

Hochschule Ostwestfalen-Lippe

Fachbereich Elektrotechnik und Technische Informatik

Bachelorarbeit

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: Implementierung eines Konzepts für die funktionale Sicherheit (Safety) für ein wandlungsfähiges Montagesystem mit Hilfe der SafetyBridge-Technologie

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

2.Prüfer: Prof. Dr.-Ing. Rolf Hausdörfer

Der Bericht umfasst 51 Seiten.

Erklärung

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

Die Ausfertigung und Anhänge liegen als CD-ROM bei.

Lemgo, den 18.11.2015

Philip Kleen

Hochschule Ostwestfalen-Lippe
University of Applied Sciences

Fachbereich Elektrotechnik und Technische Informatik

**Implementierung eines Konzepts für
die funktionale Sicherheit (Safety)
für ein wandlungsfähiges
Montagesystem mit Hilfe der
SafetyBridge-Technologie**

von

Philip Kleen

November 2015

Zusammenfassung

In dieser Bachelorarbeit wird das Sicherheitskonzept aus der Studienarbeit mit der SafetyBridge-Technologie (SBT) von Phoenix Contact implementiert. Das vorhandene wandlungsfähige Montagesystem der smartFactoryOWL besteht aus drei Systemkomponenten: dem smarten Transfersystem, einer Lasergravurmaschine und einer Roboter-montagemaschine. Diese drei Maschinen werden mit der SBT-V3 ausgestattet, um eine Kommunikation für den Austausch von sicherheitsrelevanten Daten zwischen den drei Maschinen aufzubauen. Über diese Kommunikationsverbindungen wird die Sicherheitsfunktion des maschinenübergreifenden Not-Halts aufgebaut. Mit Sensoren an den Maschinen und einer umfangreichen Auswertung in der Sicherheitssteuerung des Transfersystems wird eine Erwartungshaltung über die Anzahl von benötigten Not-Halt-Signalen aufgebaut. Dies wird vom Maschinenbediener bestätigt. Die sicherheitsgerichteten Komponenten wurden in die Standardsteuerungen integriert.

Bei der Implementierung des Sicherheitskonzepts sollten acht Maschinen berücksichtigt werden: die Integrationsumgebung und sieben mögliche Maschinenmodule, die integriert werden können. Diese Anforderung konnte nicht erfüllt werden. Zum einen war die SBT für das erstellte Konzept nicht leistungsfähig genug und zum anderen konnte keine ausreichende Bedienvorgabe erstellt werden. Aus diesen Gründen wurde die Implementierung auf drei mögliche Maschinenmodule zur Integration begrenzt. Mit dieser Einschränkung konnte eine Not-Halt-Funktion über alle integrierten Maschinenmodule implementiert werden, ohne die Wandlungsfähigkeit des Montagesystems einzuschränken. Zusätzlich wurden die bereits vorhandenen Sicherheitsfunktionen von den Maschinenmodulen überprüft und ergänzt. Bei der Implementierung stellten sich mögliche Anforderungen an zukünftige Sicherheitskonzepte und -steuerungen heraus. Es zeigten sich ähnliche Herausforderungen, für die bereits Lösungen in der Standardautomatisierungstechnik gesucht werden.

Inhaltsverzeichnis

Abbildungsverzeichnis	XI
Glossar	XII
Abkürzungsverzeichnis	XIV
1 Einleitung	1
1.1 Motivation und Zielsetzung	1
1.2 Gliederung	2
2 Stand der Technik	3
2.1 Smartes Transfersystem	3
2.2 Robotermontagemaschine	4
2.3 Graviermaschine	5
2.4 Das SafetyBridge-System	5
2.4.1 Programmierumgebung SAFECONF	7
2.4.2 Aufbau der Querkommunikation	7
2.4.3 Black-Channel-Prinzip	8
2.5 Vernetzung der Maschinen	9
2.6 Normen und Richtlinien	10
3 Anforderungen	13
3.1 Smartes Transfersystem	13
3.2 Robotermontagemaschine	14
3.3 Gravurmaschine	14
3.4 Anforderungen von der SafetyBridge-Technologie	15
3.5 Normative Anforderungen	15
4 Konzept	17
4.1 Funktionsweise der Sicherheitseinrichtungen	17
4.2 Aufbau der Hardware	18
4.3 Querkommunikation	18
4.4 Plausibilisierung	20
4.5 Weitere Funktionen	21
4.6 Testaufbau	21

5 Implementierung	23
5.1 SafetyBridge in ein PC-WORX-Projekt	23
5.2 Aufbau der Querkommunikation	24
5.3 Plausibilisierung	25
5.4 Installation in das Montagesystem	28
6 Auswertung	31
6.1 Umsetzung des Konzepts	31
6.2 Erfassung von sicheren Sensoren im Feld	32
6.3 Querkommunikation	33
6.4 Sicherheitsfunktionen der Maschinenmodule	38
6.4.1 Smartes Transfersystem	38
6.4.2 Robotermontagemaschine	40
6.4.3 Graviermaschine	40
6.5 Fazit	42
6.6 Ausblick	44
Literaturverzeichnis	48
Anlage: Inhalt der CD-ROM	51

Abbildungsverzeichnis

1	Beim Black-Channel-Prinzip setzt die Sicherheitsfunktion als eigene <i>Safety-Schicht</i> auf dem eigentlichen Übertragungsmedium auf	9
2	Programmablaufplan der Sicherheitssteuerung im Transfersystem (Master) .	19
3	Foto vom Testaufbau	22
4	Gatter um genau ein Signal von drei möglichen auszuwerten	26
5	Verlauf der Übertragungszeit zwischen zwei SafetyBridge-Logikmodulen .	33
6	Ausschnitt aus einer kontinuierlichen Aufzeichnung der Übertragungszeit zwischen den SafetyBridge-Logikmodulen	37

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.

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. [2]

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). [3]

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. [4]

Sicherheitsbezogenes elektrisches Steuerungssystem (SRECS)

en: safety-related electrical control systems

Sicherheitsbezoogenes elektrisches Steuerungssystem einer Maschine, dessen Ausfall zu einer unmittelbaren Erhöhung von Risiken führt. [4, 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 Ostwestfalen-Lippe 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. [5]

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

BCD	Binary Coded Decimal
BMAS	Bundesministerium für Arbeit und Soziales
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
DIN	Deutsche Institut für Normung
DIP	Dual In-line package
EN	Europäische Norm
HMI	Human Machine Interface
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISO	International Organization for Standardization
MRL	Maschinenrichtline
NAMUR	Normenarbeitsgemeinschaft für Mess- und Regeltechnik in der chemischen Industrie
OPC-UA	Open Platform Communication – Unified Architecture
OSI	Open Systems Interconnection
OWL	Ostwestfalen-Lippe
PL	Performance Level
PROFINET	PROcess FIeld NETwork
RFID	Radio-Frequency IDentification

SBT SafetyBridge-Technologie

SIL safety integrity level

SPS Speicher Programmierbare Steuerung

UDP User Datagram Protocol

1 Einleitung

1.1 Motivation und Zielsetzung

Das wandlungsfähige Montagesystem der smartFactoryOWL erfüllt Anforderungen der vierten industriellen Revolution. Einzelne eigenständige Maschinen werden in eine Integrationsumgebung eingebracht. Es entsteht eine Anlage zur Montage verschiedener Produkte. Die vorausgegangene Studienarbeit hat gezeigt, dass für dieses Anlagendesign ein einheitliches Konzept der funktionalen Sicherheit gefunden werden muss. In der Studienarbeit wurden Normen im Bezug auf ein modulares Maschinendesign im Sinne der NAMUR-Empfehlung *NE 148* analysiert. Mit derartigen Anlagenkonzepten sollen vielfältig einsetzbare Produktionsanlagen entstehen. Dazu stellt eine einzelne Maschine die Erledigung eines Arbeitsschrittes als Dienst zur Verfügung. Durch den Austausch einzelner Arbeitsschritte in Form von Maschinen bzw. auswechselbaren Ausrüstungen können individuelle und verschiedene Produkte gefertigt werden. Neben der Bestimmung von zutreffenden Normen wurde der Fokus auf die Analyse von technologischen Möglichkeiten eines durchgängigen Not-Halt-Konzepts gelegt. Zur Realisierung eines durchgängigen Not-Halts, der die Anforderungen von einem derartigen Anlagenkonzept erfüllt, ist der Aufbau einer sicherheitsgerichteten zertifizierten Maschine-zu-Maschine-Kommunikation eine mögliche Lösung. Dies kann über eine entsprechende P2P-Verbindung ermöglicht werden.

In der Studienarbeit wurden verschiedene Technologien von unterschiedlichen Herstellern mit dem Ergebnis verglichen, dass es nur mit erheblichem Aufwand möglich ist, einen Mechanismus zu entwickeln, der eine zuverlässige sichere Maschine-zu-Maschine-Kommunikation ermöglicht. Das bereits vorhandene Montagesystem ist mit einer am Markt etablierten Technologie der funktionalen Sicherheit auszustatten. Im Vergleich konnte unter anderem die SafetyBridge-Technologie (SBT) von Phoenix Contact die entscheidenden Anforderungen erfüllen. Ausschlaggebend war vor allem der Punkt, dass bereits Komponenten der SBT in den Maschinen verbaut worden sind.

Mit der SBT-V3 soll ein modularer und globaler Not-Halt realisiert werden. Ein bereits berücksichtigtes Maschinenmodul wird an einem vorgesehenen Platz mit dem Transfersystem verbunden und in Betrieb genommen. Das Hinzufügen und Entfernen ist ohne einen Stopp des Gesamtsystems durch die funktionale Sicherheit zu ermöglichen. Beim Hinzufügen und Entfernen von Maschinenmodulen in das Montagesystem ist eine handhabbare und bewusste Vorgehensweise zu finden. Dabei wird nur die benötigte technologische Vorgehensweise betrachtet. Zur Erfüllung der risikomindernden Maßnahmen aus der Risikobeurteilung nach DIN EN ISO 12100 sind sichere Sensoren und Aktoren auszuwählen und in Betrieb zu nehmen. Außer Acht werden Betrachtungen der Risikobeurteilung gelassen, wie beispielsweise:

ein zulässiger Zeitpunkt einer Veränderung am System oder die Sicherstellung, dass nur Maschinen integriert werden, die zu dem jeweiligen Zeitpunkt der zulässigen Maschinenart (Klassifikation) entsprechen.

1.2 Gliederung

In Kapitel 2, Stand der Technik, wird die derzeitige Realisierung des Not-Halts und die risikomindernden Maßnahmen an den Maschinen erläutert. Dabei wird das wandlungsfähige Montagesystem als bekannt vorausgesetzt. Dies ist bereits in der Studienarbeit erläutert worden. Der Stand der Technik von den Maschinenmodulen, dem smarten Transfersystem und den Normen und Richtlinien wird betrachtet. Im Weiteren wird auf die SBT eingegangen. In Kapitel 3 sind die Anforderungen formuliert, die zum Erreichen des Ziels, ein funktional sicheres wandlungsfähiges Montagesystem zu erstellen, erfüllt werden müssen. Im nachfolgenden Kapitel 4 ist das Konzept des umzusetzenden modularen Not-Halts und deren Implementierung beschrieben. Dabei wird auch auf die nicht sichere Implementierung in der Programmierumgebung PC-WORX eingegangen. Mit einer teilweisen Validierung in Kapitel 6 wird überprüft, ob die Anforderungen aus Kapitel 3 erfüllt werden. Dazu wird die garantierte Reaktionszeit ermittelt. Abschließend folgt in Kapitel 6.6 ein Ausblick auf zukünftige Anforderungen von sicherheitsrelevanten Produkten und mögliche Verbesserungen der steuerungstechnischen Umsetzung des Sicherheitskonzepts.

2 Stand der Technik

In diesem Kapitel wird der Stand der Technik des smarten Transfersystems, der Maschinenmodule und der SafetyBridge-Technologie (SBT) erläutert. In der vorausgegangenen Studienarbeit wurden mehrere mögliche Sicherheitskonzepte und zugehörige steuerungstechnische Lösungsmöglichkeiten für das wandlungsfähige Montagesystem vorgestellt. Das Konzept von Phoenix Contact basiert auf der SBT und soll in das wandlungsfähige Montagesystem integriert werden. Jedes Maschinenmodul ist eine eigenständige Maschine mit einer eigenen speicher programmierbaren Steuerung (SPS). Die Versorgung der Maschinenmodule mit Elektrizität, Druckluft und Informationen erfolgt mit definierten Schnittstellen. Über diese können die Maschinenmodule als wechselbare Ausrüstungen mit dem Transfersystem verbunden werden. Die Definition des Begriffs Sicherheit wurde bereits in der Studienarbeit erläutert, siehe [6, S. 3]. In dieser Bachelorarbeit ist ebenfalls mit *sicher* bzw. *Sicherheit* der Bezug zur funktionalen Sicherheit gemeint.

2.1 Smartes Transfersystem

Das smarte Transfersystem kann je nach Betrachtung als Integrationsumgebung gemäß DIN EN ISO 11161 oder als Grundmaschine gemäß Maschinenrichtlinie (MRL) aufgefasst werden. Das smarte Transfersystem ist ein erweitertes Objektträgersystem. Es wurde dahin gehend erweitert, dass es zum einen Integrationsplätze mit einem Versorgungsanschluss zur Verfügung stellt und zum anderen über einen RFID-Tag im Objektträger die Produktionsinformationen direkt mit dem Produkt transportiert werden. An den Integrationsplätzen können Maschinenmodule als integrierbare Maschinen oder als wechselbare Ausrüstungen zu dem System hinzugefügt werden. Des Weiteren steht durch die Bereitstellung einer Ethernet-Schnittstelle in dem Versorgungsanschluss ein weiterer Kommunikationsweg zur Verfügung. Diese kann eine mögliche Schnittstelle für die Vernetzung der funktionalen Sicherheit sein. Durch diese Eigenschaft stellt das Transfersystem mehr Funktionen bereit als der ursprünglich vorgesehenen Produkttransport. Die Automatisierung erfolgt über eine zentrale Steuerung für das gesamte Transfersystem. Diese bereitet die Sensorik und Aktorik auf und stellt diese den integrierten Maschinenmodulen über eine Software-Schnittstelle zur Verfügung. Jedoch kann das smarte Transfersystem zurzeit keine gesicherten Antworten über folgende Fragestellungen der funktionalen Sicherheit geben:

- Wie sind die Maschinen angeordnet?
- Welche Maschinen sind integriert?
- Welche Gefahren können von den integrierten Maschinenmodulen ausgehen?
- Wie viele Maschinen sind zurzeit integriert?

- Wann darf die Maschine dem Prozess hinzugefügt oder entnommen werden?
- Wann muss welche integrierte Maschine in einen sicheren Zustand überführt werden?

Ein Teil der Fragen kann bereits von der Standardautomatisierungstechnik beantwortet werden. Die Beantwortung der Fragestellungen und die zuvor beschriebenen Funktionen machen das Transfersystem ein Stück weit intelligent. Es stellt die Grundmaschine des wandlungsfähigen Montagesystems dar. Ein nicht intelligentes Transfersystem bietet nur die Möglichkeit eines Werkstücktransports mithilfe eines statischen Objektträgers. Dies beinhaltet die Organisation des Transports über Stopper und Indexierungen. Bei der Risikobeurteilung fiel auf, dass das smarte Transfersystem nur über einen Not-Aus-Schalter am Schaltschrank verfügt. Auf den Werkstückträgern ist bereits ein magnetischer Betätiger von Schmersal angebracht, um die korrekte Positionierung in verbundenen Maschinenmodulen festzustellen. Es befindet sich keine zusätzliche Schutzmaßnahme an dem Transfersystem. Das Fehlen vom Not-Halt-Schalter fiel vor allem an der Transferband-Baugruppe der Produktentnahme und am Integrationsplatz für Handmontageschritte auf.

2.2 Robotermontagemaschine

An der Montagemaschine mit einem Roboter wird der Zugang in den geschützten Bereich zum Roboter nicht überwacht. Die trennende Schutzeinrichtung ist für eine schnelle Demontage vorbereitet und kann während des Betriebs entfernt werden. Zur Einrichtung des Roboters ist die Demontage kein geeigneter Zugang, siehe Risikobeurteilung der Maschine. Weiter ist durch ein Untergreifen das Eindringen in den geschützten Bereich möglich. Des Weiteren entsteht ein Zugang in den geschützten Bereich, wenn kein Magazin angestellt ist. Das Vorhandensein eines Magazins wird nicht abgefragt. In diesem Zusammenhang ist festzustellen, dass es keine Vorrichtung gibt, die einen Betrieb ohne ein angestelltes Magazin ermöglicht. Eine Begrenzung des Arbeitsbereich und der manuelle Steuerungsbetrieb mit dem Handbediengerät wird über die Kuga-Steuerung überwacht. Über die bereits verbaute SafetyBridge-V2 wird die Freigabe für den automatischen Betrieb gesetzt und die Auswertung eines lokalen Not-Halt-Schalters übernommen. Nach der Anwendernorm *DIN EN ISO 10218-2* fehlt die eindeutige Wahl der Betriebsart. Es muss einen manuellen und automatischen Betrieb geben. Das Maschinenmodul verfügt über keine sicherheitsgerichteten Sensoren zur Feststellung, ob es in eine bzw. in die Integrationsumgebung eingebracht wurde. Eine manuelle Benutzerauswahl über eine entsprechende Betriebsart steht ebenfalls nicht zur Verfügung.

2.3 Graviermaschine

Mit dieser Maschine kann eine Gravur auf ein Produkt mithilfe eines Laserstrahls erstellt werden. Die Lasereinheit wird über einen eigenen Controller gesteuert. Dieser stellt eine Schnittstelle für Sicherheitsverrieglungen zur Verfügung, über die im Notfall der Laserstrahl sicher abgeschaltet bzw. ein Shutter geschlossen werden kann. Der Shutter verschließt sicher den Laserstrahl, sodass dieser nicht zwingend ausgeschaltet werden muss. Über den sicheren Magnetsensor von Schmersal wird das korrekte Verschließen der Laserkabine durch den Werkstückträger überprüft. Zusätzlich wird über die bereits verbaute SafetyBridge-V2 ein Not-Halt-Schalter ausgewertet und in den Not-Aus-Kreis des Lasers eingebunden. Der Zugang in die Laserkabine ist nicht für anfallende Wartungsarbeiten geeignet. Eine mögliche Öffnung der Laserkabine durch Abschrauben von Seitenelementen des Gehäuses wird nicht überwacht. Beim Gravieren von verschiedenen Materialien kann es zum Funkenflug oder zur Entstehung von Dämpfen kommen. Es ist sicherzustellen, dass keine Materialien eingesetzt werden, die einen Funkenflug verursachen können, da die Dämpfe mit einer Filteranlage abgesaugt werden. Der ordnungsgemäße Betrieb dieser Anlage wird nicht überwacht. Die Maschine kann in einem manuellen oder automatischen Betrieb bedient werden. Eine eindeutige Auswahl von Betriebsarten ist nicht vorhanden. Weitere Einzelheiten sind der Risikobeurteilung von der Maschine zu entnehmen. Dieses Maschinenmodul hat weder eine Sensorik zur Bildung von gesicherten Informationen, noch eine manuelle Möglichkeit der Vorgabe über den Einsatzort und kann somit nicht die Wahl einer zugehörigen Betriebsart überprüfen. Aus diesem Grund kann nicht unterschieden werden, ob das Maschinenmodul als auswechselbare Ausrüstung bzw. integrierbare Maschine an einem kompatiblen System oder als einzelne Maschine betrieben wird. Somit können nicht entsprechende Funktionen der funktionalen Sicherheit angewählt werden.

2.4 Das SafetyBridge-System

Die SBT von Phoenix Contact ist ein sicheres proprietäres System, welches zusammen mit verschiedenen Standard-SPSen arbeitet und sicherheitsgerichtete Daten mit Hilfe des Black-Channel-Prinzips über standardisierte Bussysteme und Komponenten austauscht.

„In allen Sicherheitsanwendungen, in denen konventionelle Sicherheitsrelais zu unflexibel sind, sich eine Parallelverdrahtung aufgrund der Ausdehnung der Sicherheitskreise als zu aufwändig erweist oder der Einsatz eines sicheren Bussystems in Verbindung mit einer sicheren Steuerung aus Kostenaspekten ausscheidet, bietet sich die SafetyBridge-Technologie von Phoenix Contact als wirtschaftliche Lösung an.“ [7, S. A-1]

Eine konventionelle Realisierung des Not-Halts wäre mit Sicherheitsrelais möglich gewesen, jedoch hätte sich diese Parallelverdrahtung durch das smarte Transfersystem als sehr aufwändig erwiesen. Ein weiterer Punkt ist, dass bereits das modulare Inline-System von Phoenix Contact zum Teil in den Maschinen verbaut ist. Die Installation der SafetyBridge-Hardware erfolgt durch Anreihen an die bestehenden Inline-Stationen. Dadurch sind bei der Installation der Module, außer den Standardrichtlinien der Inline-Technologie, keine speziellen Installationsrichtlinien zu beachten. [7, S. A-1] Das SafetyBridge-System ist modular aufgebaut und kann den Anforderungen angepasst werden. Es wird mindestens ein sogenanntes Logikmodul benötigt. Dieses stellt neben acht sicheren Ausgängen eine sichere Logik zur Verfügung und ist somit die Sicherheitssteuerung. Ein solches Modul wird als Insel bezeichnet. Die Erweiterungsmodule werden über eine Adressierung diesem Logikmodul zugeordnet. Diese werden Satelliten genannt. Bevor die SafetyBridge-Module angereiht werden, sind diese über DIP-Schalter zu adressieren. Die Übertragungsgeschwindigkeit, Adresse (Inselnummer) und Satellitennummer werden eingestellt. Die Vorgehensweise ist dem Anwenderhandbuch zu entnehmen. [7]

Die Parametrierung der Ein- und Ausgänge erfolgt über die mitgelieferte Programmierumgebung SAFECONF. Es stehen sichere Bausteine und Funktionen zur Auswertung von Sicherheitseinrichtungen zur Verfügung. Es können binäre Daten zwischen der Standardsteuerung und der Sicherheitslogik ausgetauscht werden. Auf diesem Weg kann eine individuelle Statusabfrage und eine Quittierung über die Standard-Speicher programmierbare Steuerung (SPS) erfolgen oder das Zustimmprinzip für Funktionen und Ausgänge umgesetzt werden. Ein Status aller sicheren Ein- und Ausgänge und Diagnose-Daten kann mit der Standardsteuerung ausgelesen werden. Auf den SafetyBridge-Logikmodul werden die in SAFECONF konfigurierten Funktionen ausgeführt. Eine Insel kann mit 16 weiteren Modulen, die sogenannten Satelliten, erweitert werden. Dabei können verschiedene digitale Ein- und Ausgangsmodule kombiniert werden.

Die SBT ist auf eine Standardsteuerung von Phoenix Contact, Rockwell Automation, Siemens, Schneider Electric oder auf eine CODESYS-basierte Steuerung angewiesen, die den Datentransfer zwischen dem Logikmodulen und den Satelliten organisiert. Über die zur Verfügung stehenden Funktionsbausteine aus der Bibliothek von Phoenix Contact muss das Logikmodul in die Implementierung der Standardsteuerung hinzugefügt werden. Die in SAFECONF erstellte Applikation kann in das benötigte Format exportiert und als Funktionsbaustein oder als Binär-File auf das Logikmodul geladen werden.

2.4.1 Programmierumgebung SAFECONF

SAFECONF ist die kostenlose und mitgelieferte oder herunterzuladende Programmierumgebung für TriSafe und SafetyBridge, Produkte der Firma Phoenix Contact. Mithilfe dieser Programmierumgebung können die benötigten Sicherheitsfunktionen erstellt und exportiert werden. Zur Implementierung stehen folgende sichere Bausteine zur Verfügung: Anti- und Equivalent, Schützüberwachung, 3-stufiger-Zustimmschalter, Not-Halt-Auswertung, Auswertung von trennenden und berührungsloswirkenden Schutzeinrichtungen, 5-fach-Betriebsartenwahlschalter, Muting-Bausteine für Lichtschranken, Reset und Auswertung von Zweihand-Bedieneinheiten. Die Bausteine können mit einer sicherheitsgerichteten und Standard-Logik verknüpft werden. Dazu stehen folgende Funktionen zur Verfügung: TRUE und FALSE, AND und OR, Vergleich von zwei Signalen auf Un- oder Gleichheit, Trigger auf steigende oder fallende Flanke, SR- und RS-Funktion, Ein- und Ausschaltverzögerung, Pulsgeneration, Negation, Exklusiv-Oder und Verknüpfung von einem sicheren und nicht sicheren Signal nach dem Zustimmprinzip. Über Verbinder können die Netzwerke übersichtlich gestaltet werden. Ein Signal von einem Verbinder kann erst nach dem Schreiben im weiteren Verlauf der Implementierung verwendet werden. Im Weiteren stehen 16 sichere und 32 nicht sichere Ein- und Ausgänge zum Austausch von binären Signalen mit anderen Steuerungen zur Verfügung.

2.4.2 Aufbau der Querkommunikation

Mit der SBT-V3 können die Logikmodule (Inseln) untereinander 32 Signale austauschen, 16 binäre Eingangs- und 16 Ausgangssignale. Dazu müssen die Logikmodule im einem SAFECONF-Projekt eines übergeordneten Logikmoduls als Slave im Hardwareaufbau hinzugefügt und die Adresse von der Slave-Insel parametriert werden. Es kann eine hierarchische oder flache Topologie entstehen. Diese beiden Varianten können miteinander kombiniert werden. Der Aufbau des Standard-Netzwerks ist dabei zunächst nicht von Bedeutung. Bei der Ermittlung von Abschaltzeiten ist der Netzwerkaufbau und die -auslastung entscheidend. In der Dokumentation von Phoenix Contact ist die einzige Anforderung an das Netzwerk, dass es deterministisch sein muss. Auf diese Forderung wird in Kapitel 3.4 weiter eingegangen. In der Parametrierung eines Slave-Logikmoduls ist eine Watchdog-Zeit für die sicherheitsgerichtete Kommunikationsverbindung festzulegen. Vom Phoenix Contact Competence Center Safety war zu erfahren, dass die Übertragungszeit der sicheren Kommunikationsverbindung zum Slave-Logikmodul durch ein Togglebit gemessen wird, welches von dem Logikmodul zu dem Satelliten und von diesem wieder zurück zum Logikmodul geschickt wird. Daher muss die Watchdog-Zeit der Verbindung zweimal so hoch

sein wie die Übertragungs- und Verarbeitungszeit der beteiligten Standard- und Sicherheitskomponenten. Die sichere Querkommunikation wird, wie anfangs erwähnt, durch die vorhandene Infrastruktur nach dem Black-Channel-Prinzip über die Standardkomponenten ausgetauscht, siehe Kapitel 2.4.3. Es können maximal 31 SafetyBridge-Logikmodule (Inseln) in einem System verbaut werden. An eine Insel können maximal 16 weitere Satelliten angeschlossen werden. Dazu zählen neben den Erweiterungsmodulen auch Logikmodule, die als Slave der Hardwarekonfiguration im übergeordneten SAFECONF-Projekt hinzugefügt werden. Dadurch hängt die Anzahl von möglichen Querverbindungen zu anderen Inseln von der Anzahl bereits vorhandener Module ab. Über Funktionsbausteine für Standardsteuerungen wird die SBT in die Implementierung der Standardsteuerung eingebunden. Zur sicheren Querkommunikation mit hoher Verfügbarkeit kann es nur kommen, wenn die Kommunikationsverbindung zwischen den Standardsteuerungen existiert und diese eine deterministische Eigenschaft aufweist.

Bestimmung der garantierten Abschaltzeit (t_G)

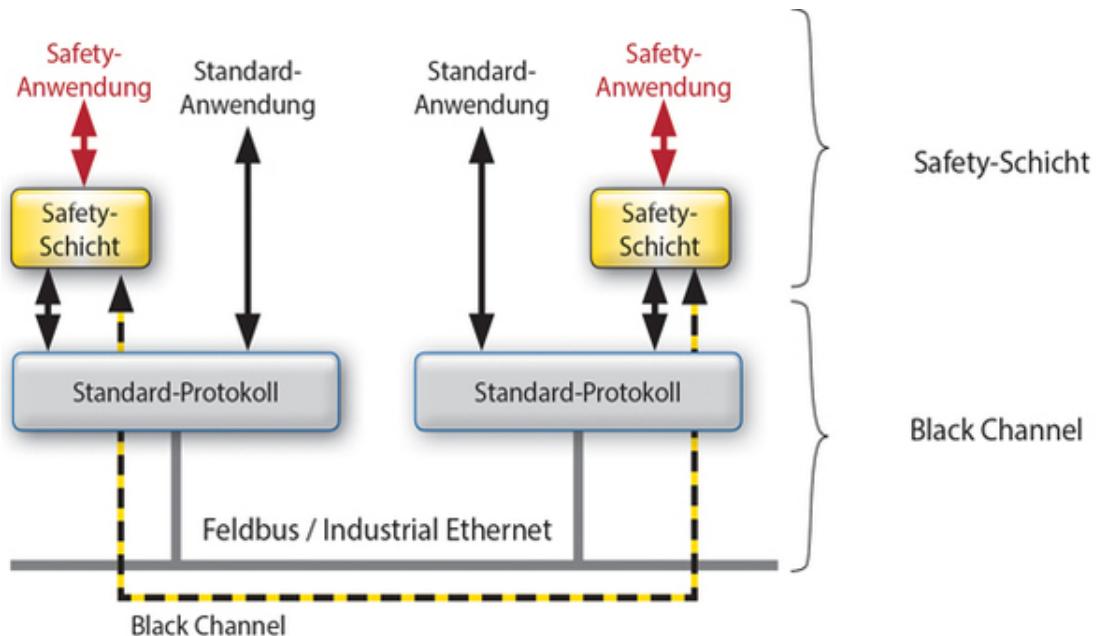
Die garantierte Abschaltzeit der SBT setzt sich aus einer Verarbeitungszeit (t_{IN}) an der Eingangsklemme, einer Übertragungszeit (t_{FWD_IN}) vom Satelliten zum Logikmodul, einer Verarbeitungszeit (t_{OUT_LPSDO}) vom Logikmodul selbst, sowie aus den parametrierten Übertagungszeiten (t_{FWD_SLb}) zu anderen Logikmodulen zusammen. Wird das Signal über Logikmodule weitergegeben, so addieren sich die Verarbeitungszeiten (t_{OUT_LPSDOa}). Von einem Logikmodul muss das Signal noch an einen Satellit mit Ausgangsklemmen weitergeben werden. Die Zeit wird mit (t_{FWD_OUT}) berücksichtigt. Zum Setzen des Ausgangs wird die Zeit (t_{OUT}) benötigt. Für einen Signalverlauf über x -Logikmodule ergibt sich die Gleichung (1) zur Bestimmung der garantierten Abschaltzeit (t_G) der SBT.

$$t_G = t_{IN} + t_{FWD_IN} + x \cdot t_{OUT_LPSDO} + \sum_{n=1}^x t_{FWD_SLn} + t_{FWD_OUT} + t_{OUT} \quad (1)$$

2.4.3 Black-Channel-Prinzip

Das Black-Channel-Prinzip kapselt den Teil für die Ausführung einer Sicherheitsfunktion von den Standardfunktionen ab. Übertragen auf ein Kommunikationssystem bedeutet das, dass alle bisher benötigten Hardwarekomponenten, Protokolle und Dienste für die Vernetzung von Automatisierungskomponenten als ein nicht weiter spezifizierter Kommunikationskanal zusammengefasst werden. Beim Analysieren von Zusammenhängen wird ein ähnliches Prinzip benutzt, welches bestimmte Zusammenhänge zur vereinfachten Betrach-

tung als *Black Box* zusammenfasst. Beim Black-Channel-Prinzip werden alle Schichten des OSI-Referenzmodells zusammengefasst und darüber wird eine *Safety-Schicht* (eine Sicherheitskommunikationsschicht) eingefügt. Das Protokoll, welches diese Schicht darstellt, muss die Anforderungen der *IEC 61784-3* erfüllen und die geforderten Maßnahmen zur Sicherstellung der erforderlichen Übertragungsgüte einhalten. „Dieses Prinzip ist mit Zertifizierern wie dem TÜV gemeinsam ausgearbeitet, wissenschaftlich fundiert untersucht und gut abgesichert. Auf diese Weise macht eine zusätzliche Safety-Schicht oberhalb des Black-Channel aus einem Standard-Feldbus oder einer Standard-Industrial-Ethernet-Lösung ein System, mit dem sich zuverlässig Daten für die funktionale Sicherheit übertragen lassen.“ [8] Das Gegenteil von dem Black-Channel-Prinzip wäre das White-Channel-Prinzip. Dabei wird der gesamte Kommunikationsweg als sicheres System betrachtet und dieser muss die Anforderungen der *IEC 61508* erfüllen. [9]



Quelle: [8]

Abbildung 1: Beim Black-Channel-Prinzip setzt die Sicherheitsfunktion als eigene *Safety-Schicht* auf dem eigentlichen Übertragungsmedium auf

2.5 Vernetzung der Maschinen

In Kapitel 3.4 wird ein deterministisches Netzwerk gefordert. Zum Verständnis wird diese Begrifflichkeit nachfolgend näher spezifiziert. Ausgehend von einer allgemeinen Definition

von Determinismus aus dem Duden, wird diese auf maschinennahe Vernetzung übertragen. In diesem Zusammenhang werden kurz einige Sachverhalte als Grundlage erläutert.

„Lehre, Auffassung von der kausalen [Vor]bestimmtheit allen Geschehens bzw. Handelns“

Übertragen auf eine Netzwerktechnologie kann die Definition folgendermaßen aufgefasst werden: Das Verhalten der Vernetzung ist insbesondere für zukünftige Ereignisse bestimmbar. Dies gilt vor allem für das zeitliche Verhalten der benutzen Technologie. Diese Eigenschaft bringt das eingesetzte Medium *Ethernet* nach IEEE 802.3x zunächst nicht mit sich. Ein Grund dafür ist, dass der Buszugriff mit dem zufälligen und nicht deterministischen Carrier Sense Multiple Access/Collision Detection (CSMA/CD)-Verfahren nach IEEE 802.3 erfolgt. Über eine Prüfsumme vom User Datagram Protocol (UDP) werden verfälschte Daten detektiert und in Folge dessen verworfen. Es werden nur korrekt übertragene Daten weiterverarbeitet, was als Datenkonsistenz aufzufassen ist. Durch das zyklische Senden der Daten kann auf ein erneutes Senden im Fehlerfall verzichtet werden. Ein bestätigter Dienst könnte dazu führen, dass veraltete Prozessdaten übertragen werden. Mit dem UDP in Kombination mit dem Internet Protocol (IP) oder durch den Einsatz von PROFINET kann das Medium Ethernet neben der Datenkonsistenz auch eine weiche Echtzeitfähigkeit erlangen. Dabei weisen die beiden Protokolle UDP/IP und PROFINET-RT einen Unterschied auf. Bei PROFINET-RT wird eine Überwachungszeit und Aktualisierungszeit der Prozessdaten vorgeben. Die Länge der Prozessdaten ist vorgegeben und kann nicht während der Laufzeit verändert werden. Um das Ethernet-basierte Netzwerk weiter bestimmbarer zu machen, ist es hilfreich, den physikalischen Aufbau und mögliche Änderungen an diesen zu kennen und zu berücksichtigen. Durch den Einsatz von managed Switches kann ein Ethernet-basiertes Busprotokoll, wie PROFINET, bevorzugt werden. Schwankungen in der Laufzeit von Datenpaketen werden weiter reduziert und das zeitliche Übertragungsverhalten wird vorhersehbarer. Mit diesen Hilfen kann in einem Ethernet-basierten Netzwerk ein Determinismus mit vorhersehbaren Toleranzen entstehen. Weitere Schritte wie Messung von Übertragungs- und Verarbeitungszeiten zwischen den Netzwerkeinheiten zur Zeitsynchronisation ermöglichen harte Echtzeitanforderungen über ein Ethernet-basiertes Netzwerk.

2.6 Normen und Richtlinien

In der Studienarbeit stellte sich mit dem Interpretationspapier [10] vom Bundesministerium für Arbeit und Soziales (BMAS) zum Thema Gesamtheit von Maschinen heraus, dass das wandlungsfähige Montagesystem keine Gesamtheit von Maschinen bildet. Voraussetzung

ist, dass sich kein produktionstechnischer und sicherheitstechnischer Zusammenhang bildet. Ausnahme ist zur Auswertung des Not-Halts eine übergeordnete Auswerteeinheit. Im Weiteren wurde die Anlage als integriertes Fertigungssystem nach *DIN EN ISO 11161* betrachtet. [11] Die zur Integration geeigneten Maschinen wurden im Positionspapier vom TÜV Süd auch als Maschinenmodule aufgefasst. [12]

Die CE-Konformität kann auch über die direkte Erfüllung der MRL nachgewiesen werden. Diese gilt nicht nur für Maschinen, sondern auch für auswechselbare Ausrüstungen, die in Artikel 2b) der MRL 2006/42/EG wie folgt definiert sind:

„[...]eine Vorrichtung, die der Bediener einer Maschine oder Zugmaschine nach deren Inbetriebnahme selbst an ihr anbringt, um ihre Funktion zu ändern oder zu erweitern, sofern diese Ausrüstung kein Werkzeug ist“ [13, Artikel 2b])

Diese Beschreibung trifft auf die Maschinen zu, die an das smarte Transfersystem gestellt oder von diesem abgezogen werden. Aus diesem Grund kann ein Maschinenmodul auch als wechselbare Ausrüstung aufgefasst und behandelt werden. „Es ist nicht gefordert, dass eine auswechselbare Ausrüstung die Definition für Maschinen erfüllen muss.“ [14] Nach Artikel 2 der MRL ist eine auswechselbare Ausrüstung in einem weiter gefassten Sinne der Richtlinie eine Maschine. Somit ist diese als separates Produkt zu betrachten. „Der Hersteller muss im Rahmen der Sicherheits- und Gesundheitsanforderungen nach Anhang I der MRL nicht nur die Ausrüstung selbst, sondern auch deren Zusammenwirken mit der Grundmaschine berücksichtigen.“ [14]

Die auswechselbare Ausrüstung soll auch einzeln betrieben werden. Dabei ergibt sich eine weitere Maschinenart, die erneut mit der MRL oder mit harmonisierten Normen zu bewerten ist. Aufgrund der verschiedenen Einsatzmöglichkeiten ergeben sich unterschiedliche Funktionsweisen und ein vielfältiger bestimmungsgemäßer Gebrauch. Dabei können sich die Sicherheits- und Gesundheitsanforderungen ändern. Dies kann zur Folge haben, dass sich ein anderes Konformitätsbewertungsverfahren ergibt. Die in dieser Bachelorarbeit betrachteten Maschinen, im engeren und weiter gefassten Sinn der MRL, stellen keine Übereinstimmung mit den in Anhang IV beschriebenen Maschinen dar. Dies ist für die nachfolgenden Anforderungen (siehe 3.5) entscheidend.

3 Anforderungen

In diesem Kapitel werden die Erkenntnisse aus dem Kapitel 2 mit messbaren Kriterien zu Anforderungen formuliert. Mithilfe dieser wird anschließend in Kapitel 4 ein Konzept ausgearbeitet und implementiert. Das zu erstellende Konzept muss die zutreffenden Anforderungen aus den harmonisierten Normen *ISO 12100*, *ISO 13849*, *ISO 13850* erfüllen. In Abhängigkeit von der Funktionsweise kann ein Maschinenmodul unterschiedlich betrachtet werden. Es ergeben sich unterschiedliche Beschreibungen des bestimmungsgemäßen Gebrauchs. Jede Funktionsweise stellt eine eigene Betriebsart dar. Für jedes Maschinenmodul muss es in jeder Betriebsart einen automatischen und manuellen Betrieb geben. Ein Maschinenmodul ist als eigenständige Maschine anzusehen, daher muss es auch einzeln, ohne Integration in ein System, ohne erhöhtes Risiko funktionieren. Dafür ist eine eigene Betriebsart vorzusehen. Im Weiteren kann die Maschine an einem kompatiblen System (Integrationsumgebung) betrieben werden. Das Maschinenmodul ist dabei als integrierbare Maschine nach *ISO 11161* oder als wechselbare Ausrüstung nach der MRL zu betrachten. Es ist eine der zwei Betrachtungsarten auszuwählen und für diese eine weitere Betriebsart am Maschinenmodul vorzusehen.

3.1 Smartes Transfersystem

Im Kapitel Stand der Technik wurde bereits festgestellt, dass keine zusätzliche Schutzmaßnahme am Transfersystem vorhanden ist, daher ist diese durch zusätzliche Not-Halt-Schalter an den Bändern vom Transfersystem nachzurüsten. Vor allem an der Produktentnahme und an dem Integrationsplatz für ein Handarbeitsmodul sind Not-Halt-Schalter für die zusätzliche Schutzmaßnahme zu installieren. In der Studienarbeit wurde unter Berücksichtigung des aktuellen Regelwerks festgelegt, dass deren Betätigung das Abschalten des gesamten Transfersystems und alle mit ihr verbundenen Maschinenmodule zur Folge hat. In der *DIN EN ISO 13850* ist keine Aussage zu einer Reaktionszeit getroffen worden. Es ist jedoch zu entnehmen, dass die Not-Halt-Funktion zu jedem Zeitpunkt verfügbar und funktionsfähig sein muss. Als ein Maß für eine angemessene Verfügbarkeit wird in dieser Bachelorarbeit eine Worst-Case-Reaktionszeit bzw. garantierte Abschaltzeit (t_G) der SBT von kleiner als 350 ms festgelegt.

Um eine Erwartungshaltung aufbauen zu können, muss das smarte Transfersystem zu jedem Zeitpunkt sicher erkennen können, wie viele Maschinenmodule an den vorgesehenen Plätzen angestellt wurden. Zur Erfüllung der in dieser Bachelorarbeit gestellten Ziele genügt diese Anforderung. Für weitere Sicherheitsanforderungen kann auch die Beantwortung der anderen Fragestellungen aus Kapitel 2.1 erforderlich sein. Dies ist bei der Erfassung

von angeschlossenen Maschinen nach Möglichkeit zu berücksichtigen. Die gewonnene Information über die Anzahl der integrierten Maschinen ist mit weiteren Signalen und Eingaben zu plausibilisieren. Das Hinzufügen und Entfernen von Maschinen muss eine bewusste Handlung sein.

3.2 Robotermontagemaschine

Die Aktivierung und Deaktivierung von Sicherheitseinrichtungen erfolgt in Abhängigkeit der Funktionsweise und somit der gewählten Betriebsart. Um die Wahl der Betriebsart zu plausibilisieren ist über sichere Sensoren festzustellen, ob sich dieses Modul wirklich im Einzelbetrieb befinden kann. Das Hinzufügen an das Transfersystem oder das Entfernen davon muss vom Maschinenbediener bewusst ausgelöst werden. Eine weitere Anforderung an dieses Maschinenmodul ist, dass es das Not-Halt-Signal des smarten Transfersystems sicherheitsrelevant weiterverarbeiten kann. In der Studienarbeit wurde bereits festgestellt, dass der Zugang in den geschützten Bereich mit einem Türschalter nach dem Vier-Stufen-Modell zu realisieren ist. [6, S. 37] Der Zugang in vier Stufen ist in der Norm *DIN EN ISO 14119:2014-03* beschrieben. Der Türschalter muss daher über eine Prozess- und Positionsüberwachung verfügen. Aus diesem Grund fällt die Reaktionszeit der lokalen Sicherheitssteuerung nicht ins Gewicht. Die Sicherheitssteuerung muss mindestens PL d mit einer Struktur der Kategorie 3 oder SIL 2 zertifiziert sein, weitere Leistungsanforderungen sind in der *DIN EN ISO 10218-2* in Abschnitt 5.2 beschrieben. [15, S. 17] Die Wahl der Betriebsart darf nur von einem bestimmten Personenkreis vorgenommen werden. Es sind die risikomindernden Schutzmaßnahmen der Risikobeurteilung umzusetzen, die über eine Sicherheits-SPS ausgewertet werden. Entsprechend der gewählten Betriebsart ist die Sicherheits-Schnittstelle X11 der Kuka-Robotersteuerung auszuwerten und anzusteuern. Es ist sicherzustellen, dass der Roboterarm im Fehlerfall nicht den geschützten Bereich überschreiten kann. Für einen möglichst großen Arbeitsraum des Roboters ist die trennende Schutzmaßnahme so auszulegen, dass diese nicht vom Roboter durchdrungen werden kann.

3.3 Gravurmaschine

Wie bei der Robotermontagemaschine steht die De- und Aktivierung von Sicherheitseinrichtungen im Zusammenhang mit der gewählten Betriebsart; daher ist auch an dieser Maschine die gewählte Betriebsart mit weiteren sicheren Sensoren zu verifizieren. Das Hinzufügen und Entfernen vom Transfersystem muss eine bewusste Handlung sein. Die Maschine muss das Not-Halt-Signal vom smarten Transfersystem weiter verarbeiten können. Die Studienarbeit setzt eine Worst-Case-Reaktionszeit der Steuerung von 50 ms voraus,

um den Laserstrahl im Fehlerfall rechtzeitig abschalten zu können. [6, S. 39] Es sind die risikomindernden Schutzmaßnahmen der Risikobeurteilung umzusetzen, die von einer Sicherheits-SPS ausgewertet werden müssen. Daraus gehen die einzelne Forderungen hervor, wie beispielsweise die Sicherstellung, dass nur graviert werden kann, wenn die Absaugung ordnungsgemäß funktioniert. Weitere Punkte können die Zugänge in die Maschine bzw. in die Laserkabine sein. Die Zugänge müssen überwacht und für die anfallenden Aufgaben geeigneten sein.

3.4 Anforderungen von der SafetyBridge-Technologie

„An die Standard-Steuerung stellt das SafetyBridge-System keine besonderen Anforderungen. Folgende Aufgaben muss sie jedoch erfüllen können:

Netzwerk:

- Deterministisches Netzwerk

Steuerung:

- Schnell genug, um Zeiterwartungen für Reaktionszeit erfüllen zu können
- Speicher muss groß genug sein, um den Konfigurations- und Parameterdatensatz speichern zu können
- Sicherstellen der Datenkonsistenz über 24 Worte.“ [7, A 2.2]

Diese Anforderungen sind aus dem SafetyBridge-Handbuch übernommen und mit dem Stand der Technik aus Kapitel 2.5 auf Seite 9 näher spezifiziert worden. Der maximale Netzwerkaufbau des wandlungsfähigen Montagesystems ist abzuschätzen und festzulegen. Dabei ist die Wandlungsfähigkeit des Montagesystems zu berücksichtigen. Es ist eine Überwachungszeit für die sichere Querkommunikation zu ermitteln. Bei den bereits verbauten Standardsteuerungen ist davon auszugehen, dass diese die Anforderungen bereits erfüllen können. Die Inseln der SBT müssen eindeutig adressiert werden. Die Vergabe von Inselnummern erfolgt über DIP-Schalter. Ein zu erstellendes Adressierungskonzept soll verhindern, dass es mehrere Maschinenmodule mit der gleichen Inselnummer integriert sind.

3.5 Normative Anforderungen

Auf ein Maschinenmodul, auch integrierbare Maschine genannt, ist die in der MRL 2006/42/EG unter Artikel 2b) zu findende Beschreibung einer auswechselbaren Ausrüstung zutreffend. In der Betriebsart *wechselbare Ausrüstung* ist ein Maschinenmodul als Maschine im weiteren Sinne der MRL aufzufassen. Daher müssen die Maschinenmodule sowohl in dieser Betriebsart als auch im Einzelbetrieb die zutreffenden Pflichten der MRL

erfüllen. In beiden Fällen müssen die grundlegenden Sicherheits- und Gesundheitsschutzanforderungen erfüllt werden. Bei einer auswechselbaren Ausrüstung muss nicht nur die Ausrüstung selbst, sondern auch das Zusammenwirken mit der Grundmaschine betrachtet werden. In dieser Bachelorarbeit werden die Maschinenmodule als integrierbare Maschinen gemäß *DIN EN ISO 11161* betrachtet. Es sind die risikomindernden Maßnahmen der vorausgegangenen Risikobeurteilung nach *DIN EN ISO 12100* umzusetzen. Im Rahmen dieser Bachelorarbeit sind hauptsächlich die risikomindernden Maßnahmen mit einem steuerungstechnischen Zusammenhang zu realisieren. Bei der Gestaltung des modularen Not-Halts sind die harmonisierten Normen *DIN EN ISO 13850* und *DIN EN ISO 11161* zu erfüllen. So kann das Konformitätsverfahren vereinfacht werden.

4 Konzept

In diesem Kapitel wird ein Konzept erstellt, welches die Anforderungen aus Kapitel 3 erfüllt. Dabei wird die in der Studienarbeit ausgewählte SafetyBridge-Technologie (SBT) berücksichtigt. Der Schwerpunkt dieses Konzept liegt in der steuerungstechnischen Umsetzung eines Sicherheitskonzepts für ein modulares Anlagendesign, welches anhand des wandlungsfähigen Montagesystems der SmartFactoryOWL erprobt wird.

4.1 Funktionsweise der Sicherheitseinrichtungen

Davon ausgehend, dass die Steuerungen fehlerfrei anlaufen und sich in den erwarteten Betriebszuständen befinden, ist zunächst der Anlauf an dem smarten Transfersystem zu quittieren. Danach muss jede Maschine einzeln quittiert werden und anschließend der automatisierte Produktionsablauf gestartet werden. Ein separates Quittieren an den integrierten Maschinen verhindert den automatischen Wiederanlauf vom Maschinenmodul. Kann sichergestellt werden, dass von einem automatischen Wiederanlauf keine Gefährdung ausgeht, kann von einer erneuten Quittierung abgesehen werden. Dies ist entsprechend in der Standard-Implementierung zu berücksichtigen. Die Produktion startet mit dem letzten Schritt, dem Starten der Bänder vom Transfersystem. Die wesentlichen Schritte sind als Programmablaufplan in Abbildung 2 dargestellt.

Durch die Wahl von *Maschine hinzufügen* werden die Plausibilitätsverknüpfungen verändert und eine Maschine kann ohne einen Produktionsstopp in die Integrationsumgebung eingebracht werden. Für diesen Vorgang steht ein angemessener Zeitraum zur Verfügung. Danach wird der Aufbau der Querkommunikationen automatisch ausgelöst und die Veränderung der Plausibilitätsverknüpfungen zurückgesetzt. Das Abmelden einer Maschine erfolgt an der betreffenden Maschine. Erneut wird für eine festgelegte Zeit die Plausibilitätsverknüpfungen verändert. Im Fehlerfall geht das System in den zugehörigen sicheren Zustand. Der Not-Halt an den verbleibenden integrierbaren Maschinenmodulen bleibt aktiv und wird nicht überbrückt. Nach *DIN EN ISO 13850:2014-06* Abschnitt 4.3.7 müssen aktivierte Not-Halt-Schalter zu erkennen sein. Dies ist mit einem beleuchteten Not-Halt-Schalter zu berücksichtigen.

Die Freigabe zur Produktion, welche nur im ordnungsgemäßen Betrieb erteilt werden kann, erfolgt in jeder Maschine. Im integrierten Betrieb ist eine entscheidende Bedingung das Vorhandensein des Not-Halt-Signals der anderen Maschinen. Dieses Signal wird über die sicherheitsgerichtete Querkommunikation der SafetyBridge übertragen. Die Quittierung von Fehlern erfolgt am betroffenen Maschinenmodul. Durch das Aufleuchten des Quittierungstasters wird die Quittierung angefordert. Die Betätigung des Quittierungstasters wird

über die Integrationsumgebung sicherheitsgerichtet an die integrierten Maschinenmodule verteilt. So kann das Fehlen des externen Not-Halts-Signals quittiert werden.

4.2 Aufbau der Hardware

Jedes Maschinenmodul wird mit einem Logikmodul der SafetyBridge-Technologie-V3 angepasst. Die Logikmodule werden dem Logikmodul vom Transfersystem hierarchisch untergeordnet. Mithilfe der sicherheitsgerichteten Querkommunikation werden binäre Signale zwischen den sicherheitsgerichteten Logikmodulen ausgetauscht und verarbeitet. Die Master-Logik für das Transfersystem wird als Insel 31 adressiert. Die Adressierung der Logikmodule von den Maschinenmodulen erfolgt der Reihe nach von eins bis sieben. Dieses Adressierungsschema ist beim Erweitern der Sammlung von kompatiblen Maschinen fortzusetzen, damit eine doppelte Adressierung ausgeschlossen werden kann.

4.3 Querkommunikation

Nach Ablauf der Zeit, die für das Hinzufügen einer Maschine vorgesehen ist, wird die sicherheitsgerichtete Querkommunikation zwischen Master und Slaves erneut aktiviert. Das als Slave eingebundene Logikmodul überträgt mit dem ersten Bit der Querkommunikation ein Lebenszeichen, auch Lebend- oder Livebit genannt. Ein solches Livebit erhält auch die integrierte Maschine vom Master, über das erste Bit. Mit dem zweiten Bit wird der Zustand des Not-Halts weiter gegeben und empfangen. Dies gilt für die Maschinenmodule sowie für das Transfersystem. Durch eine Auswertung in der übergeordneten Logik wird der Status des Not-Halts von allen Maschinen ausgewertet und an diese wieder zurückgegeben. Da es sich hier um eine zertifizierte Übertragung handelt, wird kein weiteres Bit zum Überprüfen benötigt. Im Fehlerfall fällt dieses ab und die Maschinen gehen in einen sicheren Zustand. Das dritte Bit überträgt das Abmeldesignal des jeweiligen Maschinenmoduls. Dies verändert für eine gewisse Zeit die Plausibilitätsverknüpfungen am Master. Dadurch kann eine Maschine entfernt werden, ohne dass die gesamte Produktion an dem System gestoppt werden muss. Wird an einer weiteren Maschine der Not-Halt betätigt, so wird das System dennoch in einen sicheren Zustand versetzt. Durch die Veränderung der Plausibilitätsverknüpfungen werden nicht alle Not-Halt-Signale ignoriert werden.

Abbruch der Querkommunikation

Die Verfügbarkeit der Querkommunikation wird fortlaufend innerhalb der SBT überwacht und darf die parametrierte Sicherheitszeit (F-Watchdog-Zeit) nicht überschreiten. Wird diese überschritten, werden alle übertragenen Signale der Querkommunikation abgeschaltet.

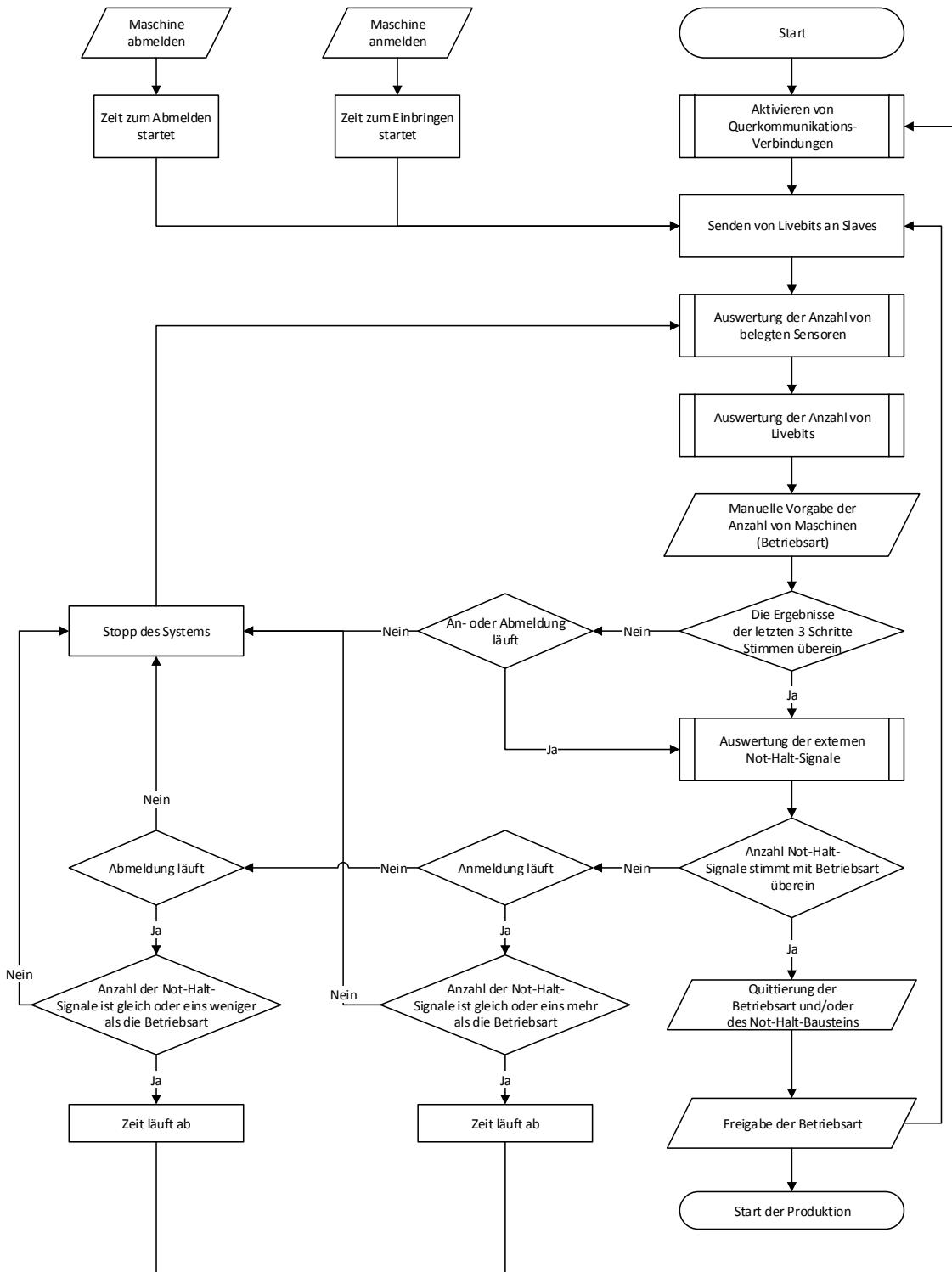


Abbildung 2: Programmablaufplan der Sicherheitssteuerung im Transfersystem (Master)

Das Not-Halt-Signal und Livebit fallen ab und ein Kommunikationsfehler kann zwischen den beiden Maschinen ausgewertet werden. Durch eine bewusste Handlung am Transfersystem kann die Verbindung neu aufgebaut werden. Da das Not-Halt-Signal abfällt, ist nach dem Aktivieren der Verbindung wie beim Betätigen eines Not-Halt-Schalters vorzugehen.

4.4 Plausibilisierung

Mithilfe von sicheren Magnetsensoren in der Arretierung an den Integrationsplätzen wird in dem übergeordneten Logikmodul des Transfersystems ausgewertet, wie viele Plätze belegt sind. Zur Überprüfung wird die Anzahl von angeschlossenen Maschinen anhand der Auswertung von den Livebits vorgenommen. Stimmen diese beiden ermittelten Anzahlen mit der vom Maschinenbediener vorgegeben Anzahl überein, so kann diese als plausibel angenommen werden und die ausgewählte Betriebsart aktiviert werden. Somit wurde nun dreimal die Anzahl von angeschlossenen Maschinen ermittelt. Damit kann eine plausible Erwartungshaltung aufgebaut werden, über die entschieden werden kann, wie viele Not-Halt-Signale von den integrierten Maschinenmodulen zu erhalten sind. Diese werden über die Querkommunikation der SBT ausgetauscht. Stimmt die Anzahl von Not-Halt-Signalen nicht mit der Erwartungshaltung überein, wird das Not-Halt-Signal zu den Slaves abgeschaltet und die Maschinenmodule gehen in den hinterlegten sicheren Zustand. Während eine Maschine an- oder abgemeldet wird, wird die Plausibilisierung durch ein internes Signal für eine bestimmte Zeit verändert. Dabei darf sich die Anzahl an Livebits und Not-Halt-Signalen nur um ein Signal verändern, anderenfalls wird das gesamte Montagesystem in einen sicheren Zustand versetzt. Passen die ermittelten Anzahlen nicht zueinander, kann das System nicht in Betrieb genommen werden. Durch ein längeres Drücken des Quittierungstasters am Transfersystems wird der Verbindungsauflaufbau erneut ausgelöst.

Eine weitere Plausibilisierung wird in jedem Maschinenmodul vorgenommen. Wie bereits erwähnt, erhält das Maschinenmodul ein Livebit von dem übergeordneten Logikmodul. Mit einem sicheren magnetischen Sensor an dem Maschinenmodul wird abgefragt, ob die Maschine mit einer anderen verbunden ist. Die Auswertung von Magnetsensor und Livebit erfolgt in dem Logikmodul des jeweiligen Maschinenmoduls. Über einen Schlüsselschalter ist die entsprechende Betriebsart auszuwählen. Stimmen die drei Signale, Livebit, Sensor und Betriebsart überein, kann in der angewählten Betriebsart der manuelle oder automatisierte Betrieb gestartet werden.

4.5 Weitere Funktionen

Verhalten vom Not-Halt

Das Betätigen eines Not-Halts wird von der SafetyBridge-Insel der jeweiligen Maschine mit dem Ergebnis verarbeitet, dass die Maschine direkt sicher gestoppt wird. Infolgedessen fällt das zweite Bit der Querkommunikation ab. Die Auswertung in der Mastersteuerung stellt das Fehlen fest und löst an den verbunden Maschinen durch die Wegnahme des zweiten Bits der Querkommunikation den sicheren Halt aus. Nach der Fehlerbehebung wird an der auslösenden Maschine auch die Quittierung des Fehlers durchgeführt. Ist die richtige Betriebsart noch ausgewählt, kann durch die mehrmalige Betätigung des Quittiertasters die Produktionsfreigabe wieder erlangt werden. Dies wird mithilfe der Querkommunikation über das Transfersystem zu den angeschlossenen Maschinenmodulen weitergegeben. Somit ist ein automatischer Wiederanlauf aus steuerungstechnischer Sicht denkbar. Möglicherweise können dadurch Gefährdungen entstehen. Befindet sich ein Maschinenmodul an dem Transfersystem, welches nicht in der zugehörigen Betriebsart ist, kommt es ebenso zu einem Not-Halt.

Auslösen von Sicherheitseinrichtungen

Das Auslösen von Sicherheitseinrichtungen, wie zum Beispiel bei der Verletzung eines geschützten Bereichs, führt nicht zu einem Stopp des gesamten Systems. Nur die betroffene Maschine wird angehalten. Dieses Verhalten ist im Zusammenhang mit den vor- und nachgelagerten Prozessen zu sehen. An dem wandlungsfähigen Montagesystem sind die Prozesse bedingt entkoppelt, da auf einer Baugruppe vom Transfersystem bis zu 10 kg aufgestaut werden können. Eine weitere Möglichkeit ist, dass bei einem lokalen Maschinenstopp und somit einer nicht verfügbaren Maschine die Produktträger vorbei an dieser weiter transportiert werden. Dabei handelt es sich um eine Funktion, die nicht sicherheitsgerichtet ausgeführt werden kann, jedoch im Sicherheitskonzept betrachtet werden muss. Für dieses Verhalten wird von der Standardsteuerung der Status der lokalen Sicherheitssteuerung entsprechend ausgewertet und weiterverarbeitet. Bei einem Stopp des automatisierten Produktionsablaufs an einem einzelnen Maschinenmodul, entsteht die gleiche Situation wie oben beschrieben und ist entsprechend zu lösen.

4.6 Testaufbau

Um sich mit der Funktionsweise von der SBT vertraut zu machen, ist ein Testaufbau zu erstellen. Dieser soll das smarte Transfersystem und zwei Maschinenmodule simulieren. Dazu

können Steuerungen wie folgt auf ein Montagegitter montiert werden. Eine RFC 470 PN ist bereits im Transfersystem des Montagesystems verbaut und kann auch am Montagegitter eingesetzt werden. Mit zwei PROFINET-Buskopplern sind zwei Inline-Stationen zu erstellen. Eine repräsentiert einen Not-Halt an einer Baugruppe vom Transferband und besteht aus einem sicheren Eingangsmodul mit acht Eingängen. Die andere ist später im Schaltschrank verbaut und besteht aus einem SafetyBridge-Logikmodul und zwei sicheren Eingangsmodulen. Der Aufbau der beiden zu simulierenden Maschinenmodule ist am Testaufbau steuerungstechnisch identisch und besteht jeweils aus einer ILC 330 PN SPS, einem Logikmodul und aus zwei sicheren Eingangsmodulen mit jeweils acht Eingängen. Zur Bedienung sind Bedienflaschen über Steckverbindungen an den Testaufbau zu montieren. Die Spannungsversorgung der Steuerungen erfolgt über diese Steckverbindung. Dadurch kann das Abziehen bzw. Anstecken der Bedienflasche das Entfernen bzw. Hinzufügen von Maschinenmodulen simulieren. Mithilfe einer Prozesssimulationsplatine ist das wandlungsfähige Montagesystem zu visualisieren. Neben jeweils drei Leuchtdioden für den Status der zugehörigen Maschine sind auch DIP-Schalter vorzusehen, womit verschiedene Sensoren simuliert werden können. Mit einem Engineering-Tool von EPLAN wurde der Testaufbau geplant, indem der zugehörige Stromlaufplan für die Verdrahtung und der Aufbauplan für die Montage erstellt wurde. Abbildung 3 zeigt ein Foto von dem Testaufbau.



Abbildung 3: rechts: Transfersystem; links oben: Maschinenmodul 1; links unten: Maschinenmodul 2

5 Implementierung

In diesem Kapitel wird die Umsetzung des Konzepts aus Kapitel 4 beschrieben. Außerdem wird auf Herausforderungen eingegangen, die sich bei der Erstellung von Sicherheitsfunktionen zeigten. Die Implementierung der Sicherheitsfunktionen erfolgte über die kostenlose und zugehörige Programmierumgebung SAFECONF. Wie bereits in Kapitel 2.4 beschrieben wurde, ist die SafetyBridge-Technologie (SBT) mithilfe der Bibliothek *SBT_V3_V1_00* in die Steuerungen von Phoenix Contact integriert worden.

5.1 SafetyBridge in ein PC-WORX-Projekt

Die Bibliothek *SBT_V3_V1_00* wurde von der Phoenix Contact Homepage heruntergeladen, mit PC-Work geöffnet und kompiliert. Im nächsten Schritt wurden die PC-WORX-Projekte um die Funktionen der SBT erweitert. Der zentrale *Operate*-Baustein ist aus der oben genannten SafetyBridge-Bibliothek entnommen worden. Für diesen und für alle weiteren Bausteine aus der Bibliothek wurden Variablen mit den dokumentierten Datentypen angelegt. Der Name wurde gleich den Ein- bzw. Ausgangsbezeichnungen des Funktionsbausteins gewählt, ergänzt mit einem Index der Inselnummer. Nach dem Aktivieren dieses Bausteins kann der Status vom Logikmodul ausgewertet werden. Auf einige Besonderheiten, auf die beim Anlegen der Variablen zu achten ist, wird im Folgenden eingegangen. Die Vorgabe der Inselnummer sollte sich zur Laufzeit nicht ändern und ist als Konstante angelegt worden. Alle Bausteine der SafetyBridge-Bibliothek werden in eine Austauschstruktur eingebunden.

Die Variablen *arrSBTOnlCntrlBuf* und *arrSBTOnlValBuf* an den Ein- und Ausgängen des *Operate*-Bausteins müssen global angelegt werden und in das Prozessdatenverzeichnis (PDD) geschrieben werden. Dies erfolgt beim Anlegen der Variablen durch die Auswahl der entsprechenden Option. Damit können später in SafeProg die Onlinewerte der Sicherheitssteuerung angezeigt werden. Der Ausgang *arr_wSBTdiagCode* kann mit dem Bibliotheksbaustein *SBT_V3_DiagCode_V1_00* ausgewertet werden. Somit kann der Status von jeden einzelnen SafetyBridge-Satelliten ausgelesen werden. Erfordert ein Satellit eine Quittierung, erfolgt dies über den Bibliotheksbaustein *SBT_V3_arrAckBuff_V1_00*, der mit dem Eingang *arrAckBuff* vom Operate-Baustein verbunden ist. Zusätzlich gibt es noch eine Bediener-Quittierung, mit der bestimmte Hardware-Fehler, wie beispielsweise ein Kommunikationsfehler der Querverbindung, quittiert werden können. In jeweils einem Doppelwort werden die 32 nicht sicheren Bits ausgetauscht. Zur besseren Handhabung ist es von Vorteil, einen Funktionsbaustein zu erstellen, der das jeweilige Doppelwort auf einzelne Bits auftrennt bzw. die 32 Bits zu einem Doppelwort zusammenfasst. Ist in der

sicheren Parametrierung des SafetyBridge-Ausgangs die Zustimmung aktiviert, kann diese über den Eingang *arr_wOutData* des Operate-Bausteins zugeführt werden. Diese Variable ist ein Array von Datentyp Wort mit 17 Einträgen. Jedem möglichen Satellit ist ein Wort zugeordnet. In dem zutreffenden Wort muss das passende Bit für den einen Ausgang von dem einem bestimmten Satelliten gesetzt werden. Zur Vereinfachung sind entsprechende Funktionsbausteine zu erstellen, die das benötigte Bit an die entsprechende Stelle schreiben. Die direkte Zustimmung über die Hardware kann zu Fehlern führen, falls der Ausgang ein Sicherheitsrelais ansteuert und die korrekte Funktionsweise von diesem überwacht wird. Der Ausgang vom Baustein zur Relaisüberwachung wird gesetzt und erwartet entsprechend der eingestellten Toleranzzeit das Kontrollsignal zur Überwachung. Dies bleibt aus, da der Ausgang bei fehlender Zustimmung nicht in der Peripherie/Hardware gesetzt wurde.

5.2 Aufbau der Querkommunikation

Für den Aufbau der Querkommunikation wird mit dem *CrossComm*-Baustein ein Array von Austauschstrukturen erstellt. An diesem Baustein ist die maximale Anzahl von vorhanden SafetyBridge-Inseln anzugeben. Die Anzahl ist wichtig, wenn mehrere Inseln von einer Steuerung verwaltet werden. Jedem Logikmodul ist an seinem zugehörigen Operate-Baustein ein Element des Arrays zuzuordnen. Die sicherheitsgerichtete Querkommunikation zwischen den Logikmodulen, die von einer Steuerung bedient werden, ist aufgebaut.

Das wandlungsfähige Montagesystem besteht aus einzelnen vollständigen Maschinen. Aus diesem Grund ist jedes Logikmodul an einer anderen Inline-Steuerung von Phoenix Contact angereiht. Dafür reicht die bereits erstellte Querkommunikation nicht aus und das Projekt der Standard-Steuerung muss mit dem Bibliotheksbaustein *DataExch* erweitert werden. In der Mastersteuerung ist für jede Insel eine Instanz einzufügen und in die gleiche Austauschstruktur zu hängen wie der *Operate*-Baustein von dem Master-Logikmodul. Der *DataExch*-Baustein gibt die Daten zum Senden aus und stellt einen Eingang für die empfangenen Daten zur Verfügung. Der Datenaustausch zwischen den Steuerungen musste erstellt werden, dieser wurde aus einem Beispielprojekt von Phoenix Contact übernommen. Im Testaufbau fiel auf, dass es immer wieder zu Verbindungsabbrüchen der sicheren Querkommunikation kam. Daraufhin wurde die Applikation für das Senden und Empfangen über die IP Bausteine, wie folgt, applikativ verbessert. Die Standardsteuerung, an der ein SafetyBridge-Logikmodul als Slave betrieben wird, sendet die Austauschstruktur der Querkommunikation immer, nachdem ein Empfang stattgefunden hat. Es wird verhindert, dass die zwei beteiligten Tasks, die auf unterschiedlichen Steuerungen ausgeführt werden, auseinander laufen und es deshalb zu größeren Übertragungszeiten kommt, als die in der Sicherheitsanwendung eingestellte Überwachungszeit. Leider führte dieses Vorgehen

nicht zu dem gewünschten Erfolg; der Phoenix Contact Support wurde kontaktiert. Eine Auswertung dieses Verhalten erfolgt in Kapitel 6.3.

Eine weitere Möglichkeit ist es, die Standard-SPS als Device im PROFINET-Bus vom Transfersystem einzubinden und die Daten von dem *DataExch*-Baustein über die Prozessdaten weiterzugeben. Anschließend wurde ein Funktionsbaustein erstellt, der an eine definierte Stelle in die PROFINET-Prozessdaten die SafetyBridge-Daten schreibt und ausliest. Zum Vergleich wurde die Kommunikation zwischen den Steuerungen über den PROFINET-Bus und über UDP/IP aufgebaut. Abschließend ist auf folgende Besonderheit des *DataExch*-Bausteins zu achten:

An der Instanz des *DataExch*-Bausteins, der für ein Slave-Logikmodul bestimmt ist, ist keine Inselnummer anzugeben. Die SafetyBridge-Austauschstruktur muss ein noch nicht verwendetes Element des Arrays sein und nicht das Element, welches am *Operate*-Baustein oder anderen Bausteinen angegeben ist. Es sei nochmal verdeutlicht, dass die auf der Mastersteuerung arbeitende *DataExch*-Instanz das gleiche Element der Austauschstruktur haben muss wie der zugehörige *Operate*-Baustein der Master-SafetyBridge-Insel.

5.3 Plausibilisierung

Wie in Kapitel 4.3 erläutert, wird von dem Master-Sicherheitslogikmodul direkt ein TRUE über das erste Bit der Querkommunikation an alle Slaves gesendet. Andersherum gibt auch ein Slave immer ein TRUE-Signal über das erste Bit aus. Über diese binären Signale kann ausgewertet werden, wie viele Steuerungen sich an dem Transfersystem befinden. Die einzige Bedienung zum Senden bzw. erfolgreichen Empfangen ist der korrekte Betrieb der SafetyBridge-Logikmodule einschließlich der Querkommunikation. Aus diesem Grund wird dieses Signal Lebendbit genannt. Ist kein Not-Halt betätigt, wird in gleicher Art und Weise ein TRUE-Signal ausgetauscht. Die Auswertung im Master erkennt das Fehlen von einem Not-Signal und setzt das Not-Signal für alle unterlagerten Sicherheitssteuerungen auf ein FALSE-Signal. Die Auswertung der binären Not-Halt-Signale erfolgt mit einem Gatter aus AND-, OR- und NOT-Funktionen. Dabei kann jeder Anwendungsfall als boolesche Algebra aufgefasst werden. Ein Signal von sieben möglichen auszuwerten, ist in Gl. 2 gezeigt. Zur weiteren Veranschaulichung ist beispielsweise die Auswertung von zwei aus sieben möglichen Signalen in Gl. 3 gezeigt. Dabei stellt jeder Term des OR-Gatters ein eigenes kleines Logikgatter dar. Die Magnetsensoren in den Arretierungen an den Integrationsplätzen vom Transfersystem werden beim Heranstellen einer Maschine betätigt und sind auf Eingänge der Sicherheitssteuerung geführt. Die Lebendbits, die Not-Halt-Signale und die Magnetsensoren werden mit den Gattern ausgewertet, die mithilfe der booleschen Algebra erstellt worden sind. Mit den vorhandenen sicheren Bausteinen kann

keine derartige Zählfunktion erstellt werden. Zum Testen wurde zunächst nur von drei Maschinen und somit möglichen Signalen ausgegangen. Beispielsweise ist in Abbildung 4 ein Gatter gezeigt, welches beim Anliegen von genau einem Signal der drei möglichen Signale ein TRUE-Signal ausgibt.

In der Sicherheitssteuerung von den Maschinenmodulen ist die Auswertung wesentlich einfacher. Ist das Maschinenmodul in der Integrationsumgebung eingebunden, ist der Magnetsensor betätigt. Dies wird von der Sicherheitssteuerung des Maschinenmoduls ausgewertet. Der Betriebsartenwahlschalter wird mit dem Signal vom Magnetsensor und dem Lebendbit verknüpft und auf den Baustein zur Betriebsartenwahl geführt. Treten alle drei Signale (Bedienungen) nicht auf, ist der Einzelbetrieb ausgewählt. Andernfalls handelt es sich um einen Fehlerfall, der für die Dauer des Hinzufügens von Maschinenmodulen in die Integrationsumgebung toleriert wird. Die Not-Halt-Schalter und das externe Not-Halt-Signal werden über den zugehörigen Bausteine überwacht. Die Schutzeinrichtungen an dem jeweiligen Maschinenmodul sind auf die SafetyBridge-Module der jeweiligen Maschine geführt und werden von dieser mithilfe der entsprechenden Bausteine überwacht. Liegt kein Fehlerfall vor, wird der Produktionsfreigabe zugestimmt und über ein Sicherheitsrelais an andere Steuerungen weitergegeben, wie beispielsweise an den Laser-Controller oder die Kuka-Steuerung.

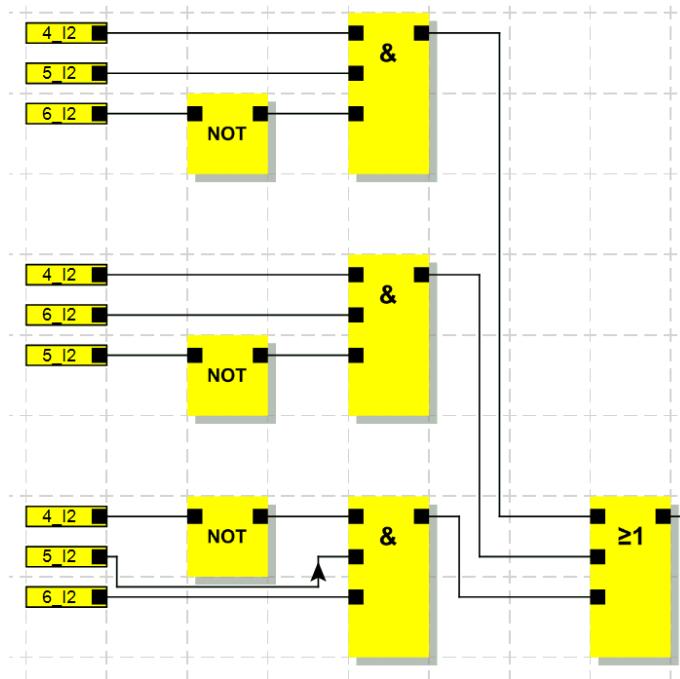


Abbildung 4: Gatter um genau ein Signal von drei möglichen auszuwerten

$$Q_1 = \bar{A}BCDEFG + A\bar{B}CDEFG + AB\bar{C}DEFG + \dots \quad (2)$$

$$\begin{aligned} Q_2 = & AB\bar{C}\bar{D}\bar{E}\bar{F}\bar{G} + A\bar{B}C\bar{D}\bar{E}\bar{F}\bar{G} + A\bar{B}\bar{C}D\bar{E}\bar{F}\bar{G} + A\bar{B}\bar{C}\bar{D}E\bar{F}\bar{G} \\ & + A\bar{B}\bar{C}\bar{D}\bar{E}F\bar{G} + A\bar{B}\bar{C}\bar{D}\bar{E}\bar{F}G + \bar{A}BC\bar{D}\bar{E}\bar{F}\bar{G} + \bar{A}B\bar{C}D\bar{E}\bar{F}\bar{G} \\ & + \bar{A}B\bar{C}\bar{D}\bar{E}\bar{F}\bar{G} + \bar{A}B\bar{C}\bar{D}\bar{E}\bar{F}\bar{G} + \bar{A}B\bar{C}\bar{D}\bar{E}\bar{F}G + \bar{A}B\bar{C}D\bar{E}\bar{F}\bar{G} \\ & + \bar{A}\bar{B}C\bar{D}\bar{E}\bar{F}\bar{G} + \bar{A}\bar{B}C\bar{D}\bar{E}\bar{F}\bar{G} + \bar{A}\bar{B}C\bar{D}\bar{E}\bar{F}G + \bar{A}\bar{B}C\bar{D}E\bar{F}\bar{G} \\ & + \bar{A}\bar{B}\bar{C}D\bar{E}\bar{F}\bar{G} + \bar{A}\bar{B}\bar{C}D\bar{E}\bar{F}G + \bar{A}\bar{B}\bar{C}\bar{D}E\bar{F}\bar{G} + \bar{A}\bar{B}\bar{C}\bar{D}E\bar{F}G \\ & + \bar{A}\bar{B}\bar{C}\bar{D}\bar{E}F\bar{G} \end{aligned} \quad (3)$$

Weiterverarbeitung der gewonnenen Informationen

Die nachfolgende Beschreibung der Implementierung bezieht sich auf das SafetyBridge-Logikmodul am Transfersystem, der Master für alle verbundenen Maschinenmodule. Zuerst wird die Anzahl der angestellten Maschinenmodule ermittelt. Die Anzahl von verbundenen Maschinen wird über einen Betriebsartenwahlschalter vom Bediener vorgegeben. Dieser ist auf sichere Eingänge geführt und gibt die Anzahl an sichere Eingänge weiter. Nach der Auswertung des Signals wird die vorgegebene Anzahl mit der ermittelten Anzahl von betätigten Magnetsensoren verknüpft und auf den Baustein zur Betriebsartenwahl geführt. Zunächst sind nur vier verschiedene Vorgaben möglich. In den nächsten Schritten wird über die erstellten Gatter zum Zählen die Anzahl von Lebendbits und Not-Halt-Signalen ermittelt. Nach der Bestimmung der Anzahl von Not-Halt-Signalen werden diese mit der gewählten Betriebsart plausibilisiert. Stimmen die Angaben überein, wird der Verbinder *Not-Halt-Signale ok* wahr. Ist abschließend am Transfersystem selbst kein Not-Halt betätigt, werden die zweiten Bits der Querkommunikationen gesetzt. Zum Ab- und Anmelden von Maschinenmodulen wurde die Auswertung der Not-Halt-Signale mit zusätzlichen Plausibilisierungen erweitert, siehe Abbildung 2.

Abschließend werden alle gewonnenen Informationen zusammengefasst. Stimmen diese überein, wird die Freigabe gesetzt. Stimmen die Anzahlen von Lebendbits, betätigten Magnetsensoren und der Bedienervorgabe überein, handelt es sich um plausible Zustände. Ist das nicht der Fall, kann durch ein gesetztes An- oder Abmeldesignal die Freigabe erhalten bleiben. Wird ein Fehler im Not-Halt-Kreis ermittelt, kommt es dennoch zum Stillstand. Die Informationen werden zur Diagnose weiter ausgewertet, damit ein Fehler in der Querkommunikation diagnostiziert werden kann. Im Fehlerfall werden die Integrationsumgebung und die mit ihr verbundenen Maschinenmodule in einen sicheren Zustand versetzt und eine mehrmalige Quittierung ist nach Behebung des Fehlers erforderlich.

5.4 Installation in das Montagesystem

Bei der Installation in das Montagesystem zeigten sich viele Herausforderungen. Aus schlaggebend war, dass das Transfersystem und die vorhandenen Maschinenmodule nicht in dem erklärten Automatisierungsgrad ausgebaut waren. Folgende Punkte mussten zunächst verbessert werden. Im Anschluss wird auf Besonderheiten bei der Erstellung von Sicherheitsfunktionen eingegangen, die an den Maschinenmodulen auffielen.

- Die Transferbandbaugruppen mussten angepasst werden, damit die verkleinerte Integrationsumgebung wieder erweitert werden konnte.
- Das Robotermontagemodul konnte aus Konstruktionsgründen nicht mehr die vorgesehene Montage von Lego-Figuren ausführen. Die Steuerungsfunktionen mussten angepasst werden, damit der Roboter wieder zu der Integrationsumgebung kompatibel wird. Der Roboter musste für die neuen Funktionen angelernt werden. Diese mussten als Montageschritte in der Integrationsumgebung bekannt gemacht werden und als benötigte Bauplanschritte mit auf den RFID-Tag für ein Produkt geschrieben werden.
- Die Bauplanschritte wurden nicht, wie erklärt, nach der Erledigung auf dem RFID-Tag entsprechend vermerkt, sondern pauschal als erledigt markiert. Dies hatte zur Folge, dass nach dem Handarbeitsplatz die Produkte laut Informationen auf dem RFID-Tag, dem Produktgedächtnis, komplett fertig gestellt waren.
- Anpassungen an den Steuerungsprojekten waren nur mit Mehraufwand möglich, da nicht die aktuellen Projekte gefunden werden konnten.

Robotermontagemaschine

In SAFECONF gibt es für die geforderte Zugangsüberwachung einen Baustein. Dieser erwartet neben einer zweikanaligen Rückmeldung der Prozesszuhal tung eine Positionsüberwachung. Die benötigte Positionsüberwachung konnte nicht mit dem vorgesehenen Produkt sicher festgestellt werden; es wurde ein neues bestimmt. Darüber hinaus benötigt der Baustein die sichere Information, dass zurzeit keine Gefährdung von dem geschützten Prozess ausgeht. In diesem Anwendungsfall wird ein sicheres Signal benötigt, welches aussagt, dass der Roboter sicher steht und der Wiederanlauf verhindert wird. Dieses wird nicht über die Hardwareschnittstelle ausgegeben. Die folgende Lösung wurde gefunden. Der Zugang wird durch den Maschinenbediener angefordert. Nach Programmablauf wird der Roboter durch die Standardsteuerung gestoppt. Anschließend wird der Anforderung des Bedieners in der

Sicherheitssteuerung zugestimmt. Nach dem Ablauf einer Sicherheitszeit wird über die Sicherheitsschnittstelle der Kuka-Steuerung die Stillstandsüberwachung des Roboters über ein Sicherheitsrelais aktiviert. Dieses Relais wird von der Sicherheitssteuerung überwacht. Das Schalten des Relais wird als sicheres Stillsetzen des Prozesses gewertet, indem die Überwachung auf den Baustein für die Zugangsüberwachung geführt wird. Der Zugang in den geschützten Bereich ist fehlerfrei möglich.

6 Auswertung

In diesem Kapitel werden Anforderungen aus Kapitel 3 mit dem Ergebnissen des umgesetzten Konzepts aus Kapitel 4 verglichen und bewertet. Abgeschlossen wird die Bachelorarbeit mit dem Ausblick, der Ansatzpunkte für zukünftige Verbesserungen gibt.

6.1 Umsetzung des Konzepts

Der geforderte Funktionsumfang konnte mit Einschränkungen umgesetzt werden. Die konzeptionierte Funktionsweise beim Hinzufügen und Entfernen von Maschinen konnte erreicht und erfüllt werden. Zur Ermittlung der Anzahl von Signalen mussten viele AND- und OR-Funktionen miteinander zu Logikgattern zusammengefügt werden. Diese Gatter auf zukünftig sieben mögliche Maschinen zu dimensionieren, stellte sich als zeitaufwändiger heraus, als zuvor angenommen.

Die graphische Implementierungsmöglichkeit ist intuitiv zu bedienen und die Sensoren konnten schnell mit vorhandenen Bausteinen ausgewertet werden. Mit fortschreitender Konfiguration der Funktionen verlor diese zunehmend an Übersichtlichkeit; eine Implementierung in einer Hochsprache stand nicht zur Verfügung. Die Gatter konnten nicht als Funktionen oder Funktionsbausteine zusammengefasst werden. Es war somit nicht möglich, die Übersichtlichkeit des Programms zu verbessern. Die Unterteilung in sogenannte *Netzwerke* konnte dies nicht entscheidend verbessern. Der sichere Speicher der SafetyBridge-Logik beträgt 30 kByte und reicht nicht für ein Projekt der geforderten Größenordnung mit sieben möglichen Maschinenmodulen aus. Damit es beim Hinzufügen und Entfernen von Maschinenmodulen zu einer bewussten Handlung kommt, gibt der Maschinenbediener die Anzahl von eingebrachten Maschinenmodulen über einen Knebelschalter vor. Es konnte nur ein Knebelschalter mit acht Schalterstellungen gefunden werden, wovon vier jeweils ein Schaltelement betätigen. Die Schalterstellung wird über den sicheren Baustein zur Betriebsartenwahl ausgewertet. Der Baustein ist für bis zu fünf verschiedene Betriebsarten ausgelegt, sodass null bis vier Maschinen angestellt bzw. vom Baustein ausgewertet werden können. Die Auswahl an Knebelschaltern mit mehr auswertbaren Schalterstellungen ist beschränkt. Oftmals wird die Schalterstellung über einen binär- oder mit dem BCD-Code bekanntgegeben und muss entsprechend ausgewertet werden. Für die Anforderung, sieben mögliche Maschinen gleichzeitig integrieren zu können, muss eine andere Lösung gefunden werden. Eine mögliche Lösung wäre die Vorgabe mit einer zugangsbeschränkten Auswahl an einem Human Machine Interface (HMI)-Panel. Nach der Veränderung der Anzahl von integrierten Maschinen muss eine Quittierung erfolgen. Dadurch ist sichergestellt, dass es bei der Veränderung der Anzahl integrierter Maschinenmodule zu einer bewussten Handlung kommt.

Zusammenfassend können folgende Gründe festgestellt werden, die eine Berücksichtigung von sieben möglichen Maschinenmodulen verhindern.

- Eingeschränkte Bedienervorgabe: es können maximal drei integrierte Maschinen vorgegeben werden.
- Aufwendig zu erstellende Logikverknüpfungen für die Auswertung.
- SAFECONF-Projekt übersteigt den Speicher des Logikmoduls.
- Es konnten maximal drei mögliche Maschinenmodule im SAFECONF-Projekt berücksichtigt werden.

Aus diesen Gründen wurde die Anzahl von möglichen Maschinenmodulen bei der Umsetzung des Sicherheitskonzepts auf drei beschränkt.

Nach der Norm *ISO 13849-2* muss noch eine dokumentierte Validierung der in der Risikobeurteilung geforderten Maßnahmen erfolgen. Dies ist in Teilen mit dieser Bachelorarbeit geschehen, da Maßnahmen aus der Risikobeurteilung in die Anforderungen in Kapitel 3 eingeflossen sind. Das Ergebnis der Umsetzung ist in Kapitel 6.4 festgehalten. Mit der nachfolgenden Querkommunikation war es möglich, eine modulare und über Ethernet vernetzte Not-Halt-Funktion zu erstellen.

6.2 Erfassung von sicheren Sensoren im Feld

Die SBT bietet keine Möglichkeit, Sensoren direkt im Feld auszuwerten oder zu bündeln und sicherheitsgerichtet in den Schaltschrank zu übertragen. Es ist eine parallele Verdrahtung durch das Transfersystem zum Schaltschrank notwendig. Neben dem erhöhten Aufwand, das gesamte Steckersystem des Transfersystems anzupassen, ist dieser Lösungsansatz auch nicht mehr zeitgemäß. Zur schnelleren und vorläufigen Realisierung wurden an den Transferbändern mit sicherheitsrelevanter Sensorik PROFINET-Buskoppler von Phoenix Contact für das Inline-System angebracht. An jeden Buskoppler wurde ein SafetyBridge-Satellit mit acht sicheren Eingängen angefügt, welcher vom Logikmodul der Insel 31 im Schaltschrank des Transfersystems ausgewertet wird. Mit dieser Lösung konnten die Sensoren sicherheitsgerichtet im Feld ausgewertet und zur Weiterverarbeitung über Ethernet sicherheitsgerichtet übertragen werden. Der Nachteil dieser Lösung ist, dass die Buskoppler sowie die Inline-Baugruppen nicht für die Installation im Feld vorgesehen sind. Ein Einbau in ein Gehäuse, welches an eine Transferband-Baugruppe montiert wird, wäre eine mögliche Lösung. Aus diesem Grund handelt es sich um eine vorläufige Lösung.

6.3 Querkommunikation

Die SBT-V3 unterstützt eine sicherheitsgerichtete Kommunikation zwischen Logikmodulen. Dabei kann über verschiedene Ethernet-basierte Protokolle und Bustechnologien hinweg kommuniziert werden. Im Testaufbau wurde zunächst über das Internet Protocol (IP) eine Netzwerkverbindung zwischen den Standardsteuerungen aufgebaut und die SafetyBridge-Austauschstruktur wurde über das UDP ausgetauscht. Die Querkommunikation zwischen den Sicherheitssteuerungen konnte erfolgreich aufgebaut werden. Eine hohe Verfügbarkeit des Systems konnte zunächst nicht erreicht werden. Durch applikative Verbesserungen im PC-WORX-Projekten der beiden Steuerungen konnte die Verfügbarkeit gesteigert werden, dennoch war das Ergebnis noch nicht zufriedenstellend. Wie in Abbildung 5 zu sehen ist, kommt es immer wieder zu Spitzen in der Übertragungszeit. Diese übersteigen die parametrierte Überwachungszeit und die sicherheitsgerichtete Verbindung wird abgebaut. Als Folge dessen wird an dem Transfersystem und an allen verbundenen Maschinenmodulen ein sicherer Halt eingeleitet. Damit ist ein Produktionstop verbunden. Das gleichzeitige Fehlen von einem Lebendbit und dem externen Not-Halt-Signal kann in der Konfiguration des Masters als Kommunikationsfehler diagnostiziert werden.

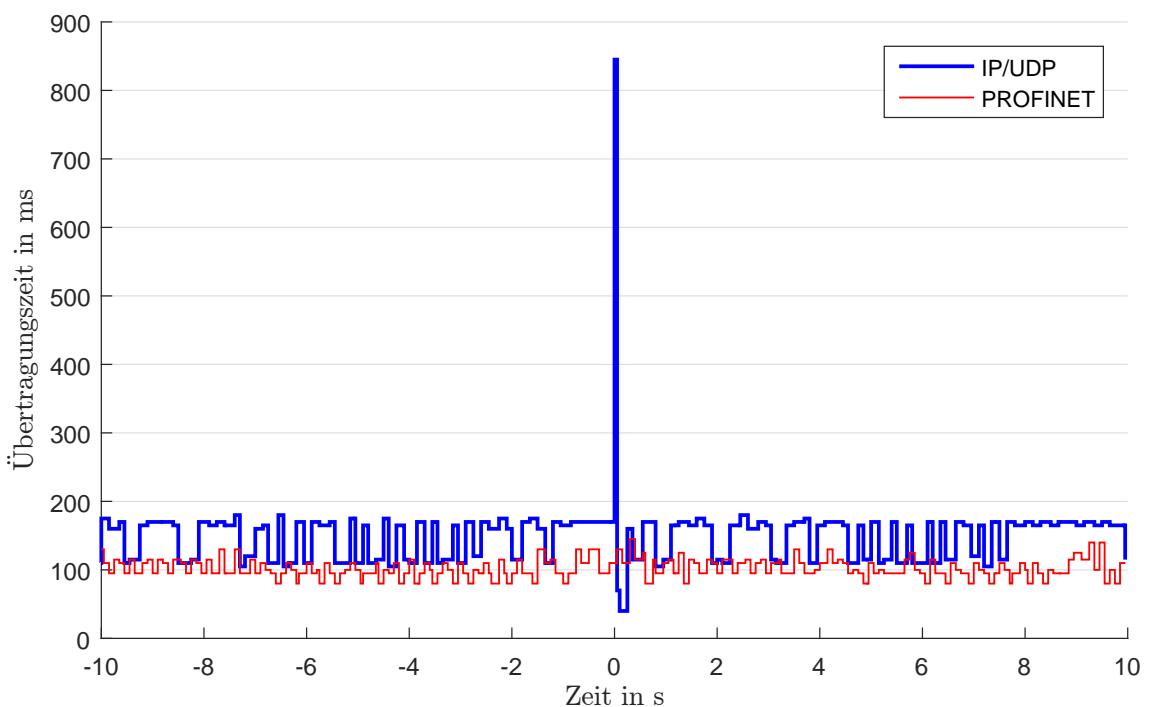


Abbildung 5: Verlauf der Übertragungszeit zwischen zwei SafetyBridge-Logikmodulen

Im Kapitel 2.5 wurden bereits einige Unterschiede zwischen UDP/IP und PROFINET erläutert. Diese Unterschiede können bereits eine Erklärung für die zufällig auftretenden Spitzen in der UDP/IP-Übertragung sein. Erfolgt der Austausch der SafetyBridge-Querkommunikation über die PROFINET-Prozessdaten, treten keine auffälligen Spitzen in der Übertragungszeit auf, siehe Abbildung 5. Auch ist zu erkennen, dass die Übertragungszeit über PROFINET geringer ist und im Gegensatz zu UDP/IP geringere Unterschiede in der Differenz der Übertragungszeit aufweist. Somit kann das Übertragungsverhalten als deterministischer aufgefasst werden und erfüllt besser die Anforderungen der SBT. Die Verfügbarkeit und Übertragungszeit konnte mit dieser Maßnahme weiter verbessert werden. Eine mögliche Erklärung für das Auftreten der Spitzen kann in der Leistungsfähigkeit der eingesetzten Steuerungen begründet werden. Die aufgebauten Kommunikationsverbindungen müssen von den Steuerungen verarbeitet werden. Dies wird vom Betriebssystem der Steuerung organisiert. Dabei werden die Daten von einer Kommunikationsschnittstelle auf einen Speicher (Stack) geschrieben. Dieser wird vom Betriebssystem mit verschiedenen Prioritäten verarbeitet. Die genaue Arbeitsweise des Betriebssystems ProConOS ist nur dem Hersteller bekannt. Dieser wurde zur Fehlerbehebung kontaktiert und konnte die oben beschriebene Erkenntnisse bestätigen, jedoch nicht im Bearbeitungszeitraum der Bachelorarbeit lösen.

Diese Erkenntnisse wurden auf das wandlungsfähigen Montagesystem übertragen und die Steuerungen der möglichen Maschinenmodule als Device in den PROFINET-Aufbau der Integrationsumgebung eingebunden. Durch diese Maßnahme wird die Anforderung eingeschränkt, ein Maschinenmodul mit kompatiblen Schnittstellen ohne weitere Anpassungen an der Integrationsumgebung einbringen zu können. Bei der Inbetriebnahme stellte sich heraus, dass sowohl die im Testaufbau parametrierten Überwachungszeiten zwischen der Insel und den Satelliten als auch zu den Slave-Inseln nicht erreicht werden konnten. Folgende Erkenntnisse konnten bei der Analyse der möglichen Ursachen festgestellt werden.

- Die größte Aktualisierungszeit der PROFINET-Prozessdaten liegt bei 16 ms.
- Deutlich mehr Netzwerkkomponenten und -teilnehmer als im Testaufbau.
- Große Laufzeitunterschiede von 1 ms bis zu 1500 ms beim Senden von Ping-Befehlen.
- Gelegentliche Ausfälle von Buskopplern aufgrund von Busfehlern. Die maximal zulässige Aktualisierungszeit der Prozessdaten beträgt 192 ms. Danach wird das Fehlen von aktuellen Prozessdaten als Busfehler gewertet.

Aufgrund dieser Erkenntnisse wurde mit den Verantwortlichen des Produktionsnetzwerkes Rücksprache gehalten, wie die Unterschiede in der Übertragungszeit minimiert werden

können. Die Erkenntnisse konnten bestätigt, eine zeitnahe Lösung jedoch nicht gefunden werden. Die oben genannten Erkenntnisse stehen nicht im Zusammenhang mit der Übertragung von Daten der funktionalen Sicherheit, daher kann ein Fehler in der Anwendung der SBT ausgeschlossen werden. Hinzu kommt, dass die SBT erfolgreich im Testaufbau in Betrieb genommen werden konnte. Es ist offensichtlich, dass das Produktionsnetz nicht die geforderten Eigenschaften wie z.B. Determinismus erfüllt. In Folge dessen sinkt die Verfügbarkeit des wandlungsfähigen Montagesystems. Dass die standardisierten Komponenten vom Produktionsnetz die Anforderungen der funktionalen Sicherheit erfüllen müssen, ist auf das Black-Channel-Prinzip zurückzuführen, siehe Kapitel 2.4.3. Eine tiefer gehende Analyse des Produktionsnetzwerks, zur Erlangung der Anforderungen, ist nicht Teil der funktionalen Sicherheit und überschreitet somit den Umfang dieser Bachelorarbeit. Ein Produktionsnetz mit den geforderten Eigenschaften wird als grundlegend vorausgesetzt. Bei dem hier betrachteten Not-Halt handelt es sich, nach der Maschinenrichtline (MRL), um eine zusätzliche Sicherheitseinrichtung, die nach der *DIN EN ISO 13850* ausgelegt wurde. Die geforderte garantierte Abschaltzeit t_G von 350 ms konnte für das wandlungsfähige Montagesystem nicht erreicht werden. Um eine angemessene Verfügbarkeit zu erlangen, mussten die parametrierten Überwachungszeiten zwischen den Logikmodulen auf 400 ms und den Satelliten im Feld des Transfersystems auf 200 ms angepasst werden. Die Überwachungszeiten zu den Satelliten, die an der gleichen Inline-Station installiert sind wie das zugehörige Logikmodul, wurden individuell parametriert. Diese Anpassung kann vorgenommen, da in der *DIN EN ISO 13850* keine Abschaltzeit genannt ist und der Prozess keine zeitkritische maschinenübergreifende Abschaltung fordert.

Analyse der Übertragungszeiten

Der Verlauf der Übertragungszeiten wurde mithilfe des *TransTime*-Bausteins aus der SBT-Bibliothek aufgezeichnet. Damit konnte eine Übertragungszeit eingestellt werden, die zur einer Verbesserung der Verfügbarkeit führt. In Abbildung 6 ist ein Ausschnitt von einer kontinuierlichen Aufzeichnung der Übertragungszeiten zwischen der Sicherheitssteuerung vom Transfersystem und den zugehörigen Satelliten zu sehen. Aus den Verläufen der Übertragungszeiten können folgende Erkenntnisse gezogen werden:

Die Satelliten eins und zehn sind nebeneinander in einer Inline-Station installiert. Im SAFECOMP-Projekt dagegen sind diese nicht nebeneinander konfiguriert, sondern als Satelliten an Stelle eins und zehn. Im Zeitverlauf in Abb. 6 ist ein ähnlicher Verlauf mit einem gewissen Offset in der Übertragungszeit festzustellen. Eine Begründung für dieses Verhalten kann möglicherweise in der internen Funktionsweise der SBT oder den zugehörigen Bibliotheksbausteinen im PC-WORX-Projekt gefunden werden.

Die Satelliten zwei, drei und vier mit jeweils einem Buskoppler sind an Transferband-Baugruppen verteilt. Es ist im Vergleich zu den anderen Verläufen eine zeitlich häufigere Veränderung der Übertragungszeit zu beobachten. Zu beobachten sind auch einzelne Spitzen in der Übertragungszeit, die in diesem Abschnitt nicht die 150 ms überschreiten. Bei einer Parametrierung der F-Watchdog-Zeit von 150 ms konnte jedoch festgestellt werden, dass sich die Verfügbarkeit des Systems verringert. Gründe für die Spitzen in der Übertragungszeit können in einer schwankenden Netzwerkauslastung liegen. Eine parallele Aufzeichnung des gesamten Netzwerksverkehr könnte eine genauere Erklärung liefern. Diese Auswertung der standardisierten Netzwerkkomponenten überschreitet den Umfang dieser Bachelorarbeit, siehe oben. Eine grundsätzliche Voraussetzung für die SBT war ein deterministisches Netzwerk. Das Auftreten von den Spitzen zeigt, dass diese Voraussetzung nicht ausreichend erfüllt ist.

Die Übertragungszeit der Querkommunikation zwischen zwei Logikmodulen an verschiedenen Steuerungen fällt deutlich höher aus. Diese verändert sich pro Zeiteinheit gesehen nicht so häufig. Die Differenz der Übertragungszeiten weist den höchsten Betrag auf. Zur Auswertung sei an dieser Stelle nochmal die Topologie des Transfersystems erwähnt, welche eine Linientopologie von Switchen aufweist. Das Maschinenmodul mit dem Roboter ist an die Transferband-Baugruppe mit dem Satelliten vier integriert. Beide zweigen vom letzten Switch der Linientopologie ab. Aus diesem Grund kann die Differenz der Übertragungsgeschwindigkeiten zwischen der Insel des Maschinenmoduls im Slave-Betrieb und dem Satelliten vier nicht allein im Netzwerk begründet werden. Eine Begründung kann in der unterschiedlichen Realisierung des Datenaustausches gefunden werden. Der Satellit am Buskoppler wird über eine Variable, die von einem Bibliotheksbaustein der SBT zur Verfügung gestellt wird, mit der Prozessdatenzuordnung eingebunden. Für die Slave-Insel wird die SBT-Austauschstruktur mit dem DataExch-Funktionsbautein extrahiert. Diese Austauschstruktur wird anschließend in die PROFINET-Prozessdaten geschrieben, die 32 Byte umfassen. Eine umgekehrte Verarbeitung erfolgt auf der Seite von der Slave-Insel. Dieser Hintergrund kann die erhöhte Übertragungszeit im Vergleich zum Satelliten erklären.

Es sei abschließend angemerkt, dass an den Inline-Stationen, die mit einer ILC-Steuerung gegründet wurden, wegen eines bereits verbauten Moduls die interne Übertragungsgeschwindigkeit nur auf 500 kBaud parametriert werden konnte. Vergleiche am Testaufbau haben gezeigt, dass eine Verbesserung der Übertragungszeit von etwa 20 ms erreicht werden kann, wenn die interne Übertragungsgeschwindigkeit der Inline-Station auf 2 MBaud parametriert werden kann.

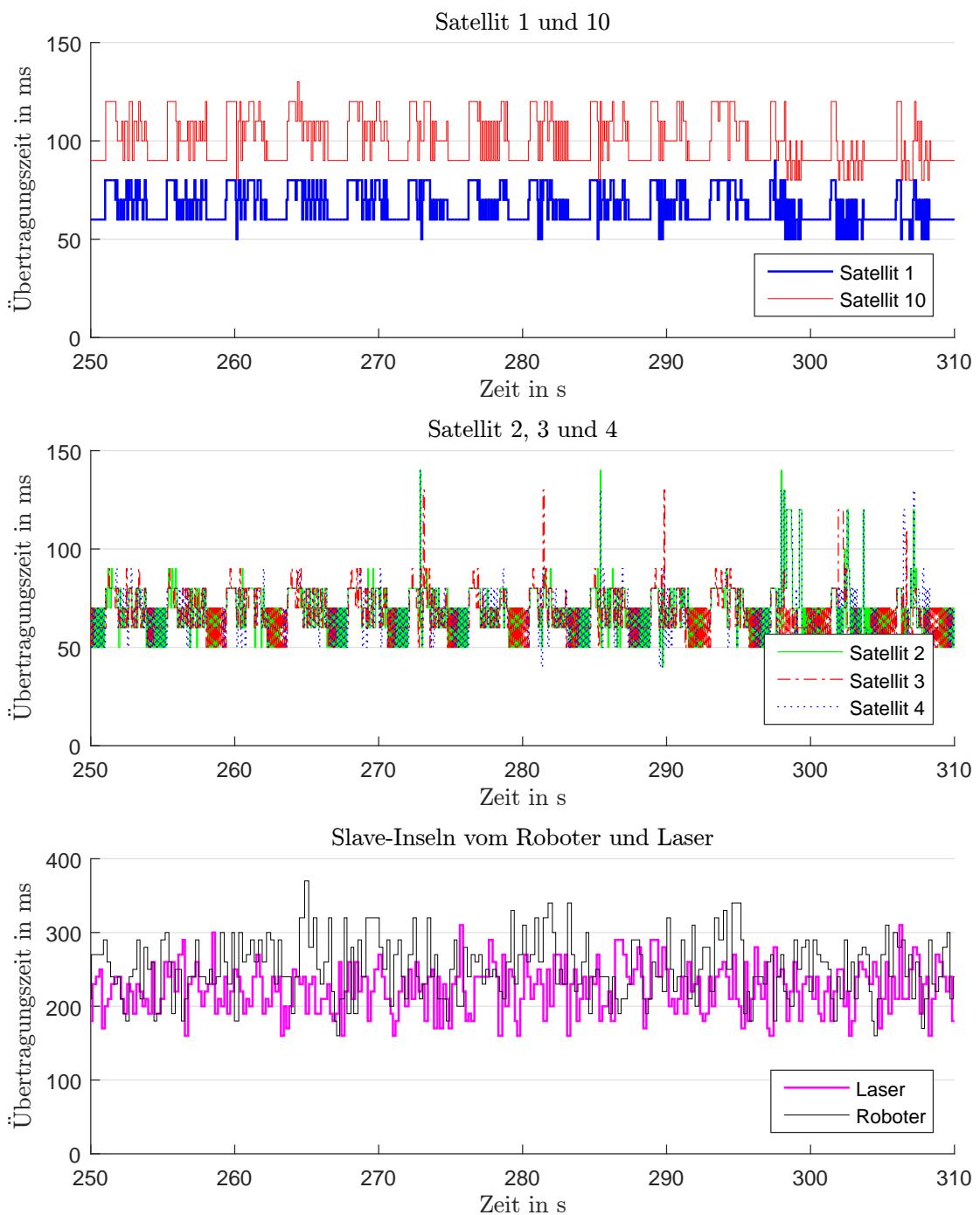


Abbildung 6: Ausschnitt aus einer kontinuierlichen Aufzeichnung der Übertragungszeit zwischen den SafetyBridge-Logikmodulen

6.4 Sicherheitsfunktionen der Maschinenmodule

In diesem Abschnitt werden die einzelnen steuerungstechnischen Funktionen der Maschinenmodule überprüft. Zur Feststellung der Erfüllung werden diese mit den Forderungen aus den Risikobeurteilungen überprüft. Im Folgenden wird vor allem auf die Funktionen eingegangen, die nicht erfüllt werden konnten. Dies hat zur Folge, dass eine erneute Risikobeurteilung bzw. ein weiterer Iterationsschritt der Beurteilung notwendig ist.

6.4.1 Smartes Transfersystem

Die Steuerung des smarten Transfersystems konnte erfolgreich um die SafetyBridge-Hardware erweitert werden. Aufgrund der vorhandenen Automatisierungskomponenten und deren Verschaltung/Aufbau können einige Aktoren nicht sicherheitsgerichtet abgeschaltet werden, bzw. deren Abschaltung stellt keine praktikable Lösung dar. Der wichtigste Punkt ist das Stoppen der Transferbänder. Zum besseren Verständnis wird deren Ansteuerung näher erläutert. Jede Transferband-Baugruppe verfügt über einen Frequenzumrichter, der über Profibus gesteuert wird. Aus diesem Grund kann die Freigabe oder auch ein kontrolliertes Stoppen des Transportbands nicht sicherheitsgerichtet ausgeführt werden. Ein Stoppen über die standardisierte Steuerung ist bei einem Not-Halt möglich, aber nicht ausreichend. Eine weitere Maßnahme zur sicheren Abschaltung wäre die sicherheitsgerichtete Abschaltung der Energieversorgung. Dies bedeutet die Abschaltung der Energieverteilung des gesamten smarten Transfersystems und infolgedessen von den integrierten Maschinenmodulen. Diese Abschaltung ist nicht praktikabel, da dies für die Maschinenmodule einen generatorischen Ausfall bedeutet und damit einen zeitaufwendigen Wiederanlauf.

Die Abschaltung der Druckluft konnte sicherheitsgerichtet ausgeführt werden. Das Abschalten der Druckluft muss bei den Sicherheitskonzepten der integrierbaren Maschinenmodule berücksichtigt werden, sodass es nicht zu einer Gefährdung durch beispielsweise Entspannen von Werkzeugen kommt.

Bestimmung der garantierten Abschaltzeit

Abschließend zum Transfersystem soll die garantierte Abschaltzeit (t_G) für ein maschinenübergreifenden Not-Halt bestimmt werden, der von diesem verarbeitet wird. Die garantierte Abschaltzeit für die Sicherheitsfunktion setzt sich aus der größten Verarbeitungszeit der an der Sicherheitsfunktion beteiligten sicheren Eingänge und der Abschaltzeit des beteiligten sicheren Ausgangs (ein- oder zweikanalig) zusammen. [7, A 9.2] Wie in Gl. (5) zu sehen, setzt sich die garantierte Abschaltzeit aus vielen Faktoren zusammen, die nachfolgend kurz beschrieben werden. Beginnend mit der Verarbeitungszeit des Eingangs (t_{IN}), die sich

nach Gl. (4) aus einer parametrierten Filterzeit (t_{Filter}) und einer konstanten Firmwarelaufzeit (t_{FW}) zusammensetzt, muss der zugehörige Satellit diese Information an die Insel übertragen. Für diese Übertragung wurde im SAFECONF-Projekt eine F-Watchdog-Zeit (t_{FWD_IN}) parametriert, die maximal beansprucht werden darf. Andernfalls geht das SafetyBridge-System in einen sicheren Zustand. Die zugehörigen Satelliten werden von dem Logikmodul des Maschinenmoduls 2 ausgewertet. Dafür werden 15 ms (t_{OUT_LPSDO2}) konstant benötigt. Mithilfe der Querkommunikation wird das Not-Halt-Signal weiter zur übergeordneten Insel 31 gegeben, zu dem Transfersystem. Für diese Übertragung wurde eine weitere F-Watchdog-Zeit (t_{FWD_SL2}) festgelegt. Die Insel 31 in dem Transfersystem benötigt maximal die Zeit ($t_{OUT_LPSDO31}$) zur Weiterverarbeitung. An dieser Stelle wird sowohl der Not-Halt am Transfersystem selbst ausgelöst als auch an den integrierten Maschinenmodulen. Dies erfolgt erneut mithilfe der Querkommunikation und benötigt zur Insel 3 maximal die parametrierte F-Watchdog-Zeit (t_{FWD_SL3}). Die Insel 3 in der Robotermontagezelle benötigt maximal die Zeit (t_{OUT_LPSDO3}) zur Weiterverarbeitung. Ähnlich der Verarbeitung des Eingangssignals kommt eine parametrierte F-Watchdog-Zeit (t_{FWD_OUT}) für die Übertragung zum Satelliten und eine Abschaltzeit des Ausgangs (t_{OUT}) hinzu. Werden die Ausgänge von der Insel benutzt, entfallen diese beiden Zeit und sind somit mit Null anzunehmen.

Diese Zeit muss um die Worst-Case-Reaktionszeiten der Sensoren (t_S) und Aktoren (t_A) sowie die Anhaltezeit (t_{STOP}) der Maschine ergänzt werden, um die gesamte maximal benötigte Abschaltzeit der Sicherheitsfunktion (t_{SF}) zu erhalten. Die Anforderung der maximalen Abschaltzeit ist erfüllt, wenn diese kleiner als die geforderte ist. Für ein Not-Halt-Signal ist normativ keine absolute Zeit gefordert. Als annehmbare garantierter Abschaltzeit sind hier 350 ms gefordert. Diese können nach dem Ergebnis von Gl. (5) nicht eingehalten werden.

$$t_{IN} = t_{Filter} + t_{FW} \quad (4)$$

$$t_{IN} = 3 \text{ ms} + 0,25 \text{ ms}$$

$$t_{IN} = 3,25 \text{ ms}$$

$$t_G = t_{IN} + t_{FWD_IN} + t_{OUT_LPSDO2} + t_{FWD_SL2} + t_{OUT_LPSDO31} + t_{FWD_SL3} \quad (5)$$

$$+ t_{OUT_LPSDO3} + t_{FWD_OUT} + t_{OUT}$$

$$t_G = (3,25 + 150 + 15 + 400 + 15 + 400 + 15 + 0 + 0) \text{ ms}$$

$$t_G = 998,25 \text{ ms}$$

6.4.2 Robotermontagemaschine

An der Robotermontagemaschine wurden die geforderten Betriebsarten erfolgreich installiert. Die Kuka-Steuerung wird über die Hardwareschnittstelle X11 sicherheitsgerichtet beeinflusst, da kein Austausch von sicherheitsgerichteten Daten zwischen PROFIsafe und der SBT möglich ist.

Bei der Wiederherstellung der Kompatibilität zwischen dem smarten Transfersystem und diesem Maschinenmodul stellte sich heraus, dass dieses Maschinenmodul nicht mehr in Verbindung mit dem vorgesehenen Materiallager eingesetzt werden kann. Aus diesem Grund ist die trennende Schutzeinrichtung zum geschützten Bereich des Roboters neu auszulegen. Bei der Risikobeurteilung im Vorfeld wurde bereits der Zugang in den geschützten Bereich für alle anfallenden Aufgaben als nicht geeignet festgestellt. Dieser sollte durch eine Tür mit Prozesszuhaltung geändert werden. Den Zugang konstruktiv anzupassen, ist nicht Teil dieser Bachelorarbeit. Ein Zugang in vier Stufen wurde bereits in der Konfiguration der Sicherheitsfunktionen berücksichtigt, siehe Kapitel 5.4. Mithilfe der dort erstellten Lösung und eines Sicherheitsschalters mit Positions- und Prozessüberwachung kann nach der Installation einer Tür ein sicherer Zugang ermöglicht werden.

Das Werkzeug vom Roboter saugt das Werkstück durch Unterdruck an, welcher mit Druckluft erzeugt wird. Im Fehlerfall wird die Druckluft abgeschaltet und das Werkstück fällt herunter. Dies führt bei den vorgesehenen Produkten zu keiner weiteren Gefährdung von Mensch, Maschine und Umwelt.

6.4.3 Graviermaschine

An der Graviermaschine wurden die geforderten Betriebsarten erfolgreich installiert. Nicht erfolgreich war hingegen die sicherheitsgerichtete Überwachung der Absaugung. Es konnte nicht sichergestellt werden, dass nur bei ordnungsgemäßem Betrieb der Absaugung eine Laserbearbeitung möglich ist. Dies ist auf fehlende sichere Rückmeldekontakte der Absaugung zurückzuführen.

Bei der Überprüfung der Sicherheitsfunktionen fiel auf, dass der Controller des Lasers nicht erwartungsgemäß funktioniert. Über einen Sicherheitsschalter wird festgestellt, dass der Bearbeitungsraum durch einen Werkstückträger geschlossen wurde. Erst dann ist das Öffnen des Shutters zulässig. Statt des Öffnens kam es jedoch zu der Fehlermeldung, dass die Laserdiode zu viel Strom aufnehme. Diese Meldung ist nicht nachvollziehbar, da die Diode nicht ausgeschaltet wurde, sondern der Shutter wieder geöffnet werden sollte. Der Hersteller wurde kontaktiert und spricht von einen bekannten Problem, welches vielleicht durch ein Update behoben werden könnte. Damit die Maschi-

ne weiter betrieben werden kann, wurde der vorherige Zustand wiederhergestellt. Der Shutter bleibt unzulässigerweise, unabhängig vom geschlossenen Bearbeitungsraum, geöffnet.

Bestimmung der maximal benötigten Abschaltzeit (t_{SF})

In diesem Abschnitt wird die maximal benötigte Abschaltzeit (t_{SF}) bestimmt, die zur Feststellung des Fehlers bis zum Schließen des Shutters benötigt wird. Die Laserbearbeitungskabine muss während des Graviervorgangs mit einem Laserstrahl durch den Objektträger geschlossen sein. Zur Überprüfung, ob der angehobene Objektträger die Kabine korrekt verschließt, ist ein magnetischer Sicherheitsschalter montiert. Der zugehörige Betätiger ist auf dem Objektträger angebracht. Dieser Schalter benötigt eine maximale Reaktionszeit (t_S) von 30 ms, bis die Ausgänge geschaltet haben. [16]

Zur Auswertung wurde der Eingang mit einer Filterzeit (t_{Filter}) von 3 ms parametriert. Die Firmware von dem zugehörigen Satelliten benötigt die Zeit (t_{FW}). [17] Der Satellit befindet sich an der gleichen Inline-Station wie die zugehörige Insel 2 (Logikmodul), die zur Auswertung benötigt wird. Für die Kommunikation zwischen diesen beiden Inline-Modulen wurde eine F-Watchdog-Zeit (t_{FWD_IN}) parametriert. Die Logik selbst benötigt zur Verarbeitung die Zeit (t_{OUT_LPSDO2}). Der zu schaltende Ausgang ist an dem Logikmodul, daher entfällt eine weitere F-Watchdog-Zeit (t_{FWD_OUT}) zur Übertragung an einen Satelliten, sowie die Reaktionszeit des Ausgangs (t_{OUT}).

Der vom Laser-Controller zur Verfügung gestellte Sicherheitskreis für den Shutter ist potenzialfrei zu schließen, damit der Shutter die Laserdiode frei gibt. Dazu wurde an den Ausgang des SafetyBridge-Logikmoduls (Insel 2) ein Sicherheitsrelais mit Rückmeldung angeschlossen. Die maximale Zeit, um abzufallen, (t_A) beträgt 20 ms. [18] Die Sicherheitskreise vom Laser-Controller sind nicht sicherheitsgerichtet und nicht genauer spezifiziert. Vom Hersteller war zu erfahren, dass eine maximale Abschaltzeit von 200 ms (t_{STOP}) angenommen werden sollte.

Dieser Zusammenhang zur Bestimmung der maximal benötigten Abschaltzeit ist in Gleichung (6) dargelegt und führt zu dem Ergebnis $t_{SF} = 368,25$ ms. Gefordert war eine Zeit von $t_{SF} = 280$ ms. Davon wurden 50 ms für das SafetyBridge-System und das Sicherheitsrelais vorgesehen. Diese Zeit kann offensichtlich nicht eingehalten werden. Folglich muss die Tiefe, die der Objektträger in die Laserbearbeitungskabine taucht, erneut berechnet werden, siehe [6, S. 40].

$$t_{SF} = t_S + t_{Filter} + t_{FW} + t_{FWD_IN} + t_{OUT_LPSDO2} + t_{FWD_OUT} + t_{OUT} + t_A + t_{STOP} \quad (6)$$

$$t_{SF} = (30 + 3 + 0, 25 + 100 + 15 + 0 + 0 + 20 + 200) \text{ ms}$$

$$t_{SF} = 368,25 \text{ ms}$$

6.5 Fazit

Mit der SafetyBridge-Technologie (SBT) konnte das Sicherheitskonzept für ein wandlungsfähiges Montagesystem implementiert werden. Gefordert war eine Anlagengröße mit sieben möglichen Maschinenmodulen. Diese Forderung musste aufgrund der Leistungsfähigkeit auf drei mögliche Maschinenmodule begrenzt werden. Die umfangreiche Plausibilisierung von Signalen zum Aufbau einer Erwartungshaltung benötigte mehr Speicher als das Logikmodul bieten kann. Ausschlaggebend war das Fehlen von einem Baustein mit folgender Funktion. Eine Anzahl von Signalen wird auf den Baustein geführt und als Ergebnis wird die Anzahl von TRUE-Signalen ausgegeben. Das Ergebnis über die ermittelte Anzahl kann über jeweils einen Ausgang des Bausteins ausgegeben werden. Mit dieser Lösung muss kein Integer-Datentyp eingeführt werden und der Einsatz von mehreren selbst zusammengestellten Logikgatter hätte vermieden werden können. Eine Alternative wäre eine erweiterte Bedienvorgabe gewesen, die mit der Schalterstellung vorgibt, an welchem Integrationsplatz welches Maschinenmodul integriert ist. Dieses Vorhaben wird durch die Anzahl von Schalterstellungen begrenzt oder die implementierten Sicherheitsfunktionen begrenzen die Wandlungsfähigkeit des Montagesystems.

Die im Sicherheitskonzept geforderten und angenommenen Worst-Case-Reaktionszeiten bzw. garantierten Abschaltzeiten konnten mit der SBT nicht erreicht werden. Dies liegt zum einen an dem vorhandenen Produktionsnetzwerk und zum anderen an der Technologie selbst. Dies kann durch einen Vergleich der Gleichungen (5) und (6) festgestellt werden. Bei der Implementierung des Sicherheitskonzepts fielen Differenzen bei der Funktionsweise des wandlungsfähigen Montagesystems und bei einigen verbauten sicherheitsrelevanten Komponenten auf. Als Beispiele seien folgende zwei Punkte genannt. Das Montagesystem konnte nicht in der beschriebenen Art und Weise, nach dem Plug-and-Work-Prinzip, mit der Robotermontagemaschine erweitert werden. Die vorgesehene Funktionsweise der Robotermontagemaschine konnte nicht ausgeführt werden und eine Entscheidung für eine neue Applikation lag nicht vor. Die Sicherheitsfunktion, die den Shutter des Lasers steuert, konnte nicht vollständig bestimmt werden. Der Laser-Controller verfügt zwar über Sicherheitsverriegelungen, die angesteuert werden können, diese sind jedoch nicht zertifiziert. Aus diesem Grund konnte die Sicherheitsfunktion nicht vollständig bestimmt werden.

Die Grundmaschine bzw. das smarte Transfersystem wurde mit einer Sicherheitssteuerung erweitert und kann jetzt den Dienst anbieten, sicherheitsrelevante Daten zwischen den integrierten Maschinenmodulen über die Sicherheitssteuerung auszutauschen. Über eine gezielte Überbrückung von Sicherheitsfunktionen kann das Montagesystem ohne einen Produktionsstopp verändert werden.

6.6 Ausblick

Bei der Implementierung der SBT hat sich gezeigt, dass diese Technologie nur beschränkt für das betrachtete Sicherheitskonzept geeignet ist. Die Anzahl von integrierbaren Maschinen kann beispielsweise durch den Einsatz von PROFIsafe verbessert werden. Dabei kann ein Teil der verbauten Komponenten weiterhin genutzt werden. Die SBT ist für die zukünftigen Anforderungen zu erweitern. Dies kann durch weitere sichere Bausteine erfolgen. Ein möglicher Baustein ist bereits in Kapitel 6.5 beschrieben, weitere können aus den unten beschriebenen zukünftigen Anforderungen resultieren. Wie die Sicherheitskonzepte in Zukunft für einen modularen Anlagenbau nach NE 148 Modulvariante II aussehen könnten, ist ungewiss. Einen Ansatz stellt der TÜV Süd mit seinem Positions-papier dar. [12] Festzustellen bleibt, dass das Regelwerk auf den zukünftigen modularen Anlagenbau angepasst werden muss, indem dieser stärker berücksichtigt wird. Welche neuen Anforderungen dadurch entstehen, kann heute noch nicht gesagt werden. Aufgrund von eigenen Erfahrungen an dem wandlungsfähigen Montagesystem der SmartFactoryOWL stellen sich die nachfolgenden Punkte als mögliche Verbesserungen und Lösungsansätze heraus.

- Von Institutionen mit Einfluss in die Normungsgremien (z.B. VDMA, TÜV) müssen Sicherheitskonzepte für den modularen Maschinenbau mit autonomen Maschinen gefunden werden.
- Hersteller von Hard- und Software der funktionalen Sicherheit müssen mit ihren Produkten einfache generische Lösungen anbieten.
- Sicherheitsrelevante Sensoren müssen wie Produkte von Standardanwendungen in dem Funktionsumfang wachsen und intelligenter werden, siehe Praxisbeispiel 1.
- Die Nutzung eines einheitlichen herstellerunabhängigen Protokolls zur Übertragung von sicherheitsrelevanten Daten, wie beispielsweise OpenSafety, ist erforderlich.
- Es ist ein zertifizierter Mechanismus zur automatischen Erkennung von weiteren Sicherheitssteuerungen zu finden, der einen Austausch von sicherheitsrelevanten Daten ermöglicht, siehe Beispiel HIMA.
- In den Sicherheitssteuerungen sollten Informationen zu Gefährdungen hinterlegt sein. Mit diesen Angaben kann von der Sicherheitssteuerung festgestellt werden, ob das überwachte Maschinenmodul in Kombination mit den anderen Maschinenmodulen in Betrieb gehen darf, ohne dass ein erhöhtes Risiko entsteht. In diesem Zusammenhang ist der Einsatz von einer Klassifikation der Maschinenmodule sinnvoll. [12]

- Über einheitliche Funktionsbausteine muss ein standardisierter Austausch von festgelegten Informationen erfolgen, ähnlich wie OPC-UA für Standardanwendungen.

Die Firma HIMA bietet den bereits zertifizierten HICore Prozessor an. Dabei handelt es sich um eine Safety-System-on-Chip Lösung. Mit dieser Hardware und der zugehörigen Programmierumgebung ist es möglich, ein Produkt zu entwickeln, welches die oben genannten Anforderungen an zukünftige Sicherheitssteuerungen erfüllen könnte. Mit diesem Chip kann beispielsweise eine Sicherheitssteuerung zur Verarbeitung weniger digitaler Signale entwickelt werden. Wie heute üblich, kann diese Steuerung modular erweiterbar sein. Neben der Verarbeitung einiger digitaler Signale sollte der Fokus auf den automatischen Aufbau einer direkten Verbindung zu der nächsten Sicherheitssteuerung liegen. Es entsteht eine Maschine-zu-Maschine-Kommunikation, die für den Austausch von sicherheitsrelevanten Daten genutzt werden kann. Über einen Algorithmus, der evtl. in der Hardware implementiert ist, wird sichergestellt, dass die Sicherheitssteuerung sich automatisch in das vorhandenen Netzwerk korrekt einbindet. Dazu kann die Übermittlung einer einmaligen Identifikationsnummer und das Vorgeben von Parametern (Klassifikation der Maschine) zur Eingliederung in das modular aufgebaute Maschinensystem gehören. Sind bereits Steuerungen vorhanden, wird die Steuerung von den anderen mit Informationen versorgt. Mit Informationen von den vorhanden Steuerungen kann die Erwartungshaltung angepasst werden. Über diese Erwartungshaltung kann die Anzahl von benötigten Not-Halt-Signalen resultieren. Weiter sind Funktionen zu berücksichtigen, die es ermöglichen, die vor- und nachgelagerten Maschinenmodule zu erkennen und deren Prozesse in einen sicheren Zustand zu versetzen. Die mit dem HICore zu entwickelnde Sicherheitssteuerung sollte eine standardisierte Schnittstelle zum Austausch von sicherheitsrelevanten Daten zwischen Maschinen bieten. Diese standardisierte Schnittstelle muss noch geschaffen werden.

Praxisbeispiel 1

Das umgesetzte Sicherheitskonzept wurde auf die Beantwortung der Frage begrenzt, wie viele Maschinenmodule integriert sind. Die Beantwortung der weiteren Fragen, siehe Kapitel 2.1 Seite 3, wurde nicht weiter verfolgt. Es wurde der Gedanke verfolgt, gleichzeitig mit der Ermittlung der Anzahl von eingebrachten Maschinenmodule auch sicherheitsgerichtet festzustellen, welches Maschinenmodul an welchem Integrationsplatz eingebracht wurde. Zur Beantwortung wurde der Einsatz von RFID-Magnetschaltern in Betracht gezogen und festgestellt, dass dies nicht möglich ist. Der RFID-Code vom Betätiger, der vom Sensor ausgelesen und verarbeitet wird, wird vom Sensor nicht zur weiteren Verarbeitung ausgegeben. Derzeit kann durch den Einsatz von RFID-Magnetschaltern nur der Manipulationsschutz

erhöht und nur die Information der korrekten Betätigung gewonnen werden. Für diese Aussage wurde das Produktofolio von den Firmen ABB, Schmersal, Pilz und Sick analysiert und Produkte wurden zum Teil getestet. Zur besseren Beantwortung der oben betrachteten Fragestellung müssen die Sensoren vielfältiger werden, indem beispielsweise die Identifikationsnummer sicherheitsgerichtet ermittelt und ausgeben wird. Der einfache binäre Sensor reicht nicht mehr aus. Dies wurde bereits für Standardanwendungen erkannt und mit dem Konzept von IO-Link ein möglicher Lösungsansatz entwickelt. Der IO-Link-Ansatz auch für die Übertragung sicherheitsrelevanter Daten einzusetzen ist derzeit nicht geplant. [19] An anderer Stelle ist zu lesen, dass für dieses Thema eine Arbeitsgruppe gegründet wurde und in zwei bis drei Jahren die ersten Resultate zu erwarten sind. [20]

Ein anderer Ansatz zur Beantwortung von weiteren sicherheitsrelevanten Fragen, siehe Seite 3, ist der Einbezug der standardisierten Automatisierungstechnik. Das Risiko der falschen Beantwortung muss dabei über bestimmte Methoden, wie Redundanz, minimiert und bestimmt werden, damit diese für sicherheitsrelevante Funktionen eingesetzt werden kann. Dieses Vorgehen bedeutet, neben einem schlüssigen und gut dokumentierten Sicherheitskonzept, eine Überprüfung und Zertifizierung durch einen externen Zertifizierer. Dieser Ansatz stellt meistens eine Einzelfalllösung dar und kann nicht generisch auf ähnlich modular aufgebaute Maschinen übertragen werden.

Eine weitere Möglichkeit zur Implementierung von Sicherheitsfunktionen für ein wandlungsfähiges Montagesystem bietet, neben den in der Studienarbeit berücksichtigten Herstellern, mittlerweile auch die Firma Pilz an. Zum Zeitpunkt der Studienarbeit war von der Firma Pilz keine Aussage und Lösungsansatz für das wandlungsfähige Montagesystem zu bekommen. Mittlerweile kann dies in der Beteiligung an dem Forschungsprojekt SmartFactory KL begründet werden. Laut Produktinformationen und Nachfragen beim Vertrieb soll es mit der Steuerung PSS 4000 möglich sein, die Anforderungen der Industrie 4.0 zu erfüllen. Ermöglicht wird dies durch ein Multi-Master-Konzept. [21]

Beispiel HIMA

Im Rahmen der Studienarbeit wurde auch ein Automatisierungskonzept der funktionalen Sicherheit der Firma HIMA vorgestellt. [6, S. 57] In diesem Konzept konnte über die vielfältigen Implementierungsmöglichkeiten der angebotenen Steuerung eine sicherheitsgerichtete Maschine-zu-Maschine-Kommunikation aufgebaut werden. Damit wäre der Verzicht auf eine übergeordnete Steuerung möglich. Die Steuerung bietet einen großen Funktionsumfang und stellte im Vergleich die höchsten Kosten dar. Außerdem war der geschätzte Implementierungsaufwand vergleichsweise hoch. Nach den jetzigen Erkenntnissen dieser Bachelorarbeit ist der Einsatz der HIMatrix F30 03 und das von HIMA erarbeitete Konzept weiter zu ver-

folgen. Die Funktionen, die zu implementieren sind, können nicht nur im wandlungsfähigen Montagesystem eingesetzt, sondern auch in anderen modular aufgebauten Anlagen mit Steuerungen von HIMA weiter verwendet werden. Im folgenden Absatz wird ein ideales Produkt erdacht, welches von den eignen Erfahrungen und Vorstellungen beeinflusst wird.

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] 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).
- [3] 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.
- [4] 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.
- [5] 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).
- [6] Philip Kleen. »Erstellung eines Konzepts für die funktionale Sicherheit (Safety) für ein wandlungsfähiges Montagesystem, Vergleich von Lösungsmöglichkeiten«. 2015.
- [7] PHOENIX CONTACT, Hrsg. *Inline - Modul mit integrierter Sicherheitslogik und sicheren digitalen Ausgängen: UM DE IB IL 24 LPSDO 8 V3-PAC: Anwenderhandbuch*. 2992035. 3. Apr. 2013.
- [8] Michael Volz. Hrsg. von WEKA Fachmedien GmbH. 2014. URL: <http://www.elektroniknet.de/automation/sonstiges/artikel/114773/1/>.
- [9] Michael Volz. Hrsg. von DKE-Tagung zur IEC 61508 in Darmstadt. 2009. URL: https://www.dke.de/de/Wirueberuns/MitteilungenderDKEGeschaefsstelle/documents/vde%20dke%20-%20tagung%20zur%20iec%2061508%20_%20pr%C3%A4sentationen/sicherheitsbezogene%20bussysteme.pdf.

- [10] Bundesministerium für Arbeit und Soziales. *Interpretationspapier zum Thema „Gesamtheit von Maschinen“*. Hrsg. von Ausgabe von Makrolog. 2011. URL: http://www.bmas.de/SharedDocs/Downloads/DE/interpretationspapier-gesamtheit-von-maschinen.pdf;jsessionid=FE237C56333B1D6E57B82B5C4A0C2559?__blob=publicationFile (besucht am 24.08.2015).
- [11] Deutsches Institut für Normung. *Sicherheit von Maschinen - Integrierte Fertigungssysteme - Grundlegende Anforderungen*. Beuth Verlag GmbH. DIN EN ISO 11161:2010-10. Berlin, 2010.
- [12] 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.
- [13] das europäische Parlament und der Rat der Europäischen Union. *Maschinenrichtlinie; Richtlinie 2006/42/EG*. Veröffentlichung im Amtsblatt. 2006.
- [14] Hans Dipl.Ing. Ostermann. *Auswechselbare Ausrüstungen*. Hrsg. von MBT Mechtersheimer GbR. 2015. URL: <http://www.maschinenrichtlinie.de/maschinenrichtlinie/neue-mrl-2006-42-eg/anwendungsbereich/auswechselbare-ausruestungen/> (besucht am 24.08.2015).
- [15] Deutsches Institut für Normung. *Industrieroboter - Sicherheitsanforderungen - Teil 2: Robotersystem und Integration*. Beuth Verlag GmbH. DIN EN ISO 10218-2:2012-06. Berlin, 2011.
- [16] K.A. Schmersal GmbH & Co. KG, Hrsg. *Datenblatt - CSS 8-180-2P+D-E-LST*. deutsch. 12. Nov. 2015.
- [17] PHOENIX CONTACT, Hrsg. *Anwenderhandbuch. UM DE IB IL 24 PSDI 8-PAC*. deutsch. 2910444. 25. Juni 2013.
- [18] PHOENIX CONTACT, Hrsg. *PSR-...-24UC/URM4/5X1/2X2/B. Sicherheitsrelais zur Kontakterweiterung*. deutsch. 100517_de_02. 12. Mai 2014.
- [19] TMG Technologie und Engineering GmbH. *FAQs. Ist die Übertragung sicherheitsrelevanter Daten, z.B. Not-Aus-Befehle über IO-Link möglich?* deutsch. 2015. URL: <http://www.io-link.com/de/FAQ/FAQs.php?thisID=9#Frage10> (besucht am 08.11.2015).
- [20] Joachim Lorenz. *PROFINews 116. IO-Link is on its way!* PNO. Mai 2014. URL: <http://www.profibus.com/newsroom/profinews-newsletter/profinews-2014-v2/profinews-116-io-link-is-on-its-way> (besucht am 08.11.2015).

- [21] Pilz GmbH & Co. KG. *Industrie 4.0. Antworten auf die Fragen der Zukunft.* deutsch. Webcode 83549. 2015. URL: <https://www.pilz.com/de-INT/company/industry40> (besucht am 09.11.2015).

Anlage: Inhalt der CD-ROM

- Bachelorarbeit_Kleen_Druck.pdf: verwendete Druckvorlage
- Bachelorarbeit_Kleen.pdf: digitale Kopie
- StromlaufplanTestaufbau.pdf: Stromlauf- und Montageplan für den Testaufbau
- Abbildungen
- digitale Quellen
- SAFECONF-Projektdateien