schnelligkeit, Flexibilität und wirtschaftliche Größenanpassung steht. Auch Technologien, die im Zusammenhang mit *Industrie 4.0* stehen, wie beispielsweise ein Produktgedächtnis, das mithilfe eines RFID-Chips in den Objektträgern verbaut ist, sind bei der Realisierung zu berücksichtigen. Die Wandlungsfähigkeit des Montagesystems soll durch einen modularen Anlagenbau erlangt werden, der im Wesentlichen aus integrierbaren Modulen und einer zugehörigen Infrastruktur besteht. Jedes integrierbare Maschinenmodul ist in seiner Funktion und seinem Einsatzbereich fest definiert und über ein smartes Transfersystem, stofflich, energetisch und automatisierungstechnisch in eine zugehörige Infrastruktur zu integrieren. Somit stellt das smarte Transfersystem die Infrastruktur zum Integrieren dar und kann als Backbone der Module (integrierbare Maschine) betrachtet werden. Jedes Modul soll über eigene Automatisierungskomponenten verfügen. Diese sind über das smarte Transfer- system beeinflussbar. Der entscheidende Schritt zum Erfolg dieses Konzepts ist es, eine möglichst automatische Erkennung und einfache Vorgehensweise beim Integrieren in das übergeordnete Leitsystem zu ermöglichen, bis hin zum Verzicht auf ein solches System. Dieses Konzept setzt auf ein Anlagendesign, das in der NAMUR-Empfehlung [10] unter dem Namen *Integrierbare Module* (Modellvariante II) beschrieben ist. In dem Aufbau der einzelnen Module ist die Möglichkeit eines modularen Aufbaus vorzusehen. Diese Art eine Anlage zu bauen, wird in der dritten Modellvariante der NAMUR-Empfehlung unter dem Namen *Modulare Module* beschrieben. In Abbildung 1 ist der Grundriss einer möglichen Anlage unter Berücksichtigung dieses Konzepts dargestellt.

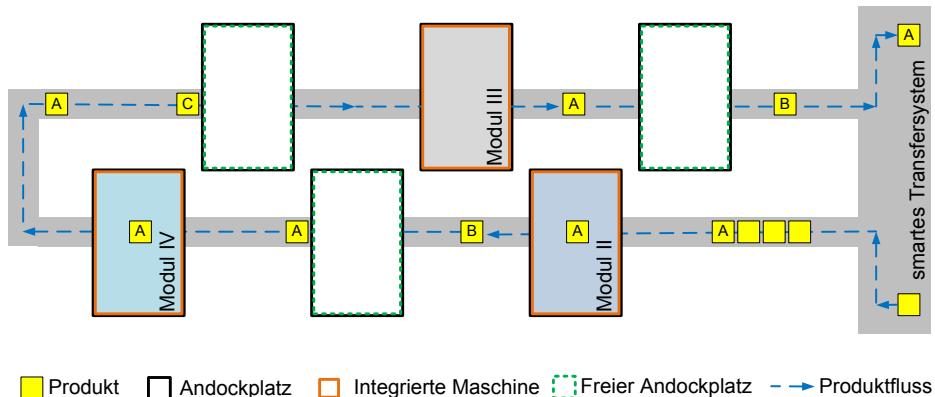


Abbildung 1: Aufbau einer Anlage mit integrierbaren Maschinenmodulen an einem smarten Transfersystem (Backbone)

### 2.1.2 Stand der Anlage

Zur Hannover Messe 2014 wurde gemeinsam vom Institut für industrielle Informations-technik der Hochschule Ostwestfalen-Lippe und dem Fraunhofer-Anwendungszentrum IOSB-INA begonnen dieses Konzept umzusetzen, mit dem Ziel, ein wandlungsfähiges Montagesystem zu schaffen. In der ersten Realisierung wurden folgende drei Maschinenmodule gebaut: ein Modul zur automatischen Montage einer Legofigur, ein Handarbeitsplatz mit *Augmented Reality*-Unterstützung und ein Modul mit einer Lasereinheit zum Gravieren. Passend zu dieser Ausbaustufe, ist eine Infrastruktur geschaffen worden, in der diese Module integriert werden können. Die Infrastruktur kann auch als Backbone aufgefasst werden und besteht im Wesentlichen aus einem modularen Transfersystem, an das die Energie- und Informationsversorgung für die integrierbaren Module montiert wurde. Über zugehörige Plug-and-Produce-Stecker werden die integrierbaren Maschinenmodule eingebunden. Die Objektträger (Werkstückträger) des Transfersystems stellen über einen RFID-Chip ein Produktgedächtnis bereit. Durch das Produktgedächtnis ergibt sich mit dem Teiletransport ein weiterer Informationsweg, der das Nachhalten von Produktdaten in einer übergeordneten Steuerung vermeidet. Diese Eigenschaften des Transfersystems machen es zu einem smarten Transfersystem, welches eine Integrationsinfrastruktur für die integrierbaren Module darstellt.

Mit Hilfe der formalisierten Prozessbeschreibung nach VDI/VDE 3682 werden die Prozesse und Zusammenhänge des wandlungsfähigen Montagesystems dargestellt. [11] In Abbildung 2 wird das gesamte System mit einem Dekompositionsschritt aufgezeigt. Ein Prozessablauf eines Moduls wird anhand der automatischen Montage in Abbildung 3 beschrieben. Des Weiteren sind in Abbildung 4 die Prozesse des smarten Transfersystems abgebildet.

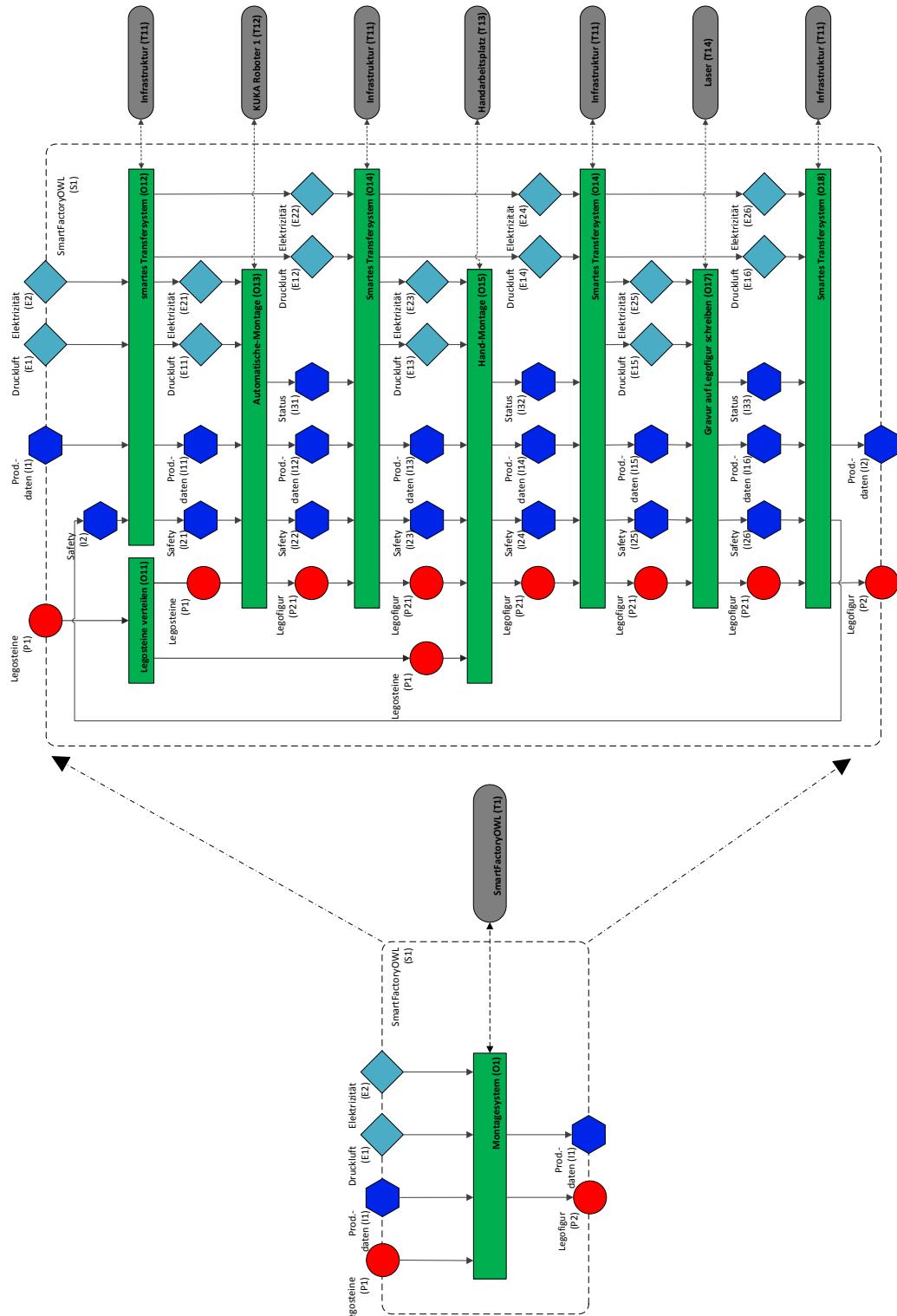


Abbildung 2: Formalisierte Prozessbeschreibung des wandlungsfähigen Montagesystems

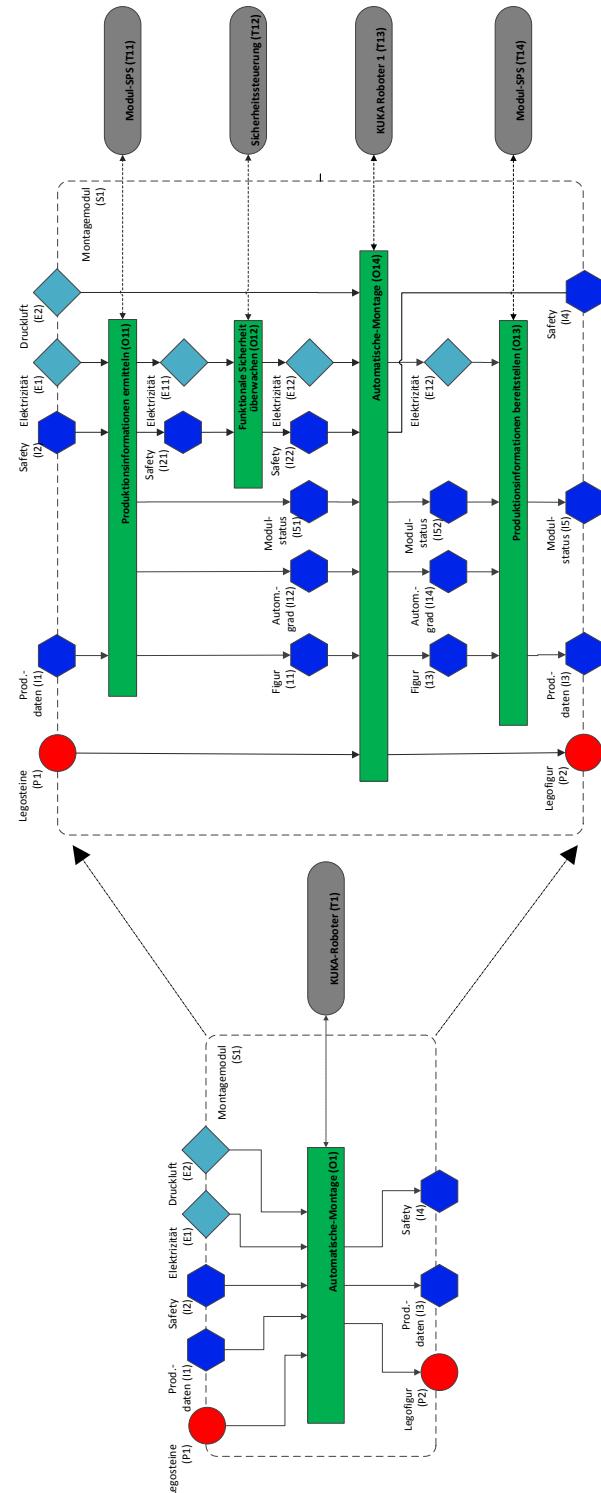


Abbildung 3: Formalisierte Prozessbeschreibung eines integrierbaren automatischen Montagemoduls

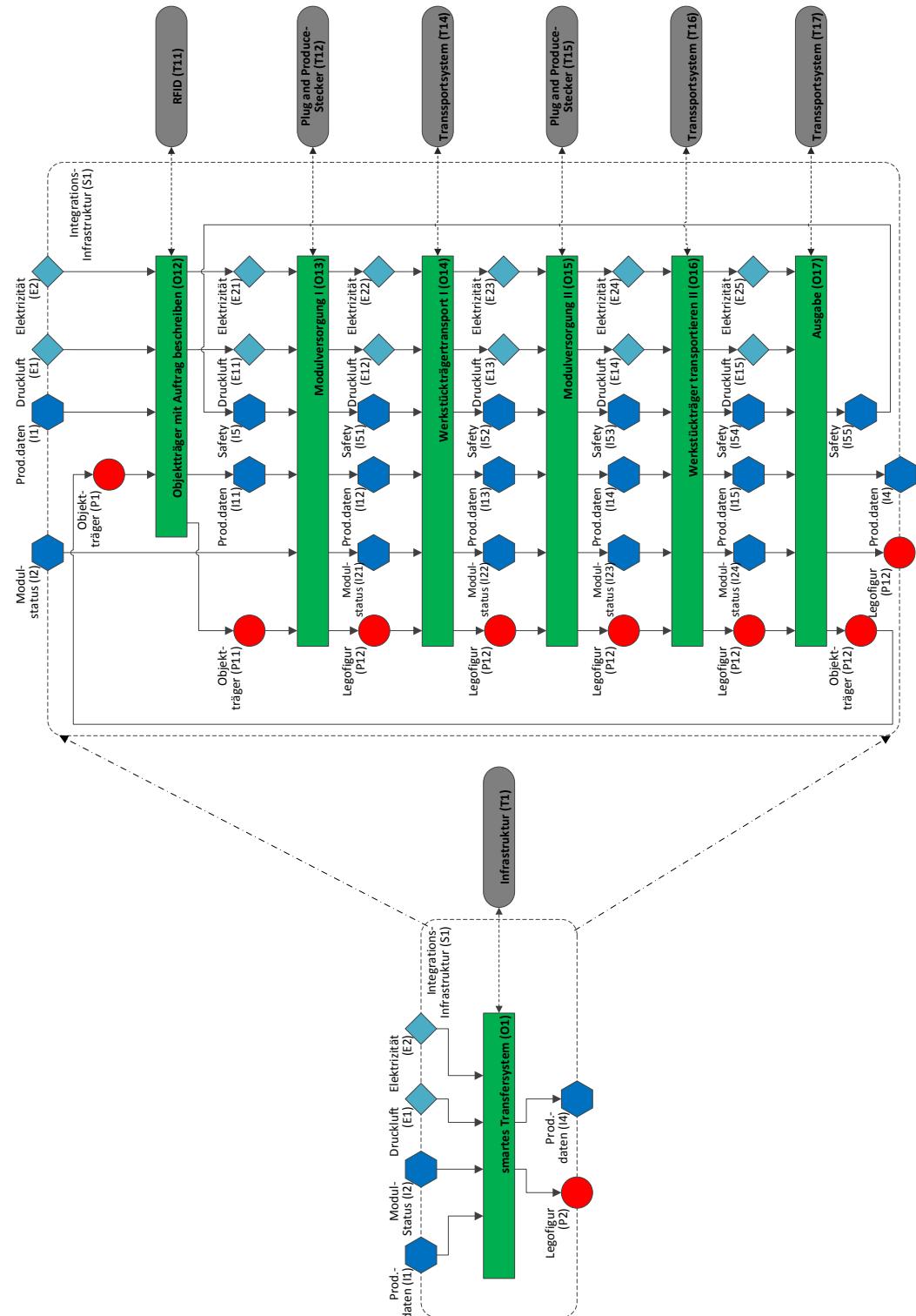


Abbildung 4: Formalisierte Prozessbeschreibung der Integreationsumgebung

## 2.2 Allgemeines zur Normgebung in Deutschland

Eine EG-Richtlinie enthält allgemeine Sicherheitsziele und legt grundlegende Sicherheitsanforderungen fest. In einer Norm werden technische Details zur Präzisierung festgelegt und durch die Veröffentlichung im Amtsblatt der EU harmonisiert. [1, S. 17] Auf internationaler Ebene gibt es zwei wichtige Gremien zur Erstellung von Normen, zum einen die International Electrotechnical Commission (IEC) und zum anderen die International Organization for Standardization (ISO). „Während sich die IEC hauptsächlich um Themen der Elektrik und Elektronik kümmert, beschäftigt sich die ISO vornehmlich mit Themen der Mechanik. Derzeit sind weit über 100 Länder in den beiden Organisationen vereint, was den von IEC und ISO erarbeiteten Normen ein erhebliches Gewicht verleiht.“ [12, S. 3-18] Auf europäischer Ebene wird die EN-Normenentwicklung genauso gegliedert. Dabei arbeitet das europäische Komitee für elektrotechnische Normung (CENELEC) die zugehörigen Themen aus. Das europäische Komitee für Normung (CEN) befasst sich mit den verbliebenen Themengebieten. Auf nationaler Ebene gibt es meistens auch ein Normungsinstitut. Im Fall von Deutschland ist es das Deutsche Institut für Normung (DIN). „Die gängige Praxis ist heute, dass Normen vom DIN direkt in Zusammenarbeit mit CEN oder CENELEC als DIN EN ISO oder DIN EN entwickelt und herausgegeben werden. Diese Normen unterscheiden sich in aller Regel nur im nationalen Vorwort von der EN, ISO oder IEC-Norm. [...] Wird eine ISO-Norm zur EN-Norm, so trägt diese den Titel EN ISO. Wird diese nun noch zur DIN-Norm, so ist der volle Titel DIN EN ISO. Je lokaler das Institut, desto weiter vorne im Namen wird es genannt. Ein kleines Kuriosum am Rande: Wird eine IEC-Norm zur EN-Norm, so entfällt die Nennung der IEC. Die IEC 61508 wird also zur europäischen EN ISO 61508 oder zur deutschen DIN EN 61508.“ [12, S. 3-18] Der Eindruck, es handelt sich bei Normen um einen Bürokratieakt, der seines gleichen sucht, kann durch folgendes Zitat widerlegt werden.

„Durch Normen können sich neue Technologien schneller am Markt durchsetzen, weil durch die Normung wesentliche Fragen der Sicherheit, der Verträglichkeit mit Gesundheit und Umwelt sowie der Gebrauchstauglichkeit und Zuverlässigkeit geklärt sind. Das schafft Vertrauen. Die Aufgabe von Normen ist es somit, den Nutzen technischer Entwicklung zu maximieren und von ihnen ausgehende Gefährdungen zu minimieren.“ [13]

Wie sich neue Bedien- und Maschinenkonzepte mit dem aktuellen Regelwerk, das den Stand der Technik widerspiegelt, umsetzen lassen, wird in dieser Studienarbeit geklärt. Dabei wird die Richtigkeit des Zitates deutlich. Mit der obigen Erläuterung lässt sich anhand der Namensgebung erkennen, ob es sich bei der Norm um einen elektrischen/elektronischen Bezug

handelt und aus welchem Normungsgremium diese stammt. Das europäische Normenwerk für Sicherheit von Maschinen ist zusätzlich noch hierarchisch geordnet und gliedert sich in drei Typen von Normen auf. Die Normensetzer ordnen die jeweilige Norm entsprechend zu und veröffentlichen dies in dem Vorwort der jeweiligen Norm.

- Typ A-Normen: Sicherheitsgrundnormen, Grundnormen z. B.  
*DIN EN ISO 12100, DIN EN 61508*
- Typ B-Normen: Sicherheitsfachgrundnormen, Gruppennormen z. B.  
*DIN EN ISO 13849, DIN EN 62061*
- Typ C-Normen: Maschinensicherheitsnormen, Produktnormen z. B.  
*DIN EN ISO 10218*

## 2.3 Erlangung der CE-Kennzeichnung

Ziel eines Maschinenbauers muss die Erlangung der **CE-Kennzeichnung** sein, da nur Produkte mit **CE-Kennzeichnung** in Verkehr gebracht werden dürfen. Dies gilt auch für Betreiber, die wie Hersteller handeln. Um das **CE-Kennzeichen** anbringen zu dürfen, muss die Konformitätserklärung ausgestellt werden, in der bestätigt wird, dass alle relevanten EG-Richtlinien angewendet bzw. über die Harmonisierung erfüllt werden. Dieses Vorgehen ist durch Artikel 95 des EG-Vertrages vorgeschrieben, in dem auch festgelegt ist, dass EG-Richtlinien in nationale Gesetze übernommen werden müssen. Dies ist aktuell mit dem **Produktsicherheitsgesetz (ProdSG)** in Verbindung mit der 9. Verordnung (9. ProdSGV) in Deutschland geschehen und somit bekommen diese Binnenmarkt-Richtlinien der EU den Status von Gesetzen. [14, S. 12] „Der einfachste Weg zur Erfüllung der EG-Richtlinien ist die Einhaltung der darunter harmonisierten europäischen Normen.“ [9, S. 16] Auf Grund der Vermutungswirkung, die bei korrekter und vollständiger Anwendung von harmonisierten Normen ausgeht, wird dieser Weg ermöglicht. Grundsätzlich können auch auf andere Weise die Schutzziele der EG-Richtlinien erreicht werden, jedoch ist der Nachweis im Schadensfall schwieriger. [9, S. 16]

## 2.4 Normenrecherche

Bei der folgenden Normenrecherche wurde der Schwerpunkt auf funktionale Sicherheit im Zusammenhang der **MRL 2006/42/EG** gelegt. Mit dieser Einschränkung verbleiben immer noch über 760 harmonisierte Normen. [7] Durch das Lesen von Produktinformationen von sicherheitsgerichteten Bauteilen, Literatur und Fachgesprächen mit erfahrenden Personen im

Bereich funktionaler Sicherheit verschiedener Unternehmen, stellten sich folgende Normen als bedeutsam heraus:

- **DIN EN 62061:2005+A1:2013:** Sicherheit von Maschinen – Funktionale Sicherheit elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme
- **DIN EN ISO 13849:** Sicherheit von Maschinen – Sicherheitsbezogene Teile von Steuerungen (alle Teile)
- **DIN EN 61508:** Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme (alle Teile)
- **DIN EN ISO 12100:2010:** Sicherheit von Maschinen – Allgemeine Gestaltungsleitsätze – Risikobeurteilung und Risikominderung

Ohne diese Einschränkung sind es zu viele Normen, von denen Kenntnis genommen werden muss und dies würde den zeitlichen Rahmen der Studienarbeit überschreiten. Daher können das erstellte Sicherheitskonzept und die zugehörigen Risikobeurteilungen Schwächen nicht betrachteter Themenbereichen aufweisen. Hier seien beispielsweise die ergonomische Gestaltung des Arbeitsplatzes und Beleuchtungsvorgaben oder der Umgang mit Lasereinheiten erwähnt. Im Verlauf der Studienarbeit stellten sich folgende Normen noch als zutreffend heraus. Deren teilweise Anwendung in der Risikobeurteilung unerlässlich war.

- **DIN EN ISO 10218-2:** Industrieroboter – Sicherheitsanforderungen – Teil: 2 Roboter-systeme und Integration
- **DIN EN ISO 11161:** Sicherheit von Maschinen – Integrierte Fertigungssysteme – Grund-legende Anforderungen
- **DIN EN ISO 13850:** Sicherheit von Maschinen – Not-Halt – Gestaltungsleitsätze
- **DIN EN ISO 13855:** Sicherheit von Maschinen – Sicherheitsabstände gegen das Errei-chen von Gefährdungsbereichen mit den oberen und unteren Gliedmaßen

## 2.5 ISO 13849 oder IEC 62061 – Ein Vergleich

Zurzeit haben Maschinen- und Anlagenbauer bei der Bestimmung von sicherheitsbezogenen elektrischen Steuerungssystemen (**SRECS**) die Auswahl zwischen zwei in der Maschinenrichtlinie harmonisierten Normen. Dieses sind die **ISO 13849** und die **IEC 62061**. Im Namen fällt schon auf, dass diese ihren Ursprung in zwei verschiedenen Normungsgremien haben.

Ein Blick auf die Geschichte erklärt die unterschiedliche Entstehung und wesentlichen Unterschiede.

### 2.5.1 Die ISO 13849

Angefangen hat es mit der *EN 954*, die zur Präzisierung der Maschinenrichtlinie 98/37/EG von der **CEN** verabschiedet wurde. „Die Verwendung elektronischer, programmierbarer Systeme für Sicherheitsfunktionen war durch diese Norm jedoch nicht abgedeckt. [...] Die Erkenntnis, dass die *EN 954-1* nicht mehr ausreichend den Stand der Technik repräsentierte, führte letztlich dazu, dass im Verlauf der vergangenen Jahre viele verschiedene und zum Teil komplexe Normen entworfen bzw. überarbeitet wurden.“ [15] So wurde die *EN 954* durch die *EN ISO 13849* im Rahmen der neuen **MRL** 2006/42/EG abgelöst. Dabei wurden die Sicherheitskategorien beibehalten und durch den komplexen probabilistischen Ansatz der **IEC 61508** ergänzt. Daraus resultierte die neue Kenngröße und der **Performance Level (PL)** wurde eingeführt. Dieser macht eine Aussage zu der mittleren Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde (**PFH<sub>D</sub>**). Mithilfe von messbaren (quantitativen) Parametern wird der **Performance Level (PL)** bestimmt. Im Abschnitt 4.5.4 der *DIN EN ISO 13849* „Vereinfachtes Verfahren zur Abschätzung eines PLs“ wird eine Verknüpfung der berechneten Kenngrößen zu den bekannten Sicherheitskategorien hergestellt. Diese wird mit widersprüchlichen Angaben zur Norm im informativen Anhang K präzisiert. Bei komplexeren Hardwarestrukturen stößt diese Norm schnell an ihre Grenzen, da diese nur vier verschiedene Architekturen (Sicherheitskategorien) kennt und die Berechnungen auf diesen basieren. Beim Begriff funktionale Sicherheit wird auf die **IEC 61508** verwiesen. Die *EN ISO 13849* macht hingegen keine Einschränkungen in der Technologie, somit ist diese auch für hydraulische, pneumatische und mechanische Sicherheitssysteme gültig.

### 2.5.2 Die IEC 62061

Wie bereits erwähnt, gibt es eine weitere einflussreiche Norm, die **IEC 61508**. Sie ist eine Grundnorm, die allerdings nicht unter der **MRL** harmonisiert ist. Ein zentraler Punkt der **IEC 61508** ist die Betrachtung von einem Sicherheitslebenszyklus mit detaillierten Anforderungen an Vorgehen und Inhalt der einzelnen Schritte. Dabei wurde der Schwerpunkt und das Anwendungsgebiet auf den Entwurf von **elektrischen/elektronischen/programmierbar elektronischen Systemen (E/E/PE)** und deren zugehörige Software gelegt. [12, S. 3-35] Aus dieser Grundnorm geht unter anderem die Sektornorm (Anwendernorm Typ B) **IEC 62061** hervor, welche unter der Maschinenrichtlinie harmonisiert ist. Dabei sind nur diejenigen Aspekte des Sicherheitslebenszyklus aus der **IEC 61508** übernommen worden, die einen Be-

zug von der Zuweisung der Sicherheitsanforderungen bis hin zur Validierung der Sicherheit haben. Die Norm *IEC 62061* verfolgt den systematischen Ansatz aus der *IEC 61508*, mit dem systematische Fehler besser zu kontrollieren sind. Dies wird in der Norm durch die Forderung nach einem Plan der funktionalen Sicherheit deutlich. Dieser setzt bestimmte Managementaktivitäten zur Planung, Dokumentation und ständigen Überprüfung voraus und muss optimaler Weise in die Arbeitsabläufe des Unternehmens integriert werden. Vergleichbar mit dem *PL* spricht die Norm von einem **Sicherheitsintegritätslevel (SIL)**, der genauso einen Bezug zum *PFH<sub>D</sub>*-Wert herstellt. Allerdings sind diese zwei Kenngrößen nicht einfach „umzurechnen“, denn das strukturelle Vorgehen, um den *SIL* zu erlangen, ist grundsätzlich zum *PL* verschieden. Die *DIN EN 62061* stellt allgemeine Anforderungen an die Sicherheitsintegrität:

- Hardware: Architektureinschränkungen (Fehlertoleranz) und Wahrscheinlichkeit zu-fälliger gefahrbringender Hardwareausfälle
- Systematische: Vermeidung und Beherrschung von systematischen Fehlern
- Systemverhalten beim Aufdecken eines Fehlers
- Entwurf und Entwicklung sicherheitsbezogener Software [9, S. 221]

„Die Architektur eines Steuerungssystems für eine bestimmte Sicherheitsfunktion entspricht in ihrer logischen Struktur der zuvor ermittelten Struktur der Sicherheitsfunktion.“ [9, S. 225] Zur Vereinfachung des Rechenansatzes werden Strukturmodelle vorgegeben.

### 2.5.3 Der Vergleich

Zusammenfassend gesagt, gibt es zwei Standards für das vermeidlich gleiche Anwendungsbereich. Die *DIN EN ISO 13849*, die unter dem Einfluss der *MRL 2006/42/EG*, *EN 954* und *IEC 61508* entstanden ist, und die *DIN EN 62061*, die als Anwendernorm aus der *IEC 61508* hervor geht. Gemeinsam haben sie ein Ziel, so heißt es in der Einleitung der *DIN EN 62061*:

„*IEC 62061* und *ISO 13849-1* legen Anforderungen für den Entwurf und die Implementierung von sicherheitsbezogenen Steuerungssystemen von Maschinen fest. Die Anwendung jeder dieser Normen in Übereinstimmung mit ihren Anwendungsbereich kann die Erfüllung der relevanten grundsätzlichen Sicherheitsanforderungen vermuten lassen.“ [5]

Dabei weist das Vorgehen unterschiedliche Methoden auf, die zwar nicht kombinierbar sind, dennoch Parallelen und sowie Vor- und Nachteile aufweisen. Die in der Tabelle 2

gegenübergestellten Begriffe können als Parallelen angesehen werden, da diese das gleiche Ziel verfolgen und eine ähnliche Wirkung erzielen. Sie können keinesfalls gegeneinander ausgetauscht oder ersetzt werden.

Ein *Umrechnen* zwischen **SIL** und **PL** kann über den **PFH<sub>D</sub>**-Parameter geschehen. Es sei erneut darauf hingewiesen, dass die *EN ISO 13849* nur bestimmte Architekturen (Kategorien) vorgibt. Dadurch wird empfohlen, von **SIL** auf **PL** zu schließen. Andersherum gibt die *DIN EN 62061:2013-09 – Tabelle 5* strukturelle Einschränkungen vor, die den Sicherheitskategorien der *DIN EN ISO 13849-1:2008-12* gegenübergestellt werden können, siehe Tabelle 1 mit nachfolgenden Anmerkungen. Die Vor- und Nachteile der Normen sind in einer tabellarischen Auflistung vom TÜV Rheinland in Abbildung 5 übernommen worden.

Tabelle 1: Vereinfachte sinnvolle Anwendung und Zuordnung von Kategorie zu PL und SIL [9, Tabelle 5.1]

DIN EN ISO 13849-1	DIN EN 62061 (VDE 0113-50)			DIN EN ISO 13849-1
Kategorie	Fehlertoleranz der Hardware	SFF=DC <sub>avg</sub>	Maximal erreichbarer	Maximal erreichbarer
	0 = einkanalig 1 = zweikanalig		SIL	PL
1	0	< 60 %	SIL 1	PL c
2	0	60 % ... 90 %	SIL 1/2	PL c/d
3	1	< 60 %	SIL 1	PL c
	1	60 % ... 90 %	SIL 2	PL d
4	1	> 90 %	SIL 3	PL e

Eine Kategorie 2 Anwendung mit einem erreichbaren PL d oder SIL 2 ist nur mit Vorsicht zu genießen.

Kategorie 4 verlangt immer einen Diagnosedeckungsgrad DC > 99 % ( $\pm 5\%$ ). Da Kategorie 3 bis 90 % ( $\pm 5\%$ ) definiert ist, ergibt die Vereinfachung DC > 90 % für Kategorie 4 Sinn.

In der Praxis gibt es aus Anwendersicht nur 99 % oder mehr. Somit wären 99 % ohne  $\pm 5\%$  realistisch. [9, S. 50]

Gemeinsamkeiten der drei Standards
<ul style="list-style-type: none"> <li>+ Probabilistische Sichtweise (Aspekte Zuverlässigkeit und Ausfallwahrscheinlichkeit)</li> <li>+ Ganzheitliche Betrachtung der vollständigen Sicherheitskette</li> <li>- Bereitstellung der sicherheitstechnischen Kenngrößen vom Hersteller</li> </ul>
IEC 61508
<ul style="list-style-type: none"> <li>+ Betrachtung des gesamten Lebenszyklus</li> <li>+ Behandelt sowohl Software als auch Hardware für einfache bis komplexe Systeme</li> <li>- Ist keine harmonisierte Norm im Sinne der MRL</li> <li>- „Überdimensioniert“ für Maschinenbau; sehr umfangreich und kompliziert</li> </ul>
EN 62061
<ul style="list-style-type: none"> <li>+ Teilweise vereinfachte Methoden im Vergleich zur IEC 61508</li> <li>+ Greifbarere Anforderungen zu QM Maßnahmen (im Vergleich zur IEC 61508)</li> <li>+ Beschreibung von Konfigurations- und Parametriersoftware sowie Embedded Software</li> <li>+ Anwendbar für alle elektrischen und elektronischen Systeme beliebiger Architekturen (SIL1 bis SIL3)</li> <li>- Weiterhin Verweise auf IEC 61508 (nicht eigenständig, nicht einfach)</li> <li>- Programmierbare Steuerungen (SPS etc) müssen IEC 61508 erfüllen</li> </ul>
EN ISO13849
<ul style="list-style-type: none"> <li>+ Verwendung von Architekturen mit unterschiedlichen Eigenschaften und spezifizierten Fehlerreaktionen (vorberechnete Markov-Modelle)</li> <li>+ Vereinfachte Methoden im Vergleich zur IEC 61508</li> <li>+ Greifbarere Anforderungen zu QM Maßnahmen (im Vergleich zur IEC 61508)</li> <li>+ Kontinuität auf Basis der DIN EN 954-1 (viele Ähnlichkeiten)</li> <li>+ Zugeschnitten auf sicherheitsgerichtete Steuerungstechnik im Maschinenbau</li> <li>+ Anwendbar für hydraulische, pneumatische und elektromechanische Systeme ohne Einschränkungen</li> <li>+ Konfigurations- und Parametriersoftware sowie Embedded Software beschrieben</li> <li>- Liefert sehr konservative sicherheitstechnische Kenngrößen</li> <li>- Ist bei komplexen programmierbaren elektronischen Systemen nur unter Einschränkungen anwendbar (bestimmte Architektur, bis PL d)</li> <li>- Nicht für alle sicherheitsgerichteten Steuerungen anwendbar</li> </ul>

Quelle: [15]

Abbildung 5: Stichpunktartiger Vergleich zwischen der *IEC 62061* und *ISO 13849* in Bezug auf die *ISO 61508*

Tabelle 2: Gegenüberstellung von Begriffen aus den beiden Normen

IEC 62061	EN ISO 13849
Safety Integrity Level (SIL)	Performence Level (PL)
Sicherheits-Lebenszyklus	Iterat. Gestaltungsprozess
SIL-Risikomatrix	Risikograph
Entwurfs- und Entwicklungsprozess	Entwurfs- und Entwicklungsprozess
Strukturelle Einschränkungen (Anforderungen)	Vorgesehene Architekturen (Kategorien)
Strukturmodelle	Säulendiagramm
Software	Software

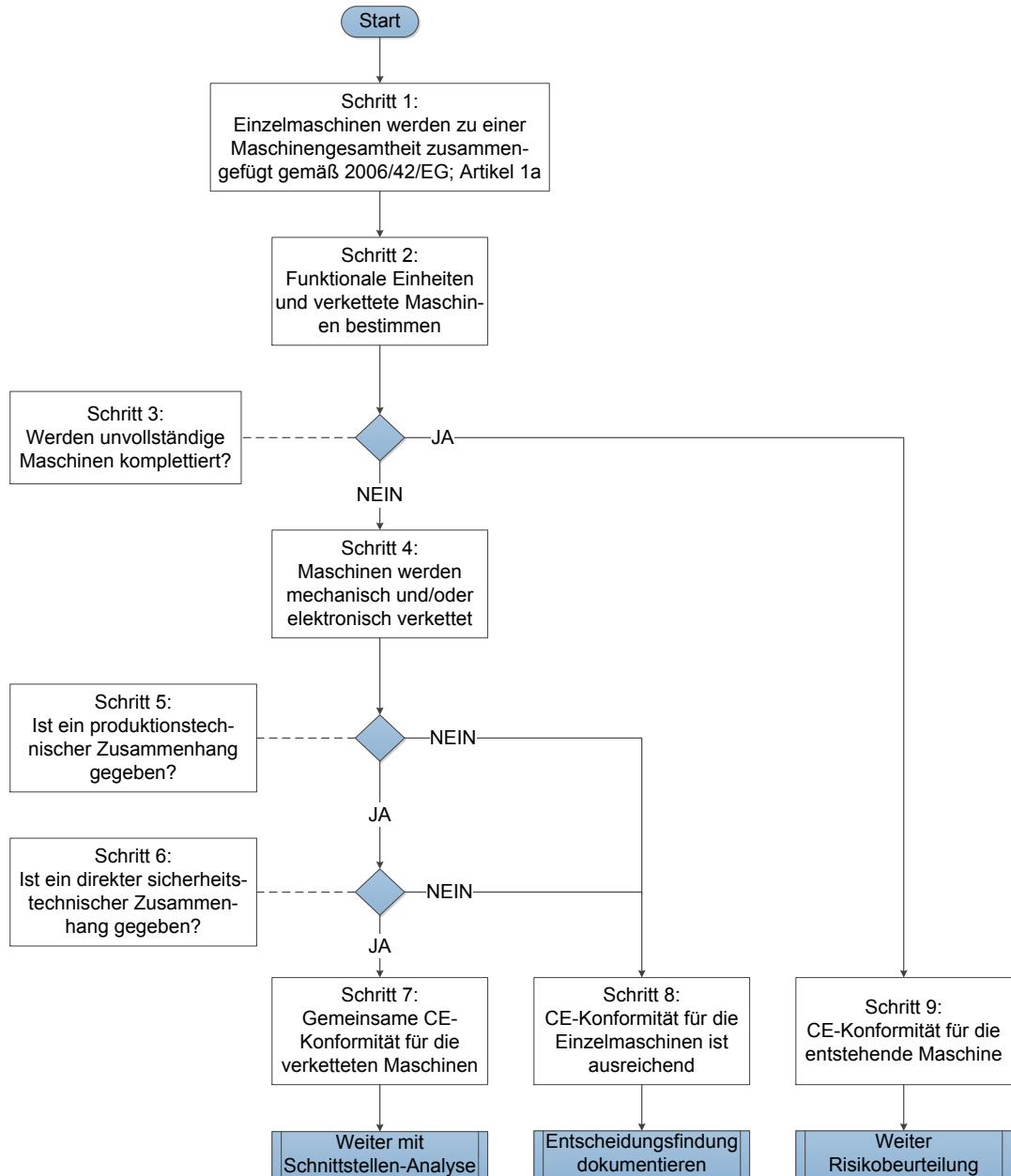
## 2.6 Verkettete Maschine oder nicht?

Besteht eine Maschine/Anlage aus mehreren Maschinen, entsteht in vielen Fällen eine Gesamtheit von Maschinen. Oftmals wird auch von einer verketteten Anlage gesprochen. „Das Bundesministerium für Arbeit und Soziales (BMAS) macht hierzu eindeutige Angaben, um die Unklarheiten auszuräumen. In seinem Interpretationspapier zum Begriff vom 5. Mai 2011 stellt die Behörde klar, dass die Entscheidung aus zwei Fragen resultiert. So handelt es sich um eine Gesamtheit von Maschinen laut der [Maschinenrichtline \(MRL\)](#), wenn

1. ein produktionstechnischer Zusammenhang besteht und
2. ein sicherheitstechnischer Zusammenhang besteht.

Trifft beides zu, dann ist für die gesamte Anlage ein Konformitätsverfahren zu durchlaufen und sie muss explizit mit dem [CE-Kennzeichen](#) versehen werden.“ [siehe Erlangen der [CE-Kennzeichnung 16](#)]. Dem Interpretationspapier ist zu entnehmen, unter welchen Kriterien von einem produktionstechnischen und sicherheitstechnischen Zusammenhang gesprochen werden kann. In dem wandlungsfähigen Montagesystem gibt es zur Zeit keine übergeordnete Steuerung, die den Fertigungsablauf überwacht und steuert. Es gibt ein Auftragssystem und eine Visualisierung, die als übergeordnet angesehen werden können. Diese haben keinen Einfluss auf die Funktionsweise der verbunden Montageeinheiten. Das Zusammenspiel der Montageeinheiten ist hier das Gegenteil von einer geschlossenen Einheit, da die Einheiten unabhängig voneinander funktionieren. Durch die Wandlungsfähigkeit kann je nach Kombination verschiedener Montagemaschinen ein anderes Produkt gefertigt werden. Dabei verfolgt jedes Maschinenmodul nur das Ziel, seine gerade benötigte Fähigkeit bereitzustellen. Sie sind nicht gemeinsam auf ein bestimmtes Ziel (Produkt) ausgerichtet. Mit diesen Aussagen kann im ersten Schritt kein produktionstechnischer Zusammenhang festgestellt werden. Jedes modular aufgebaute Maschinenmodul, kann als Gesamtheit von Maschinen aufgefasst werden, nicht dagegen der Verbund aller Montageeinheiten und damit das gesamte wandlungsfähige Montagesystem. Mit dem Interpretationspapier kann die Aussage getroffen werden, dass für den Verbund der Maschinen keine zusätzliche [CE-Konformität](#) nachgewiesen werden muss, wobei die [CE-Konformität](#) der Einzelmaschinen/Montageeinheiten vorausgesetzt wird. Eine Risikobeurteilung für die Schnittstellen der Einzelmaschinen ist mit Hilfe der [DIN EN ISO 11161](#) zu erstellen, damit ein Gefahrenübertrag ausgeschlossen oder verhindert werden kann.

Das Flussdiagramm aus dem Interpretationspapier (vgl. Abbildung 6) lässt den Anschein zu, dass beide Schritte verneint werden müssen. Im Text hingegen sind die beiden Schritte mit einem *und* verknüpft. Dies wird auch in Zöllner [16] wie folgt bestätigt: „Trifft beides zu, dann ist für die gesamte Anlage ein Konformitätsverfahren zu durchlaufen [...]“



**Quelle:** TÜV SÜD

Abbildung 6: Flussdiagramm zur Entscheidung, ob eine Maschinengesamtheit nach 2006/42/EG Artikel 2a vorliegt. Die Entscheidungssequenz lehnt sich an das Interpretationspapier vom BMAS an

Aus dem Zitat geht hervor, dass beide Zusammenhänge erfüllt sein müssen, damit die Gesamtheit von Maschinen laut **MRL** gegeben ist. Da kein produktionstechnischer Zusammenhang besteht, kann zur Klärung der Gesamtheit von Maschinen der sicherheitstechnische Zusammenhang vernachlässigt werden. Trotzdem wird nachfolgend der sicherheitstechnische Zusammenhang kurz erläutert. Im Interpretationspapier des **BMAS** ist klar geschrieben:

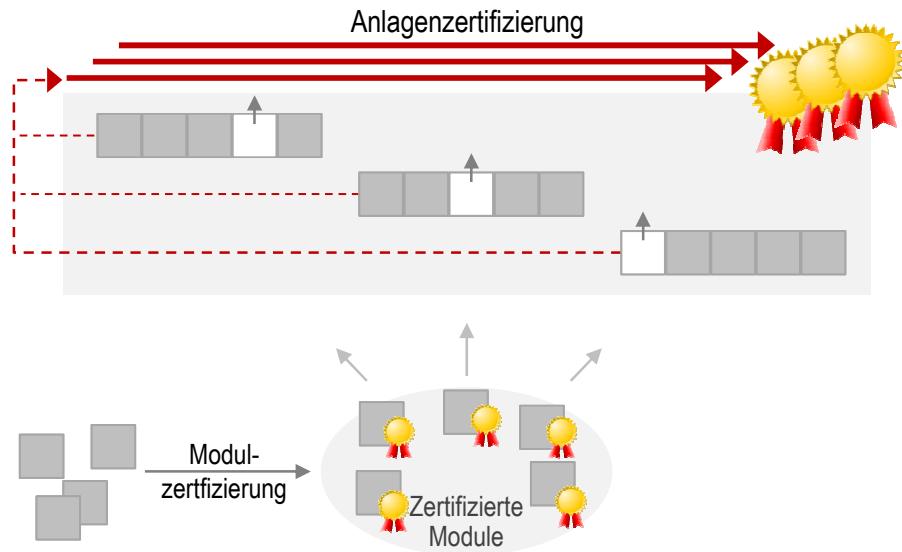
Werden Einzelmaschinen ausschließlich durch ein gemeinsames Not-Halt-Befehlsgerät verbunden, entsteht nicht allein durch diese Verbindung bereits eine Gesamtheit von Maschinen.

Daraus wird abgeleitet, dass wenn nur der Not-Halt-Befehl mit Hilfe einer übergeordneten sicherheitsgerichteten Steuerung realisiert wird, ist diese als ein Not-Halt-Befehlsgerät anzusehen. Verändert sich der produktionstechnische Zusammenhang, wenn ausschließlich für sicherheitstechnischen Maßnahmen eine übergeordnete Steuerung eingebaut wird, die die sicherheitsgerichtete Kommunikation der integrierten Maschinenmodule herstellt und überwacht? Nein, da weiterhin nicht alle Kriterien für einen produktionstechnischen Zusammenhang erfüllt sind. Aus diesem Grund bleibt es bei der bereits getroffenen Aussage, dass es sich dem Interpretationspapier nach nicht um eine Gesamtheit von Maschinen laut der **MRL** handelt. Generell muss bei jeder Änderung an einer Maschine/Anlage eine erneute Risikobeurteilung durchgeführt und entschieden werden, ob die Maschine/Anlage einer erneuten Zertifizierung bedarf.

Es verbleibt der Punkt, dass bei der Verknüpfung von vollständigen Maschinen der Gefahrenübertragung an den Schnittstellen zu bewerten und dokumentieren ist. Gegebenenfalls sind risikomindernde Maßnahmen zu ergreifen oder anzupassen. Genau das beschreibt die **DIN EN ISO 11161:2010** mit dem Begriff **Integriertes Fertigungssystem (IMS)**. Diese Norm ist auch unter der **MRL** harmonisiert und somit kann für das wandlungsfähige Montagesystem mit allen zugehörigen Montageeinheiten die **CE-Konformität** erbracht werden. Diese Aussage berücksichtigt nur die hier betrachteten Regelwerke.

Der TÜV SÜD hat innerhalb seiner Mitarbeit im Verein *Technologie-Initiative SmartFactory KL e.V.* ein Positionspapier zu dieser Problematik mit folgenden Aussagen herausgegeben. „Normen für komplexe Fertigungssystem sind noch nicht durchgängig eingeführt.“ [8] Dabei wird auch auf die Norm **EN ISO 11161:2007+A1:2010** für die Sicherheit von integrierten Fertigungssystemen verwiesen. Aktuell muss jedes Mal geklärt werden, ob ein Austausch einer Teilmaschine/Maschinenmodul eine erneute Prüfung und Risikobeurteilung notwendig macht. Jeder Konfigurationswechsel erfordert eine Rezertifizierung der gesamten Anlage. Dies ist in Abbildung 7 dargestellt, in Abbildung 13 auf Seite 42 wird vergleichsweise dargestellt wie es in Zukunft sein könnte. Auch fehlen Anforderungen an Sicherheitsfunk-

tionen, die beim Zuschalten oder Entfernen einzelner Maschinen verändert werden. Da diese für die Sicherheit der Anlage jedoch wichtig sind, werden Verfahren für eine Prüfung der funktionalen Sicherheit mit der veränderten Sicherheitsfunktion benötigt.



Quelle: TÜV SÜD

Abbildung 7: Heutige Situation der Zertifizierung bei einer konfigurierbaren Maschinensystem

## 2.7 Risikobeurteilung

Die Risikobeurteilung nach *DIN EN ISO 12100* ist unerlässlich, um die **CE-Konformität** zu erlangen und in diesem Fall die *DIN EN ISO 13849-1* richtig anwenden zu können. Eine Risikobeurteilung enthält eine Gefahren- und Risikoanalyse und eine Risikobewertung. Daraus resultiert das Sicherheits- und Bedienkonzept, zu dem auch die risikomindernden Maßnahmen gehören. Dabei müssen verschiedene Umgebungsbedienungen der Maschine/Anlage angegeben und festgesetzt werden. Das sind u. a. Lebensphasen der Maschine, Temperatur, Betriebsdauer, Standort, usw. Es sind dabei alle Arten von Gefährdungen in jeder Lebensphase zu betrachten, welche das im Detail sein können, ist der Norm zu entnehmen. „Die allgemeine Einschätzung von Risiken kann nach der *DIN EN ISO 12100* vorgenommen werden. Für die Risikoeinschätzung der sicherheitsbezogenen Teile von Steuerungen gilt ergänzend *DIN EN ISO 13849*.“ [14, S. 25] Es kann auch die **SIL-Riskomatrix** aus der *DIN EN 62061* verwendet werden. Diese kann aufgrund ihrer feineren Einteilung zu einem wirtschaftlichen Ergebnis führen. Bei den Risikobeurteilungen im Rahmen dieser Studienarbeit wird die Risikoeinschätzung für sicherheitsbezogene Teile von Steuerungen nach *DIN EN ISO 13849-1* vorgenommen, da sich das gesamte Vorgehen an ihr orientiert. Vergleichsweise kann bei sicherheitsgerichteten elektrischen, elektronischen und programmierbaren elektronischen Systemen der erforderliche **SIL** ermittelt. Um die *DIN EN 62061* umfassend zu erfüllen, ist im Vergleich mit der *EN ISO 13849*, eine andere aber vergleichbare Vorgehensweise erforderlich. (siehe Abschnitt 2.5 auf Seite 12)

## 2.8 Vorgehensweise der Risikobeurteilung

Die Risikobeurteilung ist für jede Lebensphase der Maschine/Anlage zu erstellen. Damit keine Gefährdungen übersehen werden, sollte schon vor dem Bau der Maschine, also bei der Konstruktion, die Risikobeurteilung nicht außer Acht gelassen werden. „Notwendige Schutzmaßnahmen sind im Nachhinein oft nur bedingt und in der Regel nur sehr kostenaufwendig durchführbar.“ [14, S. 17] Das in Abbildung 8 dargestellte Schema zeigt die methodische und richtlinienkonforme Vorgehensweise für eine einzelne Maschine. „Am Startpunkt beginnend und den Pfeilen folgend enthalten die einzelnen Felder alle zu berücksichtigenden Elemente einer Gefahren- und Risikoanalyse sowie eines Sicherheitskonzeptes.“ [14, S. 17] Dabei sollte das Ergebnis hier eine vollständige, sichere Montagemaschine sein, damit es bei dem Verbinden mehrerer Maschinenmodule nicht zu einer Gesamtheit von Maschinen laut **MRL** kommt. Bei dem wandlungsfähigen Montagesystem handelt es sich um vier einzelne Maschinen: Handarbeitsplatz, Maschine zur automatischen Montage, Maschine zur Lasergravur und smartes Transfersystem. Daraus resultieren vier Risikobeurteilungen. Auf Grundlage

dieser vier Beurteilungen wurde eine fünfte Risikobeurteilung des Gesamtsystems erstellt. Diese übergeordnete Risikobeurteilung stellt mit den vier untergeordneten die Beurteilung des Gesamtsystems dar. Durch ein gemeinsames Sicherheits- und Bedienungskonzept wird sichergestellt, dass zwischen Maschinenmodulen, den Schnittstellen, keine neuen Gefahren entstehen. Dieses Vorgehen ist in den Anforderungen (Abbildung 10 Seite 33) aufgezeigt. Mit dem gemeinsamen Sicherheits- und Bedienungskonzept wurden Spezifikationen für die Montagemodule und das smarte Transfersystem festgelegt. Diese sind wieder in die Risikobeurteilungen eingeflossen. Es ergab sich ein iterativer Prozess.

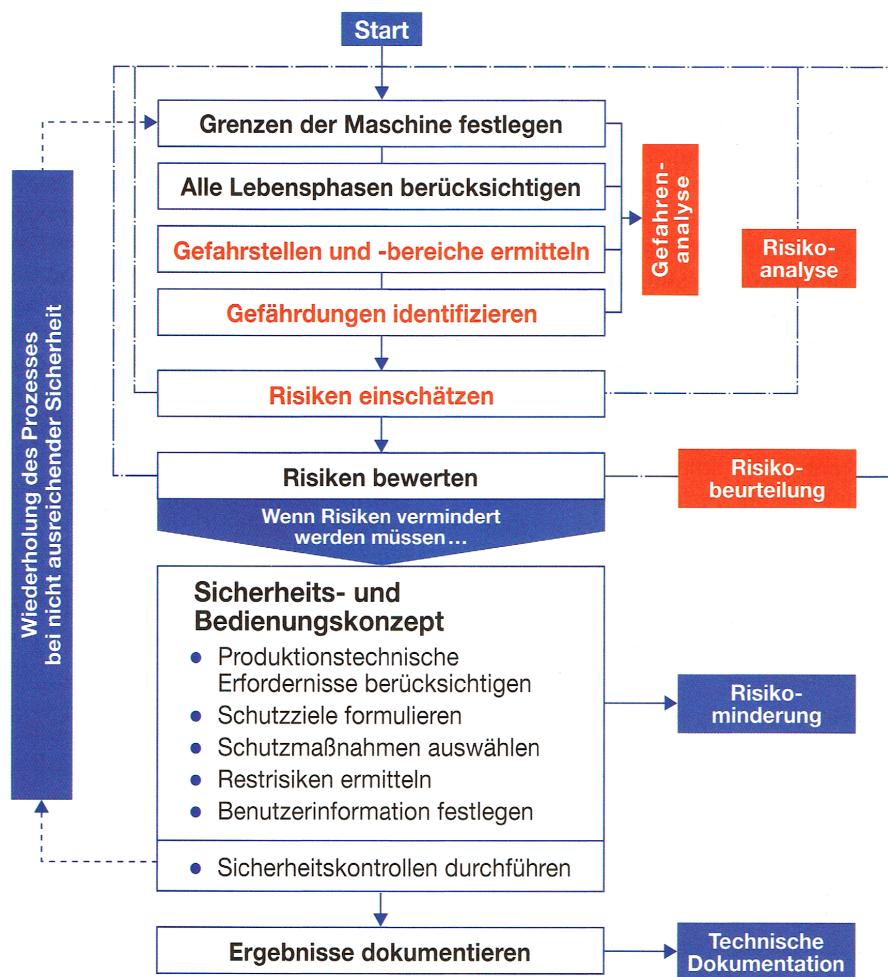


Abbildung 8: Risikobeurteilung und –minderung im Rahmen einer Sicherheitsstrategie von einer Einzelmaschine [14, S. 18]

### 2.8.1 Bestimmung der Maschinengrenzen

Die Bestimmung der Maschinengrenzen muss vor der Konstruktion einer Maschine erfolgen und bei der Risikobeurteilung berücksichtigt werden. Es sind keine Festlegungen aus der Planung bekannt und somit werden ohne weitere Prüfung ggf. Grenzen festgelegt, um eine Risikobeurteilung schematisch durchführen zu können. Dabei sieht die Norm *DIN EN ISO 12100* folgende Unterteilung vor:

- Verwendungsgrenzen
- Räumliche Grenzen
- Zeitliche Grenzen
- Weitere Grenzen

Die Verwendungsgrenzen gehen aus den jeweiligen Beschreibungen der Maschine/Anlage innerhalb der Risikoanalysen hervor. Bei dem betrachteten Montagesystem handelt es sich um einen Eigenbau. Das heißt, der Betreiber ist wie ein Hersteller tätig. Aus diesem Grund sollten die räumlichen Abmessungen, das Zusammenspiel mit dem Aufstellungsort und weitere Grenzen dem Hersteller und Betreiber bekannt sein. Die zeitliche Auslegung wird mit einem zwei Schichtbetrieb mit jeweils acht Stunden und einer fünf Tage Woche angenommen. Somit ergeben sich 4200 Betriebsstunden im Jahr. Die Anlage ist, wie in der Norm *DIN EN ISO 13849* gefordert, für eine Gebrauchsduer von 20 Jahren ausgelegt.

### 2.8.2 Lebensphasen der Anlage

Die Gefahren- und Risikoanalyse ist für alle Lebensphasen einer Maschine/Anlage durchzuführen. Dazu müssen zunächst die Lebensphasen des Montagesystems festgelegt werden. Hierfür wurde auf Kälble und Reudenbach [Anlage 1 14, S. 106] zurückgegriffen. Auch die Norm *DIN EN ISO 12100* macht in Abschnitt 5.4 Angaben zu möglichen Lebensphasen einer Maschine. Im Folgenden wird auf bestimmte Lebensphasen und deren Besonderheiten bei diesem Analgendesign eingegangen.

Wie bereits festgestellt, ist hier der Betreiber als Hersteller tätig. Trotzdem kann es zu einem Transport innerhalb des Produktionsstandorts oder zu einem anderen Standort kommen. Die einzelnen Montageeinheiten des Systems sind dazu mit Rollen versehen, jedoch können so die Lebensphasen schnell ineinander übergehen. Deshalb soll die folgende Erläuterung den Unterschied zwischen Transport und Rüsten/Einstellen verdeutlichen. Ist das betreffende Modul bereits nicht mehr eingebunden, muss es eingepackt und mit einem Transportgerät bewegt werden, so handelt es sich eindeutig um die Lebensphase Transport. Wird es hingegen aus einer Integration herausgenommen und nur wenige Meter auf den

eigenen Rollen bewegt, anschließend in ein anderes wandlungsfähiges Montagesystem (integriertes Fertigungssystem) integriert, so handelt es sich um eine Außerbetriebnahme, einen Transport und anschließende Inbetriebnahme. Die drei Lebensphasen haben einen scheinbaren fließenden Übergang. Dieser gesamte Vorgang könnte auch als Lebensphase Rüsten/Einstellen aufgefasst werden. Allerdings muss zum Transport die Energieversorgung getrennt sein. Dies bedeutet im Umkehrschluss, dass das Modul mit seinen Steuerungen erneut in Betrieb genommen werden muss. Deshalb die Unterteilung in drei Lebensphasen. Auch, wenn jede einzelne idealerweise nicht viel Zeit in Anspruch nimmt, ist dies die bessere Lösung.

Als Rüsten/Einstellen ist die Lebenszeit der Montagemaschine gemeint, in der diese auf die Integration vorbereitet wird oder Einstellungen für andere Produkte vorgenommen werden, während diese bereits über den Backbone versorgt wird. Den Vorgaben nach, soll diese Lebensphase möglichst kurz und automatisiert erfolgen. Diese Beschreibungen der Lebensphasen wurden in die Dokumentationen der Risikobeurteilungen übernommen und bei der Beschreibung der Maschine/Anlage berücksichtigt.

### 2.8.3 Ermittlung von Gefährdungen

„Unter der Berücksichtigung der Grenzen der Maschine ist der erste Schritt die Festlegung des Umfangs des zu analysierenden Systems, z.B. der (die) Abschnitt(e) des Lebenszyklus der Maschine, der (die) Teil(e) und/oder die Funktion(en) der Maschine.“ [17, S. 11] Die Funktionen gehen aus der Beschreibung der bestimmungsgemäßen Verwendung hervor. Die Lebenszyklen sind bereits unter Lebensphasen der Anlage und in der Dokumentation der Risikobeurteilung beschrieben.

„Der zweite Schritt ist die Festlegung der Aufgaben, die von Personen durchzuführen sind, die an oder in der Nähe der Maschine tätig sind, oder die von der Maschine durchzuführenden Arbeitsvorgänge in jedem der ausgewählten Abschnitte des Lebenszyklus. Bei diesem Schritt könnte die in *ISO 12100:2010, Tabelle B.3*, beschriebene Aufgabenliste verwendet werden.“ [17, S. 11] In der erstellten Vorlage zur Dokumentation der Risikobeurteilungen ist dieser Schritt unter *3.3 Nutzung* festzuhalten oder in der Beschreibung der Lebensphasen zu berücksichtigen.

„Der dritte Schritt besteht darin, die relevanten Gefährdungen und die möglichen Gefährdungssituationen für jede Aufgabe oder jeden Arbeitsvorgang in jedem einzelnen Gefährdungsbereich zu untersuchen.“ [17, S. 11] Dabei ist zu beachten welche Arbeitsgänge von der Maschine oder, der daran arbeitenden Person durchzuführen sind. Auch die Umgebungsbedingungen sind nicht außeracht zu lassen. Des Weiteren müssen mögliche Betriebszustände, unabsichtliches Verhalten des Bedienpersonals und vernünftigerweise

vorhersehbare Fehlanwendung der Maschine betrachtet werden, um Gefahrenstellen zu ermitteln. Hier sind es vor allem der Arbeitsbereich des Roboters, die Hubeinheit des Lasers, die Transferbänder und die Fixiereinheit des Handarbeitsplatzes. An diesen Punkten können kritische Gefahrenstellen entstehen. Die häufigsten sind:

- Quetsch- und Scherstellen,
- Schneid-, Stich-, Stoßstellen,
- Fangstellen und
- Einzugstellen.

Das wichtigste ist die Identifizierung von Gefährdungen. Dabei ist das systematische Vorgehen und die Betrachtung von vorhersehbaren Gefährdungen, Gefährdungssituationen und/oder Gefährdungsergebnissen in sämtlichen Lebensphasen der Maschine von großer Bedeutung. Mögliche Verfahren werden in der *DIN ISO/TR 14121-2* vorgestellt, die auch hier zur Hilfe genommen wurde. Die im Rahmen dieser Studienarbeit durchgeführte Risikobeurteilung wurde mithilfe der Gefährdungs-Checkliste aus Kälble und Reudenbach [14, 56ff] durchgeführt. Diese geht von den Gefährdungen aus und stellt somit den Bottom-up-Ansatz nach *DIN ISO/TR 14121-2* dar.

#### 2.8.4 Von der Gefährdung zum quantifizierten Risiko

„Nach der Identifizierung der Gefährdungen ist für jede Gefährdungssituation eine Risikoeinschätzung durchzuführen, indem die in 5.5.2 aufgeführten Risikoelemente bestimmt werden. Bei der Bestimmung dieser Elemente sind die in 5.5.3 festgelegten Aspekte zu berücksichtigen.“ [17, S. 23] Das heißt, sind alle möglichen Gefährdungen identifiziert und ist ihr Ausmaß bekannt, so werden diese mit Hilfe eines geeigneten Verfahrens eingeschätzt. Dazu wird der Begriff *Risiko* eingeführt. Das Risiko hängt nicht einfach nur vom Schadensausmaß ab, sondern bildet mit der Eintrittswahrscheinlichkeit des Schadens eine Funktion. Dabei sind die vorgegebenen Risikoelemente zu berücksichtigen. Die Norm macht keine Angaben, wie die Risikoelemente zu bewerten sind. Im technischen Bericht *DIN ISO/TR 14121-2* sind drei verschiedene Verfahren/Instrumente für die Risikoeinschätzung auf Basis der Risikoelemente aus der *DIN EN ISO 12100* aufgezeigt und mit einem Beispiel veranschaulicht. Die Instrumente zur Risikoeinschätzung werden zwischen Risikomatrix, Risikograph und nummerischer Bewertung unterschieden. Bei der nummerischen Bewertung kann die Objektivität der Risikohöhe gut vermittelt werden. Es sollte einem jedoch sein, dass auch hier die Vergabe der Punktzahlen subjektiv ist. [18] Mit einem der drei Instrumente oder auch durch eine Mischung zweier kann eine Risikoeinschätzung vorgenommen werden. Die Einbeziehung von Erfahrungswerten ist bei der Einschätzung

von Vorteil. Liegen hingegen keine vor, so handelt es sich viel mehr um eine subjektive Einschätzung, die durch geeignete Messmethoden oder andere Verfahren zu belegen ist. Es handelt sich bei den Risikoeinschätzungen nach *DIN EN ISO 12100* um eine allgemein gültige Einschätzung. Für spezielle Schädigungen, die z.B. durch die Kumulation von mehreren Gefährdungen auftreten, sind angepasste Risikoeinschätzungen durchzuführen. Geräuschemissionen oder wiederholte Bewegungsabläufe stellen solche dar. [18] Dieser Punkt erschwert das beliebige Hinzufügen und Entfernen von Maschinenmodulen. Die Risikoeinschätzung von sicherheitsbezogenen Teilen einer Maschinensteuerung kann nach *DIN EN ISO 13849-1* oder *DIN EN 62061* durchgeführt werden. [14, S. 27]

In Rahmen dieser Studienarbeit wird die Risikoeinschätzung nach dem Beispiel 6.5.2 der *DIN ISO/TR 14121-2:2013-02* vorgenommen. Dabei handelt es sich um eine Mischform von einer numerischen Bewertung mit einer zusammenfassenden Risikomatrix. In der Dokumentation der Risikobeurteilung ist dies unter „4.3 Gefährdungseinschätzung und -beschreibung“ festgehalten.

### 2.8.5 Risikobewertung

Um die Risikobeurteilung abzuschließen, werden die geschätzten Risiken mit dem Ziel bewertet,

- „zu entscheiden, welche Gefährdungssituationen, sofern vorhanden, eine weitere Risikominderung erfordern, und
- zu ermitteln, ob die erforderliche Risikominderung ohne Hervorrufen weiterer Gefährdungen oder Erhöhen anderer Risiken erreicht worden ist.

[...] Als allgemeine Regel ist das eingeschätzte Risiko nur ein Beitrag zur Entscheidung darüber, ob der iterative Prozess der Risikominderung zu beenden ist. Diese Entscheidung sollte weitere Betrachtungen umfassen, wie z. B. Vorschriften, Gesetze, Arbeitsorganisationen und Arbeitsmethoden, technische Grenzen und Wirtschaftlichkeit.“ [18, S. 26]

## 2.9 Risikominderung

Ziel der Risikominderung ist es, durch Beseitigung der Gefährdungen oder durch Minderung der Risikoelemente, das verbundene Risiko auf ein hinreichendes Maß zu reduzieren. Dabei ist nach dem in Abschnitt 6.1 der Norm *DIN EN ISO 12100* beschriebene *Drei Stufen Verfahren* vorzugehen. Darin wird nicht nur die Reihenfolge der Maßnahmen beschrieben, sondern es werden auch geeignete Verfahren angegeben. Die Bedingungen für die Auswahl der risikomindernden Maßnahmen sind bereits in der Risikobewertung (*DIN EN ISO 12100*

*Abschnitt 5.6)* angegeben. Diese sollten als Fragen auf einer Checkliste formuliert sein. Anhand dieser ist leicht die Wirksamkeit der Risikominderung nachzuvollziehen. [17] [14, S. 37] Dies erfolgt mit Anlage 2 der ausgearbeiteten Risikobeurteilungen.

Eine wirkungsvolle Risikominderung hängt von vielen Einflüssen ab, am offensichtlichsten von den Sicherheitsanforderungen. Darüber hinaus müssen auch die Produktionsanforderungen, die Bedienbarkeit und Wirtschaftlichkeit bei der Auswahl der Risikomindernden Maßnahmen berücksichtigt werden. Mit einem Sicherheits- und Bedienungskonzept kann ein Überblick über diese Anforderungen geschaffen werden. Dazu sind alle Erfordernisse bezüglich Sicherheit, Funktionsfähigkeit, Bedienbarkeit und Wirtschaftlichkeit einer Maschine/Anlage zu berücksichtigen (Abbildung 9). „Sämtliche Überlegungen, wie die notwendige Sicherheit erreicht werden soll, sind Bestandteil einer Risikobeurteilung gemäß EG Maschinenrichtlinie. Aus einem Sicherheits- und Bedienungskonzept sollten deshalb die strategischen Entscheidungsgründe für bzw. gegen bestimmte Lösungen ersichtlich sein.“ [14, S. 31]

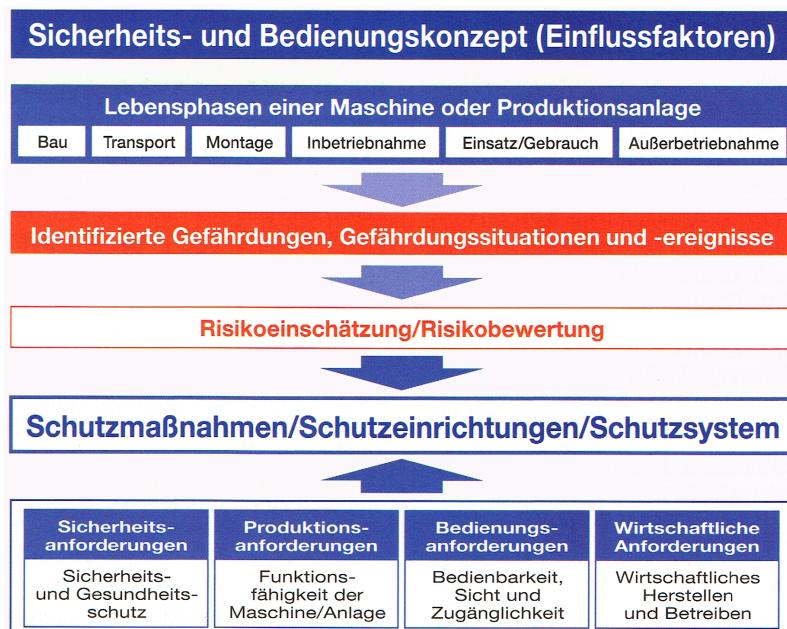


Abbildung 9: Anforderungen an ein Sicherheits- und Bedienkonzept [14, S. 31]

Bevor eine Schutzmaßnahme ausgewählt werden kann, muss das Schutzziel formuliert sein. Dabei ist meist der Personenschutz das wichtigste. Es können aber auch andere Ziele sein, wie z. B. Beschädigung an der Maschine/Anlage selbst oder von teuren Werkzeugen. Ist ein vollkommener Schutz des Bedienpersonals mit konstruktiven Maßnahmen oder durch

Schutzmaßnahmen nicht möglich, so hat dies meist technische und/oder wirtschaftliche Gründe. Ist es mit dem *Stand der Technik* nicht möglich und nicht zu vermeiden, so entstehen unvermeidbare Restrisiken. Diese können durch sichere Verhaltensweisen ausgeglichen werden. Mit entsprechenden Maßnahmen, die das Verhalten und die Qualität der Maschinenbediener sichern, kann dies gelingen. Zur Risikominderung gehört auch die Benutzerinformation. Um welche Informationen es sich neben dem Umgang mit Restrisiken und der Betriebsanleitung handelt, kann sowohl der Norm *ISO 12100* als auch der *MRL* entnommen werden. Das hier betrachtete wandlungsfähige Montagesystem mit Hilfe von sicheren Verhaltensweisen und dem Einsatz von qualifizierten Personal als sicher zu betrachten, ist sehr gewagt und kann im Fall eines Unfalls zu Schwierigkeiten führen.

Wie anfangs angedeutet, muss die Wirksamkeit der Risikominderung überprüft werden. Bei Nichteinfüllung ist ggf. eine andere Schutzmaßnahme auszuwählen, um den iterativen Prozess der Risikominderung und Risikoanalyse abschließen zu können.

## 2.10 Erstellung der Dokumentation

Im Rahmen dieser Studienarbeit wurde eine Vorlage zur Dokumentation der Risikobeurteilungen und risikomindernden Maßnahmen erstellt. Es handelt sich dabei nicht um eine vollständige Maschinendokumentation, die nach der *MRL* zum Nachweis der *CE-Konformität* ausreicht. Die geforderten Validierungen für sicherheitsgerichtete Systemteile wurden nicht durchgeführt und in der Dokumentation berücksichtigt, wie es in der *DIN EN ISO 13849-2* gefordert ist. Dies kann erst nach der Umsetzung der erforderlichen Maßnahmen erfolgen. Das gilt auch für Systeme, die nach *DIN EN 62061* beurteilt werden. Der Sicherheitsplan beinhaltet eine Validierung. In diesem Fall müsste nach dem V-Modell gearbeitet werden. Bei dem Zusammenstellen einer Vorlage für die Dokumentation der Risikobeurteilung mit anschließenden Sicherheits- und Bedienungskonzept wurden Teile von Käble und Reudenbach [14] übernommen. Weiteren Einfluss erhielt die Vorlage *MBT-RAT RiskAssessmentTool* von Ostermann [19]. Darüber hinaus wurde die Vorlage von der Firma Siemens für eine Risikobeurteilung einbezogen. Mit Blick in die *DIN EN ISO 12100* und der *DIN ISO/TR 14121-2* wurden die Inhalte zusammengestellt und dabei wurden die Anforderungen und die Gliederung übernommen. Die in den vorherigen Kapiteln erwähnten Problematiken wurden aufgegriffen und bei der Durchführung berücksichtigt.

## 2.11 Abschluss der Risikobeurteilung

Die Risikobeurteilung ist ein iterativer Prozess und muss nach der Umsetzung der Schutzmaßnahmen erneut durchgeführt werden, bis die Restrisiken der Einzelmaschinen und, in

Folge dessen, die vom Gesamtsystem vertretbar sind. Die **CE-Konformität** des integrierten Fertigungssystems, welches hier das wandlungsfähige Montagesystem darstellt, muss erneut nachgewiesen werden, wenn derzeit noch nicht berücksichtigte neue Montagemaschinen integriert werden. Es bleibt festzustellen, dass mit dem aktuellen Regelwerk, welches den Stand der Technik darstellt, kein zufriedenstellendes Sicherheitskonzept finden lässt. Nach einer Änderung der Zusammenstellung der Maschinen muss die Risikobeurteilung wiederholt werden. Eine Erneuerung der **CE-Konformität** ist nicht auszuschließen.

## 3 Anforderungen

In diesem Kapitel werden die Erkenntnisse aus dem Kapitel 2 Stand der Technik mit messbaren Kriterien zu Anforderungen formuliert. Mit Hilfe dieser werden anschließend in Kapitel 4 mögliche Lösungsansätze formuliert.

### 3.1 Normen und Richtlinien

Durch integrierbare Maschinenmodule ist ein wandlungsfähiges Montagesystem entstanden. Dieser Aufbau ist in dem Sicherheitskonzept zu berücksichtigen. Nach den Erkenntnissen aus Kapitel 2.6 auf Seite 18 gibt es zur Zeit kein durchgängiges Regelwerk für Systeme, wie es das wandlungsfähige Montagesystem darstellt. Der dort beschriebene Weg kann jedoch eine zeitweise Lösung sein. Dazu darf sich keine Gesamtheit von Maschinen laut [MRL](#) bilden. Daraus ergibt sich die Anforderung, dass jedes Montagemodul eine vollständige Maschine sein muss und über eine eigene [CE-Konformität](#) verfügt. Zwischen den Modulen darf sich kein produktionstechnischer Zusammenhang ergeben, ausgenommen ist eine übergeordnete Not-Halt-Befehlseinrichtung. Beim Austausch der Maschinenmodule muss jedes Mal geklärt werden, ob dieser Austausch eine erneute Risikobeurteilung und CE-Prüfung notwendig macht. Dabei ist die Norm [ISO 11161](#) hinzuzuziehen. Durch Standardisierung der Module kann der anfallende Aufwand für die Erstellung der Spezifikationen, den Aufbau (Verkettung), die Inbetriebnahme, den Betrieb, sowie den Austausch der modularen Systeme, reduziert werden. Die Schnittstellen müssen, wie folgt, standardisiert werden.

Spezifikation der Module:

- Verwendungsgrenzen (räumlich, zeitlich, Umgebung)
- mechanische Schnittstellen
- elektrische Schnittstellen
- Schnittstellen für die Sicherheitsfunktionen
- Software-Schnittstellen
- generische Sicherheitsklassifizierung (wichtig für die spätere dynamische Verkettung)

Spezifikationen der Anlage:

- bestimmungsgemäße Verwendung (Ziel/Produkt)
- Integration in den Betriebsprozess
- Grenzen (maximale Größe der Anlage, Anzahl der Stationen, Mensch-Maschinen Anwendung)

Diese Spezifikationen sind noch festzulegen, im Folgenden werden mögliche Anforderungen an die Schnittstellen-Komponenten abgeleitet und festgelegt, um die Anlage nach dem Stand der Technik sicher zu gestalten. [8]

### Risikobeurteilung

Die oben genannten Anforderungen sind bei jeder Risikobeurteilung von einer Maschine, die zu dem wandlungsfähigen Montagesystem gehört, zu berücksichtigen. Dies ist mit dem Vorgehen, das in Abbildung 10 gezeigt ist, mit dem Stand der Technik berücksichtigt worden. Dazu ist für jede Maschine und das smarte Transfersystem jeweils eine Risikobeurteilung zu erstellen. Anschließend ist ein einheitliches Sicherheits- und Bedienungskonzept festzulegen, welches im nächsten Schritt auf jede Maschine übertragen wird. An dieser Stelle ist es den jeweiligen Prozessanforderungen anzupassen. Eine abschließende Sicherheitskontrolle stellt die Sicherheit des Gesamtsystems fest und berücksichtigt dabei verschiedene physikalische Aufbauten und Kombinationen der Montagemaschinen. Dieses Vorgehen spiegelt den heutigen Stand der Technik aus Abbildung 7 auf Seite 21 wieder. In Zukunft ist ein Konzept zu finden, welches eine einfachere Bewertung und Dokumentation von Systemen mit Maschinenmodulen ermöglicht. Das Ändern von Montagemaschinen und Hinzufügen von derzeit noch unbekannten Maschinenmodulen, ist durch ein zukünftiges Konzept zu ermöglichen. Ohne die notwendige erneute Zertifizierung des gesamten Systems.

### Anforderungen an den Integrationsprozess

Der Integrationsprozess muss so gestaltet sein, dass durch Fehler beim Integrieren keine Gefahren entstehen. Die Anforderungen ergeben sich unter anderem durch das iterative Vorgehen der Risikobeurteilung. Das Ziel des Integrationsprozesses ist es, die globale Not-Halt-Kette anzupassen und den sicheren Austausch möglicher weiterer Signale zur Ausführung von Sicherheitsfunktionen zu ermöglichen. Das wandlungsfähige Montagesystem ist von seiner Größe überschaubar und eine Einteilung in Sicherheitsbereiche ist nicht erkennbar, daher genügt die Realisierung eines globalen Not-Halts. Weitere Anforderungen an diese zusätzliche Sicherheitsfunktion ist den Normen ISO 13850, ISO 11161 zu entnehmen. Es ist sicherzustellen, dass alle an das smarte Transfersystem angestellten Maschinen ordnungsgemäß integriert werden. Ist dies nicht gegeben, hat es einen Halt der gesamten Anlage zur Folge, um das Risiko zu mindern. Von dem Modul selbst ist ebenfalls zu erfassen, ob dieses einzeln oder an dem smarten Transfersystem betrieben wird. Nachdem Heranschieben einer Maschine ist eine angemessene Zeit bis zum Halt der Anlage einzuräumen. Mit einer zusätzlichen Betriebsart am smarten Transfersystem, kann die Problematik ebenfalls gelöst werden. Diese kann einen Halt oder die Reduzierung der Geschwindigkeit auslösen. Die Vorgehensweise beim Integrieren von Maschinen ist eine bewusste Handlung und mit einer Steuerung nach dem Plug-and-Produce-Prinzip zu gestalten (siehe Abschnitt 3.2). Neben einer sicheren automatischen Erkennung der zu integrierenden Maschine, besteht

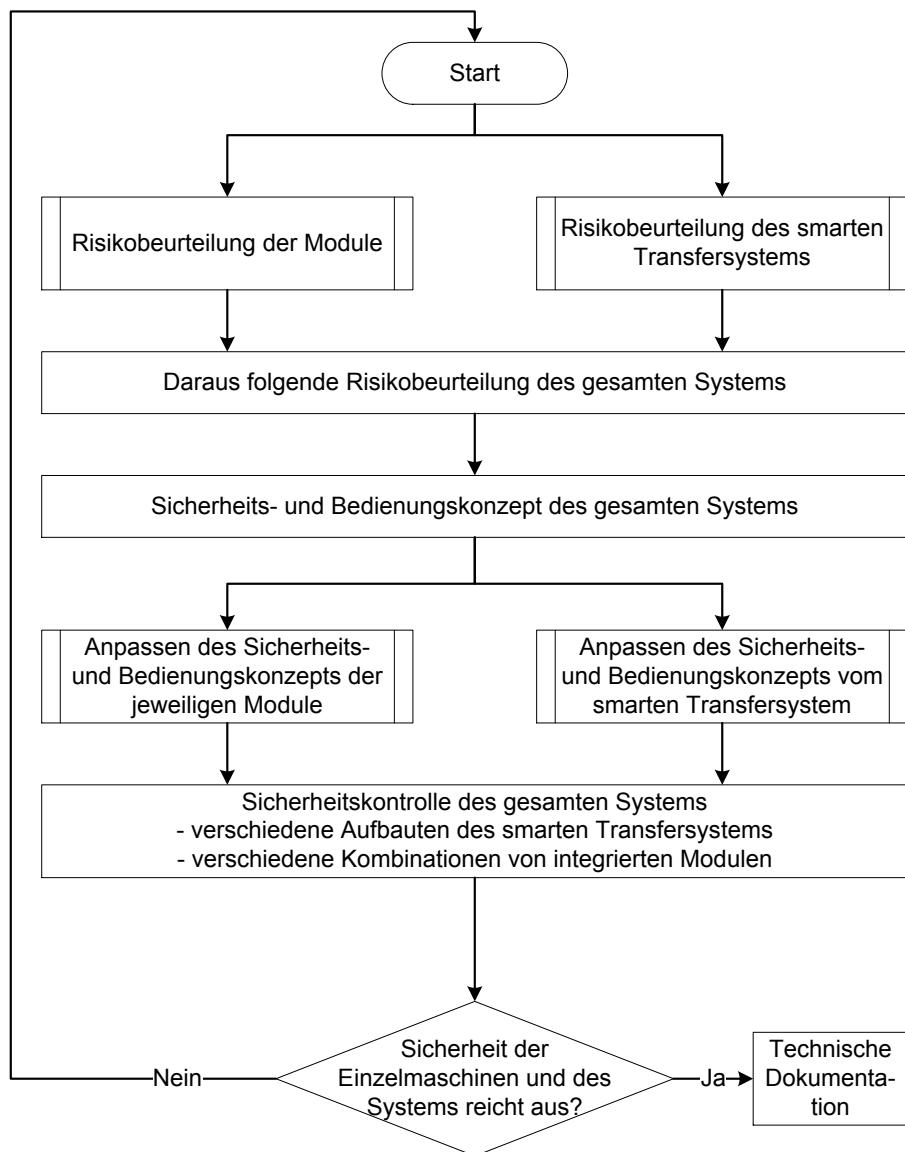


Abbildung 10: Ablauf der Risikobeurteilung

auch die Möglichkeit einer manuellen Bekanntgabe dieser Information. In jedem Fall muss die Richtigkeit dieser Information sichergestellt sein. Dies kann beispielsweise durch ein Testsignal zwischen angestellter Maschine und der Integrationsinfrastruktur oder einer Topologieerkennung geschehen. Das Entfernen einer Maschine hat einen Stillstand der Anlage zur Folge. Durch ein bewusstes Vorgehen ist dieses zu verhindern.

Die normativen Anforderungen kurz zusammengefasst: Es sind Spezifikationen für die

Schnittstellen festzulegen. Nach dem Stand der Technik muss jedes Montagemodul eine für sich sichere, richtlinienkonforme und vollständige Maschine sein, die auf die Integration in eine zugehörige Infrastruktur abgestimmt ist. Das wandlungsfähige Montagesystem stellt daher ein integriertes Fertigungssystem nach *ISO 11161* dar. Die Montagemaschinen sind Einzelmaschinen, deren Sicherheit nach *ISO 12100*, *ISO 13849* und weiteren relevanten Richtlinien und darunter harmonisierten Normen auszulegen ist. Die Konformität zu allen relevanten EG-Richtlinien ist für jedes Modul nachzuweisen. Bei einer neuen Konfiguration der Anlage ist die funktionale Sicherheit neu zu bewerten.

### 3.2 An die Steuerung

Die zuvor genannten normativen Anforderungen müssen im Gesamtkonzept der Anlage berücksichtigt werden, so haben diese unter anderem Einfluss auf die Steuerungen der einzelnen Montagemaschinen und einer möglichen übergeordneten Steuerung in der Integrationsinfrastruktur. Aus der Forderung, dass jedes Montagemodul eine sichere, integrierbare und vollständige Maschine sein muss, ergibt sich die Forderung, dass jedes Maschinenmodul über eine eigene unabhängige und sichere Steuerung verfügen muss. Diese muss die Sicherheitsfunktionen, die aus der jeweiligen Risikobeurteilung und den zutreffenden Normen (z. B. *ISO 13849* hervorgehen, erfüllen. Aus diesem Grund ist die Worst-Case-Reaktionszeit der Steuerung bzw. der integrierten Steuerungen zu ermitteln. Die Sicherheitsfunktionen der integrativen Maschinen sind lokal und unabhängig vom smarten Transfersystem umzusetzen.

Das Steuerungskonzept muss die bereits im Abschnitt 3.1 genannten Anforderungen zum Integrieren umsetzen können. Die steuerungstechnische Vorgehensweise sollte im Ergebnis eine sein, die dem Plug-and-Produce-Prinzip entspricht. Dazu gehört die Vermeidung eines Anlagenstopps beim Integrieren und Entfernen von Maschinen. Die automatische Erkennung der Maschinen ist wünschenswert. Eine bewusste Handlung muss verbleiben. Damit ist eine Auswahl oder Bestätigung der aktuellen Konfiguration nicht vollständig zu automatisieren. Damit die Integrierbarkeit nach *ISO 11161* gewährleistet ist, muss eine sicherheitsgerichtete Kommunikation zwischen den einzelnen Montageeinheiten existieren. Über diesen Kommunikationsweg sind die benötigten Sicherheitsfunktionen zu realisieren. Der Einsatz einer übergeordneten Sicherheitssteuerung im smarten Transfersystem ist denkbar, der Verzicht hingegen wünschenswert.

Im bestehenden Montagesystem kommt als Kommunikationsmedium bereits das Ethernet-basierte PROFINet-Protokoll zum Einsatz. Somit wird eine Kommunikation über das zugehörige Sicherheitsprotokoll PROFIsafe gefordert. Alternativ kann zum Aufbau der Not-Halt-Kette und des sicheren Kommunikationskanals ein anderes Protokoll benutzt wer-

den, welches das gleiche Übertragungsmedium Ethernet unterstützt. Steuerungskonzepte die ein anderes Kommunikationsmedium benutzen, sind zum Vergleich mit zu berücksichtigen. Diese können möglicherweise eine einfache Handhabung in der Umsetzung bieten. Bei der Vernetzung von den integrierten Steuerungen ist auf die Unterstützung möglichst vieler Topologien und auf die maximale Entfernung untereinander zu achten, da dies die Flexibilität des System erhält. Der aktuelle Ausbau des wandlungsfähigen Montagesystems beträgt drei integrierbare Maschinen und eine Integrationsinfrastruktur, das smarte Transfersystem. Es sind bis zu sieben integrierbare Maschinen geplant. Es ergibt sich die Forderung, diesen Ausbau zu ermöglichen und schätzungsweise acht Steuerungen aus eigenständigen Maschinen beliebig vernetzen zu können. Die Verwendung von Steuerungen verschiedener Hersteller ist wünschenswert. Alle gefundenen Steuerungskonzepte müssen am Markt verfügbar sein.

### 3.3 An die Wirtschaftlichkeit

Neben den Anschaffungskosten der benötigten Komponenten ist auch der Aufwand der Installation in die bestehende Infrastruktur und der Implementierung der Funktionen von Interesse. Bei den Installationskosten ist das Kommunikationsmedium ausschlaggebend, da die Nutzung der vorhandenen Infrastruktur den geringsten Aufwand zeigt. Die Zeit, die zur Implementierung der gewünschten Funktionen benötigt wird, erhöht den Aufwand, das Steuerungssystem umzusetzen. Hier ist zu unterscheiden, ob es sich dabei um eine Konfiguration der Steuerung handelt oder ob die Implementierung in einer Hochsprache nach *IEC 61131* erfolgt und ggf. zertifiziert werden. Zur Reduzierung und Einschätzung des Aufwands sollten häufig verwendete Funktionen in bereits zertifizierten Bausteinen implementiert sein. Der Listenpreis der benötigten Komponenten stellt ein weiteres Vergleichskriterium dar und ist im Zusammenhang mit den genannten Punkten und dem Erreichen der Steuerungsanforderungen zu sehen.

### 3.4 Aus der Risikobeurteilung

Die Anforderungen an die Risikobeurteilungen und die Vorgehensweise ist in der *ISO 12100* festgelegt (siehe Abschnitt 2.7 Seite 22). Eine vollständige Risikobeurteilung mit Kenntnis sämtlicher Normen, Richtlinien und Vorschriften würde den Umfang dieser Studienarbeit überschreiten. Aus den Risikobeurteilungen unter Beachtung einiger Normen (siehe Abschnitt 2.4 Seite 11 und der Dokumentation der jeweiligen Maschine) gehen folgende Anforderungen hervor.

### 3.4.1 Allgemein

Normativ kann die Wandlungsfähigkeit erhalten bleiben, wenn jedes Montagemodul eine vollständige und sichere Maschine ist (siehe Abschnitt 2.6). Alle Bauteile, die zur jeweiligen Montagemaschine gehören und von dieser gesteuert werden, dürfen nur an dieser befestigt sein. Dies ist insbesondere für die Indexierungen und das RFID-Lesegerät nicht der Fall, denn diese sind fest in das Transferband geschraubt. Hier ist in Bezug auf Abschnitt 2.6 eine Entscheidung zu treffen, zu welcher Maschine diese gehören. Um eine Verkettung der Maschinen zu vermeiden, ist es sinnvoll, die Baugruppen der Integrationsinfrastruktur an den Integrationsplätzen einheitlich mit Stopfern, Indexierung und RFID-Lesegerät zu gestalten. Das RFID-Lesegerät wird direkt über die Plug-and-Produce-Schnittstelle zur integrierten Maschine geführt. Des Weiteren ist an beiden Montagemaschinen der Zugang in den Gefahrenbereich möglich. Hier muss die trennende Schutzeinrichtung so konstruiert werden, dass es den Anforderungen der *DIN EN ISO 13857* und der *DIN EN ISO 13855* entspricht.

Nach der Integration an das smarte Transfersystem sollte sich diese über dem Transferband befinden. Auch das Öffnen der trennenden Schutzeinrichtung, welche gleichzeitig das Gehäuse der Maschine ist, wird weder überprüft noch verhindert und bietet in vielen Lebensphasen keinen angemessenen Zugang, der für anfallende Aufgaben benötigt wird. Die Montagemaschinen sind mit Rollen ausgestattet, somit muss auch Anhang I Abschnitt 3 der *MRL „[...] Beweglichkeit von Maschinen [...]“* beachtet werden. Daraus geht hervor, dass die Standsicherheit und das schnelle Anhalten beim Transport (Schieben) der Maschine gewährleistet sein müssen. In diesem Zusammenhang sind auch die Bedingungen für den bestimmungsgemäßen Einsatzort festzulegen. Ein integriertes Fertigungssystem kann in verschiedene Sicherheitsbereiche eingeteilt werden, wenn diese sichtlich erkennbar sind. Auf das betrachtete Montagesystem bezogen heißt das, jede Betätigung eines Not-Halts versetzt die Maschinen, die im Sichtfeld oder Gefahrenbereich des Bedieners sind, in einen sicheren Halt. Detailliertere Informationen können der *DIN EN ISO 11161:2010-10* und der *DIN EN ISO 13850* entnommen werden.

### 3.4.2 Montageroboter

An der Maschine zur automatischen Montage ist das Eingreifen in den Gefahrenbereich des Roboters während des automatischen Betriebes möglich. Zur Bestimmung geeigneter Schutzmaßnahmen wird die Norm *DIN EN ISO 10218-2:2011* herangezogen. Diese ist eine anwendungsspezifische Norm und beschreibt die Integration eines Roboters in eine Maschine. Die risikomindernde Maßnahme der trennenden Schutzeinrichtung muss zur Erledigung

der anfallenden Aufgaben einen geeigneten Zugang in den Gefährdungsbereich erhalten. Zur Bestimmung des Zugangs ergibt sich folgende Situation, die in Abbildung 11 skizziert ist. Der maximale Raum (grün) vom Roboter ist wesentlich größer, als es die räumlichen Grenzen der Maschine zulassen (geschützter Raum/schwarz). Aus diesem Grund ist die Roboterbewegung zu begrenzen. Dies kann nicht-mechanisch über die Software der Robotersteuerung erfolgen, indem ein Betriebsraum vorgegeben wird. Verlässt der Manipulator diesen Raum, wird ein sicherer Halt über die Steuerung des Roboters ausgelöst und der Manipulator gestoppt. Der dafür benötigte Anhalteweg addiert sich zu dem eingeschränkten Raum. Dieser ist zum Teil größer als der zur Verfügung stehende geschützte Raum (Gehäuse). Eine mechanische Begrenzung der Achsen ermöglicht einen kleineren eingeschränkten Raum, der immer noch die vorhandenen räumlichen Grenzen der Maschine überschreitet. Aus diesem Grund ergibt sich, dass die äußere trennende Schutzeinrichtung (Gehäuse des Moduls) als Begrenzungseinrichtung nach *DIN EN ISO 10218-2:2011* Abschnitt 5.4.3 zu gestalten ist.

Bei der Auslegung von Mindestabständen wird auf die *DIN EN ISO 13855:2010* verwiesen. Demnach ist der Mindestabstand (S) zwischen dem Gefährdungsbereich (eingeschränkter Raum) und dem Zugang nach Gleichung (1) zu berechnen. Dabei setzt sich die benötigte Abschaltzeit, wie in Gleichung (2) gezeigt, zusammen. Zur Berechnung wurde eine ungefähre Reaktionszeit für den Sicherheitstürschalter angenommen. Diese Reaktionszeit ist durch den Wert des tatsächlich verbauten Sicherheitstürschalters zu ersetzen. Mit Hilfe von Gleichung (3) wurde eine mögliche Zeit zur Türöffnung ermittelt, bis in den Gefährdungsbereich eingegriffen werden kann. Es ergibt sich ein Sicherheitsabstand von 904 mm. Dieser ist in den vorhanden räumlichen Grenzen nicht umzusetzen. Auch die Verringerung der Verzögerungszeit des Schalters führt nicht zu dem benötigten Ergebnis. Daher ergibt sich als Anforderung an den Zugang eine verriegelnde trennende Schutzeinrichtung mit Zuhaltung. Diese lässt sich erst öffnen, wenn der Manipulator sicher abgeschaltet ist oder eine entsprechende manuelle Betriebsart gewählt wurde.

Über die Sicherheitssteuerung müssen folgende Betriebsarten realisiert sein: ein Automatikbetrieb und verschiedene manuelle Betriebsarten. Das Ingangsetzen des Robotersystems muss durch eine gesonderte Betätigung erfolgen. Weitere Anforderungen an die Betriebsarten und deren Auswahl sind der Norm *DIN EN ISO 10218-2:2011* Abschnitt 5.6 zu entnehmen.

$$S = (K \cdot (T - t_3)) \quad (1)$$

$$S = (1600 \text{ mm s}^{-1} \cdot (590 \text{ ms} - 25 \text{ ms}))$$

$$S = 904 \text{ mm}$$

$$T = t_{Schalter} + t_{Sicherheitssteuerung} + t_{Roboter} \quad (2)$$

$$T = 260 \text{ ms} + 50 \text{ ms} + 280 \text{ ms}$$

$$T = 590 \text{ ms}$$

$$t_3 = \frac{e}{v} \quad (3)$$

$$t_3 = \frac{50 \text{ mm}}{2000 \text{ mm s}^{-1}}$$

$$t_3 = 25 \text{ ms}$$

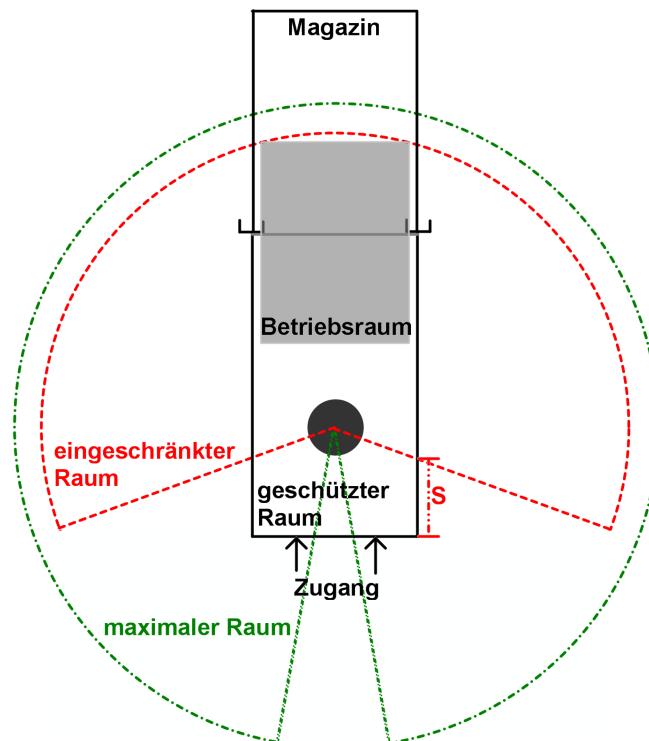


Abbildung 11: Räume des Roboters zur Ermittlung der risikomindernden Maßnahmen

### 3.4.3 Smartes Transfersystem

Bei dem Transfersystem gibt es eine erhebliche Anzahl von Gefährdungen, die schwierig zu bewerten waren. Zur besseren Einschätzung wurden weitere Informationen vom Hersteller der Transferbänder angefordert. Das Transfersystem besitzt keinen eigenen Not-Halt. Am Schaltschrank befindet sich nur ein Not-Aus-Schalter, welcher nicht ausreichend ist. An den Baugruppen zur Produktentnahme direkt am Transferband sind einrastende Not-Halt-Taster anzubringen. Stellt ein Handarbeitsplatz direkt am Transfersystem eine Montagemaschine dar, so ist dieser Bereich auch mit einem Not-Halt Einrichtung zu versehen.

### 3.4.4 Gravurmaschine

An der Montagemaschine mit einem Laser ist bereits abzusehen, dass eine vorhandene Schutzmaßnahme umgangen wird. So ist an der Laserkabine, in der das Werkstück graviert wird, bereits das angeschraubte Blickglas nur noch mit einer Schraube fixiert. Dies deutet darauf hin, dass die Schutzeinrichtung nicht für alle anfallenden Aufgaben geeignet ist. Zur Zeit ist der Eingriff in den Gefahrenbereich über den Weg der Material- und Produktzufuhr möglich. Die trennende Schutzeinrichtung (Gehäuse) ist entsprechend der Norm *ISO 13857* anzupassen. Bei der Konstruktion sollte eine geeignete Möglichkeit des Zugangs berücksichtigt werden. Die Laserkabine wird durch die Hubindexierung der Integrationsinfrastruktur geschlossen. Somit stellt diese Maschine keine vollständige im Sinne *MRL* dar. Dieser Zusammenhang ist konstruktiv zu beheben.

Das korrekte Schließen der Laserkabine ist in jedem Fall sicherzustellen, bevor der Shutter des Lasers sich öffnet. Dies wird zurzeit an dieser Maschine über einen sicheren induktiven Näherungsschalter an der Lasersteuerung ausgewertet. In der verbauten Gerätegeneration ist das Abschalten durch eine Signaländerung an einem Eingang der Steuerung nicht nach *DIN EN ISO 13849* oder *DIN EN 62061* zertifiziert. Der Laser ist nur durch die sichere Energiewegnahme sicher abzuschalten und in den gefahrenfreien Zustand zu bringen. Nach Rücksprache mit dem Hersteller schließt der Shutter des Lasers im Worst-Case-Fall innerhalb von 200 ms durch die interne Programmierung, auf die der Kunde kein Einfluss nehmen kann. Die neuere Gerätegeneration unterstützt das sichere Abschalten nach *SIL* und *PL*. Die Hubindexierung benötigt für den 100 mm Hub im Mittelwert eine Zeit von ca. 2 s, wobei der Bewegungsverlauf als linear angenommen wurde. Ausgehend von der in Gleichung (4) dargestellten Zeitkette ergibt sich mit Gleichung (5) eine Tiefe (s), die die Hubindexierung in die Laserkabine mindestens eindringen muss. Diese wird im Fehlerfall benötigt um den Shutter des Lasers zu schließen, bevor es zur Öffnung der Laserkabine

kommt. Zur Berechnung wurde der verbaute Schmersal Sicherheitsschalter *CCS 8-180-2P+D-E-LST* berücksichtigt. Durch das Zwei-Wege-Ventil der Hubindexierung bleibt bei einem Ausfall der Pneumatik (des Luftdrucks) die Hubindexierung an ihrer Hubposition stehen.

$$T = t_{Schalter} + t_{Sicherheitssteuerung} + t_{Laser} \quad (4)$$

$$T = 30 \text{ ms} + 50 \text{ ms} + 200 \text{ ms}$$

$$T = 280 \text{ ms}$$

$$s = v \cdot T + S_{ar} \quad (5)$$

$$s = \frac{100 \text{ mm}}{1,5 \text{ s}} \cdot 0,28 \text{ s} + 10 \text{ mm}$$

$$s = 28,67 \text{ mm}$$

## 4 Konzept

In dem in Kapitel 2.1.1 beschriebenen und bereits umgesetzten Anlagenkonzept ist ein Maschinenmodul unabhängig von den anderen automatisiert. Das bezieht sich auf deren Benutzung und auf die Koordination der Arbeitsschritte der jeweiligen Module. Es ergibt sich ein Gebilde von Steuerungen ohne Kommunikation untereinander. Zunächst wird ein mögliches normatives Konzept für die Zertifizierung von konfigurierbaren Systemen aufgezeigt. Anschließend sind allgemeine Lösungskonzepte der Sicherheitsfunktionen mit dem Stand der Technik beschreiben. Des Weiteren werden diese durch die spezifischen Lösungsansätze einiger etablierter Firmen konkretisiert und miteinander verglichen.

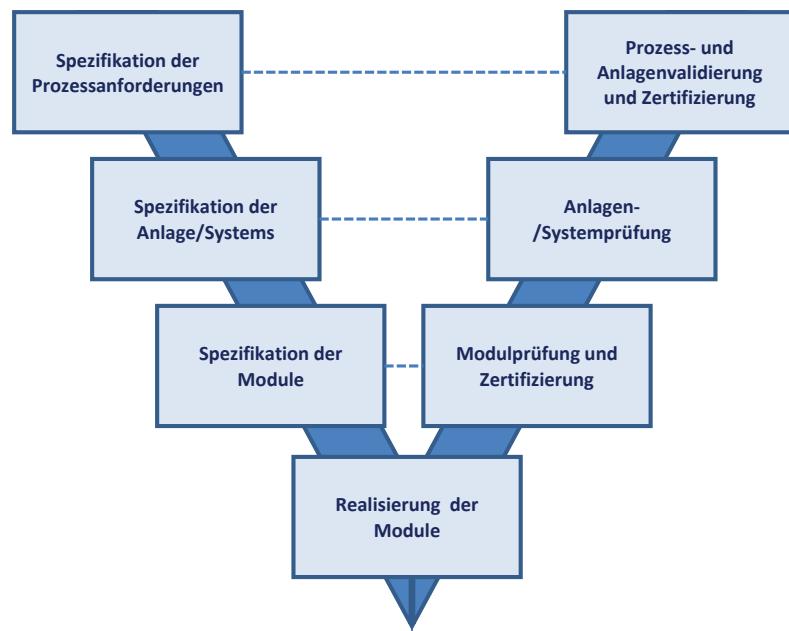
### 4.1 Normativer Lösungsansatz - Konzept: Modulare Zertifizierung

Das nachfolgende beschriebene Konzept der modularen Zertifizierung ist vom TÜV SÜD innerhalb der Mitgliedschaft im Verein *SmartFactory KL* entstanden und hier übernommen worden. Dieses Konzept wurde auf einem Positionspapier [8] veröffentlicht und stellt nicht eine Lösungsmöglichkeit der aktuellen Regelwerke dar. „Durch die Zertifizierung soll nachgewiesen werden, dass die Gesamtanlage den gesetzlichen Anforderungen entspricht. Die Vorgehensweise basiert auf einem V-Modell, das die Produktspezifikationen auf Prozess-, Anlagen-(System) und Modulebene sowie die Prüfspezifikation für die jeweilige Ebene festlegt. Durch die standardisierte Vorgehensweise wird folgendes erreicht:“ [8] Spezifikationsebene:

Die Anforderungen aus der Prozessschicht sind spezifiziert und werden auf die Anlagen- und Systemebene übertragen. Die Besonderheiten des Prozesses sind in der Anlagen-/Systemspezifikation enthalten und werden auf die Module übertragen. Daraus resultiert die Modulspezifikation mit den Anforderungen an den Prozess der Anlage. Ist ein Modul nach diesen Spezifikationen konstruiert worden, ist es funktionsfähig und sicher. Alle Schnittstellen sind so ausgelegt, dass dieses Modul mit weiteren Modulen in einer Verkettung arbeiten kann. Beim Entfernen eines Moduls bleibt die Anlage sicher. [8] Dieser Ansatz wurde bereits mit der gesonderten Risikobeurteilung der Schnittstellen mit dem Stand der Technik umgesetzt. (siehe Abschnitt 2.8 Seite 22).

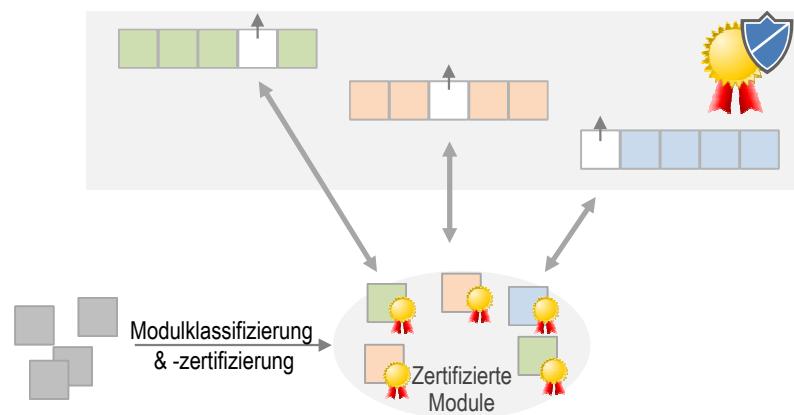
Weiteres Vorgehen bei der Verifizierung und Validierung ist direkt dem Interpretationspapier zu entnehmen. Das in Abbildung 12 dargestellte V-Modell beinhaltet 3 Schritte: Prozess, System und Modul. Dabei sind alle Schnittstellen und die Prüfungsgrundlage auf Basis der bestehenden Normen aus den angrenzenden Bereichen festzulegen. [8] Das Ziel von diesem Konzept ist es, die einzelnen Module zu klassifizieren und zu zertifizieren. Anschließend können Module mit der gleichen Klassifizierung zu einem dynamischen konfigurierbaren

System zusammengestellt werden. Dabei wird die digitale Infrastruktur genutzt, um das An- und Abmelden von Komponenten (Sensoren, Aktoren, modulare Maschinen) zu ermöglichen. Dies ist in Abbildung 13 angedeutet und wird beim Vergleich mit Abbildung 7 auf Seite 21 deutlich.



Quelle: [8]

Abbildung 12: V-Modell für eine intelligente Fertigungsanlage



Quelle: TÜV SÜD

Abbildung 13: Entstehung dynamisch konfigurierbarer Systeme durch Modulklassifizierung

## 4.2 Steuerungstechnischer Lösungsansatz der Sicherheitsfunktionen

Nach dem Heranstellen eines Maschinenmoduls an das smarte Transfersystem wird an dieser der *Integrationsprozess* ausgelöst. Ohne die bereits integrierten Maschinen anzuhalten wird ein sicherer Kommunikationskanal zu allen integrierten Maschinen aufgebaut. Dabei wird idealerweise keine übergeordnete Steuerung im smarten Transfersystem beansprucht. Ist das Integrieren erfolgreich beendet und sind alle Schutzeinrichtungen im ordnungsgemäßen Zustand, so kann das Montagemodul im integrierten Automatikmodus betrieben werden. Der entscheidende Punkt der anschließenden Lösungsansätze liegt im Aufbau eines sicheren Kommunikationskanals über ein zertifiziertes Ethernet-basiertes Protokoll zu jeder integrierten Maschine. Zur Erläuterung der Problematik dient das folgende Beispiel. Angenommen der Not-Halt-Befehl wird an alle Steuerungen über einen Broadcast weitergegeben, dann ist nicht sichergestellt, dass auch wirklich alle Teilnehmer diesen erhalten. Der Absender kann dies nicht überprüfen, da er keine Informationen darüber hat, wer *alle* sind. Das liegt in der Situation begründet, dass dieser keine gesicherten Informationen über die anderen Module hat. Im Umkehrschluss heißt das, eine Steuerung hat keine Erwartungshaltung, ob und von wem ein Not-Halt-Befehl zu erwarten ist. Alle nachfolgenden Lösungsansätze berücksichtigen folgende Punkte gemeinsam:

- Jede integrierbare Maschine ist eine vollständige sichere Maschine. Das impliziert eine eigene **CE-Kennzeichnung** und Sicherheitssteuerung zur Ausführung aller Sicherheitsfunktionen.
- Die Steuerungen sind am Markt verfügbar und können mit dezentraler I/O erweitert werden.
- Die Indexierungen und Stopper sind mit dem Transfersystem verschraubt und gehören auch zu diesem. Das RFID-Lesegerät ist über die Plug-and-Produce-Verbindung direkt auf die integrierte Maschine geführt.

### 4.2.1 Mit übergeordneter Steuerung

Der Aufbau eines sicheren Kommunikationskanals erfolgt mit einer übergeordneten Steuerung. In dieser werden alle Kombinationsmöglichkeiten von bekannten Modulen an dem smarten Transfersystem hinterlegt. Der Anlagenführer wählt den aktuellen Aufbau und gibt diesen der Steuerung bekannt, damit die richtige sicherheitsgerichtete Konfiguration aktiviert wird. Hierbei können Fehler auftreten, die geradezu menschlich sind. Daher muss der angegebene Aufbau noch sicherheitsgerichtet überprüft werden. Zum Beispiel durch Drücken eines Tasters an der zu integrierenden Maschine kann die sichere Kommunikation

zwischen Modul und der übergeordneter Steuerung sichergestellt werden. Zusätzlich kann mit Sensoren festgestellt werden, an welchen Integrationsplatz sich eine Maschine befindet. Zum Entfernen eines integrierten Moduls muss dieses Vorhaben der übergeordneten Steuerung bekannt gegeben und anschließend die neue Konfiguration geladen werden. Der Prozess ist so gestaltet, dass auf einen Stopp der gesamten Anlage verzichtet werden kann. Ist ein angestelltes Modul nicht integriert, so führt das zu einem Stopp des betreffenden Moduls und nach angemessener Zeit zu einem Halt der gesamten Anlage. Eine Überwachung der Integrationsplätze muss realisiert werden. Dabei ist zu berücksichtigen, dass die Module unabhängig von einander funktionieren und auch ohne das smarte Transferband sicher sein müssen. Eine Erweiterung der verfügbaren Module zieht bei diesem Lösungsansatz einen hohen Implementierungsaufwand mit sich. Die Zahl der möglichen Kombinationen steigt. Die Kombinationen müssen vor dem Einsatz des neuen Moduls in die Steuerung implementiert werden.

#### 4.2.2 Ohne übergeordnete Steuerung

Eine Erwartungshaltung ohne eine übergeordnete Steuerung aufzubauen, ist eine Herausforderung. Dazu muss ein sicheres Hand-Shake-Verfahren entwickelt werden, mit dem es bereits integrierten Modulen ermöglicht wird, einen sicherheitsgerichteten Kommunikationskanal zu eröffnen. Beim Integrieren der Maschine wird dieser Vorgang beispielsweise durch einen Schlüsselschalter ausgelöst. Die Schwierigkeit, ist sicherzustellen, dass eine Kommunikation zu allen integrierten Modulen aufgebaut wurde. Dazu müssen in der Steuerung der zu integrierenden Maschine die Punkt-zu-Punkt-Verbindungen zu allen Maschinen des Systems hinterlegt sein. Es muss sichergestellt werden, dass zu allen integrierten Maschinen eine Verbindung aufgebaut werden kann, damit die Verbindungen zu nicht erreichten Maschinen/nicht integrierten Maschinen zuverlässig deaktiviert werden können. Wird eine weitere Maschine integriert, ist die deaktivierte Verbindung wieder zu aktivieren. Bei der Realisierung dieser Vorgehensweise sind entsprechende Sicherungsmechanismen der Normen zu entnehmen, damit die benötigte Zertifizierung erreicht werden kann. Ein gesamter Anlagenstopp ist dabei unerwünscht. Um dies sicher im Sinne der Normen umzusetzen, muss ein Hersteller von Steuerungen gefunden werden, dessen Hardware und Sicherheitsprotokoll flexibel genug ist, um dieses Vorhaben zu implementieren und idealerweise keine Zertifizierung mehr benötigt.

#### 4.2.3 Einfach ohne Ethernet

Eine einfache Lösung ohne übergeordnete Steuerung wäre mit dem Verzicht auf eine Kommunikation über Ethernet möglich. Dabei wird ein sicherer Ausgang eines integrierten

Moduls, über den Plug-and-Produce-Stecker vom smarten Transfersystem auf einen sicheren Eingang des nächsten Moduls geführt. Von diesem Modul wird wieder ein sicherer Ausgang auf einen sicheren Eingang vom nächsten Modul geführt, usw. Dabei ist auf die galvanische Trennung zur Verbesserung der elektromagnetischen Verträglichkeit zu achten. Durch die Nutzung des einheitlichen Steckers zu allen Modulen spielt die Reihenfolge und Anzahl dieser keine Rolle. Es bildet sich eine Sicherheitsschleife, die im fehlerfreien Zustand nach dem Ruhestromprinzip geschlossen ist. Wird diese im Fehlerfall von einem Montagemodul unterbrochen, so werden auch die anderen Maschinen in einen sicheren Halt gebracht. Der Vorteil liegt in der Einfachheit und wohl möglichen kostengünstigen Umsetzung (Sicherheitsrelais würden genügen). Neben dem zusätzlichen Verdrahtungsaufwand gibt es noch weitere Nachteile. Zum einen ist die Übertragung von Statusinformationen an eine andere Steuerung beschränkt und zum anderen ist der Austausch weiterer Signale mit weiteren paralleler Verdrahtung verbunden. Des Weiteren hängt die Reaktionszeit von der Anzahl der integrierten Maschinen ab und es können unter Umständen lange Reaktionszeiten stehen. Ein Anlagenstopp beim Hinzufügen und Herausnehmen von Maschinen kann nicht verhindert werden. In Zeiten von maschinennaher Vernetzung ist dieser Lösungsansatz nicht mehr zeitgemäß.

#### 4.2.4 Der theoretische Lösungsansatz

Theoretisch wäre auch hier die Nutzung eines Mediums denkbar, welches die übergeordnete Steuerung ablöst. In diesem Anwendungsfall ist dies ein sicherheitsgerichteter RFID-Chip, den es zurzeit nicht auf dem Markt gibt. Dazu müsste der RFID-Chip zweimal durch die aktuelle Konfiguration der Anlage geführt werden. Bei der ersten Fahrt wird an jedem Steckplatz für ein Modul überprüft, ob und welches vorhanden ist. Die Eigenschaften der sicherheitsgerichteten Steuerung werden auf dem RFID-Chip sicherheitsgerichtet gespeichert, z.B. in Form einer [GSDML](#)-Datei. Nach Beendigung der ersten Fahrt ist die aktuelle Anlagenkonfiguration auf dem Chip gespeichert. Bei dem erneuten Transport durch die Anlage liest jedes Modul diese Informationen aus und lädt anhand dessen die entsprechende Konfiguration. Dieser Vorgang ist bei jeder Änderung der integrierten Module erneut durchzuführen, wozu ein Leerfahren und Stopp der Anlage notwendig ist. Ein weiterer Nachteil ist, dass in jedem Modul eine passende Konfiguration hinterlegt sein muss, die anhand der GSMDL-Dateien geladen wird. Des Weiteren wird dieser Lernprozess in großen und verzweigten Anlagen relativ lange dauern und schwierig umzusetzen sein. Als problematisch kann sich die Tatsache erweisen, dass ein Teil der Anlage bereits in Betrieb sein muss, um den Objektträger durch die Anlage zu befördern. Dies kann normativ durch geschultes Personal und bestimmte Betriebsarten gelöst werden.

Abschließend ist festzustellen, dass die sicherheitsgerichteten Systeme über ausreichende Intelligenz (sichere Sensoren) verfügen müssen, dass diese sich automatisch gegenseitig erkennen und eine sichere Kommunikation zu anderen Modulen aufbauen.

## 4.3 Der Vergleich spezifischer Lösungsansätze

### 4.3.1 Auswahl der Firmen

Im Folgenden werden die Vergleichskriterien und das Vorgehen der Marktanalyse erläutert. Mit einer Recherche in Katalogen, im Internet und auf Fachmessen wurden mit Hilfe eigener Erfahrungen im Schaltschrankbau folgende Firmen für diesen Vergleich herangezogen. Nachfolgend ein Überblick in alphabetischer Reihenfolge mit einer kurzen Begründung der Auswahl:

ABB hat mit dem modularen All-Master-System Pluto mit der Aussage Interesse geweckt, die Modularität des Montagesystems gut beibehalten zu können.

B&R konnte mit dem offenen Protokoll openSAFETY und einem Optionsmanagement in der übergeordneter Steuerung überzeugen.

Beckhoff hat auf der Hannover Messe eine passende Anwendung gezeigt und hat mit den zertifizierten Baustein zur Verbindungssteuerung eine gute Möglichkeit in Aussicht gestellt.

HIMA überzeugte mit safeethernet und vielfältigen Implementierungsmöglichkeiten der Kommunikationsschnittstelle.

Phoenix Contact ist ebenso wie das inIT im CIIT ansässig und bot mit den bereits verbauten SafetyBridge-Komponenten eine gute Voraussetzung.

SICK überzeugte mit der Aussage, mit FlexiLine die Wandlungsfähigkeit gut beibehalten zu können.

Siemens wurde als großer komplett und PROFINet/PROFIsafe Anbieter mit in den Vergleich genommen.

Vertreter der Firmen waren vor Ort, um sich ein Bild von dem wandlungsfähigen Montagesystem zu machen. Dabei wurden Aspekte der vorausgegangen Risikobeurteilung und das Konzept des wandlungsfähigen Montagesystems in Bezug auf Sicherheitsanwendungen diskutiert. Zum Abschluss wurden alle gebeten, den präsentierten Lösungsansatz kurz schriftlich zu fixieren. Aufgrund der nachfolgenden Vergleichskriterien wurden Rückfragen gestellt, um die Lösungsansätze vergleichbarer zu gestalten.

### 4.3.2 Vergleichskriterien

Die Vergleichskriterien gehen aus den Anforderungen hervor und werden nachfolgend zusammengefasst. Gefordert ist eine Kommunikation über das bereits vorhandene PROFInet. Das zugehörige Sicherheitsprotokoll ist PROFIsafe und setzt als Übertragungsmedium genauso auf die Ethernet-Technologie (IEEE 802.3). Damit können Produkte akzeptiert werden, die auf den Ethernet-Standard basieren und einen gleichzeitigen Betrieb von PROFInet zulassen. Zum Vergleich wurden andere vernetzte Technologien betrachtet, damit der Vergleich nicht zu spezifisch und auf die Beispielanwendung bezogen ist. In diesem Zusammenhang sind weitere Gesichtspunkte zu betrachten wie mögliche Topologien, maximale Entfernungen zwischen zwei Modulen, maximale Anzahl von Maschinen, die zeitgleich integriert werden können, die Worst-Case-Reaktionszeit und die Kompatibilität zu anderen Herstellern. Zum Schluss ist noch die Zertifizierung der Hardware, Implementierung und des Protokolls zu nennen.

Ein weiteres Kriterium ist, wie weit eines der idealen Konzepte voraussichtlich umzusetzen ist. Dabei wurde die mögliche Umsetzung in Absprache mit dem jeweiligen Unternehmen erarbeitet und kurz beschrieben. Vom besonderen Interesse war die Vorgehensweise, die erforderlich ist, um eine sichere Verbindung zu allen integrierten Modulen herzustellen. Auch der Gesichtspunkt des voraussichtlichen Aufwands der Implementierung der Funktionen ist zu betrachten. Dabei wurde die Vielfältigkeit der Implementierungsmöglichkeiten wie beispielsweise die Benutzung von Hochsprachen oder die Nutzung der [IEC 61131](#) berücksichtigt. Oder handelt es sich viel mehr um ein Konfigurieren? Durch den Einsatz von zertifizierten Bausteinen kann das Implementieren vereinfacht werden. Abschließend ist zu klären, ob eine zusätzliche Zertifizierung notwendig ist oder die vorgeschriebene Validierung genügt.

Die Leistungsfähigkeit und Wirtschaftlichkeit des möglichen Automatisierungssystems ist anhand folgender Beispielsituation zu vergleichen: Es ist von vier bestimmungsgemäß integrierten Modulen auszugehen, die sich im integrierten Automatikbetrieb befinden oder von drei Modulen und einer übergeordneten Steuerung im smarten Transfersystem. Dabei sind die Steuerungen der jeweiligen Maschinen in Linientopologie miteinander verbunden. Es ist von 50 m Leitungslänge zwischen den Maschinen auszugehen. Für Übertragungen über Ethernet sind Variablen für nicht bekannte Verzögerungen einzusetzen. Dies kann z.B. eine angenommene Watchdog-Zeit sein. Die Reaktionszeiten von Sensoren und Aktoren sind zu vernachlässigen. Mit diesem Aufbau ist die Worst-Case-Reaktionszeit von der Eingangsklemme in dem ersten Modul bis zur Ausgangsklemme in dem letzten Modul zu ermitteln. Die verwendeten Quellen wie z.B. Datenblätter sind nach Möglichkeit zu nennen.

## 4.4 Lösungsvorschlag ABB

Die Firma ABB hat mit der sicherheitsgerichteten Steuerung *Pluto* eine einfache Möglichkeit geschaffen, die Steuerungen zur Ausführung der Sicherheitsfunktionen dezentral zu verteilen. Das All-Masters-Konzept ermöglicht ein gutes Hinzufügen und Entfernen von Anlagenteilen. Mit dem Anschluss eines Identifier (ID-Fix) werden die *Pluto*-Steuerungen adressiert. In diesem ist eine 12 stellige Hex-Zahl hinterlegt, die den Bezug zur Hard- und Software herstellt. Es besteht die Möglichkeit, die Konfiguration auf den Identifier zu speichern. Jede *Pluto*-Steuerung kann mit weiteren Baugruppen an die Anforderungen der jeweiligen Maschine angepasst werden. Zum sicheren Datenaustausch mit anderen *Pluto*-Steuerungen wird der *Pluto-Bus* verwendet. Dieser basiert auf den CAN-Bus mit eigenem Sicherheitsprotokoll. Mit einer verdrillten Zweidrahtleitung können bis zu 32 *Pluto*-Steuerungen in Linientopologie sicher verbunden werden. Die Geschwindigkeit der Übertragung hängt von der Leitungslänge zwischen den einzelnen Steuerungen ab und liegt zwischen 100 kBit/s bei 600 m und 400 kBit/s bei 150 m Leitungslänge. Aufgrund des CAN-Bus ist auch keine galvanische Trennung gegeben, deshalb müssen Maßnahmen zur elektromagnetischen Verträglichkeit beachtet werden. Über Gateways können Statusinformationen mit verschiedenen anderen Feldbussen, unter anderem mit PROFINet, nicht sicher ausgetauscht werden. Das *Pluto* System erfüllt die Anforderungen des **safety integrity level (SIL) 3** oder vom **PL e**. Aus dem vorausgegangenen Text wird klar, dass die Anforderungen an Sicherheitsfunktionen nur dann erfüllt werden können, wenn in jeder Montagemaschine eine *Pluto*-Steuerung verbaut ist. Letztendlich entsteht eine Bindung zu diesem Produkt und dem Hersteller.

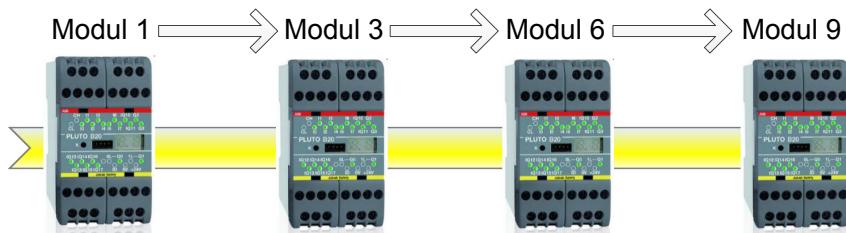


Abbildung 14: Mögliche Konfiguration; Module 2, 4, 5, 7 und 8 sind deaktiviert

### Aufbau der Kommunikation

Auf jeder *Pluto*-Steuerung ist das gleiche Programm abgelegt, das aufgrund der Programmierung Live-Bits von den anderen *Pluto*-Steuerungen erwartet. Mit Hilfe eines

Betriebsartenwahlschalters wird der jeweilige Aufbau den Steuerungen bekanntgegeben. Es muss für jede sinnvolle Zusammenstellung der Module eine Schalterstellung geben. Anhand dessen werden die fehlenden Live-Bits der nicht integrierten Module überbrückt. Der Betriebsartenwahlschalter kann nicht über ein **Human Machine Interface (HMI)**-Panel ersetzt werden, da dieses keine sicherheitsgerichtete Kommunikation zulässt. Die Pluto-Steuerung mit dem Betriebsartenwahlschalter muss immer vorhanden sein. Zusätzlich können Sicherheitssensoren an jedem Modul und an den Integrationsplätzen montiert werden. So ist ein Vergleich zwischen der ausgewählten und der tatsächlichen Konfiguration möglich.

### Implementierung

Über die Programmierumgebung *Pluto Manager* können die mit dem Bus verbundenen Pluto-Steuerungen programmiert werden. Dabei kann das Programm in Kontaktplan-Format oder in boolescher Algebra erstellt werden. Zur Verfügung stehen Zeitglieder, Merker, Register, Ablaufprogrammierung und vom TÜV-zugelassene Funktionsblöcke. So ist auch bereits ein Funktionsbaustein zur Auswertung von acht verschiedenen Betriebsarten vorhanden. Der Implementierungsaufwand für eine globale Not-Halt-Funktion ist verhältnismäßig gering. Der Aufwand steigt mit der Anzahl der Montageeinheiten, da eine Betriebsart eine mögliche Kombination der Montageeinheiten darstellt.

### Anwendungsbeispiel

Im Folgenden wird die Worst-Case-Reaktionzeit ermittelt, die für das Beispielszenario benötigt wird.

$T_{Ü}$ : Übertragungszeit bei benötigter Leitungslänge und Datenmenge  
 $\text{Anz.d.Stationen} \cdot \text{zusätzlicheAnsprechzeit}$

$T_L$ : Angenommene Logikausführungszeit

$T_{DI}$ : Verarbeitungszeit eines digitalen Eingangs; mit Filter

$T_{DO}$ : Verarbeitungszeit eines Relaisausgangs

$$T_t = T_{DI} + T_{Ü} + T_L + T_{DO} \quad (6)$$

$$T_t = 5 \text{ ms} + 4 \cdot 10 \text{ ms} + 10 \text{ ms} + 33 \text{ ms}$$

$$T_t = 88 \text{ ms}$$

### Preisliche Gestaltung

Die in der Tabelle 3 aufgeführten Komponenten werden für den Aufbau des Anwendungsbeispiels benötigt. Es sind die Listenpreise angegeben. Ein Gateway zur Übertragung von Statusinformationen in die PROFINet-Umgebung wurde berücksichtigt.

Tabelle 3: Listenpreise der Komponenten von ABB

Pos	Bezeichnung	Anzahl	Einzelpreis	Gesamtpreis
1	Typ: PLUTO B20 V2 Sicherheits-SPS mit 8 fehlersicheren Eingängen, 8 nichtfehlersicheren Ausgängen/fehlersicheren Eingängen, 2 einzeln fehlersicheren Relaisausgängen, 2 einzeln fehlersicheren Halbleiterausgängen; ohne Stromüberwachung. Für den Einsatz mit PLUTO Sicherheitsbus.	4 Stk	911,00 €	3.644,00 €
2	Potokollumsetzer für die bidirektionale Datenübertragung zwischen PLUTO Sicherheitsbus und Ethernet. Kommunikation für Ethernet/IP, PROFINet, Modbus TCP.	1 Stk	566,00 €	566,00 €
3	Identifier: ordnet Pluto eine Adresse zu. Diese Version ist beschreibbar	4 Stk	18,80 €	75,20 €
4	Programmierkabel USB für PLUTO. Zum Laden von SPS-Programmen und zur Überwachung	1 Stk	53,00 €	53,00 €
Gesamt				4.338,20 €

### 4.5 Lösungsvorschlag B&R

Die Firma B&R verfolgt zur sicheren Vernetzung einen offenen Ansatz und benutzt dazu eine Sicherheitslösung, die auf das openSAFETY-Protokoll aufbaut. OpenSAFETY ist unabhängig vom Transportlayer, da dies nur auf dem Applikationslayer arbeitet. Somit kann das Protokoll theoretisch über jeden Feldbus übertragen werden. B&R setzt bei der Umsetzung von openSAFETY auf Powerlink und Modbus. Um ein System mit openSAFETY und B&R-Komponenten in einer PROFINet-Umgebung zu realisieren, ist der Einsatz einer übergeordneten B&R Steuerung (SPS/X20CPU) notwendig. Die Steuerung wird mit einem Modbus Koppler und einem PROFINet Slave erweitert. Zur Ausführung des sicherheitsge-

richteten Optionsmanagement muss zusätzlich eine übergeordnete B&R-Sicherheits-CPU über Powerlink angeschlossen werden. Eine ähnliche Hardwarekonstellation ist in jedem Montagemodul zu verbauen. Statt einer kompletten Sicherheits-CPU genügt die Ergänzung mit einem intelligenten programmierbaren Modul, welches openSAFETY unterstützt. Die nachfolgende Abbildung 15 stellt den Aufbau der Topologie dar. Zur Kommunikation mit anderen Maschinenmodulen wird die nicht sichere B&R Steuerung über einen Switch mit PROFINet verbunden. Zusätzlich wird mit der zweiten Kommunikationsschnittstelle der Steuerung der Modbus aufgebaut. Bedingt dadurch, dass nicht alle verbauten Sicherheitskomponenten das openSAFETY Protokoll unterstützen, wird eine UDP-Verbindung aufgebaut, die den gemeinsamen Nenner zwischen PROFINet und Modbus darstellt. Über diese wird in weiterer Folge die sicherheitsgerichtete Kommunikation über das Black-Channel-Prinzips realisiert. Eine direkte Nutzung über PROFINet ist mit B&R nicht möglich. Diese Kommunikation kann auch über das Ethernet/IP Protokoll (unterstützt bei der Fa. Rockwell) realisiert werden. Die nicht sichere Kommunikation erfolgt über das vorhandene PROFINet. Die Verwendung von offenen Standards ermöglicht den Einsatz verschiedener Hersteller und ist herstellerunabhängig. Der Markt mit Herstellern, die diesen Standard unterstützen, ist überwiegend in Asien zu finden.

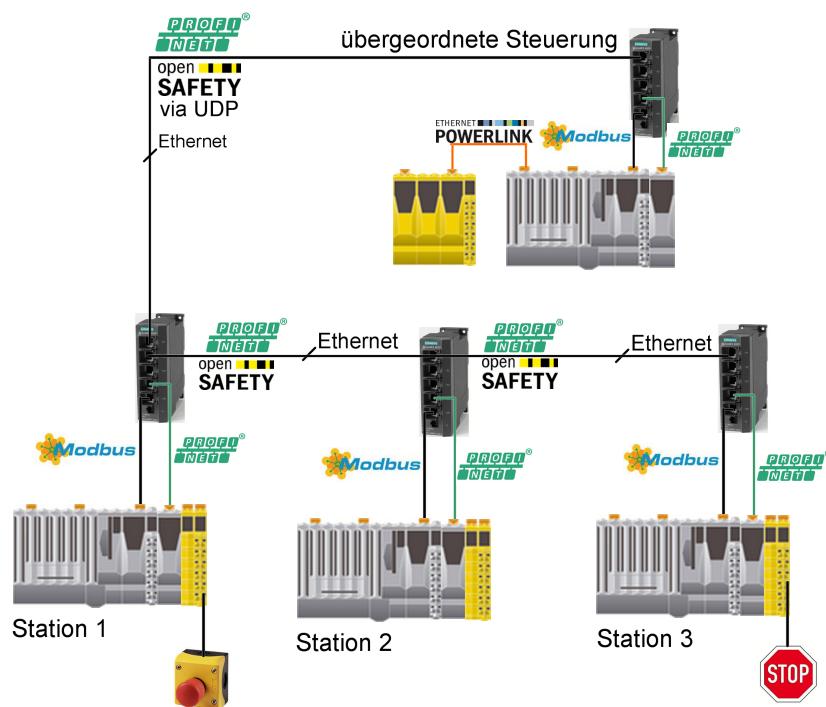


Abbildung 15: Aufbau mit Powerlink, openSAFETY und Komponenten von B&R

Die B&R-Sicherheits-CPU ist für den **SIL 3** und **PL e** zertifiziert. Die Kommunikation über openSAFETY ist vom TÜV-SÜD und TÜV-Rheinland **SIL 3** zertifiziert.

### Aufbau der Kommunikation

Das smarte Transfersystem ist mit der übergeordneten Steuerung und dem zugehörigen sicheren Optionsmanagement zu erweitern. Mit Hilfe dieses Optionsmanagement kann openSAFETY Hot-plug-fähigkeit erlangen. Über eine zu erstellende Bedienoberfläche am **HMI**-Panel wird die aktuelle Konfiguration der angeschlossenen Maschinenmodule vom Bedienungspersonal ausgewählt. Anhand dieser Auswahl werden im Optionsmanagement die entsprechenden Optionen angewählt und die jeweiligen Steuerungen in den Montagemodulen de- oder aktiviert. Um zu verhindern, dass ein nicht ordnungsgemäß integriertes Modul in Betrieb gehen kann, können folgende Maßnahmen realisiert werden:

- Über einen Schlüsselschalter (**HMI**-Panel mit Zugangssperre) wird das Modul auf *Verbund* gestellt und über die übergeordnete Steuerung zusätzlich freigegeben, oder
- mit einem Taster wird die korrekte Konfiguration getestet und nach erfolgreichem Abschluss der Betrieb zugelassen, oder
- das Montagemodul erkennt, dass dies integriert wurde und wartet auf die Freigabe aus dem Optionsmanagement.

Alle Ansätze verfolgen das gleiche Ziel. Es muss eine Möglichkeit gefunden werden, die sicherstellt, dass nur ein korrekt integriertes Modul in den Betrieb gehen kann. Dafür muss die sichere Kommunikation zu der übergeordneten Steuerung und zu allen integrierten Steuerungen vorhanden sein. Bei der Umsetzung müssen entsprechende Parameter gefunden werden.

### Implementierung

Mit voraussichtlich viel Implementierungsaufwand können die notwendigen Funktionen umgesetzt werden, die von qualifizierten Bedienungspersonal sicher zu handhaben sind. Die Implementierung erfolgt mit der Programmierumgebung Automation Studio und dem SafeDESIGNER von B&R. Im SafeDESIGNER sind neben den Funktionsbausteinen nach **IEC 61131** auch bereits vom TÜV zertifizierte Funktionsbausteine enthalten. Bei der freien Programmierung nach **IEC 61131** muss der Programmcode ggf. zertifiziert werden. Eine Validierung hingegen ist auf jeden Fall durchzuführen und entsprechend zu dokumentieren.

### Anwendungsbeispiel

Der *openSAFETY Configuration Manager*, der im B&R System auf der SafeLogic arbeitet, errechnet anhand der konfigurierten Komponenten und der verwendeten Topologien automatisch die Worst-Case-Reaktionszeit. Diese Zeit hängt von vielen Faktoren und noch unbekannten Größen ab. Die Firma B&R nennt für diese Beispielkonfiguration eine realistische Reaktionszeit von 66,7 ms. Dieser Wert ist abhängig von der Netzwerkstruktur.

### Preisliche Gestaltung

Die in Tabelle 4 aufgelisteten Komponenten werden für die Lösung in Abbildung 15 benötigt. Die verbauten intelligenten programmierbaren Module stehen auch im Einzelbetrieb für eine begrenzte Anzahl an sicherheitsgerichteten Aufgaben zur Verfügung. Diese sind für die erforderliche Anwendung ausreichend, um die jeweiligen sicherheitsrelevanten Funktionen einer Montagemaschine auszuführen.

## 4.6 Lösungsvorschlag Beckhoff

Mit der Markteinführung der PC-basierten Steuerungstechnik hat Beckhoff im Jahr 1986 einen weltweiten Standard für die Automatisierung geschaffen. Softwareseitig ist die Automatisierungssuite TwinCAT das Herzstück der Steuerungen von Beckhoff. Mit TwinSAFE wurde eine Sicherheitslösung in die PC-basierte Beckhoff-Steuerung integriert. Zur Standardkommunikation wird das EtherCAT-Protokoll verwendet. Zur sicheren Kommunikation kommt TwinSAFE/[FailSafe over EtherCAT \(FSOE\)](#) zum Einsatz. Dieses Protokoll ist vom TÜV für Anwendungen bis [SIL 3](#) zertifiziert. Durch Funktionen wie Hot-Connect, Connection-shutdown oder das [EtherCAT Automation Protocol \(EAP\)](#) können flexible Topologien realisiert werden. Durch die Offenheit des EtherCAT-Protokolls ist es möglich, viele verschiedene Bussysteme zu integrieren. Den EtherCAT-Bus parallel zu einem anderen Ethernet-basierten Feldbus z.B. PROFInet zu betreiben, ist nicht ohne weiteres möglich, da der EtherCAT-Bus spezielle Teilnehmer erfordert. Für das Anwendungsbeispiel stehen drei Möglichkeiten zu Verfügung:

- Zusätzlich zu dem vorhandenen Ethernet-Netzwerk kann der EtherCAT-Bus installiert werden. Es ist der Einsatz einer übergeordneten Steuerung notwendig und in den Modulen müssen Steuerungen verbaut sein, die einen Slave/Master-Betrieb ermöglichen. Zusätzlich muss es möglich sein, diese als Hot-Connect-Teilnehmer zu konfigurieren. Die Linientopologie ist mit Hilfe eines Sternverteiler zu vermeiden, da sonst nachfolgende EtherCAT-Teilnehmer (Maschinenmodule) nicht mehr zu Verfügung stehen.

Tabelle 4: Listenpreise der Komponenten von B&amp;R

Pos	Bezeichnung	Anzahl	Einzelpreis	Gesamtpreis
1	5CFCRD.0512-06 CompactFlash 512 MByte B&R (SLC)	4 Stk	29,00 €	116,00 €
2	X20BC0087 X20 Bus Controller, Modbus Schnittstelle, 2-fach Switch	4 Stk	83,00 €	332,00 €
3	X20BM33 Busmodul für X20 Safe IO-Module, interne I/O Versorgung durchverbunden	7 Stk	14,00 €	98,00 €
4	X20CP3584 X20 Zentraleinheit, ATOM 0,6 GHz, 256 MByte DDR2 RAM, 1 MByte SRAM, tauschbarer Anwenderspeicher: CompactFlash, 3 Einschubsteckplätze	4 Stk	950,00 €	3.800,00 €
5	X20IF10E1-1 X20 Schnittstellenmodul für DTM-Konfiguration, PROFINet RT Controller (Master)	4 Stk	360,00 €	1.440,00 €
6	X20MK0203 X20 SafeKEY, 8 MByte, für X20SL80xx Serie	1 Stk	48,00 €	48,00 €
7	X20SL8001 X20 SafeLOGIC, für bis zu 100 Safety Nodes, 32 Maschinenoptionen, POWERLINK safety Gateway, tauschbarer Anwenderspeicher: Memory Key, 2-fach Hub	1 Stk	605,00 €	605,00 €
8	X20SLX410 X20 Sicher digitales Eingangsmodul, sichere Steuerung, 11 Safety Nodes, 4 fehlersichere Eingänge, 4 Pulsausgänge	3 Stk	235,00 €	705,00 €
9	X20SO4110 X20 Sicher digitales Ausgangsmodul, 4 fehlersichere Halbleiterausgänge, mit Stromüberwachung, 24 VDC, 0,5 A	3 Stk	185,00 €	555,00 €
10	X20TB52 X20 Feldklemme, 12-polig, Safety Gesamt	6 Stk	4,00 €	24,00 €
				7.723,00 €

- In jeder Maschine und dem smarten Transfersystem wird eine Steuerung (CX8090) als Master installiert. Über Ethernet können diese mit Hilfe des **EAP** vernetzt werden.
- In jeder Maschine und dem smarten Transfersystem wird eine Steuerung mit einem geswitchten PROFInet-Port (CX8093) als Master installiert. Über PROFInet RT können diese mit Hilfe des **EAP** vernetzt werden. Es ergibt sich der in Abbildung 16 gezeigte Aufbau.

Die Steuerungen werden mit Hilfe von TwinSAFE-EtherCAT-Klemmen an die Anforderungen der Sicherheitsfunktionen angepasst. Für das Anwendungsbeispiel sind das: TwinSAFE-PLC (EL6900), 4-Kanal-Digital-Eingangsklemme (EL1904), 4-Kanal-Digital-Ausgangsklemme (EL2904). Mit einer zusätzlichen Klemme kann ein sicheres Gateway zu PROFIsafe geschaffen werden. **FSOE** arbeitet auf der Anwendungsschicht von EtherCAT und funktioniert nach dem Black-Channel-Prinzip. Das heißt, kann eine EtherCAT-Kommunikation aufgebaut werden, so steht auch der sichere Kommunikationskanal zur Verfügung. Bei Punkt 2 und 3 gibt es keine hierarchisch übergeordnete Steuerung. In den folgenden Abschnitten zeigt sich, dass es notwendig ist, die Steuerung vom smarten Transfersystem mit übergeordneten Funktionen auszustatten. Da eine Realisierung vom ersten Punkt in dem bereits vorhanden System zu aufwändig ist, werden im folgenden nur noch Punkt 2 und 3 betrachtet.

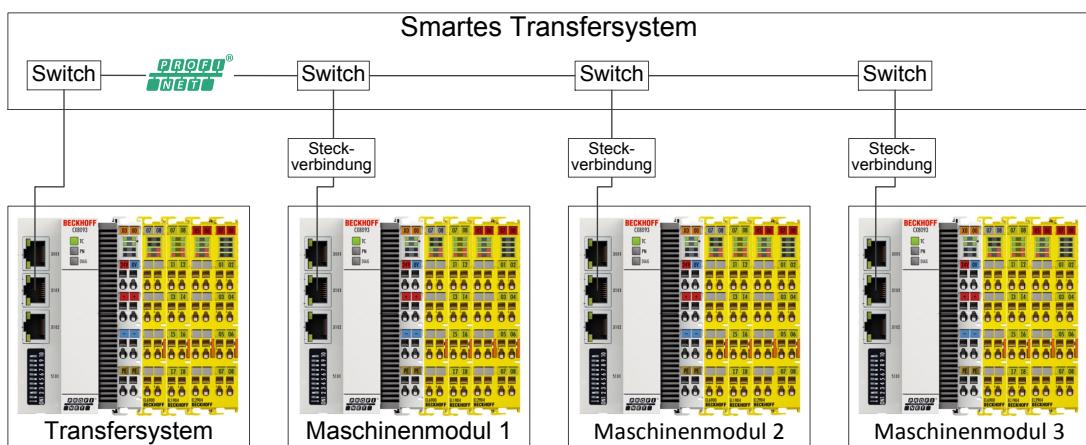


Abbildung 16: Möglicher Aufbau mit jeweils einem EtherCAT-Master in jedem Modul und einer Vernetzung über PROFInet

## Aufbau der Kommunikation

Mit Hilfe des **EAP** können sicherheitsgerichtete Daten zwischen zwei Steuerungen/EtherCAT-Master ausgetauscht werden. Die Funktion Hot-Connect steht dabei nicht zur Verfügung. Die sichere Verbindung zum Austausch von Daten der funktionalen Sicherheit entsteht zwischen zwei TwinSAFE-PLCs (**FSOE**-Master). Bevor ein EtherCAT-Master außer Betrieb genommen werden kann, muss dieser durch eine bewusste Handlung beendet werden. Damit kann ein Stopp der gesamten Anlage vermieden werden. Wird die Maschine wieder integriert, muss die Verbindung wieder von der Steuerung, die zuvor diese beendet hat, wieder aktiviert werden. Dies erfordert einen **FSOE**-Master, mit dem die jeweiligen Verbindungen zu den anderen **FSOE**-Master de- oder aktiviert werden können. Mittels Schlüsselschalter oder über ein **HMI**-Panel kann dies durch den Maschinenbediener ausgelöst werden. Kann eine aktivierte Verbindung nicht aufgebaut werden, so hat das einen Stopp der gesamten Anlage zur Folge. Mit sicheren Sensoren an den Integrationsplätzen kann die Anzahl der integrierten Maschinen erfasst und mit der Anzahl der aktivierten Verbindungen verglichen werden. Widersprechen sich diese Angaben für eine gewisse Zeit, erfolgt ein Stopp der gesamten Anlage.

## Implementierung

Die Implementierung erfolgt über TwinCAT. Für die Programmierung der Sicherheitsfunktionen wird keine zusätzliche Software benötigt. Dabei stehen derzeit nur zertifizierte Funktionsbausteine zur Verfügung. Dies hat den Vorteil, dass die Implementierung später nicht zertifiziert werden muss. Es ist nach **DIN EN ISO 13849-2** eine Validierung und eine **Fehlermöglichkeits- und -einflussanalyse (FMEA)** vorzunehmen. Für den Verbindungsau- und abbau gibt es den Funktionsbaustein *Connection Shutdown*. Einen vernetzten globalen Not-Halt zu implementieren, ist mit überschaubaren Aufwand zu erledigen. Das System mit derzeit noch unbekannten Maschinenmodulen zu erweitern, erfordert keinen hohen zeitlichen Aufwand. Es muss jeweils eine neue Verbindung zu den neuen **FSOE**-Master hinzugefügt werden.

## Anwendungsbeispiel

Die Worst-Case-Reaktionszeit hängt mit der Verfügbarkeit des Systems zusammen. Die wichtigste Zeit ist der Watchdog. Dieser hängt mit der Auslastung des Netzwerks zusammen und ist zu ermitteln. Dabei ist auf die Verfügbarkeit des Systems zu achten. Möglicherweise ist hier die Vernetzung der EtherCAT-Master über PROFINet RT vom Vorteil, da Ethernet nicht echtzeitfähig ist.

### Preisliche Gestaltung

Die in Tabelle 5 aufgelisteten Komponenten werden für die Lösung in Abbildung 16 benötigt. Dabei können alle Sicherheitsfunktionen des jeweiligen Maschinenmoduls erfüllt werden. Für die übergeordnete Steuerung im smarten Transfersystem werden möglicherweise weitere Eingänge benötigt. Die Software TwinCAT muss nur einmalig angeschafft werden und ist auch als 30-tägige Testversion kostenlos mit vollem Funktionsumfang erhältlich.

Tabelle 5: Listenpreise der Komponenten von Beckhoff

Pos	Bezeichnung	Anzahl	Einzelpreis	Gesamtpreis
1	CX8093 Embedded-PC Hutschienen-Industrie-PC; 32 Bit, 400 MHz CPU (TC3:20); 256 MB MicroSD Flash-Speicher; 64 MB interner Arbeitsspeicher; Protokoll: PROFINet-RT-Device; [...]	4 Stk	325,00 €	1.300,00 €
2	EL6900 EtherCAT-Klemme TwinSAFE-PLC	4 Stk	138,00 €	552,00 €
3	EL1904 EtherCAT-Klemme 4-Kanal-Digital-Eingangsklemme, TwinSAFE, 24 V DC	4 Stk	149,00 €	596,00 €
4	EL2904 EtherCAT-Klemme 4-Kanal-Digital-Ausgangsklemme, TwinSAFE, 24 V DC, 0,5 A	4 Stk	169,00 €	676,00 €
5	TwinCAT 2 Gesamt	1 Stk	1073,17 €	1073,17 €
				4.197,17 €

### 4.7 Lösungsvorschlag HIMA

Die Firma HIMA Paul Hildebrandt GmbH hat bereits 1997 zur sicheren Vernetzung ein eigenes safeethernet-Protokoll entwickelt. Dies basiert auf der Standard-Ethernet-Technologie (IEEE 802.3) und lässt die gleichzeitige Kommunikation von sicheren und nicht sicheren Daten zu. Jede Maschine muss über eine HIMA-Steuerung (HIMatrix F30) verfügen, damit diese über das vorhandene Ethernet-Netzwerk mit dem safeethernet-Protokoll kommunizieren kann. Dabei spielt es keine Rolle, aus welchen Komponenten die vorhandene Ethernet-Infrastruktur besteht. Aufgrund des eigenen (nicht standardisierten) Sicherheitsprotokolls besteht bei der Auswahl der Steuerung eine Herstellerabhängigkeit. Zusätzlich können verschiedene Ethernet basierte Feldbus-Protokolle in der Steuerung aktiviert werden, z. B. PROFINet Version 2.2 und PROFIsafe Version 2.5c. Mit safeethernet kann neben Stern- Linien- und Baumtopologien auch eine Ringtopologie erstellt werden, um so die Verfügbarkeit zu erhöhen. Mit Redundanz kann die Verfügbarkeit des safeethernet Systems

weiter gesteigert werden. Die HIMatrix F30 erfüllt den **SIL 3** oder **PL e**. Die Kommunikation über safeethernet ist **SIL 3** zertifiziert. „Die Gewährleistung der erforderlichen Reaktionszeit ermöglicht flexible Systemstrukturen für eine dezentrale Automatisierung.“ [20]

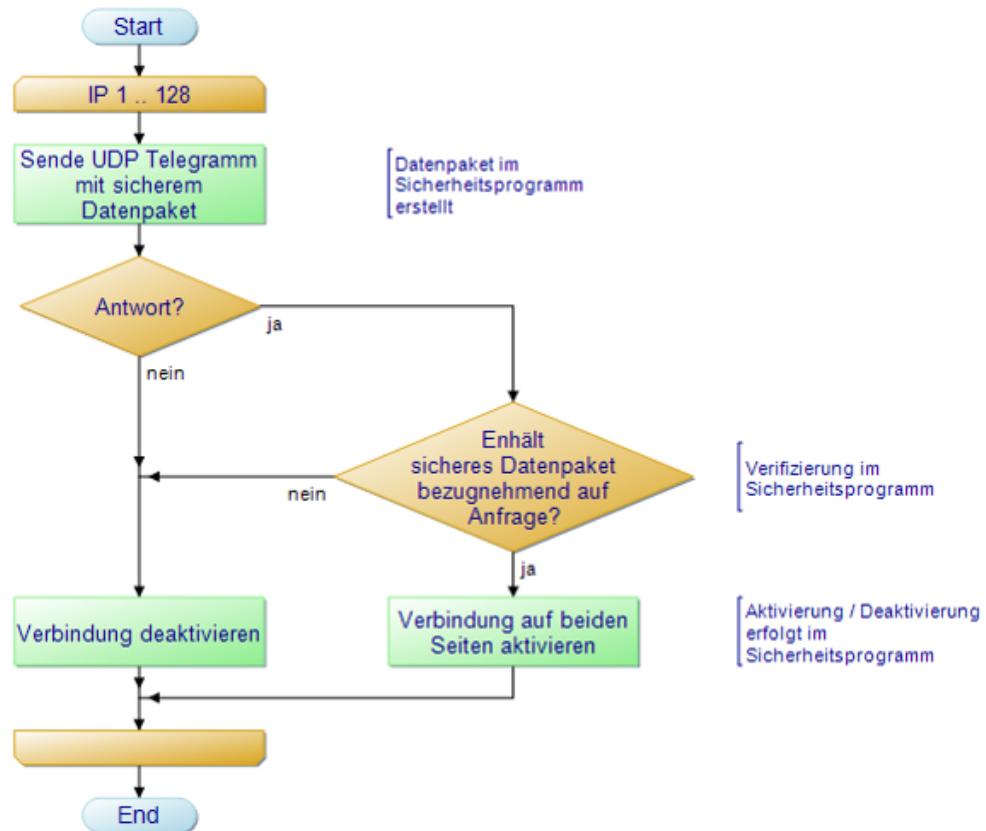
### Aufbau der Kommunikation

Bei HIMA-Steuerungen ist neben der Programmierung des sicherheitsgerichteten Prozessorsystems eine zusätzliche Programmierung des Kommunikationssystems (COM) möglich. Das COM bietet eine freie Programmierung seiner Callback Funktionen und eine individuelle Bedienung der Feldbus- und Ethernet-Schnittstellen an. Die Callback Funktionen sind nicht sicherheitsgerichtet und rückwirkungsfrei zum sicheren Anwenderprogramm. Sie können jedoch zum Erstellen einer Sicherheitsfunktion/-kommunikation mittels Black-Channel-Prinzip (alle möglichen Fehler der Kommunikationsstrecke können aus dem Anwenderprogramm heraus detektiert werden) über das sichere Anwenderprogramm angewendet werden.

Nach dem Integrieren eines Moduls mit einer Steuerung von HIMA wird über einen Taster (Schlüsselschalter) eine Initialisierungsaufforderung ausgelöst und der selbstständige Kommunikationsaufbau erfolgt. Dies kann in Absprache mit HIMA wie folgt ablaufen:

- Es wird ein beliebiger IP-Adressbereich für die Maschinenmodule in der Programmierumgebung vorgesehen und als Proxy Ressource (einfaches **SPS Template**) abgebildet.
- Beim Steuerungsanlauf sind zunächst alle safeethernet-Verbindungen aktiviert.
- Die Initialisierungsaufforderung löst die Anfrage des definierten IP-Bereichs über die Callback-Funktion des COM aus.
- Beim Erkennen der IP-Adresse wird über ein sicheres Handshake-Verfahren (gesicherte Daten, CRC-Prüfsumme) aus dem Sicherheitsprogramm die Identifizierung der Station eingeleitet. Ist der Teilnehmer keine Steuerung eines Moduls, so wird die Verbindung deaktiviert oder andernfalls in beiden Steuerungen aktiviert. Der Verbindungszustand wird über Lampen oder an einem **HMI**-Panel angezeigt und durch den Einrichter quittiert.
- Dabei gibt es keine zentrale Verwaltung. Die Intelligenz wird dezentral auf jede Station abgelegt. Somit hat jede Steuerung das gleiche Programm zum Aufbau der Punkt-zu-Punkt-Verbindungen. Durch die CRC-Prüfsumme des Programms bzw. des entstandenen Bausteins wird der Zertifizierungsaufwand beim Adaptieren neuer Stationen reduziert.

Dieses Vorgehen ist von HIMA erstellt und in Abbildung 17 veranschaulicht worden. Es stellt ein ungefähres Grundgerüst dar, welches mit genauen Randbedienungen zu spezifizieren ist. Als weiterer Schritt wurde bereits angedeutet, dass auch über das Kommunikationssystem ein kontrolliertes Deaktivieren realisiert werden kann. Das Entfernen eines Montagemoduls ist dann ohne einen Stopp weiterer Montagemodule möglich.



Quelle: HIMA

Abbildung 17: Ablaufdiagramm zur Herstellung der dynamischen Verbindungen

## Implementierung

Die Implementierung erfolgt über die Programmierumgebung SILworX von HIMA. Dabei können Funktionsbausteine und die Ablaufsprache der *IEC 61131-3* verwendet werden. Unterstützt werden dabei alle Funktionen und Variablen-Typen. Die Programmierung des Kommunikationssystems erfolgt in C. Eine zusätzliche Bibliothek mit zertifizierten Funktionen erleichtert die Arbeit. Für den Aufbau der sicheren Kommunikation ist mit

Hilfe einer [FMEA](#) ein Kommunikationsbaustein auf dem COM zu implementieren. Je nach ermittelten Sicherheitsanforderungen müssen geeignete Sicherungsverfahren gefunden und implementiert werden. Dabei kann sich an der Norm [EN 61784-3](#) orientiert werden. Dieses Vorgehen kann sich als aufwändig erweisen, da ggf. über eine Zertifizierung die Sicherheitsparameter, wie der [Probability of Dangerous Failure per Hour \(PFH<sub>D</sub>\)](#) Wert, nachgewiesen werden müssen. Bei der Implementierung dieses Bausteins ist das Vorgehen den entsprechenden Normen z.B. [ISO 61508](#) zu entnehmen. Die einzelnen Sicherheitsfunktionen des jeweiligen Montagemoduls lassen sich voraussichtlich mit geringem Aufwand umsetzen, nachdem die sichere Kommunikation aufgebaut ist.

### Anwendungsbeispiel

Die Bestimmung der Worst-Case-Reaktionszeit für die Beispielanwendung hängt von vielen Faktoren ab. Deshalb wird nur das Vorgehen zur Bestimmung erläutert. Ein wichtiger Bestandteil ist die Verzögerung (Delay) des Ethernet-Netzwerks. Diese muss unter sinnvoller Auslastung gemessen oder berechnet werden. Hinzu kommt die Bestimmung der Zykluszeit der Steuerung, die unter voller Last am Control-Panel abgelesen werden kann. Mit  $4 \cdot Delay + 5 \cdot max.Zykluszeit$  berechnet sich eine Überwachungszeit (ReceiveTMO). In dieser Zeit wird eine korrekte Antwort vom Kommunikationspartner erwartet. Andernfalls wird das System in den hinterlegten sicheren Zustand versetzt. Diese Überwachungszeit ist für die Stecke zwischen zwei HIMatrix-Steuerungen als Verzögerungszeit anzunehmen. Hinzu addiert sich noch die Sicherheitszeit der jeweiligen HIMatrix-Steuerungen ( $2 \cdot Watchdogzeit$ ). Dieses Vorgehen ist in Abbildung 18 veranschaulicht.

Die aus der Risikobeurteilung ermittelte Worst-Case-Reaktionszeit (TR) wird in der Steuerung eingestellt und dessen Überwachung erfolgt über die interne Watchdogzeit. Je nach [SPS](#)-Zykluszeit und eingestellter Watchdogzeit ergibt sich ein verfügbares System. Kann das System die eingestellte Reaktionszeit nicht erreichen, so ist es nicht verfügbar. Stellt sich dieser Zustand heraus, so kann alternativ wie folgt vorgegangen werden. Jede Montagemaschine hat eine eigene benötigte Sicherheitszeit. Die höchste wird zur Vereinfachung für alle anderen Module angenommen. Die verbleibende Zeit zur gesamten Reaktionszeit stellt die Anforderung an die Reaktionszeit für die Kommunikation (ReceiveTMO). Diese hängt von der maximalen Anzahl zulässiger SPSen (definierter IP-Adressbereich) ab. Mit der Größe dieses Bereichs steigt auch die Reaktionszeit der Kommunikation (ReceiveTMO). Übertragen auf das wandlungsfähige Montagesystem heißt das, beim Integrieren von neuen noch nicht berücksichtigten Montagemodulen ist auf die Leistungsfähigkeit des Ethernet-Netzwerks zu achten. Stellt ein bisher nicht berücksichtigtes Montagemodul wesentlich höhere Sicherheitsanforderung, so muss ggf. das gesamte System überprüft und angepasst werden.

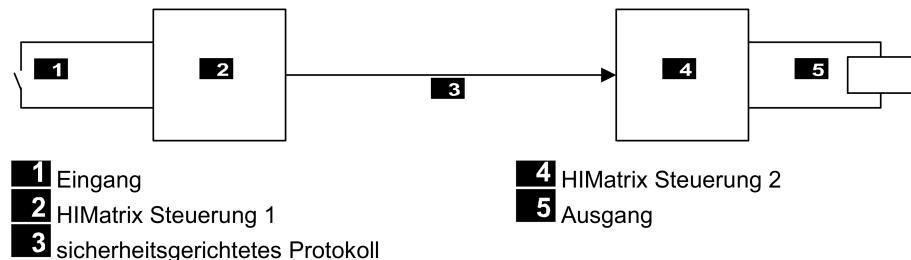


Bild 13: Reaktionszeit bei Verbindung zweier HiMatrix Steuerungen

$$TR = t_1 + t_2 + t_3$$

TR Worst Case Reaction Time

t<sub>1</sub> 2 \* Watchdog-Zeit der HiMatrix-Steuerung 1

t<sub>2</sub> ReceiveTMO

t<sub>3</sub> 2 \* Watchdog-Zeit der HiMatrix-Steuerung 2

Quelle: HIMA-Kommunikationshandbuch Kap. 4.7.5

Abbildung 18: Beispiel für eine Berechnung der Worst-Case-Reaktionszeit

### Preisliche Gestaltung

Die in der Tabelle 6 aufgeführten HIMA-Komponenten mit dem zugehörigen Listenpreis werden für die Anwendung benötigt. Dabei können die verbauten Steuerungen die benötigen Sicherheitsfunktionen des jeweiligen Maschinenmoduls ausführen. Da es keine übergeordnete Steuerung gibt, gilt dies auch im Einzelbetrieb.

Tabelle 6: Listenpreise der Komponenten von HIMA

Pos	Bezeichnung	Anzahl	Einzelpreis	Gesamtpreis
1	HiMatrix F30 03	4 Stk	3.050,00 €	12.200,00 €
Gesamt				12.200,00 €

### 4.8 Lösungsvorschlag Phoenix Contact

Die Firma Phoenix Contact bietet zum Aufbau einer sicherheitsgerichteten Kommunikation zwei verschiedene Technologien an, entweder die SafetyBridge-Technologie oder das standardisierte PROFIsafe-Protokoll. SafetyBridge bietet eine sichere Kommunikation über verschiedene Busprotokolle hinweg. Dabei muss das jeweilige Protokoll die Datenkonsistenz sicherstellen und über ein hinreichend schnelles Zeitverhalten verfügen. Das SafetyBridge-

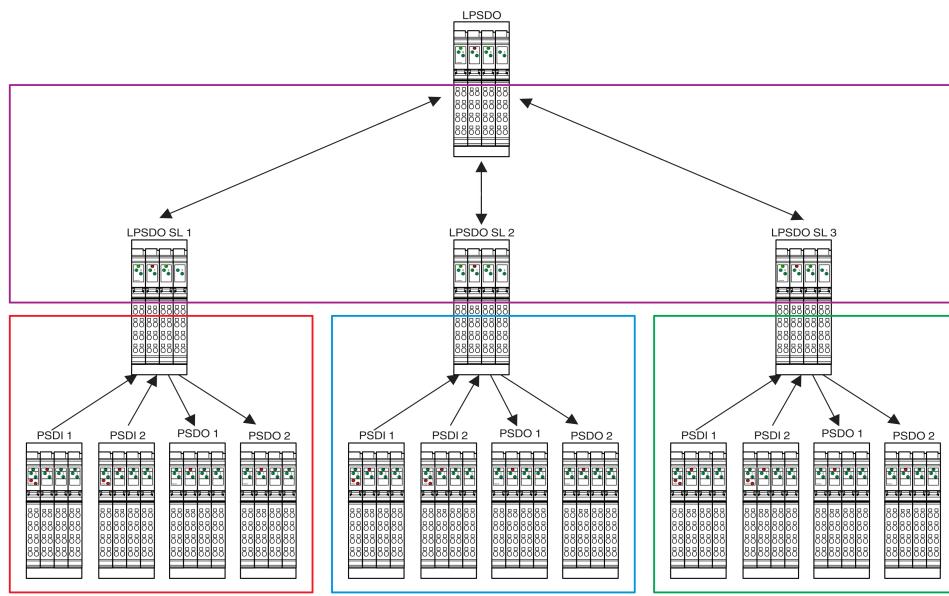
Protokoll kann dabei über verschiedene Netze/Netzübergänge und Routergrenzen hinweg übertragen werden. Die SafetyBridge-Technologie kann als nicht sicheres IO-System in anderen Steuerungen verwendet werden oder über diese hinweg sicher kommunizieren. Mit diesen Eigenschaften entsteht eine bedingte Herstellerunabhängigkeit. Die Bedingung ist, dass in jedem Maschinenmodul SafetyBridge zur Umsetzung der funktionalen Sicherheit zum Einsatz kommt. Alle anderen Automatisierungsaufgaben könnten auch mit Systemen anderer Hersteller umgesetzt werden.

Eine SafetyBridge-Insel besteht aus einem Logikmodul und bis zu 16 verbundenen Ein- bzw. Ausgabemodulen. Das entspricht bis zu 256 Eingangs- und 136 Ausgangskanälen. Wird diese Systemgrenze überschritten, können bis zu 30 weitere Logikmodule mit Ein- und Ausgabemodulen verbaut werden, die untereinander sicherheitsgerichtet Daten austauschen. So kommt man auf ein sicherheitsgerichtetes Gesamtsystem mit >400 Modulen in einem Netzwerk. Somit steht die Gesamtleistungsfähigkeit von SafetyBridge-Technologie anderen Protokollen/Systemen in nichts nach. Die einzige Einschränkung ist die fehlende Kommunikationsmöglichkeit zu PROFIsafe-Geräten und anderen sicheren Protokollen. Ist eine Kommunikation zu anderen PROFIsafe-Geräten erforderlich, so kommen als sichere Ein- und Ausgänge die gleichen Komponenten wie bei SafetyBridge zum Einsatz. Die sicheren Intelligenzen (Logikbausteine) der SafetyBridge werden durch größere und kostenintensivere Steuerungen ersetzt. Diese funktionieren als PROFINet-Controller für das Modul und stellen ein I/O-Device für das smarte Transfersystem bereit. In beiden Technologien können bereits verbaute Komponenten im vorhandenen Ethernet-Netzwerk betrieben werden. Sowohl im PROFIsafe- als auch im SafetyBridge-Betrieb sind die Geräte bis **SIL 3/PL e** einsetzbar und zertifiziert. Ein möglicher hierarchischer Aufbau mit SafetyBridge für drei Module ist in Abbildung 19 gezeigt. Das übergeordnete Logikmodul würde sich in diesem Anwendungsfall im smarten Transfersystem befinden.

### Aufbau der Kommunikation

Von Phoenix Contact wurden mehrere Möglichkeiten zum Aufbau der sicheren Kommunikation zwischen den Modulen angeboten. Diese werden nachfolgend aufgeführt und ermöglichen alle eine beliebige Zuordnung von Integrationsplatz und Modul. Alle Optionen können derart erweitert werden, dass die Kopplung zu einem Maschinenmodul sicher aufgehoben werden kann. Ein unangekündigter Verbindungsabbruch oder ein Nichtentfernen nach Ankündigung führt zu einem Not-Halt des gesamten Systems.

- Option Schlüsselschalter:  
Ein Schlüsselschalter am Modul de- oder aktiviert den Einzelbetrieb des Moduls.



Quelle: Phoenix Contact [Bild A-6 21, S. 80]

Abbildung 19: SafetyBridge Topologie für das Anwendungsbeispiel, dezentrale Logik

Ein weiterer Schlüsselschalter am übergeordneten System de- oder aktiviert den Integrationsplatz am smarten Transfersystem. Das Deaktivieren des Platzes kann im laufenden Betrieb erfolgen. Im Sicherheitsprogramm wird dieser entsprechend überbrückt. Das Modul darf nur am Steckplatz in Betrieb gehen, wenn dieser aktiviert und der Einzelbetrieb am Modul deaktiviert ist.

- Option Brückenstecker:  
Der Plug-and-Produce-Stecker verfügt über Kontakte, die bei Nichtvorhandensein eines Moduls bzw. durch das Transfersystem über einen Brückenstecker kontaktiert werden. Diese Brücke wird im Sicherheitsprogramm abgefragt und die Not-Halt-Verkettung entsprechend aufgehoben.
- Option Sicherheitsprogrammlogik:  
Ein Modul wird im PROFINet automatisch erkannt, die Parametrierung der sicheren Kommunikation wird durchgeführt und zeitlich überwacht. Das Modul kann nur in Betrieb genommen werden, wenn es aktiv Integriert ist.

Die letzte Option wird den Anforderungen an den Integrationsprozess gerecht und wird im Folgenden weiter betrachtet. Mit einer Risikobeurteilung bzw. **FMEA** ist zu überprüfen, ob diese Option genügend Sicherheit bietet oder mit weiteren Mechanismen die Sicherheit zu

erhöhen ist. Dies kann ggf. mit dem zusätzlichen Einsatz der anderen Option erfolgen. Wie aus der nachfolgenden Beschreibung der Implementierung hervor geht, ist der Aufwand dieser Option relativ hoch. So sind die anderen Optionen nicht gleich zu Verwerfen, sondern als Alternativen aufzufassen.

### Implementierung

Bei der Implementierung der letzten Option müssen zunächst alle bekannten Module im überlagerten Steuerungsprojekt angelegt werden. Ist ein Modul nicht integriert, so kommt es zu einem PROFInet-Fehler des betroffenen Moduls. Alle anderen Module können jedoch weiter betrieben werden. Zur Fehlerunterdrückung können, z. B. über eine Visualisierung, die verschiedenen Module an- oder abgewählt werden. Diese ist zu erstellen, damit die Verbindungen bewusst zu schalten und Fehlermeldungen zu vermeiden sind. Zur Erkennung werden über PROFInet die Gerätenamen ermittelt. Anhand der Nachbarschaftserkennung über **LLDP** wird ermittelt, welches Modul sich an welchem Steckplatz befindet. Dies erfolgt nicht sicherheitsgerichtet. Der sichere An- und Abmeldeprozess muss daher sicherheitsgerichtet sequenz- und zeitüberwacht werden. Bei einem Fehler wird ein Not-Halt ausgelöst. Die Risikobeurteilung kann weitere Plausibilisierungen fordern, die einen Betrieb nur möglich machen, wenn der Not-Halt korrekt eingebunden und aktiviert ist.

Die Implementierung erfolgt über die kostenlose Programmierumgebung SafeConf von Phoenix Contact. Dabei handelt es sich um eine Form der **FBS** mit eingeschränktem Befehlssatz (**LVL**), der den Anwender vor typischen Fehlern schützt. Es stehen zertifizierte Funktionsbausteine und Logikfunktionen zur Verfügung. Das reduziert den Abnahmearaufwand bei der Verifikation der Software erheblich, da der Anwender die Dinge, die die Software von Haus aus erkennt, nicht manuell prüfen muss. Die beschriebenen Funktionen mit den zertifizierten Funktionsbausteinen umzusetzen, stellt trotzdem einen beachtlichen Aufwand dar. Über die kostenpflichtige Programmierumgebung SafetyProg können die Funktionen der PROFIsafe-Steuerungen implementiert werden. Diese verfügt gegenüber SafeConf über weitere Möglichkeiten, wie beispielsweise der Einsatz der Programmiersprache **ST**, kann jedoch nicht für SafetyBridge verwendet werden.

### Bestimmung der Reaktionszeit

Zur Bestimmung einer typischen Reaktionszeit für die Beispielanwendung können die Zeiten aus der Tabelle 7 angenommen und mit Gleichung (7) berechnet werden.

Entscheidend für die maximale Reaktionszeit und somit ausschlaggebend für die Worst-Case-Reaktionszeit ist die eingestellte Watchdogzeit. Diese hat keinen Einfluss auf den in Glei-

chung (7) dargestellten Normalbetrieb und kann zwischen 1 ms und 10 s betragen. Über die Risikobeurteilung ist die maximale Reaktionszeit zu bestimmen und die Watchdogzeit entsprechend einzustellen. Mit dieser Zeit steigt die Verfügbarkeit des Systems und gleichermaßen die Worst-Case-Reaktionszeit.

Tabelle 7: Reaktionszeiten der Hardware

Bezeichnung	T in ms	Summe in ms
Eingangsmodul: IB IL 24 PSDI 8-PAC		
Filterzeit	3 ms	
Firmware-Laufzeit	1 ms	$T_{DI} = 4 \text{ ms}$
Datenübertragung	4 ms	
Laufzeit Standard CPU	5 ms	$T_U = 9 \text{ ms}$
Ausgangsmodul mit Logik: IB IL 24 LPSDO8 V3	15 ms	$T_{L/DO} = 15 \text{ ms}$

$$T_t = T_{DI} + 2 \cdot T_U + T_{L/DO} \quad (7)$$

$$T_t = 4 \text{ ms} + 2 \cdot 9 \text{ ms} + 15 \text{ ms}$$

$$T_t = 37 \text{ ms}$$

### Preisliche Gestaltung

Die in Tabelle 8 aufgelisteten Komponenten werden für die in Abbildung 19 dargestellte Lösung benötigt. Mit den in jeder Maschine installierten Komponenten können alle notwendigen Sicherheitsfunktionen ausgeführt werden. Die Preisaufstellung berücksichtigt kein vorhandenes System. Es ist zu beachten, dass die bereits vorhandenen INLINE-Systeme von Phoenix Contact keinen erneuten Kauf des Buskopplers notwendig machen. Die sicheren Module sind an das vorhandene System anzufügen.

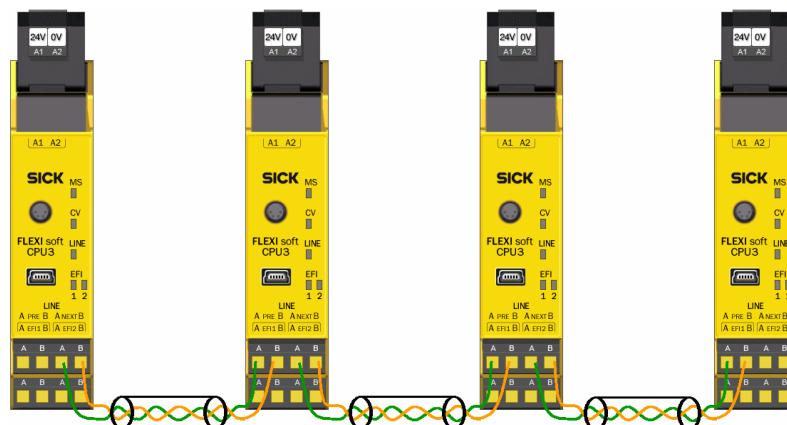
Tabelle 8: Listenpreise der Komponenten

Pos	Bezeichnung	Anzahl	Einzelpreis	Gesamtpreis
1	Eingangsmodul: IB IL 24 PSDI 8-PAC	4 Stk	225,00 €	900,00 €
2	Ausgangsmodul mit sicherer Logik: IB IL 24 LPSDO8 V3-PAC	4 Stk	435,00 €	1.740,00 €
3	optional: Buskoppler PROFInet: IL PN BK DI8 DO4 2TX-PAC	4 Stk	309,00 €	1.236,00 €
	Gesamt			3.876,00 €

## 4.9 Lösungsvorschlag SICK

Die Firma Sick verfolgt zur sicheren Vernetzung einen proprietären Ansatz. Dieser wird FlexiLine genannt und basiert auf dem CAN-Bus. Die CPU-Module (FlexiSoft-Hauptmodule) werden in Linientopologie mit einer zweiseitigen Twisted-Pair-Leitung vernetzt (siehe Abbildung 20). Die Geschwindigkeit und Leistungsfähigkeit des Systems hängt von der maximalen Leitungslänge zwischen zwei CPU-Modulen ab. Die sicherheitsgerichtete adresslose Kommunikation über FlexiLine funktioniert nur mit den CPU-Modulen der Firma Sick. Es können bis zu 32 CPU-Module miteinander verbunden werden. Dies ist bis zu **SIL 3** und **PL e** möglich.

In jedes zu integrierende Maschinenmodul kommt eine FlexiSoft-Station, die kompatibel mit der FlexiLine ist. Diese kann in modularer Bauweise mit Hilfe des internen FLEXBUS+ mit bis zu 12 Erweiterungsmodulen an die jeweiligen Anforderungen des Moduls angepasst werden. Das können unter anderem sein: Ein-/Ausgangserweiterungen mit verschiedenen Ein-/Ausgangsarten bis **SIL 3** oder **PL e**, bis zu zwei aus zehn verschiedenen nicht sicheren Gateways, Relaisausgänge, Antriebsüberwachung.



Quelle: [Abb. 34 22, S. 79]

Abbildung 20: Anschluss und Topologie eines Flexi-Line-Systems

### Aufbau der Kommunikation

Auf jeder FlexiSoft-Station muss sich dasselbe Prozessabbild befinden, damit diese zukünftig an dieser FlexiLine betrieben werden kann. Ist diese Konfiguration erfolgt, können Maschinenmodule in beliebiger Reihenfolgen in einer Linientopologie verbunden werden. An einer Station wird über einen Taster das *Teachen* ausgelöst und die sicherheitsgerichtete

Kommunikation steht zwischen allen Stationen zu Verfügung. Wird nun eine Maschine mit der FlexiSoft-Station entfernt und durch eine Andere ersetzt, werden die sicheren Ausgänge aller Module abgeschaltet (Safe-off). In folge dessen werden alle Maschinen angehalten. Nach dem Hinzufügen der anderen Montagestation kann durch das *Teach*en die sichere Kommunikation wiederhergestellt werden. Wird eine Montagestation entfernt und keine andere eingebunden, so muss über einen Dummystecker die FlexiLine-Leitung wieder verbunden werden. Bei diesem Vorgehen wird aus Sicht der benachbarten Stationen eine Station im laufenden Betrieb überbrückt. In diesem Fall kann nicht einfach neu *geteacht* werden, sondern es ist ein Neustart des Systems notwendig. Der Systemanlauf kann entweder über die Software an einer eingebunden Station oder über ein kurzzeitiges Spannungsfreischalten aller FlexiSoft-Stationen erfolgen. Das *Teach*en sollte durch einen Schlüsselschalter nur geschultem Personal zugänglich gemacht werden.

### Implementierung

Jede FlexiSoft-Station wird individuell mit Hilfe des kostenlosen FlexiSoft-Designers konfiguriert. Bei der Konfiguration der ersten Station wird auch die FlexiLine konfiguriert. Dazu wird das benötigte Prozessabbild festgelegt. In dem Prozessabbild sind die Bits mit dem zugehörigen Routing verknüpft. Das bestimmt, wie der Zustand des Bits weitergegeben werden soll. Es lassen sich folgende Optionen kombiniert auswählen: nach rechts und/oder links, nur an die beiden Nachbarstationen. Mit der Möglichkeit, das Prozessabbild zu exportieren, kann dieses bei jeder Konfiguration einer zugehörigen FlexiSoft-Station eingebunden werden. Die Konfiguration muss nicht zusätzlich zertifiziert werden. Zur Verfügung stehen Logikbausteine, die häufig verwendet werden, und Funktionsbausteine wie: Restart, Zweihandauswertung, Zweikanalauswertung, Taktgeneratoren, usw..

### Anwendungsbeispiel

Die Reaktionsgeschwindigkeit des Systems wird anhand eines Anwendungsbeispiel bestimmt. Es wurde ein einkanaliger Not-Halt über die gesamte Anlage und die Teach-Funktion der FlexiLine realisiert. Die Konfiguration benötigte insgesamt 7 (von 255) Funktionsbausteinen. Damit gab die Software eine Auslastung der Logik von 32 % mit einer benötigten Ausführungszeit von 4 ms an. Beim Erreichen einer Auslastung von 100 % erhöht sich die Ausführungszeit und die prozentuale Berechnung beginnt erneut.

$T_U$ : Übertragungszeit bei benötigter Leitungslänge und Datenmenge  
 $\text{Anz.d. Stationen} (10 \text{ ms} + 2 \cdot \text{Sendzyklus})$

$T_{LX}$ : Angenommene Logikausführungszeit der Station X

$T_{DI}$ : Verarbeitungszeit eines digitalen Eingangs; ohne Filter, Verzögerungen oder Berücksichtigung von Testimpulsen

$T_{DO}$ : Verarbeitungszeit eines digitalen Ausgangs, von der Logik ausgeführt

$$T_t = T_{DI} + 2 \cdot T_{L1} + T_U + 2 \cdot T_{L2} + T_{DO} \quad (8)$$

$$T_t = 6,5 \text{ ms} + 2 \cdot 4 \text{ ms} + 4(10 \text{ ms} + 2 \cdot 2 \text{ ms}) + 2 \cdot 4 \text{ ms} + 4,5 \text{ ms}$$

$$T_t = 83 \text{ ms}$$

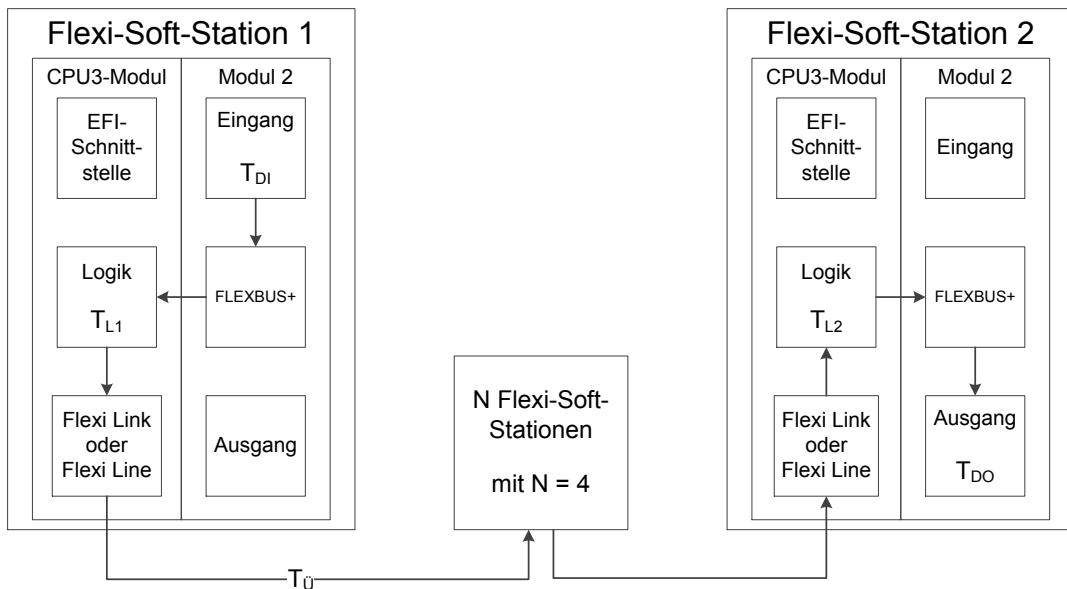


Abbildung 21: Verzögerungen im Signalfluss des FlexiLine-Systems

### Preisliche Gestaltung

Die in Tabelle 9 aufgelisteten Komponenten werden für den in Abbildung 20 dargestellten Aufbau benötigt und um sichere Ein- und Ausgangsmodule und ein Gateway erweitert. Mit den in jeder Montagemaschine installierten Komponenten können alle notwendigen Sicherheitsfunktionen ausgeführt werden.

Tabelle 9: Listenpreise der Komponenten von SICK

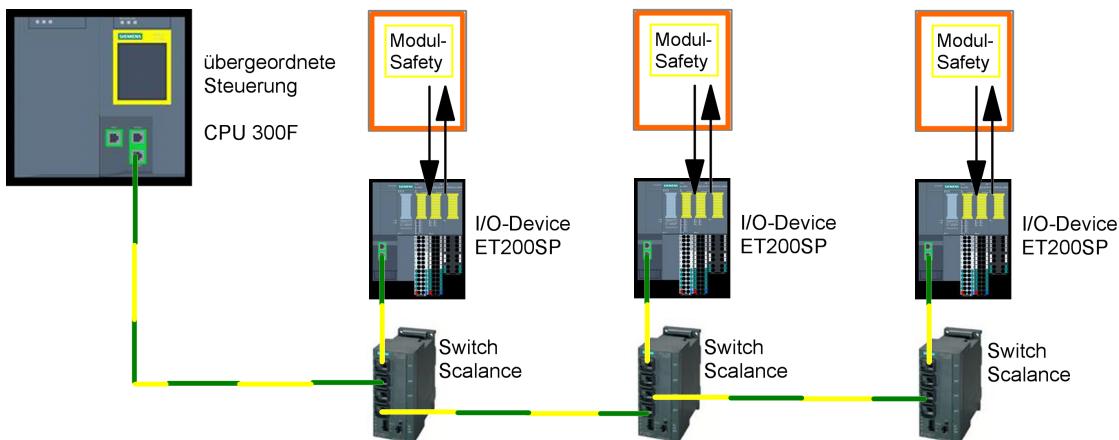
Pos	Bezeichnung	Anzahl	Einzelpreis	Gesamtpreis
1	Sicherheits-CPU: FX3-CPU320002	4 Stk	309,00 €	1.236,00 €
2	Stecker für Spannungsversorgung: FX3-MPL100001	4 Stk	34,70 €	138,80 €
3	Safety I/O-Modul: FX3-XTIO84002	4 Stk	273,00 €	1.092,00 €
4	Gateway, PROFInet: FX0-GPNT00000	4 Stk	340,00 €	1.360,00 €
5	Programmierkabel: Stecker M8 4-polig, auf Stecker USB-A, gerade: DSL-8U04G02M025KM1	1 Stk	52,50 €	52,50 €
Gesamt				3.879,30 €

## 4.10 Lösungsvorschlag Siemens

Die Firma Siemens arbeitet mit dem PROFIsafe-Protokoll, um eine sichere Kommunikation in einer PROFInet-Umgebung aufzubauen. Dabei erfolgt die Übertragung auf der Ethernet-Technologie (IEEE 802.3). Es können auch Komponenten von anderen Herstellern eingesetzt werden, die die PROFIsafe- und PROFInet-Protokolle unterstützen. Durch die Programmierumgebung von Siemens ist dies nur eingeschränkt möglich. PROFInet unterstützt Linien-, Baum- und Sterntopologie, wobei später das Vorhaben auf Linientopologie beschränkt werden muss. Zur Umsetzung ist eine übergeordnete Steuerung (SIMATIC F-CPU) notwendig, die das Optionshandling mit I/O-Geräten (ET200SP) unterstützt. Jede Montageeinheit hat seine eigene notwendige Sicherheitstechnik verbaut. Parallel werden die benötigten Signale auf das I/O-Gerät geführt oder für Abschaltbedienungen entnommen. Die Montagemaschine wird über einen Switch (SCALANCE X204) in die Linientopologie eingehängt. In Abbildung 22 ist der Aufbau für drei Montagemaschinen mit einer übergeordneten Steuerung im smarten Transfersystem dargestellt. Das PROFIsafe-Protokoll erfüllt die Anforderungen vom SIL 3 oder vom PL e. Die eingesetzte Hardware kann bis zu SIL 3 oder PL e verwendet werden.

### Aufbau der Kommunikation

Der folgende Ablauf zum Aufbau der Kommunikation ist in Abbildung 23 dargestellt. Je nach zu fertigenden Produkten gibt es eine PROFInet-Solltopologie, die beschreibt, wie die beteiligten Maschinenmodule angeordnet sein müssen, um diese Produkte zu montieren. Diese Solltopologie kann, z. B. vom Anlagenführer, über ein HMI-Panel unsicher vorgegeben werden. Diese Information muss zur Sicherheitssteuerung weitergegeben werden und über entsprechende Mechanismen in einen sicheren Zustand überführt werden, damit



Quelle: Bild von Siemens nachempfunden

Abbildung 22: Möglicher Aufbau der Hardware für drei Montagestationen und das smarte Transfersystem

gewährleistet ist, dass die Datenvorgabe korrekt ist. Anhand von Applikationsbeispielen von Siemens kann dieses Vorgehen nachvollzogen werden. [23, 24, 25] Benötigt wird zu einem Vergleich mit der Solltopologie die Isttopologie. Diese wird zweimal eingelesen, einmal durch ein übergeordnetes Steuerungssystem und ein weiteres Mal durch die Sicherheitssteuerung. Ist der Vergleich dieser zwei positiv, wird die ermittelte Isttopologie in die Sicherheitssteuerung übernommen und mit der Solltopologie verglichen. Es muss sich eine Information ergeben, die nach ISO 13849-1 belastbar ist. Das Aktivieren von I/O-Geräten mit Hilfe der Topologieerkennung ist zurzeit nur für eine Linientopologie verfügbar. Anhand dieser Information werden die fehlenden I/O-Geräte abgemeldet bzw. die vorhandenen angemeldet und im Sicherheitsprogramm entsprechende Programmteile ein- und ausgeblendet. Nach der Aktivierung der vorhanden I/O-Geräte muss an jeder Maschine eine Quittierung erfolgen, die das Not-Halt-Signal setzt (Lowaktiv). Ist dieses Signal von allen aktiven Montagestationen vorhanden, kann über eine zentrale Quittierung die Freigabe der Produktion erfolgen. Die Kommunikation ist aufgebaut und es können neben dem Not-Halt weitere sicherheitsrelevante Daten über PROFIsafe kommuniziert werden.

### Implementierung

Die Implementierung erfolgt über die Programmierumgebung SIMATIC STEP 7 Professional, die mit dem F-Programmiertool für die Sicherheitssteuerung ergänzt wird. Mit Hilfe der IEC-Programmiersprachen Strukturierter Text (ST), Kontaktplan (KOP) und Funkti-

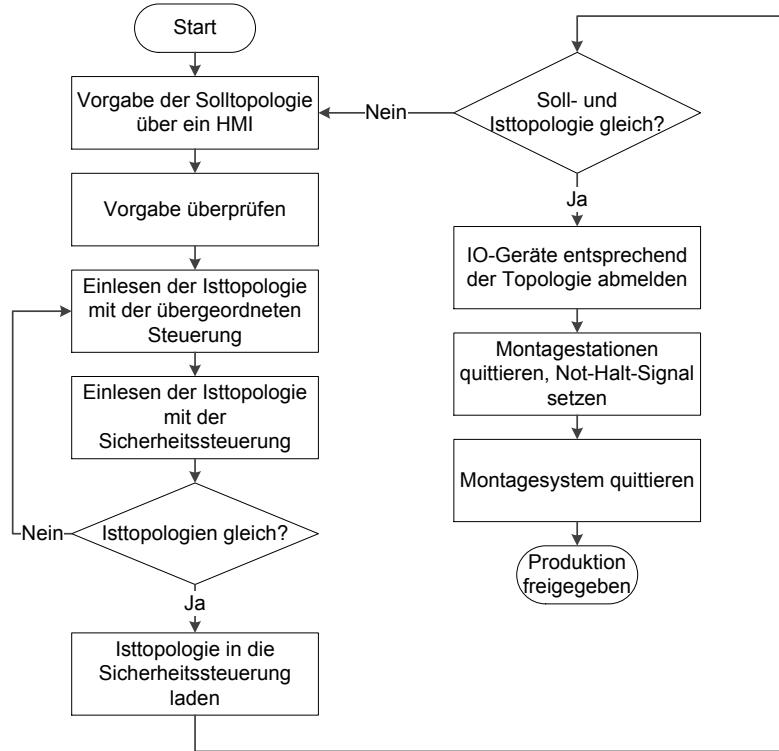


Abbildung 23: Sequendiagramm: Aufbau der Kommunikation

onsplan (FUP) können die Controller programmiert werden. Einige Controller unterstützen zusätzlich die Anweisungsliste (AWL) und die Schrittkettenprogrammierung (GRAPH, SFC). Der Implementierungsaufwand kann mit Hilfe der Dokumente [26, 27] [28, S. 16.3] als relativ hoch eingeschätzt werden.

### Anwendungsbeispiel

Die Firma Siemens stellt zur Abschätzung und Berechnung die *Cotia*-Tabelle zur Verfügung. In diese können voraussichtliche Programmparameter oder tatsächliche Programmparameter eingetragen werden. Anhand dieser Informationen werden verschiedene Reaktionszeiten berechnet. Für das betrachtete Anwendungsbeispiel hat Herr Schütte von Siemens mit der Tabelle eine typische Reaktionszeit im fehlerfreien Zustand von 71 ms ermittelt. Diese kann bei beliebigen Laufzeiten des Standard-Systems, also im Worst-Case-Fall, auf 219 ms ansteigen. Da diese Reaktionszeiten von vielen Faktoren abhängt, würde eine detaillierte Darstellung den Rahmen dieser Studienarbeit überschreiten.

### Preisliche Gestaltung

Die in Tabelle 10 aufgelisteten Komponenten werden für die in Abbildung 22 dargestellte Lösung benötigt. Zu beachten ist, dass in jedem Montagemodul ein IO-Gerät eingebaut wird. Für den Einzelbetrieb werden weitere Sicherheitskomponenten benötigt. Dieser Ansatz geht von einem sicheren Montagemodul aus und stattet es mit der Fähigkeit aus, sicherheitstechnisch in das wandlungsfähige Montagesystem integriert werden zu können.

Tabelle 10: Listenpreise der Komponenten von Siemens

Pos	Bezeichnung	Anzahl	Einzelpreis	Gesamtpreis
1	CPU 1515F-2 PN	1 Stk	2.370,00 €	2.370,00 €
2	Memory Card, 4 Mbyte	1 Stk	51,00 €	51,00 €
3	IM 155-6 PN HF inkl. Servermodul	3 Stk	250,00 €	750,00 €
4	F-DI 8x24VDC HF	3 Stk	188,00 €	564,00 €
5	F-DQ 4x24VDC/2A PM HF	3 Stk	218,00 €	654,00 €
6	F-RQ 1xDC24V/AC24. 230V/5A	3 Stk	96,00 €	288,00 €
7	Busadapter 2xRJ45	3 Stk	48,00 €	144,00 €
8	BU-Typ A0, 16 Push-In, 10 AUX, 2 Einspeisekl. getrennt (Digital-/Analog, max.24 VDC/10 A) zum Beginn einer Lastengruppe	3 Stk	27,50 €	82,50 €
9	Farbkennzeichnungsschilder 16 Prozessklemmen, grau/rot, CC01, 10 Stk.	3 Stk	10,50 €	31,50 €
10	BU-Typ A0, 16 Push-In, 10 AUX, 2 Einspeisekl. Gebrückt (Digital-/Analog, max.24VDC/10A)	3 Stk	17,50 €	52,50 €
11	Farbkennzeichnungsschilder 16 Prozessklemmen, grau/blau, CC02, 10 Stk	4 Stk	10,50 €	31,50 €
12	BU-Typ F0	3 Stk	18,00 €	54,00 €
13	SIMATIC STEP 7 PROFESSIONAL V13 FLOATING LICENSE	1 Stk	1.986,00 €	1.986,00 €
14	SIMATIC S7, F-PROGRAMMIERTOOL, STEP 7 SAFETY ADVANCED V13	1 Stk	586,00 €	586,00 €
Gesamt				7.645,00 €

## 4.11 Tabellarischer Vergleich

In der nachfolgenden Tabelle 11 sind die Eckpunkte der Lösungskonzepte tabellarisch gegenübergestellt und Grundlage der anschließenden Bewertung.

Tabelle 11: Tabellarischer Vergleich der Lösungsansätze

	ABB	B&R	Beckhoff	HIMA	Phoenix Contact	Sick	Siemens
Kommunikationsmedium	CAN-Bus	Ethernet	Ethernet	Ethernet	Ethernet	CAN-Bus	Ethernet
Protokoll	Pluto	openSAFETY	FSOE, PROFIsafe	safeethernet	PROFIsafe, SafetyBridge	FlexiLine	PROFIsafe
Herstellerabhängigkeit	Ja	Nein <sup>*2</sup>	Nein <sup>*2</sup>	Ja	Nein <sup>*2</sup>	Ja	Nein <sup>*2</sup>
Sicherheitsfunktionen im Einzelbetrieb	Ja	Ja	Ja	Ja	Ja	Ja	Nein <sup>*1</sup>
Funktionsumfang erfüllt Anforderungen	Ja	Ja	Ja	Ja	Ja	Ja	Nein <sup>*1</sup>
übergeordnete Steuerung	Nein	Ja	Ja	Nein	Ja	Nein	Ja
erweiterbar mit IO-Geräten	Ja, AS-i	Ja	Ja	Ja	Ja	Ja; EFI, FlexiLoop	Ja
Integrieren und Entfernen einer bekannten Maschine: Anlagenstopp/ zeitlicher Aufwand/ Merkmale	Ja/ mittel/ Konfigu- ration mit Anlagenstopp/ zeitlicher Aufwand/ Merkmale	Nein <sup>*3</sup> / mittel/ Konfiguration am HMI-Panel auswählen, auswählen, an Sta- tion Dummy- stecker am freien An- dockplatz	Nein/ gering/ Ver- bindungen de- oder aktivieren auswählen, an Sta- tion bestätigen	Nein <sup>*3</sup> / ge- ring/ startet Kom- munikati- onsaufbau	Nein/ gering/ automatische Erkennung, bewusstes Abmelden	Ja/ gering/ Wiederan- lauf aller Stationen, Teachen von FlexiLine auslösen, Dummyste- cker	Ja/ mittel/ Konfigura- tion vom HMI-Panel wird mit der Ist-Konfi- guration verglichen, Stationen quittieren

Tabelle 11: Tabellarischer Vergleich der Lösungsansätze (Fortsetzung)

	ABB	B&R	Beckhoff	HIMA	Phoenix Contact	Sick	Siemens
zeitlicher Aufwand das System zu erweitern/ notwendige Schritte	gering/ Auf allen Stationen muss das selbe Programm erweitert werden	mittel/ das Opti- onsmanage- ment muss angepasst werden	gering/ weitere Ver- bindungen müssen hinzugefügt werden	hoch/ anpassen der P2P-Verbin- dungen, Reakti- onszeiten berücksichti- gen	mittel/ Anpassung der Steue- rung not- wendig	gering/ ggf. neues Prozessab- bild auf allen Statio- nen	mittel/ das Options- handling an- passen
Aufwand der Hardware Installation	hoch nachrüsten von CAN-Bus	gering Modbus In- tegration	gering	gering	gering	hoch nachrüsten von CAN-Bus	gering paralleler IO- Anschluss
Aufwand der Implementierung/ Zertifizierung	gering/ Nein	mittel/ evtl. Zerti- fizierung	gering/ Nein	hoch/ Ja	hoch/ Nein	gering/ Nein	mittel/ evtl. Zerti- fizierung vom Topologien- vergleich
Preis	4.338,20 €	7.723,00 €	4.197,17 €	12.200,00 €	3.876,00 €	3.879,30 €	7.645,00 €

Anmerkungen:

\*1 mit anderen Komponenten möglich

\*2 wird von weiteren Herstellern angeboten

\*3 sicheres An- und Abmelden mit entsprechender Implementierung denkbar

## 5 Bewertung und Auswahl

Dieses Kapitel bewertet nachvollziehbar die Konzepte aus Kapitel 4 mit den Anforderungen aus Kapitel 3. Abschließend wird anhand einer Bewertungsmatrix (siehe Tabelle 12) eine Auswahl getroffen.

### 5.1 Bewertung

#### ABB

Der dezentrale Aufbau des Pluto-Konzepts ist mit einem All-Master-System realisiert. Die erforderliche sichere Kommunikation erfolgt dabei über ein eigenes Sicherheitsprotokoll, welches auf den CAN-Bus basiert. Die Forderung, eine sichere Kommunikation über Ethernet zu realisieren, ist nicht möglich. Die aktuelle Kombination von integrierten Maschinen kann nur mit einem Betriebsartenwahlschalter sicher festgelegt werden. Mit steigender Anzahl der Kombinationsmöglichkeiten und damit benötigten Schalterstellungen (Betriebsarten), kann die Auswahl unübersichtlich werden. Die Wahl der aktuellen Kombination mit den Betriebsartenwahlschalter bestimmt, welche Live-Bits zu erwarten sind. Aus diesem Grund kann das System mit relativ wenig Aufwand erweitert werden. Die Implementierung erfolgt über die mitgelieferte Software und stellt ein Konfigurieren dar. Dies reduziert den Aufwand, da viele Funktionen als zertifizierte Bausteine zur Verfügung stehen. Eine Zertifizierung der Konfiguration für die Steuerung ist nicht notwendig. Die Art der Auswahl von integrierten Maschinen begrenzt die Flexibilität und den Ausbau des wandlungsfähigen Montagesystems. Ein Anlagenstopp ist nicht zu vermeiden. Es muss immer ein und die selbe Steuerung in der Anlage verbleiben, auch wenn diese hierarchisch nicht übergeordnet ist. Aus diesen Gründen ist dieses System nicht weiter in Betracht zu ziehen.

#### B&R

Durch den Einsatz des Kommunikationsprotokoll openSAFETY ist der Lösungsvorschlag vom Hersteller unabhängig und bietet eine Kommunikation über Ethernet. OpenSAFETY kann durch das Black-Channel-Prinzip in viele Industrial-Ethernet-Lösungen implementiert werden. Die Firma B&R unterstützt keine direkte Kommunikation über PROFINet. Mit der Möglichkeit parallel, ein Modbus-TCP aufzubauen, kann openSAFETY mit Komponenten von B&R in das wandelbare Montagesystem gebracht werden. Mit einem entsprechenden Implementierungsaufwand kann über das Optionsmanagement ein Hot-plug-fähiges System entstehen, welches ein Integrieren und Entfernen von Maschinen ohne Anlagenstopp ermöglicht. Der zeitliche Aufwand, eine Maschine zu Integrieren oder Entfernen ist leicht erhöht, da

die richtige Konfiguration ausgewählt werden muss. Die Erstellung des Optionsmanagement mit der zugehörigen Bedienoberfläche erfordert viel Kenntnis im Umgang der zugehörigen Programmierumgebung und stellt einen hohen zeitlichen Aufwand dar. Das System mit neuen Maschinen zu erweitern, erfordert eine Anpassung des Optionsmanagement und stellt einen erhöhten Aufwand dar. Für dieses Konzept steht die Herstellerunabhängigkeit durch das offene openSAFETY-Protokoll. Für diesen Lösungsansatz spricht, dass Maschinen ohne einen Anlagenstopp integrieren und entfernen zu können. Nachteilig ist der zusätzliche Aufbau eines Modbus-TCP und die aufwändige Implementierung zusehen. Diese kann in den Programmiersprachen der [IEC 61131](#) erfolgen und muss ggf. zertifiziert werden. Dieses Konzept kann die Wandlungsfähigkeit des Montagesystems aufrecht erhalten.

### **Beckhoff**

Den EtherCAT-Bus parallel im vorhanden Ethernet-Netzwerk zu betreiben, ist nicht möglich, obwohl dieser über Ethernet-Kabel erstellt wird. Das Sicherheitsprotokoll **FSOE** arbeitet auf der Anwendungsschicht und ist vom Kommunikationsmedium unabhängig. EtherCAT bzw. **FSOE** ist ein eingetragener offener Standard (IEC 61158), der überwiegend von Beckhoff vorangetrieben wird, somit kann dieser bedingt als herstellerunabhängig angesehen werden. Zur Organisation der Verbindungen ist eine übergeordnete Steuerung notwendig, hierarchisch betrachtet sind alle Steuerungen EtherCAT Master bzw. PROFInet-Slaves. Dank des zertifizierten *Connection Shutdown* Funktionsbaustein ist das De- und Aktivieren von Sicherheitsverbindungen zwischen TwinSAFE PLC-EtherCAT-Klemmen einfach zu konfigurieren. Dadurch ist der Aufwand beim Hinzufügen von jetzt noch unbekannten Modulen relativ gering. Bei richtiger Vorgehensweise ist kein Anlagenstopp notwendig und die Vorgehensweise beim Integrieren oder Entfernen von Maschinen entspricht dem geforderten Plug-and-Produce-Prinzip. Die Implementierung der Sicherheitsfunktionen erfolgt über zertifizierte Bausteine und stellt nachdem erstellen der EtherCAT-Topologie einen geringen Aufwand dar. Des Weiteren erfordert diese keine weitere Zertifizierung. EtherCAT nachträglich in die bereits vorhandene PROFInet-Umgebung zu integrieren, ist mit Einschränkungen möglich. Ist die Wahl des Kommunikationsprotokolls noch offen, ist EtherCAT eine gute und relativ effiziente Möglichkeit, verschiedene Maschinenmodule miteinander zu vernetzen.

### **HIMA**

Mit dem safeethernet-Protokoll stellt die Firma HIMA ein herstellerspezifisches Lösungskonzept, welches mit dem Ethernet-Standard arbeitet und parallel zu PROFInet übertragen werden kann. Zusammen mit der Hardware zeichnet es sich durch einen hohen Maß an

Sicherheit und Flexibilität aus. Genau diese Flexibilität macht die Implementierung aufwendig und erfordert eine Zertifizierung dieser. Positiv zu bewerten ist die Möglichkeit einer Implementierung nach der Norm [IEC 61131-3](#). Hingegen ist die Implementierung der automatischen Erkennung ohne eine übergeordnete Steuerung mit Hilfe des Kommunikationsprozessors nur mit fundierten Kenntnissen in der Programmierung von funktionaler Sicherheit in der Programmiersprache C möglich. Durch diese vielfältigen Lösungswege ist es möglich, eine sichere Ethernet-basierte Kommunikation ohne eine übergeordnete Steuerung aufzubauen. Mit entsprechendem Implementierungsaufwand kann ermöglicht werden, dass ein Tastendruck ausreicht, um die Maschine sicher zu integrieren. Dies ist in diesem Vergleich ein Alleinstellungsmerkmal. Negativ für dieses System ist neben dem hohen Implementierungsaufwand der hohe Preis. Dieser ist darin begründet, dass die Leistungsfähigkeit des sicherheitstechnischen Funktionsumfangs der Steuerung über den Bedarf einer einzelnen zu integrierenden Maschine liegt. Eine Erweiterung des Gesamtsystems ist mit hohen Aufwand verbunden, da das Kommunikationssystem aller Steuerungen angepasst werden muss, falls eine Erweiterung bei der Erstellung nicht berücksichtigt wurde.

### **Phoenix Contact**

Phoenix Contact bietet zwei Lösungskonzepte an, die proprietäre SafetyBridge-Technologie und einen mithilfe des PROFIsafe-Protokolls. Empfohlen von Phoenix Contact und in diesem Vergleich berücksichtigt wurde die SafetyBridge-Technologie. SafetyBridge kann über verschiedene Industrial-Ethernet-Lösungen hinweg sicher kommunizieren mit der Einschränkung, dass diese Technologie nur von Phoenix Contact angeboten wird. Das Lösungskonzept von Phoenix Contact bietet mehrere Lösungen zum Integrationsprozess an, deren Vorgehensweise sich mit steigendem Implementierungsaufwand immer weiter dem Plug-and-Produce-Prinzip annähert. So kann zeitnah ein Sicherheitskonzept in dem wandlungsfähigen Montagesystem realisiert werden, welches im weiteren Verlauf schrittweise automatisiert werden kann. Am Ende kann eine automatische Erkennung der integrierten Maschinen stehen, die vom Anlagenbediener bewusst bestätigt werden müssen. Für dieses Lösungskonzept ist eine übergeordnete Steuerung in der Integrationsinfrastruktur nötig. Die aufwendige Implementierung erfolgt in [FBS](#) mit einem eingeschränkten Befehlssatz ([LVL](#)) in der kostenlosen Programmierumgebung von PhoenixContact. Durch den eingeschränkten Befehlssatz und die bereits zertifizierten Bausteinen ist eine Zertifizierung der Implementierung nicht notwendig. Die Leistungsfähigkeit des Systems erlaubt eine umfangreiche Erweiterung des Montagesystems. In dem Montagesystem sind bereits viele Phoenix Contact Komponenten verbaut. Die Anforderungen können von dem Lösungskonzept zufriedenstellend erfüllt werden. Aus diesem Grund ist dies zu empfehlen.

**SICK**

Der dezentrale Aufbau mit der FlexiLine erfolgt ohne übergeordnete Steuerung. Die sichere Kommunikation basiert auf dem CAN-Bus. Dies entspricht nicht den Anforderungen. Des Weiteren handelt es sich dabei um ein proprietäres System, welches vom Hersteller abhängig ist. Die Neukonfiguration (Teachen) des Systems, nachdem eine Maschine integriert oder Entfernt wurde, ist ein Kompromiss. Es ist ein Stopp der gesamten Anlage nötig und ein fehlerfreier Neustart kann mit einer erneuter Inbetriebnahme (kurzes spannungsfrei schalten) der Steuerungen erfolgen oder mit dem Einsatz eines Programmiergeräts. Dies entspricht nicht den Anforderungen. Die Erweiterung des gesamten Systems ist relativ einfach, aber auf ca. 32 CPU-Module begrenzt. Ein Vorteil des Systems liegt in der Implementierung, die als Konfigurieren aufgefasst werden kann. Wie Anfangs erwähnt, kommt dieses System ohne eine übergeordnete Steuerung aus.

**Siemens**

Die Firma Siemens bietet eine Lösung an, die auf dem PROFIsafe-Protokoll basiert. Die Lösung von Siemens unterscheidet sich von den anderen Lösungskonzepten im Aufbau. Bei den bisher bewerteten Lösungskonzepten ist in jeder Maschine eine Steuerung verbaut, die die Sicherheitsfunktionen der Maschine ausführt und gleichzeitig kompatibel zu dem gesamten System sind. Der Vorschlag von Siemens war, nur ein Remote-I/O in jeder zu integrierenden Maschine einzubauen. So kann jeder Maschinenhersteller seine Sicherheitssteuerung verbauen und legt zusätzlich nach Vorgaben die benötigen Signale parallel auf das I/O-Gerät. Damit kann die Herstellerabhängigkeit reduziert werden. Alternativ ist auch ein Lösungskonzept mit Steuerungen möglich, die die Sicherheitsaufgaben der jeweiligen Maschine übernehmen. Aus den Anwendungsbeispielen geht hervor, dass das gewünschte Systemverhalten erreicht werden kann. Die Implementierung erfolgt in der kostenpflichtigen Programmierumgebung SIMATIC STEP 7 Professional, die bereits vorliegt und eine Implementierung mit IEC-Programmiersprachen zulässt. Der zeitliche Aufwand zur Implementierung lässt sich aus den Anwendungsbeispielen als relativ hoch einschätzen. Nachteilig ist, dass evtl. eine Zertifizierung der Implementierung nötig ist. Diese Lösung setzt eine übergeordnete Steuerung voraus. Diese ist bei einer Systemerweiterung mit relativ viel Aufwand anzupassen.

Tabelle 12: Bewertungsmatrix zur Auswahl

	ABB	B&R	Beckhoff	HIMA	Phoenix Contact	SICK	Siemens
Kommunikationsmedium/Protokoll	0	3	3	3	3	0	5
Herstellerunabhängigkeit der Steuerung	0	5	3	0	3	0	3
keine übergeordnete Steuerung	3	0	0	5	0	5	0
Beim Integrieren ohne Anlagenstopp	0	5	5	5	5	0	5
Vorgehensweise beim Integrieren	3	5	5	5	5	0	5
Aufwand einer Systemerweiterung	5	3	5	3	3	5	3
Aufwand der Implementierung	5	3	3	0	3	5	3
keine Zertifizierung der Implementierung	5	3	5	0	5	5	3
Preis	5	3	5	0	5	5	5
Summe der Punkte	26	30	34	21	32	25	27
in Prozent	58	67	76	47	71	56	60

## 5.2 Auswahl

Von den in dieser Studienarbeit dargestellten Lösungsvorschlägen ist einer auszuwählen, der die Anforderungen erfüllt. Der Bewertungsmatrix zu entnehmen, ist der Lösungsvorschlag von Beckhoff derjenige mit der größten Übereinstimmung, dicht gefolgt vom Lösungsvorschlag der Firma Phoenix Contact. Welches System das passende für das vorhandene wandlungsfähige Montagesystem ist, soll im Folgenden geklärt werden.

Die Lösungsansätze von ABB und SICK sind aufgrund ihrer Vernetzung über einen CAN-Bus ausgeschieden. Diese konnten mit der einfachen Umsetzung der Funktionen punkten, aber boten gleichzeitig nicht genug Funktionsumfang. Der Integrationsprozess ließ sich nicht genug automatisieren.

Mit dem Lösungskonzept und Steuerungen von HIMA ist vieles möglich, so auch ein flexibler Aufbau von Steuerungen ohne eine übergeordnete Steuerung. Nachteilig und zum Ausscheiden im Rahmen dieser Studienarbeit hat geführt, dass dieses wünschenswerte Systemverhalten mit viel Aufwand und Kenntnis in der Programmierung von sicherheitsrelevanten Systemen noch zu implementieren und zertifizieren ist. Im Allgemeinen kann ein Maschinenhersteller, der dieses Systemverhalten mit HIMA-Steuerungen implementiert, viel Know-How sein eigen nennen. Die hohe Leistungsfähigkeit einer HIMA-Steuerung kann den Preis rechtfertigen. Bezogen auf die hier betrachtete Anlage ist die Steuerung

überdimensioniert.

Der Vertreter von Siemens war gut mit der Thematik vertraut und hatte den Vorschlag, dem Maschinenhersteller die Wahl der Sicherheitssteuerung zu überlassen und somit herstellerunabhängiger zu werden. Im Lastenheft kann den Maschinenhersteller vorgegeben werden, welche Signale dieser über ein Siemens I/O-Device bereitzustellen hat. Es konnte keine Aussage zur Verhinderung eines Stopps der gesamten Anlage gefunden werden. Das gewünschte Systemverhalten zu implementieren, beansprucht schätzungsweise einen hohen zeitlichen Aufwand und fundierten Umgang mit der Programmierumgebung.

Der Lösungsansatz von B&R basiert auf einem zertifizierten Optionsmanagement, welches Hot-Plug-Fähigkeit verspricht. Die Auswahl ist durch verschiedene Parameter sicherzustellen und kann auch ohne eine/n Topologieerkennung und -vergleich auskommen. Das Alleinstellungsmerkmal dieses Ansatzes ist das openSAFETY-Protokoll. Dieses kann frei verwendet werden und ist damit nicht herstellerspezifisch. Der Kreis der Hersteller, die das Protokoll zur Zeit unterstützen, ist begrenzt. Zur Abwertung gegenüber Phoenix Contact führte die Aussage, eventuell die Implementierung noch zertifizieren zu müssen.

Der Lösungsansatz mit Produkten von Beckhoff stellt die größte Übereinstimmung dar, obwohl nicht alle EtherCAT-Vorteile genutzt werden können. Punkte der Worst-Case-Reaktionszeit und der Umgang mit einem fehlenden PROFInet-Slave sind nicht abschließend geklärt und lassen Fragen offen. Wird EtherCAT zur Vernetzung des gesamten Systems verwendet, so lässt dieses System keine Fragen offen. Die benötigten Reaktionszeiten sind wahrscheinlich zu erlangen. Durch die vorhandene PROFInet-Umgebung ist der Lösungsvorschlag nur mit Kompromissen umzusetzen.

Phoenix Contact bietet mit SafetyBridge eine netzwerkübergreifene geschlossene Lösung an, die ähnliche Möglichkeiten wie die Steuerungskonzepte von B&R und Siemens ermöglicht. Der zeitliche Aufwand der Implementierung von den benötigten Sicherheitsfunktionen ist schätzungsweise größer als bei dem Lösungsansatz mit Beckhoff-Komponenten. Der Unterschied liegt hier nicht nur im Preis. Die SafetyBridge-Technologie kann parallel zu anderen Feldbus-Protokollen auf der Basis von Ethernet betrieben werden. Hinzu kommt, dass bereits Inline-Baugruppen und Steuerungen von Phoenix Contact im wandlungsfähigen Montagesystem verbaut sind. Aus diesem Grund fällt für das betrachtete System die Entscheidung, den Lösungsansatz von Phoenix Contact umzusetzen.

## Literatur

- [1] Patrick Gehlen. *Funktionale Sicherheit von Maschinen und Anlagen: Umsetzung der europäischen Maschinenrichtlinie in der Praxis*. Siemens. Erlangen: Publicis Publ, 2010. ISBN: 978-3-89578-366-1.
- [2] Deutsches Institut für Normung. *Sicherheit von Maschinen - Integrierte Fertigungssysteme - Grundlegende Anforderungen*. Beuth Verlag GmbH. DIN EN ISO 11161:2010-10. Berlin, 2010.
- [3] NAMUR – Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V. *NAMUR Startseite*. Hrsg. von NAMUR – Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V. 2015. URL: <http://www.namur.net/> (besucht am 24.01.2015).
- [4] Deutsches Institut für Normung. *Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze*. Beuth Verlag GmbH. DIN EN ISO 13849-1:2008-12. Berlin, 2008.
- [5] Deutsches Institut für Normung. *Sicherheit von Maschinen - Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme*. Beuth Verlag GmbH. DIN EN 62061 (VDE 0113-50):2013-09. Berlin, 2013.
- [6] Fraunhofer-Anwendungszentrum Industrial Automation. *SmartFactoryOWL*. Hrsg. von Fraunhofer-Anwendungszentrum Industrial Automation. 2014. URL: <http://www.smartfactory-owl.de/index.php/de/smartfactory> (besucht am 26.01.2015).
- [7] DIN Deutsches Institut für Normung e. V. *DIN - Erfolg durch Normung*. 2014. URL: <http://www.din.de/cmd;jsessionid=SUM8KHW5Z32XW1FQX7JIIZYT.3?level=tpl-bereich&menuid=47388&languageid=de&cmsareaid=47388> (besucht am 26.01.2015).
- [8] Holger Allmang. »Industrie 4.0 - Modulare Zertifizierung für dynamisch konfigurierbare Industrie-Systeme«. Positionspapier im persönlichem Gespräch erhalten; TÜV SÜD Product Service GmbH-01.05.2105. 2015.
- [9] Patrick Gehlen. *Sicherheitsfibel zur Maschinensicherheit: Funktionale Sicherheit und Sicherheitsfunktionen - Erläuterungen zur DIN EN 62061 (VDE 0113-50) bei der Verwendung von sicherheitstechnischen Kennwerten auf Basis des VDMA-Einheitsblatts 66413*. Bd. 152. VDE-Schriftenreihe - Normen verständlich. Berlin: VDE-Verl, 2014. ISBN: 9783800735655.

- [10] NAMUR – Arbeitskreis 1.12. »Anforderungen an die Automatisierungstechnik durch die Modularisierung verfahrenstechnischer Anlagen«. In: Hrsg. von NAMUR – Arbeitskreis 1.12. NE 148. Leverkusen, 22.10.2013.
- [11] VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik. *Formalisierte Prozessbeschreibungen: Konzept und grafische Darstellung*. Hrsg. von VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik. Beuth Verlag GmbH. Entwurf VDI/VDE 3682. Berlin, 2014.
- [12] Pilz GmbH & Co. KG. *Das Sicherheitskompendium: Für den Umgang mit Normen zur funktionalen Sicherheit*. Hrsg. von Pilz GmbH & Co. KG. 2013. URL: [http://www.pilz.com/imperia/md/content/documentation/offen/produkt\\_bergreifend/promotional\\_literature/Safety\\_Compendium\\_DE\\_2013\\_10.pdf](http://www.pilz.com/imperia/md/content/documentation/offen/produkt_bergreifend/promotional_literature/Safety_Compendium_DE_2013_10.pdf) (besucht am 26.01.2015).
- [13] DIN Deutsches Institut für Normung e. V. *DIN - Erfolg durch Normung - Sicherheit und Nachhaltigkeit*. 2014. URL: <http://www.din.de/cmd?cmsrubid=47461&menurubricid=47461&level=tpl-rubrik&menuid=47388&languageid=de&cmsareaaid=47388> (besucht am 26.01.2015).
- [14] Bodo Kälble und Rolf Reudenbach. *Sichere Maschinen in Europa: Anleitung für die praktische Durchführung; mit Musterbeispiel nach EG-Maschinenrichtlinie 2006/42/EG und DIN EN ISO 12100*. 5., überarb. Aufl. Bochum: DC Verl, 2012. ISBN: 978-3-943488-04-3.
- [15] Thomas Steffens und David Schepers. *Die drei Standards der Maschinensicherheit: EN ISO 13849, EN 62061 und IEC 61508*. Hrsg. von Vogel Business Media GmbH & Co. KG. 2013. URL: <http://www.elektrotechnik.vogel.de/steuerungen/articles/394828/>. (besucht am 27.08.2014).
- [16] Rolf Zöllner. »Sicher + sicher = sicher?« In: *Funktionale Sicherheit* Juli (2013), S. 14–19.
- [17] Deutsches Institut für Normung. *Sicherheit von Maschinen - Risikobeurteilung - Teil 2: Praktischer Leitfaden und Verfahrensbeispiele*. Beuth Verlag GmbH. DIN ISO/TR 14121-2 (DIN SPEC 33885):2013-02. Berlin, 2013-02.
- [18] Deutsches Institut für Normung. *Sicherheit von Maschinen - Allgemeine Gestaltungslösätze - Risikobeurteilung und Risikominderung*. Beuth Verlag GmbH. DIN EN ISO 12100:2011-03. Berlin, 2011. URL: <http://www.beuth.de/de/norm/din-en-iso-12100/128264334> (besucht am 26.02.2015).

- [19] Hans Dipl.Ing. Ostermann. *maschinenrichtline.de*. Hrsg. von MBT Mechtersheimer GbR. 2014. URL: <http://www.maschinenrichtlinie.de/home/>. (besucht am 23.09.2015).
- [20] Thomas Dipl. Ing. Janzer. *Sicherheitsgerichtete Automatisierung mit safeethernet und HIMatrix: Sichere Kommunikation mit Ethernet*. Hrsg. von HIMA Paul Hildebrandt GmbH + Co KG. URL: [http://www.hima.de/\\_filenet/Download.asp?ID=PU00004777&Tag=Fachbeitrag\\_safeethernet](http://www.hima.de/_filenet/Download.asp?ID=PU00004777&Tag=Fachbeitrag_safeethernet) (besucht am 12.05.2015).
- [21] PHOENIX CONTACT, Hrsg. *Inline - Modul mit integrierter Sicherheitslogik und sicheren digitalen Ausgängen: UM DE IB IL 24 LPSDO 8 V3-PAC: Anwenderhandbuch*. 2992035. 2013.
- [22] SICK AG Industrial Safety Systems. *Betriebsanleitung: Flexi Soft: Modularer Sicherheitssteuerung Hardware*. Hrsg. von SICK AG Industrial Safety Systems. 2013. URL: <https://www.sick.com/media/pdf/7/57/157/IM0028157.PDF> (besucht am 31.01.2015).
- [23] Siemens AG. *Vorgabe von Grenzwerten für sichere Geschwindigkeit (SLS) von einem nicht-sicheren HMI: Distributed Safety: Applikationsbeschreibung März 2013*. Hrsg. von Siemens AG. 19.04.2013. URL: <http://support.automation.siemens.com/WW/view/de/67634251> (besucht am 06.02.2015).
- [24] Siemens AG. *PROFINET Topologien erkennen und IO-Devices aktivieren: Applikationsbeschreibung 03/2014*. Hrsg. von Siemens AG. 12.05.2014. URL: <http://support.automation.siemens.com/WW/view/de/90924135> (besucht am 07.02.2015).
- [25] Siemens AG. *PROFINET: PROFINET mit STEP 7 V13: Funktionshandbuch*. Hrsg. von Siemens AG. 12.12.2014. URL: <http://support.automation.siemens.com/WW/view/de/49948856> (besucht am 06.02.2015).
- [26] Siemens AG. *Wie können Sie im Anwenderprogramm einer S7-300 oder S7-400 CPU mit integrierter PN-Schnittstelle die aktuelle Topologie des angeschlossenen PROFINET IO-Systems auslesen?* Hrsg. von Siemens AG. 17.09.2009. URL: <http://support.automation.siemens.com/WW/view/de/38566021> (besucht am 16.02.2015).
- [27] Siemens AG. *Wie kann ich einen Slave abschalten (abkoppeln) ohne dass ein Fehlereintrag im OB 86/OB 122 erscheint?* Hrsg. von Siemens AG. 7.10.2014. URL: <http://support.automation.siemens.com/WW/view/de/5608020> (besucht am 16.02.2015).

- [28] Siemens AG. *System- und Standardfunktionen für S7-300/400 Band 1 und Band 2*. Hrsg. von Siemens AG. 4.08.2010. URL: <http://support.automation.siemens.com/WW/view/de/44240604> (besucht am 16.02.2015).

## **Anlage: Inhalt der CD-ROM**

- Risikobeurteilung\_Laser.pdf: vorläufige Risikobeurteilung vom Modul zum Gravieren
- Risikobeurteilung\_Roboter.pdf: vorläufige Risikobeurteilung vom automatischen Montagemodul
- Risikobeurteilung\_Schnittstellen.pdf: vorläufige Risikobeurteilung der Schnittstellen zu den berücksichtigten Maschinenmodulen
- Risikobeurteilung\_Transferbaender.pdf: vorläufige Risikobeurteilung vom smarten Transfersystem (ohne Schnittstellenbetrachtung)
- Risikobeurteilung\_Vorlage.pdf: Vorlage der Risikobeurteilungen
- Studienarbeit\_Kleen\_Druck.pdf: verwendete Druckvorlage