

Lehrstuhl für
Fördertechnik Materialfluss Logistik
der Technischen Universität München

**Sicherheit automatisierter Krananlagen
im personenzugänglichen Umfeld**

Ingomar Schubert

Vollständiger Abdruck der von der Fakultät für Maschinenwesen der Technischen Universität München zur Erlangung des akademischen Grades eines

Doktor-Ingenieurs (Dr.-Ing.)

genehmigten Dissertation.

Vorsitzender: Univ.-Prof. Dr.-Ing. M. Zäh

Prüfer der Dissertation:

1. Univ.-Prof. Dr.-Ing. W. A. Günthner
2. Univ.-Prof. Dr. rer.nat. H. Bubb

Die Dissertation wurde am 29.09.2005 bei der Technischen Universität München eingereicht und durch die Fakultät für Maschinenwesen am 30.11.2005 angenommen.

Danksagung

Die vorliegende Arbeit entstand während meiner Tätigkeit als wissenschaftlicher Mitarbeiter am Lehrstuhl für Fördertechnik Materialfluss Logistik der Technischen Universität München.

Meinem verehrten Doktorvater, Herrn Prof. Dr.-Ing. W.A. Günthner, danke ich für die Überlassung der interessanten Themenstellung, seine ständige Hilfs- und Diskussionsbereitschaft und für das große Interesse, das er meiner Arbeit entgegen gebracht hat.

Herrn Prof. Dr.rer.nat. H. Bubb danke ich für die bereitwillige Übernahme des Ko-referats zu dieser Arbeit.

Herrn Prof. Dr.-Ing. M. Zäh danke ich für die Übernahme des Vorsitzes der Prüfungskommission.

Meinen Kollegen und denjenigen Mitarbeitern des Institutes, die durch ihre Mithilfe zur Fertigstellung dieser Arbeit beigetragen haben, besonders Herrn Dipl.-Ing. Niels Blomeyer und Herrn Dr.-Ing. Martin Webhofer, möchte ich an dieser Stelle ebenfalls danken.

Schließlich gilt mein Dank meiner Familie, die durch ihr Verständnis und ihre Geduld zum Gelingen dieser Arbeit beigetragen hat.

München im Dezember 2005

Ingomar Schubert

Inhaltsverzeichnis

1	Einleitung	. 1
1.1	Problemstellung	. 3
1.2	Ziel der Arbeit	. 4
1.3	Lösungsweg	. 4
2	Begriffsabgrenzungen	. 7
2.1	Schaden	. 7
2.2	Gefahr und Gefährdung	. 8
2.3	Sicherheit	. 9
2.4	Unfall, Gefahrenfall, Störfall, Zwischenfall	. 9
2.5	Risiko	. 9
2.6	Versagen	. 10
2.7	System	. 11
3	Stand der Technik	. 13
3.1	Automatisierte Krane	. 13
3.2	Steuerungstechnik	. 17
3.3	Bestehende Richtlinien und Vorschriften	. 18
3.3.1	Das europäische Regelwerk	. 18
3.3.2	Nationale Vorschriften	. 21
3.3.3	Unfallverhütungsvorschriften	. 21
3.3.4	VDI-Richtlinien	. 23
3.3.5	Normen zur Sicherheit	. 24
3.3.6	Normen für Steuerungstechnik	. 25
3.3.7	Normen für sicherheitsrelevante Software	. 25
3.4	Anwendbarkeit auf Krane	. 27

4	Systemanalyse	29
4.1	Logische Strukturen und Systemfunktionen	29
4.2	Verteilungsfunktionen und statistische Kenngrößen	31
4.3	Funktionale Abläufe	33
4.4	Bauteile	43
4.4.1	Bauteile des manuellen Kranes	43
4.4.2	Bauteile des automatisierten Kranes	43
5	Die Sicherheitsanalyse	45
5.1	Aufgaben und Ziele	45
5.2	Allgemeiner Ablauf	46
5.3	Vorläufige Gefahrenanalyse	49
5.3.1	Das Verfahren der vorläufigen Gefahrenanalyse	49
5.3.2	Nutzen und Grenzen der vorläufigen Gefahrenanalyse	54
5.4	Fehler Möglichkeits- Einflussanalyse	55
5.4.1	Das FMEA-Verfahren	55
5.4.2	Nutzen und Grenzen der FMEA	57
5.5	Fehlerbaumanalyse	59
5.6	Weitere Methoden	60
5.7	Menschliches Versagen	63
5.7.1	Quantifizierung	64
5.8	Das SHEL-Modell	65
5.9	Sicherheitsanalyse automatisierter Krane	69
6	Gefährdungen	73
6.1	Gefahren durch äußere Umstände	73
6.1.1	Physikalische Gefahren	73
6.1.2	Gefahr durch Vibration	74
6.1.3	Gefahr durch Eingeschlossensein	74
6.1.4	Gefahr durch Betreten	74
6.1.5	Gefahr durch Wartungsarbeiten	75
6.1.6	Gefahr durch unvollständige Arbeit	75
6.1.7	Gefahr durch Änderungen	75
6.2	Fehler aus Software	75
6.3	Gefahren aus dem Kranbetrieb	76
6.3.1	Gefahren aus <i>Position teachen</i>	76

6.3.2 Gefahren durch falsche Inbetriebnahme	76
6.3.3 Gefahren durch Kranruf	77
6.3.4 Gefahren der Leerfahrt	77
6.3.5 Gefahren aus der Lastaufnahme	77
6.3.6 Gefahren der Lastfahrt	78
6.3.7 Gefahren aus der Lastabgabe	78
6.3.8 Gefahren aus der Quittierung der manuellen Kranfahrt	78
6.4 Fehlerbaumanalyse	79
7 Sichere Maschinen	85
7.1 Erreichen der Sicherheit	85
7.2 Auswahl von Schutzeinrichtungen	88
7.3 Verhalten bei Fehlern	93
7.4 Rolle des Menschen	93
8 Sicherheitsleitlinien	95
8.1 Horizontale Kranbewegung	96
8.2 Vertikale Kranbewegung	100
8.3 Lastaufnahme	102
8.4 Lastabgabe	107
8.5 Lastaufnahmemittel	108
8.6 Übergabestationen	110
8.7 Steuerung und Kommunikation	117
8.8 Leitlinienkatalog	124
9 Zusammenfassung	129
10 Literaturverzeichnis	131
A Liste der wichtigsten nationalen Vorschriften für Krane	135
B Tabelle zur Gefahrenanalyse	141

Abbildungsverzeichnis

1-1	Kranunfälle nach auslösenden Ursachen	3
2-1	Risikokurve	10
2-2	Grenz- und Restrisiko	10
3-1	Betriebsarten Brückenkrane	14
3-2	Versuchsanlage am Lehrstuhl fml	16
3-3	Regelwerk für Krane	20
3-4	Übersicht der Normen im Bereich Steuerung	25
4-1	Systemanalyse	31
4-2	Ausfallrate in Abhängigkeit von der Zeit (Badewannenkurve)	32
4-3	Zustandsänderungen der Betriebsarten	33
4-4	Manueller Kranbetrieb	35
4-5	Versandbetrieb	36
4-6	Rufbetrieb	37
4-7	Ruf- und Versandbetrieb	38
4-8	Ruf- und Versandbetrieb mit automatischer Lastaufnahme	39
4-9	Ruf- und Versandbetrieb mit automatischer Lastabgabe	40
4-10	Versandbetrieb mit automatischer Lastabgabe	41
4-11	Vollautomatischer Betrieb	42
4-12	Manueller Brückenkrane	43
4-13	Automatisierter Brückenkrane	44
5-1	Stufen der Sicherheitsanalyse 1	47
5-2	Stufen der Sicherheitsanalyse 2	48
5-3	Fehlerbaumsymbole	59
5-4	Das SHEL Modell	67
5-5	Methode der Gefahrenermittlung	69
5-6	Durchführung der Gefahrenermittlung	70
6-1	Fehlerbaum Teil 1	80
6-2	Fehlerbaum Teil 2	81
6-3	Fehlerbaum Teil 3	82

6-4	Fehlerbaum Teil 4	82
6-5	Fehlerbaum Teil 5	83
7-1	Iterativer Prozess zum Erreichen der Sicherheit	86
7-2	Mögliche Auswahl der Schutzkategorien nach EN 954-1	88
7-3	IEC 61508	92
8-1	Kranlastspiel	96
8-2	Sichere Raumstruktur	97
8-3	Mögliche selbstsichere Verriegelungen	98
8-4	Sicherheitsabstand	99
8-5	Positionierung von LAM und Last über Lichttaster	104
8-6	Unsichere Palette auf sicherer Adapterpalette	105
8-7	Sichere Transporteinheit aus Adapterpalette und geschlossenem LAM	107
8-8	Lastaufnahmemittel nur für geschlossene GLT	109
8-9	Geschlossenes Lastaufnahmemittel	110
8-10	Varianten zur Sicherung von Übergabestationen	112
8-11	Logik zur Absicherung von Übergabestationen	113
8-12	Logik mit Anlaufstufung	114
8-13	Lichttaster zur Positionsüberwachung	115
8-14	Sichere Übergabestation und ihre Elemente	117
8-15	Sicheres Steuerungskonzept	121

Tabellenverzeichnis

3-1	Entwicklungspotentiale automatisierter Krane	15
3-2	Unfallverhütungsvorschriften	23
3-3	Relevante DIN-Normen zur Sicherheit	24
3-4	Normenreihe: Funktionale Sicherheit	26
3-5	Definition der Anforderungsstufen	26
3-6	Gegenüberstellung der Anforderungsklassen	27
4-1	Rechenregeln für boolesche Operationen	30
5-1	Ergebnistabelle der PHA	52
5-2	Auslöser für Unfälle	53
5-3	Einteilung der Unfallhäufigkeit	54
5-4	Faktoren zur Berechnung der RPZ	58
5-5	Leitworte und deren Bedeutungen	61
5-6	Gängige Methoden zur Sicherheitsanalyse	64
5-7	TESEO-Faktoren	66
7-1	Sicherheitsmaßnahmen im Maschinenbau	88
7-2	Schutzkategorien nach DIN EN 954-1	90
7-3	Entscheidungsweg zur Kategorieauswahl nach EN 954-1	91
7-4	Sicherheitsfunktionen von Antriebssystemen in Maschinen	94
8-1	Signalmatrix 1	122
8-2	Signalmatrix 2	123

Abkürzungsverzeichnis

BG	Berufsgenossenschaft
BGV	Berufsgenossenschaftliche Vorschriften
CPU	Central Processing Unit
DIN	Deutsches Institut für Normung
EMV	Elektromagnetische Verträglichkeit
EN	Europäische Norm
EWG	Europäische Wirtschaftsgemeinschaft
FMEA	Fehler Möglichkeits- Einflussanalyse
FTA	Fault Tree Analysis
GLT	Großladungsträger
GSG	Gerätesicherheitsgesetz
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
KLT	Kleinladungsträger
LAM	Lastaufnahmemittel
MOSAR	Method Organized for a systematic Analysis of Risk
PAAG	Prüfen, Auffinden, Auswirkungen und Gegenmaßnahmen
PHA	Preliminary Hazard Analysis
RCM	Reliability Centered Maintenance
SPS	Speicherprogrammierbare Steuerung
TESEO	Tecnica Empirica Stima Errori Operatori
TÜV	Technischer Überwachungsverein
UVV	Unfallverhütungsvorschrift
VBG	Verwaltungs-Berufsgenossenschaft
VDI	Verein Deutscher Ingenieure
VDE	Verband der Elektrotechnik, Elektronik und Informationstechnik

1 Einleitung

Flexible Fertigungsstrukturen brauchen flexible Materialflusssysteme. Für diese Forderung ist ein den Anforderungen einer sich ständig im Wandel befindlichen Produktion entsprechendes leicht anpassbares Fördersystem für den innerbetrieblichen Transport notwendig. Eine Möglichkeit, dieser Anforderung gerecht zu werden, besteht darin, den Materialtransport mit einem Kran in eine Ebene oberhalb der Produktionsebene zu verlagern. Durch einzelne Krane oder verbundene Krananlagen hat man den Vorteil, dass der Materialfluss unabhängig vom Produktionslayout gestaltet werden kann, da je nach Bedarf über die Produktionsanlagen hinweg andere Positionen mit dem Kran angefahren werden können [1].

Im Sinne der vorliegenden Arbeit dienen Krane, ähnlich wie viele andere Maschinen und Geräte in der gewerblichen Wirtschaft, dem innerbetrieblichen Transport von Material. Vom Fachmann werden Krane als Hebezeuge bezeichnet, bei denen Lasten mit einem Tragmittel (z.B. Seil mit Haken) gehoben und zusätzlich in eine oder mehrere Richtungen bewegt werden können.

Entscheidend für die Entwicklung dieser Krane ist der Wandel in der Automatisierungstechnik. Aufgrund der hohen Automatisierungskosten haben sich stufenweise programmgesteuerte Kransysteme in den Ausprägungen

- manueller Kran
- teilautomatischer Kran mit automatischen Leer- und Lastfahrten
- vollautomatischer Kran mit automatisierter Lastübergabe

als wirtschaftlich erwiesen [1].

Krane gelten als programmgesteuert, wenn nach Erteilung eines entsprechenden Befehls eine oder mehrere Kranbewegungen selbsttätig ablaufen. Es handelt sich dabei um solche Krane, bei denen ein Kranführer, der die Bewegungen des Kranes, der Lastaufnahmeeinrichtung und der Last ständig beobachtet sowie jederzeit steuernd eingreifen kann, nicht vorhanden ist [2].

Für Krananlagen, die bereits und zukünftig vermehrt für diese Aufgaben in unterschiedlichen Automatisierungsstufen oberhalb der Produktion, also in für Personen

zugänglichen Bereichen im Einsatz sind, gibt es keine einheitlichen Vorschriften, Richtlinien und Abnahmekriterien. Jede Automatikkrananlage wird gesondert untersucht, geprüft und abhängig von Hersteller und Prüfer in unterschiedlichen Ausführungsformen in Betrieb genommen.

Aus der oben geschilderten Notwendigkeit, den Transport im personenzugänglichen Umfeld durchzuführen, und der Tatsache, dass kein Kranführer den Kranbetrieb überwacht, entstehen erhebliche Gefahren. Von diesen Gefährdungen wären nicht nur die unmittelbar mit dem Kran Beschäftigten, sondern auch Personen, die im Arbeitsbereich von Kranen beschäftigt sind oder sich dort aufhalten, betroffen.

Weiterhin besteht, unabhängig davon, ob der Kran automatisiert oder manuell betrieben wird, ein Verbesserungspotential hinsichtlich der Arbeitssicherheit. Im Jahre 2002 wurden etwa 5800 Unfälle durch Krane gemeldet, 343 Fälle mussten aufgrund ihrer Verletzungsschwere einer neuen Unfallrente zugeführt werden. Es waren 23 Todesfälle zu beklagen. Darüber hinaus sind Unfälle durch Krane mit relativ schweren Verletzungsfolgen verbunden. Jeder 17. meldepflichtige Arbeitsunfall führte 2002 zu einer Rentenzahlung, während im Mittel über alle betrieblichen Arbeitsunfälle in der gewerblichen Wirtschaft nur jeder 51. Arbeitsunfall zu einer neuen Unfallrente führte. Dabei treten bezüglich der Unfallzahlen klar drei Krantypen hervor. In 2002 wurden 36% der meldepflichtigen Unfälle für Brückenkranen und 14% für Turmdrehkrane bzw. 21% für Mobilkrane ausgewiesen. Mit deutlich niedrigeren Fallzahlen sind Portal- und Auslegerkrane aufgelistet [3].

Die Statistik belegt, dass sich nur 22% der Unfälle, die durch Krane, deren Teile oder die angeschlagene bzw. transportierte Last ausgelöst wurden, beim Bedienen oder Steuern ereigneten. 26% der Unfälle kommen beim Handhaben bzw. Umgehen mit Hilfsmitteln, wie z.B. Anschlagmitteln, Lastaufnahmeeinrichtungen, Transportbehältern u.Ä., zustande.

Eine statistische Feinanalyse der Unfälle von Kranen, wie in Abbildung 1-1 dargestellt, weist nach, dass für 2001 und 2002 allein ein Anteil von über 50% der Fälle darauf zurückzuführen ist, dass die angeschlagene bzw. transportierte Last für die Auslösung des Unfalls verantwortlich war. In etwa einem Fünftel der Fälle geht aus der Unfallschilderung hervor, dass das mit dem Kran fest verbundene Tragmittel (Seil mit Haken, Flasche, Greifer u.Ä.) das zur Verletzung führende Ereignis ausgelöst hat. Weitere 7% der meldepflichtigen Unfälle können auf den Aufstieg zum Führerstand des Kranes zurückgeführt werden.

Möchte man nun Krananlagen nicht nur für einzelne schwere und große Lasten, sondern auch vermehrt für den innerbetrieblichen Behältertransport, insbesondere im personenzugänglichen Bereich, einsetzen, ist ein Sicherheitskonzept anzustreben, mit dem die bisherigen Unfallzahlen zumindest nicht überschritten werden.

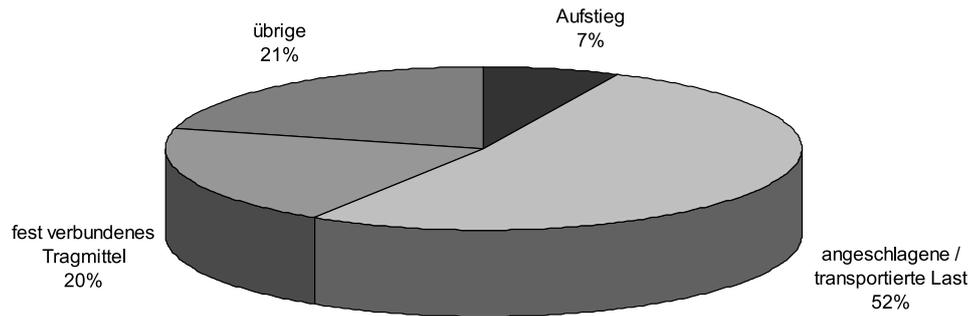


Abb. 1-1: Kranunfälle nach auslösenden Ursachen

Ein weiteres Problem stellt sich dem Hersteller solcher Krananlagen hinsichtlich des bestehenden Regelwerkes für die sicherheitstechnische Auslegung automatisierter Krananlagen. Hier offenbaren sich große Spielräume, die das wirtschaftliche Risiko erheblich erhöhen, wenn die sicherheitstechnische Abnahme der Anlage nicht vorherzusehen ist.

Flexible Automatikkran- und Automatikbahnanlagen sind nur dann effiziente Transportsysteme im innerbetrieblichen Materialfluss, wenn verlässliche Aussagen für die im jeweiligen Automatisierungsgrad notwendige Sicherheitstechnik gemacht werden können. Dies führt zu Einsparungen im Projektierungsaufwand bei Umbau- und Aufrüstungsmaßnahmen zur Anpassung des Transportsystems an veränderte Produktionsstrukturen.

Aus der Notwendigkeit viele Ursachen für Unfälle, die im manuellen Kranbetrieb entstehen können, zu eliminieren, und dem Fehlen eines einheitlichen Regelwerkes hat es sich als notwendig erwiesen, Leitlinien zur sicherheitsgerechten Auslegung von Automatik-Krananlagen für den personenzugänglichen Bereich zu ermitteln.

1.1 Problemstellung

Ein Schlüsselaspekt beim Einsatz von Automatikkrananlagen im produzierenden Umfeld ist die erreichbare Sicherheit. Aus der Notwendigkeit, Transporte im personenzugänglichen Umfeld durchzuführen, und der Tatsache, dass kein Kranführer den Kranbetrieb überwacht, entstehen erhebliche Gefährdungen.

Von diesen Gefährdungen wären nicht nur die unmittelbar mit dem Kran Beschäftigten, sondern auch Personen, die im Arbeitsbereich von Kranen tätig sind, betroffen. Bei Konstruktion, Bau und Betrieb von Kranen ist deshalb die Einhaltung von sicherheitstechnischen Prinzipien unbedingte Voraussetzung für die Vermeidung von Gefährdungen, die sich z.B. aus einem Lastabsturz oder Versagen der Krankonstruk-

tion für Leben und Gesundheit von Personen sowie Sachen und Umwelt ergeben können.

Eine systemtechnische Einbindung von Automatikkrananlagen in den innerbetrieblichen Materialfluss erfordert stets eine Klärung der Anlagensicherheit in der jeweiligen Ausgestaltung. Die Flexibilität, die für die Realisierung der einzelnen Anwendungen und Automatisierungsstufen notwendig ist, wird zumeist durch modulare Systemgestaltung erreicht. Eine frühe Einbeziehung der Anlagensicherheit in die konzeptionellen und konstruktiven Überlegungen zu diesem Baukastensystem hat eine hohe Bedeutung. Die Erhöhung des Automatisierungsgrades erfordert beispielsweise stets Erweiterungen im Sicherheitskonzept, um die erweiterten Automatikvorgänge abzusichern. Deshalb muss das Sicherheitskonzept so durchgängig sein, dass es für die jeweilige Automatisierungsstufe anpassbar ist.

Vorgaben dafür liefert neben den Unfallverhütungsvorschriften der Berufsgenossenschaften [4, 5, 6, 7] die VDI-Richtlinie 3653 „Automatisierte Kransysteme“ [8]. Aus Gründen der Einbuße an Ortsflexibilität kommen einige mögliche Maßnahmen zur Absicherung der automatischen Lastfahrt, wie z.B. das Unterfangen der Last über Zwischendecken oder Abschränken des Kranbereiches, nicht in Betracht.

Hinzu kommt zukünftig die Anforderung, dass ein Kransystem, welches aus einzelnen Bausteinen zusammengesetzt und in unterschiedlichen Automatisierungsstufen arbeiten kann, in jeder der möglichen Konfigurationen die Sicherheitsanforderungen erfüllen muss. Der in der EG-Maschinenrichtlinie geforderte Sicherheitsnachweis kann mit der Anwendung der genannten Empfehlungen alleine nicht erbracht werden. Zusammenfassend gilt: Den besonderen Anforderungen eines gemeinsam mit Personen in einem Arbeitsraum operierenden automatisierten Kransystem wird letztlich keine der genannten Normen und Richtlinien gerecht.

1.2 Ziel der Arbeit

Ziel der vorliegenden Arbeit ist die Erstellung eines durchgängigen Sicherheitskonzepts für Automatikkran- und -hängebahnanlagen für den innerbetrieblichen Behältertransport und die Erarbeitung von Leitlinien für deren sicherheitstechnische Auslegung.

Dieses zu schaffende Sicherheitskonzept ist im Einvernehmen mit dem Fachausschuss Hebezeuge/Krane der Berufsgenossenschaften abzustimmen, da die Berufsgenossenschaften als Versicherungsträger das verbleibende Restrisiko versichern müssen.

1.3 Lösungsweg

Um ein sicherheitstechnisch vollständiges Regelwerk zu erhalten, sind hier die wesentlichen Schritte, die zur Erarbeitung von Sicherheitsleitlinien für Automatikkran-

anlagen für den innerbetrieblichen Behältertransport im produzierenden Umfeld notwendig sind, angegeben:

- Analyse bestehender Vorschriften und Richtlinien zu Krananlagen: Die in Unfallverhütungsvorschriften (UVV) und Richtlinien genannten Vorschriften werden zusammengestellt und die enthaltenen Handlungsanweisungen auf die Anwendbarkeit für den beschriebenen Einsatzfall überprüft.
- Systemanalyse automatisierter Krananlagen: Analyse, aus welchen Bauteilen ein Kran besteht. Untersuchung, welche zusätzlichen Merkmale einen automatisierten Kran auszeichnen und in welchen Betriebszuständen automatisierte Krane genutzt werden.
- Ermittlung einer Methodik zur Durchführung der Sicherheitsanalyse: Eine Reihe von Normen und Normentwürfen (DIN 25419, DIN 25424-1 und -2, DIN 25448, DIN EN 1050, ...) gibt Hinweise und Hilfestellungen für die Erfassung von Gefährdungsursachen. Hieraus soll eine Methodik für die Umsetzung einer Gefahrenanalyse für Automatikkrananlagen im produzierenden Umfeld erarbeitet werden.
- Zusammenstellung eines vollständigen Katalogs möglicher mechanischer und steuerungstechnischer Gefahrenursachen: Mit der Methodik aus dem vorhergehenden Schritt wird ein Gefährdungsursachenkatalog für das Baukastensystem Automatikran-Automatikbahn in den verschiedenen Automatisierungsstufen zusammengestellt. Hierbei ist zu überprüfen, ob die Fehlerursachen voneinander unabhängig sind.
- Ermittlung von Ursachen und Wirkungsbeziehungen: Anhand des Ursachenkatalogs werden Wirkungen untersucht. Es ist zu berücksichtigen, dass gleichzeitig nur eine Störungsursache angenommen werden muss (Ein-Fehler-Sicherheit), diese jedoch eine Schar von Wirkungen erzeugen kann.
- Auswertung der Ergebnisse der Sicherheitsanalyse: Für die ermittelten Ursache-Wirkungsbeziehungen werden Maßnahmen zur Vermeidung erarbeitet und in einem Katalog zusammengestellt.
- Formulierung von Handlungsanweisungen für die sicherheitsgerechte Gestaltung von Automatikkrananlagen für den innerbetrieblichen Behältertransport.

2 Begriffsabgrenzungen

In der Begriffswelt der Zuverlässigkeits- oder Sicherheitstechnik gibt es in vielen Technologie-Ländern teils erbitterte, stets aber unfruchtbare Streitigkeiten [9], welche aus dem Problem resultieren, dass die Umgangssprache sich nur schlecht als Fachsprache einer Ingenieurdisziplin eignet.

Aus diesem Grund sollen in den folgenden Abschnitten Begriffe der Sicherheitstechnik erläutert werden.

2.1 Schaden

Das Wort Schaden hat, je nach dem in welchem Zusammenhang es verwendet wird, verschiedene Bedeutungen. Die sprachliche und ingenieurmäßige Bedeutung dieser Worte kann durch ihre Verschiedenheit einen entgegengesetzten Eindruck hervorrufen. Auf der einen Seite wird im normalen Umgang das Wort Schaden verwendet, wenn etwas zerbrochen oder so weit beschädigt ist, dass es nicht mehr verwendet werden kann. Auf der anderen Seite gibt es die andere alltägliche Sichtweise, dass Schaden mehr durch ein Ereignis und weniger durch den normalen Gebrauch einer Sache verursacht wird.

Matthews [10] definiert den Begriff Schaden auf andere ingenieurmäßige Weise. Aus seiner Sicht ist Schaden nicht unbedingt als das Ergebnis eines Ereignisses zu betrachten, obwohl das auch so sein kann, sondern er definiert Schaden durch den Zustand, in dem eine plastische Deformation an einem Gegenstand aufgetreten ist, wenn dieser mit dem als neu bezeichneten Zustand des Gegenstandes verglichen wird. Das Wichtigste bei dieser Definition ist, dass das beschädigte Bauteil weiter verwendet werden kann. Schaden heißt bei Matthews also nicht unbedingt Versagen. Im weitesten Sinne schließt der Schaden die Auswirkungen der Ermüdung, Abnutzung oder Korrosion mit ein, so dass Schaden sichtbar oder auch unsichtbar sein kann.

Im rechtlichen Bereich wird unter „Schaden“ jede Beeinträchtigung einer Person an ihren Rechtsgütern verstanden. Der Begriff Rechtsgüter wird heute vor allem auch auf Natur und Umwelt ausgedehnt. Hinsichtlich der Sicherheitswissenschaft ist allerdings eine Einschränkung vorzunehmen. Unter „Schaden“ kann man im Rahmen der

Sicherheitswissenschaft nur solche Beeinträchtigungen verstehen, die aufgrund der Nutzung der Technik auftreten. Unter Beachtung des vorher Gesagten kann folgende Begriffsfestlegung nach Kuhlmann [11] gewählt werden:

„Schaden“ im Sinne der Sicherheitswissenschaft ist die Beeinträchtigung einer Person an ihren Rechtsgütern aufgrund der physikalisch-chemischen Einwirkungen infolge der Nutzung der Technik.

Verglichen mit der ersten Definition von Matthews werden hier auch Personen mit in die Definition eingeschlossen, wo hingegen bei Matthews nur Gegenstände betrachtet werden.

Für die vorliegende Arbeit soll die erweiterte Definition nach Kuhlmann verwendet werden, da es sich bei der Entwicklung der Sicherheitsleitlinien besonders darum handelt, die Sicherheit für Personen zu erhöhen.

Weiterhin können noch zwei weitere Arten von Schaden unterschieden werden, die zwar in erster Linie nicht technischer Natur sind, aber oft benutzt werden, und deshalb auch hier behandelt werden sollen. Dabei handelt es sich um die Begriffe „Direkter Schaden“ und „Folgeschaden“. Diese Begriffe lassen sich anhand eines sehr stark vereinfachten Beispiels erläutern. Dazu soll folgendes Szenario betrachtet werden:

Das Litzenseil eines Brückenkranes reißt beim Heben einer Last, die schwerer als das zulässige Hubgewicht ist. Die Last besteht aus einem schweren und zerbrechlichen Gut, das beim Aufschlag auf den Boden zerbricht. Durch den Aufprall wird auch der Boden beschädigt. Das zerrissene Seil zerschlägt Steuerelemente auf der Kranbrücke.

Direkter Schaden:

Der direkte Schaden ist der Schaden, der Teil des fehlerhaften Ereignisses ist. In diesem Fall ist es das zerrissene Seil, das den direkten Schaden erlitten hat. Dabei ist zu beachten, dass der direkte Schaden mit dem Fehler (Heben einer zu schweren Last) in Verbindung gebracht werden kann.

Folgeschaden:

Schaden, der als Folgeschaden eingestuft wird, muss eine Folge des direkten Schadens sein, enthält aber nicht den direkten Schaden. In diesem Beispiel ist es die zerstörte Steuerung auf der Kranbrücke, die zerbrochene Ladung und die Beschädigung am Boden.

2.2 Gefahr und Gefährdung

Gefahr kann von der Nutzung eines technischen Systems ausgehen und bedeutet die Möglichkeit einer Schädigung von Mensch oder Sachgut.

Gefährdung kann sich für Mensch und Sachgut ergeben, wenn ein technisches System genutzt wird und sich Mensch und Sachgut in seinem Wirkungsbereich befinden.

2.3 Sicherheit

Der Begriff Sicherheit enthält – entsprechend dem im vorangehenden Abschnitt Gesagten – das Maß an Gewissheit, dass die möglichen Schäden nicht auftreten. Bei CoVan [12] wird Sicherheit als relative Akzeptanz für Verluste angesehen, nicht wie die sonst allgemein angewandte Definition von der Abwesenheit von Risiko und Gefahr.

2.4 Unfall, Gefahrenfall, Störfall, Zwischenfall

- Ein Unfall ist ein unvorhergesehen eintretendes, zeitlich begrenztes Ereignis, das eine Körperschädigung oder Sachbeschädigung mit sich führt [11]. Etwas allgemeiner ist nach CoVan [12] ein Unfall eine ungeplante Unterbrechung der Geschäftsaktivität, die allgemein zu einem Verlust führt.
- Ein Gefahrenfall ist ein unvorhergesehen eintretendes, zeitlich begrenztes Ereignis, das die Gefahr einer Körperschädigung oder Sachbeschädigung mit sich führt. „Gefahrenfall“ ist somit ein Oberbegriff von „Unfall“ [11].
- Ein Störfall ist ein unvorhergesehen eintretender, zeitlich begrenzter Ereignisablauf in einem technischen System, bei dem nicht von vornherein auszuschließen ist, dass ein Gefahrenfall vorliegt [11].
- Ein Zwischenfall ist ein unerwünschter, unvorhergesehen eintretender, zeitlich begrenzter Ereignisablauf („gestörter Betrieb“) in einem technischen System. „Zwischenfall“ ist ein Oberbegriff von „Störfall“ [11].

2.5 Risiko

Eine sehr allgemeine Definition für Risiko gibt CoVan [12]. Demnach ist Risiko das Ergebnis einer Verlust-Ereigniswahrscheinlichkeit und der Akzeptanz dieses Verlusts. Andere gängige Definitionen des Individualrisikos lauten hingegen

$$\text{Risiko} = \text{Schadensumfang} \times \text{mittlere Schadenshäufigkeit}$$

oder

$$\text{Risiko} = \text{Schadensumfang} \times \text{Schadenseintrittswahrscheinlichkeit}$$

Es besteht ein funktionaler Zusammenhang zwischen der Eintrittswahrscheinlichkeit und der Ernsthaftigkeit bzw. dem Schadensumfang. Dieser ist in Abbildung 2-1 dargestellt. Je größer darin das Ausmaß des Schadens ist, desto geringer ist die Eintrittswahrscheinlichkeit für diesen Schaden.

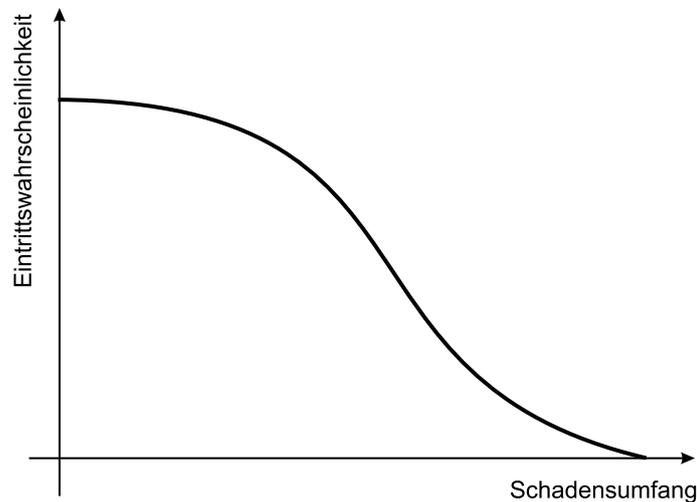


Abb. 2-1: Risikokurve

Neben dem Oberbegriff Risiko gibt es noch die Begriffe Restrisiko und Grenzzisiko. Das Restrisiko bezeichnet das, wie in Abbildung 2-2 dargestellte, verbleibende um die tatsächliche Risikoreduzierung verringerte Risiko. Das Grenzzisiko ist das maximal vertretbare Restrisiko, das nach einer Mindest-Risikoreduzierung verbleibt.

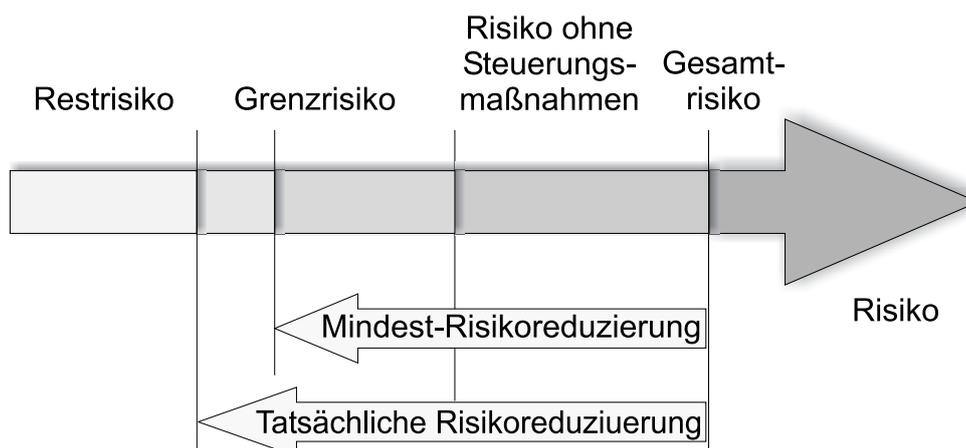


Abb. 2-2: Grenz- und Restrisiko

2.6 Versagen

Matthews [10] unterscheidet je nach Zusammenhang zwei Bedeutungen für das Wort Versagen. Zum einen gibt es eine rein sprachliche Definition mit der offensichtlichen

Bedeutung, dass etwas verbogen, verdreht oder gebrochen ist. In der Folge kann es in irgendeiner Weise nicht mehr für die Aufgabe, für die es gedacht war, verwendet werden. Demnach ist im normalen Sprachgebrauch das Versagen das Ergebnis eines Versagensereignisses.

Zum anderen gibt es die strenge ingenieurmäßige Definition, die auch in der vorliegenden Arbeit verwendet wird. Hier beschreibt das Wort Versagen einen allgemeinen Ausdruck für einen Zustand, in dem ein Bauteil eine plastische Verformung erfährt, wobei sich ein Bauteil, das sich rein formal in einem Versagenszustand befindet, in verschiedenen Zuständen, wie zum Beispiel in einem verbogenen, angebrochenen oder vollständig zerbrochenen Zustand, befinden kann.

2.7 System

Im Folgenden wird von einem System gesprochen, wenn von einer automatisierten Krananlage die Rede ist. Unter einem System werden in diesem Fall alle Faktoren und Komponenten sowie unabhängige und abhängige Aktivitäten verstanden, die in einer vorhersehbaren Art und Weise interagieren, um etwas innerhalb gewisser Grenzen zu beschreiben [12].

3 Stand der Technik

Automatisierte skalierbare Hängekran- oder Hängebahnanlagen für den innerbetrieblichen Behältertransport bestehen noch nicht sehr lange. Daher existieren über diese Art von Materialflusssystemen nur wenige Arbeiten. Im folgenden Kapitel wird auf den Stand der Technik für automatisierte Krananlagen in Bezug auf Entwicklung, Betriebsarten und Steuerung eingegangen. Im letzten Abschnitt werden bestehende Richtlinien und Gesetze hinsichtlich ihrer Anwendbarkeit auf automatisierte Krananlagen beschrieben.

3.1 Automatisierte Krane

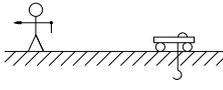
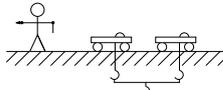
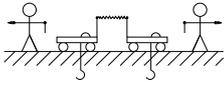
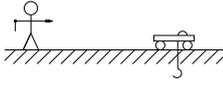
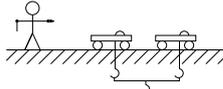
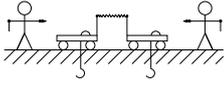
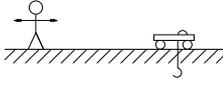
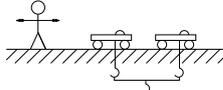
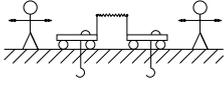
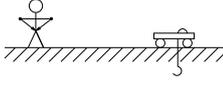
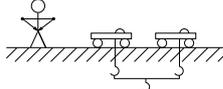
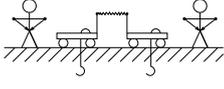
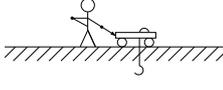
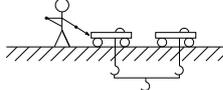
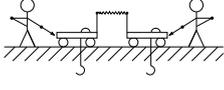
Die Entwicklung des Krans vollzieht einen Wandel vom reinen Hebezeug für schwere Lasten mit Bedienung durch einen Kranführer, bis hin zum Materialflusssystem auch für leichte und mittlere Lasten in unterschiedlichster Automatisierung. Entscheidend für diesen Wandel ist die Entwicklung der Automatisierungstechnik. Aufgrund der hohen Kosten wurde der Trend zur Vollautomatik im Prozesskranbereich durch eine skalierbare Automatisierung des Kransystems in den drei Stufen abgelöst:

- Manueller Kran,
- Teilautomatisierter Kran mit automatischer Leer- und Lastfahrt und
- Vollautomatischer Kran, der auch die Lastübergabe mit einschließt.

Wie in Abbildung 3-1 dargestellt, kann diese Unterscheidung noch genauer getroffen werden. Nach [13] wird nicht nur zwischen Hand- und Automatikbetrieb sondern auch zwischen den teilautomatischen Betriebsarten

- Rufbetrieb,
- Versandbetrieb sowie
- Ruf- und Versandbetrieb

unterschieden. Sollen Krane im Duobetrieb eingesetzt werden, also eine Last mit zwei Kranbrücken gehoben werden, wird noch zwischen einer mechanischen und einer informatorischen Kopplung unterschieden.

Kopplung	Ohne	Mechanisch	Informativ
Bedienung			
Rufbetrieb			
	Rufeinzelbetrieb	Rufkoppelbetrieb	Rufduobetrieb
Versandbetrieb			
	Versandeinzelbetrieb	Versandkoppelbetrieb	Versandduobetrieb
Ruf- und Versandbetrieb			
	Ruf- und Versand-einzelbetrieb	Ruf- und Versand-koppelbetrieb	Ruf- und Versand-duobetrieb
Automatikbetrieb			
	Automatik-einzelbetrieb	Automatik-koppelbetrieb	Automatik-duobetrieb
Handbetrieb			
	Handeinzelbetrieb	Handkoppelbetrieb	Handduobetrieb

Quelle:[13]

Abb. 3-1: Betriebsarten Brückenkran

In Tabelle 3-1 sind den vier Hauptvorteilen der Automatisierung ihre wesentlichen Anwendungsnutzen zugeordnet. Diese sehr allgemeine Übersicht ergibt sich, um die ganze Breite der Einsatzmöglichkeiten erfassen zu können [13].

In der neuesten mechanischen Entwicklung geht der Trend vom reinen Hebezeug für schwere Lasten hin zu „leichten“ Hängekränen, die für Lasten bis zu 1t ausgelegt sind und somit den Großteil der notwendigen innerbetrieblichen Transporte bewältigen können. Sie sind mit ihren Eigenschaften für automatisierte Materialflüsse von wachsender Bedeutung [14]. Die Verbindung von Kranen und Hängebahnen durch Verriegelungen, die Kranbrücken mit Hängebahnschienen zeitweise verbinden, ermöglichen die Überfahrt von Katzen in Kran- bzw. Bahnbereiche. Dadurch lassen sich Kran- und Bahnanlagen beliebig miteinander und untereinander zu einem „Leichtfördersy-

stem im Überflurbereich“ kombinieren [15], [16]. Produktionsbereiche können sowohl durch das Hängekransystem flächendeckend als auch durch das Hängebahnsystem linienförmig erschlossen werden. Es lassen sich alle Positionen eines Fertigungsumfeldes bedienen, ohne Wegflächen zu beanspruchen. Sind keine Bereiche für die Überfahrt gesperrt, so kann stets der direkte Weg für den Transport gewählt werden. Damit liegen die Vorteile gegenüber den Flurförderzeugen und der Stetigförderertechnik auf der Hand. Die Anwendungsbereiche umfassen Transporttechnik, Lagerbedienung und direkte Maschinenbedienung [17].

Nutzen	Anwendungsnutzen
Optimieren der Zweckfunktion	Maximieren der Arbeitsgeschwindigkeiten
	Minimieren der Arbeitswege
	Optimieren des Bewegungsablaufs
	Systematisieren des Umschlags und Lagerns
Vereinfachen der Bedienfunktion	Teilprogrammieren der Arbeitsbewegungen
	selbsttätiger Betrieb von programmierbarer Dauer (Roboterbetrieb)
	gebrauchsgleichwertige Fernbedienung
	Reduzieren des Rüst- und Umrüstaufwands
Erweitern der Überwachungsfunktion	Beanspruchungen
	End- und Kollisionslagen
	Lebensdauer
	Prozeßgrößen
Vereinfachen der Führungsfunktion	Vereinfachen der Tragstruktur
	Vereinfachen der Stützstruktur
	Kopplung selbständiger Funktionseinheiten
	neue Führungsstrukturen

Tabelle 3-1: Entwicklungspotentiale automatisierter Krane

Der Anwender automatisierter Krananlagen kann, je nach Bedarf, in einer Erstausrüstung mit einem niedrigen Automatisierungsgrad beginnen, z.B. mit einer automatisierten Leerfahrt (Rufbetrieb), und den Kran nachträglich um weitere Automatisierungsstufen erweitern, z.B. um eine automatisierte Lastfahrt (Versand- bzw. Ruf- und Versandbetrieb). In einer Endausbaustufe kann schließlich ein Vollautomatikbetrieb einschließlich automatisierter Lastauf- und Lastabgabe erreicht werden.

Verglichen mit den in Abbildung 3-1 dargestellten Betriebsarten ist für automatisierte Krananlagen im innerbetrieblichen Behältertransport der Duobetrieb allerdings nicht zu erwarten, da die in diesem Falle zu transportierenden Lasten von einem Gewicht bis zu ca. einer Tonne und dem Volumen von bis zu zwei Kubikmeter leicht mit nur

einem Kran transportiert werden können. Befinden sich allerdings in einem Kranfeld mehrere Kranbrücken, um einen höheren Durchsatz im Materialfluss gewährleisten zu können, ergeben sich zwischen diesen Kranbrücken zwangsläufig Abhängigkeiten, die steuerungs- wie sicherheitstechnisch gelöst werden müssen.

Nur eine konsequent modulare Gestaltung des Hängekran-Hängebahnsystems und die Berücksichtigung der systemtechnischen Einbindung in den innerbetrieblichen Materialfluss ermöglichen die beschriebenen Ausgestaltungsmöglichkeiten [18]. Die Modularität umfasst sowohl die Steuerungstechnik aller Automatisierungsstufen als auch die Mechanik der Kran- bzw. Bahnsysteme sowie universelle Lastaufnahmemittel und Behältersysteme, Lastübergabestellen und die an der Lastübergabe beteiligten Fördergeräte. Die resultierende Vielzahl der „Schnittstellen“ zwischen den unterschiedlichen Teilsystemen ist weitestgehend vereinheitlicht, um eine flexible Austauschbarkeit einzelner Komponenten zu gewährleisten.

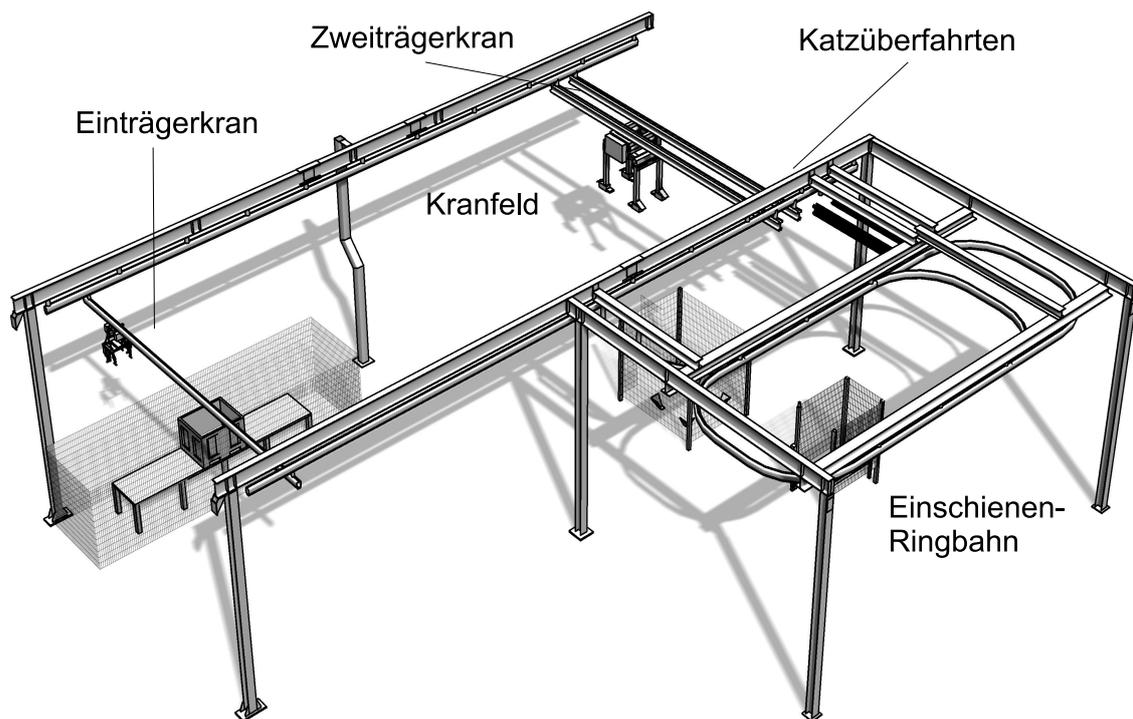


Abb. 3-2: Versuchsanlage am Lehrstuhl fml

Dieser modulare Aufbau ermöglicht eine wirtschaftliche Auswahl eines flexiblen innerbetrieblichen Materialflusssystems, welches sich leicht an dynamische Fertigungsstrukturen mit kurzen Produktlebenszyklen, kurzen Durchlaufzeiten und schnellen Layoutwechseln adaptieren lässt. Es erfüllt damit alle Voraussetzungen an das System der Zukunft [19].

Um die Machbarkeit eines automatisiert flurfreien Fördersystems zu demonstrieren, wurde am Lehrstuhl für Fördertechnik Materialfluss Logistik (fml) eine Versuchsanlage aufgebaut, welche, wie in Abbildung 3-2 dargestellt, aus zwei Kranbrücken und einer Einschienen-Ringbahn mit der Möglichkeit zur Katzüberfahrt besteht. Das Hauptaugenmerk dieser Anlage liegt auf der Umsetzung der beschriebenen Skalierbarkeit, der Modularität und der Verknüpfung mit Lager- und Stetigfördertechnik.

3.2 Steuerungstechnik

Der Stand der Technik für Kransteuerungen ist von Pietryga [20], [21] anschaulich zusammengefasst worden.

Ein konventionelles Steuerungskonzept besteht aus einer zentralen Steuerung und einer zentralen Ein- und Ausgabeperipherie mit einem fest verdrahteten Sicherheitskreis. Gelegentlich kann es auch eine dezentrale Ein- und Ausgabeperipherie für große Anlagen geben, um den Verkabelungsaufwand zu minimieren. In diesem Konzept verarbeitet die SPS keine besonderen Sicherheitsfunktionen. Alle sicherheitsrelevanten Signale werden über den fest verdrahteten Sicherheitskreis, der mit entsprechenden Schaltgeräten und Schützsicherheitskombinationen ausgestattet wird, verarbeitet. Vorteilhaft an diesem Aufbau ist, dass dieser sehr einfach und günstig gehalten werden kann. Nachteilig sind die eingeschränkte Verwendung für komplexe Anforderungen und die inflexible Struktur.

Bei einem erweiterten Steuerungskonzept mit redundanter Steuerung werden dann sicherheitsgerichtete Signale durch die Steuerung verarbeitet. Dazu wird parallel zur zentralen Steuerung eine zweite redundante Steuerung verwendet, die antriebsnah in die jeweiligen Antriebsschränke eingebaut ist. Die sicherheitsgerichteten Signale werden sowohl in der zentralen als auch in der redundanten Steuerung verarbeitet. Die erhöhte Sicherheit resultiert daraus, dass sicherheitsgerichtete Signale, wie Not-Endschalter, Überlast, Überdrehzahl zur Überwachung der Hubwerke usw., redundant verarbeitet werden. Die Vorteile dieser Anordnung sind der Einsatz erprobter Steuerungskomponenten, sicherheitsgerichtetes Verarbeiten von Signalen mit der SPS und eine Softwareentwicklung mit standardisierten Programmen ohne besondere Zusatzprogramme. Die Nachteile sind eine doppelte Ein- und Ausgabeperipherie für die sicherheitsgerichteten Signale, zusätzliche CPUs, eine aufwändige Softwarepflege und ein erweiterter, bei der Abnahme notwendiger, Funktionstest.

Beim erweiterten Steuerungskonzept mit zentraler Steuerung wird im Gegensatz zum vorhergehenden Konzept auf eine zweite Steuerung verzichtet. Die notwendigen Maßnahmen zu Verarbeitung von sicherheitsgerichteten Signalen beschränken sich auf die redundante Ausführung der Ein- und Ausgabekarten sowie den Einsatz spezieller Programmteile und einer speziellen Programmiermethode (z.B. Trennung von normalen

und sicherheitsgerichteten Programmteilen). Die Vorteile dieses Konzeptes sind eine einfache Softwarepflege für nur eine Steuerung, die Softwareentwicklung mit Standardprogrammen und die Nutzung eines erprobten Industriebusses.

Das sicherheitsgerichtete Steuerungskonzept verwendet nur durchgängige, vom Technischen Überwachungsverein (TÜV) geprüfte Geräte. Es wird bei komplexen Krananlagen angewandt, bei denen die Risikobeurteilung entsprechende Maßnahmen vorsieht. Dabei kann auch, je nach Hersteller, auf die fest verdrahteten Sicherheitskreise verzichtet werden. Bei neueren Geräten ist auch die gleichzeitige Nutzung von sicherheitsgerichteter und normaler Technik innerhalb der Steuerung möglich.

Als Alternative zu dem sicherheitsgerichteten Steuerungskonzept kann es auch noch sicherheitsgerichtete Systeme mit einem Standardfeldbus geben, der mit speziell ausgestatteten Ein- und Ausgabemodulen verwendet wird und über einen Sicherheitsmonitor die sicherheitsgerichtete Abschaltung realisiert.

3.3 Bestehende Richtlinien und Vorschriften

In diesem Abschnitt werden die zum Stand der Technik gehörenden Vorschriften und Richtlinien zu Krananlagen analysiert. Dazu wird zunächst ein Überblick über die allgemeinen Regelwerke und deren Einordnung in das europäische Richtliniengefüge gegeben. Im Weiteren wird auf die wichtigsten nationalen Richtlinien, die für die sicherheitstechnische Auslegung von automatisierten Krananlagen von Bedeutung sind, eingegangen. Abschließend wird das bestehende Regelwerk hinsichtlich seiner Anwendbarkeit überprüft und bewertet.

3.3.1 Das europäische Regelwerk

Ausgangspunkt für die neue Verfahrensweise beim Inverkehrbringen von Erzeugnissen war eine Festlegung im EWG-Vertrag von 1957, den freien Warenverkehr im europäischen Binnenmarkt ohne jegliche Hemmnisse zu gestalten. Eine wichtige Rolle spielt dabei die Maschinenrichtlinie. Bei den ersten EG-Richtlinien war man noch bestrebt, Produktmerkmale und Sicherheitsanforderungen vollständig zu erfassen. Das konnte sich aus verschiedenen Gründen nicht durchsetzen. Es waren damit auch Handelshemmnisse verbunden. Eine neue vereinfachte Regelung musste gefunden werden. Daraufhin hat der EG-Rat bereits 1985 mit seiner EntschlieÙung über die „Neue Konzeption“ auf dem Gebiet der technischen Harmonisierung andere Normungsmethoden eingeführt.

Im Ergebnis der neuen Konzeption enthalten die EG-Richtlinien für den Warenverkehr hauptsächlich nur Grundanforderungen, zum Beispiel Schutzziele, nicht aber konkrete oder vollständige sicherheitstechnische Lösungen. Der Nachweis über die Herstellung fehlerfreier bzw. verwendungssicherer Produkte wird einer Gefahrenana-

lyse überlassen. Einzelheiten müssen die Hersteller und Montagebetriebe abklären. Sie können so die Produktlösungen im Wesentlichen selbst gestalten. [22]

Das EU-weit geltende Regelwerk zur Sicherheit von Maschinen und Anlagen ist, wie in Abbildung 3-3 dargestellt, hierarchisch aufgebaut. Die grundlegenden Anforderungen werden in den europäischen Richtlinien festgelegt. Neben der für den Maschinen- und Anlagenbau zentralen Maschinenrichtlinie 98/37/EG können für den Konstrukteur auch andere Richtlinien von Bedeutung sein. Zu diesen Richtlinien gibt es Normen und andere Schriften, in denen die Anforderungen konkretisiert werden.

Im sicherheitstechnischen Regelwerk ist zwischen europäischem und nationalem Recht zu unterscheiden. Die auf europäischer Seite vertretenen allgemeinen Richtlinien werden, wie z.B. die EG-Maschinenrichtlinie durch die 9. Verordnung zum Gerätesicherheitsgesetz, in nationales Recht umgesetzt. Unter diesem allgemeinen Aufbau finden sich dann Normen und andere allgemein anerkannte Regeln der Technik, wie z.B. ZH1-Schriften und VDI-Richtlinien, zur Konkretisierung der oben genannten Schutzziele, die in den Richtlinien innerhalb der EU entweder harmonisiert oder nicht harmonisiert sind [22].

Eine detailliertere Darstellung der rechtlichen Vorschriften findet man u.a. in der Literatur bei Krywald [23] und den Berufsgenossenschaften [24]. Anhand des oben beschriebenen Aufbaus werden im Folgenden alle bestehenden Regelwerke für automatisierte Krananlagen untersucht.

Mit der Richtlinie 89/392/EWG des Rates der Europäischen Gemeinschaft vom 14. Juni 1989 zur Angleichung der Rechtsvorschriften der Mitgliedsstaaten für Maschinen (Maschinenrichtlinie), umgesetzt in nationales Recht durch die 9. Verordnung zum Gerätesicherheitsgesetz (Maschinenverordnung), ist seit dem 1. Januar 1993 eine neue Rechtsgrundlage gegeben.

Die Maschinenrichtlinie 89/392/EWG ist bindend für die Hersteller von Maschinen. Bis heute sind drei Änderungsrichtlinien zur Maschinenrichtlinie verabschiedet worden: Zunächst die erste Änderungsrichtlinie 91/368/EWG vom 20. Juni 1991, gefolgt von der zweiten Änderungsrichtlinie 93/44/EWG vom 14. Juni 1993 und die CE-Kennzeichnungsrichtlinie 93/68/EWG vom 22. Juli 1993. Die vorbezeichneten Richtlinien haben durch die Zusammenfassung zu einer konsolidierten und kodifizierten Fassung die Bezeichnung 98/37/EG erhalten.

Durch diese Richtlinie wird der Hersteller dazu verpflichtet, eine Gefahrenanalyse vorzunehmen, um alle mit seiner Maschine verbundenen Gefahren zu ermitteln. Es gibt keine Festlegung darüber, mit welcher Methode und mit welchem Aufwand die Gefahrenanalyse durchzuführen ist. Es sind mehrere Teile einer Gefahrenanalyse aus unterschiedlichem Blickwinkel möglich, die am Ende zusammengeführt werden. Der Hersteller muss die Maschine dann unter Berücksichtigung seiner Analyse entwerfen

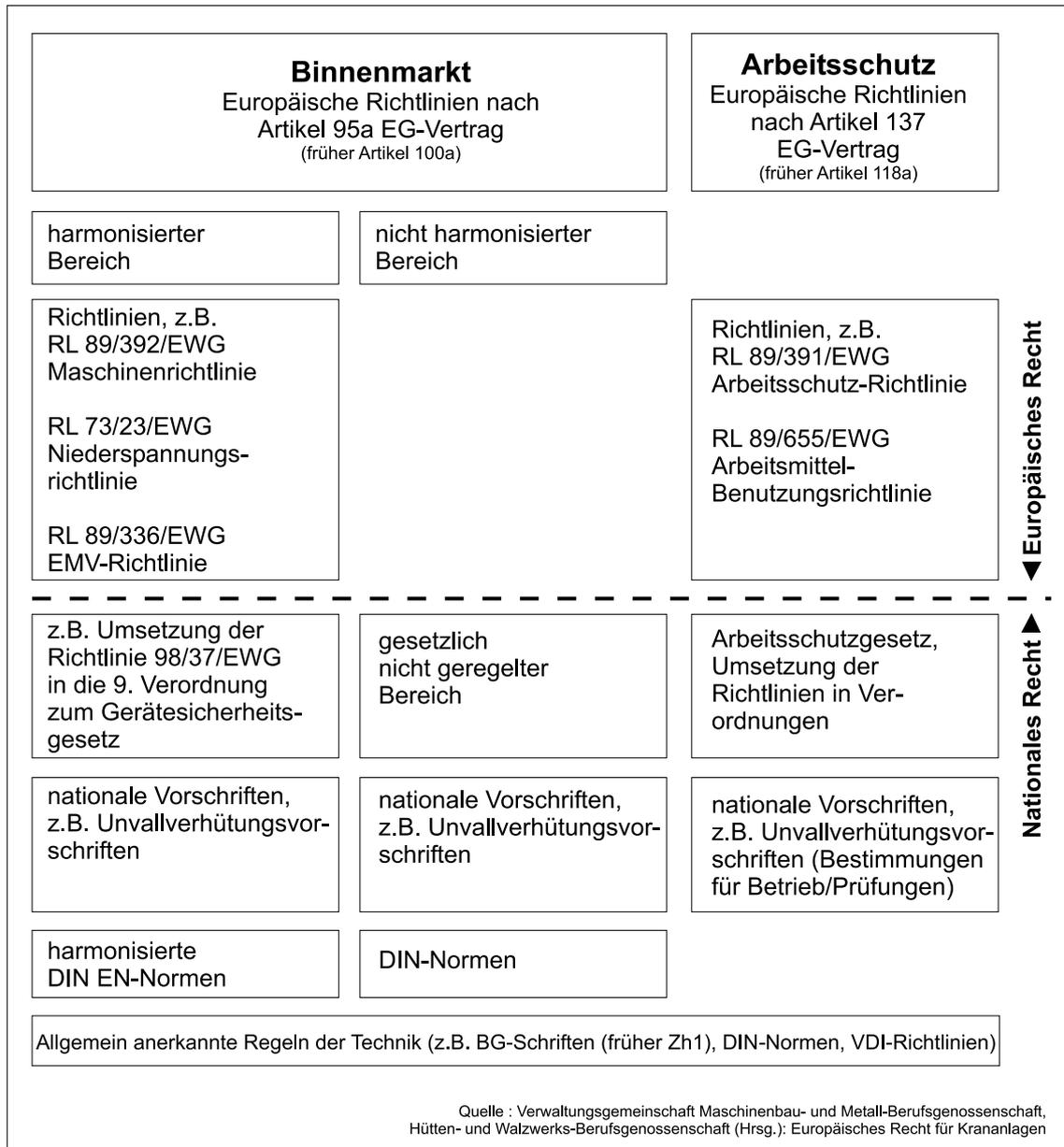


Abb. 3-3: Regelwerk für Krane

und bauen. Am Ende muss jedoch der Stand der Technik den gewählten Lösungen und Zusatzmaßnahmen gegenübergestellt und mindestens ein gleiches oder kleineres Restrisiko nachvollziehbar begründet sein. Dieses Dokument bildet dann auch die Grundlage für die Konformitätsprüfung.

Diese Konformitätsprüfung muss ein Unternehmen für eine Maschine oder Anlage vornehmen, das diese im EU-Raum in Verkehr bringt. Als Zeichen der Konformität wird daran das CE-Zeichen angebracht, welches garantiert, dass bei der Planung und Konstruktion die in der EG-Maschinenrichtlinie formulierten Schutzziele berücksichtigt und umgesetzt wurden. Der Hersteller bzw. Inverkehrbringer kann diese Erklärung in Eigenverantwortung ausstellen. Nur bei den im Anhang IV A der Ma-

schinenrichtlinie aufgeführten gefährlichen Maschinen muss eine autorisierte Stelle hinzugezogen werden [23].

Wegen der Unterschiedlichkeit aller Maschinen können die Maschinenrichtlinien nur allgemein gültige Vorgaben und Leitsätze enthalten und geben somit keine konkreten Vorschläge für ein Sicherheitskonzept für Automatikkrane im personenzugänglichen Umfeld.

Neben der Maschinenrichtlinie sind von den Herstellern noch weitere EG-Richtlinien zu beachten:

- Niederspannungsrichtlinie 73/23/EWG,
- Richtlinie über die elektromagnetische Verträglichkeit 89/336/EWG - EMV,
- Arbeitsschutz-Rahmenrichtlinie 89/391/EWG und
- Arbeitsmittelbenutzungsrichtlinie 89/655/EWG mit der Änderungsrichtlinie 95/63/EWG.

Diese Richtlinien sind jedoch nur für die allgemeinen Sicherheitsvorschriften einer Krananlage zu beachten und somit nicht speziell für Automatikkrane geeignet und werden deshalb nicht genau untersucht.

3.3.2 Nationale Vorschriften

Grundlage der nationalen Vorschriften ist das Gerätesicherheitsgesetz (GSG). Aufbauend darauf bestehen die Arbeitsschutz- und Unfallverhütungsvorschriften, wie z.B. die Arbeitsstättenverordnung und die UVV „Krane“, zur Konkretisierung der allgemeinen EG-Richtlinien. Als eine dritte Ebene existieren die allgemein anerkannten Regeln der Technik von DIN, VDI und VDE.

§ 3 GSG

„Technische Arbeitsmittel, für die in Rechtsverordnungen nach diesem Gesetz keine Anforderungen enthalten sind, dürfen nur in den Verkehr gebracht werden, wenn sie nach den Regeln der Technik sowie den Arbeitsschutz- und Unfallverhütungsvorschriften so beschaffen sind, dass Benutzer oder Dritte bei ihrer bestimmungsgemäßen Verwendung gegen Gefahren aller Art geschützt sind, wie es die Art der bestimmungsgemäßen Verwendung gestattet.“

Im oben zitierten § 3 GSG wird auf die Regeln der Technik, wie Unfallverhütungsvorschriften und Normen, hingewiesen, womit diese mehr oder weniger für den Hersteller als verbindlich zu betrachten sind. Allerdings ist zu beachten, dass Normen keine Gesetze sind, sondern dem Konstrukteur als Hilfestellung dienen. Er kann die in der Maschinenrichtlinie genannten Schutzziele auch auf anderem Wege erreichen, muss dies jedoch durch eine Sicherheitsanalyse nachweisen.

3.3.3 Unfallverhütungsvorschriften

Unfallverhütungsvorschriften sind autonome Rechtsverordnungen, d.h. Regelungen, die gegenüber Mitgliedsbetrieben und Versicherten einer Berufsgenossenschaft wie Gesetze wirken und für sie deshalb gleichermaßen verbindlich sind. Für den Kranbau ist zunächst die UVV „Krane“ von größter Bedeutung. Hier werden Handlungsanweisungen und Maßnahmen zur Unfallvermeidung genannt. Neben vielen allgemein für Krananlagen gültigen Regeln werden in den §§ 23 und 24 die automatisierten Krananlagen behandelt:

§ 23 UVV „Krane“

„Bei programmgesteuerten Kranen müssen Arbeits- und Verkehrsbereiche so gesichert sein, dass Personen weder durch die Kranbewegung noch durch herabfallende Lasten verletzt werden.“

Nach der allgemein gültigen Auslegung aus [15] ist der Schutz gegen Verletzungen durch die Kranbewegungen erfüllt, wenn der Gefahrenbereich abgeschränkt ist.

Ein ausreichender Schutz gegen herabfallende Lasten ist gewährleistet, wenn

- der Lastweg unterfangen,
- die Last verklammert oder
- der Gefahrenbereich abgeschränkt ist.

Aufgrund der Personenzugänglichkeit des Kranbereiches widerspricht die Auslegung der UVV „Krane“ hinsichtlich einer Abschränkung dem geforderten Betriebskonzept. Eine Unterfangung ist mit der geforderten Flexibilität für die Anlage und aus Kostengründen nicht zu vereinbaren.

Ein weiterer Anhaltspunkt zur Sicherheit bei Automatikkränen findet sich in § 24 bezüglich Nothalteinrichtungen:

§ 24 UVV „Krane“

„An handbedienten Be- und Entladestellen programmgesteuerter Krane sowie deren Arbeitsbereich müssen Nothalteinrichtungen vorhanden sein, die leicht zugänglich und schnell erreichbar sind, dass der Kran bei Gefahr unverzüglich stillgesetzt werden kann. Die Nothalteinrichtungen müssen als solche auffällig gekennzeichnet sein.“

Man erkennt an den vorliegenden Ausschnitten, dass die Unfallverhütungsvorschriften hier nicht greifen, da sie einerseits einem personenzugänglichen Betriebskonzept widersprechen, indem sie eine Absperrung des Kranbereiches fordern und andererseits sehr allgemein gehalten sind.

Andere Unfallverhütungsvorschriften, wie z.B. *Winden, Hub- und Zuggeräte (BGV D8)* oder *Lastaufnahmeeinrichtungen im Hebezeugbetrieb (VBG 9a)*, können keine weiteren Aufschlüsse hinsichtlich einer Automatisierung geben und sind außerdem zu allgemein gehalten, um besonders auf Automatikkrane bezogene Sicherheitshinweise zu bekommen. Eine vollständige Liste der wichtigsten Unfallverhütungsvorschriften und Sicherheitsregeln, die mit Kranen in Verbindung stehen, ist in Tabelle 3-2 zusammengefasst

Vorschrift	Titel
BGV A2	Elektrische Anlagen (bisher VBG 4)
VDI	Steuerungseinrichtungen mit vereinbarter gesicherter Funktion
BGV D6	Krane (bisher VBG 9)
VDI 3653	Automatisierte Kransysteme
BGV D8	Winden, Hub- und Zuggeräte
VBG 9a	Lastaufnahmeeinrichtungen im Hebezeugbetrieb (bisher VBG 8)
ZH 1/547	Richtlinien für Funkfernsteuerungen von Kranen

Tabelle 3-2: Unfallverhütungsvorschriften

3.3.4 VDI-Richtlinien

Neben den Unfallverhütungsvorschriften der Berufsgenossenschaften gibt es noch die VDI-Richtlinie 3653 „Automatikkrane“. Diese Richtlinie gibt bei den Sicherheitsanforderungen für vollautomatisierte Krananlagen nur pauschale Empfehlungen. Es werden lediglich zum Schutz von Personen folgende Punkte empfohlen:

- Schutz vor bewegten Lasten und Lastaufnahmemitteln durch
 - Hub- und Fahrwegvorgabe für den Kran mit Wegtrennung zu Personen.
- Schutz beim betriebsmäßigen Aufnehmen und Abgeben von Lasten durch
 - Absperrung und berührungslos wirkende Schutzeinrichtungen und
 - Freigabe durch Personen.
- Schutz vor Absturz von Lasten durch
 - formschlüssige Lastaufnahme,
 - Unterfangen der Last und
 - Absicherung mittels baulicher Einrichtungen.

Diese Punkte widersprechen sich, ähnlich wie bei den Unfallverhütungsvorschriften, zum einen bezüglich der geforderten Personenzugänglichkeit, indem eine Absperrung des Kranbereiches gefordert wird, zum anderen, wenn für eine automatisierte Anlage

eine Person zur Freigabe der Lastabsenkung gefordert wird. Weiterhin ist ein Unterfangen der Last oder sind andere baulich geforderten Maßnahmen nicht mit der nötigen Flexibilität der Anlage in Einklang zu bringen.

3.3.5 Normen zur Sicherheit

Neben den oben genannten Richtlinien von Berufsgenossenschaft und VDI gibt es noch eine Vielzahl von Normen, die sich direkt oder indirekt mit Kranen und Sicherheitstechnik befassen.

Das europäische Normenwerk wird zunehmend vereinheitlicht. Dabei werden die harmonisierten Normen in folgende drei Ebenen gegliedert, um so unnötige Wiederholungen in den einzelnen Normen zu vermeiden:

A-Normen: Dies sind Grundnormen, die Begriffe und Gestaltungsleitsätze der CE-Richtlinien klären.

B-Normen: Dies sind Gruppennormen, die bestimmte Produktgruppen gleichermaßen betreffen.

C-Normen: Dies sind Produktnormen, die sich auf einzelne Produkte beziehen.

Vorschrift	Titel
DIN EN 1050	Leitsätze zur Risikobeurteilung
DIN EN 954-1	Sicherheitsbezogene Teile von Steuerungen
DIN EN 0801	Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben
DIN EN 292	Sicherheit von Maschinen
DIN EN 60204	Elektrische Ausrüstung von Maschinen
DIN EN 418	NOT-AUS-Einrichtung
DIN EN 1088	Verriegelungseinrichtungen in Verbindung mit trennenden Schutzeinrichtungen
DIN V 19250	MSR Schutzeinrichtungen
DIN EN 61496-1	Berührungslos wirkende Schutzeinrichtungen
DIN EN 811	Sicherheitsabstände gegen das Erreichen von Gefahrenstellen
DIN 15018	Krane: Grundsätze für Stahltragwerke
DIN 15030	Abnahmeprüfung von Krananlagen
DIN EN 12077-2	Begrenzungs- und Anzeigeeinrichtungen

Tabelle 3-3: Relevante DIN-Normen zur Sicherheit

In Tabelle 3-3 werden die wichtigsten DIN-Normen für eine automatisierte Krananlage im personenzugänglichen Umfeld für den innerbetrieblichen Behältertransport aufgelistet.

3.3.6 Normen für Steuerungstechnik

Bei den Normen für Steuerungstechnik wird zwischen der funktionalen und der elektrischen Sicherheit unterschieden. Dabei versteht man unter elektrischer Sicherheit den Schutz vor Gefährdungen, die durch die Elektrizität ausgehen, wie z.B. beim Berührungsschutz. Die funktionale Sicherheit beschreibt den Schutz, mit der die Steuerung und somit die Anlage korrekt funktioniert.

Die Norm IEC 61508 beschreibt das Thema der funktionalen Sicherheit sehr ausführlich. Damit ist im Bereich Maschinensteuerungen ein neues technisches Regelwerk für sicherheitsgerichtete Steuerungen entstanden. Die EN 954-1 orientiert sich an einer quantitativen Fehlerbetrachtung und definiert 4 Kategorien, die ähnlich wie in der DIN V 19 250 auf der Basis einer Risikoanalyse ermittelt werden. Die Kategorien werden beschrieben durch die Art und Anzahl der Fehler, die nicht zu einem gefährlichen Betriebszustand führen dürfen.

Die in Abbildung 3-4 dargestellten Normen finden im Bereich der Steuerungen für Krane Anwendung.

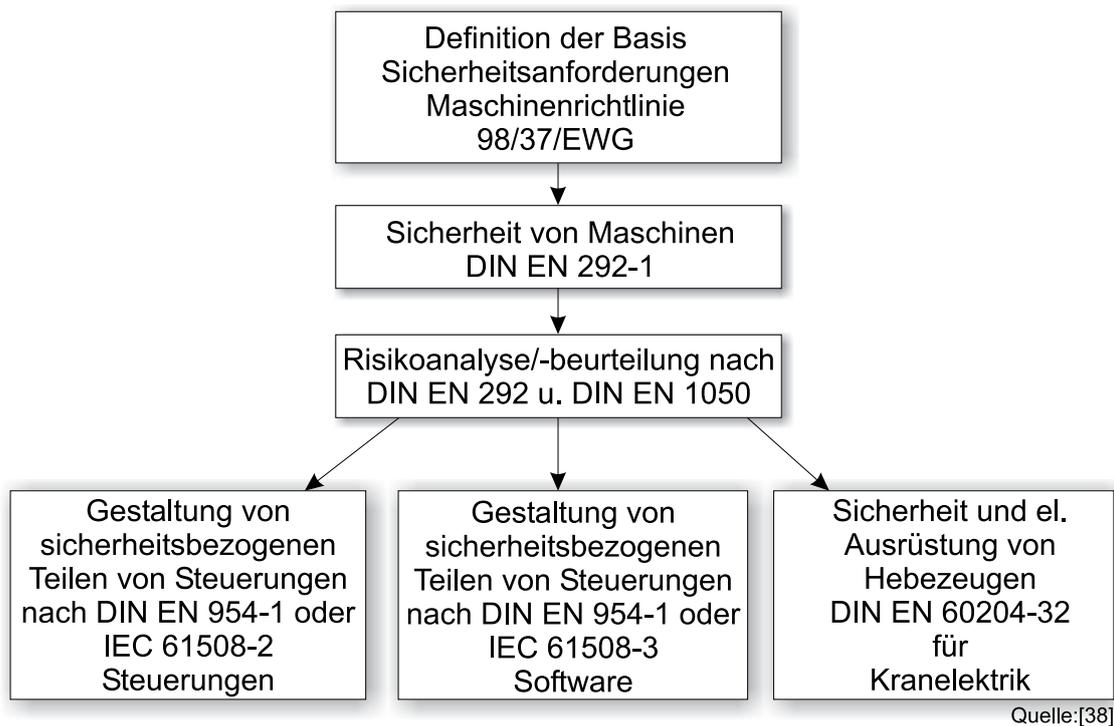


Abb. 3-4: Übersicht der Normen im Bereich Steuerung

Mit Hilfe der DIN EN 292 und der DIN EN 1050 ist es möglich, wie oben beschrieben, eine Sicherheitsanalyse und Risikobeurteilung durchzuführen. Mit der DIN EN 954 und DIN EN 60204-32 lassen sich dann Maßnahmen festlegen, die notwendig sind, um ein vertretbares Restrisiko zu erreichen.

3.3.7 Normen für sicherheitsrelevante Software

Grundlage für den heutigen Stand des technischen Regelwerkes bei der Erstellung von Software in Rechnern mit sicherheitsrelevanten Funktionen bildet die vom Normungskomitee IEC 65A erarbeitete Normenreihe „Funktionale Sicherheit“.

Mit dieser Normenreihe stehen heute im Einzelnen folgende Teile zur Verfügung (Tabelle 3-4):

Draft IEC 1508	VDE	Titel
IEC 65A/179/CDV 1995	VDE 0801 Teil 1 1996	Allgemeine Anforderungen
IEC 65A/254/CDV 1998	VDE 0801 Teil 2 1998	Anforderungen an sicherheitsbezogene elektrische /elektronische / programmierbare elektronische Systeme
IEC 65A/181/CDV 1995	VDE 0801 Teil 3 1996	Anforderungen an Software
IEC 65A/182/CDV 1995	VDE 0801 Teil 4 1996	Definitionen
IEC 65A/183/CDV 1995	VDE 0801 Teil 5 1996	Anwendungsrichtlinien für Teil 1
IEC 65A/255/CDV 1998	VDE 0801 Teil 6 1998	Anwendungsrichtlinien für Teile 2 und 3
IEC 65A/185/CDV 1996	VDE 0801 Teil 7 1996	Erläuterungen zu Maßnahmen

Tabelle 3-4: Normenreihe: Funktionale Sicherheit

Die genannten vier *safety integrity level* (SIL) oder auch sicherheitsbezogenen Anforderungsstufen definieren die Zuverlässigkeit für Systeme. Eine Festlegung ergibt sich nach Tabelle 3-5:

Sicherheitsbezogene Anforderungsstufe	Betrieb im Anforderungsmodus Wahrscheinlichkeit eines Ausfalls einer vorgesehenen Funktion bei Anforderung	Betrieb im ununterbrochenen hohen Anforderungsmodus Wahrscheinlichkeit eines gefährlichen Ausfalls pro Jahr
4	$\geq 10^{-5}$ bis $< 10^{-4}$	$\geq 10^{-5}$ bis $< 10^{-4}$
3	$\geq 10^{-4}$ bis $< 10^{-3}$	$\geq 10^{-4}$ bis $< 10^{-3}$
2	$\geq 10^{-3}$ bis $< 10^{-2}$	$\geq 10^{-3}$ bis $< 10^{-2}$
1	$\geq 10^{-2}$ bis $< 10^{-1}$	$\geq 10^{-2}$ bis $< 10^{-1}$

Tabelle 3-5: Definition der Anforderungsstufen

Des Weiteren ist die Hardwarefehlertoleranz in Abhängigkeit des Diagnosedeckungsgrades und des *safety integrity levels* festgelegt. Nur mit beiden Normenwerken gemeinsam, SIL und Hardwarefehlertoleranz, kann ein im Sinne der IEC ausgeführtes System spezifiziert werden.

Eine Gegenüberstellung der Anforderungsklasse, des SIL's, der Kategorie und eine verbale Beschreibung, wie sie in der Vergangenheit üblich war, zeigt Tabelle 3-6.

Diese gilt nur, wenn bei Anwendung der IEC 65A die gleiche Hardwarefehlertoleranz zugrunde gelegt wird wie z. B. in der EN 945-1.

Anforderungs- klasse nach DIN V 19250	Sicherheits- bezogene Anforderungs- stufe nach Draft IEC 65A	Steuerungs- kategorie nach EN 954-1	Beschreibung
1	0	B	Steuerungen gemäß Stand der Technik
2/3	1	1/2	Sicherheitstechnisch bewährte Komponenten und Prinzipien, Testung
4	2	3	Redundanz mit partieller Fehlererkennung, soweit nach Stand der Technik möglich
5/6	3	4	Selbstüberwachung
7/8	4	-	Im Maschinenschutz nicht von Bedeutung

Tabelle 3-6: Gegenüberstellung der Anforderungsklassen

3.4 Anwendbarkeit auf Krane

Nach Durchsicht aller Richtlinien und Normen lässt sich abschließend sagen, dass das bestehende Regelwerk hinsichtlich der Sicherheitsanforderungen für automatisierte Krananlagen nur allgemeine Vorschläge enthält. Diese Richtlinien sind nicht ausreichend, um dem Hersteller die Gewissheit zu geben, eine von der Berufsgenossenschaft oder vom Gewerbeaufsichtsamt abnahmefähige Anlage zu verkaufen. Den besonderen Anforderungen eines automatisierten Kransystems im personenzugänglichen Umfeld wird letzten Endes keine der genannten Normen und Richtlinien einzeln wie auch kombiniert gerecht. Durch die nur allgemeinen Sicherheitsanforderungen und die große individuelle Anwendbarkeit entstehen große Spielräume bei der sicherheitstechnischen Auslegung von Automatikkränen.

Ausgehend von dieser Situation zeigt sich, dass die Notwendigkeit besteht, für Automatikkrane im personenzugänglichen Umfeld ein für den Hersteller anwendbares Regelwerk zu schaffen, das eine sicherheitstechnische Abnahme der Anlage gewährleistet.

Eine Liste, die den Stand und Inhalt nationaler Vorschriften wiedergibt, ist in Anhang A angeführt.

4 Systemanalyse

Für eine genaue Sicherheitsanalyse ist eine genaue Systemanalyse grundlegend. Eine Systemanalyse kann dabei in drei Einzelschritte unterteilt werden:

- Die Analyse der logischen Strukturen eines Systems,
- die Beschreibung der funktionalen Abläufe sowie
- die Beschreibung der enthaltenen mechanischen Komponenten.

Zur Untersuchung der logischen Strukturen technischer Systeme kann deren Darstellung mit Hilfe mathematischer Funktionen vorgenommen werden. Die wesentlichen Grundlagen dieser Funktionen werden in der Folge nach Kuhlmann [11] beschrieben.

4.1 Logische Strukturen und Systemfunktionen

Betrachtet wird ein technisches System S mit den Komponenten K_1, K_2, \dots, K_n . Von den Komponenten und dem Gesamtsystem wird ein Verhalten erwartet, wie es für die Erfüllung der vorgegebenen Funktionen notwendig ist. Das Abweichen der Komponente K_i von dem erwünschten Verhalten definiert das unerwünschte Ereignis A_i , das Eintreten des erwünschten Verhaltens ist das Ereignis \bar{A}_i .

Um zur Definition einer Systemfunktion zu gelangen, ordnet man jeder Komponente K_i eine Variable Z_i zu, die den Wert 1 hat, wenn das Ereignis A_i eintritt, und den Wert 0, wenn das Ereignis \bar{A}_i eintritt. Das Ereignis A_i ist dann identisch mit dem Ereignis $Z_i = 1$, das Ereignis \bar{A}_i identisch mit dem Ereignis $Z_i = 0$. Eine solche Variable heißt BOOLESCHE Variable. Entsprechend lässt sich für das System S eine BOOLESCHE Variable Z_s festlegen, indem man dem Eintreten des unerwünschten Ereignisses A_s den Wert $Z_s = 1$ zuordnet und dem komplementären Ereignis \bar{A}_s den Wert $Z_s = 0$. Zusammengefasst erhält man folgende Zuordnung:

$$\begin{aligned}
 A_i &\rightarrow Z_i = 1, \\
 \bar{A}_i &\rightarrow Z_i = 0, \\
 A_s &\rightarrow Z_s = 1, \\
 \bar{A}_s &\rightarrow Z_s = 0.
 \end{aligned}
 \tag{4-1}$$

Entsprechend gilt für die Eintrittswahrscheinlichkeiten q bzw. p :

$$\begin{aligned}
 q_i &= W(A_i) = W(Z_i = 1), \\
 p_i &= W(\bar{A}_i) = W(Z_i = 0) = 1 - q_i, \\
 q_s &= W(A_s) = W(Z_s = 1), \\
 p_s &= W(\bar{A}_s) = W(Z_s = 0) = 1 - q_s.
 \end{aligned}
 \tag{4-2}$$

Sind Z_a und Z_b bzw. Z beliebige Zustandsvariablen, so bezeichnen

$$\begin{aligned}
 Z' &= Z_a \wedge Z_b, \\
 Z' &= Z_a \vee Z_b, \\
 Z' &= \bar{Z}
 \end{aligned}
 \tag{4-3}$$

Verknüpfungsregeln zwischen den Zustandsvariablen. Diese werden mit den Ausdrücken „UND“, „ODER“ und „Negation“ bezeichnet. Tabelle 4-1 zeigt eine Übersicht der Verknüpfungen der Zustandsvariablen mit den zugeordneten Rechenregeln.

Bezeichnung	Werte der Zustandsvariablen	Rechenregeln
„UND“ $Z' = Z_a \wedge Z_b$	$ \begin{array}{c cccc} Z_a & 0 & 0 & 1 & 1 \\ Z_b & 0 & 1 & 0 & 1 \\ \hline Z' & 0 & 0 & 0 & 1 \end{array} $	Zustandsvariable $Z' = Z_a \cdot Z_b$
„ODER“ $Z' = Z_a \vee Z_b$	$ \begin{array}{c cccc} Z_a & 0 & 0 & 1 & 1 \\ Z_b & 0 & 1 & 0 & 1 \\ \hline Z' & 0 & 1 & 1 & 1 \end{array} $	Zustandsvariable $Z' = Z_a + Z_b - Z_a Z_b$
„Negation“ $Z' = \bar{Z}$	$ \begin{array}{c cc} Z_a & 0 & 1 \\ \hline \bar{Z} & 1 & 0 \end{array} $	Zustandsvariable $Z' = Z - 1$

Tabelle 4-1: Rechenregeln für boolesche Operationen

Den Vektor (Z_1, Z_2, \dots, Z_n) der Zustandsvariablen der Komponenten K_1, K_2, \dots, K_n eines Systems bezeichnet man als Zustandsvektor des Systems. Die Systemfunktion $\varphi(Z_1, Z_2, \dots, Z_n)$ des Systems ist definiert durch:

$$Z_s = \varphi(Z_1, Z_2, \dots, Z_n) \tag{4-4}$$

Die Systemfunktion ordnet jedem Wertesatz des Zustandsvektors den Wert $Z_s = 1$ bzw. $Z_s = 0$ zu, je nachdem ob dem Zustand des Systemereignisses A_s bzw. \bar{A}_s zugeordnet ist. Die Systemfunktion lässt sich sowohl als BOOLESCHE Funktion als auch rechnerisch in Abhängigkeit von den Zustandsvariablen Z_i darstellen. Die rechnerische Form stellt die logische Struktur des Systems formelmäßig dar. Sind die Zustände der Komponenten unabhängig voneinander, so ergibt sich, wenn man eine geeignete rechnerische Darstellung von φ_s wählt und darin Z_i durch q_i ersetzt,

unmittelbar die Wahrscheinlichkeit q_s dafür, dass im Gesamtsystem das Ereignis A_s bzw. der Zustand $Z_s = 1$ eintritt:

$$q_s = \varphi_s(q_1, q_2, \dots, q_n) \quad (4-5)$$

In Abbildung 4-1 ergibt sich somit folgender Zusammenhang für die Systembeschreibung:

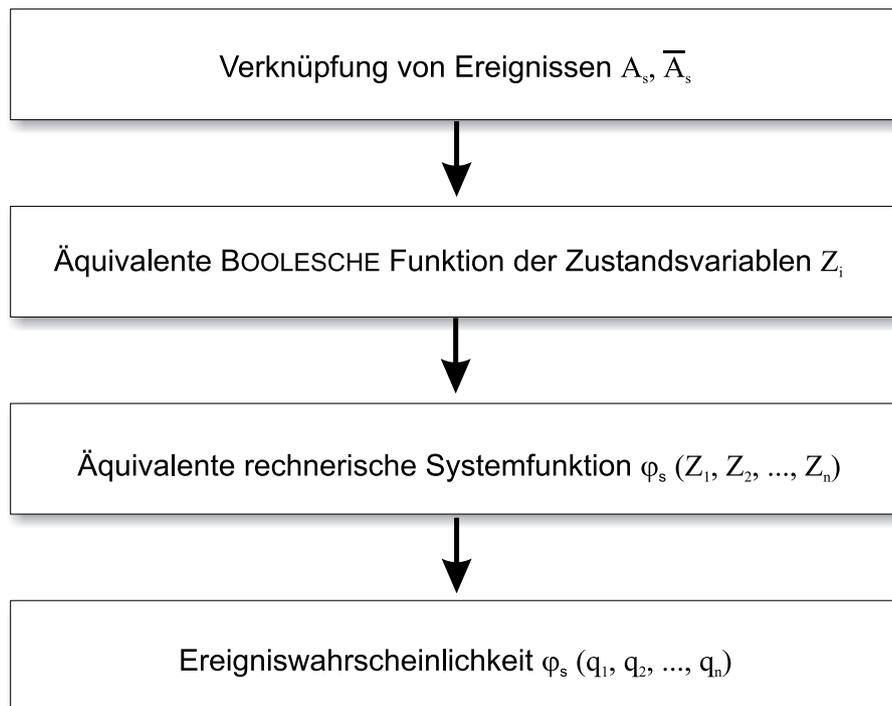


Abb. 4-1: Systemanalyse

4.2 Verteilungsfunktionen und statistische Kenngrößen

Die Eintrittswahrscheinlichkeiten für bestimmte Ereignisse an Komponenten oder Teilsystemen eines betrachteten Gesamtsystems hängen von Eigenschaften ab, deren Werte statistisch verteilt sind und die durch Verteilungsfunktionen beschrieben werden können. Besondere Bedeutung für die Auswertung von Daten und für die Ermittlung statistischer Kenngrößen aus Datenmengen haben die GAUSSverteilung und die WEIBULLverteilung.

Die Anwendung der GAUSSverteilung ist vielfältig und somit z.B. auch für Verschleißausfälle möglich. Wegen ihrer großen Anpassungsfähigkeit ist die WEIBULLverteilung mit der Verteilungsfunktion

$$F(x) = 1 - \exp\left[-[(x - \alpha)/\beta]^\gamma\right] \quad (4-6)$$

für viele Fälle zur Datenauswertung hervorragend geeignet. Allerdings bereitet die exakte Ermittlung der drei Parameter α , β und γ , die sie bestimmen, manchmal erhebliche Schwierigkeiten, insbesondere bei unzureichend großen Datenmengen.

Ein Sonderfall der WEIBULLverteilung ist die Exponentialverteilung mit $\alpha = 0$ und $\gamma = 1$. Dann wird mit $\frac{1}{\lambda} = \beta$ die Verteilungsfunktion zu

$$F(x) = 1 - \exp(-\lambda x) \quad (4-7)$$

Die Exponentialverteilung wird häufig eingesetzt, was auf den Aufbau mit $\lambda = \text{konst.}$ und die damit verbundene leichte Handhabung zurückzuführen ist. Im Prinzip ist dieser Ansatz bei Bauteilen, die einem Verschleiß unterliegen, physikalisch falsch. Dies gilt auch dann, wenn aus den vorhandenen Daten eine Zeitabhängigkeit nicht schlüssig abgeleitet werden kann. Der Fehler kann, über kurze Zeiten betrachtet, allerdings vernachlässigbar sein. Dies zeigt deutlich die so genannte „Badewannenkurve“, in Abbildung 4-2.

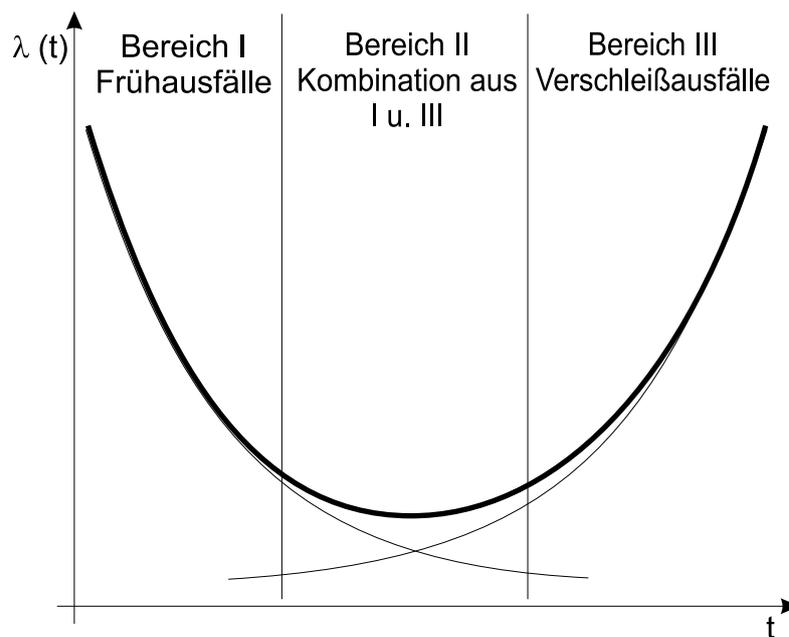


Abb. 4-2: Ausfallrate in Abhängigkeit von der Zeit (Badewannenkurve)

Dort ist der Verlauf der Ausfallrate $\lambda(t)$ in Abhängigkeit von der Zeit dargestellt. Bereich I kennzeichnet den Zeitraum, in dem Frühausfälle beobachtet werden, zum Beispiel durch mangelnde Herstellqualität oder unvorhergesehene Betriebsverhältnisse. Im anschließenden Bereich II ist eine Überlagerung aus zwei Verhaltensweisen erkennbar, aus abnehmenden Frühausfällen und zunehmenden Verschleißausfällen. Als Folge der Überlagerung kann für einen bestimmten Zeitraum die Ausfallrate $\lambda(t)$ praktisch als konstant betrachtet werden. Bereich III beschreibt den Zeitraum der Verschleißausfälle. Die Ausfallrate wächst mit fortschreitender Zeit stark an.

4.3 Funktionale Abläufe

Der Betriebsablauf eines Kranes ist zum einen durch den eigentlichen Transportvorgang, bestehend aus Lastaufnahme, Transport der Last und Lastabgabe, zum anderen durch die manuelle, teilautomatisierte und vollautomatische Betriebsart gekennzeichnet. Anhand dieser Parameter lassen sich die in Abbildung 4-3 dargestellten Kranspiele ermöglichen. Sie stellen ein so genanntes erweitertes Kranspiel dar, bei dem nicht nur die reinen Abläufe der Kranbewegung, sondern auch das Handhaben der Last mit berücksichtigt sind. Es werden nur die sinnvollen Ablaufvarianten aufgenommen. Neben dem reinen Ablauf des Kranspieles sind auch die jeweiligen Änderungen zwischen den Betriebsarten manuell und automatisiert gut erkennbar.

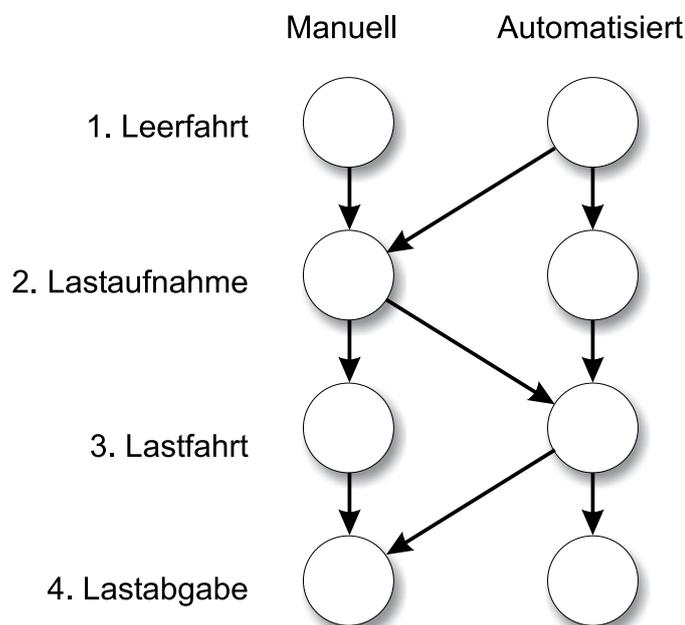


Abb. 4-3: Zustandsänderungen der Betriebsarten

In Abbildung 4-3 sind acht Kranspiele erkennbar. Diese sind in ihrem Ablauf in den folgenden Abbildungen 4-4 bis 4-11 einzeln dargestellt.

Abbildung 4-4 zeigt ein ausschließlich manuelles Kranspiel, mit manueller Leerfahrt, manueller Lastaufnahme, manueller Lastfahrt und manueller Lastabgabe, wie es bis jetzt in Produktionsbetrieben durchgeführt wird.

Abbildung 4-5 zeigt ein Kranspiel mit manueller Leerfahrt, manueller Lastaufnahme, einem Wechsel in den automatischen Betrieb für eine automatische Lastfahrt und einem weiteren Wechsel zurück in den manuellen Betrieb für die manuelle Lastabgabe. Ein solches Kranspiel wird als Versandbetrieb mit manueller Abgabe bezeichnet.

Abbildung 4-6 zeigt ein Kranspiel mit automatischer Leerfahrt, einem Wechsel in die manuelle Betriebsart für die Lastaufnahme, Lastfahrt und Lastabgabe. Die Anforder-

rung des Kranes erfolgt mittels Ruftaster. Ein solches Kranspiel wird als Rufbetrieb bezeichnet.

Abbildung 4-7 zeigt ein Kranspiel mit automatischer Leerfahrt, einem Wechsel in die manuelle Betriebsart für die Lastaufnahme, einem weiteren Wechsel in die automatische Betriebsart für die Lastfahrt und einem letzten Wechsel zurück in den manuellen Modus für die Lastabgabe. Ein solches Kranspiel wird als Ruf- und Versandbetrieb bezeichnet.

Abbildung 4-8 zeigt ein Kranspiel mit automatischer Leerfahrt, automatischer Lastaufnahme, automatischer Lastfahrt und einem Wechsel in die manuelle Betriebsart für die manuelle Lastabgabe. Die Positionierung der Last am Aufnahmepunkt kann automatisiert, z.B. durch eine Rollenbahn, oder manuell erfolgen. Ein solches Kranspiel wird als Ruf- und Versandbetrieb mit automatischer Lastaufnahme bezeichnet. Das Bereitstellen der Last in der Übergabeposition kann manuell oder automatisiert, z.B. über eine Rollenbahn, erfolgen.

Abbildung 4-9 zeigt ein Kranspiel mit manueller Leerfahrt, manueller Lastaufnahme und einem Wechsel in die automatische Betriebsart für die automatische Kranfahrt und automatische Lastabgabe. Ein solches Kranspiel wird als Ruf- und Versandbetrieb mit automatischer Lastabgabe gekennzeichnet. Das Entfernen der Last aus der Übergabeposition kann manuell oder automatisiert, z.B. über eine Rollenbahn, erfolgen.

Abbildung 4-10 zeigt ein Kranspiel mit automatischer Leerfahrt, einem Wechsel in die manuelle Betriebsart für die manuelle Lastaufnahme, einem weiteren Wechsel in die automatische Betriebsart für die automatische Lastfahrt und die automatische Lastabgabe. Ein solches Kranspiel wird als Versandbetrieb mit automatischer Lastabgabe bezeichnet.

Abbildung 4-11 zeigt ein ausschließlich automatisiertes Kranspiel, mit automatisierter Leerfahrt, automatisierter Lastaufnahme, automatisierter Lastfahrt und automatisierter Lastabgabe.

Für jede automatisierte Krananlage sind die Zielpositionen für die Kranfahrt vor Beginn des automatisierten Kranbetriebes festzulegen, was im Einrichtungsbetrieb oder „Teachmodus“ vorgenommen wird. Neben den manuellen, teilautomatisierten und automatischen Betriebsmodi ist daher auch der Teachmodus bei einer Sicherheitsanalyse mit zu berücksichtigen.

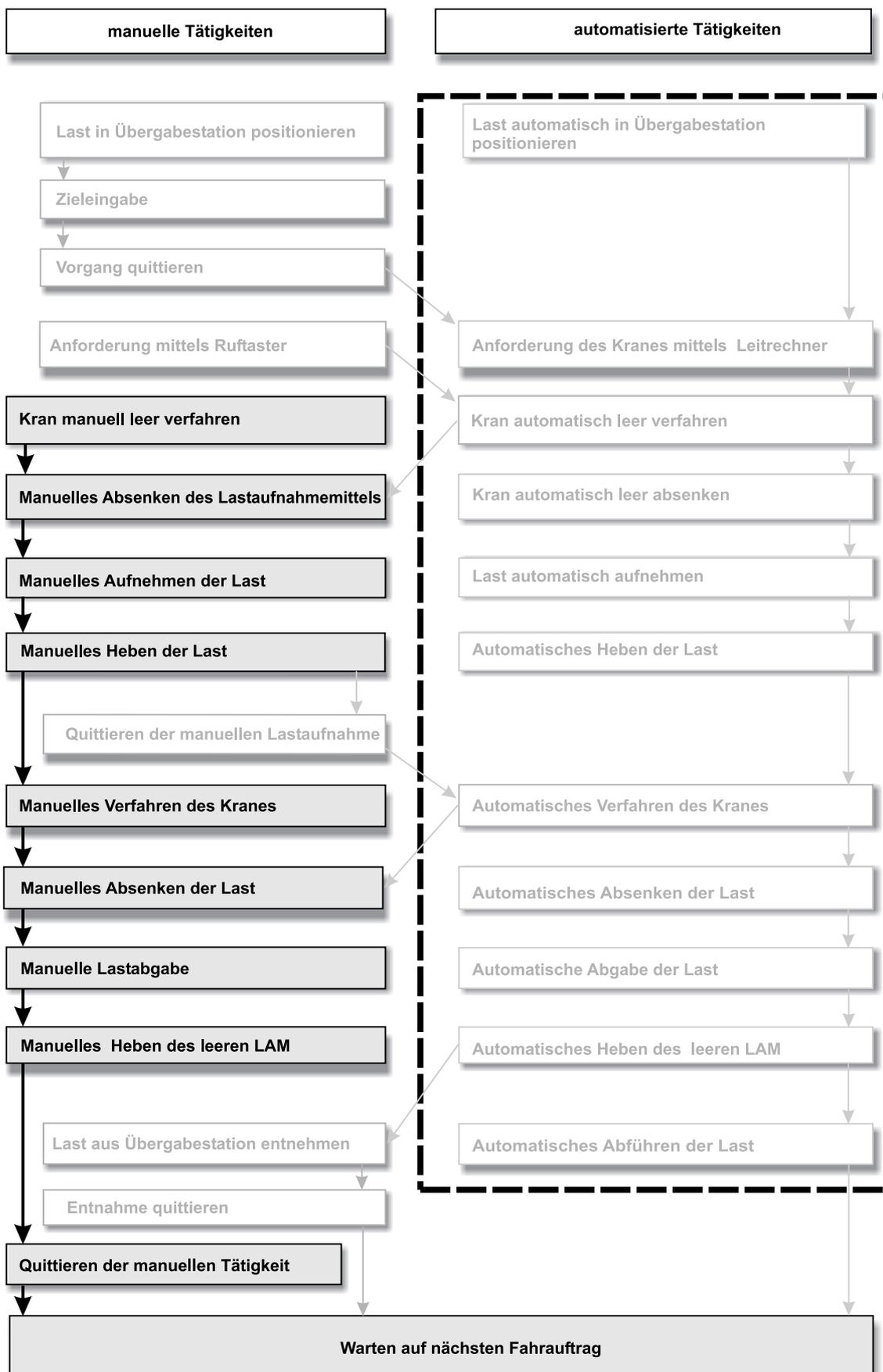


Abb. 4-4: Manueller Kranbetrieb

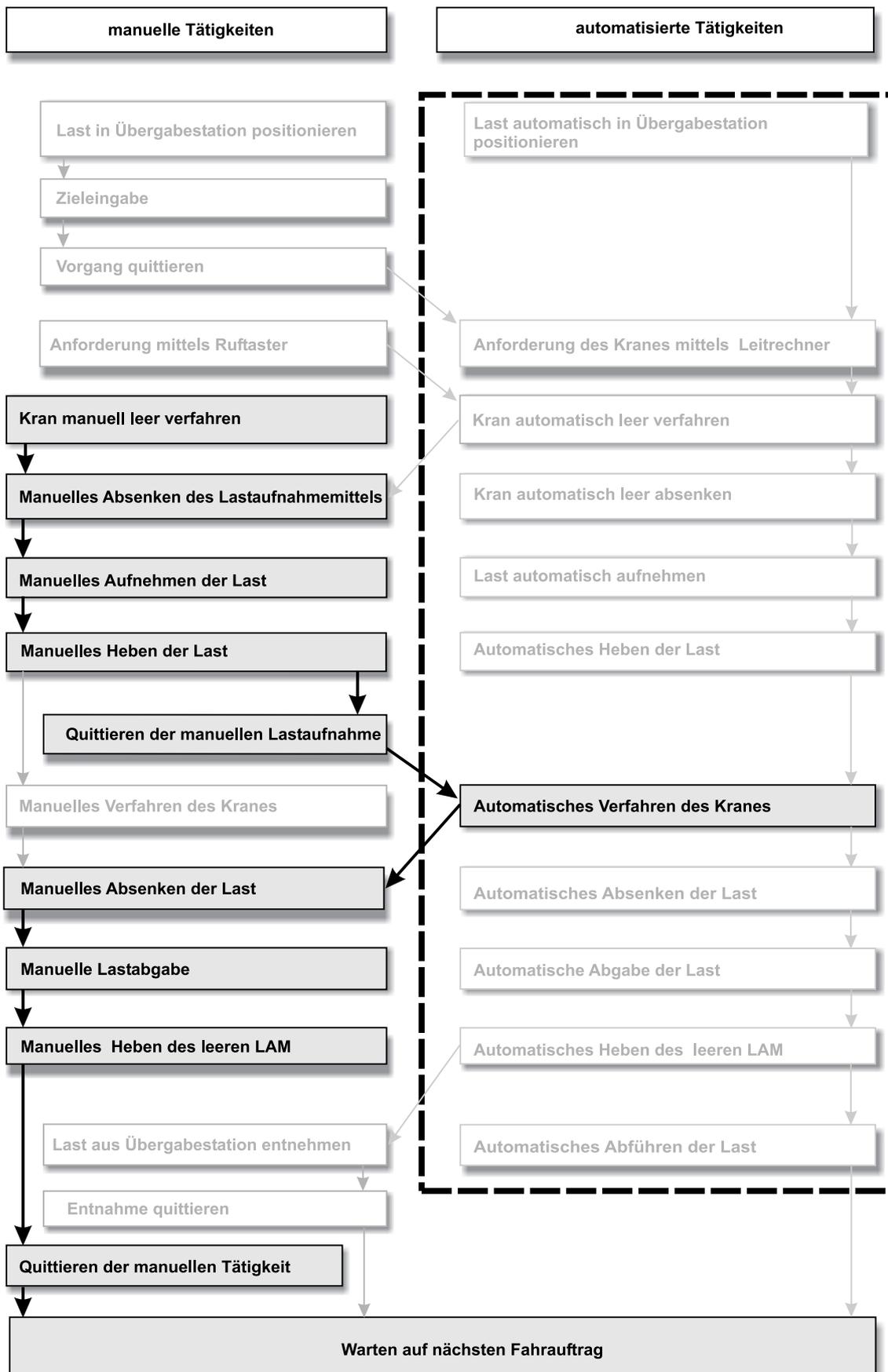


Abb. 4-5: Versandbetrieb

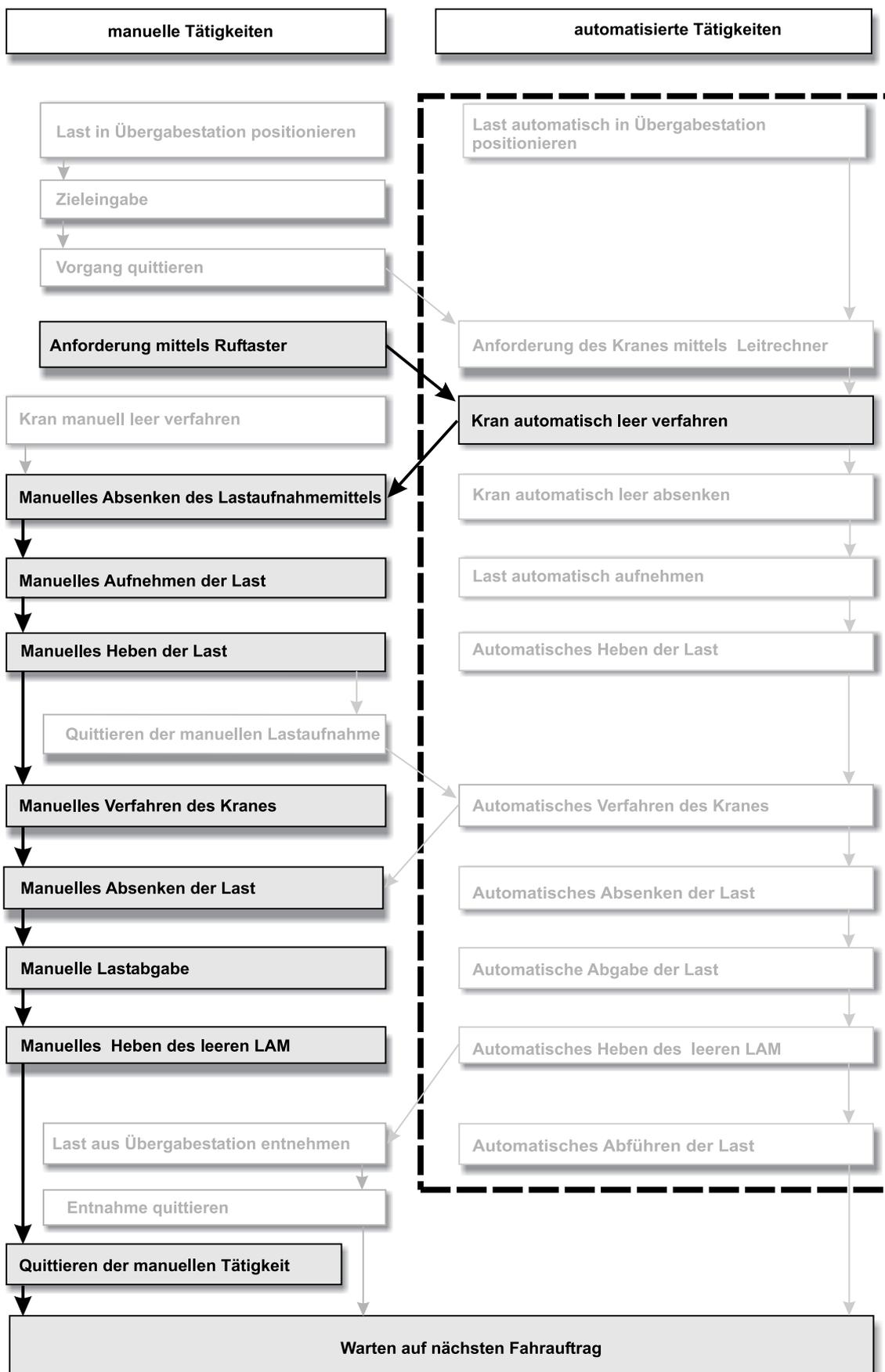


Abb. 4-6: Rufbetrieb

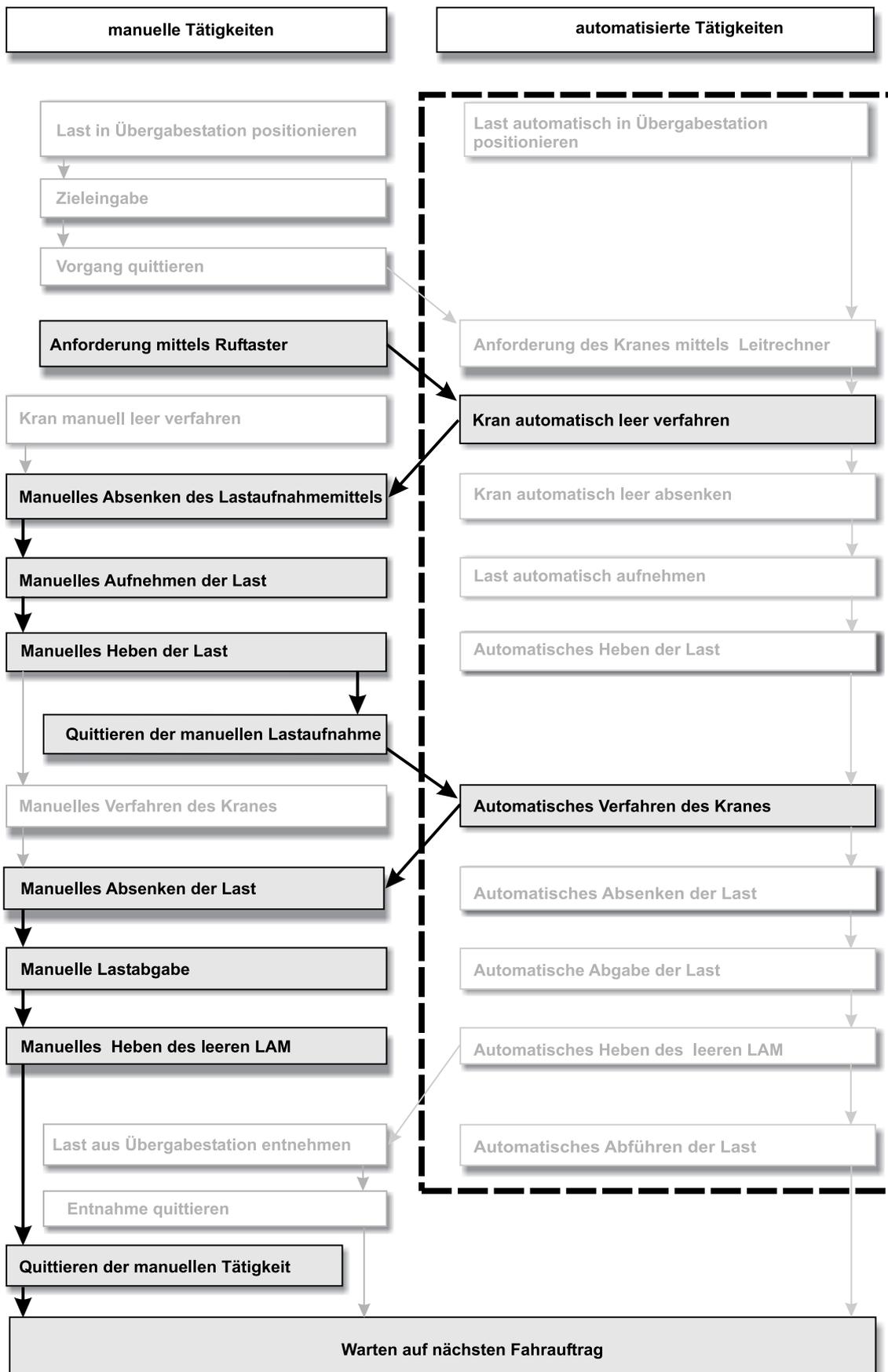


Abb. 4-7: Ruf- und Versandbetrieb

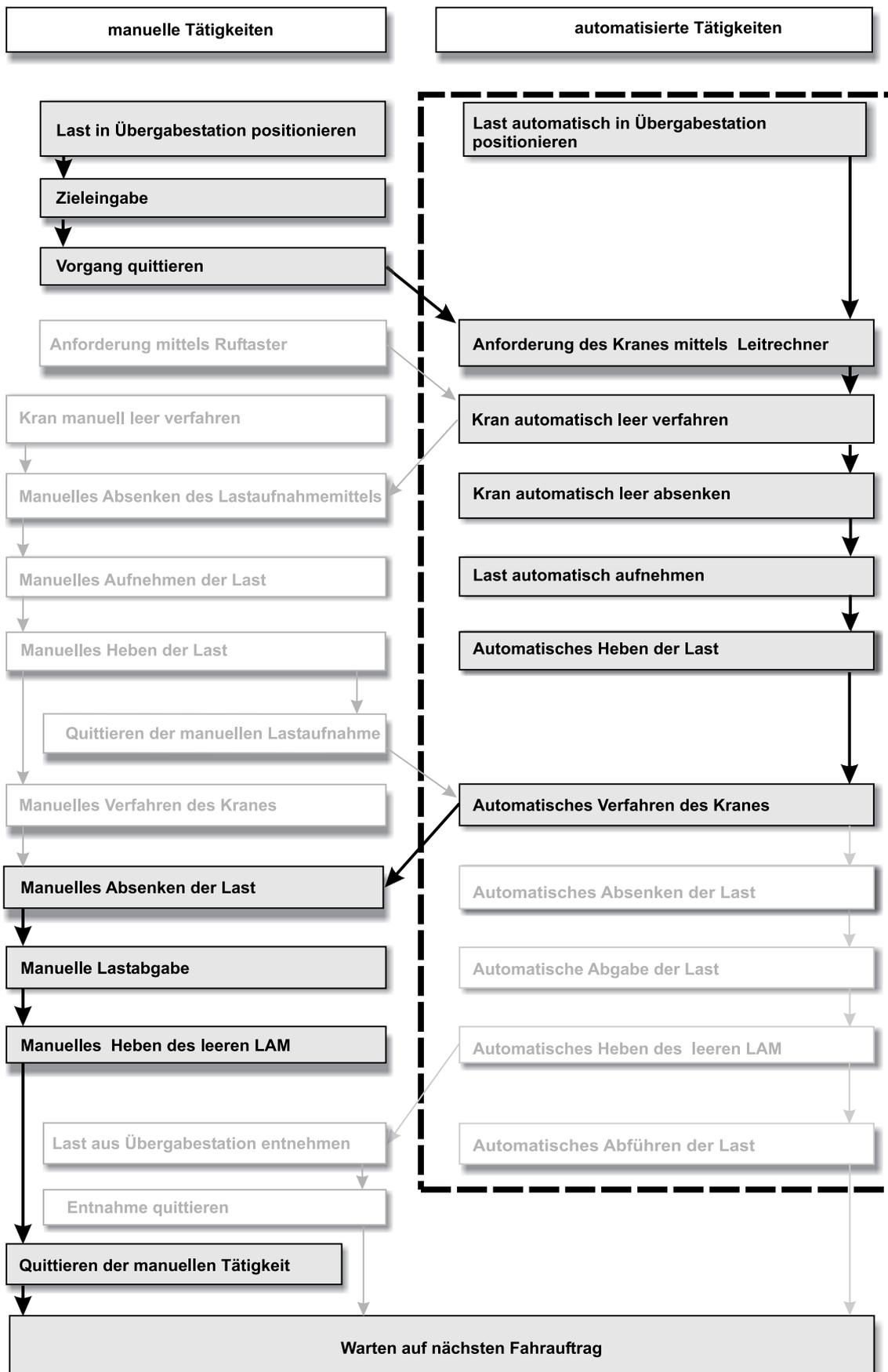


Abb. 4-8: Ruf- und Versandbetrieb mit automatischer Lastaufnahme

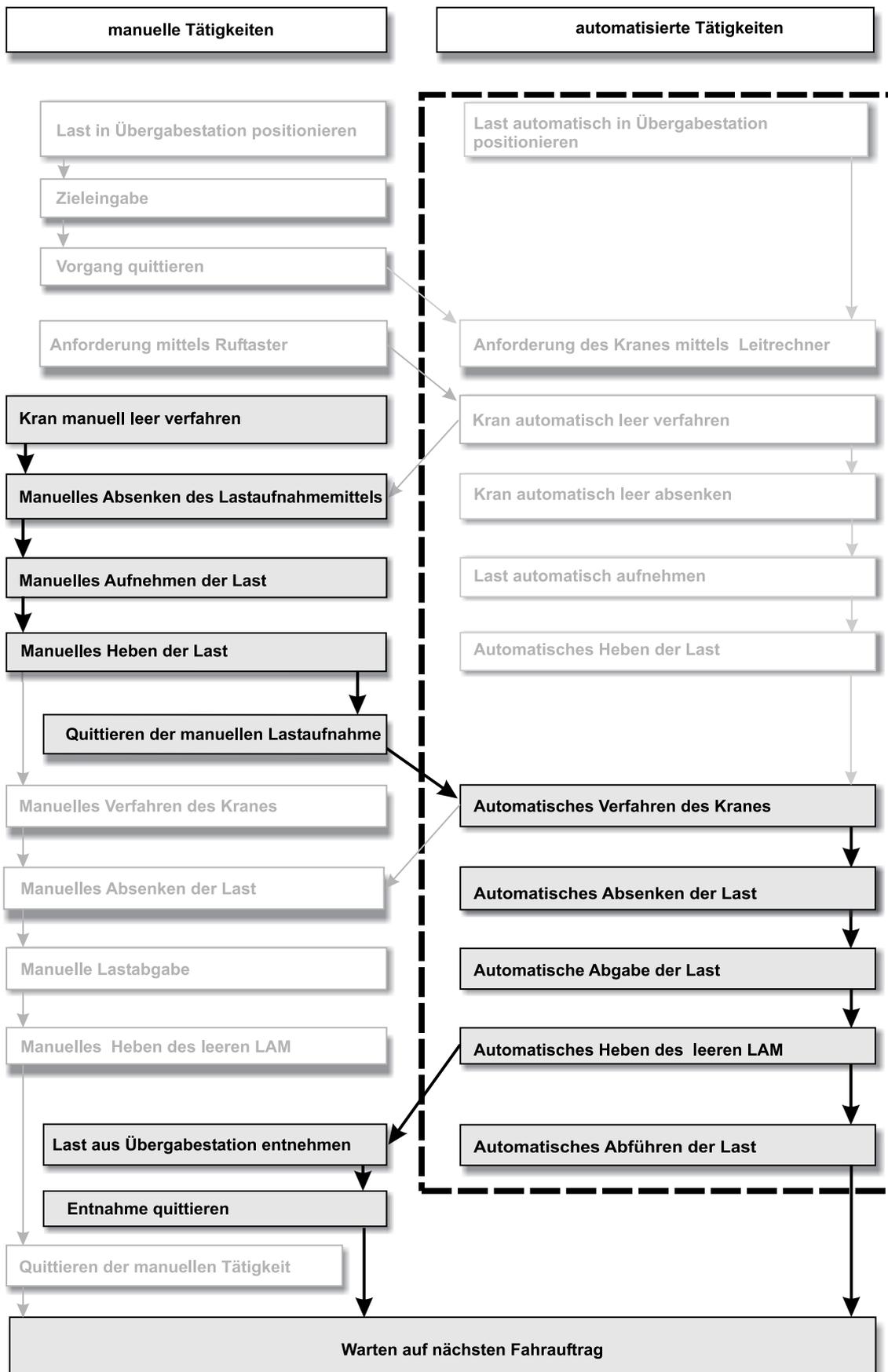


Abb. 4-9: Ruf- und Versandbetrieb mit automatischer Lastabgabe

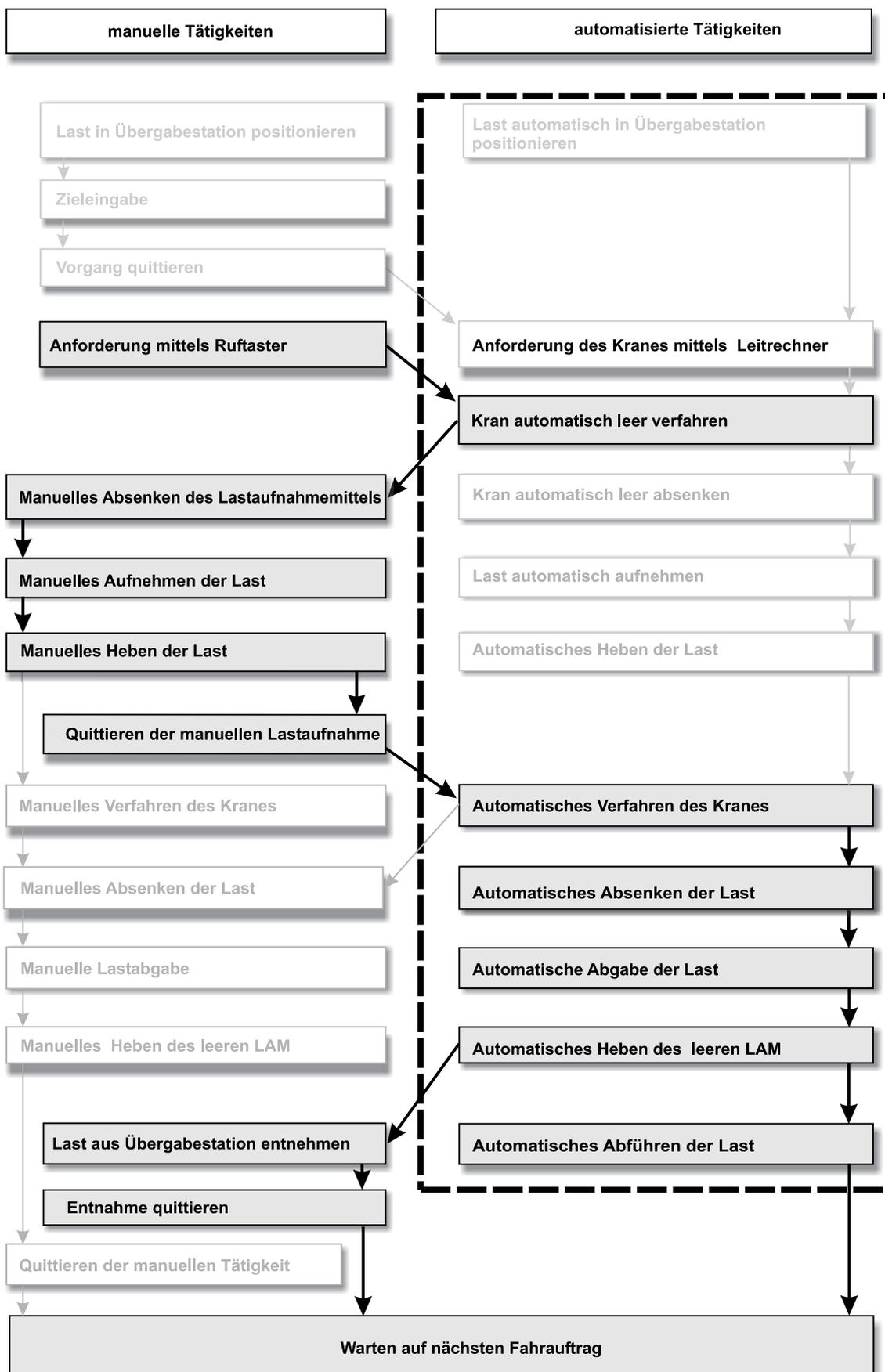


Abb. 4-10: Versandbetrieb mit automatischer Lastabgabe

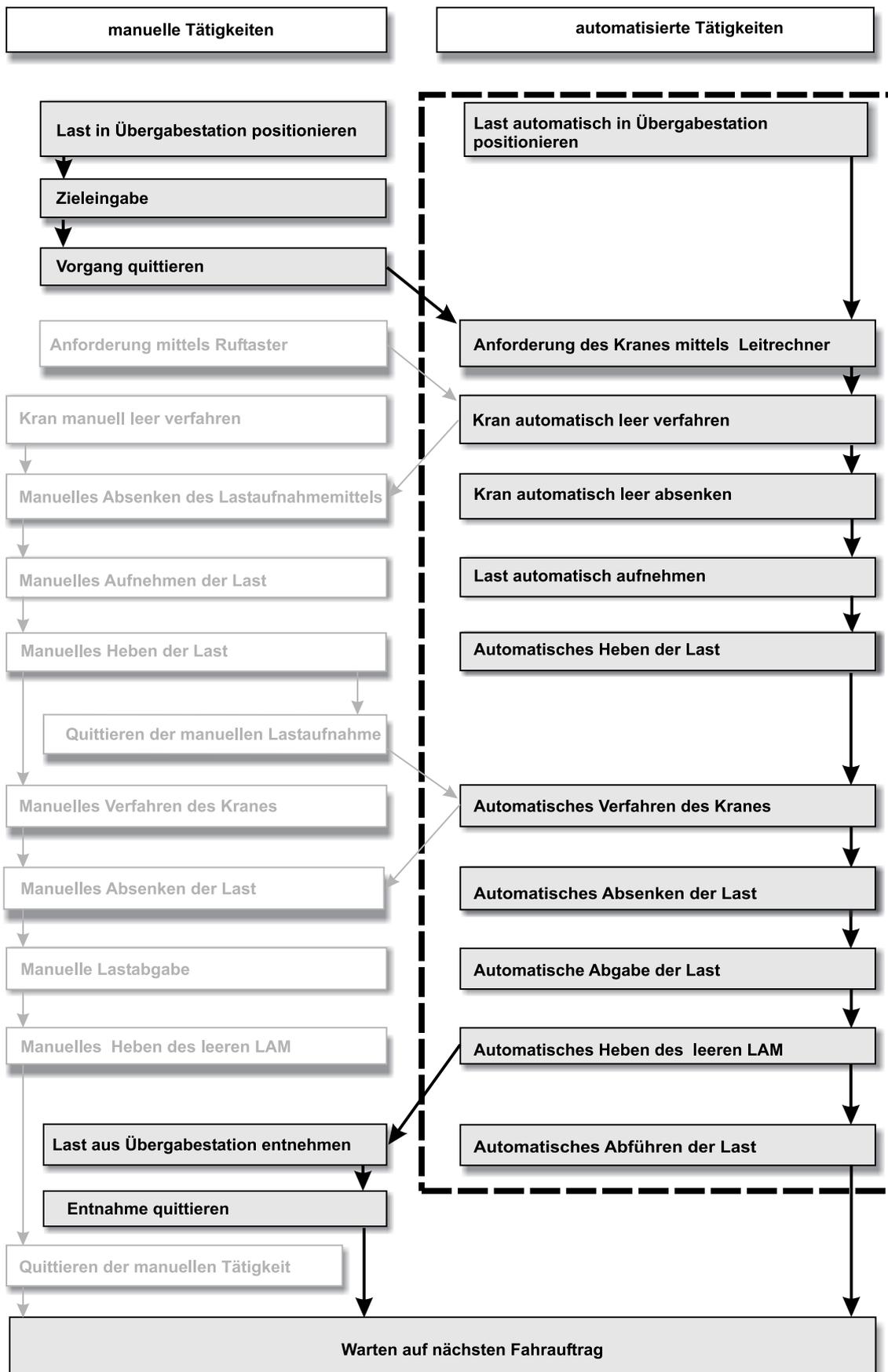


Abb. 4-11: Vollautomatischer Betrieb

4.4 Bauteile

4.4.1 Bauteile des manuellen Kranes

Für eine systematische Zerlegung eines Kranes in seine Grundbausteine eignet sich die „Top Down“-Methode. Dabei wird auf die wichtigsten Antriebselemente und Bauteile eingegangen.

Als erstes ist der Stahlbau oder das Tragwerk, auf dem die Kranschiene liegen, zu nennen. Nach einer strengen Definition gehören diese zwar nicht direkt zum Kran, bilden jedoch die mechanische Verbindung des Kranes zur Außenwelt, und sind somit ein fundamentaler Bestandteil.

In Abbildung 4-12 ist beispielhaft ein auf Kranschiene fahrender Kran dargestellt. Dieser wiederum besteht aus den Fahrwerken und der Kranbrücke. Die Fahrwerke enthalten Antriebe und Bremsen.

Auf der Kranbrücke fährt die Katze. Die Katze besteht aus einem Katzfahrwerk und dem Hubwerk. Das Katzfahrwerk enthält Antrieb und Bremsen. Das Hubwerk, die eigentliche Hebeeinrichtung am Kran, besteht aus Antrieb, Getriebe, Bremse sowie Seiltrommel und Seil.

Am unteren Ende des Seiles befindet sich im Falle eines Standardhallenkranes meistens ein Haken oder irgendein anders geartetes Lastaufnahmemittel.

Zuletzt ist noch die zu transportierende Last zu betrachten. Diese gehört zwar nicht zum Kran selbst, ist aber elementarer Bestandteil eines Transportvorganges.

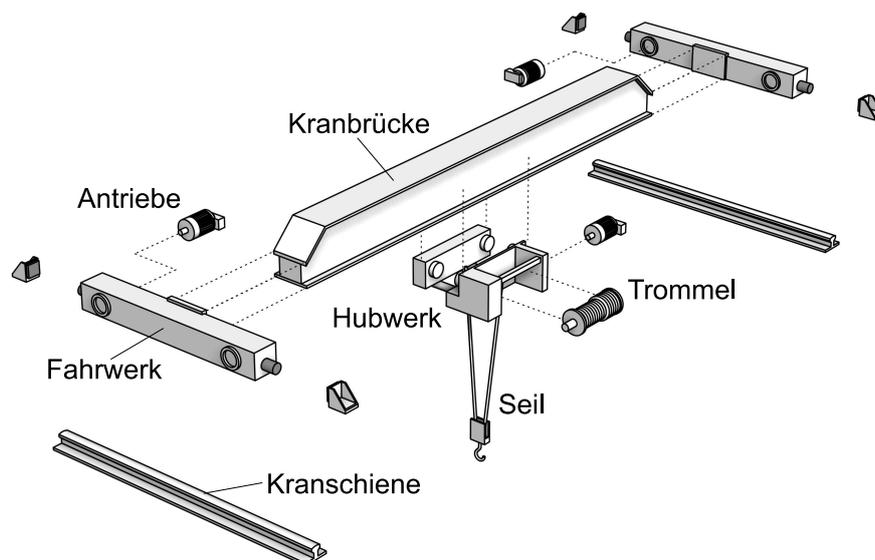


Abb. 4-12: Manueller Brückenkrane

4.4.2 Bauteile des automatisierten Kranes

Jeder automatisierte Kran enthält die gleichen Elemente, wie sie oben für den manuellen Hallenkran beschrieben wurden. Zusätzliche Komponenten zur Automatisierung sind auf jeden Fall eine Steuerung, die die Bewegungen des Kranes steuert und den Menschen als überwachendes Element ersetzt, sowie ein Wegmesssystem, das der Steuerung Informationen über die Position von Kranbrücke, Katzfahrwerk, und Hubhöhe des Lastaufnahmemittels liefert.

Für einen automatisierten Betrieb ist auch ein Lastaufnahmemittel zur automatisierten Aufnahme der Last erforderlich. Abbildung 4-13 stellt einen automatisierten Brückenkran schematisch dar.

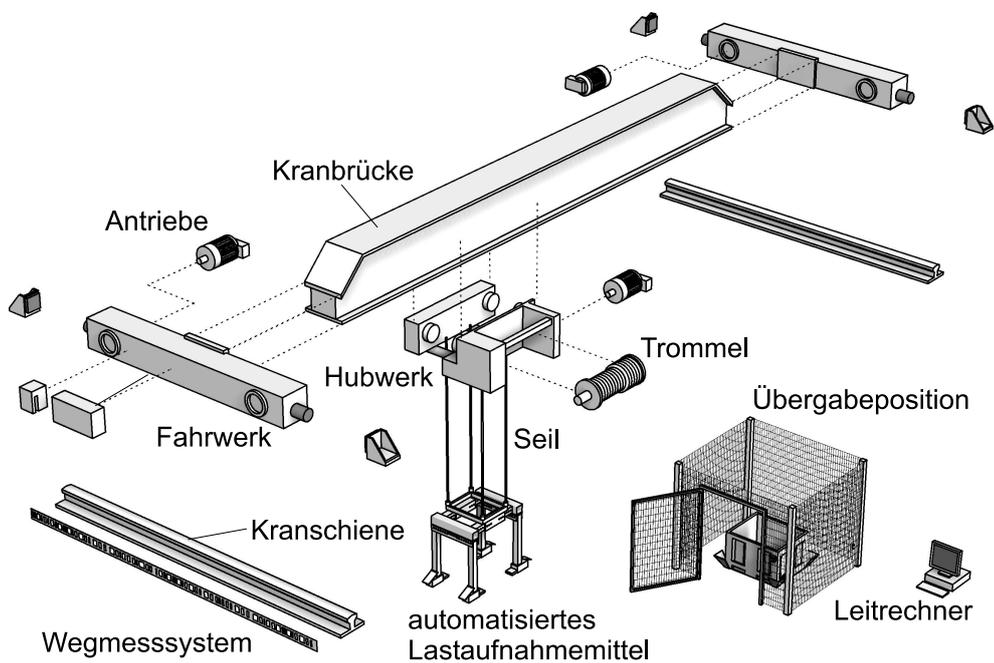


Abb. 4-13: Automatisierter Brückenkran

5 Die Sicherheitsanalyse

Um Gefahrenquellen auszuschließen und Unfälle verhindern zu können, müssen die potentiellen Gefahren zunächst einmal durch eine Sicherheitsanalyse erkannt werden. Die Sicherheitsanalyse eines technischen Systems ist, knüpft man an das vorhergehende Kapitel an, eine Systemanalyse unter sicherheitstechnischen Gesichtspunkten. Im folgenden Kapitel werden verschiedene Verfahren für eine Sicherheitsanalyse vorgestellt. Ausgehend von den bestehenden Analyseverfahren, wird eine neue speziell für automatisierte Krananlagen abgestimmte Sicherheitsanalyse entwickelt.

5.1 Aufgaben und Ziele

Die wesentliche Aufgabe einer Sicherheitsanalyse besteht darin, Gefahren, die von einem technischen System ausgehen können, zu ermitteln und die Behandlung der Fragen nach den Reduzierungsmöglichkeiten solcher Gefahren. Dabei betrachtet die Sicherheitsanalyse das technische System als Gesamtheit aller Elemente, die miteinander in Wechselwirkung stehen, und das Verhalten, das sich aus dem Zusammenwirken dieser Elemente ergibt [11].

Ihre Aufgabe besteht zuerst in der Beantwortung folgender Fragen:

- Welche Störfälle sind als wesentlich zu betrachten?
- Welche Störfälle können durch geeignete Änderungen der Systemstruktur verhindert werden?
- Welche Störfälle sind nicht vollständig auszuschließen und mit welcher Häufigkeit bzw. Wahrscheinlichkeit ist ihr Auftreten zu erwarten?
- Welcher Art und Größe sind deren Auswirkungen auf Personen und Sachen der näheren und weiteren Umgebung und welche Schutzmaßnahmen müssen getroffen werden?

Zur Durchführung einer Sicherheitsanalyse ist es speziell für automatische Krananlagen notwendig, ein möglichst vollständiges Verfahren zu wählen, da man sich wegen der mangelnden Erfahrung bei Betrieb solcher Anlagen auf dieses neuartige Konzept

einer Krannutzung nicht darauf verlassen kann, durch Intuition alle Gefahren zu erkennen. Aus den oben genannten Rahmenbedingungen ergeben sich somit folgende Anforderungen an eine Sicherheitsanalyse für automatische Krananlagen:

- Die Methode soll alle Gefahren, die in allen Betriebsarten auftreten, erkennen.
- Erfolgsaussichten sollen gewährleistet sein.
- Es soll der Mensch-Maschine-Einfluss berücksichtigt werden, da Krane auch teilautomatisiert betrieben werden.
- Die Methode sollte sich für Analysen in der Planungs- und Betriebsphase eignen, da man für eine Grundlagenuntersuchung unabhängig von bestehenden Systemen sein möchte, sofern es denn welche gibt.
- Die Methode braucht keine Verknüpfung von Fehlern zu berücksichtigen, da eine Ein-Fehler-Sicherheit aus wirtschaftlichen und technischen Gründen als ausreichend erachtet wird.
- Der Zeitaufwand sollte eine untergeordnete Rolle spielen, da es sich hier um eine Grundlagenarbeit handelt, bei der Sorgfalt an erster Stelle steht.

5.2 Allgemeiner Ablauf

Die Eingangsdaten für die Sicherheitsanalyse sind Zahlen und Fakten des eingesetzten Produktionsverfahrens, der gehandhabten Stoffe, der technischen Gestaltung der Anlage, der Betriebsorganisation und der Umwelt. Alles zusammen definiert gemeinsam den Untersuchungsgegenstand.

Die optimale Lösung ist erreicht, wenn die Sicherheit den von außen vorgegebenen Anforderungen, z.B. Risikogrenzwerten, genügt und wenn für die zu fordernde Sicherheit der wirtschaftliche Aufwand möglichst gering bleibt. Ist bei einer Anlagenkonzeption mit wirtschaftlich vertretbarem Aufwand ein ausreichendes Maß an Sicherheit nicht möglich, so müssen Änderungen dieser Konzeption in Betracht gezogen werden. Der Umfang der Sicherheitsanalyse reicht von der groben qualitativen Abschätzung der Gefahrenquellen über die detaillierte qualitative Analyse bis zur quantitativen Analyse mit Zahlenangaben über die zu erwartende Häufigkeit und Auswirkung von Störfällen und hat sich nach der Aufgabenstellung zu richten.

Allgemein geht man in der Praxis so vor, dass zunächst eine grobe qualitative Analyse zur Ermittlung von Gefahrenquellen als Grundlage für detaillierte Untersuchungen erfolgt. Je nach Bedarf werden danach Umfang und Tiefe der Analyse schrittweise erweitert. Quantitative Analysen beziehen sich in der Regel nur auf einen sicherheitstechnisch besonders wichtigen Teil der Anlage.

Das Ablaufschema des Vorgehens mit Entscheidungspunkten über das schrittweise Handeln [11] zeigen die Abbildungen 5-1 und 5-2.

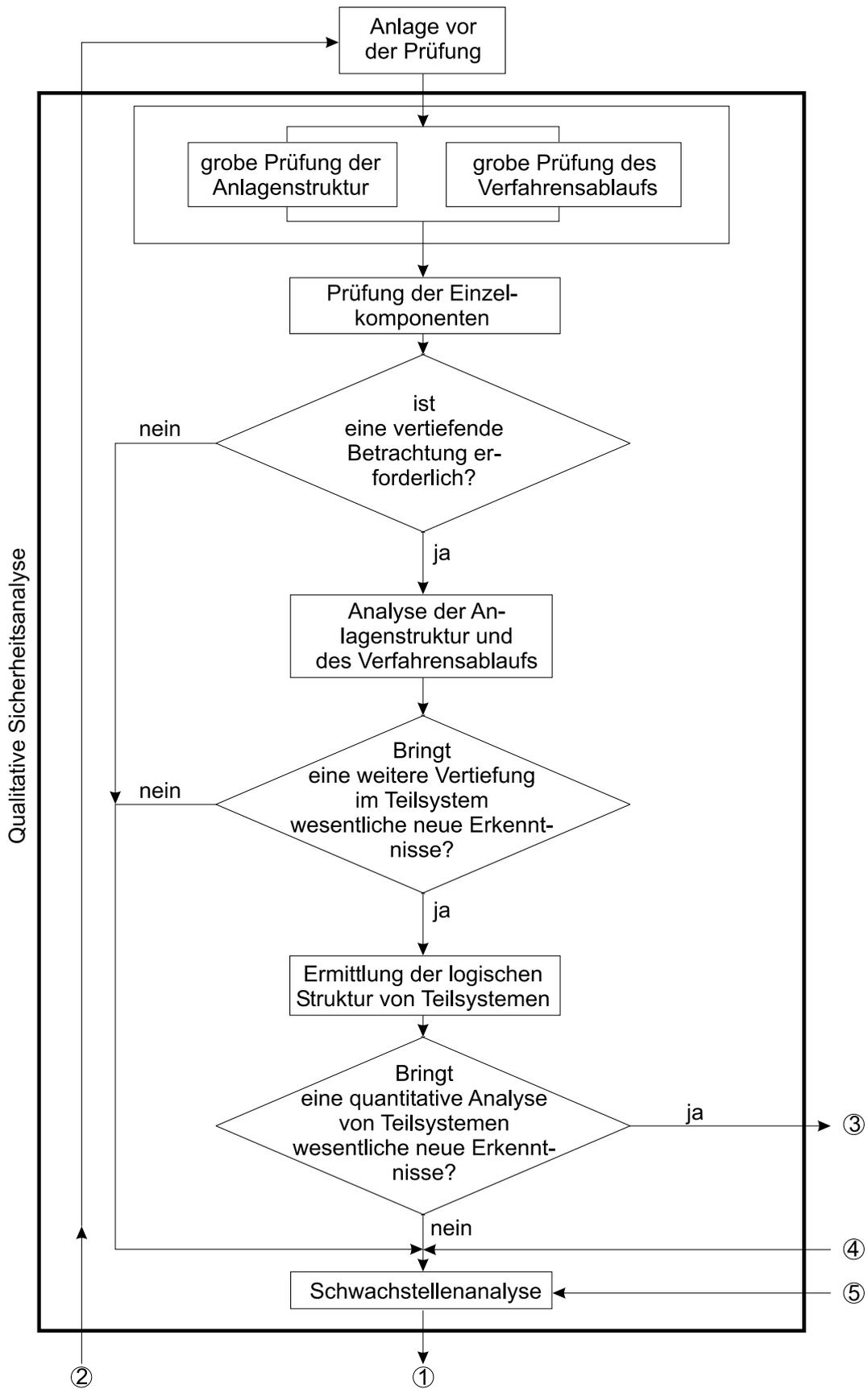


Abb. 5-1: Stufen der Sicherheitsanalyse 1

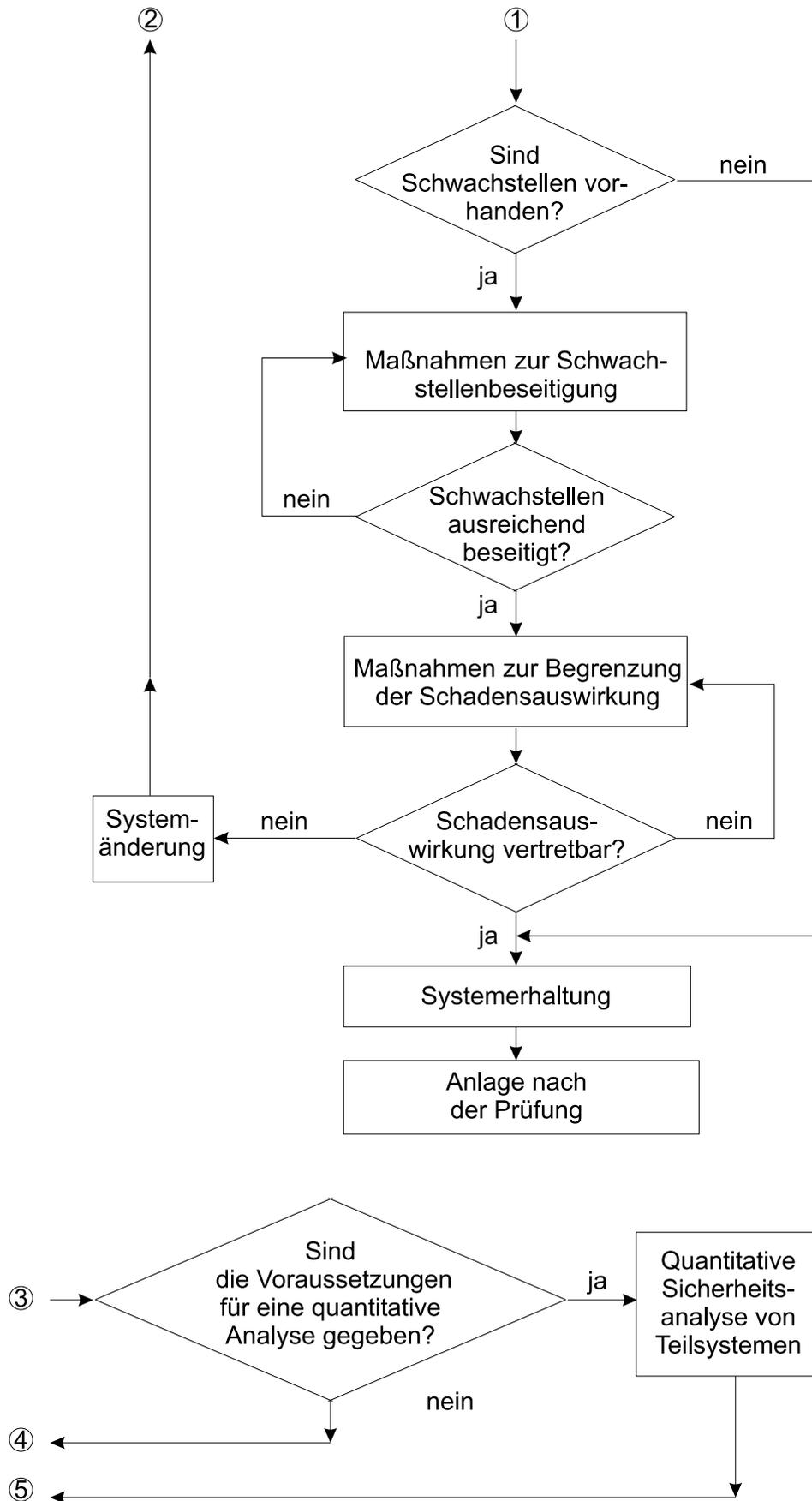


Abb. 5-2: Stufen der Sicherheitsanalyse 2

Nach der Definition der Anlage kann in einfach gelagerten Fällen eine komponentenorientierte Analyse ausreichen, die sich in der Feststellung erschöpft, ob die Anforderungen an die Komponenten und ihre Auslegung einander entsprechen. In vielen Fällen wird eine Analyse zur Anwendung kommen, welche die eingesetzten Stoffe, Prozessparameter sowie Mess- und Regeltechnik berücksichtigt. Diese Analyse bietet sich vor allem an, wenn neuartige technische Verfahren zur Anwendung kommen, besonders komplexe Zusammenhänge zu betrachten sind, ein höheres Gefährdungspotential bei Betrieb vorhanden ist oder auch wirtschaftliche Gründe hierfür sprechen. In einem weiteren Schritt kann die Analyse bis zur Ermittlung der logischen Systemstruktur vertieft werden. Dies wird dann notwendig, wenn sehr detaillierte Ergebnisse zu fordern sind oder der Übergang zu einer quantitativen Analyse geschaffen werden muss. Die quantitative Analyse setzt dann allerdings auch hinreichende Datenkenntnisse voraus.

Die Sicherheitsanalyse findet ihren Abschluss in der Ermittlung der Schwachstellen und in Vorschlägen zu deren Entschärfung bzw. zur Beseitigung durch geeignete Maßnahmen.

5.3 Vorläufige Gefahrenanalyse

Die vorläufige Gefahrenanalyse (Preliminary Hazard Analysis, PHA) ist eine allgemeine Art der Gefahrenanalyse, die sich vom Sicherheitsstandpunkt aus ein Gesamtbild über ein System verschafft. Sie dient als Grundlage für detailliertere weiter unten beschriebene Analysemethoden für Einzelkomponenten oder Einzelsysteme, wie z.B. Fehlermöglichkeitseinflussanalyse (FMEA) oder Fehlerbaumanalyse, die erst nach einer vorläufigen Gefahrenanalyse durchgeführt werden. Über den Zeitpunkt der Anwendung der vorläufigen Gefahrenanalyse gibt es in der Literatur geteilte Meinungen. Während bei Sundarajan [25] die vorläufige Gefahrenanalyse nur während der einzelnen Entstehungsschritte, also in der Konstruktionsphase eines Systems durchgeführt wird, ist für Ridley und Pearce [26] die Anwendung an Systemen während ihres vollständigen Lebenszyklus möglich, um die Gefahren und deren Einfluss auf die Sicherheit zu identifizieren. Betrachtet man den im Folgenden beschriebenen Ablauf der Analyse, so kann man erkennen, dass je länger das System existiert, desto genauere Aussagen über das System getroffen werden können, da die Datenbasis und der Erfahrungsraum viel umfangreicher und genauer sind. Somit liegt auch der Schluss nahe, diese Art der Analyse immer anzuwenden.

5.3.1 Das Verfahren der vorläufigen Gefahrenanalyse

Die Vorläufige Gefahrenanalyse besteht aus folgenden Schritten [25]:

- I. Daten Sammeln

II. Identifikation der Gefahrenquellen

III. Erstellen einer Tabelle mit den Gefahren und deren Auswirkungen.

Jeder dieser Schritte ist in den folgenden Abschnitten beschrieben.

zu I. Daten Sammeln

Die Arbeitsgruppe, die eine vorläufige Gefahrenanalyse durchführt, sollte alle verfügbaren Informationen über Bauteile, verwendete Werkstoffe, Prozesse, Versuchsergebnisse und Verfahrensabläufe, die mit dem zu untersuchenden System in Verbindung stehen, analysieren. Da die vorläufige Gefahrenanalyse normalerweise während der konzeptionellen Phase eines Systems durchgeführt wird, fehlen meistens detaillierte Zeichnungen und Daten. In diesem Fall sollen Systemzeichnungen, die die ungefähre Positionen von Komponenten, Bedienstationen oder den Prozessablauf darstellen, zur Untersuchung herangezogen werden.

zu II. Identifikation der Gefahrenquellen

Bei diesem Verfahren ist jedes Bauteil, jeder verwendete Werkstoff, sowie der Prozess oder Verfahrensablauf als Gefahrenquelle (gefährliches Element) zu betrachten, da jedes dieser Elemente unter irgendwie gearteten Umständen Tod, Verletzungen oder Sachschaden hervorrufen kann. Dabei ist zu beachten, dass unter normalen Umständen diese Elemente ungefährlich sind, aber unter gewissen anormalen Umständen potentielle Auslöser für Unfälle sein können. Alle gefährlichen Quellen, ob Bauteile, Werkstoffe, Prozesse oder Verfahrensabläufe, sollten identifiziert und dokumentiert werden. Wie weit man bei der Betrachtung der Bauteile in die Tiefe geht ist je nach System, Ziel der Gefahrenanalyse und natürlich auch nach Fortschritt der Planungen unterschiedlich. In einer Vorplanungsphase ist sicherlich noch keine Detailanalyse auf Bauteilebene möglich, andererseits können bei einer Änderung des Verfahrens an einer bestehenden Anlage mehrere Baugruppen bis auf die Bauteilebene untersucht werden.

Nach Durchführung der vorläufigen Gefahrenanalyse erhält man eine Liste potentieller Gefahren. Als Hilfestellung lassen sich in der Literatur folgende allgemeine Gefahrenquellen für Maschinen finden:

- Explosive Materialien
- Brennbare Materialien
- Sehr hoher oder sehr niedriger Druck
- Sehr hohe oder sehr niedrige Temperatur
- Hochspannung
- Radioaktive Materialien
- Giftige Substanzen

- Zyklisch bewegte Teile
- Rotierende Teile
- Federvorgespannte Teile
- Fallende Objekte
- Hängende Objekte

Diese Liste ist selbstverständlich nicht als vollständig zu bezeichnen, sondern soll dem Anwender nur als Unterstützung dazu dienen, die wesentlichen Gefahren nicht zu übersehen. Wichtig ist auch, dass der Nutzer sich nicht durch derartige Hilfestellungen vereinnahmen lässt, sondern auch weiterhin versucht, durch eine objektive Betrachtung des Systems andere Gefahrenquellen zu finden.

Es ist wichtig, wie auch bei anderen Methoden zur Gefahrenanalyse, von Beginn der Planungen an die gefährlichen Elemente nicht nur während des normalen Betriebes des Systems, sondern auch während der Installation, im Versuchsbetrieb, während der Wartung und beim Abbau des Systems zu berücksichtigen.

Bei der bisherigen Betrachtung der vorläufigen Gefahrenanalyse wurde nur versucht, primäre Gefahrenquellen zu finden. Allerdings sollten für die vorläufige Gefahrenanalyse auch sekundäre Effekte berücksichtigt werden. Unter sekundären Effekten werden hier Ereignisse verstanden, die erst durch die Verkettung mit einem primären Ereignis eintreffen können, z.B. ein in großer Höhe angebrachtes Bauteil, das weit entfernt vom Personenbereich montiert ist und so keine direkte Gefahr für Personen darstellt. Sollte dieses Bauteil sich jedoch lösen (primäres Ereignis) und dadurch wiederum z.B. einen unterhalb angeordneten Behälter mit giftigen Substanzen zerstören (sekundäres Ereignis), wären Personen in Gefahr. Deshalb müssen alle auch objektiv harmlos erscheinenden Bauteile untersucht werden, die mit den oben genannten gefährlichen Quellen interagieren können. Wie viele Stufen in mögliche Kausalketten aufgenommen werden, hängt auch von den Zielen der Gefahrenanalyse und dem akzeptierten Restrisiko ab.

zu III. Erstellen einer Tabelle mit Gefahren und deren Auswirkungen

Tabelle 5 - 1 zeigt ein Beispiel für eine Tabelle mit Gefahren und deren Auswirkungen.

In dieser Tabelle sind für jedes potentiell gefährliche Element zehn Punkte abzuarbeiten. Manche dieser Punkte können je nach Ziel der Analyse ausgelassen werden. Jeder Punkt wird im Folgenden erklärt.

1. Gefahrenquelle

Die im zweiten Schritt der Gefahrenanalyse oben beschriebene und identifizierte Gefahrenquelle.

		Gefährliche Elemente		
		1	2	n
1.	Gefahrenquelle			
2.	Ort und Bezeichnung der Gefahrenquelle			
3.	Auslöser			
4.	Unfall			
5.	Auswirkungen des Unfalls			
6.	Warneinrichtungen			
7.	Präventivmaßnahmen			
8.	Effektminderungsmaßnahmen			
9.	Häufigkeit des Unfalls			
10.	Umfang des Unfalls			
11.	Bemerkungen			

Tabelle 5-1: Ergebnistabelle der PHA

2. Ort und Benennung der Gefahrenquelle

Die Benennung der Gefahrenquelle kann sich aus Zeichnungskordinaten oder aus anderen sinnvollen Bezeichnungen, z.B. nach einem Gebäudenamen, ergeben. Wichtig ist nur, dass eine eindeutige Bezeichnung gewählt wird. Die Bezeichnung des Ortes ist wichtig, da viele Unfälle vermieden werden können, indem die Gefahrenquelle von ihrem Auslöser räumlich getrennt wird. So können Brennstoffe möglichst weit von Zündquellen gelagert werden.

3. Auslöser

Wie oben schon gezeigt wurde, muss ein gefährliches Element unter normalen Umständen keine Gefahr darstellen. Durch einen Auslöser oder ein auslösendes Ereignis können diese Elemente zu Fehlfunktionen oder gefährlichen Zuständen führen. Möchte man Fehler verhindern, die durch nur einen einzelnen Auslöser auftreten, spricht man von der Ein-Fehler-Sicherheit. In vielen Fällen werden allerdings zwei oder mehrere Auslöser für einen Unfall benötigt. Um diese Unfälle zu verhindern, wird eine Zwei- oder Mehr-Fehler-Sicherheit verlangt. Zur Erkennung dieser Gefahrenquellen sind entsprechend viele Kombinationen von auslösenden Ereignissen zu untersuchen. Hier zeigen sich schon die Grenzen der vorläufigen Gefahrenanalyse, da eine Untersuchung für alle erdenklichen Kombinationen von Auslösern weder wirtschaftlich noch vom technischen Standpunkt her sinnvoll ist. Tabelle 5-2 zeigt eine mögliche Auswahl von Auslösern.

Da nicht jeder Auslöser oder die Kombination von verschiedenen Auslösern bei je-

- | | |
|--------------------------|---------------------------------------|
| a) Chemische Reaktion | j) Überspannung |
| b) Korrosion | k) Sehr hoher oder niedriger Druck |
| c) Explosion | l) Sehr hohe oder niedrige Temperatur |
| d) Feuer | m) Erschütterung |
| e) Leckagen | n) Bauteilversagen |
| f) Überlast (elektrisch) | o) Strukturversagen |
| g) Überlast (mechanisch) | p) Energieversagen |
| h) Vibration | q) Menschliches Versagen |
| i) Materialermüdung | r) Sabotage |

Tabelle 5-2: Auslöser für Unfälle

der Gefahrenquelle zwangsläufig zu einem Unfall führen, lässt sich die Anzahl der möglichen Kombinationen einschränken.

4. Unfall

Beschreibung des möglichen Unfalls, bestehend aus der Wechselwirkung von Gefahrenquelle und einem auslösenden Ereignis.

5. Auswirkung des Unfalls

Die Auswirkungen eines Unfalls können Tod, Personenschaden und/oder Sachschaden sein.

6. Möglichkeit für Warnungen

Einige Unfälle treten nicht sofort ein, andere hingegen sind eine sofort eintretende Katastrophe. Die Auswirkungen eines nicht sofort eintretenden Unfalls können durch ein Warnsystem vermindert werden. Feueralarmsysteme oder Gasdetektoren können hierfür beispielsweise genannt werden.

7. Präventivmaßnahmen

Präventivmaßnahmen können Unfälle zwar nicht vollständig verhindern, aber die Wahrscheinlichkeit eines Unfalls jedoch erheblich mindern. Sie können z.B. Schulungen für Mitarbeiter, mechanische Schutzeinrichtung oder regelmäßige Prüfungen von Bauteilen sein.

8. Effektminderungsmaßnahmen

Negative Auswirkungen des Unfalls können durch Effektminderungsmaßnahmen, wie beispielsweise Feuerlöscher, verkleinert werden.

9. Häufigkeit des Unfalls

Während der Durchführung der vorläufigen Gefahrenanalyse ist selten die Häufigkeit eines Unfalls vorhersehbar. Grobe Abschätzungen dafür können jedoch in der Ergebnistabelle berücksichtigt werden. Dabei ist zu berücksichtigen, dass z.B. Präven-

tivmaßnahmen die Häufigkeit eines Unfalls verringern können. Dieser Aspekt wird auch bei vielen Analysen weggelassen. Man kann eine sehr einfache Einteilung, wie in Tabelle 5-3 dargestellt, der Unfallhäufigkeiten vornehmen [25]:

	Unfallhäufigkeit:
I Sehr selten:	kleiner $10^{-6}/h$
II Selten:	zwischen 10^{-5} und $10^{-6}/h$
III Möglich:	zwischen 10^{-4} und $10^{-5}/h$
IV Wahrscheinlich:	größer als $10^{-4}/h$

Tabelle 5-3: Einteilung der Unfallhäufigkeit

Dies ist nicht die einzig mögliche Einteilung. Je nach vorhandener Datenbasis kann man auch andere Einteilungen wählen.

10. Umfang des Unfalls

Den Umfang eines Unfalls kann man für eine Bewertung innerhalb der vorläufigen Gefahrenanalyse in verschiedene Grade einteilen:

- I Unbedeutend: Unfall verursacht sehr geringen Sachschaden.
- II Gering: Unfall verursacht Schaden am System; Reparatur ist notwendig; jedoch sind Tod, Verletzung und Krankheit nicht möglich.
- III Kritisch: Unfall kann Tod, Verletzung und Krankheit verursachen oder schweren Sachschaden hervorrufen, aber die Zeit für Arbeiter reicht aus, schlimmeren Schaden zu verhindern.
- IV Katastrophe: Unfall verursacht sofort Tod, Verletzung und Krankheit oder auch schweren Sachschaden (keine Zeit für Reaktionen).

Diese Einteilung ist nicht die einzige Möglichkeit, Unfälle zu klassifizieren. Man kann diesen Aspekt auch weglassen, wenn nur ungenügende Informationen über das System vorliegen.

11. Bemerkungen

Die Ergebnistabelle ist offen für weitere Eintragungen, wie z.B. Verbesserungsvorschläge.

5.3.2 Nutzen und Grenzen der vorläufigen Gefahrenanalyse

Die vorläufige Gefahrenanalyse ist am besten geeignet, um mögliche Unfallgefahren durch einen oder maximal zwei Auslösemechanismen zu finden. Unfälle mit mehreren Auslösemechanismen zu finden, ist sehr aufwändig oder gar unmöglich. Dafür sind andere Analysemethoden, wie z.B. die Fehlerbaumanalyse, geeignet, die einen methodischeren Ansatz verfolgen. Sofern die in den Formblättern aufgeführten Ausfalleffekte mit Ausfallhäufigkeiten oder Ausfallraten belegt werden können, sind diese

die Basis für ein quantitatives Prognoseverfahren. Eine weitere Schwäche dieser Analyse ist, dass die Ergebnisse nur so gut wie die verfügbaren Informationen bzw. die doch subjektiv geprägten Abschätzungen der durchführenden Personen sind.

5.4 Fehler Möglichkeits- Einflussanalyse

Die Fehler Möglichkeits- Einflussanalyse (Failure Modes and Effekt Analysis, FMEA) oder auch Ausfalleffektanalyse genannt, ist im Wesentlichen ein qualitatives Prognoseverfahren. Die Ausfalleffektanalyse ist eine geeignete Analysetechnik zur Überprüfung von Systementwürfen, da sie ohne mathematischen Aufwand durchgeführt werden kann, wobei verschiedene Fehlermöglichkeiten von Einzelteilen, welche ein Gesamtsystem bilden, und deren Auswirkungen auf die Zuverlässigkeit des Systems betrachtet werden. Indem man die Auswirkungen eines einzelnen Bauteils bis auf Systemebene zurückverfolgt, können die Gefährlichkeit dieses Bauteils bestimmt und verbessernde Maßnahmen ergriffen werden, indem Wege zum Ausschluss von Fehlern oder eine Verringerung der Auftrittswahrscheinlichkeit eines gefährlichen Fehlers gefunden werden.

Im Allgemeinen ist die FMEA die effektivste Methode, wenn sie auf ein System ohne Redundanzen angewandt wird. Sie kann in diesem Fall dazu verwendet werden, kritische Bereiche einer Anlage zu identifizieren, die zusätzliche redundante Komponenten, Unterbaugruppen, zusätzliche Teile oder andere Hilfsmittel brauchen, um die Sicherheit zu erhöhen.

Die FMEA ist eine „Bottom-Up“-Analyse, die im Gegensatz zu „Top-Down“-Methoden, wie z.B. der Fehlerbaumanalyse (fault tree analysis FTA), steht. Die zwei Techniken sind einander ergänzend, da die Ergebnisse der FMEA als Startereignisse für eine detaillierte Fehlerbaumanalyse genutzt werden können. Die FMEA wird im Allgemeinen auf einer sehr detaillierten Ebene (für Bauteile oder Unterbaugruppen) und deshalb meistens während oder nach der Detailplanung durchgeführt.

Die FMEA bedarf äußerst zeitaufwendiger Detailarbeit und muss vollständig dokumentiert sein, um eine klares und richtig interpretierbares Ergebnis zu erhalten.

5.4.1 Das FMEA-Verfahren

Das Verfahren enthält dabei folgende Schritte:

1. Systemdefinition / Strukturanalyse:

Das System besteht aus einzelnen Systemelementen, die zur Beschreibung und Gliederung des Konzeptes dienen. Die Systemstruktur ordnet vom Produkt als oberster Ebene ausgehend die einzelnen Systemelemente auf unterschiedlichen hierarchischen Ebenen an. Das zu untersuchende System, die funktionalen Zu-

sammenhänge der Bauteile in diesem System und die Ebene, auf der die Analyse durchgeführt werden soll, müssen definiert werden.

2. Fehlermöglichkeiten analysieren:

Alle potentiellen Fehlermöglichkeiten, die auf der niedrigsten in Schritt 1 definierten Ebene des Systems existieren, müssen identifiziert werden. Man geht die Funktionsanalyse durch und benennt mögliche Abweichungen von den spezifizierten Funktionen. Dies geschieht zunächst nach Art eines „Brainstormings“. Eine Bewertung der möglichen Fehler erfolgt in späteren Schritten. Mögliche Abweichungen von den spezifizierten Funktionen sind:

- Die Funktion ist nicht vorhanden oder fällt total aus.
- Ein Funktionsmerkmal liegt außerhalb der spezifizierten Toleranz.
- Die Funktion ist nicht unter allen spezifizierten Bedingungen vorhanden. Bedingungen können Temperatur, Druck, Feuchte, Schock, Verschmutzungsgrad, Vibration, Netzqualität, elektromagnetische Verträglichkeit (EMV), sein.

3. Effektanalyse:

Die Auswirkung eines jeden Fehlers auf die direkte Funktion der Baugruppe und jede höhere Baugruppenebene sowie die Funktion der gesamten Anlage müssen bestimmt werden. Dieser Schritt kann auch die Auswirkungen auf Bedienpersonal enthalten.

4. Schadenminimierung (optional):

Dieser Punkt enthält die direkte Reaktion eines Bedieners, um das Ausmaß des Schadens zu minimieren oder, um die Möglichkeit wieder herzustellen, korrigierend eingreifen zu können. Dazu gehören auch alle notwendigen Wartungsaktivitäten, um den Fehler zu beheben. Die in diesem Punkt gesammelten Daten können auch als Basis für ein späteres sicherheitsgerichtetes Wartungsprogramm verwendet werden.

5. Fehlerwahrscheinlichkeit quantifizieren (optional):

Wenn ausreichend Daten vorliegen, sollte die Auftrittswahrscheinlichkeit und Fehlerfrequenz einer Fehlerart bestimmt werden.

6. Analyse der Gefährlichkeit:

Aus der Wahrscheinlichkeit des Auftretens eines Fehlers und dem Effekt eines Fehlers kann seine Gefährlichkeit bestimmt werden. Die Analyse der Gefährlichkeit kann quantitativ oder qualitativ sein. Bei einer quantitativen Bewertung kann die sog. Risikoprioritätszahl (*RPZ*) aus

$$RPZ = B \times A \times E$$

berechnet werden, wobei B die Bedeutung, A die Auftrittswahrscheinlichkeit und E die Entdeckungswahrscheinlichkeit eines Fehlers darstellen. Eine Möglichkeit zur Bestimmung der Faktoren für eine quantitative Bewertung ist in Tabelle 5-4 gegeben.

7. Systemoptimierungsvorschläge:

Im Zuge der FMEA können jeweils Änderungen am System und am Verfahren entworfen werden, um die Auswirkungen oder die Wahrscheinlichkeit eines Fehlers zu verringern.

Die FMEA wird gewöhnlich mit Formularen durchgeführt, die verschiedene Spalten für jeden oben beschriebenen Punkt 1 bis 7 besitzen. Wie das Formular auszusehen hat und welche Punkte aufgenommen werden, hängt von der zu untersuchenden Maschine ab.

5.4.2 Nutzen und Grenzen der FMEA

Die wichtigsten Vorteile der FMEA bestehen in einem klaren Zusammenhang zwischen möglichen Fehlern und Fehlfunktionen des Systems sowie einer eindeutigen Ursache-Wirkungs-Kette. Weitere Vorteile sind unter anderem das erleichterte Auffinden wichtiger Fehler und die Möglichkeit, die Ergebnisse übersichtlich und kompakt darzustellen.

Die Durchführung einer FMEA ist normalerweise durch die Zeit, die verfügbaren Ressourcen und das Vorhandensein einer ausreichend detaillierten Datenbasis während der Analyse, wie z.B. einer genauen Systemdefinition, aktueller Zeichnungen, Ausfallraten usw., eingeschränkt. Um ein aussagekräftiges Ergebnis zu erhalten, sollte sich die FMEA auf die kritischen Teile konzentrieren, die durch frühere Analysen oder durch andere Kriterien, wie Sicherheit, Kosten, Komplexität, schwieriger Zugang zu Wartungszwecken usw., ermittelt wurden. Die FMEA wird oft entweder als Eingabe für eine quantifizierte Risikoanalyse (z.B. Fehlerbaumanalyse FTA) oder als Teil eines sicherheitsgerichteten Wartungsprogramms (Reliability Centered Maintenance RCM) benutzt.

Nachteilig bei der FMEA sind der große Aufwand bei komplexen Systemen und die erschwerte Durchführbarkeit bei Systemen mit redundanten Komponenten. Eine Beschränkung auf kritische Teile zur Reduktion des Aufwandes ist nur dann sinnvoll, wenn die kritischen Teile auch bekannt sind. Bei vollkommen neuartigen Systemen sind allerdings die kritischen Teile unbekannt, weshalb eine Reduktion auf angeblich kritische Teile immer mit dem Risiko verbunden ist, tatsächlich kritische Teile zu übersehen. Genauso lässt sich die Frage, auf welcher Systemebene die FMEA durchgeführt wird, nicht immer eindeutig beantworten, da bei einer zu groben Analyse auf

Be- wer- tung	Bedeutung (B)	Auftritts- wahr- schein- lichkeit (A)		Entdeckungs- wahr- schein- lichkeit (E)	
		Beschreibung	p(A)	Beschreibung	p(E)
10	Gefährdung, Verstoß gegen Gesetze	Fehler nahezu sicher; zahlrei- che Fehler mit gleichen oder ähnlichen Kon- struktionen bekannt	$> 0,316$	Keine Ent- deckungsmaß- nahmen be- kannt oder geplant	$< 90\%$
9	Gefährdung, Verstoß ge- gen Gesetze möglich	Sehr große Zahl von Fehlern wahrscheinlich	$0,316$	Entdeckung möglich aber unsicher	90%
8	Totaler Funk- tionsausfall, Kunde sehr verärgert	Große Zahl von Fehlern wahrscheinlich	$0,134$	Sehr geringe Wahr- schein- lichkeit einer Entdeckung	
7	Funktionen stark einge- schränkt, Kun- de verärgert	Mäßig große Zahl von Feh- lern wahr- scheinlich	$0,046$	Geringe Wahr- scheinlichkeit einer Ent- deckung	98%
6	Ausfall einzel- ner Hauptfunk- tionen, Kun- de, ziemlich verärgert	Mittlere Zahl von Fehlern wahrscheinlich	$0,012$	Nahezu mittlere Wahr- schein- lichkeit der Entdeckung	
5	Mäßige Ein- schränkung des Gebrauchsnut- zens, Kunde etwas verärgert	Gelegentliche Fehler wahr- scheinlich	$0,003$	Mittlere Wahr- scheinlich- keit der Ent- deckung	
4	Gebrauchs- nutzen wenig eingeschränkt, Kunde verdros- sen	Wenige Fehler wahrscheinlich	$0,0005$	Mäßig hohe Wahr- schein- lichkeit der Entdeckung	$99,7\%$
3	Gebrauchs- nutzen ge- ringfügig ein- geschränkt, Kunde leicht verdrossen	Sehr wenige Fehler wahr- scheinlich	$6,3 \cdot 10^{-5}$	Hohe Wahr- scheinlich- keit der Ent- deckung	
2	Auswirkung sehr gering, Kunde kaum berührt	Fehler selten	$6,8 \cdot 10^{-6}$	Sehr hohe Wahr- schein- lichkeit der Entdeckung	$99,9\%$
1	Kunde bemerkt Auswirkungen nicht	Fehler unwahr- scheinlich, ähn- liche Konstruk- tionen bisher ohne Fehler.	$< 5,8 \cdot 10^{-7}$	Nahezu sichere Entdeckung	$99,99\%$

Tabelle 5-4: Faktoren zur Berechnung der RPZ

einer sehr hohen Ebene wichtige Gefahrenquellen übersehen werden können und bei einer zu feinen Analyse der Aufwand den Nutzen übersteigt.

5.5 Fehlerbaumanalyse

Die *Fehlerbaumanalyse* (Fault Tree Analysis, FTA) wurde im Jahr 1961 von Watson von den Bell Telephone Laboratories entwickelt [27].

Diese ist ein deduktives Verfahren, deren Ziel das Erkennen von Gefahren ist und bei dem alle kritischen Pfade, die zum unerwünschten Ereignis führen, herausgefunden werden. Eine wichtige Voraussetzung für die Anwendung dieser Methode ist die genaue Kenntnis des Systems und seiner möglichen Einzelausfallursachen. Durch das Abschätzen von Fehlerwahrscheinlichkeiten und die Verwendung geeigneter logischer Ausdrücke erlaubt die Analyse Berechnungen über die Zuverlässigkeit und die Wahrscheinlichkeit des Eintritts einer gefährlichen Situation. Die Wirkung von Schutzmaßnahmen kann mit diesem Verfahren schnell überschaut werden. Durch ihren deduktiven Charakter ist die Methode gut zur Bestimmung von Unfallursachen geeignet [28]. Die Methode wird in der Norm IEC 1025 beschrieben. Das Ergebnis wird in Form eines Fehlerbaumes dargestellt.

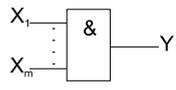
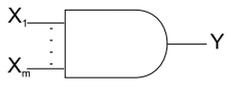
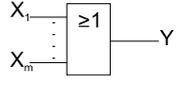
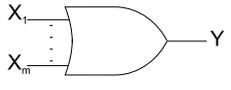
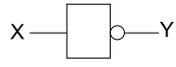
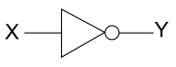
Verknüpfung	Bedeutung	DIN(IEC)	USA (DoD)
Konjunktion (UND)	$Y = X_1 \wedge X_2 \wedge \dots \wedge X_m$ $= X_1 X_2 \dots X_m$		
Disjunktion (ODER)	$Y = X_1 \vee X_2 \vee \dots \vee X_m$		
Negation (NICHT)	$Y = \bar{X} = 1 - X$		

Abb. 5-3: Fehlerbaumsymbole

Ein Fehlerbaum eines technischen Systems zeigt an, in welchen Kombinationen Komponentenfehler den Systemfehler bewirken können. Genauer gesagt, können diverse Kombinationen von $X_1 = 1, X_2 = 1, \dots, X_n = 1$ bewirken, dass $X_S = 1$, wobei X_S von $X_S = \varphi(X_1, \dots, X_n)$ die Ausgangsgröße des Fehlerbaumes ist. Dabei ist zu beachten, dass ein und dieselbe Komponente verschiedene Fehler haben kann. Normalerweise schließen sich diese jedoch aus.

Zur Darstellung eines Fehlerbaumes haben sich die Schaltgattersymbole nach DIN bzw. nach internationalem Standard durchgesetzt. Gatter sind Schaltelemente für die Grundverknüpfungen der Booleschen Algebra. Zu ein und derselben Fehlerbaumfunktion φ kann es verschiedene Darstellungsformen und demgemäß nach Abbildung 5-3 verschiedene gleichwertige Fehlerbäume geben.

Aus der Booleschen Funktion des Fehlerbaumes können nach Schneeweiss [29] in einem weiteren Schritt die

- Systemverfügbarkeit
- mittlere System-Ausfallhäufigkeit und verwandte Größen sowie die
- mittlere System-Lebensdauer

bestimmt werden, sofern die Einzelverfügbarkeiten oder Einzellebensdauern der Systemkomponenten bekannt sind oder sich sinnvoll abschätzen lassen.

5.6 Weitere Methoden

Neben den oben genannten Methoden zur Sicherheitsanalyse gibt es noch weitere Verfahren, Systeme sicherheitstechnisch zu bewerten. Im folgenden Abschnitt werden zu den in Anhang B der DIN 1050 genannten Methoden zur Gefahrenanalyse und noch weitere erläutert. Teilweise sind diese jedoch nur Varianten oder Kombinationen der oben genannten Grundformen oder greifen direkt auf diese zurück.

Checklistenmethoden

Zu den Checklistenmethoden gehören die sog. „*W-Methoden*“ und die „*Kreativen Checklisten*“. Mit ihnen kann man sich einen groben Überblick über Gefährdungspotentiale, die in einer Anlage offen oder verborgen vorhanden sind, verschaffen. Die „*W-Methode*“ ist ein Verfahren zur Grobeinteilung eines technischen Systems in Gefährdungsbereiche unterschiedlicher Qualität. Unter Anwendung von mit dem Buchstaben „W“ beginnenden Frageworten (wie, wer, was, ... usw.) sollen Gefahrenpunkte aufgezeigt werden [28]. Die *Checklistenmethode* arbeitet ähnlich wie die schon oben beschriebene *Vorläufige Gefahrenanalyse*, die einen groben Überblick ermöglicht. Sie ist nur für die Vorplanungsphase eines Projektes geeignet.

PAAG-Verfahren

Das *PAAG-Verfahren* (*Prüfen, Auffinden, Auswirkungen und Gegenmaßnahmen*) gehört, zu den Verfahren, die einerseits mit sehr viel Systematik, andererseits aber auch mit einem großen Aufwand an kreativem und phantasievollen Denken Probleme sehr gründlich erfassen und lösen helfen. Die grundlegende Philosophie, die hinter dem *PAAG-Verfahren* steht, ist, dass hypothetische Störungen durch Verwendung bestimmter Leitworte in einem technischen System erzeugt werden, nach realen

Ursachen hierfür gesucht wird und im positiven Fall durch Gegenmaßnahmen Abhilfe geschaffen wird, bevor in der Realität eine Situation entsteht, die Menschen und Maschinen gefährdet.

Das Verfahren besteht aus den Schritten:

1. Auswahl eines Anlagenteils
2. Definition der Sollfunktion
3. Erzeugung hypothetischer Störungen (Abweichung von der Sollfunktion)
4. Überprüfung ob diese Störung realisierbar ist
5. Abschätzung der Auswirkungen
6. Auffinden von Gegenmaßnahmen
7. Dokumentation und Aufarbeitung

Die erforderlichen Leitworte mit ihrer Bedeutung sind der Tabelle 5-5 zu entnehmen.

Leitworte	Bedeutungen	Kommentare
NEIN oder NICHT (KEIN oder KEINE)	Die völlige Verneinung dieser Funktion	Kein Teil der Funktionen wird ausgeübt, aber es geschieht auch nichts anderes.
MEHR WENIGER	Quantitativer Zuwachs oder Quantitative Abnahme	Das bezieht sich auf Mengen und Eigenschaften, wie Mengenströme und Temperaturen, aber auch auf Funktionen, wie erwärmen und reagieren.
SOWOHL ALS AUCH TEILWEISE (ZUM TEIL)	Ein qualitativer Zuwachs Eine qualitative Abnahme	Alle vorgegebenen Funktionen und Betriebsvorgänge werden erreicht. Zusätzlich passiert jedoch auch etwas anderes. Nur einige Teile der Sollfunktion werden erreicht, manche nicht.
UMKEHRUNG	Das logische Gegenteil der Soll-Funktion	Das betrifft hauptsächlich Funktionen, z.B. entgegengesetztes Fließen oder entgegengesetzte chemische Reaktion
ANDERS ALS	völliger Austausch	Es wird nicht eine einzige der ursprünglich festgelegten Funktionen ausgeführt. Etwas völlig anderes geschieht.

Tabelle 5-5: Leitworte und deren Bedeutungen

Die Leitworte können dabei sowohl auf Funktionen, wie Reagieren, Befördern, Lagern, Regeln usw., als auch auf Zustände, wie Temperatur, Druck, Viskosität, angewendet werden.

Das *PAAG-Verfahren* ist auf alle Arten von Anlagen sowohl in der Planungsphase als auch bei schon bestehenden Anlagen, z.B. nach wesentlichen Abänderungen, anwendbar. Die ganze Anlage wird dabei Stück für Stück logisch untersucht, wobei nach Ansicht von erfahrenen Teamleitern mehr als 90% der möglichen Störungen

erkannt werden [28]. Nachteilig ist der große Zeitaufwand. Für jedes Bauteil oder jede Arbeitsanweisung werden nach Rindfleisch [28] bis zu 5 Minuten Überprüfungszeit im Team veranschlagt. Darüber hinaus sind auch die Vorbereitungszeiten und Nachbearbeitungszeiten sehr umfangreich.

Weiterhin wird in der Literatur die *Gefährdungs- und Maßnahmenanalyse* genannt. Diese sowie das *PAAG-Verfahren* sind der *Fehler Möglichkeits-Einflussanalyse* ähnlich, indem einzelne Komponenten auf ihren Ausfall hin untersucht werden. Allerdings sind deren Erfolgsaussichten nicht so groß, da deren Leitwortkataloge nicht sehr ausgefeilt sind [28].

MOSAR-Verfahren

Das *MOSAR-Verfahren* (Method Organized for a systematic Analysis of risks) ist ein vollständiges Verfahren in zehn Schritten. Das zu analysierende System (Maschine, Prozess, Einrichtung usw.) wird als eine Anzahl von wechselwirkenden Subsystemen angesehen. Es wird eine Tabelle benutzt, um die Gefährdungen, Gefährdungssituationen und Gefährdungsereignisse zu identifizieren.

Die Eignung der Schutzmaßnahmen wird mit Hilfe einer zweiten Tabelle untersucht, in einer dritten Tabelle wird ihre gegenseitige Abhängigkeit berücksichtigt.

Eine Untersuchung mit den bekannten Mitteln wie FMEA gibt die möglichen gefährlichen Ausfälle zu erkennen. Dies führt zur Ausarbeitung von Unfallszenarien. Die Szenarien sind in einer Tabelle, welche die Experten im gemeinsamen Konsens erstellt haben, nach dem Schadensausmaß sortiert. Eine weitere, ebenfalls im gemeinsamen Konsens erarbeitete Tabelle, verbindet das Schadensausmaß mit den Zielstellungen, die bei den Schutzmaßnahmen angestrebt werden, und legt die Leistungsebenen der technischen und organisatorischen Maßnahmen fest.

Die Schutzmaßnahmen werden dann in Logikbäume aufgenommen und die Restrisiken mit einer im gemeinsamen Konsens ausgearbeiteten Akzeptanztafel analysiert. Das *MOSAR-Verfahren* [28] dient mehr zu Bewertung von Gefahren und Schutzmaßnahmen. Das Erkennen von Gefahren wird durch die bereits oben beschriebenen Verfahren der FMEA vorgenommen. Weiterhin setzt die Anwendung dieser Methode eine große Detailkenntnis der zu untersuchenden Anlage voraus, da Gefahren bereits bekannt sein müssen.

Delphi-Methode

Die *Delphi-Methode* beruht auf der Befragung von Experten. Ein großer Expertenkreis wird in mehreren Schritten befragt, wobei das Ergebnis des vorhergehenden Schrittes zusammen mit zusätzlichen Informationen allen Teilnehmern übermittelt wird. In weiteren Schritten konzentriert sich die Befragung auf die Punkte, zu denen bisher keine Übereinstimmung erzielt wurde. Dieses Verfahren ist besonders effektiv,

weil ausschließlich Fachleute beteiligt sind [28]. Es gibt jedoch nur wenige Fachleute, die Experten für das Erkennen von Gefahren von automatischen Krananlagen im personenzugänglichen Umfeld sind. So kann das Verfahren bei der hier genannten Problemstellung höchstens zur Bewertung des Risikos eingesetzt werden, jedoch nicht zur detaillierten Gefahrenerkennung.

Fehlersimulation von Steuerungen

Eine *Fehlersimulation von Steuerungen* stellt hier kein vielversprechendes Verfahren dar, weil zu dem Zeitpunkt der Untersuchung eine konkrete Steuerung noch nicht existiert. Weiterhin ist jede Steuerung einer automatisierten Krananlage so spezifisch, dass eine Bewertung zu speziell für eine bestimmte Anlage wäre. Die hier gemachten Aussagen über die Sicherheit sollen jedoch Richtliniencharakter besitzen und somit allgemeinerer Natur sein.

Nohl und Thiemecke [30], [31] schlagen eine *Systematik zur Durchführung von Gefährdungsanalysen* vor. In diesem Verfahren werden die Arbeitsabläufe in Teilvorgänge unterteilt. Diese überschaubaren Teilvorgänge können dann wiederum auf ihre Sicherheit hin untersucht werden, indem bewusst der Arbeitsvorgang falsch ausgeführt wird. Abschließend werden die Auswirkungen des Fehlverhaltens untersucht. So hat man mit diesem Verfahren die Möglichkeit, menschliches Fehlverhalten zu berücksichtigen.

Hoyos und Ruppert [32] haben einen *Fragebogen zur Sicherheitsdiagnose (FSD)* erarbeitet. Dieser Fragebogen beschreibt ein verhaltensorientiertes Verfahren für die betriebliche Sicherheitsarbeit. Die Methode zur Gefahrenerkennung basiert auf einer Liste möglicher schädlicher Energiearten. Diese Liste ist nur sehr oberflächlich gehalten. Das Verfahren ist wie die Checklistenmethoden nicht vollständig.

Schmidt [33] hat das *Umweltenkonzept* entwickelt, das ausschließlich für das Erkennen von Gefahren geeignet ist. Es sieht vor, das sich u.U. erst geplante oder im Entwurfsstadium befindende System, Teilsystem oder Element in eine lückenlose, geschlossene Hierarchie von Umwelten einzubetten. Die Systemgrenzen sind räumlich geschlossen. Das Systemverhalten und somit auch die daraus resultierenden Gefährdungen können über die Schnittstellen verfolgt werden. So lassen sich Gefahren erkennen, die weder aus dem Arbeitsablauf bedingt sind, noch aus dem Versagen eines Bauteiles entstehen.

Tabelle 5-6 enthält eine Zusammenfassung der gängigen Methoden für eine Sicherheitsanalyse, wobei darüber hinaus eine Bewertung hinsichtlich ihrer Eignung für automatisierte Krananlagen vorgenommen wird.

	Phase	Mensch/ Maschine	Aufwand	Erfolgs- aussichten	Bemerkung
Vorläufige GA	Vorprojekt Planung	nein	gering	gering	nicht vollständig
W-Methoden	Vorprojekt Planung	ja	gering	informativ	nicht vollständig
Kreative Checklisten	Vorprojekt Planung	nein	gering	gering	nicht vollständig
Fehlerbaumanalyse -zustandsanalyse	Planung Betrieb	ja	groß	detailliert	Berechnungen möglich Wirkung von Schutz erkennbar
PAAG-Verfahren	Planung Betrieb	nein	groß	detailliert	Auswahl Anlagenteil Prüfung auf Ausfall
Gefährdungs- maßnahmenanalyse	Planung Betrieb	nein	groß	gut	wie PAAG
Ausfalleffektanalyse FMEA	Planung Betrieb	nein	groß	informativ	Komponentenbetrachtung wie PAAG
Verfahren von Nohl und Thiemecke	Planung Betrieb	ja	groß	gut	Betrachtung von Arbeitsabläu- fen, dabei Fehlerbetrachtung
MOSAR-Verfahren	Planung Betrieb	ja	groß	k.A.	weniger Erkennen mehr Bewerten, keine Literatur
Fragebogen zur Sicherheitsdiagnose	Betrieb	ja	groß	k.A.	Nicht möglich, da an Anlage noch nicht gearbeitet wurde
Delphi-Methode	Planung Betrieb	ja	groß	k.A.	mehr zur Bewertung des Risikos
Fehlersimulation für Steuerungen	Planung Betrieb	nein	groß	k.A.	Experimente an der Anlage

Tabelle 5-6: Gängige Methoden zur Sicherheitsanalyse

5.7 Menschliches Versagen

Unfälle in komplexen, risikoreichen Systemen, wie chemischen Produktionsanlagen und Kernkraftwerken oder in der Raum-, Luft- und Schifffahrt, lassen sich selten auf eine einzelne Ursache zurückführen. Vielmehr sind sie meist nur durch das Zusammenwirken menschlicher, technischer, organisatorischer und umweltbezogener Faktoren zu erklären. Betrachtet man Unfälle als Ereignisketten, steht am Ende fast immer der Mensch, sei es als Operator in der Schaltwarte, als Kapitän auf der Brücke oder als Pilot im Cockpit. Wirken sich Fehler bis zu diesem letzten Glied der Kette aus, gibt es nur noch das Entweder-Oder: Handelt der Mensch im entscheidenden Moment falsch, wird die Unfallursache als menschliches Versagen bezeichnet. Gelingt es ihm aber die Auswirkungen des Fehlers gleichsam im letzten Moment zu verhindern, so hat „das System“ funktioniert. Der folgende Abschnitt versucht vor diesem Hintergrund den Stellenwert des so genannten „Human Factor“ näher auszuleuchten und die Rolle des Menschen im Zusammenwirken mit Technik, Organisation und Umwelt zu erklären.

5.7.1 Quantifizierung

Menschliches Versagen kann niemals vollständig ausgeschlossen werden. Um das Risiko des menschlichen Versagens quantifizieren zu können, wurde darüber viel geforscht. Dabei haben sich bis zu 38 Faktoren in fünf verschiedenen Wahrnehmungsebenen er-

geben, die berücksichtigt werden müssen, wenn der Mensch als Fehlerquelle in einer quantitativen Sicherheitsanalyse berücksichtigt werden soll. Verschiedene Methoden, die das Risiko menschlichen Versagens quantifizieren, finden sich bei Humphries [34]. Die dort beschriebenen Methoden stammen ursprünglich aus dem Bereich der Nukleartechnik, allerdings sind diese auch hilfreich, um das Risiko beim Betrieb von anderen Anlagen abzuschätzen. Ein Nachteil dieser Methoden besteht jedoch in der Notwendigkeit, die Nutzer der zu untersuchenden Anlage detailliert zu kennen.

Als Einführung in das Thema der Quantifizierung des Risikos menschlichen Versagens soll hier eine einfache Methode genügen, zumal in der vorliegenden Arbeit keine spezielle Anlage untersucht werden soll, sondern nur der Einfluss des Menschen im allgemeinen berücksichtigt wird. Diese Methode wurde von Bello und Columbori [35] entwickelt und ist unter dem Namen TESEO (Tecnica Empirica Stima Errori Operatori) in der Fachwelt bekannt. TESEO ist eine Methode, die nur fünf statt der 38 Faktoren berücksichtigt und deshalb als nicht so aussagekräftig erachtet wird. Für allgemeine Abschätzungen sollte diese jedoch genügen.

Nach der TESEO- Methode kann das Risiko menschlichen Versagens auf folgende Weise berechnet werden:

$$P = K1 \times K2 \times K3 \times K4 \times K5$$

Wobei die Faktoren $K1$ bis $K5$ (Tabelle 5-5) definiert sind als:

$K1$ Aktivitätsfaktor; Art der Betätigung,

$K2$ Temporärer Stressfaktor,

$K3$ Qualifikation des Bedieners,

$K4$ Angstfaktor,

$K5$ Ergonomiefaktor.

In Tabelle 5-7 werden die TESEO-Fehlerwahrscheinlichkeitsfaktoren erläutert:

Das Ergebnis dieser Berechnung ist eine Wahrscheinlichkeit, die einen Unfall pro einer Anzahl Arbeitsvorgänge quantifiziert.

5.8 Das SHEL-Modell

Die Suche nach den Faktoren, die einen Unfall verursacht haben, ist oft schwierig: Häufig sind diese Faktoren versteckt und nur schwer auszumachen, andere dagegen erscheinen als Ursache fast allzu plausibel. Doch gerade bei diesen „menschlichen Faktoren“ handelt es sich oft nur um Symptome einer tieferliegenden Ursache. Vor dem Hintergrund dieser Erkenntnis ist es daher zwingend, für die Analyse von Unfällen (Accidents) und Beinahe-Unfällen (Incidents) einen Ansatz zu wählen, der nicht nur die Geschehnisse an der Oberfläche, sondern auch die darunter liegenden versteckten Faktoren berücksichtigt.

Aktivitätsfaktor	K1
einfache Routine	0,001
braucht etwas Aufmerksamkeit, aber Routine	0,01
nicht Routine	0,1
Temporärer Stressfaktor für Routinearbeiten	K2
verfügbare Zeit in Sekunden: 2	10
10	1
15	0,5
Temporärer Stressfaktor für Nicht-Routinearbeiten	K2
verfügbare Zeit in Sekunden: 3	10
30	1
45	0,3
60	0,1
Qualifikation des Bedieners	K3
sorgfältig ausgewählt sehr gut ausgebildet	0,5
durchschnittliches Wissen und Ausbildung	1
wenig Wissen und Training	3
Angstfaktor	K4
schwerer Notfall	3
potentieller Notfall	2
normale Situation	1
Ergonomiefaktor	K5
beste Arbeitsbedingungen und gut gestaltete Schnittstelle	0,7
gute Arbeitsbedingungen und gut gestaltete Schnittstelle	1
akzeptierbare Arbeitsbedingungen und gut gestaltete Schnittstelle	3
akzeptierbare Arbeitsbedingungen und schlecht gestaltete Schnittstelle	7
schlechte Arbeitsbedingungen und schlecht gestaltete Schnittstelle	10

Tabelle 5-7: TESEO-Faktoren

Zur Untersuchung der Bedeutung des „Human Factor“ ist in der Wissenschaft seit 1972 das Modell von Edwards [36] verbreitet. Es zeigt die Beziehungen, also die Schnittstellen zwischen dem Menschen und verschiedenen Systemkomponenten in ihrem Umfeld. Die physischen Eigenschaften des Systems – wie Ausrüstung und Material – bildet die Hardware. Regeln, Gesetze, Verordnungen, Standard Operating Procedures etc. werden als Software bezeichnet. Sie legt die Prozesse und Abläufe fest und zeigt die Kommunikationswege innerhalb des Systems auf. Der Mensch oder die Crew, die mit der Hard- und Software umzugehen haben, bilden die Lifeware. Die Ressourcen Hard-, Soft- und Lifeware sind dabei immer im Kontext eines Umfelds (Environment) zu sehen, das sich aus physischen, ökonomischen, politischen und sozialen Faktoren zusammensetzt. Mit Hilfe des SHEL-Modells lässt sich die Human

Factor-Forschung auch als Disziplin beschreiben, die auf dem Studium der Lifeware-Komponente basiert und sich mit Design und Management aller in Abbildung 5-4 dargestellten Schnittstellen

- Lifeware / Software,
- Lifeware / Hardware,
- Lifeware / Environment sowie
- Lifeware / Lifeware

befasst. Bei diesem Modell können organisatorische Aspekte nur schwierig und nicht eindeutig zugeordnet werden, was ein Nachteil ist.

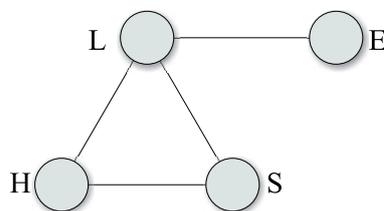


Abb. 5-4: Das SHEL Modell

Für die Analyse möglichen menschlichen Versagens können weiterhin die folgenden Ergebnisse der Human Factor-Forschung berücksichtigt werden [37]:

Die Technologien, die in komplexen Arbeitssystemen zur Anwendung kommen, haben sich in den letzten Jahren rasant weiterentwickelt, und es ist kein Ende dieser Entwicklung abzusehen. Dabei drängt die fortschreitende Automatisierung den Menschen immer mehr in die Rolle des Systemüberwachers, da Steuerungs- und Regelfunktionen zunehmend von der Technik übernommen werden.

Dabei stellt sich jedoch die Frage, ob es klug ist, den Menschen als wesentlichen Risikofaktor als letztes Ziel der Automatisierung aus solchen Systemen zu entfernen. Die Statistik gibt darauf keine Antwort, denn sie berücksichtigt nur Unfälle und Katastrophen, bei denen menschliches Fehlverhalten als Ursache eine bedeutende Rolle gespielt hat, nicht jedoch jene Unfälle und Katastrophen, die durch richtiges menschliches Handeln verhindert werden konnten.

Es gibt menschliche Fähigkeiten, die denen der Technik überlegen sind — wie zum Beispiel Prädiktion (Vorhersage) und Antizipation (Vorwegnahme einer Entwicklung), Flexibilität im Denken oder Entscheiden in unvollständig definierten Situationen. Trotzdem wird seine Stellung im komplexen Arbeitssystem zunehmend geschwächt. Die neu definierte Arbeitsaufteilung zwischen Mensch und Technik hat zu einer neuen Generation menschlichen Fehlverhaltens geführt: Bei Menschen, die in hochautomatisierten Systemen Überwachungsfunktionen ausüben, lässt sich ein

Nachlassen ihrer Fähigkeit feststellen, Systemfehler zu entdecken und manuelle Bedienungsaufgaben auszuführen. Diese Schwäche lässt sich auf zwei Phänomene zurückführen, die jede Automatisierung begleiten, nämlich zum einen die Rückbildung manueller Fähigkeiten und zum anderen den Verlust der „situation awareness“.

Die Rückbildung manueller Fähigkeiten ergibt sich, wenn sie nicht mehr oder nur noch selten gebraucht werden. Studien belegen, dass Personen, die ein automatisiertes System nur überwachen, im Vergleich zu jenen, die ein System manuell bedienen, langsamer und ineffizienter sind, wenn sie das System nach einer Störung wieder unter Kontrolle bringen müssen. Dies ist auch der Fall, wenn es sich um ehemals erfahrene und geübte Systembediener handelt. Die Folge ist, dass der Bediener im Fall einer Störsituation die erforderlichen Fertigkeiten für die manuelle Übernahme nicht besitzt und die Belastung für ihn in solchen Situationen deshalb noch höher wird.

Eine wichtige Voraussetzung für die Bewältigung eines Störfalls ist, den Überblick über die aktuelle Situation zu bewahren. „Situation awareness“ umfasst die ständige und fortlaufende Wahrnehmung relevanter Zustandsvariablen eines Systems, das Verständnis der Bedeutung des aktuellen Systemzustandes in Bezug auf das Ziel des Operators sowie, basierend auf diesem Verständnis, die Projektion künftiger Trends und Ereignisse auf das System. An Beispielen von Flugunfällen in den letzten Jahren wird ersichtlich, dass der Verlust der „situation awareness“ in vielen Fällen eine wesentliche Rolle spielte. Dabei ist gerade auch das Einschätzen der für das richtige Reagieren zur Verfügung stehenden Zeit ein wichtiger Faktor, der in der Störsituation aber oft vergessen wird. Einer der Gründe, weshalb es gerade in technisierten Systemen häufig zum Verlust der „situation awareness“ kommt, liegt darin, dass bei vorwiegender Überwachungstätigkeit der Aufmerksamkeitsgrad ab-, die „complacency“ dagegen zunimmt. „Complacency“ wird in diesem Fall mit Bequemlichkeit, Gleichgültigkeit oder Selbstzufriedenheit übersetzt. Diese Erscheinung ist eng gekoppelt mit zu großem Vertrauen in die Automation. Diese „Complacency“ wird durch ein übermäßiges Vertrauen in die Automation noch verstärkt. Zudem wurde der Mensch im Zuge der Automation vom „aktiven Prozessor“ zum „passiven Informationsempfänger“ degradiert, was seiner Aufmerksamkeit ebenfalls abträglich ist. Neben dem Verlust manueller Fähigkeit sind organisatorische Einflüsse von großer Bedeutung. Die Auswirkungen solcher Einflüsse lassen sich am einfachsten mit einem Beispiel aus einer verfahrenstechnischen Anlage erläutern.

Im Prozessleitstand einer petrochemischen Anlage wird mitten in der Nacht der einzige Bediener durch Warnsignale auf eine Störung aufmerksam gemacht. Im Laufe der nächsten Stunden versucht er, vergeblich den Prozess durch manuelle Korrekturen wieder ins Lot zu bringen. Schließlich überhitzt sich ein Reaktor und explodiert. Aus

Sicht des Managements ist das Verhalten des Bediener unverständlich, ist doch nach Betriebsvorschrift in einem solchen Störfall entweder sofort der Prozessverantwortliche herbeizurufen oder die Anlage notfallmäßig abzuschalten. In seiner Beurteilung berücksichtigte das Management jedoch nicht, dass der pflichtbewusste Bediener unter dem Druck der kürzlich verordneten Vorgaben zur allgemeinen Kostensenkung und Steigerung des Profits nur das Ziel im Auge hatte, die Anlage um jeden Preis laufen zu lassen, um letztlich seinen Arbeitsplatz nicht zu verlieren.

5.9 Sicherheitsanalyse automatisierter Krane

Für die Durchführung einer Sicherheitsanalyse für automatische Krananlagen im personenzugänglichen Umfeld müssen aus den oben beschriebenen Methoden zur Sicherheitsanalyse die relevanten Methoden zusammengestellt werden.

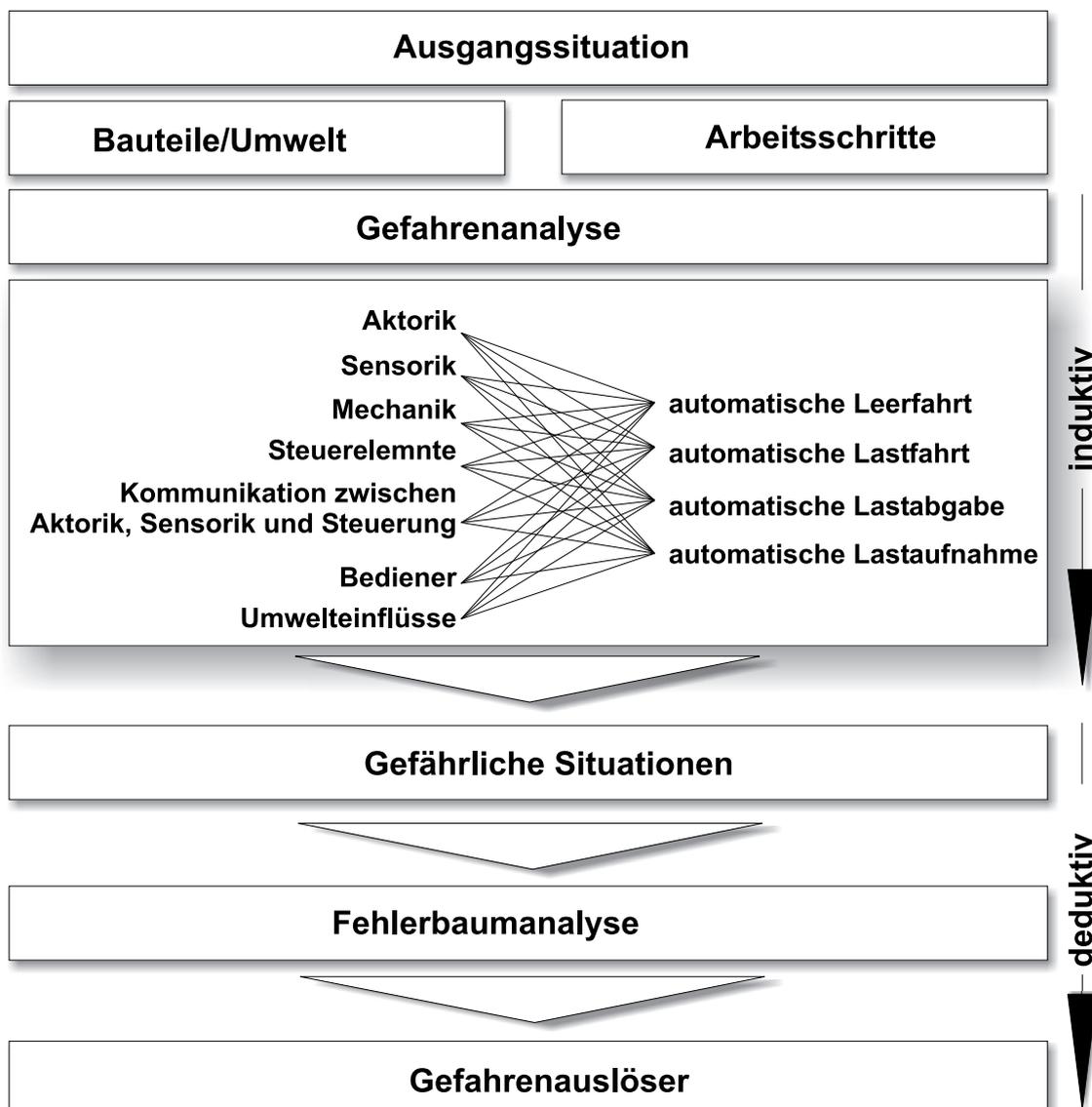


Abb. 5-5: Methode der Gefahrenermittlung

Dafür müssen einerseits die Anlagenkomponenten, die Bedienung und somit die Mensch-Maschine-Schnittstelle sowie die Einordnung der Anlage in ihre Umgebung betrachtet werden. So hat man die drei Gesichtspunkte Mensch, Maschine und Umwelt berücksichtigt. Abbildung 5-5 beschreibt graphisch die Vorgehensweise zur Gefahrenermittlung.

Zur sicherheitstechnischen Beurteilung der Anlagenkomponenten erweist sich eine vorläufige Gefahrenanalyse (siehe Abschnitt 5.3) oder das *PAAG-Verfahren* (siehe Abschnitt 5.6) als besonders vielversprechend, weil es die größten Erfolgsaussichten besitzt. Nach Expertenmeinung sollen auf diese Weise bis zu 90% aller Gefährdungen so aufgedeckt werden [28]. Es sollen, wie es PHA und viele ähnliche Methoden vorschlagen, Anlagenteile ausgewählt und durch eine hypothetische Störung dieser Teile auf ihre Gefahren hin untersucht werden. Die Auswahl der Anlagenteile soll dabei einem systematischen Muster folgen, indem zwischen Aktorik, Sensorik und Mechanik unterschieden wird.

Unter Aktorik fallen zunächst alle aktiven Bauteile wie Antriebe des Kranes, des Hubwerkes und des Lastaufnahmemittels.



Abb. 5-6: Durchführung der Gefahrenermittlung

Das Anlagenverhalten wird jeweils, wie in Abbildung 5-6 verdeutlicht, bei der

- richtigen Funktion,
- bei nicht vorhandener Funktion und

- falscher Funktion

des Aktors oder Bauteiles hinsichtlich Gefahren betrachtet. Unter der Sensorik wird zunächst nur das Wegmesssystem betrachtet. Von der Betrachtung einer weiteren Sensorik für Sicherungsmaßnahmen wird hier abgesehen, da dies schon zu einer speziellen Ausführungsform einer Krananlage gehören würde. In der Untersuchung folgen die mechanischen Bauteile, wie Katze, Zugmittel, ... usw. (siehe Anhang B). Zuletzt werden Steuerelemente und die Kommunikation zwischen Aktorik, Sensorik und Steuerung betrachtet.

Zur Untersuchung des menschlichen Einflusses auf die Sicherheit im Anlagenbetrieb zeigt sich die *Systematik zur Durchführung von Sicherheitsanalysen* von Nohl und Thiemecke als vielversprechender Ansatz [30], [31]. Wie in diesem Verfahren vorgeschlagen, werden die Arbeitsabläufe der Anlagenbedienung betrachtet. Bei jedem Arbeitsschritt kann ein absichtliches Fehlverhalten angenommen werden, das dann auf seine Gefahren hin untersucht wird. Bei der Einteilung in Arbeitsabläufe hat es sich als vorteilhaft herausgestellt, den verschiedenen Automatisierungsgraden der Anlage zu folgen. Die Bedienung wird hinsichtlich einer

- richtigen Bedienung,
- keiner Bedienung,
- fehlerhaften Bedienung,
- zu frühen Bedienung und einer
- zu späten Bedienung

untersucht.

Den umweltbezogenen dritten Aspekt liefert das *Umweltenverfahren* von Schmidt [33]. Mit dieser Methode können noch Gefahren, die nicht unmittelbar dem Ausfall eines Anlagenteils oder dem Fehlverhalten eines Bedieners zuzuordnen sind, gefunden werden. Dabei werden thermische, mechanische, elektromagnetische und akustische Einflüsse untersucht. Zu den Umwelteinflüssen wird hier auch ein Energieausfall gezählt.

Aufgrund der Komplexität einer automatischen Krananlage ist es nicht ausreichend, nur eine induktive Gefahrenanalyse durchzuführen. Wie schon oben dargestellt, dienen die Ergebnisse einer vorläufigen Gefahrenanalyse und ihren verwandten Verfahren als Dateneingabe für deduktive Sicherheitsanalyseverfahren. Zur Vervollständigung der Gefahrenanalyse bietet es sich daher an, die Sicherheitsanalyse mit einer Fehlerbaumanalyse zu vervollständigen. So wird die Anlage mit einem induktiven und deduktiven Ansatz untersucht.

Zusammenfassend kann gesagt werden, dass mit der oben beschriebenen Methode durch einen induktiven Ansatz die Anlagenteile und der Einfluss des Menschen für

jeden Arbeitsschritt einzeln betrachtet werden. Durch das *Umweltenverfahren* findet eine Einordnung in die Umgebung der Anlage statt. Mit dem deduktiven Ansatz der Fehlerbaumanalyse wird die Methode vervollständigt.

Die Prüfliste für die einzelnen Arbeitsschritte ist in Anhang B angeführt.

6 Gefährdungen

In den vorhergehenden Abschnitten wurden die verschiedenen Methoden zur Sicherheitsanalyse erläutert. Aufbauend darauf werden in diesem Kapitel die Ergebnisse der Sicherheitsanalyse dargestellt. Dazu werden zunächst allgemeine Gefahren, wie sie immer vorhanden sind und in der Literatur allgemein beschrieben werden, aufgezeigt. Anschließend werden die Ergebnisse der speziell für automatisierte Krananlagen entwickelten Sicherheitsanalyse erläutert.

6.1 Gefahren durch äußere Umstände

Allgemeine Gefahren für Personen, die aus äußeren Umständen resultieren, können auf folgende Art eingeteilt werden [38]:

- Physikalische Gefahren,
- Gefahr durch Vibration,
- Gefahr durch Eingeschlossensein,
- Gefahr durch Betreten,
- Gefahr durch Wartungsarbeiten,
- Gefahr durch unvollständige Arbeit,
- Gefahr durch Änderungen,
- Gefahr durch menschliches Versagen,
- Feuergefahr,
- Gefahr durch große Höhen.

In den folgenden Abschnitten wird auf die für automatisierte Krananlagen hauptsächlich zutreffenden Gefahren eingegangen.

6.1.1 Physikalische Gefahren

Physikalischen Gefahren werden nach der Art der Energie, durch die sie hervorgerufen werden, unterschieden. Dabei werden Ursachen der Gefahren in folgende Energiearten eingeteilt:

- Potentielle Energie: Z.B. bei Herabfallen einer Last durch mangelhafte Befestigung oder Absturz von Personen wegen fehlender Geländer.
- Kinetische Energie: Z.B. Loslassen beweglicher Gegenstände oder Kontakt mit bewegten Gegenständen.
- Elektrische Energie: Z.B. fehlerhafte Isolierung unter Spannung stehender Komponenten, oder gespeicherte Restenergien z.B. in Spulen oder Kondensatoren.
- Chemische Energie: Z.B. Säuren, Gifte und Explosionen.

Nach einer exakten Klassifizierung würden die Gefahren durch Vibration auch noch zu den physikalischen Gefahren gehören. In der Literatur werden diese allerdings immer gesondert aufgeführt.

6.1.2 Gefahr durch Vibration

Alle Maschinen und Anlagen schwingen auf unterschiedliche Art und Weise. Dadurch wird Schall emittiert und Vibrationen werden auf die Maschinenstruktur übertragen. Die Vibrationen beanspruchen und schwächen die Maschinenstruktur und Bauteilverbindungen.

Auch wenn es für automatisierte Krananlagen weniger relevant ist, sei aber der Vollständigkeit halber erwähnt, dass das Nervensystem des Menschen durch Schall und Vibration beansprucht wird, was zu einer erhöhten Wahrscheinlichkeit menschlichen Versagens führen kann. Zudem kann der dauerhafte Gebrauch von vibrierenden Gegenständen, die in der Hand gehalten werden, Verletzungen im Hand- und Armbereich verursachen.

6.1.3 Gefahr durch Eingeschlossensein

In kritischen Situationen können versperrte oder zugestellte reguläre Ein- und Ausgänge sowie Fluchtwege bewirken, dass Personen nicht ausreichend schnell vor einer Gefahr fliehen können. Während der Entwicklungsphase eines Systems sollte möglichst genau darauf geachtet werden, dass mindestens zwei Fluchtwege in entgegengesetzte Richtungen für den Gefahrenfall vorhanden sind.

Die zur Verfügung stehende Zeit, vor einer herabfallenden Last zu fliehen, ist bei Kranbetrieb als eher gering einzustufen, auch wenn Fluchtwege aus dem Kranbereich vorhanden sein sollten, um vor unkontrollierbaren Betriebszuständen fliehen zu können.

6.1.4 Gefahr durch Betreten

In allen Fällen muss das Eintreten in einen Gefahrenbereich für nicht autorisierte Personen verhindert werden. Besonders gefährdet sind Handwerker oder andere Personen, die sich für gewöhnlich nicht im Gefahrenbereich aufhalten und sich der sie umgebenden Gefahren nicht bewusst sind.

Wie später auch beschrieben, sind innerhalb des Gefahrenbereichs von automatisierten Krananlagen für Personen gewisse Verhaltensregeln notwendig. Wenn nicht autorisierte Personen diese Verhaltensregeln nicht kennen, erhöhen sich die potentiellen Gefahren (Kollision Kran mit Mensch oder Kran mit Element der Umwelt).

6.1.5 Gefahr durch Wartungsarbeiten

Die Gefahren liegen hier besonders bei nicht vollständig getrennter Energiezufuhr, z.B. von Strom, Treibstoff, Druckluft oder einer möglichen Bewegung von Maschinen aufgrund einer fehlenden Stillstandssicherung (z.B. Sicherung von hydraulischen Zylindern). Neben der Gefährdung durch eine unvollständig getrennte Energiezufuhr sind auch falsche Tätigkeiten im Gefahrenbereich von besonderer Bedeutung. Dazu gehört z.B. Schweißen in feuergefährdeten Bereichen durch nicht ausreichend eingewiesene Handwerker, was immer wieder zu Bränden führt, oder der Aufenthalt im Bewegungsbereich eines Roboters.

Speziell für automatisierte Krananlagen sind hier Wartungsarbeiten im Bewegungsbereich des Kranes zu nennen oder für den automatisierten Betrieb nicht vollständig gesperrte Bereiche, weil sie im Wartungszustand nicht sicher automatisch betrieben werden können.

6.1.6 Gefahr durch unvollständige Arbeit

Wann immer eine nicht abgeschlossene Arbeit, z.B. für eine nachfolgende Schicht, zur Erledigung hinterlassen wird, sind potentielle Gefahren, wie Missverständnisse, Fehlinterpretationen oder mangelnde Kommunikation, nicht mehr auszuschließen und können zu schwerwiegenden Unfällen führen.

6.1.7 Gefahr durch Änderungen

Änderungen an einem System bergen Gefahren, die im Allgemeinen übersehen werden. Sie sind besonders tückisch. Jede Maschine oder Anlage, die sicher und zuverlässig arbeitet, kann durch Änderungen in ihrer Arbeitsweise gefährlich werden. In diesem Fall muss eine vollständig neue Gefahrenanalyse durchgeführt werden. Es könnten in der veränderten Anordnung neue Wechselbeziehungen zwischen Anlagenkomponenten auftreten, die nicht erkannt werden. Es können beispielsweise Systemelemente über mögliche Grenzwerte belastet werden, oder Sicherheitsmaßnahmen könnten außer Funktionen gesetzt worden sein. Eine intensivere Nutzung könnte den Verschleiß beschleunigen. Neben den mechanischen Änderungen ist auch der Mensch bzw. die Mensch-Maschine-Schnittstelle betroffen. Mechanische Veränderungen können das dem Menschen geläufige Anlagenverhalten verändern. Außer Kraft gesetzte Routinehandgriffe und Automatismen stellen hier eine Gefahr dar, bis der Mensch umgelernt hat.

6.2 Fehler aus Software

Software allein kann keinen Schaden zufügen, Gefahr kann nur von ihr ausgehen, wenn sie über die Aktionen eines realen Systems entscheidet. Software muss deshalb als integrierter Bestandteil des Systems betrachtet werden.

Software zeigt keine Abnutzungserscheinungen. Softwarefehler entstehen also nicht durch den Betrieb, sondern es handelt sich dabei um Systemfehler. Da Software vom Menschen geschaffene Information ist, sind diese Fehler ausschließlich auf menschliches Irren zurückzuführen [39].

Die häufigsten und auch schlimmsten Fehler entstehen während der Anfangsphasen des Lebenszyklus von Software, wenn diese nicht ausreichend erprobt wurde. Hier schlagen sich die Auswirkungen des „Faktors Mensch“ am stärksten nieder.

6.3 Gefahren aus dem Kranbetrieb

Die Anwendung der in Kapitel 5 beschriebenen Methode für eine Sicherheitsanalyse zeigt die potentiellen Gefahren im Betrieb einer automatisierten Krananlage auf. Wie in der Systemanalyse beschrieben, wird dabei anhand aller Tätigkeiten, die im Zusammenhang mit dem automatischen Kranbetrieb auftreten, ein Lastspiel untersucht. In diesem Abschnitt werden die Ergebnisse dieser Sicherheitsanalyse aufgelistet.

6.3.1 Gefahren aus *Position teachen*

Bevor man den Kran automatisch fahren lassen kann, sind für den automatischen Betrieb Positionen zu speichern, die der Kran anfahren darf. Diesen Vorgang nennt man „Position teachen“.

- Der Teachprozess kann den Kranbetrieb beeinflussen. Durch Teachprozesse im laufenden Kranbetrieb können Gefährdungen durch unvorhersehbare Steuerungszustände oder nicht erkannte Fehler auftreten.
- Das Teachen einer falschen Position kann Gefährdungen hervorrufen. Wird eine Position falsch geteacht, z.B. in einem Bereich, der nicht im Automatik-Modus befahren werden darf, oder in Bereichen von Hindernissen, kann dies zu Kollisionen oder unerwarteten Gefährdungen führen.

6.3.2 Gefahren durch falsche Inbetriebnahme

Jede automatisierte Krananlage muss vor Beginn jeglicher Tätigkeiten in Betrieb genommen werden. Zu Beginn der Arbeit, nach Stromausfällen oder sonstigen Störungen ist die Anlage wieder an das Stromnetz anzuschließen, sind die Steuerungsprogramme zu starten und die Sensoren, insbesondere das Wegmesssystem, zu initialisieren.

Die hieraus resultierenden Gefahren ergeben sich aus einem unkontrollierten Anlaufen von Fahrtrieben oder des Hubwerks bei Anschluss an das Stromnetz oder einem fehlerhaft initialisiertem relativen Wegmesssystem mit den daraus entstehenden fehlerhaften Positionen im Steuerungsprogramm und den sich daraus ergebenden Gefahren von Kollisionen.

6.3.3 Gefahren durch Kranruf

Wird der Kran halbautomatisiert betrieben, muss zunächst der Kran gerufen werden. Dies kann z.B. mittels eines Ruftasters erfolgen. Bei voll automatisiertem Betrieb erfolgt der Kranruf anhand eines Prozessleitsystems zu einer bestimmten Position. Die Gefahren aus dem Kranruf sind folgende:

- Der Kran kann durch einen Steuerungs- oder Programmierfehler in einer anderen manuellen Betätigung beeinflusst werden. Somit können Personen gefährdet werden, die gerade manuell mit diesem Kran arbeiten.
- Der Kran kann an falsche Position gerufen werden und so Gefährdungen hervorrufen. Das unerwartete Erscheinen eines Kranes kann gefährlich sein, wenn dieser Bereich Hindernisse oder Ähnliches aufweist.
- Der Kran kann irgendeine andere unerwünschte Aktion durchführen, die durch Steuerungs- oder Programmierfehler hervorgerufen wird, wodurch allgemein Gefahren auftreten können.

6.3.4 Gefahren der Leerfahrt

Nachdem die Daten für die Zielposition der Kranfahrt übermittelt worden sind, beginnt der Kran zu seinem Ziel zu fahren. Dabei besteht bei horizontalen wie auch bei vertikalen Bewegungen die Gefahr der Kollision mit anderen Kranen oder Elementen der Umwelt. Die Ursachen dafür sind z.B. Fehler der Steuerung oder Fehler der Wegmesssysteme für Katz- und Kranposition sowie Hubhöhe.

Wird im teilautomatisierten Betrieb gearbeitet, so ist darauf zu achten, dass die manuelle Kranfahrt den Automatikbetrieb nicht gefährdet, da automatisierte und manuell betriebene Krane sich auf einer Bahn befinden und beeinflussen können.

6.3.5 Gefahren aus der Lastaufnahme

Nach der Systemanalyse kann eine manuelle Lastaufnahme einer manuellen oder automatischen Leerfahrt folgen sowie durch eine manuelle oder automatische Lastfahrt fortgesetzt werden. Eine automatisierte Lastaufnahme kann nur einer automatischen Lastaufnahme folgen und durch eine automatische Lastfahrt fortgesetzt werden.

Für den ersten Fall ergeben sich Gefahren aus einem unkorrekten Betriebsartwechsel vom automatisierten in den manuellen Modus. Ein noch nicht vollständig in den

manuellen Modus umgeschalteter Kran könnte gefährliche Situationen im Personenbereich hervorrufen.

Für den zweiten Fall einer automatisierten Lastaufnahme ergeben sich die Gefahren bei der Positionierung der Last an der Übergabeposition, wenn Personen sich in der Nähe von automatisch absenkenden Lastaufnahmemitteln aufhalten.

Der eigentliche Vorgang der Lastaufnahme unterscheidet sich nicht im voll- oder teilautomatisierten Kranbetrieb, da dieser in beiden Fällen den gleichen strengen Kontrollen unterliegt, damit ein Lastabsturz im weiteren Verlauf der automatisierten Lastfahrt verhindert werden kann. Werden beispielsweise im teilautomatisierten Betrieb Lasten manuell aufgenommen und diese im automatischen Modus weitertransportiert, können sonst menschliche Fehler zu Gefahren aus einer unkorrekten Lastaufnahme führen.

Gefahren aus der Lastaufnahme ergeben sich durch ungeeignete oder fehlerhafte Ladehilfsmittel, falsche Lasten, die zu groß, zu klein oder zu schwer sind, sowie durch einen unvollständigen nicht formschlüssigen Greifvorgang. Eine falsche Positionierung der Last birgt ebenfalls die Gefahr einer Kollision der Last mit dem Lastaufnahmemittel oder einer falschen Lastaufnahme.

6.3.6 Gefahren der Lastfahrt

Ähnlich wie bei der Leerfahrt beginnt der Kran zu seinem Ziel zu fahren, nachdem die Daten für die Zielposition der Kranfahrt übermittelt worden sind. Dabei besteht sowohl bei horizontalen als auch vertikalen Bewegungen die Gefahr der Kollision mit anderen Kranen oder Elementen der Umwelt. Auch hier sind Fehler der Steuerung oder des Wegmesssystems sowie eine zur Kollision führende zu große Last die Ursache der Gefahren.

Wird im teilautomatisierten Betrieb gearbeitet, so ist darauf ebenfalls zu achten, dass die manuelle Kranfahrt den Automatikbetrieb nicht gefährdet, da automatisierte und manuell betriebene Krane sich auf einer Bahn befinden und beeinflussen können.

Weiterhin besteht die Gefahr des Lastabsturzes.

6.3.7 Gefahren aus der Lastabgabe

Gefahren aus der Lastabgabe ergeben sich wie bei der Lastaufnahme aus der Nähe von Personen zu bewegten Kranelementen sowie aus einer unvollständigen Lastabgabe. Weiterhin kann die Situation, in der die Last gelöst wird, unpassend sein, wenn die Last noch schwebt oder auf einer unebenen Position zum Stehen kommt.

6.3.8 Gefahren aus der Quittierung der manuellen Kranfahrt

Nach Beendigung eines manuellen Arbeitsganges kann der Kran wieder für den Automatikmodus freigegeben werden. Dies birgt jedoch die Gefahr, dass der Kran noch nicht für den Automatikmodus bereit sein kann, wodurch ein unüberschaubarer Zustand entsteht. Dies ist zum Beispiel dann der Fall, wenn sich eine Last noch am Lastaufnahmemittel befindet, die nicht für den automatisierten sondern nur für den manuellen Betrieb geeignet ist.

6.4 Fehlerbaumanalyse

Bei der Gefahrenanalyse in Abschnitt 6.3 wurden Gefahren durch Betrachtung von Arbeitsschritten mit dem Ausfall eines Betriebselementes oder einer fehlerhaften Handlung ermittelt. Ein weiterer Ansatz besteht darin, die Ursachen für die Gefahren zu ermitteln. Für diesen zweiten deduktiven Schritt der Gefahrenanalyse wird die Fehlerbaumanalyse verwendet.

Das Ergebnis der oben durchgeführten Gefahrenanalyse lässt sich bei genauerer Betrachtung zu drei Gefahren zusammenfassen, die auf ihre Ursache hin untersucht werden. Dabei ist das wichtigste Ereignis die Gefährdung eines Menschen. Die Gefährdung kann drei Ursachen besitzen:

- Lastabsturz
- Selbstzerstörung der Anlage
- Kollision eines Kranelementes mit einem Element der Umwelt, wobei hier zwischen
 - Kollision Kran mit Kran
 - Kollision Kran mit Mensch
 - Kollision Kran mit Last
 - Kollision Kran mit anderen Umweltelementen

unterschieden werden kann.

Ausgehend von diesen Gefahren wird im Folgenden die Fehlerbaumanalyse durchgeführt, die in den Abbildungen 6-1 bis 6-5 als Fehlerbaum graphisch dargestellt wird.

In Abbildung 6-1 ist die Verletzung eines Menschen das absolut zu vermeidende Ereignis, von dem ausgehend die Ursachen gesucht werden. Es zeigt sich, dass dieses Ereignis durch einen Lastabsturz, durch eine Selbstzerstörung der Anlage oder durch eine Kollision mit anderen Elementen der Umwelt auftreten kann.

Die Ursachen für die Kollision mit einem Element der Umwelt werden in den Abbildungen 6-2 bis 6-5 dargestellt.

Abbildung 6-2 zeigt die möglichen Ursachen, die zu einer Kollision des Kranes mit Menschen führen kann. Dabei sind zunächst zwei Ursachen zu unterscheiden: Der

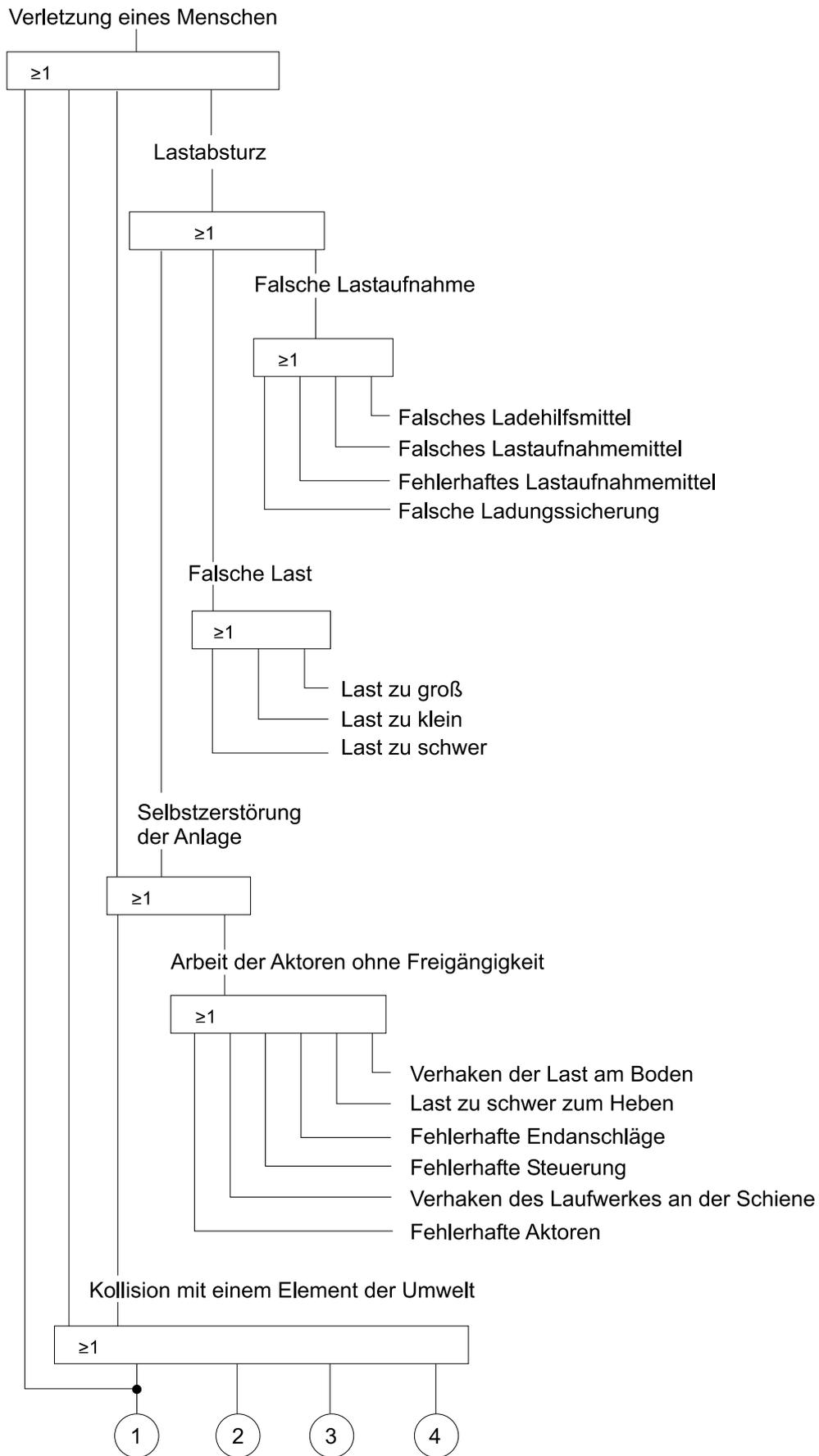


Abb. 6-1: Fehlerbaum Teil 1

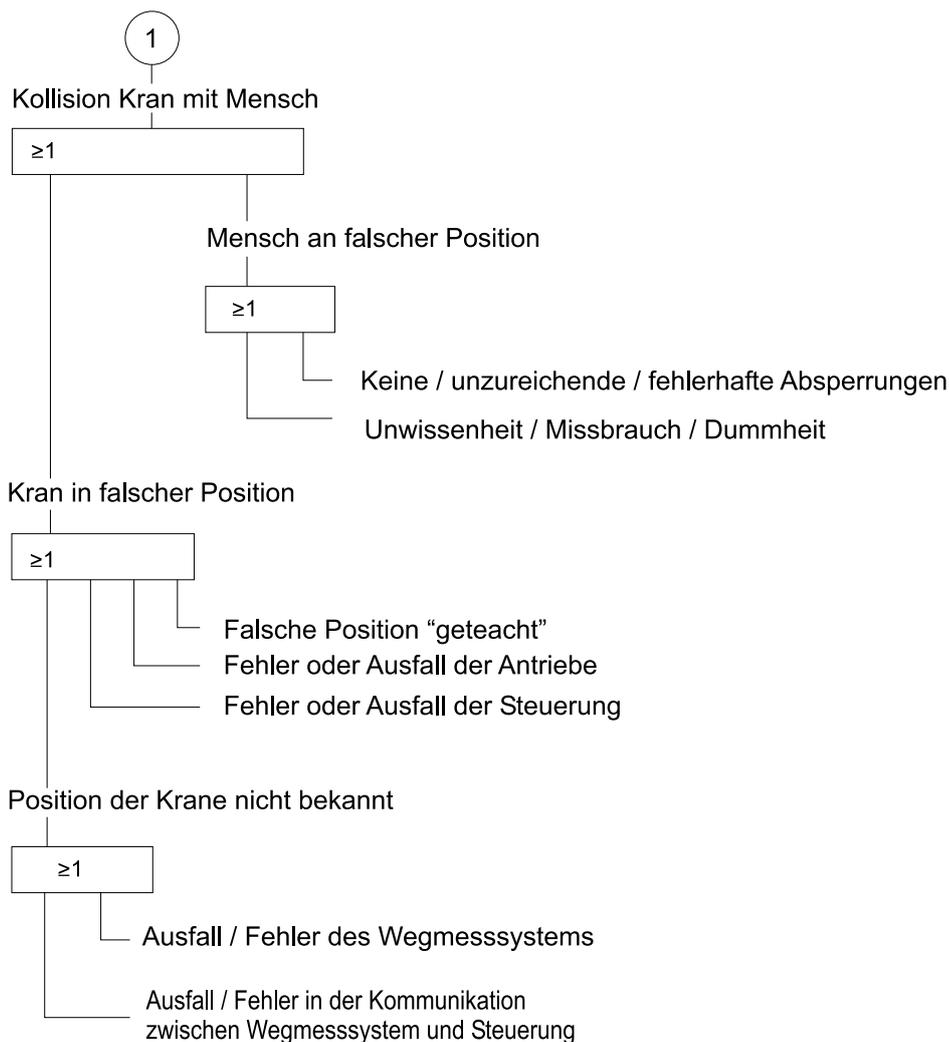


Abb. 6-2: Fehlerbaum Teil 2

Mensch kann sich in einer falschen Position befinden, oder der Kran kann sich in der falschen Position befinden. Befindet sich der Mensch in einer falschen Position, so sind die Ursachen dafür keine oder unzureichende Absperrungen, vorsätzliche Missachtung von Warnungen oder Unwissenheit der Personen, die sich im Kranbereich aufhalten. Die Ursache für eine falsche Position des Kranes kann eine falsch gespeicherte Zielposition, fehlerhafte Antriebe oder eine fehlerhafte Kransteuerung sein. Ebenso ein Ausfall des Wegmesssystems oder der Kommunikation zwischen Wegmesssystem und Steuerung, mit dem damit verbundenen Verlust der Kranposition.

Sollten zwei Krane miteinander kollidieren, so ist die Ursache, wie in Abbildung 6-3 dargestellt, hauptsächlich bei einer falschen Kranpositionierung zu suchen. Dies kann, wie schon oben beschrieben, durch einen Ausfall des Wegmesssystems, einen Fehler in der Kommunikation oder auch durch fehlerhafte Antriebe und Steuerungen bedingt sein.

Abbildung 6-4 zeigt die möglichen Gefahrenursachen für eine Kollision des Kranes mit

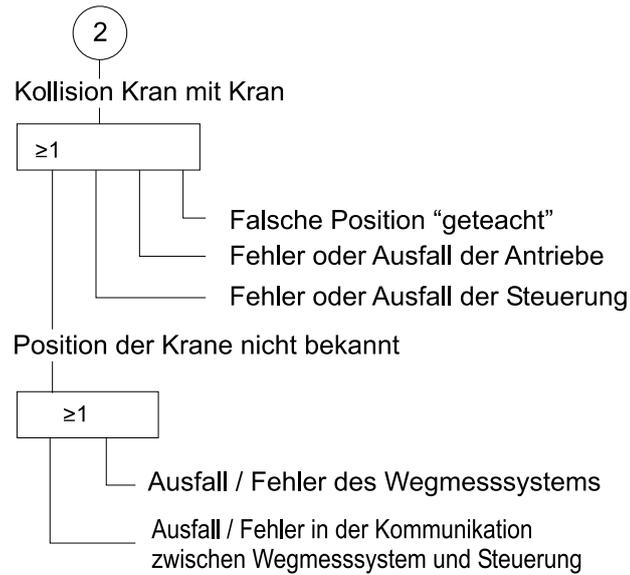


Abb. 6-3: Fehlerbaum Teil 3

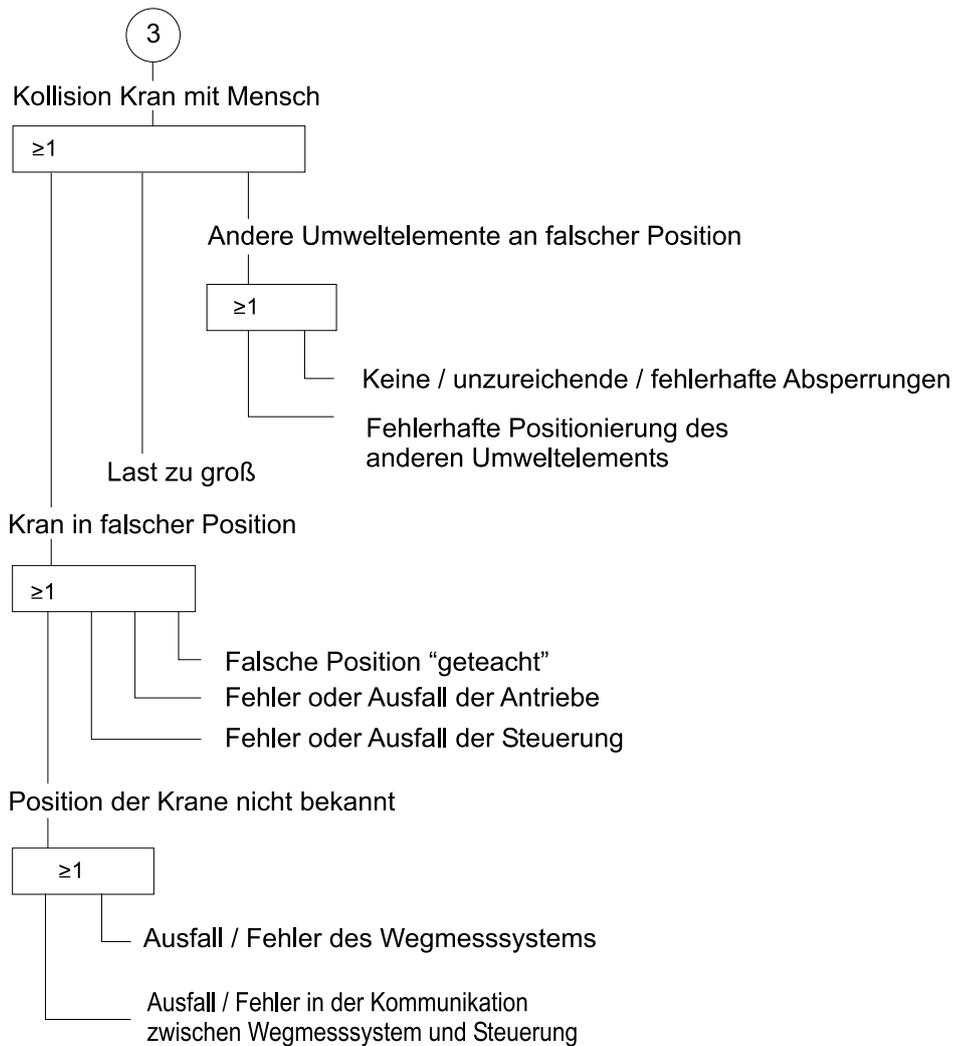


Abb. 6-4: Fehlerbaum Teil 4

anderen Elementen der Umwelt. Unter anderen Elementen der Umwelt sind die Halle, in der sich die Krananlage befindet, Einrichtungsgegenstände wie Fertigungsmaschinen oder Flurfördertechnik zu verstehen. Weiterhin können dies auch Gegenstände aller Art sein, wie z.B. Leitern, die zum Austausch der Deckenbeleuchtung aufgestellt, oder Kartons, die von Mitarbeitern auf Maschinen gelagert werden.

Die Ursachen für eine Kollision liegen auch hier wieder in einer falschen Kranposition, einer zu großen Last oder einem anderen Umweltelement, welches sich unzulässigerweise im Bewegungsbereich des Kranes befindet.

Der letzte Ast des Fehlerbaumes untersucht in Abbildung 6-5, inwieweit eine Kollision des Kranes mit der Last stattfinden kann. Die Ursachen dafür sind in einem nicht aufnahmebereiten Lastaufnahmemittel, einer falschen Position des Lastaufnahmemittels, einer falschen Last, einem falschen Ladehilfsmittel oder einer falschen Kranposition zu suchen.

Aus den Abbildungen 6-1 bis 6-5 ist zu erkennen, dass der Schwerpunkt hinsichtlich der sicherheitsrelevanten Bauteile beim Wegmesssystem, bei der Kommunikation und der Steuerung der Anlage liegt. Da jedoch alle Ursachen, wie eine falsche Lastaufnahme, resultierend aus einem falschen Ladehilfsmittel oder Lastaufnahmemittel zu einem Lastabsturz mit seinen fatalen Folgen führen können, wird für jede Eingabesituation des Fehlerbaumes eine Lösung im Sicherheitskonzept gesucht.

7 Sichere Maschinen

Bei der Konstruktion, dem Bau und Betrieb von Kranen ist die Einhaltung von sicherheitstechnischen Prinzipien unbedingte Voraussetzung für die Vermeidung von Gefährdungen, die sich z.B. aus einem Lastabsturz oder Versagen der Krankonstruktion für Leben und Gesundheit von Personen sowie für Gegenstände und die Umgebung ergeben können.

7.1 Erreichen der Sicherheit

Zu den grundlegenden Überlegungen, die das gesamte Normenwerk durchziehen, gehört die in Anhang 1 der Maschinenrichtlinie festgelegte und in EN 292 präzierte Vorgehensweise bei der Konstruktion einer sicheren Maschine. Dort wird der in Abb. 7-1 gezeigte iterative Vorgang zum Erreichen einer ausreichenden Sicherheit dargestellt. Der Prozess ist durch die Risikoanalyse und die Risikobewertung geprägt. Innerhalb der Risikoanalyse werden in einem ersten Schritt die Grenzen der Maschine einschließlich

- Lebensdauer,
- Einsatzbereiche und
- Ausbildungsniveau der Anwender

bestimmt.

In einem weiteren Schritt ist die Identifizierung der Gefährdungen mit einer Gefahrenanalyse durchzuführen. Die verschiedenen Methoden der Gefahrenanalyse sind ausführlich in Kapitel 5 beschrieben worden. Das Ergebnis der Gefahrenanalyse ist in Kapitel 6 zusammengefasst.

Zuletzt folgt die Risikoabschätzung, die nach in DIN 1050 vorgeschlagen folgenden Punkten vorgenommen werden kann (siehe auch EN 954-1, B2, in Abschnitt 7.2 dieses Kapitels):

- Schwere der Verletzung
- Häufigkeit und/oder Dauer der Gefährdungsexposition
- Möglichkeit zur Vermeidung der Gefährdung.

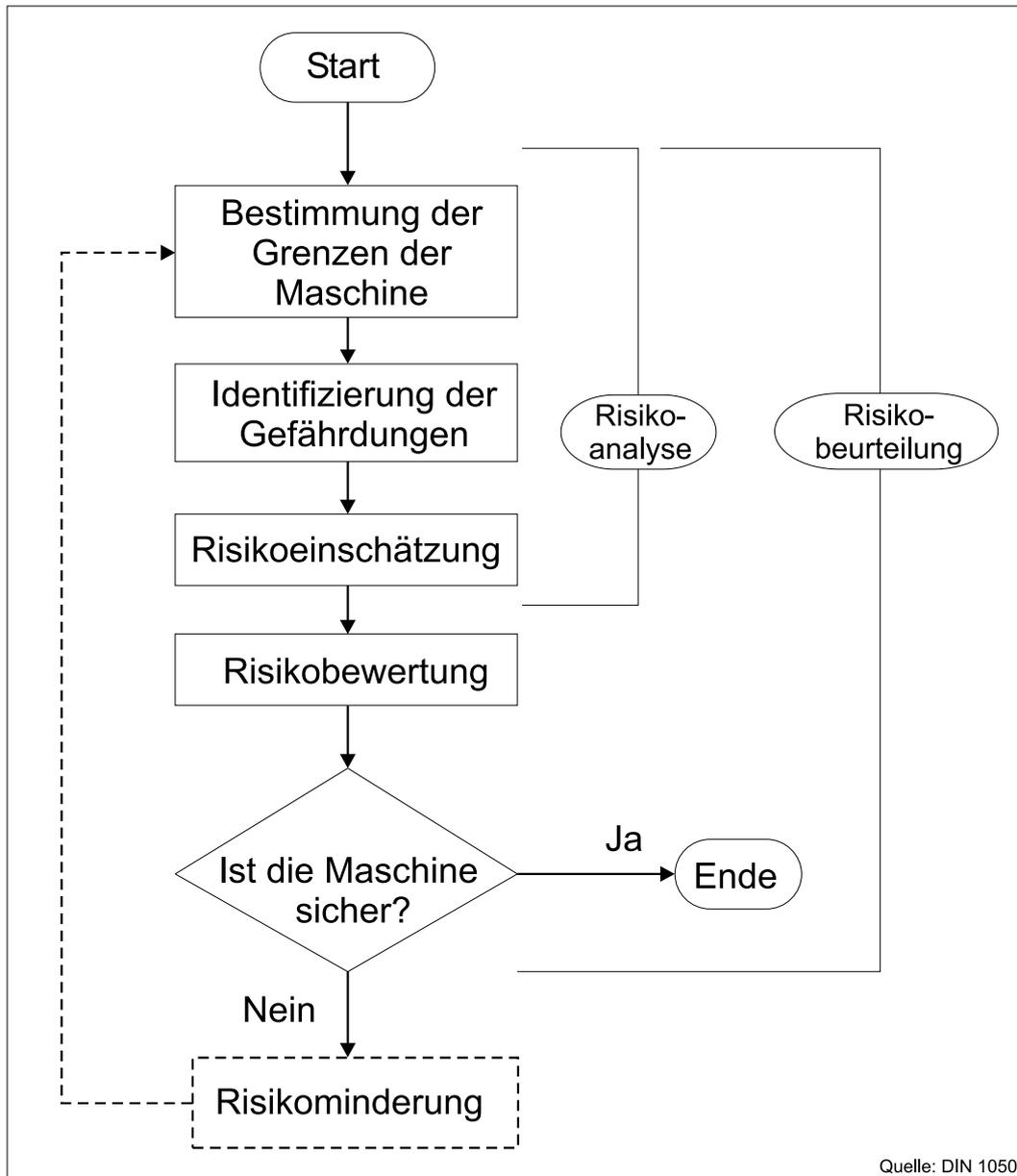


Abb. 7-1: Iterativer Prozess zum Erreichen der Sicherheit

Nach der Risikoeinschätzung muss eine Risikobewertung durchgeführt werden, um zu entscheiden, ob eine Risikominderung notwendig ist oder ob Sicherheit erreicht wurde. Falls diese nicht erreicht wurde, ist das Risiko zu vermindern und die Maschine einer erneuten Prüfung zu unterziehen.

Um das von einer Maschine ausgehende Risiko zu reduzieren, muss der Hersteller nach DIN EN 292-1 die Maschine zunächst durch unmittelbare Sicherheitstechnik so konstruieren, dass Gefährdungen vermieden oder möglichst gering gehalten werden. Die unmittelbare Sicherheitstechnik setzt bereits während der Konstruktion auf den Einsatz der aktiv an der Funktionserfüllung beteiligten Komponenten. Prinzipien unmittelbarer Sicherheitstechnik sind dabei das safe-life-Verhalten sowie die Verwen-

dung redundanter Funktionen[40].

Beim safe-life-Verhalten wird von einem sicheren Bestehen der Funktion ausgegangen. Beim fail-safe-Verhalten hingegen ist das Versagen innerhalb der Konstruktion berücksichtigt, so dass sich das technische System nicht in einen gefährlichen Zustand bewegt. Sicherheitsrelevante Funktionen bleiben in diesem Fall erhalten, wobei von einer Einschränkung des Betriebs ausgegangen werden muss [41].

Mit dem Begriff Redundanz wird, wie in DIN 19250 beschrieben, die Ausführung einer vorgesehenen Aufgabe mit mehr als den notwendigen Mitteln beschrieben. Dabei wird zwischen aktiver und passiver Redundanz unterschieden. Unter einer aktiven Redundanz ist dabei die gleichzeitige Beteiligung aller funktionserfüllenden Komponenten zu verstehen, während die passive Redundanz erst beim Ausfall von Funktionsträgern mit Hilfe eines Schaltvorganges die bislang nicht genutzten Elemente aktiviert.

Redundante Anordnungen dienen häufig auch der Fehlererkennung, indem die Ergebnisse mehrerer steuerungstechnischer Komponenten auf ihre Übereinstimmung hin überprüft werden. Soll nur das Vorhandensein eines Fehlers aufgedeckt werden, spricht man von einer Vergleichsredundanz. Für die Kenntnis einer Fehlerursache ist allerdings eine Überzahl fehlerfreier Ergebnisse im Vergleich zum fehlerbehafteten Ergebnis erforderlich. In diesem Fall liegt eine Auswahlredundanz vor. Zur Erlangung von einander unabhängigen Größen für einen Vergleich, welche auch systematischen Fehlereinflüssen widerstehen, ist der Einsatz unterschiedlicher Wirkprinzipien notwendig. So erhält man eine Prinzipienredundanz, die auch als Diversität bezeichnet wird[25] [42].

Ist unmittelbare Sicherheitstechnik nicht anwendbar, müssen Gefährdungen durch mittelbare Sicherheitstechnik ausgeschlossen werden.

Zu den mittelbaren Sicherheitsmaßnahmen zählen Schutzeinrichtungen, die eine Gefahr nicht zu einer Gefährdung für den Menschen oder die Umwelt werden lassen. Dabei wird in DIN 292-1 in trennende, nicht trennende, und abweisende Schutzeinrichtungen unterschieden, welche die Sicherheit durch Fernhalten des Menschen von der Gefahrenquelle erreichen.

Wenn auch dies nicht wirksam ist, muss der Hersteller deutlich durch hinweisende Sicherheitstechnik auf die verbleibenden Restrisiken hinweisen.

Die Sicherheitsmaßnahmen im Maschinenbau sind in Tabelle 7-1 dargestellt.

1. Stufe	2. Stufe	3. Stufe	Zusätzliche Vor- sichtsmaßnahmen
Risikominderung durch Konstruktion	Technische Schutzmaßnahmen	Benutzer- information	
unmittelbare Sicherheitstechnik	mittelbare Sicherheitstechnik	hinweisende Sicherheitstechnik	
Gefährdungen vermeiden	Gefährdungen sichern	auf Restrisiken hinweisen	

Tabelle 7-1: Sicherheitsmaßnahmen im Maschinenbau

7.2 Auswahl von Schutzeinrichtungen

Je nach verbleibendem Restrisiko ist für Bauteile und Steuerungen ein Sicherheitsstandard zu finden. EN 954-1 bietet hierzu die Möglichkeit, die Anforderungen an sicherheitsbezogenen Teilen von Steuerungen mittels Schutzkategorien festzulegen. Eine mögliche Auswahl der Kategorien ist in Abb. 7-2 dargestellt.

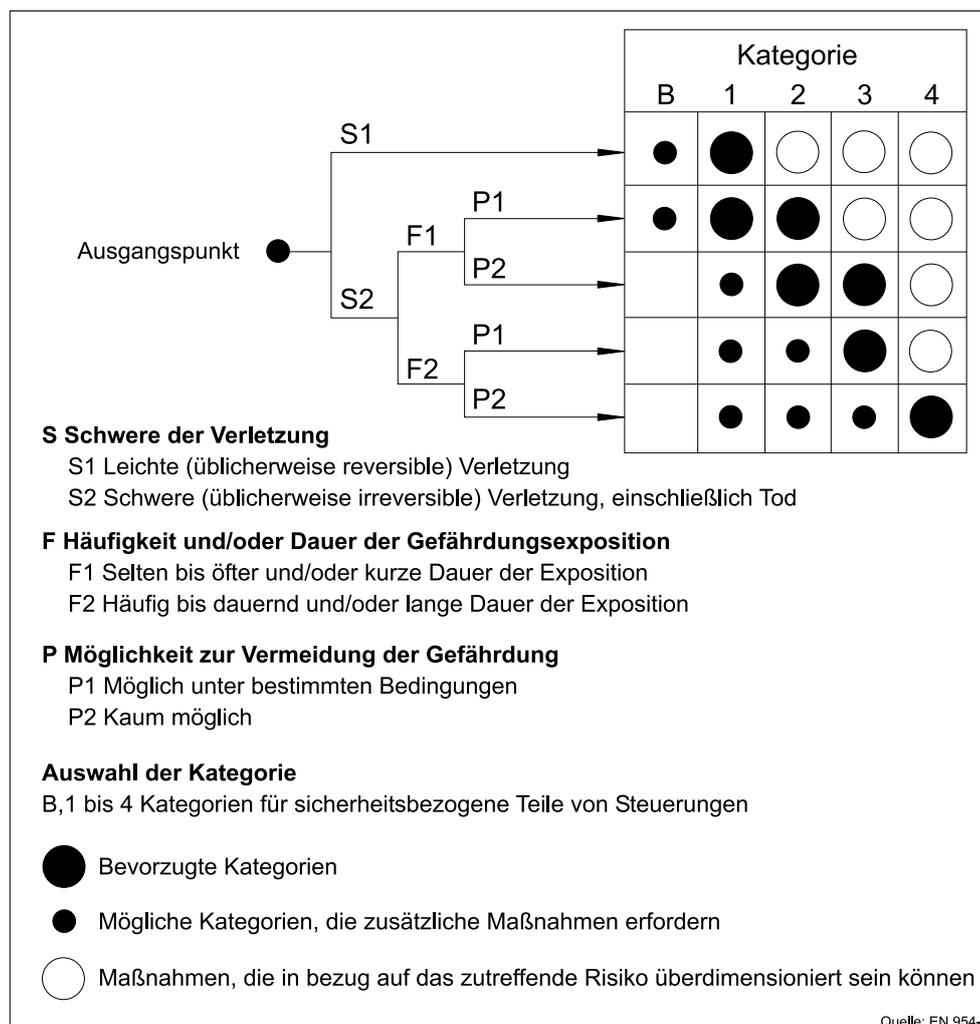


Abb. 7-2: Mögliche Auswahl der Schutzkategorien nach EN 954-1

Zu den Faktoren, die bei der Risikoabschätzung heranzuziehen sind, gehören:

- die Häufigkeit und Dauer der Gefährdungsexposition (F),
- der höchste vorhersehbare Schweregrad einer Verletzung (S),
- die mögliche Vermeidung von Gefährdungen (P).

Eine genauere Beschreibung, wie die Parameter S, F und P zu wählen sind, findet sich in DIN EN 954-1 Anhang B.2

Wenn diese Parameter im Rahmen der Risikoabschätzung bestimmt werden, ergibt sich eine von fünf Schutzkategorien (B, 1, 2, 3, 4).

An jede der Kategorien werden in DIN EN 954-1 Anforderungen, wie z.B. an die Fehlerbeherrschung der Steuerung, gestellt. Die Anforderungen, die zu den Schutzkategorien aus DIN EN 954-1 vereinbart wurden, sind in Tabelle 7-2 zusammengefasst.

Die höchsten vorhersehbaren Verletzungen (S), die man durch automatische Krananlagen im personenzugänglichen Umfeld verursachen kann, reichen von leichten bis zu schweren auch irreversiblen Verletzungen bis einschließlich Tod. Diese Verletzungen können durch Kollision eines Menschen mit einem Element der Krananlage oder durch einen Lastabsturz auftreten.

Die Häufigkeit und Dauer der Gefährdungsexposition (F) kann ohne weiteres von häufig bis dauernd eingestuft werden, da sich der Kran im personenzugänglichen Umfeld bewegt und somit Menschen jederzeit Zugang zur Anlage haben.

Im letzten Schritt ist zu prüfen, ob die Möglichkeit zur Vermeidung der Gefährdung (P) gegeben ist. Hierzu wird geprüft, ob die Gefahr direkt oder nur durch Messinstrumente zu erkennen ist.

Weitere wichtige Gesichtspunkte sind:

- beaufsichtigter oder unbeaufsichtigter Betrieb,
- Betrieb durch Fachpersonal oder Laien,
- Geschwindigkeit des Auftretens der Gefahr, z.B. schnell oder langsam,
- Möglichkeiten zur Vermeidung der Gefährdung, z.B. durch Flucht oder Eingreifen Dritter,
- praktische Erfahrungen mit der Sicherheit in Bezug auf den Prozessverlauf.

Tabelle 7-3 enthält den Entscheidungsweg zur Auswahl der Schutzkategorien.

Kat. ¹⁾	Anforderungen	Systemverhalten ²⁾	Prinzipien zum Erreichen der Sicherheit
B	Die sicherheitsbezogenen Teile von Steuerungen und/oder ihre Schutzrichtungen sowie ihre Bauteile müssen in Übereinstimmung mit den zutreffenden Normen so gestaltet, gebaut, ausgewählt, zusammengestellt und kombiniert werden, dass sie den zu erwartenden Einflüssen standhalten können.	Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen.	Überwiegend durch Auswahl von Bauteilen charakterisiert
1	Die Anforderungen von B müssen erfüllt sein. Bewährte Bauteile und bewährte Sicherheitsprinzipien müssen angewendet werden.	Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion führen. Die Wahrscheinlichkeit des Auftretens ist geringer als in Kategorie B.	
2	Die Anforderungen von B und die Verwendung bewährter Sicherheitsprinzipien müssen erfüllt sein. Die Sicherheitsfunktion muss in geeigneten Zeitabständen durch die Maschinensteuerung geprüft werden.	<ul style="list-style-type: none"> • Das Auftreten eines Fehlers kann zum Verlust der Sicherheitsfunktion zwischen den Prüfungsabständen führen. • Der Verlust der Sicherheitsfunktion wird durch die Prüfung erkannt. 	Überwiegend durch die Struktur charakterisiert
3	Die Anforderungen von B und die Verwendung bewährter Sicherheitsprinzipien müssen erfüllt sein. Sicherheitsbezogene Teile müssen so gestaltet sein, dass <ul style="list-style-type: none"> • ein einzelner Fehler in jedem dieser Teile nicht zum Verlust der Sicherheitsfunktion führt und • wann immer in angemessener Weise durchführbar, der einzelne Fehler erkannt wird. 	<ul style="list-style-type: none"> • Wenn der einzelne Fehler auftritt, bleibt die Sicherheitsfunktion immer erhalten. • Einige, aber nicht alle Fehler werden erkannt. • Eine Anhäufung unerkannter Fehler kann zum Verlust der Sicherheitsfunktion führen. 	
4	Die Anforderungen von B und die Verwendung bewährter Sicherheitsprinzipien müssen erfüllt sein. Sicherheitsbezogene Teile müssen so gestaltet sein, daß <ul style="list-style-type: none"> • ein einzelner Fehler in jedem dieser Teile nicht zum Verlust der Sicherheitsfunktion führt und • der einzelne Fehler bei oder vor der nächsten Anforderung an die Sicherheitsfunktion erkannt wird. Wenn dies nicht möglich ist, darf eine Anhäufung von Fehlern nicht zum Verlust der Sicherheitsfunktion führen. 	<ul style="list-style-type: none"> • Wenn Fehler auftreten, bleibt die Sicherheitsfunktion immer erhalten. • Die Fehler werden rechtzeitig erkannt, um einen Verlust der Sicherheitsfunktion zu verhindern. 	

1) Die Kategorien sind nicht dazu bestimmt, in irgendeiner gegebenen Reihenfolge oder hierarchischen Anordnung in Bezug auf die sicherheitstechnischen Anforderungen angewendet zu werden.

2) Aus der Risikobeurteilung wird sich ergeben, ob der gesamte oder teilweise Verlust der Sicherheitsfunktion(en) aufgrund von Fehlern akzeptabel ist.

Tabelle 7-2: Schutzkategorien nach DIN EN 954-1

Kriterien	Auswahl	
Schwere der Verletzung	Schwere Verletzungen einschließlich Tod durch Lastabsturz möglich	S2
Häufigkeit und/oder Dauer der Gefährdungsexposition	Dauernde Gefährdungsexposition	F2
Möglichkeiten zur Vermeidung der Gefährdung: - beaufsichtigter oder unbeaufsichtigter Betrieb - Betrieb durch Fachpersonal oder Laien - Schnelligkeit des Auftretens der Gefahr, - Möglichkeiten zur Vermeidung der Gefährdung, z.B. durch Flucht, Eingreifen Dritter - praktische Erfahrungen mit der Sicherheit in Bezug auf den Prozeßverlauf.	- unbeaufsichtigter Betrieb - automatischer Betrieb - sehr schnell bei Lastabsturz - keine Flucht möglich bei Lastabsturz - keine Erfahrungen bei Betrieb	P2

Tabelle 7-3: Entscheidungsweg zur Kategorieauswahl nach EN 954-1

Unter Berücksichtigung des oben gezeigten Auswahlschemas erkennt man, dass für die Steuerung die Kategorien 1 bis 3 mit Zusatzmaßnahmen oder Kategorie 4 zu verwenden sind. Nach Absprache mit dem Fachausschuss Hebezeuge der Berufsgenossenschaft in Düsseldorf kann für automatisierte Krananlagen für den innerbetrieblichen Behältertransport auch Kategorie 3 ohne Zusatzmaßnahmen verwendet werden. Die niedrigeren Kategorien 1 und 2 mit Zusatzmaßnahmen werden hier wegen der mangelnden Erfahrung bei Betrieb als zu unsicher ausgeschlossen. So stehen die Kategorien 3 und auch 4 nach DIN EN 954-1 für sicherheitsrelevante Teile der Steuerung und Sensoren zur Verfügung.

Ähnlich wie DIN EN 954-1 für Bauteile und Steuerungen gibt es den internationalen Standard IEC 61508 (Abbildung 7-3) speziell für Systeme mit elektrischer, elektronischer und programmierbarer Elektronik (E/E/PE). Diese Norm hilft herauszufinden, wie groß die Reduzierung des Risikos und der *safety integrity level* sein müssen.

Die Untersuchungskriterien für diese Norm zur Reduzierung des Risikos sind:

- Auswirkungen,
- Häufigkeit der Gefahr,
- Möglichkeit, die Gefahr zu vermeiden,
- Wahrscheinlichkeit des ungewollten Ereignisses.

Diese Punkte werden wiederum aufgeschlüsselt in Auswirkungen:

- C1 Geringe Verletzungen,
- C2 Ernsthafte Verletzung mit bleibenden Schäden an einer oder mehreren Personen,
- C3 Tod für mehrere Personen,
- C4 Viele Personen sterben.

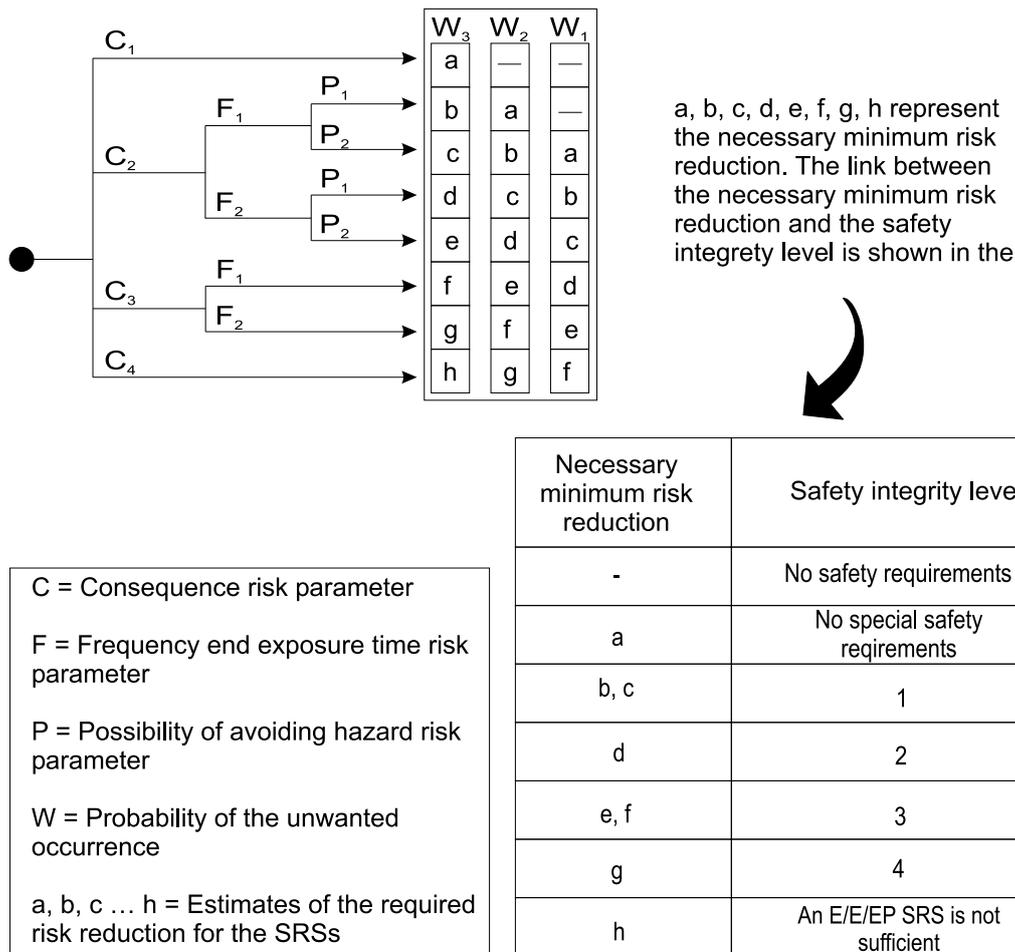


Abb. 7-3: IEC 61508

Häufigkeit der Gefährdung:

- F1 Seltene bis häufige Gefährdung,
- F2 Häufige bis dauerhafte Gefährdung.

Möglichkeit die Gefahr zu vermeiden:

- P1 Möglich unter bestimmten Bedingungen,
- P2 Meist unmöglich.

Wahrscheinlichkeit des unerwünschten Ereignisses:

- W1 Sehr geringe Wahrscheinlichkeit, dass unerwünschte Ereignisse eintreten. Sehr wenige unerwünschte Ereignisse sind möglich.
- W2 Geringe Wahrscheinlichkeit, dass unerwünschte Ereignisse eintreten. Wenige unerwünschte Ereignisse sind möglich.
- W3 Eine relativ hohe Wahrscheinlichkeit, dass unerwünschte Ereignisse eintreten. Viele unerwünschte Ereignisse sind möglich.

Der *safety integrity level* für automatisierte Krananlagen ergibt sich durch die drei Annahmen:

- Tod für mehrere Personen (C3),
- Häufige bis dauerhafte Gefährdung (F2) und
- eine geringe Wahrscheinlichkeit, dass das unerwünschte Ereignis eintritt (W2).

Die Möglichkeiten, die Gefährdung zu vermeiden, werden ab C3 nicht mehr berücksichtigt. Aus den oben genannten Annahmen ergibt sich eine notwendige Reduzierung des Risikos der Kategorie f und damit ein *safety integrity level* der Stufe 3.

7.3 Verhalten bei Fehlern

Bei einem Kran ist im Allgemeinen der sichere Zustand erreicht, wenn der oder die Antriebe stillgesetzt und die Bremsen eingefallen sind sowie die Leistungsenergie abgeschaltet wurde. Der sichere Zustand muss bei einem Kran in einer sehr kurzen Zeit erreicht werden. Es ist deshalb erforderlich, die Reaktionszeit der Steuerung so kurz wie möglich zu halten (Größenordnung ca. 50ms), andernfalls können durchaus gefährliche Betriebszustände für den Kran entstehen.

In der DIN EN 60204-32 sind fünf unterschiedliche Arten der Abschaltung definiert:

1. Not-Aus, vollständiges Trennen vom Netz
2. Not-Halt, Abschalten des Antriebes, sofort Trennen der Energie (Kategorie 0)
3. Ungesteuertes Stillsetzen, sofort Trennen der Energie (Kategorie 0)
4. Gesteuertes Stillsetzen, erst Stop, dann Trennen der Energie (Kategorie 1)
5. Gesteuertes Stillsetzen, ohne Trennen der Energie (Kategorie 2)

Für eine Schutzkategorie 3 nach DIN EN 954-1 ergeben sich die nach [43] in Tabelle 7-4 beschriebenen sicheren Antriebsfunktionen, die für den Einsatz von Maschinen geeignet sind.

Die Steuerung muss den an die unterschiedlichen Abschaltmethoden gestellten Anforderungen gerecht werden.

7.4 Rolle des Menschen

Es besteht ein Konsens darüber, dass auch in vollautomatisierten Systemen die Verantwortung über das Gesamtsystem beim Menschen liegen muss, da solche Systeme immer wieder in unvorhergesehe Zustände geraten können.

Trotz aller Sicherheitsvorkehrungen kommt es immer wieder zu Unfällen. Das liegt daran, dass sich komplexe Systeme unter anderem dadurch auszeichnen, dass sie sich aus einer Vielzahl von Komponenten zusammensetzen und einen hohen Grad von Vernetztheit sowie eine gewisse Eigendynamik und Intransparenz aufweisen. Das

Funktion	Beschreibung
Sicherer Halt	Die Antriebe sind nicht in Regelung. Es erfolgt eine sichere (elektronische) Unterbrechung der Energieversorgung.
Sicherer Betriebshalt	Die Antriebe bleiben in Lageregelung. Der Stillstand wird sicher überwacht. Bei unerwartetem Anlauf erfolgt ein sicheres Stillsetzen.
Sicher reduzierte Geschwindigkeit	Bei Überschreitung eines vorgegebenen Geschwindigkeitsgrenzwertes erfolgt ein sicheres Stillsetzen.
Sicher begrenztes Schrittmaß	Bei Überschreitung eines vorgegebenen Grenzwertes für das Schrittmaß erfolgt ein sicheres Stillsetzen.
Sicher begrenztes Absolutmaß	Bei Erreichen einer bestimmten Position erfolgt ein sicheres Stillsetzen.
Sicherer Lagegrenzwert-Ausgang	Bei Überschreiten eines vorgegebenen Lagegrenzwertes wird ein sicheres Ausgangssignal erzeugt, das anwendungsabhängig verwendet werden kann.
Sicheres Stillsetzen	Stillsetzen entsprechend der Gefahrensituation ohne externe Schütze und Zeitglieder.

Tabelle 7-4: Sicherheitsfunktionen von Antriebssystemen in Maschinen

bedeutet, dass es bei derartigen Systemen immer wieder zu Störungen bei verschiedenen Komponenten und Abläufen kommen kann, die kein Konstrukteur und kein Betreiber vorher bedacht hat und auf die kein Operator oder Pilot vorbereitet war. Daher können aus fast jedem Unfall neue Erkenntnisse über Systemzusammenhänge gewonnen werden, die dazu beitragen, ähnliche Unfälle künftig zu vermeiden. Glücklicherweise können bereits aus Beinahe-Unfällen – und nicht nur aus Unfällen – Erkenntnisse gewonnen und entsprechende Schlüsse abgeleitet werden. Allerdings besteht die Gefahr, dass als Folge neuer Erkenntnisse oft einfach nur ein zusätzliches Sicherheitssystem angefügt wird. Eine solche Überlagerung von Sicherheitssystemen macht das System als Ganzes jedoch noch komplexer und somit für den Menschen noch weniger durchschaubar [37].

Obwohl man sich darüber einig ist, dass der Mensch auch in automatisierten Systemen die Verantwortung trägt, ist der Umkehrschluss, dass mehr menschliche Überwachung von Systemen mehr Sicherheit bringt, nicht unbedingt richtig. Eine beliebte Methode, die Sicherheit von Systemen zu erhöhen, ist, verschiedene Kontrollmechanismen in redundanter Art und Weise für Bauteile auszuführen, was zum gewünschten Ergebnis führt. Für Personen gelten solche Mechanismen allerdings nicht.

Sind mehrere Personen für eine Sache verantwortlich, wird das Risiko, einen Fehler zu übersehen, nicht vermindert. Im Gegenteil, es nimmt in manchen Situationen sogar noch zu, weil sich die verantwortlichen Personen aufeinander verlassen, die ausführende Arbeit zu erledigen.

8 Sicherheitsleitlinien

Der sichere Zustand einer automatisierten Krananlage ist dann erreicht, wenn die Antriebe stillgesetzt, der Energiezufluss unterbrochen und die Bremsen eingefallen sind sowie kein automatischer Wiederanlauf möglich ist [44]. Geht man von diesem Zustand aus, so erhält man eine Krananlage, die immer still steht. Es sind also Lösungen zu finden die es einerseits ermöglichen, die bestehenden Gefährdungen für Personen zu minimieren und andererseits den Betrieb und die Flexibilität so wenig wie möglich einzuschränken.

Ausgehend von der in Kapitel 6 durchgeführten Gefahrenanalyse können nun gezielt die Gesichtspunkte in Bezug auf das Sicherheitskonzept einer automatischen Krananlage betrachtet werden, die hinsichtlich einer Gefährdung für Personen von Bedeutung sind. Diese hier vorgestellten Lösungen wiederum sind einer sicherheitstechnischen Prüfung unterzogen worden, um einerseits deren Wirksamkeit feststellen und andererseits zeigen zu können, dass von diesen Sicherheitsmassnahmen selbst keine Gefahren ausgehen.

Um aus den bekannten Gefahren und dem bekannten Risiko die richtigen Schlüsse zu ziehen, ist es sinnvoll, sich nochmals die auftretenden Gefahren anhand eines wie schon in Kapitel 4 erläuterten Kranlastspieles zu vergegenwärtigen. Dabei lassen sich die drei in Abbildung 8-1 dargestellten Teilarbeitsschritte

- Lastaufnahme,
- Kranbewegung und
- Lastabgabe

zur genaueren Untersuchung unterscheiden, wobei sich die Lastaufnahme in das *Positionieren der Last in der Übergabestation* und *Last greifen* gliedert. Bei der Kranbewegung lassen sich *horizontale* und *vertikale Bewegungen* unterscheiden. Die Lastabgabe gliedert sich in *Lösen der Verbindung von Last und Lastaufnahmemittel* und *Entfernen der Last aus der Übergabestation*.

Neben den zu untersuchenden Arbeitsschritten des Lastspieles ist noch zu unterscheiden, in welchem Automatisierungsgrad der Kran betrieben wird. Dabei sind die Betriebsarten *Manuell*, *Teilautomatisiert* und *Vollautomatisiert* zu unterscheiden. In

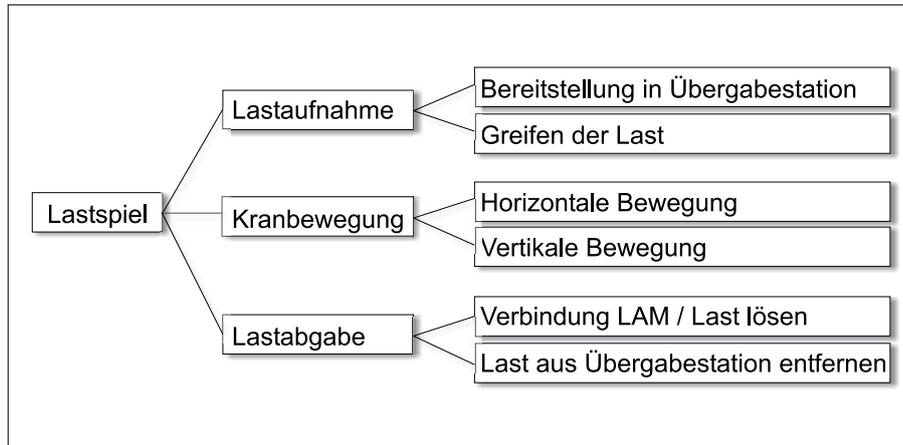


Abb. 8-1: Kranlastspiel

der teilautomatisierten Betriebsart ist wiederum zu unterscheiden, welche Übergänge zwischen der manuellen und automatisierten Betriebsart auftreten.

Der Bereich der rein manuellen Kranbedienung sei hier nur der Vollständigkeit halber aufgeführt. Dafür sind keine besonderen Sicherheitsmaßnahmen notwendig, da es sich hier um einen klassischen Kran handelt, der bei Betrieb durch den Kranführer überwacht wird.

In den folgenden Abschnitten werden die einzelnen Teilpunkte eines Kranlastspieles erläutert. Dabei wird davon ausgegangen, dass die Reihenfolge eines Lastspieles immer mit dem Bereitstellen der Last beginnt. Danach folgt die Leerfahrt in die Position für die Lastaufnahme. Abgeschlossen wird das Lastspiel mit der Lastfahrt und der anschließenden Lastabgabe.

8.1 Horizontale Kranbewegung

Hier wird darauf eingegangen, wie man das Risiko, das von den automatischen Kranbewegungen ausgeht, minimieren kann. Dabei sind horizontale und vertikale Kranbewegungen zu unterscheiden. Horizontale Kranbewegungen treten bei Leerfahrt oder Lastfahrt auf. Vertikale Kranbewegungen finden jeweils vor und nach einer Lastaufnahme oder Lastabgabe statt.

Nach Bereitstellung einer Last zur Lastaufnahme und der Quittierung dieses Vorganges setzen sich Kran und Katze gemeinsam oder getrennt in Bewegung, nachdem der Kran durch einen Leitreechner oder durch einen manuellen Kranruf einen Fahrauftrag zur Position für die Lastaufnahme erhalten hat. Dabei muss nicht unterschieden werden, ob der Kran sich im teil- oder vollautomatisierten Modus befindet, da in beiden Fällen die gleiche automatische Bewegung vorliegt.

Um eine Kollision mit Personen oder anderen Elementen der Umwelt zu vermeiden, ist für horizontale Kranbewegungen das Fahren in höchster Laststellung vorgesehen. Diese Vorgabe wird erfüllt, wenn automatische Kranbewegungen in einem Raum min-

destens 2,7m oberhalb des Personenbereichs ablaufen. Zusätzlich darf der Abstand zu Hindernissen in alle Richtungen eine Entfernung von 0,5m nicht unterschreiten [DIN 292-1], damit hier keine Gefährdungen durch Kollisionen mit Elementen der Umwelt auftreten.

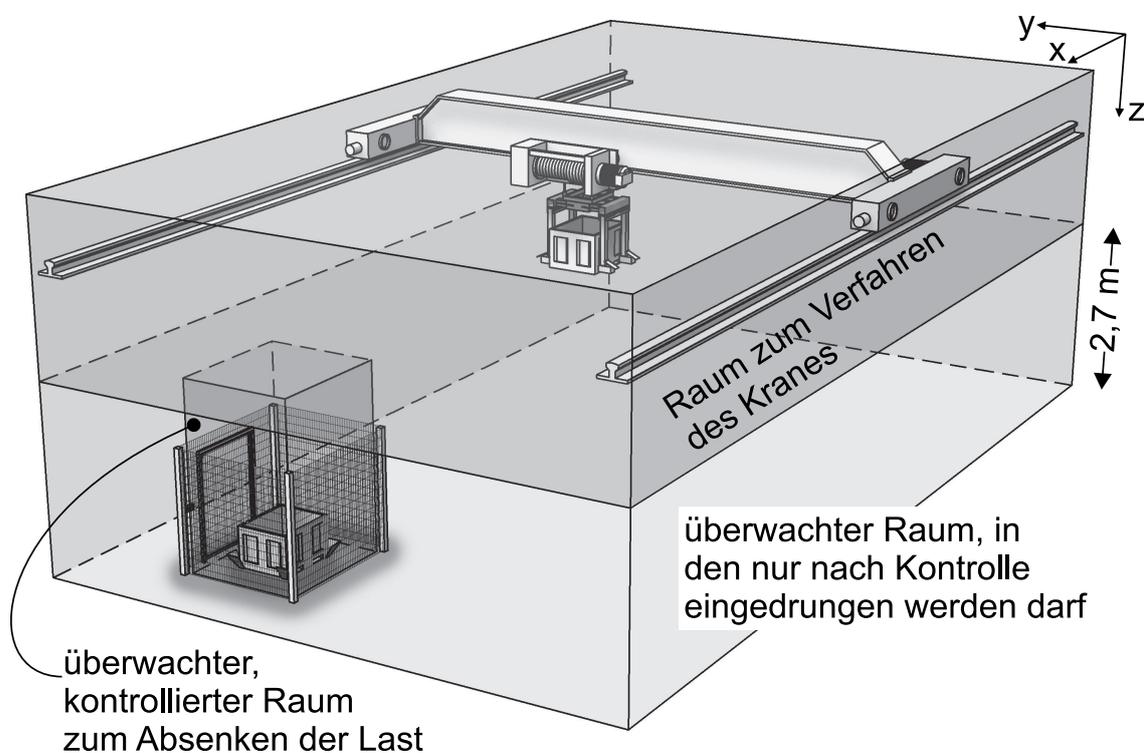


Abb. 8-2: Sichere Raumstruktur

So erhält man, wie in Abbildung 8-2 dargestellt, einen überwachten und kontrollierten Raum über einem sog. Schutzraum, in dem sich Menschen aufhalten. Dieser Raum zum Verfahren des Kranes ist frei von Hindernissen, womit eine Kollision mit anderen Elementen der Umwelt weitestgehend ausgeschlossen werden kann. Bei einer Gefahrenanalyse für dieses Konzept stellt sich das Problem, wie ein unbeabsichtigtes Verlassen des Kranes aus seinem Bewegungsraum und ein unbeabsichtigtes Eindringen anderer Elemente der Umwelt in den Verfahrraum verhindert werden können. Für ein unbeabsichtigtes Verlassen des Kranes aus seinem Bewegungsraum kann eine Verriegelung zwischen Krankatze und Lastaufnahmemittel ein ungewolltes Absenken der Last durch Steuerungsfehler, evtl. das Versagen des Hubwerks (Versagen der Bremse, Bruch der Antriebswelle, Seilriss) oder das Kippen des Motors in den Personenbereich, verhindern und somit die Sicherheit des Systems zusätzlich erhöhen. Für Verriegelungen zwischen Krankatze und Lastaufnahmemittel gibt es bereits viele bewährte und erfolgreich getestete Systeme. Solch eine Verriegelung muss selbstsicher gestaltet sein, d.h. dass sie im energielosen Zustand sicher greift, damit unter allen Umständen der sichere – also verriegelte – Zustand erreicht wird. Hier können

beispielsweise federgeführte Haken oder Bolzen, wie in Abbildung 8-3 dargestellt, die elektromagnetisch entriegelt werden, eine Lösung darstellen. Durch eine geeignete Führung des Lastaufnahmemittels gegen seitliches Schwingen (aus Gründen der Übersicht nicht in der Abbildung dargestellt) kann erreicht werden, dass die Bolzen oder Haken sich immer in der sicheren Position befinden. Bei einem Einsatz von Verriegelungen ist jedoch darauf zu achten, dass bei einem Fehlverhalten vom System keine größere Gefahr ausgeht als von einem System ohne Verriegelung. So darf bei einem Absenken der Last ohne vorher geöffnete Verriegelung das Seil von der Trommel nicht abgewickelt werden. Dies kann jedoch wiederum durch die Schlaffseilsicherung des Hubwerks verhindert werden.

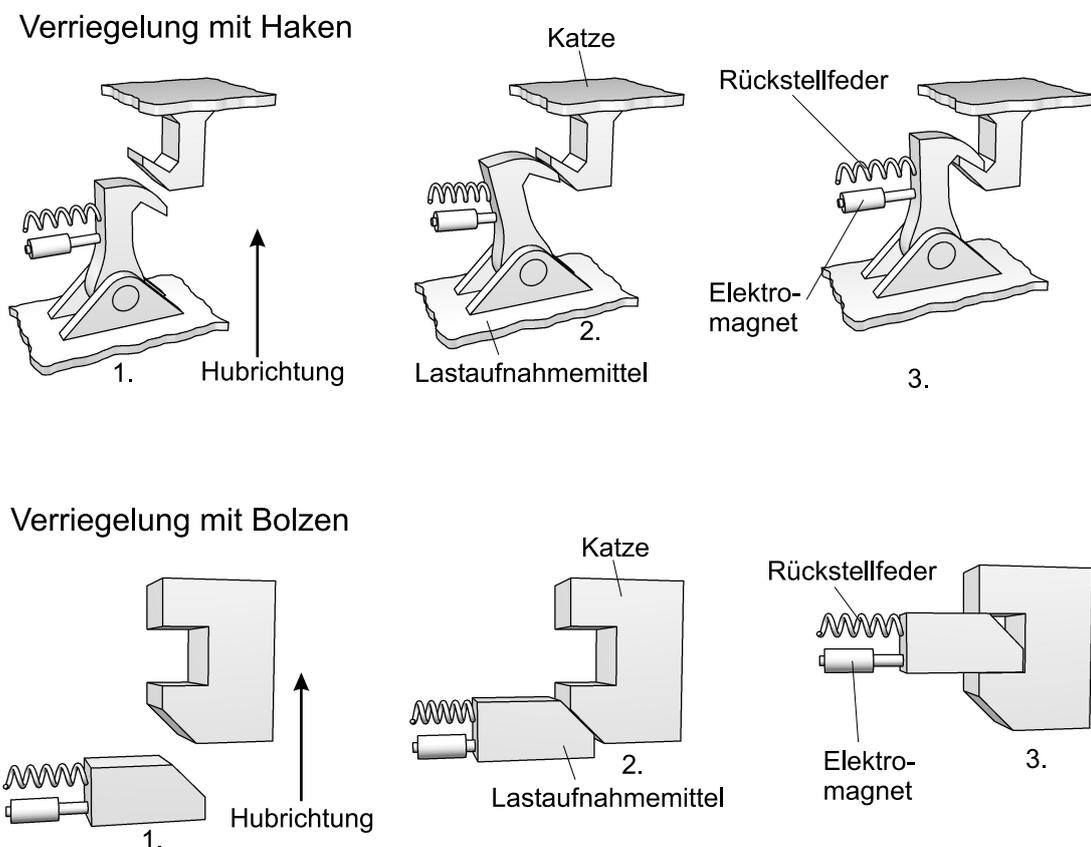


Abb. 8-3: Mögliche selbstsichere Verriegelungen

Hat man ein Kranfeld mit mehreren Kranbrücken oder Kranbrücken mit mehreren Krankatzen, so sind Kollisionen von Krankatzen oder Kranbrücken untereinander, hervorgerufen durch Fehler im Steuerungs- oder Wegmesssystem, zu verhindern. Dies kann durch Näherungsschalter an Lanzen und Endschalter verhindert werden. Ein Ausfall dieser Sensoren, z.B. durch einen Drahtbruch, stellt einen aktiven Fehler dar, der das Stillsetzen des Kranes zur Folge haben muss. Passive Fehler dieser Sensoren werden dann nur bei einem gleichzeitigen Fehler der Kransteuerung zu Gefährdungen

führen.

Betreibt man ein Kransystem mit mehreren Kranbrücken auf einer Kranbahn und diese gemischt manuell und automatisiert, so ist darauf zu achten, dass es zwischen Kranen, die in verschiedenen Modi betrieben werden, keine Beeinträchtigungen gibt. Da ein automatisch fahrender Kran die zukünftigen Bewegungsabläufe eines manuell bedienten Kranes nicht vorhersehen kann, ist hier ein gewisses Gefahrenpotential vorhanden. Lösbar ist dies, indem sich ein automatisch bedienter Kran nur bis zu einem bestimmten Bereich an einen manuell bedienten Kran und umgekehrt nähern darf. Dieser Sicherheitsabstand richtet sich nach der Geschwindigkeit und dem Bremsvermögen der beiden Krane, ohne einen Lastabsturz zu provozieren. Ein Mindestabstand von einem halben Meter, wie in Abbildung 8-4 dargestellt, wie auch zu anderen Hindernissen, ist auf jeden Fall einzuhalten. Demnach muss auch einem manuell bedienten Kran im Umfeld von automatisiert fahrenden Kranen die Position der automatisiert fahrenden Krane jederzeit vorliegen, um ggf. eine Kollision verhindern zu können. Liegen die Positionsdaten nicht vor oder ändern sich diese trotz eingeschalteter Antriebe nicht, darf keine Kranbewegung stattfinden.

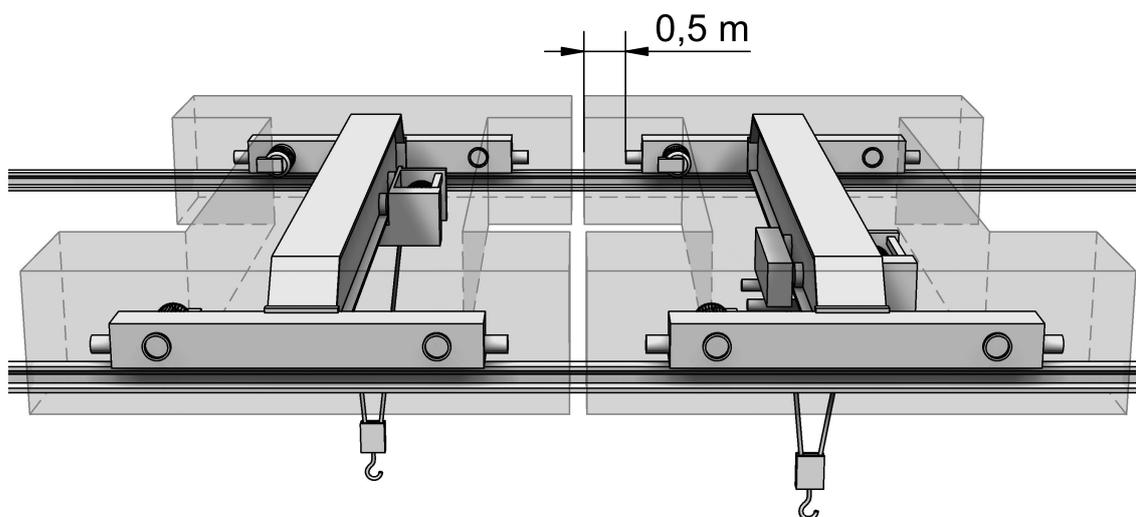


Abb. 8-4: Sicherheitsabstand

Bekannte und ortsunveränderliche Hindernisse im Bewegungsraum des Kranes müssen durch Umfahrsteuerungen umgangen werden. Dabei sind die Positionen der Katze und Kranbrücke durch ein absolutes Wegmesssystem zu überwachen, damit durch einen Stromausfall kein Verlust der Positionsdaten oder Fehlpositionierungen durch falsche Referenzierungen auftreten können. Bei absoluten Wegmesssystemen bleibt die jeweils erreichte Position im System erhalten oder ist leicht wieder herzustellen. Fehler im Steuerungssystem, die eine falsche Interpretation der Positionsdaten zur Folge haben, können allerdings nur schwer erkannt werden. Daher sind, wie später

beschrieben, Sicherheitssteuerungen und die unten beschriebenen Hilfsmittel zur redundanten Positionsüberprüfung zu verwenden.

Ein unbeabsichtigtes Eindringen in den Verfahrraum des Kranes ist technisch sehr aufwendig zu lösen, weshalb hier eine Lösung durch hinweisende Sicherheitstechnik und entsprechende Einarbeitung des Personals zum Erreichen der Sicherheit angestrebt wird. Eine technische Lösung erfordert ein dreidimensionales Abtasten des Verfahrraumes nach Hindernissen. Dazu sind Sensoren, wie z.B. Laserscanner, an fünf Seiten, nämlich den vier Seitenflächen und auf der Unterseite, anzubringen, um in alle Bewegungsrichtungen eine Raumbewachung zu ermöglichen. Ein Sicherungssystem dieser Art ist einerseits wegen der hohen Investitionskosten unwirtschaftlich und andererseits auch wegen seiner schweren Einstellbarkeit durch nicht immer gleiche Abstände zu Hindernissen nicht zuverlässig zu realisieren. Die Flexibilität und Verfügbarkeit der Anlage wäre damit sehr beeinträchtigt, was dem Grundgedanken, ein automatisiertes flurfrees Fördersystem zu verwenden, grundlegend widerspricht. Die hinweisende Sicherheitstechnik und entsprechende Einarbeitung des Personals sind nach Ansicht der Berufsgenossenschaft ausreichend, da auch bei manuell bedienten großen Brückenkränen nicht der ganze Verfahrraum des Kranes durch den Kranführer von seinem Führerstand aus kontrolliert werden kann. Es sind also entsprechende Verhaltensregeln beim Gebrauch großer Gegenstände, die in den Verfahrraum des Kranes hineinragen können, wie z.B. Leitern oder Montagegerüste, erforderlich. Die Praxis im Bereich von großen Brückenkränen hat gezeigt, dass das verbleibende Restrisiko vertretbar ist.

Vor einer horizontalen Kranbewegung sind also die vertikale Position des Lastaufnahmemittels und dessen Verriegelung in höchster Laststellung zu überprüfen. Außerdem ist für die Hindernisfreiheit des Fahrweges zu sorgen, um sicher zu stellen, dass sich der Kran in einem freien Fahrbereich befindet.

8.2 Vertikale Kranbewegung

Vertikale Kranbewegungen sind, genauso wie horizontale Kranbewegungen, vom Personenbereich zu trennen. Eine automatische vertikale Kranbewegung darf nur stattfinden, solange der Kran sich über einem überwachten kontrollierten Raum zum Absenken der Last befindet. Überwachte und kontrollierte Bereiche erhält man durch eingezäunte oder anders abgesicherte Übergabestationen. Innerhalb dieser Bereiche bewegt sich die Last in einem gesicherten Raum, damit es nicht, wie im Fehlerbaum der Abbildungen 6-1 bis 6-5 dargestellt, zu einer Kollision zwischen Kran und Mensch kommt. Eine genauere Beschreibung der Übergabestationen findet sich nachfolgend in Abschnitt 8.6.

Bei den vertikalen Kranbewegungen ist ebenfalls zu beachten, dass keine Fehler aus

Teachvorgängen oder Fehler des Wegmesssystems wirksam werden. Um sicher zu stellen, dass ein Absenken einer Last nur innerhalb des kontrollierten und überwachten Raumes stattfindet, ist die Position der Krankatze mit einem diversitären System vor einer automatischen vertikalen Bewegung zu überprüfen. Hierzu bietet sich z.B. ein Lichttaster zwischen Katze und Übergabestation an. Befindet sich die Katze an der richtigen Position, wird das Lichtsignal des Lichttasters durch einen Reflektor, der an der Übergabestation befestigt ist, reflektiert. Somit wird eine Freigabe für das Absenken einer Last erteilt. Der Ausfall dieses Systems birgt keine weiteren Gefahren, da in diesem Fall keine Kranbewegung gestattet wird. Die Empfindlichkeit der Lichttaster kann so eingestellt werden, dass eine Reflexion von anderen Gegenständen im Raum ausgeschlossen werden kann. Sie dürfen ohnehin durch den Sicherheitsabstand von einem halben Meter nicht so nah an den Verfahrraum des Kranes heranreichen.

Weiterhin sind vor und während des Absenkens einer Last noch weitere Zustände zu prüfen. Es ist sicherzustellen, dass Kranbrücke und Katze vor und während des Hubvorganges nicht in Bewegung sind. Dies kann durch einen kontinuierlichen Vergleich der Soll- und Istwerte der Positionsdaten oder durch die oben beschriebene redundante Positionsüberwachung erreicht werden. Sollte sich die Position von Kranbrücke oder Katze während des Hubvorganges ändern, ist der Hub sofort zu beenden.

Zusätzlich ist vor dem Absenken des Lastaufnahmemittels zu prüfen, ob ein Kranzugriff auf die Übergabestation erfolgen darf. Erst nachdem eine Freigabe von der Übergabestation vorliegt, darf das Lastaufnahmemittel in diese Übergabestation abgesenkt werden. Eine Freigabe darf erst dann erfolgen, wenn sich kein Mensch in der Übergabestation befindet und die Zugänge geschlossen und überwacht sind. Weiterhin muss beim Absenken von Lasten in die Übergabestation eine Belegungsprüfung erfolgen, damit nicht zwei Lasten aufeinandergestellt werden können.

Wird ein leeres Lastaufnahmemittel abgesenkt, um eine Last aufzunehmen, sind die Positionen der Greifer am Lastaufnahmemittel zu überprüfen, damit nicht der Greifmechanismus des Lastaufnahmemittels und die Last kollidieren. Außerdem ist die Lastfreiheit des Lastaufnahmemittels zu prüfen, damit nicht zwei Lasten in der Übergabestation kollidieren.

Beim Anheben von Lasten oder des leeren Lastaufnahmemittels ist die Freigängigkeit der Last zu prüfen, um ein Verklemmen oder Verhaken der Last am Boden oder anderen Elementen der Umwelt, z.B. an Zentrierschrägen zur Positionierung der Last oder Zäunen, zu erkennen. Damit wird die Selbstzerstörung der Anlage verhindert. Die Freigängigkeit der Last wird mit der Überlastsicherung des Hubwerks bereits geprüft, so dass hier keine weiteren Maßnahmen erforderlich sind.

Zusätzlich ist es sinnvoll, für Senkvorgänge die Schlaffseilsicherung zur Feststellung von Kollisionen bei vertikalen Bewegungen zu verwenden, damit der Senkvorgang

beendet wird, falls die Last unvorhergesehen aufsetzt. Es ist allerdings zu vermerken, dass bei schweren Lasten dies keinen Personenschutz darstellt, da die Personen dann vor der Schlaufseilerkennung verletzt werden. Auf diese Weise können nur noch ein Kippen der Last und damit auch Folgegefährdungen, wie z.B. ein Herabfallen von Gegenständen, verhindert werden.

Wird der Kran im teilautomatisierten Modus betrieben, ist bei vertikalen Bewegungen besonders der Übergang vom manuellen in den automatisierten Modus zu betrachten. Hubbewegungen außerhalb von Übergabestationen können auch im teilautomatisierten Betrieb ab einer Höhe von 2,7m automatisch ablaufen. So ist der Bediener nicht darauf angewiesen den Hubvorgang bis zu Ende zu beobachten, sondern nur innerhalb des Bereiches, in dem Gefahren für Personen auftreten können. Wenn die Last noch nicht in höchster Laststellung verriegelt ist und sich bereits Personen unterhalb dieser schwebenden Last aufhalten, entsteht bei dieser Betriebsart ein erhöhtes Risiko. Ein mechanischer Defekt bei Seil oder Hubwerk würde hier ggf. zum Unfall führen. Das verbleibende Restrisiko wird allerdings als sehr gering angesehen.

Ein automatisches Absenken der Last außerhalb von Übergabestationen, auch nur auf Teilhöhen, verbietet sich von selbst, da hier die Verriegelung aufgehoben wird und somit deren Schutzwirkung aufgehoben ist. Hier darf nur unter Kontrolle eines Bedieners gearbeitet werden.

8.3 Lastaufnahme

Die Lastaufnahme gliedert sich in das Bereitstellen der Last an dem Ort, an dem diese vom Kran aufgenommen werden soll, und in das Greifen der Last durch das Lastaufnahmemittel (LAM). Unter „Greifen der Last“ wird hier das Herstellen einer formschlüssigen Verbindung zwischen Last und Lastaufnahmemittel verstanden. Bei vollautomatisiertem Betrieb hat das Bereitstellen der Last in Übergabestationen zu erfolgen. Diese sind so anzuordnen, dass Menschen, wie bereits oben beschrieben, durch die automatisierte vertikale Kranbewegung nicht gefährdet werden. In Abschnitt 8.6 wird eine Übergabestation genauer beschrieben.

Das Bereitstellen einer Last kann manuell oder automatisiert durch Flurfördertechnik erfolgen. Bevor eine Last in der Übergabestation positioniert wird, ist zu überprüfen, ob diese bereit ist eine Last aufzunehmen und ob die Übergabestation bereit zum Betreten oder zur automatischen Bereitstellung der Last ist. Die Bereitschaft der Übergabestation ist immer dann gegeben, wenn kein Kranzugriff vorliegt, um Gefährdungen für Personen durch ein sich absenkendes Lastaufnahmemittel auszuschließen.

Um zu verhindern, dass ein Zutritt zu einer Übergabestation erfolgt, wenn diese durch

einen Kranzugriff belegt ist, ist die Zugangstür zur Übergabestation zu überwachen. Bei einem Öffnen der Tür ist die Kranbewegung dann unverzüglich still zu setzen. Einen höheren Sicherheitscharakter haben Türzuhaltungen, die die Tür erst nach Beendigung des Kranzugriffes auf die Übergabestation freigeben. Damit ließe sich auch der Vorteil einer erhöhten Verfügbarkeit realisieren, da der Kran in seiner Tätigkeit nicht unabsichtlich durch Personen beeinträchtigt wird.

Befindet sich der Mitarbeiter für eine manuelle Bereitstellung der Last in der Übergabestation, ist sicherzustellen, dass kein Zugriff durch einen Kran auf diese Übergabestation erfolgt. Ein Kranzugriff darf nur erfolgen, wenn der Kran eine Freigabe zum Zugriff von der Übergabestation erhalten hat. Diese darf nur, wie bereits oben beschrieben, gegeben werden, wenn eine Quittierung für den Bereitstellungsvorgang der Last in der Übergabestation vorliegt.

Damit es zu keiner Kollision von Last und Lastaufnahmemittel bzw. Ladehilfsmittel kommt, sind diese richtig zueinander zu positionieren. Die richtige Positionierung der Last in der XY-Ebene kann auf sehr einfache Weise durch Zentrierschrägen erfolgen, die das Positionieren der Last nur an einer bestimmten Stelle innerhalb der Übergabestation ermöglichen. Weiterhin kann auch ein Greifsystem mit großen Greiftoleranzen Fehler aus einer schlechten Positionierung ausgleichen. Die richtige Positionierung in der Z - Achse (Höhe des LAM zur Last) kann durch optische Sensoren, die sich an der Kontur des Ladehilfsmittels orientieren oder durch Schalter, die beim Aufsetzen auf das Ladehilfsmittel das Hubwerk stillsetzen, erfolgen.

Ist die Last in der Übergabestation positioniert, muss dieser Vorgang vom Mitarbeiter quittiert werden, damit der Kran wieder auf die Übergabestation zugreifen kann. Mit dieser Quittierung bestätigt der Mitarbeiter, dass er die Last richtig in der Übergabestation positioniert hat und sich nach dem Schließen der Tür keine weiteren Personen in der Übergabestation befinden. Die Quittierung kann nur erfolgen, wenn die Tür zu Übergabestation geschlossen ist. Das Quittieren darf nur über einen von außen erreichbaren Schalter erfolgen, damit der Mitarbeiter, der die Last in der Übergabestation positioniert, diese erst verlassen muss.

Ist die Last in der Übergabestation positioniert und ist dieser Vorgang quittiert, fährt der Kran zur Übergabestation und senkt das Lastaufnahmemittel ab, um die Last zu greifen. Für eine erfolgreiche Lastaufnahme ist zunächst auf eine richtige Positionierung von Ladehilfsmittel (z.B. Gitterbox, Palette) und Lastaufnahmemittel (Greifer) zueinander zu achten, damit ein formschlüssiger Greifvorgang stattfinden kann. Nur das formschlüssige Greifen kann als sicher betrachtet werden, da dieses auch bei einem Energieverlust die Last sicher hält.

Für den richtigen Greifvorgang sind die richtige Positionierung in der XY Ebene (Position des Lastaufnahmemittels über der Last) und die richtige Positionierung in

der Z Achse (Höhe des Lastaufnahmemittels zur Last) zu überprüfen. Die Positionierung in XY-Ebene erfolgt, wie bereits oben beschrieben, über Zentrierschragen. Die Überprüfung der richtigen Position in Z-Richtung kann durch vielerlei optische und taktile Sensoren erfolgen. Ein Lösungsvorschlag ist das Abtasten der Geometrie durch Lichttaster [45],[46].

Wie in Abbildung 8-5 dargestellt, werden hier zwei Lichttaster übereinander am Lastaufnahmemittel montiert. Wird das Lastaufnahmemittel abgesenkt, erhält man je nach Position des Lastaufnahmemittels zum Ladehilfsmittel unterschiedliche Rückmeldungen der Lichttaster. Ein Schließen des Greifmechanismus ist dann erst erlaubt, wenn die unteren Lichttaster kein Hindernis für die Greifer melden und die oberen Lichttaster das Vorhandensein eines Ladehilfsmittels bestätigen.

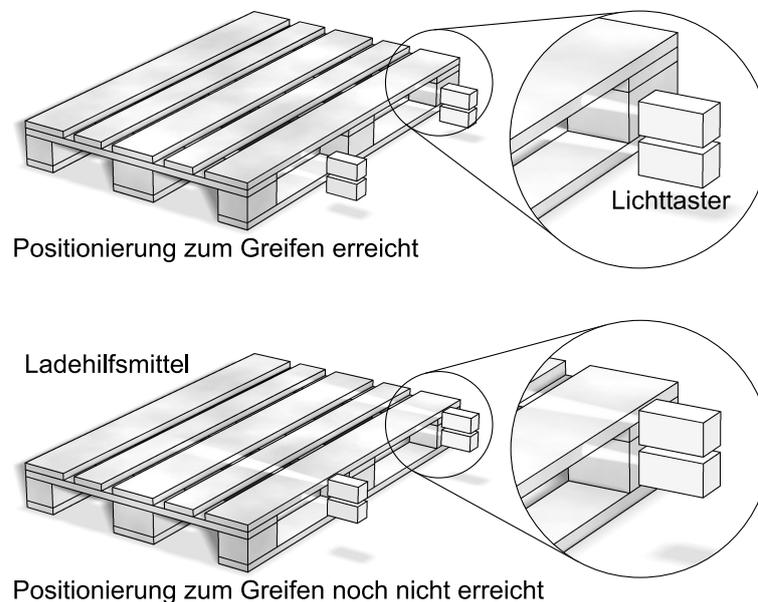


Abb. 8-5: Positionierung von LAM und Last über Lichttaster

Eine weiterhin sehr praktische Lösung stellt ein Lastaufnahmemittel dar, das sich selbst über der Last zentriert, und somit Positioniertoleranzen ohne aufwendige Sensorik ausgleicht. Auf diese Weise wird ein formschlüssiges und sicheres Greifen der Last ermöglicht [45],[46].

Neben dem Greifvorgang ist auch die zu transportierende Last auf ihre Transportfähigkeit im automatisierten System zu überprüfen. Die zu greifende Last besteht aus einem Ladehilfsmittel und dem zu transportierenden Gut. Dabei darf das Ladehilfsmittel nicht zu groß sein, um Kollisionen mit dem Lastaufnahmemittel zu vermeiden. Darüber hinaus darf das Ladehilfsmittel nicht zu klein sein, damit ein korrekter formschlüssiger Greifvorgang stattfinden kann, und das Ladehilfsmittel richtig mit dem Lastaufnahmemittel verbunden ist. Weiterhin müssen Lastaufnahmemittel und Ladehilfsmittel zum formschlüssigen Greifen geeignet sein.

Um die oben genannten Punkte wirkungsvoll während des Betriebes überprüfen zu können, ist eine Vielzahl optischer oder taktiler Sensoren zur Überprüfung einer erforderlichen Greifgeometrie notwendig. Andere Punkte, wie der ordnungsgemäße Zustand einer Euro-Palette, sind sehr schwer automatisiert zu überprüfen. Daher ist es sinnvoll, in einem Betrieb standardisierte Behälter zu verwenden, die den Ansprüchen eines automatisierten Transportes genügen. Lasten auf nicht sicheren Ladehilfsmitteln, wie zum Beispiel Holzpaletten, sind, wie in Abbildung 8-7 dargestellt, für den automatischen Weitertransport auf eine sichere Adapterpalette aus Metall oder Kunststoff zu setzen. Dadurch können beliebige Lasten in den automatisierten Materialfluss sicher eingeschleust werden. Auf diese Weise wird nicht nur die Sicherheit des Kranbetriebes, sondern auch die Flexibilität der Anlage beträchtlich erhöht, da eine uniforme Ladeeinheitenbildung vorliegt. Diese standardisierten Adapterpaletten können einer periodischen Kontrolle einfach unterzogen werden, um hier sicherheitsgefährdende Beschädigungen frühzeitig zu erkennen. Weiterhin kann man auf diese Weise die Belastungen der verwendeten Ladehilfsmittel kontrollieren, wodurch ein rechtzeitiger Austausch am Ende der Lebensdauer veranlasst werden kann. In Verbindung mit einem geschlossenen Lastaufnahmemittel ergibt sich, wie nachfolgend beschrieben, eine sicher transportierbare Einheit.

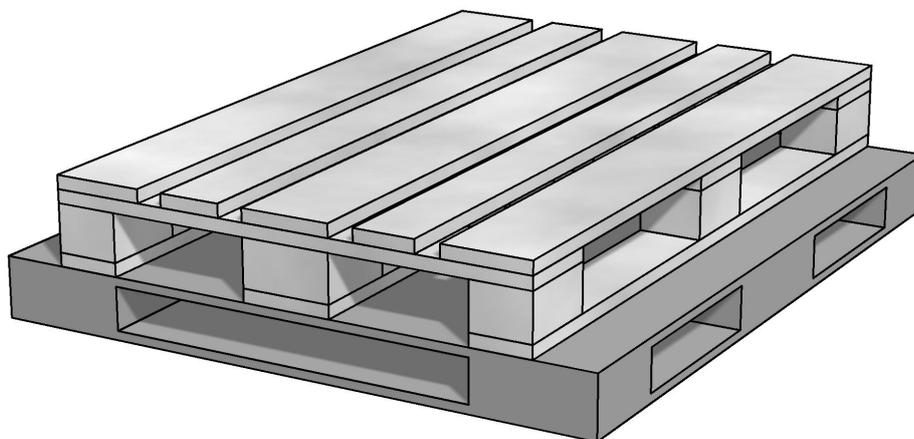


Abb. 8-6: Unsichere Palette auf sicherer Adapterpalette

Die Integration der Adapterpalette in den innerbetrieblichen Materialfluss erfolgt an den Schnittstellen zur automatisierten Krananlage. Diese Schnittstellen liegen entweder innerhalb eines Betriebes oder an der Schnittstelle zur Außenwelt, z.B. Wareneingang oder Warenausgang.

Wird die Schnittstelle zur Krananlage in den Bereich des Wareneingangs gelegt, können ohne Mehraufwand Güter, die durch den Vorgang des Entladens ohnehin gehandhabt werden müssen, mittels Gabelstapler oder Hubwagen auf die Adapter-

palette gestellt werden. Liegt die Schnittstelle im innerbetrieblichen Bereich, kann die Europalette über Palettendoppler, die zum Auf- und Abstapeln von bzw. auf Trägerpaletten verwendet werden, auf die Adapterpalette gehoben werden. Dies ist dann besonders günstig, wenn sich die Europalette bereits auf einer Rollenbahn befindet. Genauso lässt sich Übergabe von einem Regalbediengerät oder anderen Hubeinrichtungen nutzen, um eine Europalette auf eine Adapterpalette abzusetzen. Für ein manuelles Aufdoppeln eignen sich Elektrohubwagen oder Handhubwagen. Die Adapterpaletten müssen an den Schnittstellen zur automatisierten Krananlage gepuffert werden.

Neben dem richtigen Ladehilfsmittel ist auch die Richtigkeit der Last sowie deren Gewicht und Größe zu überprüfen. Das Gewicht wird durch eine Standard-Überlastsicherung geprüft. Bei zu hohem Gewicht wird der Hub durch die Steuerung verweigert. Der Größe der Last kommt eine erhebliche Bedeutung zu. Ist die Last zu groß, kann diese mit Elementen der Umwelt kollidieren, da das Lichtraumprofil des Fahrweges überschritten wird. Ist die Last zu klein, kann diese aus einem Behälter, wie z.B. einer Gitterbox, herausfallen. Um diese Gefährdungen auszuschließen, ist ein geschlossenes Lastaufnahmemittel, wie in Abbildung 8-7 beispielhaft dargestellt, erforderlich. So kann die Aufnahme zu großer Lasten ausgeschlossen werden, da das Lastaufnahmemittel vor einem Greifvorgang mit der Last kollidiert. Zusätzlich werden durch geschlossene Lastaufnahmemittel oder Ladehilfsmittel sehr kleine Lasten daran gehindert herabzufallen. Das Positionieren zu großer Lasten in der Übergabestation kann ausgeschlossen werden, indem die Öffnung der Übergabestation so gestaltet wird, dass nur Lasten bis zu einer bestimmten Größe durch diese Öffnung transportiert werden können.

Nach einer erfolgreichen Lastaufnahme mit den oben beschriebenen Überprüfungen ist weiterhin ein Absturz der Last oder von Teilen der Last in den Personenbereich auf jeden Fall zu verhindern, da beim automatisierten Kranbetrieb auch über Personen hinweggefahren wird, was eine besondere Gefährdung darstellt. Wie gesagt, sind dazu eigensichere Schutzmaßnahmen, wie ein geschlossenes Lastaufnahmemittel oder geschlossene Ladehilfsmittel, geeignet. Zur sicheren Verbindung zwischen Lastaufnahmemittel und Krankatze sind ein Mehrseilbetrieb und ein Mehrgreiferbetrieb von Bedeutung. Eine gesicherte Kraftkette vom Motor bis zur Seiltrommel muss durch eine Bremse an der Seiltrommel gewährleistet sein. Mit einer zusätzlichen Maßnahme kann das Lastaufnahmemittel unterfangen oder durch eine mechanische Verriegelung mit der Katze gesichert werden.

Wird die Krananlage manuell oder teilautomatisiert genutzt, ist bei einer manuellen Lastaufnahme auszuschließen, dass nicht geeignete Ladehilfsmittel für einen weiteren automatischen Transport verwendet werden können. Die Lastaufnahmemittel sind

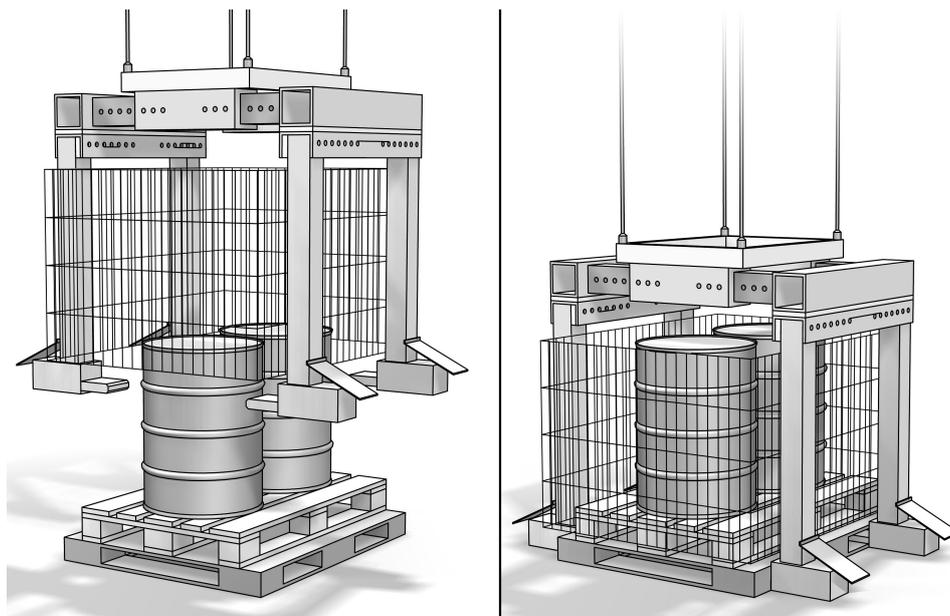


Abb. 8-7: Sichere Transporteinheit aus Adapterpalette und geschlossenem LAM

derart zu gestalten, dass nur Ladehilfsmittel gegriffen werden können, die für einen weiteren automatisierten Transport sicher sind. Dabei ist weniger die Lastaufnahme, die vom Kranführer überwacht wird, als das Ergebnis der Lastaufnahme sicherheitstechnisch zu betrachten, da dieses für die weitere automatische Handhabung von Bedeutung ist. Aus diesem Grund sind die gleichen Sicherheitsüberprüfungen, wie oben auch für den vollautomatischen Betrieb beschrieben, durchzuführen.

8.4 Lastabgabe

Die automatische Lastabgabe stellt ein geringeres Problem als die Lastaufnahme dar, denn das Ausschleusen von Elementen aus einem automatisierten System ist einfacher als das Einschleusen. Bei der Lastabgabe ist die Situation, in der das Lastaufnahmemittel die Verbindung zum Ladehilfsmittel löst, zu überprüfen. Hier darf das Lastaufnahmemittel nur dann die Verbindung zum Ladehilfsmittel lösen, wenn die Last nicht mehr schwebt, damit es zu keinem Lastabsturz kommt. So ist zu überprüfen, ob das Ladehilfsmittel auf einer geeigneten Stelle steht. Hierbei kann die Überlastsicherung als Waage prüfen, ob das Lastaufnahmemittel lastfrei ist. Weiterhin kann auch mit dem oben beschriebenen Lichttastersystem festgestellt werden, ob das Ladehilfsmittel schon auf festem Grund steht oder noch, an dem Lastaufnahmemittel hängend, in der Luft schwebt. Sobald die Last nicht mehr an dem Lastaufnahmemittel hängt, können die Greifer geöffnet werden. Eine Überprüfung der Lastfreiheit aller einzelnen Greifer ist erforderlich, um festzustellen, dass auch alle Greifer geöffnet werden können. Sollten hier Differenzen vorliegen, ist davon auszugehen, dass die Last nicht eben steht, und somit auch nicht freigegeben werden darf.

Weiterhin darf, wie bei der Lastaufnahme, der Kran nicht mehr in Bewegung sein. Vor dem Anheben des leeren Lastaufnahmemittels ist die geöffnete Position / Stellung aller Greifer zu kontrollieren, damit das Lastaufnahmemittel die Last nicht asymmetrisch wieder an nur einem Greifer anhebt und diese abstürzen kann. Generell ist beim Wiederanheben das Lastaufnahmemittel auf Lastfreiheit zu kontrollieren, um ausschließen zu können, dass noch irgendein Fremdelement am Lastaufnahmemittel verhakt ist. Hierzu kann auch die Überlastsicherung verwendet werden.

Der letzte Punkt der Lastabgabe besteht darin, die Last aus der Übergabestation zu entfernen. Hier gilt wieder, wie bei der Positionierung der Last in der Übergabestation, dass die Übergabestation bereit zum Betreten ist. Dies bedeutet, dass kein Kranzugriff vorliegen darf, damit ein Mensch, der sich gerade zum Entnehmen einer Last in der Übergabestation befindet, nicht durch das absenkende Lastaufnahmemittel gefährdet wird. Weiterhin ist zu prüfen, dass die Last vollständig aus der Übergabestation entfernt worden ist, um spätere Kollisionen zu verhindern, unabhängig ob dieser Vorgang automatisch oder manuell durchgeführt wurde. Der Vorgang der korrekten manuellen Entnahme der Last – und somit auch die Freigabe der Übergabestation – ist vom Bediener zu quittieren.

Analog zur automatischen Lastabgabe sind bei der manuellen Lastabgabe, die gleichen Kontrollen am Lastaufnahmemittel durchzuführen, da im teilautomatischen Modus bei einer anschließenden automatischen Leerfahrt keine Gefährdungen entstehen dürfen. Das gleiche gilt, wenn im automatischen Betrieb zwischenzeitlich eine manuelle Lastfahrt erfolgen sollte. Alle manuellen Tätigkeiten sind nach ihrer Beendigung zu quittieren. Dies darf nur nach Überprüfung der Lastfreiheit und der Position des Lastaufnahmemittels in höchster Laststellung erfolgen. Mit diesen Kontrollen werden einerseits der Weitertransport von Lasten, die ohne die besonderen Kontrollen der automatisierten Lastaufnahme nur für den manuellen Transport gedacht waren, und andererseits automatische Bewegungen durch einen Kranruf im personenzugänglichen Raum ausgeschlossen.

8.5 Lastaufnahmemittel

Beim Transport von Lasten mit einem Kran hat das Lastaufnahmemittel die Verbindung zwischen der Last und dem Kran herzustellen. Für den automatisierten Transport sind diese Lastaufnahmemittel mit Befestigungs- oder Greifmechanismen ausgestattet, um selbständig eine Last greifen zu können.

Für einen automatisierten Transport über Personen hinweg hat das Lastaufnahmemittel noch Schutzfunktionen zu erfüllen, die erforderlich sind, um einen Lastabsturz zu verhindern. Wie schon im vorhergehenden Abschnitt erläutert, ist es dabei wichtig, dass eine formschlüssige und somit unabhängig von der Energiezufuhr sichere Verbin-

dung zwischen Last und Lastaufnahmemittel besteht. Weiterhin muss das LAM so gestaltet sein, dass keine falschen, also zu große oder zu kleine Lasten, aufgenommen werden können.



Abb. 8-8: Lastaufnahmemittel nur für geschlossene GLT

Abbildung 8-8 zeigt beispielsweise ein Lastaufnahmemittel, das für den Transport von geschlossenen Großladungsträgern (GLT) vorgesehen ist. Diese sind einer Gitterbox mit den Maßen von 1000 x 1200 mm ähnlich. Der GLT wird hier von unten gegriffen, indem an jeder der vier Seiten ein Riegel unter das Ladehilfsmittel geschoben wird. Möchte man eine größere Fördergutflexibilität erreichen, also auch Gegenstände greifen, die auf Europaletten gestapelt sind, kann man dieses Lastaufnahmemittel wie in Abbildung 8-9 dargestellt mit einem Gitter verkleiden. Jetzt übernimmt das Gitter die Schutzfunktion gegen das Herausfallen der Last. Damit kann man mit einer Europalette, wie schon in Abschnitt 8-3 beschrieben, auf einer sicheren Adapterpalette beliebige Güter transportieren. Es ist allerdings darauf zu achten, dass die Größe der Güter nicht kleiner als die Maschenweite des Schutzgitters ist. Andere Materialien als ein Schutzgitter, wie z.B. engmaschige Netze oder Unterfangungen des ganzen Lastaufnahmemittels, sind möglich. Grundsätzlich darf keine Möglichkeit bestehen,

dass Teile der Last oder die ganze Last, bedingt durch Kollisionen oder eine falsche Ladungssicherung auf dem Ladehilfsmittel, in den Personenbereich herunterfallen.

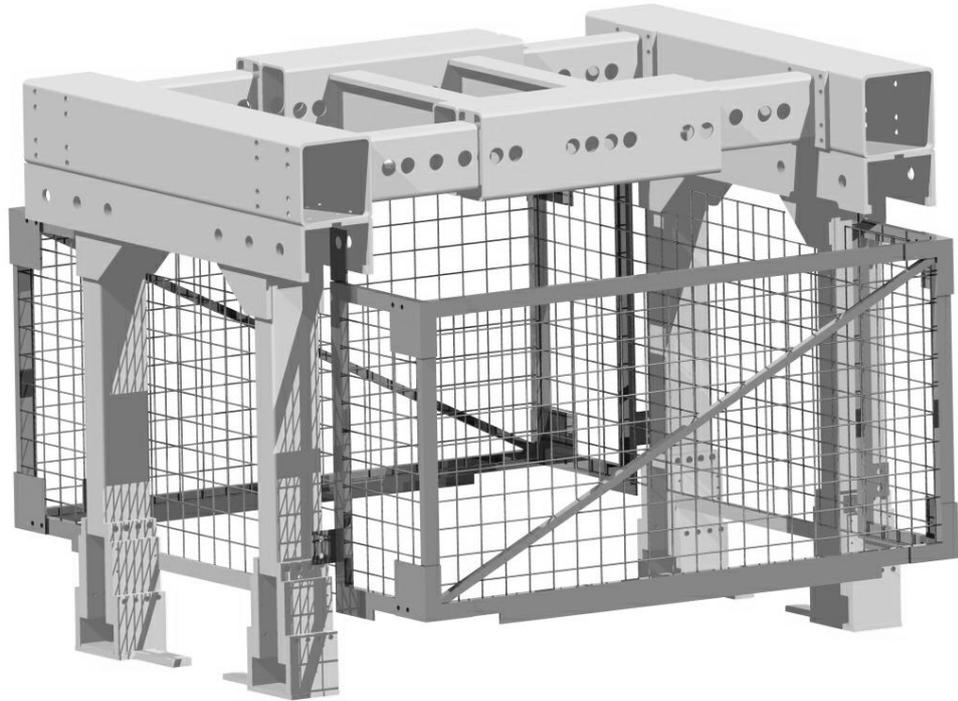


Abb. 8-9: Geschlossenes Lastaufnahmemittel

Möchte man keine große Lasten aufnehmen, sondern nur kleine, z.B. in Form von Kleinladungsträgern (VDA-KLT), so ist auch dabei zu beachten, dass keine kleinen Gegenstände herausragen oder herausfallen können. Auch hier können Lastaufnahmemittel verwendet werden, die den KLT umschließen, wenn dieser von unten gegriffen wird. Wenn der KLT von oben gegriffen werden soll, kann die Sicherheit durch Zudecken des KLT von oben durch das LAM erreicht werden.

Bei der Gestaltung des Greifmechanismus ist darauf zu achten, dass dieser ein formschlüssiges Greifen ermöglicht. Um die Sicherheit für das Verhindern eines Lastabsturzes durch ungewolltes Öffnen des Greifmechanismus zu erhöhen, kann die Leistung der Antriebe zum Öffnen der Greifer so gering ausgelegt werden, dass diese nur im lastfreien Zustand öffnen können. Eine weitere Möglichkeit besteht darin, den Reibwert zwischen Ladehilfsmittel und Greifer des Lastaufnahmemittels so weit zu erhöhen, dass die Greifer nur im lastfreien Zustand betrieben werden können. Zusätzlich verhindert eine Verriegelung der Greifer in ihrer geschlossenen Position ein ungewolltes Öffnen.

8.6 Übergabestationen

Als Schnittstelle für einen verketteten Materialfluss zwischen der automatisierten Krananlage und dem Personenbereich oder weiterer Flurfördertechnik dienen Übergabestationen, in denen die Last in das automatisierte System ein- bzw. ausgeschleust wird. Diese Übergabestationen unterliegen besonders wichtigen Sicherheitsauflagen, da hier das Gefahrenpotential durch die große Nähe von Personen zu den automatisch bewegten Maschinenteilen am größten ist.

Im ersten Schritt eines jeden Lastspieles muss eine Last an einer Übergabestation positioniert sein, damit diese vom Kran aufgenommen werden kann. Übergabestationen für automatische Krananlagen sind so auszuführen, dass Menschen den in Kapitel 6 beschriebenen Gefahren nicht ausgesetzt werden können. Durch geeignete Maßnahmen sind

- Kollision von Last oder Kran mit Personen und
- Kollision von Last oder Kran mit Teilen der Übergabestation

zu verhindern.

Aus den in Kapitel 6 beschriebenen Gefahren ergibt sich zwingend die Übergabestation so zu gestalten, dass Personen vor bewegten Kranteilen, nämlich dem Lastaufnahmemittel mit oder ohne Last beim Heben oder Senken, geschützt werden. Die Absicherung muss einen gesicherten und überwachten Eingangsbereich besitzen. Weiterhin muss sichergestellt sein, dass ein Absenken der Last in den Personenbereich auch immer innerhalb des gesicherten Bereiches einer Übergabestation stattfindet. Dafür ist die Kranposition auf redundante und diversitäre Art festzustellen.

Um Personen im Bereich von Übergabestationen zu schützen, bieten sich eingezäunte Bereiche an, in denen der Kran sich bewegt. Eine weitere Möglichkeit besteht darin, die Übergabestation ohne Zaun – also offen – zu gestalten, aber dann über Lichtschranken oder Lichtvorhänge im Vorfeld abzusichern. Dabei ist zu beachten, dass die Reaktionszeit des Kranes zum Stillsetzen der Antriebe bei der Einstellung des Abstands zwischen den optischen Sicherungselementen und der Übergabestation berücksichtigt wird. Mischformen aus Zaun und optischen Sensoren sind ebenfalls denkbar, wie sie in Abbildung 8-10 dargestellt sind.

Der Bereich der Übergabestation kann durch einen Zaun abgesperrt, der Zugang allerdings durch Lichtschranken gesichert sein. Zugänge sollten nach Möglichkeit so gestaltet sein, dass nur Lasten und nicht Personen den Gefahrenbereich erreichen können. Hierzu bieten sich Öffnungen für Übergabestationen an, die nur für die Größe der Last konzipiert, aber für Personen zu klein sind.

Bei der Absicherung durch einen Zaun mit einem durch eine Tür gesicherten Zugangsbereich kann man durch eine Türzuhaltung, die bei einem Kranzugriff aktiviert wird,

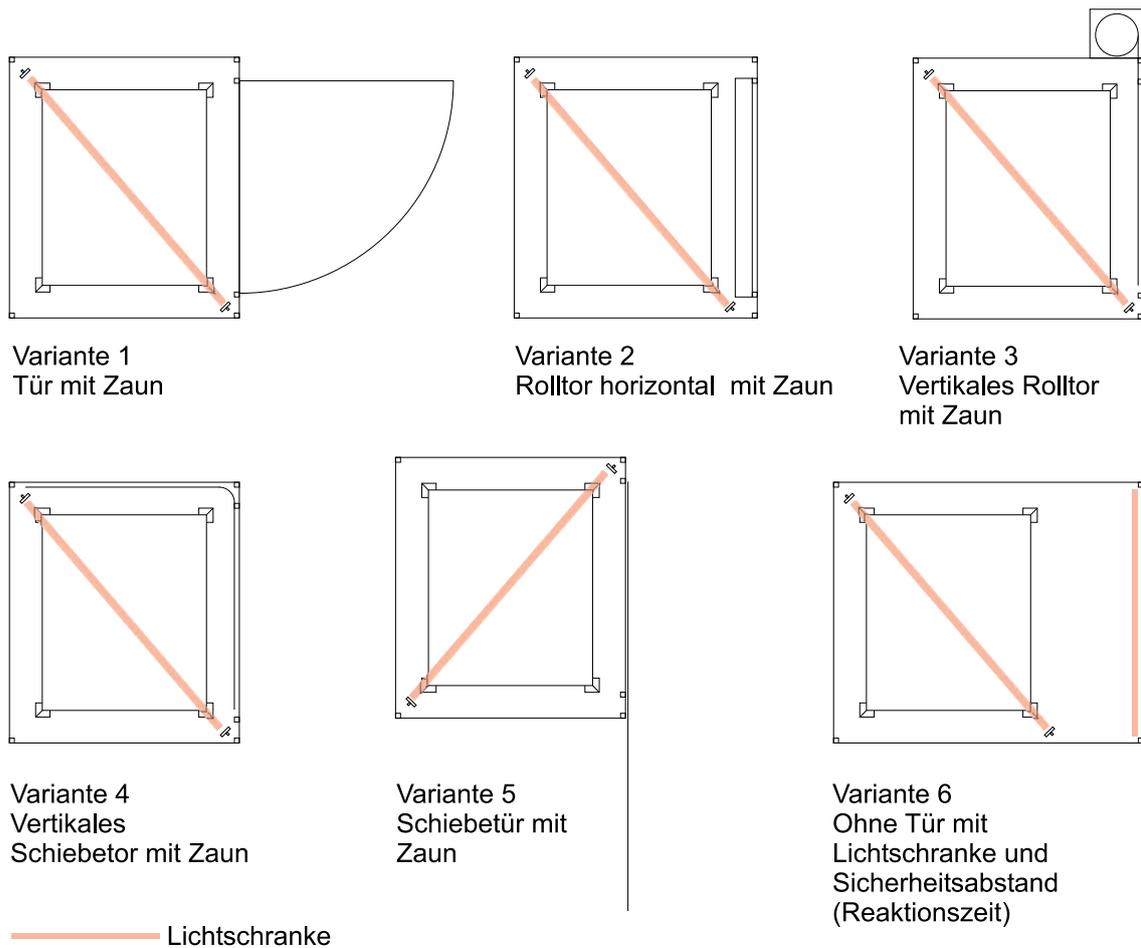


Abb. 8-10: Varianten zur Sicherung von Übergabestationen

oder durch einen Türkontaktschalter, der während eines Kranzugriffs beim Öffnen der Tür das Hubwerk stillsetzt, die geforderte Sicherheit erreichen. Aus Gründen der Verfügbarkeit des Systems ist allerdings die Türzuhaltung vorzuziehen, da hier der Kran bestimmt, wann die Übergabestation betreten werden kann, womit unnötige Störzeiten ausgeschlossen werden können.

Bei einer Schaltung, wie in Abbildung 8-11 dargestellt, werden gefahrbringende Zustände bei geöffnetem Schutzgitter durch eine Öffner-Schließer-Kombination unterbrochen bzw. verhindert. Zusätzlich wird das Sperrmittel (Zuhaltung) durch einen zwangsläufig wirkenden Positionsschalter überwacht. Die hier mit herkömmlichen Schaltplansymbolen dargestellte Logik kann auf einfache Weise im Programm der Kransteuerung implementiert werden. Die Merker $K1$ und $K2$ schalten den Freigabepfad. Wird das Schutzgitter geöffnet, werden über die Schalter $S1$, $S2$ oder $S3$ die Merker $K1$ und $K2$ auf die logische Null gesetzt. Wird nur das Sperrmittel aus der verriegelnden Position bewegt, wird der Merker $K2$ auf die logische Null gesetzt. Weiterhin können über den STOP-Schalter beide Merker auf die logische Null gesetzt

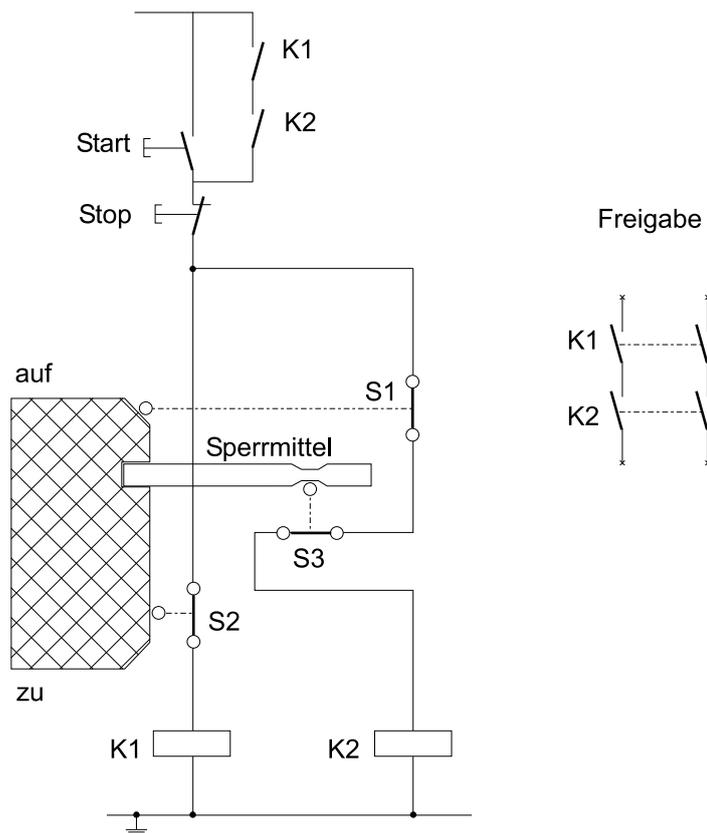


Abb. 8-11: Logik zur Absicherung von Übergabestationen

werden. Über die parallel zum Start-Taster geschalteten Merker $K1$ und $K2$ wird die Memory-Funktion erhalten, die es erlaubt bis zum Betätigen der Stop-Taste oder einem der Schalter $S1$ bis $S3$ die Merker $K1$ und $K2$ auf der logischen Eins zu halten, ohne dauerhaft den Start-Schalter betätigen zu müssen.

Soll noch eine Anlaufprüfung implementiert werden, die bei geöffneter Schutztür erfolgt, ist die in Abbildung 8-12 dargestellte Logik zu verwenden.

In diesem Fall ist die Sicherheitsfunktion auch erfüllt, wenn ein Bauteil ausfällt eintritt. Alle Fehler werden während des Betriebes oder beim Betätigen (Öffnen und Schließen) der Schutzvorrichtung durch Unterbrechung der Freigabe erkannt. Nur eine Fehlerhäufung zwischen zwei aufeinanderfolgenden Betätigungszeitpunkten kann zum Verlust der Sicherheitsfunktion führen, wobei dann nicht mehr die Ein-Fehler-Sicherheit, sondern eine Mehr-Fehler-Sicherheit abgedeckt werden müsste.

Um sicherzustellen, dass das automatische Absenken einer Last auch immer innerhalb des gesicherten Bereiches einer Übergabestation stattfindet, ist es notwendig, durch ein redundantes und diversitäres Wegmesssystem die Position von Kran und Katze zu bestimmen.

Da nur oberhalb der Übergabestationen eine redundante Positionsbestimmung notwendig ist, kann auch von einem Positionserfassungssystem gesprochen werden, denn

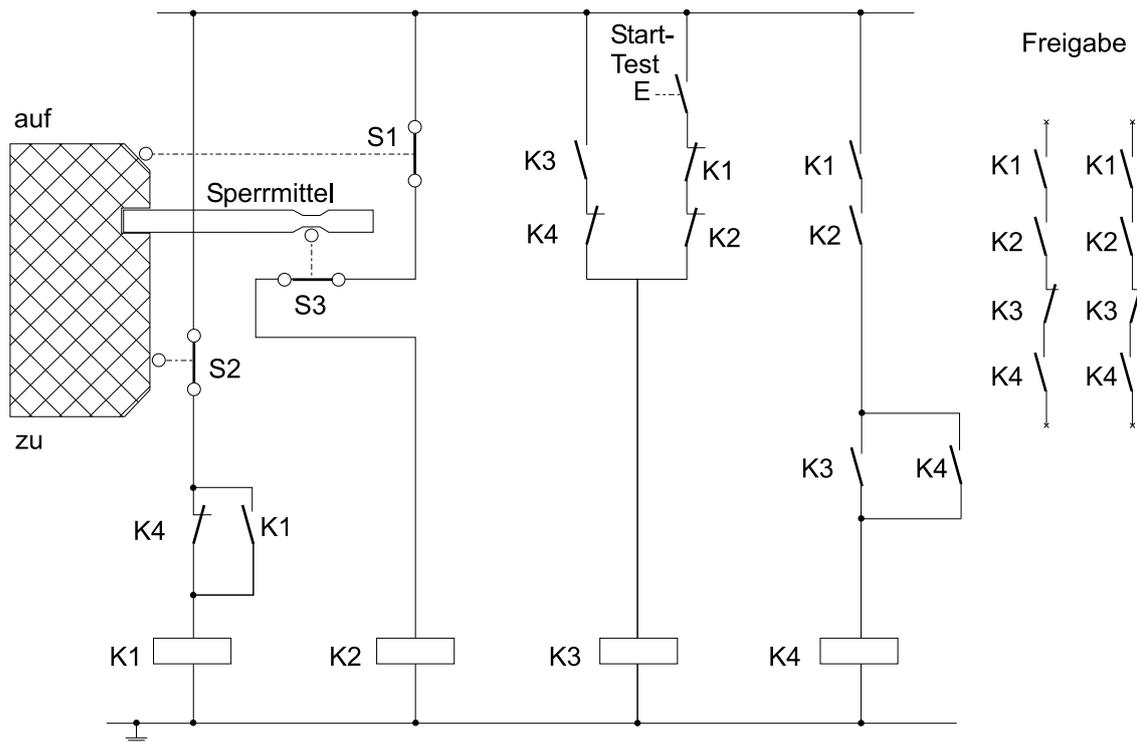


Abb. 8-12: Logik mit Anlaufstestung

es muss nur eine bestimmte Position des Kranes verifiziert werden. In den anderen Bereichen des Kranes ist diese redundante und diversitäre Positionserfassung nicht erforderlich, da hier ein Absenken in den personenzugänglichen Bereich während des automatischen Betriebes nicht stattfindet.

Die Überprüfung der Position kann auf zwei Arten erfolgen:

Zum einen kann man ein zweites Wegmesssystem implementieren und mit beiden Systemen die absolute Position der Krankatze bzw. Kranbrücke im Raum bestimmen. Sollten bei einem Vergleich der beiden Positionswerte zu große Unterschiede auftreten, ist davon auszugehen, dass ein Fehler in der Positionserfassung vorliegt.

Zum anderen man kann nur eine relative Position zur Übergabestation, z.B. mittels eines Lichttasters, bestimmen und nur so den wirklich sicherheitstechnisch relevanten Bereich redundant absichern.

Die Vorteile eines Lichttasters sind:

- Es besteht keine Möglichkeit für eine Kollision und Beschädigung.
- Eine genaue Positionskontrolle ist möglich.
- Er besitzt einen einfachen Aufbau.
- Er ermöglicht eine gute Wandelbarkeit des Systems in Hinblick auf die Flexibilität der Anlage.
- Die Lösungsvariante ist sehr kostengünstig.

Dieses System hat jedoch den Nachteil, dass die richtige Position durch Schwanken der Krankatze oder durch Verschmutzung der Reflektorspiegel nicht erkannt wird. In beiden Fällen entsteht jedoch keine weitere Gefahr, denn das System verhält sich dann so, als wenn die Kranposition zur Übergabestation nicht erreicht wäre, und der Kran senkt die Last nicht ab. Lediglich ist mit einer geringeren Verfügbarkeit des Kranes zu rechnen. Mit einer periodischen Reinigung der Reflektorspiegel, die im Zuge einer obligatorischen Inspektion der Übergabestation mit einhergeht, sollte dieser Nachteil nicht weiter ins Gewicht fallen.

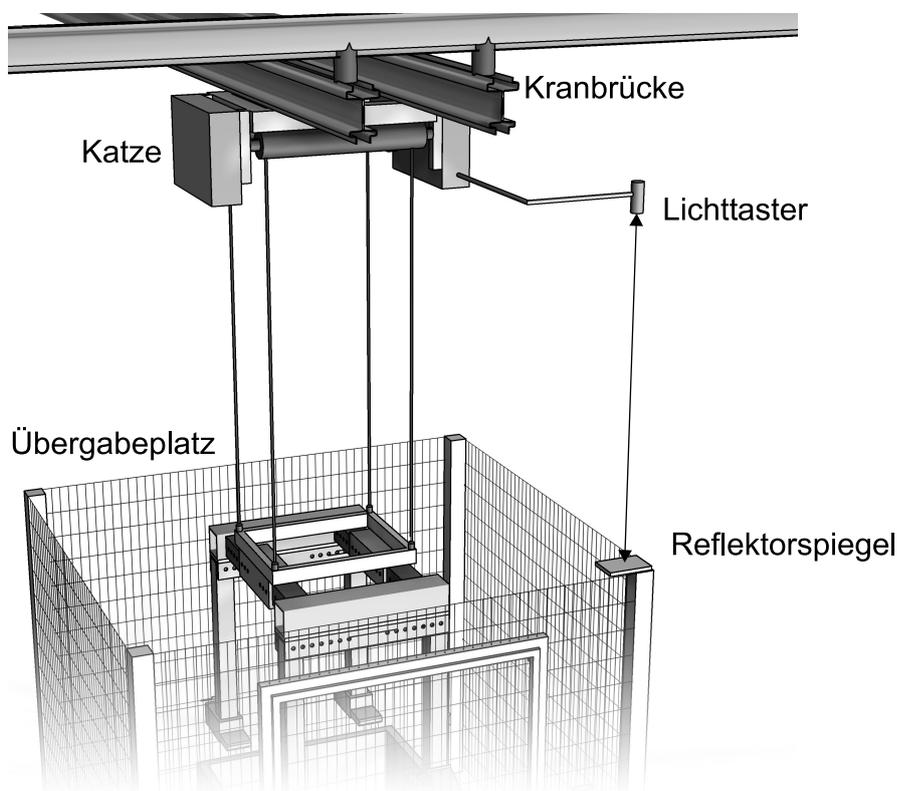


Abb. 8-13: Lichttaster zur Positionsüberwachung

Ein Ausfall des Systems während des Lastabsenkens stellt einen aktiven Fehler dar und bewirkt, dass das Absenken einer Last in den Bereich der Übergabestation gestoppt wird. Daraus resultiert jedoch keine weitere Gefahr.

Das vorliegende Konzept zur redundanten Bestimmung der Kranposition über einer Übergabestation, wie in Abbildung 8-13 dargestellt, stellt eine einfache und kostengünstige, aber dennoch sehr zuverlässige Lösung dar. Gerade im Hinblick auf die Forderung nach Wandelbarkeit bietet das System sehr große Freiheitsgrade, da die

Sensoren bei einer Neustrukturierung des Materialflusses ihre Position mit verändern und die Einrichtzeit auf einen einfach durchzuführenden Einstellprozess des Reflektorspiegels beschränkt ist.

Personen, die den Bereich der Übergabestation betreten haben, müssen beim Verlassen den ordnungsgemäßen Zustand für einen automatisierten Zugriff auf die Übergabestation quittieren. Diese Quittierung hat durch den Bediener zu erfolgen, der die Last in der Übergabestation positioniert, denn die Quittierung darf nur dann möglich sein, wenn sich, wie in Abschnitt 8-2 beschrieben, keine Personen mehr im Gefahrenbereich aufhalten. Wenn der Quittierschalter derart an der Übergabestation angebracht ist, dass dieser nur außerhalb des Gefahrenbereiches zu bedienen ist, erhält man die Gewissheit, dass sich keine Person mehr im Gefahrenbereich aufhält, wenn das Bereitstellen einer Last nur durch eine Person erfolgt. Dadurch, dass beim Quittieren die Tür der Übergabestation geschlossen sein muss, kann man eine fahrlässige Quittierung durch eine zweite Person ausschliessen.

Weiterhin ist ein Sensor zur Belegungsprüfung der Übergabestation notwendig. Damit wird geprüft, ob sich eine Last in der Übergabestation befindet und die Übergabestation für eine Laustaufnahme oder eine Lastabgabe bereit ist. Ist die Übergabestation belegt, darf nur eine Lastaufnahme erfolgen, da sonst bei einer weiteren Lastabgabe zwei Lasten aufeinander gestapelt würden. Dies stellt zwar nicht eine unmittelbare Gefahr für Personen dar, jedoch kann es so zu Schäden an der Anlage kommen, was zumindest deren Verfügbarkeit beeinträchtigt. Ist die Übergabestation nicht belegt und ist der Kran auf eine Lastaufnahme eingestellt, besteht keine Gefahr, da keine Last aufgenommen werden und keine Kollision stattfinden kann. Es sollte nur eine Fehlermeldung für eine nicht vorhandene Last abgegeben werden.

Abschließend sei noch beispielhaft in Abbildung 8-14 beschrieben, wie eine Übergabestation für den Einsatz eines automatisierten Kranes im innerbetrieblichen Behältertransport aussehen kann. Sie ist auf drei Seiten mit einem Zaun umgeben, auf der vierten Seite befindet sich die Tür für den Zugang. An der Tür ist eine Zuhaltung montiert, um den Zutritt in den Gefahrenbereich während eines Kranzugriffes zu verhindern.

Im Inneren befinden sich die Zentrierschrägen, um die genaue Positionierung der Last sicherzustellen. Eine Lichtschranke diagonal zur Abstellposition prüft die Belegung der Übergabestation.

Der Quittierschalter ist so montiert, dass dieser nur außerhalb der Übergabestation bedient werden kann, damit sich die Bedienperson während eines Kranzugriffes nicht im Inneren der Übergabestation aufhalten kann. Die redundante Überwachung der Kranposition wird mit dem oben beschriebenen Lichttaster realisiert, um sicherzustellen, dass das Lastaufnahmemittel nur in den gesicherten Bereich der Übergabestation

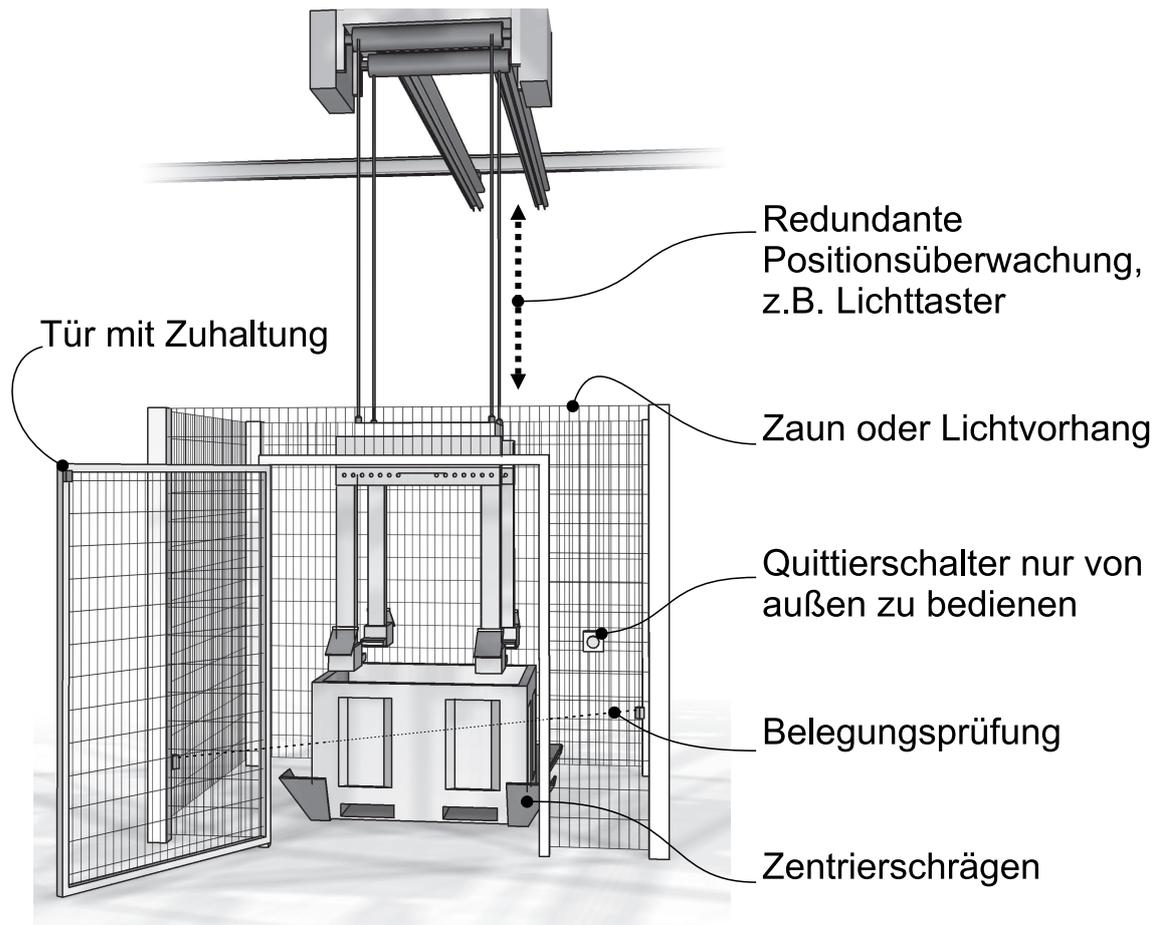


Abb. 8-14: Sichere Übergabestation und ihre Elemente

abgesenkt werden kann.

8.7 Steuerung und Kommunikation

An die Steuerung der Hubwerke und Fahrtriebe des Kranes sind besondere Anforderungen zu stellen, da sie die einzelnen oben beschriebenen sicherheitsrelevanten Überprüfungen vorzunehmen hat. Dieses Steuerungs- und Kommunikationssystem muss interne Fehler der Steuerung ausschließen, damit die Krananlage nicht in unkontrollierte Zustände gerät, die für Personen in nächster Umgebung eine große Gefahr darstellen.

In der DIN V 19251 wird bei den Fehlerklassen zwischen zufälligen, systematischen, aktiven und passiven Fehlern unterschieden. Bei dieser Betrachtungsweise spielen nur die auftretenden Fehler eine Rolle, die einen Einfluss auf die Sicherheitsfunktionen der Anlage selbst haben. Aktive Fehler bewirken durch eine geregelte Abschaltung einen direkten Übergang in den sicheren Zustand der Anlage. Hierzu zählt beispielsweise der Drahtbruch zu einem Endschalter, der durch das Ruhestromprinzip der Schaltung erkannt wird, d.h. Fehler dieser Klasse werden durch die Anlagensteuerung selbst erkannt und bedürfen keiner weiteren Maßnahme zur Beherrschung. Gefährlich sind

nach sicherheitstechnischem Verständnis passive Fehler, die die Anlage nicht in einen sicheren Zustand überführen und unentdeckt bleiben können, wenn sie nicht durch das Steuerungskonzept sicher erkannt werden [47].

Seit dem Inkrafttreten der einschlägigen Normen und Sicherheitsrichtlinien für Menschen, Maschinen und Anlagen gibt es neben den bewährten speicherprogrammierbaren Steuerungen (SPS) für die nicht-sicheren Signale der Sensoren einen oder mehrere Schaltkreise für sicherheitsrelevante Funktionen. Die Sicherheit dieser Schaltkreise wurde in der Vergangenheit grundsätzlich konventionell, d. h. mit Sicherheitsschaltgeräten, gewährleistet. Die wachsenden Anforderungen an sicherheitstechnische Funktionen und ihre zunehmende Komplexität machen den Einsatz sicherer Elektronik sinnvoll und notwendig.

Die programmierbaren Sicherheitssteuerungen bieten wesentliche Vorteile hinsichtlich Projektierung, Abnahme und Betrieb. Die Funktionen der herkömmlichen Sicherheitsschaltgeräte werden zunehmend durch von der BG bzw. vom TÜV abgenommene und verschlüsselte Softwarebausteine ersetzt. Fehler- und Diagnosetools runden die komfortable Handhabung dieses elektronischen Sicherheitssystems ab. In Verbindung mit sicheren Sensoren erhält man mit dieser Systemkombination eine sichere Komplettlösung von der Eingangs- bis zur Ausgangsseite.

Geprüfte und abgenommene Standardfunktionsbausteine für alle wichtigen Funktionen von NOT-AUS bis zur Steuerung stehen bereits heute für viele Maschinen, wie z.B. eine Presse, zur Verfügung. Sie verkürzen deren Entwicklungszeit und erleichtern die Inbetriebnahme. Zur Kommunikation mit übergeordneten Systemen oder für den Anschluss eines Visualisierungssystems stehen serielle Schnittstellen oder entsprechende Kommunikationsbaugruppen zur Verfügung.

Für die Verarbeitung der sicherheitsrelevanten Signale sind Sicherheitssteuerungen zu verwenden. Bei diesen Steuerungen besteht die zentrale Recheneinheit CPU aus mehreren unabhängig voneinander arbeitenden Mikrorechnern. Jeder Mikrorechner besteht aus einer Prozessoreinheit, einem Bussystem sowie einem Bus-Interface und bearbeitet unabhängig von den anderen Rechnern das Anwenderprogramm. Um die geforderte hohe Sicherheit zu erreichen, überwachen sich die Rechner gegenseitig. Die Eingangssignale werden verglichen. Nur bei fehlerfreiem Abgleich der Ergebnisse wird das Anwenderprogramm bearbeitet. Ist der Abgleich fehlerhaft, schaltet die Sicherheitssteuerung in den sicheren Zustand.

Ausgangssignale werden nur dann gesetzt, wenn alle Kanäle die gleichen Werte berechnet haben. Die durch die unterschiedlichen Bearbeitungszeiten beim Ein- und Auslesen der Daten der Prozessoren erforderliche Synchronisation wird vom Betriebssystem der Steuerung durchgeführt.

Die Kommunikation zwischen den einzelnen Sicherheitssteuerungen hat über ein Si-

cherheitsbussystem zu erfolgen, damit Übertragungsfehler ausgeschlossen werden. Den Anforderungen von Standard-Feldbussystemen stehen in der Sicherheitstechnik einige Besonderheiten entgegen. In der Sicherheitstechnik besteht die Forderung nach störunanfälligen, d.h. nach sicheren und daher meist gekapselten Einheiten. Diese speziellen Anforderungen der Sicherheitstechnik münden heutzutage in kleine Dimensionen der Netze für störunanfällige bzw. sichere Einheiten und eine lokale Konfiguration der Sicherheitskomponenten.

Sicherheitsbussysteme verhindern Fehler in der Kommunikation, z.B. durch das „Umkippen“ eines Bits, die zu einer Gefährdung des Menschen führen können. Verschiedene Sicherheitsprotokolle sowie interne Plausibilitätsprüfungen und das redundante Rechnen mit zwei verschiedenen CPUs ermöglichen es, dass von der logischen Verarbeitung keine Gefährdungen ausgehen.

Um geeignete Sicherheitsbussysteme für den automatisierten Kranbetrieb zu finden, wurde in Bereichen der Automobil- und Luftfahrtindustrie nach vorhandenen Systemen gesucht, da hier schon viele Sicherheitsfunktionen über Bussysteme realisiert sind, wie z.B. „fly by wire“ oder „steer by wire“. Auch in der Kranentwicklung besteht ein eindeutiger Trend, elektronische Systeme statt mechanische Komponenten einzusetzen und darin immer mehr Sicherheitsfunktionen zu realisieren. Dies bedeutet eine ständig steigende Komplexität der Elektronikkomponenten mit einer schnell wachsenden Anzahl von Funktionen, Sensoren und Aktoren. Diesen Anforderungen wird ein herkömmliches zentrales Steuergerät nicht mehr gerecht, denn durch die Flexibilität, die einem automatisierten Kransystem abverlangt wird, ist eine klassische Parallelverdrahtung aller sicherheitsrelevanten Signale nicht mehr möglich. Zudem erfordert die wachsende Zahl von Funktionen eine leichte Erweiterbarkeit des Systems. Zusätzlich ist die Berücksichtigung von allgemeinen Rahmenbedingungen, wie z.B. schnellere Entwicklungs- und Reaktionszeiten auf neue Marktanforderungen sowie hohe Qualitätsanforderungen bei niedrigen Systemkosten, eine weitere Grundvoraussetzung für die Steuerung eines Kransystems. Die Lösung ist eine Vernetzung der verschiedenen Elektronikbaugruppen über einen Hochleistungs-Datenbus zur Reduzierung des Verkabelungsaufwandes und Mehrfachnutzung von Sensordaten [48].

Für die sicherheitsgerichteten Hochleistungsdatenbussysteme wurden verschiedene Datenprotokolle entwickelt.

Einige wichtige Vertreter dieser Bussysteme sind:

- Das **byteflight**-Protokoll [49], das von der BMW AG in Zusammenarbeit mit den Firmen Motorola, Siemens AG und ELMOS AG für sicherheitsrelevante Anwendungen entwickelt wurde. Es bietet ein deterministisches Verhalten, eine flexible Bandbreitennutzung und Systemerweiterbarkeit, eine hohe Übertra-

gungsrates und Datenintegrität, eine durch die optische Übertragung sehr hohe Störsicherheit bei der Kommunikation, einen Software-Download über den Bus und eine Online-Diagnosemöglichkeit.

- FlexRay [50], das von einem Konsortium (bestehend aus BMW, DaimlerChrysler, Motorola und Philips) entwickelt wurde, soll einmal für die Karosserie-Kontrolle in Autos eingesetzt werden. Es unterscheidet sich von den anderen Bussystemen dadurch, dass seine Funktionalität in zeit- und ereignisgesteuerte Aktivitäten aufgeteilt ist. FlexRay kann sowohl eine „aktive“ Stern-Topologie oder eine „passive“ Bus-Topologie aufweisen. FlexRay ist aufgrund seiner Mischung aus zeit- und ereignisgesteuerter Operation interessant und aufgrund der industriellen Herkunft seiner Entwickler potentiell bedeutsam.
- INTERBUS Safety [51]: Bei INTERBUS muss der Anwender neben sicheren E/A-Einheiten lediglich eine auch nachträglich installierbare Überwachungseinheit (SafeControl) in den Bus integrieren, die ausschließlich die Sicherheitstechnik überwacht.
- HIMA Safe Ethernet [52] von der Firma HIMA, das besonders in den Bereichen der sicheren Anlagenautomatisierung und der Verfahrenstechnik Anwendung findet.
- SafetyBus p von Pilz [53], ein echter Sicherheitsbus auf Controlled Area Network(CAN)-Technologie basierend, der zusammen mit Sicherheitssteuerungen ein in sich geschlossenes Sicherheitssystem bildet.

Das Steuerungsprogramm, ein ebenso wichtiger Bestandteil der Steuerung, ist so zu gestalten, dass es selbst wiederum Plausibilitätsprüfungen vornimmt, um Programmierfehler zu erkennen und unwirksam werden zu lassen. Als selbstverständlich werden qualitätssichernde Maßnahmen, wie sie in DIN V 19250 und IEC 61508 für sicherheitsgerichtete Software dargestellt sind, bei der Programmierung begleitend angewandt. Eine geeignete Simulation sowie ein intensiver Testbetrieb sind eine unbedingte Voraussetzung dafür, das Produkt in den Normalbetrieb überführen zu können. Geeignete Methoden zur Erstellung sicherheitsgerichteter Software finden sich bei [54] und [55].

Bei der Gestaltung des Steuerungsprogramms ist die Modularität, wie sie die Anlage schon durch ihre mechanische Ausprägung besitzt, beizubehalten. Dabei kann eine zentrale oder dezentrale Steuerungsarchitektur verwendet werden.

Bei einer zentralen Steuerungsarchitektur werden die einzelnen Komponenten über sichere Eingabemodule und einen Sicherheitsbus mit der Steuerung verbunden. Die zentrale Steuerung übernimmt in diesem Fall alle Überwachungs- und Steuerungsaufgaben. Sollte in einem Bereich des Sicherheitssystems ein Fehler auftreten, kann dieser Bereich, bei entsprechender Aufteilung in Sicherheitsgruppen, über die siche-

ren Eingabemodule einzeln stillgesetzt werden, ohne die Sicherheitseinrichtungen der anderen Bereiche außer Betrieb zu nehmen.

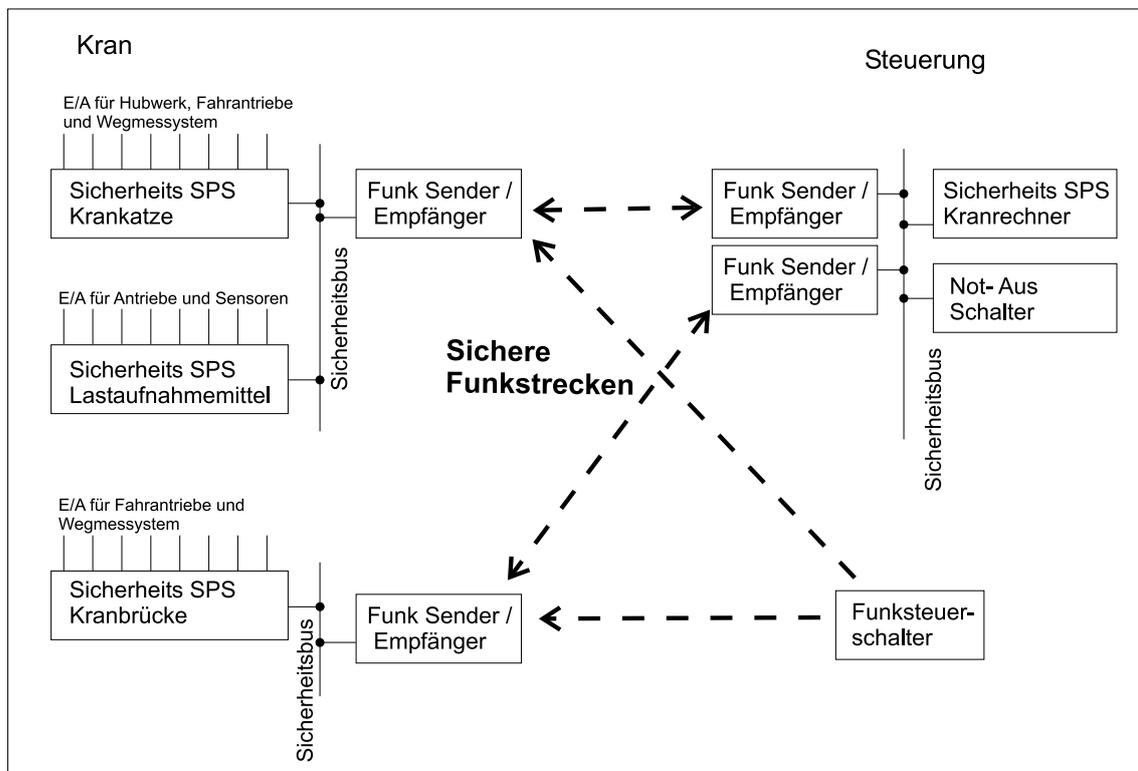


Abb. 8-15: Sicheres Steuerungskonzept

Im Falle einer dezentralen Steuerung, wie in Abbildung 8-15 dargestellt, hat jede größere Krankomponente, wie Hubwerk, Katzantrieb, Lastaufnahmemittel und Kranbrückenantrieb, seine eigene Steuerung. Dabei kommunizieren die einzelnen Steuerungen über den Sicherheitsbus miteinander. Eine Steuerung erhält den Master-Status und kontrolliert somit das System. Für die teilautomatisierten Betriebsarten werden Funksteuerschalter mit gesicherten Funkstrecken verwendet.

Falls man einen weiteren Kran in das System implementieren möchte, ist der Vorteil dieser Anordnung, dass hier eine größere Flexibilität des Systems vorliegt und die Komponenten nur über Standardprotokolle miteinander kommunizieren. Diese Standardprotokolle beschränken sich dann auf die Freigaben und Quittierungen zum Heben, Senken, Kranfahren sowie auf die Lastaufnahmemittel zum Öffnen und Schließen. Der eigentliche Ablauf wird dann über die lokale Steuerung abgewickelt, bis entweder dieser die Freigabe durch einen Sicherheitsfall entzogen oder die Tätigkeit vollendet und als fertig quittiert wird.

Dies hat auch den Vorteil, dass solche einzelnen Programmabschnitte einfacher auf ihre Sicherheit hin überprüft werden können. Dabei sind Abschnitte für die Kranbrücke, die Krankatze und das Lastaufnahmemittel für die Kranseite sowie die Über-

	Katze verfahren	Kran verfahren	Anfahren	Bremsen	LAM leer senken
NOT-HALT: vorhanden / nicht vorhanden	nicht vorhanden	nicht vorhanden	nicht vorhanden	nicht vorhanden	nicht vorhanden
Bremse: gelüftet / geschlossen	gelüftet	gelüftet	gelüftet	gelüftet	geschlossen
Zielposition: vorhanden / nicht vorhanden	vorhanden	vorhanden	vorhanden	vorhanden	vorhanden
Ist-Position: vorhanden / nicht vorhanden	vorhanden	vorhanden	vorhanden	vorhanden	vorhanden
Verriegelung LAM - Katze: verriegelt / nicht verriegelt	verriegelt	verriegelt	verriegelt	verriegelt	nicht verriegelt
Horizontaler Endschalter: erreicht / unerreicht	nicht erreicht	nicht erreicht	nicht erreicht	nicht erreicht	
Türkontakt: offen / geschlossen					geschlossen
Türverriegelung ÜG.: aktiviert / deaktiviert					aktiviert
Belegung Übergabestation : belegt / nicht belegt					belegt
Quittierung des Bedieners: vorhanden / nicht vorhanden					vorhanden
Greiferposition: geöffnet / geschlossen					geöffnet
LAM Belegung: belegt / nicht belegt					nicht belegt
Vertikale Ist-Position: vor- handen / nicht vorhanden					vorhanden
Vertikale Soll-Position: vor- handen / nicht vorhanden					vorhanden
Schlaffseil: vorhanden / nicht vorhanden					nicht vorhanden
Positionssignal LAM Last: Position o.k. / nicht o.k.					
Last / Überlast: vorhanden / nicht vorhanden / zu schwer	keine Überlast	keine Überlast	keine Überlast	keine Überlast	Last vorhanden
Endschalter vertikal: erreicht / nicht erreicht					nicht erreicht

Tabelle 8-1: Signalmatrix 1

gabestationen für die flurgebundene Seite zu nennen. Wenn jede dieser Baugruppen mit Eingabemodulen für dezentrale Baugruppen ausgestattet ist, und wenn diese Baugruppen über ein Sicherheitsbussystem miteinander verbunden sind, erhält man ein in sich geschlossenes in einzelne Gruppen abschaltbares Steuerungssystem.

Die Unterteilung in kleine Gruppen hat sich außerdem als sinnvoll erwiesen, weil dadurch bei Störungen nur einzelne Bereiche abgeschaltet werden und andere Sicherheitsfunktionen weiterlaufen können. So können einzelne Kranelemente abgeschaltet

	LAM voll senken	Greifer öffnen	Greifer schließen	LAM leer heben	LAM voll heben
NOT-HALT: vorhanden / nicht vorhanden	nicht vorhanden	nicht vorhanden	nicht vorhanden	nicht vorhanden	nicht vorhanden
Bremse: gelüftet / geschlossen	geschlossen	geschlossen	geschlossen	geschlossen	geschlossen
Zielposition: vorhanden / nicht vorhanden	vorhanden			vorhanden	vorhanden
Ist-Position: vorhanden / nicht vorhanden	vorhanden			vorhanden	vorhanden
Verriegelung LAM - Katze: verriegelt / nicht verriegelt	nicht verriegelt	nicht verriegelt	nicht verriegelt	nicht verriegelt	nicht verriegelt
Horizontaler Endschalter: erreicht / unerreicht					
Türkontakt: offen / geschlossen	geschlossen	geschlossen	geschlossen	geschlossen	geschlossen
Türverriegelung ÜG.: aktiviert / deaktiviert	aktiviert	aktiviert	aktiviert	aktiviert	aktiviert
Belegung Übergabestation : belegt / nicht belegt	nicht belegt				
Quittierung des Bedieners: vorhanden / nicht vorhanden	vorhanden			vorhanden	vorhanden
Greiferposition: geöffnet / geschlossen	geschlossen	geschlossen	geöffnet	geöffnet	geschlossen
LAM Belegung: belegt / nicht belegt	belegt		belegt	nicht belegt	belegt
Vertikale Ist-Position: vorhanden / nicht vorhanden	vorhanden			vorhanden	vorhanden
Vertikale Soll-Position: vorhanden / nicht vorhanden	vorhanden			vorhanden	vorhanden
Schlaffseil: vorhanden / nicht vorhanden	nicht vorhanden			nicht vorhanden	nicht vorhanden
Positionssignal LAM Last: Position o.k. / nicht o.k.		o.k.	o.k.		
Last / Überlast: vorhanden / nicht vorhanden / zu schwer	Last vorhanden	Last nicht vorhanden	Last nicht vorhanden	Last nicht vorhanden	Last vorhanden keine Überlast
Endschalter vertikal: erreicht / nicht erreicht	nicht erreicht			nicht erreicht	nicht erreicht

Tabelle 8-2: Signalmatrix 2

werden, ohne dass allgemeine Sicherheitsfunktionen ausgelöst werden.

Eine Übersicht über die von einer Kransteuerung zu kontrollierenden Zustände für die einzelnen Kranaktivitäten ist in den Tabellen 8-1 und 8-2 zusammengefasst. Eine Aktion des Kranes darf nur durchgeführt werden, wenn alle entsprechend geforderten Zustände für diese Aktion erreicht sind.

8.8 Leitlinienkatalog

Eine vollständige Übersicht über die in diesem Kapitel vorgeschlagenen Maßnahmen zur Sicherheit automatisierter Krananlagen im personenzugänglichen Umfeld ist in den folgenden Tabellen zu einem Leitlinienkatalog zusammengefasst.

Für jeden Teilarbeitsgang werden in der linken Spalte die jeweils zu überprüfen oder zu erreichenden Zustände aufgezählt. Die dazugehörigen Lösungsvorschläge werden in der rechten Spalte aufgelistet.

Teilarbeitsgang Last in Übergabestation positionieren

zu erreichen	Lösungsvorschläge
kein Betreten der Übergabestation bei Kranzugriff	Absperrung der Übergabestation durch Zäune oder Sichern durch Lichtschranken im Reaktionsabstand zum Gefahrenbereich
	Türen in Absperrung mit Türzuhalten, die bei Kranzugriff aktiviert wird oder Türkontaktschalter, der während eines Kranzugriffs beim Öffnen der Tür das Hubwerk stillsetzt, und solange kein Kranzugriff vorliegt, keine Reaktion auslöst
zu erreichen	Lösungsvorschlag
keine falsche Position der Last innerhalb der Übergabestation	Zentrierschrägen für die Last in der Übergabestation

Teilarbeitsgang: Kranbewegung horizontal

zu erreichen	Lösungsvorschläge
keine Kollision mit der Umwelt (Hindernisfreiheit des Fahrweges)	Fahren in höchster Laststellung
	Fehler im Wegmesssystem durch Redundanz mit Näherungsschaltern und Endschaltern verhindern
	Abstand von mindestens 0,5m zu allen Umweltelementen
	Umfahrsteuerungen für bekannte feste Hindernisse
	Hinweisende Sicherheitstechnik, um unvorhergesehene Hindernisse im Fahrraum des Kranes zu verhindern oder optische Sensoren zum dreidimensionalen Abtasten des Raumes auf Hindernisse
zu prüfen	Lösungsvorschlag
Lastaufnahmemittel in höchster Laststellung	Verriegelung des Lastaufnahmemittels in höchster Laststellung
	Endschalter am Lastaufnahmemittel

Teilarbeitsgang: Kranbewegung vertikal

Allgemein	
zu erreichen	Lösungsvorschläge
keine Kollision mit der Umwelt (Hindernisfreiheit des Hubweges)	Automatische vertikale Bewegungen nur in abgesperrten und überwachten Bereichen (Übergabestationen)
	Schlaffseilsicherung zur Erkennung von Kollisionen beim Absenken
zu erreichen / zu prüfen	Lösungsvorschlag
richtige Position der Last über der Aufgabe- / Abgabeposition	Redundante Kontrolle der Position der Katze z.B. mit Lichttaster zwischen Katze und Übergabestation
zu prüfen	Lösungsvorschläge
keine Person in der Übergabestation	Nur von außen erreichbare Freigabetaster für Bediener an der Übergabestation
	Türzuhaltung, um Zutritt während der Übergabe zu verhindern
	Türkontaktschalter mit Not-Halt verknüpft
	Belegungsprüfung durch Lichtschranken
zu erreichen	Lösungsvorschlag
redundante Hubhöhenmessung	Endschalter für höchste und niedrigste Hubposition des Lastaufnahmemittels
zu prüfen	Lösungsvorschläge
Katze und Kranbrücke nicht in Bewegung	Verriegelung der Fahrwerke, während Lastaufnahmemittel nicht in höchster Laststellung
	Kontrolle der Kranposition mit Lichttaster zwischen Katze und Übergabestation
	zusätzlich Werte des Wegmesssystems auf Veränderung kontrollieren
Heben von Lasten	
zu prüfen	Lösungsvorschlag
Freigängigkeit der Last (Verklemmen am Boden)	Erkennen durch Überlastsicherung
Senken von Lasten	
zu prüfen	Lösungsvorschlag
keine Last in der Übergabestation	Belegungsprüfung durch Lichtschranken
	Sensorik am Lastaufnahmemittel, die eine Belegung der Übergabestation feststellt, z.B. Bilderkennungssystem
Senken des leeren Lastaufnahmemittels	
zu prüfen	Lösungsvorschlag
Richtige Stellung der Greifer am Lastaufnahmemittel	Erkennen durch Prüfschalter

Teilarbeitsgang: Lastaufnahme (manuell und automatisch)

Allgemein	
zu prüfen / zu erreichen	Lösungsvorschläge
Richtige Positionierung in der XY - Ebene (Position des Lastaufnahmemittels über der Last)	Positionierung über Wegmesssystem
	Zentrierhilfen am Lastaufnahmemittel
	Greifsystem mit großen Toleranzen im Greifbereich
	Zentrierschrägen zur Ausrichtung der Last in der Übergabestation
Optische Sensoren, die sich an der Kontur des Ladehilfsmittels orientieren	
zu prüfen / zu erreichen	Lösungsvorschlag
Richtige Positionierung in der Z - Achse (Höhe des LAM zur Last)	Schalter, die beim Aufsetzen auf das Ladehilfsmittel das Hubwerk stillsetzen
	Optische Sensoren, die sich an der Kontur des Ladehilfsmittels orientieren
Ladehilfsmittel	
zu prüfen	Lösungsvorschlag
Ladehilfsmittel zum automatischen Transport geeignet (Kein Herausfallen oder Überstehen der Last möglich)	Nur standardisierte und geschlossene Ladehilfsmittel formschlüssig greifbar, geeignet für den automatisierten Transport verwenden oder
	Hinweisende Sicherheitstechnik für geeignete Ladehilfsmittel
	Geschlossene Lastaufnahmemittel verwenden
zu prüfen	Lösungsvorschlag
Ladehilfsmittel nicht beschädigt	Wiederholte Prüfungen in festgelegten Zeiträumen zur Kontrolle der Ladehilfsmittel
	Hinweisende Sicherheitstechnik mit Hinweistafel auf intaktes Ladehilfsmittel
	Optische Sensoren zur Kontrolle
zu prüfen	Lösungsvorschlag
Ladehilfsmittel zum formschlüssigen Greifen geeignet	Optische oder taktile Sensoren, die eine erforderliche Greifgeometrie am Ladehilfsmittel überprüfen
zu prüfen	Lösungsvorschlag
Ladehilfsmittel nicht zu groß	Lastaufnahmemittel als Lehre verwenden. Durch ein vorzeitiges Aufsetzen auf dem zu großen Ladehilfsmittel wird die Last nicht gegriffen.
zu prüfen	Lösungsvorschlag
Ladehilfsmittel nicht zu klein	Überprüfung der Größe des Ladehilfsmittels mit optischen Sensoren (Lichttaster oder Scanner)

Teilarbeitsgang: Lastaufnahme (manuell und automatisch) Fortsetzung

Last	
zu prüfen	Lösungsvorschlag
Last nicht zu schwer	Überlastsicherung
	Leistungsaufnahme des Hubwerks kontrollieren
	Last in Übergabestation wiegen
zu prüfen	Lösungsvorschlag
Last nicht zu groß	Geschlossene Lastaufnahmemittel
	Erkennen durch optische Sensoren
	Einhausung und Öffnung der Einhausung der Übergabestation so gestalten, dass keine größeren Teile als erlaubt einzuschleusen sind
zu prüfen	Lösungsvorschlag
Last nicht zu klein	Geschlossene Lastaufnahmemittel
	Geschlossene Ladehilfsmittel
zu prüfen	Lösungsvorschlag
Korrektur Zugriff des Greifmechanismus (formschlüssiges Greifen)	Geschlossene Position der Greifer überprüfen
	Greifer verriegeln

Teilarbeitsgang: Lastabgabe (manuell und automatisch)

zu erreichen	Lösungsvorschläge
Last nicht mehr schwebend	Überlastsicherung als Waage verwenden
	Schwache Greiferantriebe, die wegen der aufliegenden Last sich nicht öffnen lassen
	Lichttaster zur Kontrolle der Stellung von Ladehilfsmittel und Lastaufnahmemittel zueinander
zu prüfen	Lösungsvorschlag
Last steht auf geeigneter Stelle	Überprüfung der Lastfreiheit aller einzelnen Greifer
zu prüfen	Lösungsvorschlag
Kran nicht mehr in Bewegung	siehe Kranbewegung vertikal
zu prüfen	Lösungsvorschlag
Geöffnete Stellung aller Greifer	Lichttaster oder Schalter
zu prüfen	Lösungsvorschläge
Lastfreiheit des Lastaufnahmemittels beim Wiederaufheben	Überlastsicherung zur Lasterkennung verwenden
	Kontrolle der Leistungsaufnahme des Hubwerks
	Lichttaster zur Belegungsprüfung des Lastaufnahmemittels

Teilarbeitsgang: Last aus Übergabestation entfernen

zu erreichen	Lösungsvorschläge
Übergabestation bereit zum Betreten	siehe „Last in Übergabestation positionieren“
zu erreichen	Lösungsvorschläge
vollständiges Entfernen der Last	Lichtschränke
	nur von außen erreichbare Freigabetaster für Bediener an der Übergabestation
	Waage in der Übergabestation

Schutz vor Steuerungsfehlern

zu erreichen	Lösungsvorschläge
keine Steuerungsfehler	Gesichertes Bussystem
	Sicherheits-SPS
	Kommunikation über Lichtwellenleiter, um elektromagnetischen Einflüssen vorzubeugen
	Qualitätssichernde Maßnahmen (DIN 19250)
	Verriegelung der Aktoren zum Schutz vor ungewollten Bewegungen
	Plausibilitätsprüfungen vor Freigabe der Aktoren

Schutz vor mechanischen Fehlern

zu erreichen	Lösungsvorschläge
keine mechanischen Fehler	Mehrseilbetrieb am Lastaufnahmemittel
	Verriegeln der Last in höchster Laststellung als Sicherung für ein Versagen des Antriebsstranges im Hubwerk
	Mehrgreiferbetrieb am Lastaufnahmemittel

9 Zusammenfassung

Die vorliegende Arbeit enthält sicherheitstechnische Lösungsvorschläge zur Ausgestaltung automatisierter Krananlagen für den innerbetrieblichen Behältertransport. Sie ist damit ein Beitrag zur sicheren Implementierung flurfreier flexibler Materialflusssysteme im personenzugänglichen Umfeld.

Ausgangspunkt für die vorliegenden Überlegungen sind nur allgemeine oder uneinheitliche sicherheitstechnische Vorschriften sowie Richtlinien mit großem Ermessensspielraum. Jede Automatikkrananlage wird zur Zeit gesondert untersucht, geprüft und, abhängig von Hersteller und Prüfer, in unterschiedlichen Ausführungsformen in Betrieb genommen. Dazu wurden die bestehenden Regelwerke zur sicherheitstechnischen Auslegung von automatisierten Krananlagen in einem ersten Schritt analysiert und deren ungenügende Anwendbarkeit festgestellt.

Für das Erarbeiten eines neuen und einheitlichen Sicherheitskonzeptes wurde eine Systemanalyse als grundlegende Voraussetzung für eine Sicherheitsanalyse durchgeführt. Dabei werden die logischen Strukturen des Systems festgestellt, die möglichen Betriebsabläufe in den verschiedenen Automatisierungsstufen definiert und vorhandene Bauteile, die einen automatisierten Kran kennzeichnen, ermittelt.

In einem weiteren Schritt zeigt die Arbeit anhand einer Gefahrenanalyse die Gefahren von automatisierten Krananlagen im personenzugänglichen Umfeld auf. Dafür wurden die bestehenden Methoden der Gefahrenanalyse beschrieben und speziell auf automatisierte Krananlagen angepasst.

Das Ergebnis der Gefahrenanalyse wurde in einem Gefahrenkatalog zusammengefasst, der als Ausgangspunkt für die Entwicklung eines durchgängigen Sicherheitskonzeptes verwendet wird. Dazu werden die in der Gefahrenanalyse aufgezeigten Gefahren Schritt für Schritt durch Sicherungsmaßnahmen minimiert.

Der daraus entstandene Lösungskatalog enthält Vorschläge zum Erreichen der Sicherheit. In diesem Lösungskatalog werden die Kranbewegungen von Personen und Hindernissen getrennt gehalten, d.h. der Kran bewegt sich in einem Raum oberhalb von Personen und anderen Hindernissen. Ein Absenken des Lastaufnahmemittels in den Personenbereich findet nur nach vorhergehender Überprüfung in abgesperrten und

gesicherten Bereichen statt. Die Lasten werden über standardisierte Ladehilfsmittel formschlüssig gegriffen und durch ein geschlossenes Lastaufnahmemittel sicher über Menschen hinweg transportiert. Die Lastabgabe erfolgt ebenso wie die Lastaufnahme nach vorhergehender Überprüfung in Übergabestationen. Die Krananlage wird mit über ein Sicherheitsbussystem verbundene Sicherheitssteuerungen, die durch interne Plausibilitätsprüfungen Fehler ausschließen, gesteuert.

Zusammenfassend kann gesagt werden, dass ein geschlossenes Sicherheitskonzept entwickelt wurde, das über ein ganzes Kranlastspiel hinweg greift. Angefangen bei der richtigen Lastaufnahme über die sichere Kranfahrt bis hin zur Lastabgabe sind die Vorgänge abgesichert worden, um Gefährdungen auszuschließen. Die hier entwickelten Lösungsvorschläge zeigen einen Weg auf, der den teilautomatisierten als auch den vollautomatisierten Kranbetrieb im personenzugänglichen Umfeld ermöglicht. Die dazu vorgeschlagenen Sicherheitskonzepte sind zusätzlich so gestaltet, dass der Flexibilitätsgedanke, mit dem automatisierte Krananlagen für den innerbetrieblichen Behältertransport entwickelt wurden, nicht eingeschränkt wird.

10 Literaturverzeichnis

- [1] Handrich, W.: Entwicklung eines stufenweise automatisierbaren Leichtförder-systems im Überflurbereich, in: Günthner, W.A., Reinhart, G.: Forschungspro- jekt MATVAR - Abschlussbericht. UTZ, München, 2000
- [2] Hannover, H.-O., Mechtold, F., Koop, J., Lenzkes, D.: Sicherheit bei Kranen. 7. Auflage, Heidelberg, 1997
- [3] Hoffmann, B., Rostek, R.: Arbeitsunfallstatistik 2002. Hauptverband der ge- werblichen Berufsgenossenschaften (HVBG), Sankt Augustin, Mai 2004
- [4] VBG 9: UVV Krane
- [5] VBG 9a: UVV Lastaufnahmeeinrichtungen im Hebezeugbetrieb
- [6] VBG 8: UVV Winden, Hub- und Zuggeräte
- [7] VBG 4: Elektrische Anlagen
- [8] Verein Deutscher Ingenieure, VDI 3653 Automatisierte Kransysteme, Beuth, Düsseldorf 1995
- [9] Laprie, J.: Dependability: Basic Concepts and Terminology; in English, French, German, Italian, and Japanese. Wien/New York, Springer 1992
- [10] Matthews, C.: A Practical Guide to Engineering Failure Investigation. Profes- sional Engineering Publishing, London, 1998
- [11] Kuhlmann, A.: Einführung in die Sicherheitswissenschaft. Köln, 1981.
- [12] CoVan, J.: Safety Engineering. John Wiley & Sons, New York, 1995
- [13] Eckardt, G., Horn, P.: Zum Mikrorechnereinsatz in Kranen, in: Pajer, G., Scheffler, M., et. al.: Unstetigförderer 1. VEB Verlag Technik Berlin, 5. stark bearbeitete Auflage, 1989, S. 182-185
- [14] Pauly, B.: Neue Konzeptionen für flurfreie Materialflußsysteme. Technica, Band 44 (1995) Heft 10, S. 39-43

- [15] Günthner, W.A., Handrich, W.: Einsatzmöglichkeiten eines Leichtfördersystems im Überflurbereich, Logistik aktuell: Automatisierte Krane- Einsatzverfahren und Entwicklungstendenzen. Dresden, 15. Mai 1998, Hrsg.: H.-G. Marquardt
- [16] Günthner, W.A., Handrich, W.: Ein Ansatz für mehr Flexibilität: Leichtfördersystem im Überflurbereich. fördern und heben f+h 48, (1998) Nr. 5, S. 349-352
- [17] Hesse, W.: Technik und Anwendung automatisierter Krane. Hebezeuge und Fördermittel, Band 35 (1995) Heft 12, S. 521-524
- [18] Günthner, W.A., Bambynek, A.: Schnittstellenbaukasten: Integrierbarkeit eines flurfreien Leichtfördersystems. Hebezeuge und Fördermittel, Band 38 (1998), S. 593-595
- [19] Bambynek, A.: Flurfreie Fördersysteme im automatisierten Materialfluss. München, 2000
- [20] Pietryga, U.: Trends in der Steuerungstechnik von Großkranen. Tagungsbeiträge zur 11. Kranfachtagung 16. Mai 2003, Dresden, S.116-131
- [21] Pietryga, U.: Sicherheit von Steuerungen. fördern und heben f+h 48, (1998) Nr. 10 S.773-775
- [22] Fiedler, M.: Gefahrenanalysen für Aufzüge und deren Sicherheitsbauteile. Lift-Report 23 (4) Juli/August, S. 16-19, 1997
- [23] Krywald, P.-H.: Anwenderhandbuch EG-Konformität für Maschinen. Heidelberg, 1998
- [24] Verwaltungsgemeinschaft Maschinenbau- und Metall-Berufsgenossenschaft, Hütten- und Walzwerks-Berufsgenossenschaft (Hrsg.): Europäisches Recht für Krananlagen. Düsseldorf, 1999
- [25] C. Sundarajan, Guide to Reliability Engineering. Van Nostrand Reinhold, New York, 1991
- [26] Ridley, J., Pearce, D.: Safety with Machinery. Butterworth-Heinemann, Oxford, 2002
- [27] Lee, W., Grosh, D., Tillman, F., Lie, C., Fault tree analysis, methods, and applications - a review. IEEE Transactions R34 (1985), S. 194 - 203
- [28] Rindfleisch, H.-N.: Untersuchung zur Methodik von Sicherheitsanalysen. Dortmund, 1984

- [29] Schneeweiss, W. G.: The Fault Tree Method (in the Fields of Reliability and Safety Technology). Hagen, 1999
- [30] Nohl, J., Thiemecke, H.: Systematik zur Durchführung von Gefährdungsanalysen, Teil 1: Theoretische Grundlagen. Bremerhaven, 1987
- [31] Nohl, J., Thiemecke, H.: Systematik zur Durchführung von Gefährdungsanalysen, Teil 2: Praxisbezogene Anwendung. Bremerhaven, 1987
- [32] Hoyos, C., Ruppert, F.: Der Fragebogen zur Sicherheitsdiagnose FSD. Bern, 1993
- [33] Schmidt, E.: Sicherheit und Zuverlässigkeit aus konstruktiver Sicht; Ein Beitrag zur Konstruktionslehre. Darmstadt, 1981
- [34] Humphries, P.: (Ed) Human Reliability assessors guide, RTS88/89Q, NCSR, UKAEA. Warrington, 1988
- [35] Bello, G.C., Columbori, V.: Reliability Engineering 1, (1),3, 1980
- [36] Edwards, E., 1972, Man and machine: Systems for safety. Proceedings of British Airline Pilots Associations Technical Symposium (British Airline Pilots Associations, London), pp. 21-36
- [37] Klampfer, B., Favre, R.: Der Mensch – schwächstes Glied der Kette?. Publikation der Schweizerischen Rückversicherungs-Gesellschaft, 1997
- [38] Wong, W.: How Did That Happen? - Engineering Safety and Reliability. Professional Engineering Publishing, London, 2002
- [39] Maier, T.: Techniken und Werkzeuge für die Gewährleistung funktionaler Sicherheit von Software in technischen Systemen. Diss., Bericht aus dem Institut A für Mechanik, Stuttgart, 2000
- [40] Neudörfer, A.: Konstruieren sicherheitsgerechter Produkte – Methoden und systematische Lösungssammlung. Berlin, Springer, 1997
- [41] Pahl, G., Beitz, W.: Konstruktionslehre - Methoden und Anwendung, Berlin, Springer, 1997
- [42] Hölscher, H., Rader, J.: Mikrokomputer in der Sicherheitstechnik; Eine Orientierungshilfe für Entwickler und Hersteller. Köln, Verlag TÜV Rheinland, 1984
- [43] Deutsche Elektrotechnische Kommission im DIN und VDE (Hrsg.): Sicherheitsgerichtete Funktionen elektrischer Antriebssysteme in Maschinen. Positionspapier des DKE-AK 226.03, 1998

- [44] Pietryga, U.: Trends in der Steuerungstechnik von Großkranen. Tagungsbeiträge zur 11. Kranfachtagung 16. Mai 2003, Dresden, S.116-131
- [45] Handrich, W.: Flexible. flurfreie Materialflusstechnik für dynamische Produktionsstrukturen. München: Herbert Utz Verlag, 2001
- [46] Günthner, W.A; Bambynek, A.; Handrich, W.: Automatikkrane im Produktionsumfeld: Wie lässt sich die geforderte Sicherheit erreichen? fördern und heben f+h 51 (2001) Nr. 10 S. 742-744
- [47] Pietryga, U.: Sicherheit von Steuerungen, fördern und heben f+h 48 (1998) Nr. 10 S.773-775
- [48] Rushby, J.: A Comparison of Bus Architectures for Safety-Critical Embedded Systems. Menlo Park, USA: SRI International, September 2001
- [49] Griebßbach, R.; Berwanger, J.; Peller, M.: byteflight - neues Hochleistungs-Datenbussystem für sicherheitsrelevante Anwendungen. Automotive Electronics, Sonderausgabe von ATZ und MTZ, 1999
- [50] Belschner, R., Berwanger, J., Führer, T., u.a.: FlexRay Requirements Specification. Version 1.9.7, 7.September 2001
- [51] INTERBUS Club Deutschland e.V.: White Paper INTERBUS Safety. Blomberg: INTERBUS Club Deutschland, 2000
- [52] Janzer, T., HIMA Paul Hildebrandt GmbH + Co KG Industrie Automatisierung: Flexible Automatisierungslösungen für dezentrale zeitkritische Sicherheitsanwendungen. www.hima.de
- [53] Pilz GmbH, Ostfildern, FS Systembeschreibung S.4-2 bis 4-3 Systemhandbuch modulare/kompakte PSS
- [54] Konakovsky, R.: Definition und Berechnung der Sicherheit von Automatisierungssystemen. Braunschweig, 1977
- [55] Kapp, K.-H.: Eine Methode zur Konstruktion und Überprüfung sicherheitsrelevanter Automatisierungssoftware. Karlsruhe, 1985

Anhang A

Liste der wichtigsten nationalen Vorschriften für Krane

Vorschrift	Titel	Fassung
Unfallverhütungsvorschriften		
VBG 1	Allgemeine Vorschriften	01.07.91
VBG 4	Elektrische Anlagen und Betriebsmittel	01.04.79
VBG 5	Kraftbetriebene Arbeitsmittel	01.01.93
VBG 8	Winden, Hub- und Zuggeräte	01.04.96
VBG 9	Krane	01.10.93
VBG 9a	Lastaufnahmeeinrichtungen im Hebezeugbetrieb	01.01.93
VBG 11	Schienenbahnen	01.01.93
VBG 12	Fahrzeuge	01.01.93
VBG 74	Leitern und Tritte	01.10.92
VBG 121	Lärm	10.96
Sicherheitsregeln / Richtlinien		
ZH 1/26	Sicherheitsregeln für höhenbewegliche Steuerstände von Kranen	04.90
ZH 1/64	Richtlinien für Kranführeraufzüge	04.83
ZH 1/74	Sicherheitsregeln für Hydraulik-Schlauchleitungen	04.88
ZH 1/461	Sicherheitsregeln für hochziehbare Personenaufnahmemittel	10.89 10.89
ZH 1/547	Richtlinien für Funkfernsteuerungen von Kranen	06.76
DIN-Normen		
DIN 685-2	Geprüfte Rundstahlketten; Sicherheitstechnische Anforderungen	11.81
DIN 685-3	Geprüfte Rundstahlketten; Prüfung	11.81
DIN 685-4	Geprüfte Rundstahlketten; Kennzeichnung, Prüfzeugnis	11.81
DIN 685-5	Geprüfte Rundstahlketten; Benutzung	11.81
DIN 1142	Drahtseilklemmen für Seil-Endverbindungen bei sicherheitstechnischen Anforderungen	01.82
DIN 3051-4	Drahtseile aus Stahldrähten; Grundlagen; Technische Lieferbedingungen	03.72

Vorschrift	Titel	Fassung
DIN 3052	Drahtseile aus Stahldrähten; Spiralseil 1 x 7	03.72
DIN 3053	Drahtseile aus Stahldrähten; Spiralseil 1 x 19	03.72
DIN 3054	Drahtseile aus Stahldrähten; Spiralseil 1 x 37	03.72
DIN 3055	Drahtseile aus Stahldrähten; Rundlitzenseil 6 x 7	03.72
DIN 3056	Drahtseile aus Stahldrähten; Rundlitzenseil 8 x 7	03.72
DIN 3057	Drahtseile aus Stahldrähten; Rundlitzenseil 6 x 19 Filler	03.72
DIN 3058	Drahtseile aus Stahldrähten; Rundlitzenseil 6 x 19 Seale	03.72
DIN 3059	Drahtseile aus Stahldrähten; Rundlitzenseil 6 x 19 Warrington	03.72
DIN 3060	Drahtseile aus Stahldrähten; Rundlitzenseil 6 x 19 Standard	03.72
DIN 3061	Drahtseile aus Stahldrähten; Rundlitzenseil 8 x 19 Filler	03.72
DIN 3062	Drahtseile aus Stahldrähten; Rundlitzenseil 8 x 19 Seale	09.73
DIN 3063	Drahtseile aus Stahldrähten; Rundlitzenseil 8 x 19 Warrington	09.73
DIN 3064	Drahtseile aus Stahldrähten; Rundlitzenseil 6 x 36 Warrington-Seale	03.72
DIN 3065	Drahtseile aus Stahldrähten; Rundlitzenseil 6 x 35 Warrington gedeckt	03.72
DIN 3066	Drahtseile aus Stahldrähten; Rundlitzenseil 6 x 37 Standard	03.72
DIN 3067	Drahtseile aus Stahldrähten; Rundlitzenseil 6 x 38 Warrington-Seale	03.72
DIN 3068	Drahtseile aus Stahldrähten; Rundlitzenseil 6 x 24 Standard + 7 Fasereinlagen	03.72
DIN 3069	Drahtseile aus Stahldrähten; Spiral-Rundlitzenseil 18 x 7, drehungsarm	03.72
DIN 3070	Drahtseile aus Stahldrähten; Flachlitzenseil 10 x 10, drehungsarm	03.72
DIN 3071	Drahtseile aus Stahldrähten; Spiral-Rundlitzenseil 36 x 7, drehungsfrei	07.72
DIN 3089-1	Drahtseile aus Stahldrähten; Spleiße; Spleißverbindungen an Drahtseilen	05.90
DIN 3089-2	Drahtseile aus Stahldrähten; Spleiße; Langspleiß	04.84
DIN 3090	Kauschen; Formstahlkauschen für Drahtseile	08.89
DIN 3091	Kauschen; Vollkauschen für Drahtseile	12.88
DIN 3093-1	Preßklemmen aus Aluminium-Knetlegierungen; Rohlinge aus Flachovalrohren mit gleichbleibender Wanddicke; Technische Lieferbedingungen	12.88
DIN 3093-2	Preßklemmen aus Aluminium-Knetlegierungen; Preßverbindungen; Sicherheitstechnische Anforderungen	12.88

Vorschrift	Titel	Fassung
DIN 3095-1	Flämische Augen mit Stahlpreßklemmen; Stahlpreßklemmen; Sicherheitstechnische Anforderungen, Prüfung	12.88
DIN 3095-2	Flämische Augen mit Stahlpreßklemmen; Formen; Sicherheitstechnische Anforderungen, Prüfung	12.88
DIN 4132	Kranbahnen; Stahltragwerke; Grundsätze für Berechnung, bauliche Durchbildung und Ausführung	02.81
DIN 5648-1	Rundstahlketten für Hebezeuge; Güteklasse 5, lehrenhaltig, geprüft	05.84
DIN 5648-2	Rundstahlketten für Hebezeuge; Güteklasse 6, lehrenhaltig, geprüft	05.84
DIN 5648-3	Rundstahlketten für Hebezeuge; Güteklasse 8, lehrenhaltig, geprüft	05.84
DIN 5687-1	Rundstahlketten; Teil 1: Güteklasse 5; mittel toleriert, geprüft	04.96
DIN 15003	Hebezeuge; Lastaufnahmeeinrichtungen, Lasten und Kräfte; Begriffe	02.70
DIN 15006	LKW-Ladekrane; Anordnung und Betätigungsrichtung von Stellteilen bei der Handbedienung am Kran vom Flur aus	02.81
DIN 15018-1	Krane; Grundsätze für Stahltragwerke; Berechnung	11.84
DIN 15018-2	Krane; Stahltragwerke; Grundsätze für die bauliche Durchbildung und Ausführung	11.84
DIN 15018-3	Krane; Grundsätze für Stahltragwerke; Berechnung von Fahrzeugkranen	11.84
DIN 15019-1	Krane; Standsicherheit für alle Krane außer gleislosen Fahrzeugkranen und außer Schwimmkranen	09.79
DIN 15019-2	Krane; Standsicherheit für gleislose Fahrzeugkrane; Prüfbelastung und Berechnung	06.79
DIN 15020-1	Hebezeuge; Grundsätze für Seiltriebe; Berechnung und Ausführung	02.74
DIN 15020-2	Hebezeuge; Grundsätze für Seiltriebe; Überwachung im Gebrauch	04.74
DIN 15025	Krane; Betätigungssinn und Anordnung von Stellteilen in Krankabinen	01.78
DIN 15026	Hebezeuge; Kennzeichnung von Gefahrenstellen	01.78
DIN 15030	Hebezeuge; Abnahme von Krananlagen; Grundsätze	11.77
DIN 15063	Hebezeuge; Seilrollen; Technische Lieferbedingungen	12.77
DIN 15070	Krane; Berechnungsgrundlagen für Laufräder	12.77
DIN 15085	Hebezeuge; Laufräder; Technische Lieferbedingungen	12.77
DIN 15105	Lasthaken für Hebezeuge; Bundhaken	08.85
DIN 15106	Lasthaken für Hebezeuge; Hakenmaulsicherung	09.82

Vorschrift	Titel	Fassung
DIN 15400	Lasthaken für Hebezeuge; Mechanische Eigenschaften, Werkstoffe; Tragfähigkeiten und vorhandene Spannungen	06.90
DIN 15401-1	Lasthaken für Hebezeuge; Einfachhaken, Rohteile	11.90
DIN 15401-2	Lasthaken für Hebezeuge; Doppelhaken; Fertigteile mit Gewindenschaft	09.83
DIN 15404-1	Lasthaken für Hebezeuge; Technische Lieferbedingungen für geschmiedete Lasthaken	12.89
DIN 15404-2	Lasthaken für Hebezeuge; Technische Lieferbedingungen für Lamellenhaken	11.88
DIN 15405-1	Lasthaken für Hebezeuge; Überwachung im Gebrauch von geschmiedeten Lasthaken	03.79
DIN 15405-2	Lasthaken für Hebezeuge; Überwachung im Gebrauch von Lamellenhaken	11.88
DIN 15407-1	Lasthaken für Hebezeuge; Lamellen-Einfachhaken für Roheisen- und Stahlgießpfannen; Zusammenstellung, Hauptmaße	09.77
DIN 15407-2	Lasthaken für Hebezeuge; Lamellen-Einfachhaken für Roheisen- und Stahlgießpfannen; Einzelteile	08.89
DIN 15410	Serienhebezeuge; Unterflaschen für Elektrozüge; einrollig und zweirollig; Zusammenstellung	07.82
DIN 15411	Hebezeuge; Lasthaken-Aufhängungen für Unterflaschen	08.83
DIN 15428	Hebezeuge; Lastaufnahmeeinrichtungen; Technische Lieferbedingungen	08.78
DIN 15429	Hebezeuge; Lastaufnahmeeinrichtungen; Überwachung im Gebrauch	07.78
DIN 15434-1	Antriebstechnik; Trommel- und Scheibenbremsen; Berechnungsgrundsätze	01.89
DIN 15434-2	Antriebstechnik; Trommel- und Scheibenbremsen; Überwachung im Gebrauch	01.89
DIN 15436	Antriebstechnik; Trommel- und Scheibenbremsen; Technische Anforderungen für Bremsbeläge	01.89
DIN 15437	Antriebstechnik; Bremstrommeln und Bremsscheiben; Technische Lieferbedingungen	01.89
DIN 31001-1	Sicherheitsgerechtes Gestalten technischer Erzeugnisse; Schutzeinrichtungen; Begriffe, Sicherheitsabstände für Erwachsene und Kinder	04.83
DIN 31003	Ortsfeste Arbeitsbühnen einschließlich Zugänge; Begriffe, Sicherheitstechnische Anforderungen, Prüfung	02.81

Vorschrift	Titel	Fassung
DIN VDE 0100-726	Errichten von Starkstromanlagen mit Nennspannungen bis 1000 V; Hebezeuge	03.90
DIN VDE 0100-726 A1	Errichten von Starkstromanlagen mit Nennspannungen bis 1000 V; Teil 726: Hebezeuge; Änderung 1	04.95

Quelle: [24]

Anhang B

Tabelle zur Gefahrenanalyse

Teilarbeitsvorgang

Situation	Resultierende Situation	Bewertung
Aktoren		
Antrieb Katze		
richtige Funktion		
keine Funktion		
falsche Funktion		
Antrieb Kranbahn		
richtige Funktion		
keine Funktion		
falsche Funktion		
Antrieb Hubwerk		
richtige Funktion		
keine Funktion		
falsche Funktion		
Antrieb Lastaufnahmemittel		
richtige Funktion		
keine Funktion		
falsche Funktion		
weitere Aktoren...		
Sensoren		
Wegmeßsystem		
richtige Funktion		
keine Funktion		
falsche Funktion		

Teilarbeitsvorgang

Situation	Resultierende Situation	Bewertung
Mechanik		
Kranbahn		
richtige Funktion		
keine Funktion		
falsche Funktion		
Katze		
richtige Funktion		
keine Funktion		
falsche Funktion		
Fortsetzung Sensoren		
Überlastsicherung		
richtige Funktion		
keine Funktion		
falsche Funktion		
weitere Sensoren...		
Mechanische Bauelemente		
Kranbrücke		
richtige Funktion		
keine Funktion		
falsche Funktion		
Katze		
richtige Funktion		
keine Funktion		
falsche Funktion		
Zugmittel		
richtige Funktion		
keine Funktion		
falsche Funktion		
Lastaufnahmemittel		
richtige Funktion		
keine Funktion		
falsche Funktion		
Ladehilfsmittel		
richtige Funktion		
keine Funktion		
falsche Funktion		
weitere mechanische Bauelemente		

Teilarbeitsvorgang

Steuerelemente	Resultierende Situation	Bewertung
Handsteuerschalter		
richtige Funktion		
keine Funktion		
falsche Funktion		
Rufschalter		
richtige Funktion		
keine Funktion		
falsche Funktion		
dezentrale Steuerelemente		
richtige Funktion		
keine Funktion		
falsche Funktion		
Leitrechner		
richtige Funktion		
keine Funktion		
falsche Funktion		
Software		
richtige Funktion		
keine Funktion		
falsche Funktion		
Kommunikation zwischen Aktorik Sensorik und Steuerung		
richtige Kommunikation		
keine Kommunikation		
falsche Kommunikation		
Kommunikation zwischen Steuerung und Katze		
richtige Kommunikation		
keine Kommunikation		
falsche Kommunikation		

Teilarbeitsvorgang

Situation	Resultierende Situation	Bewertung
Kommunikation zwischen Steuerung und Kranbrücke		
richtige Kommunikation		
keine Kommunikation		
falsche Kommunikation		
Kommunikation zwischen Steuerung und Lastaufnahmemittel		
richtige Kommunikation		
keine Kommunikation		
falsche Kommunikation		
Kommunikation zwischen Steuerung und Wegmeßsystem		
richtige Kommunikation		
keine Kommunikation		
falsche Kommunikation		
weitere Steuerelemente...		
Bediener		
Aufgabe ausführen		
Aufgabe nicht ausführen		
Aufgabe unkorrekt ausführen		
Aufgabe zu früh ausführen		
Aufgabe zu spät ausführen		
Umwelteinflüsse		
thermisch		
mechanisch		
elektrisch		
akustisch		
Energieausfall		
weitere Umwelteinflüsse...		