



Bernd Ebert

Prozessoptimierung bei Industrie 4.0 durch Risikoanalysen

Gefährdungen erkennen und minimieren

EBOOK INSIDE

 Springer Vieweg

Prozessoptimierung bei Industrie 4.0 durch Risikoanalysen

Bernd Ebert

Prozessoptimierung bei Industrie 4.0 durch Risikoanalysen

Gefährdungen erkennen und minimieren

 Springer Vieweg

Bernd Ebert
Groß-Zimmern, Deutschland

ISBN 978-3-662-55728-0

ISBN 978-3-662-55729-7 (eBook)

<https://doi.org/10.1007/978-3-662-55729-7>

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Springer Vieweg

© Springer-Verlag Berlin Heidelberg 2018

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften. Der Verlag, die Autoren und die Herausgeber gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag noch die Autoren oder die Herausgeber übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen. Der Verlag bleibt im Hinblick auf geografische Zuordnungen und Gebietsbezeichnungen in veröffentlichten Karten und Institutionsadressen neutral.

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer-Verlag GmbH, DE und ist ein Teil von Springer Nature.

Die Anschrift der Gesellschaft ist: Heidelberger Platz 3, 14197 Berlin, Germany

Vorwort

Für die Verbesserung von wirtschaftlichen Prozessen hat sich mit der Thematik „Industrie 4.0“ eine neue Arbeitsrichtung herausgebildet. Nach der Mechanisierung der Arbeit, der elektrifizierten Massenproduktion und der digitalen Ausstattung der Produktion wird mit dem Zählmodus „4.0“ eine höhere Stufe der Herstellung charakterisiert. Diese beinhaltet eine komplette Datenvernetzung und –flexibilisierung bis hin zu autonomer Prozessregelung. Die Konzepte zu diesem aktuellen Entwicklungsziel haben einen Status erreicht, der über das Stadium bloßer Denkansätze hinausgeht und von zahlreichen Beteiligten bereits mit konkreten Entwicklungsvorhaben präzisiert und graduell umgesetzt wurde. Als treibende Kräfte haben sich insbesondere der Maschinenbau, die Elektronik/Elektrotechnik sowie der Bereich von EDV-Hard- und Software etabliert. Deren Forschungs- und Entwicklungsvorhaben zu Industrie 4.0 widmen sich verschiedenen Aspekten intelligenter Maschinen; ihre große Anzahl zeigt bereits den Umfang der erforderlichen Neuerungen für das angestrebte höhere Technologie-Niveau. Die F/E-Ergebnisse wurden und werden auf Foren und Workshops in breitem Maße dargestellt. Neben den inhaltlichen Details scheint auch eine „mentale“ Kernaussage hindurch, nämlich im Sinne von „Wir kriegen das hin!“. Dieser Enthusiasmus ist ansteckend und er mobilisiert nicht nur neue Impulse in den oben genannten Branchen, sondern darüber hinaus auch in der Logistik, bei Vertrieb und Marketing, in der Metallurgie und der stoffverarbeitenden Industrie. Auch in juristische Aspekte reichen die Konsequenzen des angestrebten Fertigungsniveaus. Ohne diese angrenzenden Bereiche ist der volle Erfolg von Industrie 4.0 (ab hier: I4.0) – bzw. der *cyber-physischen Systeme* als Prinzip (ab hier: CPS) – nicht gesichert. Dieses Prinzip impliziert de facto die zentrale IT-Kontrolle über alle *Prozessschritte*, *Schnittstellen* und Daten eines kompletten Fertigungsprozesses. Die dafür erforderlichen virtuellen Modelle müssen sehr komplexe Strukturen abbilden. Daraus resultiert die Notwendigkeit, dass diese Komplexität sowohl im Detail als auch im Gesamt-Überblick kritisch hinterfragt werden sollte.

Hierfür sind Instrumentarien geeignet, die bereits für die Analyse einzelner, auch komplexer Produktionsprozesse eingesetzt wurden und sich bewährt haben. Diese Instrumentarien sollten so angelegt sein, dass nicht nur eine kritische Analyse möglich ist, sondern ebenso – was das eigentlich Zielführende ist – eine Methodik zur Eliminierung bzw. Minimierung der erkannten Risiken. Dafür gibt es – abgeleitet aus dem Bereich der

Sicherheitstechnik – Methoden zur Prüfung von *Schwachstellen* jeder Art (z. B. Funktion und/oder Sicherheit), die unter den Begriffen Risikoanalysen oder *Gefährdungsbeurteilungen* (ab hier: *Risikoanalyse*) als bewährte Vorgehensweisen eingeführt sind. Mehr noch: Der Gesetzgeber sowie die technischen *Prüfgremien* (TÜV, DEKRA usw.) verlangen diese Prüfungen zwingend für technische Verfahren (nicht nur für neue technische Systeme, sondern auch für wesentliche Änderungen an vorhandener Technik). Diese Methoden sind insofern hilfreich, als sie nicht nur für das Aufspüren von Schwachstellen geeignet sind, sondern bis zu möglichen Gegenmaßnahmen ausgeweitet werden können. Diese Vorgehensweise soll im Rahmen dieser Arbeit angewandt werden, um weitere Impulse auf dem Weg zu I4.0 zu ermöglichen. Der hier vorgestellte Ansatz versteht sich als ein Element der ganzheitlichen Betrachtung, der für I4.0 notwendig ist. Dessen Ergebnisse und Hinweise sollen als Anregungen verstanden werden. Sicher werden zahlreiche weiterführende Diskussionen von den Fachleuten der beteiligten Branchen und Gewerke folgen und zur Optimierung im Sinne von „Industrie 4.0“ beitragen.

Die vorliegende Arbeit befasst sich mit wesentlichen technischen Aspekten von I4.0. Weiterführende Betrachtungen, z. B. eine Ausdehnung auf betriebswirtschaftliche Kriterien, ist nicht vorgesehen. Die hier vorgestellte Risikoanalyse hat allgemeinen Charakter. Eine ökonomische Nutzenbetrachtung ist stets an ein konkretes technisches System gebunden. Dies muss im jeweiligen Einzelfall erfolgen und dient dann als Entscheidungsbasis für die Realisierung entsprechender Investitionen.

Jede konkrete Fertigung besitzt spezifische Merkmale. Die dargestellten Zusammenhänge sind als Vorschläge zu verstehen, die im jeweiligen Bedarfsfall angepasst werden können. Aus den dort gewonnenen Erkenntnissen werden sich ggf. neue oder präzisiertere Methoden für vernetzte Fertigungen ergeben. Dies ist die Intention des Autors, der sich hiermit auch herzlich für die Hinweise und die Unterstützung von Freunden und Kollegen bedankt.

Inhaltsverzeichnis

1	Einleitung	1
1.1	Grundsätzliche Anforderungen an Industrie 4.0	2
1.2	Zielrichtung einer Risikoanalyse	4
2	Zur Methodik von Risikoanalysen	7
2.1	Bewertung von Prinzipien für eine Risikoanalyse	8
2.2	Datenbasis für eine Risikoanalyse	9
2.2.1	Schwierigkeitsstufen bei Risikoanalysen	9
2.2.2	Datenbedarf je Schwierigkeitsgrad der Risikoanalyse	11
2.3	Ablauf-Schema für eine Risikoanalyse	12
2.3.1	Fixierung der Rahmenbedingungen	13
2.3.2	Eingrenzung des Analyseobjekts	13
2.3.3	Erarbeitung der Analyse-Kriterien	14
2.3.4	Durchführung der Risikoanalyse	17
2.4	Möglichkeiten und Grenzen bei komplexen Risikoanalysen	18
3	Schwerpunkte bei der Entwicklung zu Industrie 4.0	23
3.1	Konsequenzen aus den allgemeinen Anforderungen	23
3.1.1	Globalität	24
3.1.2	Steuerungs-Anforderungen an Produkte und Maschinen	24
3.1.3	Spezifika bei den Auftrags-Anpassungen	28
3.1.4	Anforderungen an die IT-Systeme	30
3.1.5	Einbettung in die natürliche Umwelt	34
3.1.6	Anforderungen an die Mensch-Maschine-Kommunikation	35
3.1.7	Weitere Anforderungen	37
3.2	Beschreibung und Klassifizierung der Einzelanforderungen	38
3.2.1	Kategorien für die Klassifizierung	39
3.2.2	Zuordnung der Einzelanforderungen	46
3.2.3	Strukturelle Aspekte der Selbstoptimierung	64
3.3	Zuordnungen und Schnittstellen der Teilfunktionen	71
3.3.1	Fokussierung der Teilfunktionen	72

3.3.2	Festlegung und Detaillierung von Arbeitsebenen	73
3.3.3	Beschreibung der Schnittstellen zwischen den Arbeitsebenen	82
3.3.4	Abläufe bei Neubau und Umbau von Prozessanlagen	87
3.3.5	Abläufe bei Auftragsänderungen und Selbstoptimierungen	91
3.4	Abkürzungen	95
4	Durchführung der Risikoanalysen für die Arbeitsebenen	97
4.1	Strukturierung der Analysen	98
4.1.1	Festlegung der Risikoanalysen je Arbeitsebene	98
4.1.2	Spezifische Stichworte für die Analyse-Themen	98
4.1.3	Charakterisierung eines technischen Systems zur Risikoanalyse	102
4.2	Risiken für die Ebene der Fertigung	110
4.2.1	Durchführung der Risikoanalysen	110
4.2.2	Schlussfolgerungen aus den Risikoanalysen der Fertigung	156
4.3	Risiken für die Ebene der Fertigungssteuerung	166
4.3.1	Durchführung der Risikoanalysen	166
4.3.2	Schlussfolgerungen aus den Risikoanalysen der Fertigungssteuerung	207
4.4	Risiken für die Ebene der Managementsteuerung	212
4.4.1	Durchführung der Risikoanalysen	212
4.5	Allgemeine Schlussfolgerungen aus den Risikoanalysen	245
4.6	Abkürzungen	246
5	Risiken in der Einführungsphase von Industrie 4.0	247
5.1	Entwicklungsstufen bis zum Niveau von Industrie 4.0	248
5.2	Anpassung von Fertigungen mit und ohne I4.0-Charakter zueinander	253
5.2.1	Datenübernahme auf Kleincomputer	255
5.2.2	Taktung zwischen Fertigungen mit und ohne I4.0-Charakter	256
5.3	Anpassung von stück- und von mengenbezogenen Fertigungen	257
5.3.1	Identifikation an den Schnittstellen	257
5.3.2	Durchgängige Sicherung der Parameter	259
5.3.3	Charakteristik mengenbezogener Fertigungen	262
5.4	Anforderungen an die Planung für Industrie 4.0	269
	Literatur	271
	Sachverzeichnis	273

Zusammenfassung

Die Komplexität und der Umfang des Entwicklungsziels „Industrie 4.0“ sind so weitläufig, dass ihre Erfassung – bereits im Stadium der Konzeptionen – nach einer Methodik verlangt. Hierfür wird als mögliches Arbeitsprinzip die Methodik einer Risikoanalyse vorgestellt.

Die Grundsatz-Dokumente zu „Industrie 4.0“ beinhalten einen wesentlichen Grund-Tenor: Die deutsche Industrie soll wettbewerbsfähiger, ja möglichst Vorreiter in den künftigen Produktions-Abläufen sein. Als Mittel zum Zweck soll hochgradig I4.0. dienen. In diesem Sinn wurden bisher weitreichende Ziele und Visionen in diesen Begriff hineinprojiziert. Deren Umfang gilt es zu transformieren in konkrete technische Aspekte, die daraufhin mit der Methodik der Risikoanalyse bzgl. ihrer *Schwachstellen* geprüft werden können. Für Automatisierungstechniker und Verfahreningenieure ist es z. B. eine erwiesene Tatsache, dass bereits bei mehr als 4 Grundoperationen (dies im Sinne der physischen Stoffumwandlung oder -behandlung) eine Arbeitsebene für die Regelung nicht mehr ausreicht, sondern bereits mehrere MSR- bzw. *IT-Hierarchieebenen* erforderlich sind (z. B. für jede Grundoperation einzeln, dann für die übergreifende Regelung/Steuerung sowie ggf. für Optimierung und/oder Prozessanalyse, Freigaben, Eingriffe bzgl. Daten und Maschinenparameter).

Beispiel

Betrachtet man den Umfang der Herstellung eines feinmechanischen Bauteils, sozusagen die „*Kettenlänge*“ seiner Fertigung, so beginnt diese bereits beim Roheisen. Dies wird z. B. deutlich, wenn man die heutige Inbetriebnahme von Druckbehältern analysiert: Die erforderliche Dokumentation ist lückenlos zu erbringen von der Zusammensetzung des Stahls beim Hochofen-Abstich bis zur Druckprobe vor der Auslieferung. Dies gilt sinngemäß bereits auch z. B. für Sensoren/Aktoren der Regelungs-/Automati-

sierungstechnik, Pumpen und produktberührte Werkstoffe in der chemischen Industrie. Diese und weitere Angaben sind in den Bestückungen der Halbzeuge und Werkstücke auf dem Niveau von I4.0 zu realisieren, auf jedem einzelnen und möglichst ab dem Beginn der Herstellung (sofern möglich). Die dabei anfallenden Datenmengen sind entlang der *Herstell-Kette* zu verarbeiten. Parallel sind auch die angrenzenden Fertigungslinien zu berücksichtigen incl. ihrer Auslastung und ihrer *Zustands-Parameter*. Weiterhin sind alle diese Systeme eingebunden in Fabrik-Strukturen, die ihr Funktionieren ermöglichen und die somit relevant für I4.0 sind.

Es zeigt sich demnach, dass der Umfang der Änderungen für I4.0 nicht zu unterschätzen ist. Nur eine lückenlose und zeitlich abgestimmte Vorbereitung und Realisierung kann zum Erfolg führen. Dieser Umfang muss möglichst komplett und in seinen jeweils konkreten Zusammenhängen erkannt werden und dies möglichst rechtzeitig. Sind diese Systeme auf praktisch endlos lange Produktionslinien zu erweitern, die zusätzlich mit anderen Linien kommunizieren, ergibt dies einen enormen Koordinations-Aufwand, der sowohl rechentechnisch als auch softwareseitig zu bewältigen ist. Die Priorität der möglichen Bediener- und Programm-Eingriffe würde diese Aspekte noch verstärken. Im Gesamtkontext kann es nicht nur um die Betrachtung von Herstell-Ketten gehen, die „fix und fertig“ für I4.0 sind – wesentlich ist auch der Weg dorthin. Dies beinhaltet u. a. die Fragestellungen der Einführung von I4.0, von möglichen *Niveau-Unterschieden* zwischen einzelnen „Gliedern“ dieser Kette, von der Verschiedenheit der verbundenen Produktionsstränge (z. B. Metallurgie mit Werkstück-Fertigungsstraßen und diese mit chemisch hergestellten Komponenten in Flüssigkeits- und Gas-Form). Einen weiteren Aspekt bildet die Logistik bzgl. notwendiger Zwischenpuffer, Zuführung zu und Ausschleusung von Komponenten aus Fertigungslinien, Transportverpackungen zwischen verschiedenen Fertigungsschritten (z. B. Seetransport über mehrere Wochen), deren Entsorgung u. ä. Als Basis für diese Betrachtungen ist die Gesamtheit der technischen Anforderungen an I4.0 zu erfassen sowie die Risikoanalyse als Methodik der Untersuchung darzustellen.

1.1 Grundsätzliche Anforderungen an Industrie 4.0

Das Entwicklungs-Ziel „Industrie 4.0“ wird in den programmatischen Dokumenten des Bundesministeriums für Bildung und Forschung sowie weiteren richtungweisenden Publikationen durch konkrete Anforderungen an die technischen Möglichkeiten präzisiert. Im Einzelnen sind dies

Gemäß BMBF-Dokument „Zukunftsbild Industrie 4.0“ (Berlin 2013) [1]

hochleistungsfähige „Kleinstcomputer“, die in alle möglichen Materialien und Gegenstände integriert werden

Daten aus der natürlichen Umwelt erfassen, verarbeiten und auf dieser Basis ihre Umgebung zugleich beeinflussen

globale Datennetze, in denen Daten in großen Volumina und stetig steigender Geschwindigkeit verarbeitet werden

Über große räumliche Distanzen hinweg können hochkomplexe technische Prozesse gesteuert werden

punktgenaue Koordinierung zwischen allen Betrieben, die an der Wertschöpfung beteiligt sind

Funkchips in den Transportpaletten

Gemäß BMBF-Dokument „Zukunftsprojekt Industrie 4.0“ (Berlin 2016) [2]

starke Individualisierung der Produkte unter den Bedingungen einer hoch flexibilisierten (Großserien-) Produktion

IT-Sicherheit (mittels) Sicherheits-Referenzsystem

Gemäß BMBF-Dokument „Industrie 4.0 – Innovationen für die Produktion von morgen“ (Bonn 2015) [3]

Produktions- und Logistikprozesse ... müssen ... umfassend dynamisch reagieren.

Produktionssysteme ... mittels Cyber-Physischer Systeme (CPS) gesteuert

Produkte, Maschinen und Anlagen können sich mit ihrer Hilfe (Anm. BE: von Sensoren und Aktoren) selbst optimieren und rekonfigurieren und so an sich ändernde Aufträge und Betriebsbedingungen anpassen

CPS können ... „plug & work“ ermöglichen

Rechenintensive Teile ... in die Cloud verlagern

Optimales Zusammenwirken von Mensch, Maschine und IT-Systemen

Gemäß Schriftenreihe DKE: „Deutsche Normungs-Roadmap Industrie 4.0“ (Frankfurt/Main 2016) [4]

(Teil)-Autonomie im Verhalten auf äußere Einwirkungen und intern gespeicherte Vorgaben

Bauerhansl et al.: „Industrie 4.0 – Herausforderungen und Anforderungen aus Sicht der IT und der Automatisierungstechnik“ (Wiesbaden 2014) [5]

Digitale Netze untereinander verbunden ... sowohl lokal als auch global

Weltweit verfügbare Daten und Dienste nutzen

Multimodale Mensch-Maschine-Schnittstellen ... differenzierte und dedizierte Möglichkeiten ... z. B. Sprache und Gesten

Ähnliche Anforderungen werden auch durch andere Industriestandorte und Gremien auf die Tagesordnung gesetzt, vgl. Sandler [6], Chui et al. [7] und Porter et al. [8]

Diese genannten Anforderungen beinhalten nicht nur technische Aspekte. Mindestens gleichwertig sind die Ziele in psychologischer Hinsicht (Mensch-Maschine-Kommunikation), soziologisch (weltweite Vernetzung und Interaktion), juristisch (z. B. zum Datenaustausch, aber auch zu den Vertrags-Modalitäten für derartig intensive weltweite

Kooperationen). Im Rahmen der vorliegenden Arbeit sollen im wesentlichen die technischen Anforderungen betrachtet werden. Diese werden ausgehend von Kap. 3 detailliert betrachtet.

1.2 Zielrichtung einer Risikoanalyse

Das wirtschaftliche und das gesellschaftliche Leben beinhalten eine Vielzahl von Abläufen und Prozessen, von denen viele eine hohe Komplexität besitzen und sehr viele sich gegenseitig beeinflussen und durchdringen. Deshalb ist es – besonders in der Sphäre der Wirtschaft – für die Stabilität der Prozesse von großer Bedeutung, die ihnen immanenten Schwachpunkte und Gefahrenmomente zu erkennen. Sind diese identifiziert, können geeignete Gegenmaßnahmen konzipiert und bereits vor ihrer Umsetzung und Implementierung bewertet werden. Denn sind Entscheidungs-Maßnahmen erst getroffen, sollen diese auch die gewollten Effekte bewirken und möglichst keine Negativ-Folgen nach sich ziehen. In einer beträchtlichen Zahl von großen Firmen werden z. B. Abteilungen nicht nur mit *Risikoanalysen* über die Produktionsprozesse, sondern auch über die Geschäftsfelder insgesamt – vom Marketing, über Zeithorizonte für Neuentwicklungen bis zur Produktion – beauftragt. Aus Sicht der Gesetzgeber (EU sowie Bundesregierung incl. ihrer verschiedenen Kommissariate bzw. Ministerien) ist der Gesamtbegriff für die Bewertung von Risiken die Gefährdungsbeurteilung. Dies ist zwingend vorgeschrieben in mehreren Gesetzen sowie deren Verordnungen. Die Anwendung dieser Methodik reicht von der Bewertung eines Büro-Arbeitsplatzes bis zur Untersuchung komplexer technischer Systeme. Jede Maschine, die im Geltungsbereich der EU in Verkehr gebracht wird, muss eine Risikoanalyse für den Nachweis ihrer gefahrlosen Nutzung aufweisen, siehe *Maschinenrichtlinie* 2006/42/EG [9]. Hier wird auch explizit festgelegt, dass die Gefährdungen bereits vor Beginn der Konstruktion zu kennen, einzuschätzen und zu bewerten sind [9]. Auch unter diesem Aspekt scheint eine Risikoanalyse bzgl. I4.0 in gewissem Maße überfällig. Weiterhin sind demnach alle Maschinen- und Anlagenbauer und darüber hinaus alle „In-Verkehr-Bringer“ mit dieser Methodik vertraut. Der Erfolg ihrer Anwendung dokumentiert sich u. a. darin, dass die Forderung nach einer Risikoanalyse aktuell in verschiedenen Gesetzen und Standards verankert ist, vgl. auch die EG-Ver-

Abb. 1.1 Generelle Zielrichtungen für Risikoanalysen

Risikoart	Immer	Bei Bedarf	Optional
Arbeitssicherheit	X		
Anlagensicherheit	X		
Dabei Brand-/Ex-Schutz		X	
Reinheit/GMP		X	
Funktion/Zuverlässigkeit			X

ordnung 1272/2008 zur Einstufung, Kennzeichnung und Verpackung von Stoffen [10], die EG-Verordnung „REACH“ 1907/2015 und ff. zur Registrierung, Bewertung, Zulassung und Beschränkung chemischer Stoffe [11], die Betriebssicherheitsverordnung (BetrSichV) Bundesgesetzblatt Februar 2015 [12], die Gefahrstoffverordnung (GefStoffV) Bundesgesetzblatt Juni 2015 [13]. Die Notwendigkeiten bzw. Möglichkeiten für die Anwendung einer Risikoanalyse sind Abb. 1.1 zusammengefasst.

Dies wird nachfolgend im Detail erläutert.

Zusammenfassung

Risikoanalysen sind erprobte Methoden, um Schwachstellen bzgl. Sicherheit, Reinheit, Funktion und Zuverlässigkeit zu ermitteln. Gleichzeitig ermöglichen sie die Erkennung von Verbesserungspotenzialen. Dies ist anwendbar auf Produkte und Herstellverfahren. Verschiedene Arbeits-Prinzipien werden je nach Anwendungsfall dargestellt.

Die Notwendigkeit von Risikoanalysen wurde erstmals in den 30er-Jahren erkannt, als in Industrie und Militär gravierende Unfälle auftraten und deren Ursachen in offensichtlichen Gefahrenpotenzialen gefunden wurden. Die ersten empirischen Vorgehensweisen in diesem Kontext stammen aus den 50er-Jahren des 20. Jahrhunderts und wurden ca. ab 1973 intensiv wissenschaftlich präzisiert. Als eine systematische Analyse begann, wurde dies vorerst retrospektiv vorgenommen, d. h. vorhandene Anlagen wurden untersucht und ggf. sicherheitsseitig geändert. Später verlagerte sich der Schwerpunkt auf die prospektive Analyse, d. h. auf die Risikountersuchung vor der Erstellung technischer Systeme, im Zuge der Planung bzw. Konstruktion von Maschinen, z. B. im Lastenheft. Je nach untersuchtem Objekt kann das Arbeitsprinzip variieren. Allen Arbeitsprinzipien gemeinsam ist jedoch die Vorgehensweise in den folgenden Einzelschritten vgl. [14]:

1. Risiko-Identifizierung
2. Risiko-Bewertung, ggf. -Quantifizierung
3. Risiko-Management
4. Risiko-Aggregation (mehrerer gleichzeitig auftretender Risiken – nur bei Bedarf angewandt)

Eine Risikoanalyse ist demnach „nur“ eine Methodik; sie beschreibt kein naturwissenschaftliches Wirkprinzip und gibt nicht per se eine Lösung vor. Sie zeigt Wege zur Analyse und damit zur Lösung erkannter Problemstellen auf.

Risikoanalysen benötigen eine breite Datenbasis, die nicht nur aus Berechnungen und Schemata besteht, sondern auch aus den Erfahrungen der betrieblichen Abläufe stammen muss. Aus Erfahrung kann postuliert werden, dass erfolgreiche Analysen fast immer aus einer Diskussion zwischen Fachleuten der planenden Bereiche, der Betriebs-Funktionen und der technischen Betreuung hervorgehen. Zielgebiete für Risikoanalysen waren in den vergangenen ca. 40 Jahren

- *Sicherheits*-Anforderungen an technische Systeme
- Funktionalitäts-Tests für Produkte
- *Reinheits*-Garantien für Prozesse und Produkte
- *Zuverlässigkeits*-Tests und -Verhalten von Prozessen

Welche Analyse-Prinzipien bewährt sind und wo die Anwendungsfelder der jeweiligen Vorgehensweisen liegen, ist zu betrachten, um die geeignete Methodik zu erkennen.

2.1 Bewertung von Prinzipien für eine Risikoanalyse

Folgende Analyse-Methoden wurden im Wesentlichen angewandt:

Fehlerbaum- oder Überlebensbaum-Graphen [15]

Beschreibt die Kausalität „Ereignis → Einfluss auf das Objekt“

Ergebnis ist nicht das „innere“ Verhalten des Systems, sondern nur, ob es in Funktion bleibt oder ausfällt.

Niveau der Ergebnisse: „0 – 1“-Aussagen

Wesentliche Anwendung: Zuverlässigkeitsbetrachtungen von Systemen

Markow-Ketten [16]

Vorhersage eines Prozesses nach Kenntnis von dessen Vorgeschichte mit dem Ergebnis einer Verhaltens-Wahrscheinlichkeit des Systems, die durch komplexe Rechnungen (Ketten erster bis n-ter Ordnung mit aufsteigender Komplexität) ermittelt wird.

Niveau der Ergebnisse: Wahrscheinlichkeits-Werte

Wesentliche Anwendung: Zuverlässigkeitsbetrachtungen von Systemen

Experten-Befragung/-Diskussion

Detail-Analyse zu Einzelproblemen

Dient vorrangig der intensiven Ermittlung von einzelnen Fehlerursachen

Niveau der Ergebnisse: Aussagen zur Konstruktion bzw. Funktionalität

Wesentliche Anwendung: Beseitigung einzelner Fehler (meist in einem Produkt oder Bauteil) und/oder Verbesserung der Funktion eines Bauteils

Failure Mode & Effects Analysis (FMEA) [17, 18]

Analyse eines Prozesses, der im Detail bekannt und beschrieben ist, nach Schlagworten bzw. Schlüssel-Fragen, mit deren Hilfe Abweichungen vom Normalverhalten aufzudecken sind.

Die Kausalität zwischen einem Ereignis und den Auswirkungen in einem Prozess wird analysiert und geeignete Gegenmaßnahmen werden konzipiert und abgestimmt.

Niveau der Ergebnisse: Qualitative Aussagen „innerhalb“ eines Systems

Wesentliche Anwendung: Schwachstellen und Gefahren-Potenziale werden erkannt, Beseitigung durch Gegenmaßnahmen hat sich bewährt; als anerkannte Methode zugelassen und zertifiziert

Zustands-Zeit-Diagramme (ZZD)

Basierend auf der Kausalitätsbetrachtung einer FMEA werden die Auswirkungen in Zeitabhängigkeit betrachtet. Gekoppelt mit einfachen Berechnungs-Algorithmen sind auch quantitative Aussagen möglich.

Niveau der Ergebnisse: Qualitative Aussagen „innerhalb“ eines Systems, auch quantitative Analyse möglich

Zeitverlauf einer Zustands-Abweichung sichtbar

Wesentliche Anwendung: bisher nur für Zuverlässigkeits-Betrachtungen (selten)

Da die Analyse für ein sehr komplexes Untersuchungsobjekt durchgeführt werden soll, sind „einfache“ Betrachtungen wie z. B. „System fällt aus oder funktioniert weiter“ nicht ausreichend. Derartige Bewertungen können demnach nicht angewandt werden und es bleiben die FMEA- und die ZZD-Methode als Mittel der Wahl. Da das Instrument der FMEA bisher weit verbreitet ist und bereits vielfach angewandt wird, soll dieses Arbeitsprinzip die Grundlage für die Risikoanalyse bilden.

2.2 Datenbasis für eine Risikoanalyse**2.2.1 Schwierigkeitsstufen bei Risikoanalysen**

Unabhängig von der Größe des ausgewählten Analyse-Teams ist ein Mindestumfang an Daten über das zu betrachtende technische System erforderlich. Dieser Umfang kann variieren

- Nach der „Größe“ des analysierten Systems (Büroarbeitsplatz oder CNC-Taktstraße)
- Nach dessen Komplexität (eine Pumpe incl. Verrohrung oder Schweißroboter mit FiFo-Puffer und Zuführ-/Abführ-Manipulatoren)
- Nach der Anzahl der in einem System durchgeführten Prozesse (Glühofen mit mehreren Fahrweisen oder Chemie-Reaktor für Lösen, Rühren, Destillieren, Kristallisieren)

- Nach dem Gefahrenpotenzial des Systems und der beinhaltenden Halbzeuge, Zwischenprodukte, Medien und Hilfsstoffe (z. B. inerte Stick-Gase, Hochtemperatur-Glühungen/-Trocknungen, rotierende Teile, Explosionsgefahr, Quetschgefahr beim Bedienen, elektrostatische Aufladungen)
- Analysen unterschieden nach permanenten und temporären Prozessen

Diese unterschiedlichen Schwierigkeitsstufen sollten im Vorfeld der Analyse möglichst umfassend erkannt werden. Dies ist leicht möglich, wenn es z. B. um Arbeitsplätze geht: am PC, beim Warentransport oder bei rotierenden Maschinen. Schwieriger wird es, wenn Komplexitäten und/oder Gefahrenpotenziale nicht erkannt werden.

Beispiel

Bei einer Fertigungsstraße wird – nach Abschluss des Basic Engineerings – ein zusätzlicher Fertigungsschritt vorgesehen. Dieser weist ein neues Gefahrenpotenzial auf, das bisher nicht auftrat. Die bereits durchgeführte Risikoanalyse ist um dieses Gefahrenmoment zu erweitern (z. B. durch eine zusätzliche Fahrweise) oder ggf. komplett neu durchzuführen (wenn z. B. die Gestaltung der Fertigungsstraße wesentlich geändert werden muss).

Hierfür sind die Erfahrungen aus dem Analyse-Team von großer Bedeutung, um derartige Änderungen rechtzeitig zu erkennen und bereits prospektiv in die Analyse einfließen zu lassen. Treten derartige Zusatzanforderungen dennoch im Nachhinein auf, sind die bis dahin durchgeführten Analyse-Schritte nochmals zu überprüfen. Auch aus diesem Grund ist es entscheidend, im Zuge der Bearbeitung die jeweilige Dokumenten-Basis mit Revision usw. im Detail festzuhalten. Dies beginnt mit dem Deckblatt gemäß Beispiel in Abb. 2.1.

Abb. 2.1 Deckblatt für eine Risikoanalyse

FMEA / HAZOP

Failure Mode Effects Analysis / Hazard and Operability Study

Kunden-Firma / Ing.-	:
Planung	:
Prozess	:
Standort	:
Betrieb	:
Gebäude	:
Haupt-Komponente(n)	:
Anlagennummer	:
Teilanlagennummer	:
Sollfunktion	:
Projekt-Status	:/
Projekt Nr.	:
Start-Datum FMEA/HAZOP	:

2.2.2 Datenbedarf je Schwierigkeitsgrad der Risikoanalyse

Im Idealfall könnte die Datenbasis aus einem komplett durchgeführten *Basic Engineering* bestehen. Dies wird in der Praxis kaum zutreffen, da nach der durchzuführenden Risikoanalyse alle Dokumente nochmals überarbeitet werden müssten. Dazu würden gehören die Aufstellungspläne, die Fließbilder, die Mengen- und Energiebilanzen, die Spezifikation der Ausrüstungen und Gewerke-Umfänge, die Sicherheitstechnik bis hin zum Lastenheft. Ein derartiger Aufwand ist nicht zu rechtfertigen. Um den Änderungsaufwand so gering wie möglich zu halten, sind alle Engineering-Bereiche bestrebt, die Risikoanalyse(n) möglichst frühzeitig und mit dem geringst notwendigen Dokumenten-Umfang durchzuführen. Welcher Umfang dies ist, soll nachfolgend betrachtet werden – nicht aus theoretischen Erwägungen heraus, sondern als pragmatischer Ansatz (ggf. auch mit einem gewissen „Mut zur Lücke“). Diese *Datenbasis* kann sich an den o. g. Kriterien orientieren.

Der Arbeitsstand der o. g. Daten und Dokumente kann im jeweiligen Einzelfall variieren. Ob z. B. die Bedienwege im einzelnen „ausgezirkelt“ vorliegen oder grob skizziert, hängt davon ab, wie eng die Maschine räumlich platziert wird (z. B. bei Nachrüstungen in einem Altbau).

Generell ist auch zu beachten, dass schwierige *Montagen* und *Inbetriebnahmen* eine Risikoanalyse erfordern – dann jedoch nicht für den laufenden Prozess, sondern für das Einbringen (ggf. mit Wand-Aufbrüchen), die Behinderung vorhandener Anlagenteile und Bedienvorgänge, die temporäre Stillsetzung von Medien-Rohrleitungen und/oder Lüftungen u. ä. Dies entspricht der Problematik „permanente oder temporäre Prozesse“. Hierfür sind neben dem eigentlich betrachteten System auch die angrenzenden Systeme zu betrachten und datenmäßig zu belegen. Dies beinhaltet nicht nur die o. g. Dokumente und Daten, sondern auch derartige Fakten wie das *Produktionsregime*, mögliche Stillstands- und/oder Umrüst-Zeiten. Diese Kenntnisse können im Wesentlichen nur vom Produktions-Management erbracht werden. Auf der Gesamtheit dieser Daten kann die Risikoanalyse im Team begonnen werden.

Beispiel

Eine Fertigungsstraße, die – auch für künftige Herstellprozesse – sehr vielfältige Bearbeitungen zulässt, soll mit einer weiteren Herstellung belegt werden. Diese beinhaltet – im Unterschied zu den vorhergehenden – einen Arbeitsschritt „Werkstück spannungsfrei glühen“. Hierfür ist die Erweiterung der Risikoanalyse erforderlich, nämlich durch Analyse dieses zusätzlichen Fertigungsschrittes. Dabei kann es nicht nur um das Werkstück an sich gehen, sondern auch darum, wo das Werkstück nach dem Glühen abgekühlt wird (auf einem Transportband, in einem zusätzlichen Lager?), wie Einbringen in und Entnahme aus dem Glühofen ablaufen (Handlingsgerät mit hoher Temperatur, als bewegtes Teil mit Berührungsschutz o. ä.). Es wird deutlich, dass sich hierdurch Fragen der Arbeitsabläufe, der Anlagensicherheit und des Arbeitsschutzes intensiv vermengen.

Ziel-Kriterium:	<i>Sicherheit / Qualität / Reinheit / Funktion / Zuverlässigkeit?</i>	Arbeitsdatum:
Verfahren bzw. Produkt:	<i>Fließbild(er):</i> <i>Aufstellung(en), Lageplan:</i> <i>Zielkriterien im Detail:</i> <i>Gesetzliche Vorgaben:</i> <i>Arbeits-Vorschriften/Produktbeschreibung:</i> 1. 2. 3. 4.	Anlage/Teilanlage:
Basis-Dokumente: <i>(bitte auflisten)</i>		
Analysierte Funktionen/Schritte:		
Vor-Zustand des Systems:		<i>Zustand/Betriebsparameter (je Apparat/Funktionsteil):</i> <i>Ein-/Ausgänge:</i> <i>Zustand Logistik:</i>

Annahmen, auf denen diese Risikoanalyse basiert	
Betrachtungseinheiten	Annahme

Abb. 2.2 Dokumente-Nachweis und Rahmenbedingungen für eine Risikoanalyse

Generell ist die Datenbasis für eine Risikoanalyse genau aufzulisten mit Dokumentname, Revisionsdatum usw. Eine bewährte Darstellungsform ist in Abb. 2.2 vorgestellt.

2.3 Ablauf-Schema für eine Risikoanalyse

Liegen die Basis-Daten gemäß Abschn. 2.2 in ausreichendem Umfang vor, kann das Bearbeitungsteam für die Risikoanalyse starten. Zu diesem Team sollten alle diejenigen gehören, die Kenntnisse des bzw. der Prozesse besitzen und für die weitere Planung und Realisierung verantwortlich sind. Dazu gehören neben dem Verfahrensgeber bzw. -verantwortlicher (er stammt häufig aus der Entwicklungsabteilung), dem Verfahrensplaner (dies kann auch ein Team sein ggf. aus mehrerer Disziplinen, auch Logistikplaner), den späteren Prozess-Verantwortlichen (vom Meister bis zum Betriebsleiter), den MSR-Ingenieuren (bis hin zum Betreiber bzw. Planer der Datennetze) sowie einer Fachkraft für Anlagensicherheit.

Einer der Beteiligten sollte als Moderator fungieren. Dafür geeignet sind aufgrund ihrer Vorkenntnisse z. B. die Sicherheits-Fachkraft (aufgrund der Erfahrungen mit Risikoanalysen) oder der Verfahrensplaner bzw. -geber (aufgrund der Prozesskenntnisse). Bei Bedarf können zu dem Team auch weitere Fachleute herangezogen werden, z. B. der Bauleiter bei gefahrbeaufschlagten Montagen, Umschlüssen und Inbetriebnahmen. Hat sich das Team etabliert, ist die Risikoanalyse in folgenden Schritten abzarbeiten:

2.3.1 Fixierung der Rahmenbedingungen

Der Rahmen eines oder mehrerer Fertigungen bzw. Prozesse wird gebildet durch die Umgebungs-Einflüsse und die „Historie“ des/der Prozesse/s. Demnach sind festzuhalten,

- Welche Medien mit welchen Parametern und welchen Reinheiten/Qualitäten
- Welche Übergabe-Parameter bei Rohstoffen und Produkten, z. B.
 - Temperaturen, Drücke, Mengenströme, Konzentrationen
 - Gefahrenpotenziale der Stoffe
 - Gesetzliche Grenzwerte für Handling bzw. Abgabe
- Welche Umgebungsbedingungen klimatisch oder bzgl. Reinraum
- Welche Zustands-Bedingungen beim Betrachtungs-Beginn (detailliert für den gesamten Prozess)
- Bei Bedarf: welche Hauptschritte beim Start bzw. Hochfahren auf Prozessparameter

vorliegen und zu beachten sind. Dies ist in der Dokumentation für die Risikoanalyse als Ausgangs-Betrachtung festzuhalten und ist beim Start der Analyse für eine Fahrweise bzw. einen Prozessschritt nochmals heranzuziehen. Eine mögliche Darstellungsform ist in Abb. 2.2 aufgezeigt.

2.3.2 Eingrenzung des Analyseobjekts

Die Festlegung der zu betrachtenden Prozessschritte sollte anhand der in der Fertigungslinie geplanten Funktionalitäten erfolgen. Es ist zu empfehlen, für alle Funktionen einer Linie die Prozessschritte vom jeweiligen Anlagenstillstand „durch“ die komplette Arbeitsweise bis zurück zum Stillstand zu verfolgen (d. h. vom Anfahren der Technik bis zum Ablauf der Fertigung und anschließender Stillsetzung der Maschinen). Bei dieser Festlegung ist zu prüfen, ob mögliche Abweichungen von der vorgesehenen Funktion in diesem Zusammenhang mit betrachtet werden sollen oder ob dafür eine separate Analyse erforderlich ist.

Beispiel

In einer automatisierten Werkstück-Umverpackung kann als *Abweichung* vom Sollzustand z. B. eine Ungenauigkeit der Robotik auftreten. Dies kann im Rahmen der „normalen“ Analyse betrachtet werden (mit dem Ergebnis, dass eine kurzgetaktete Selbst-Diagnose der Sensoren oder Greifer zu parametrisieren ist).

Ist die Abweichung jedoch ein Defekt der Folien-Verschweißung, kann dafür eine separate Analyse erforderlich werden. Denn hier können mehrere Abweichungen auftreten, z. B. „zu heiß“ oder „nicht vollständig“ (verschweißt) oder „Materialstau“. (Die Stichworte werden nachfolgend behandelt.)

In der betrieblichen Realität ist oft zu beobachten, dass die Planung der technischen Systeme für die Normal-Funktion treffsicher durchgeführt wurde, jedoch für die Abweichungen geringe Vorkehrungen getroffen wurden und dies besonders durch die Risikoanalyse zutage tritt und entsprechend ergänzt werden muss. Dies trifft auch auf die An- und Abfahr-Prozesse von Fertigungslinien zu.

Ist ein technisches System für viele Funktionen ausgelegt, kann der Umfang der Risikoanalyse (bzw. der zu betrachtenden Funktionen) auf folgende Weise reduziert werden: Von allen Funktionen werden diejenigen herausgesucht, die die höchsten Anforderungen an das System stellen. Betrachtet man diese, werden die maximalen Anforderungen des *Normalbetriebs* analysiert. Wohlgedenkt: des Normalbetriebs; die Risiken der Abweichungen sind unabhängig davon nochmals im Detail zu durchleuchten.

Beispiel

Eine Fertigungslinie, die z. B. eine CNC-Bearbeitung sowie einen Klebe-Prozess umfasst, kann z. B. durch die folgenden Normal-Funktionen analysiert werden:

- Größte Bearbeitungstiefe bzw. -durchmesser
- Größte Werkstück-Abmaße bzw. größte Masse
- Zeitlich längster Klebe-Vorgang (mit maximal freiwerdender Lösungsmittel-Menge in Gasform)

Damit ist es möglich, die Normalfunktionen abzudecken; solche Schritte wie das Reinigen der Klebe-Werkzeuge (als Wartungsschritt) oder ein Wechsel der Klebpaste und ggf. des Lösungsmittels sind damit noch nicht erfasst.

Wenn die zu betrachtenden Zustände des Systems festgelegt sind, ist bereits (wie an den Beispielen sichtbar wird) ein intensives „Hineindenken“ in die Funktionen und Abläufe erfolgt. Auf dieser Basis ist es relativ leicht, den nächsten Arbeitsschritt, nämlich die Festlegung der Analyse-Kriterien, in Angriff zu nehmen.

2.3.3 Erarbeitung der Analyse-Kriterien

Die Stichworte für die Risikoanalyse sollen verschiedene Anforderungen erfüllen. Jedes von ihnen soll

- Abweichungen vom Sollzustand beschreiben („zu heiß“ oder „zu schnell“)
- kurz, klar und prägnant sein
- allgemein und nicht zu speziell sein

Und: Keine Gefährdung soll vergessen sein! Falls dies nicht im ersten Wurf gelingt, können *Analyse-Stichworte* noch während der Bearbeitung ergänzt werden – dann sind jedoch die bereits abgehandelten Punkte nochmals „retrospektiv“ durchzusehen!

Firma/Gebäude:		Arbeitsdatum:								
Teilanlage/Produkt:										
Fließbild(er):										
Fkt./Schritt:										
<u>Funktionalität eines Produkts</u>										
Nr.	Abweichung	Ursache	Auswirkung	RK	Gegenmaßnahme	Typ	Vh.	Verantw.	Termin	Bemerkung
1	Optisch unpassend									
2	große Masse									
3	Mobilität schwierig									
4	läuf. Verletzungsgefahr									
5	Bedienung nicht intuitiv									
6	Startprozedur lang									
7	Startprozedur aufwendig									
8	Teilfunktionen schlecht									
9	Fkts.-Parameter falsch									
10	Fkts.-Änderg. schwierig									
11	Datenanzeige gering									
12	Datenanzeige langsam									
13	Datenanzeige langsam									
14	Energ.-Verbrauch hoch									
15	viele Hilfsstoffe									
16	Immobilie Hilfsstoffe									
17	Stand by aufwendig									
18	Betriebskosten hoch									
19	Emissionen hoch									
20	viele Alt-Gebinde									
21	Neu-Gebinde komplex									
22	Reinigungsphase lang									
23	Rein.-Phase aufwendig									
24	Entsorgung schwierig									
25	Abfahren langwierig									
26	Abfahren aufwendig									
27	Brandeinwirkung									
28	Stromausfall									
29	Steuerluftausfall									
30	Ausfall Inertisierung									
31	Äußerer Alarm									

Abb. 2.3 Stichworte für Risikoanalysen zur Funktionalität

Risikoanalyse für

[Bezeichnung des technischen Systems]

**Anlagen-
Funktion**

[Bezeichnung von Prozessschritt/Funktion]

3: sehr hoch
3 sehr selten
3: schwerwiegend

1: sehr selten
1: sehr hoch
1: schwerwiegend

Zelle Nr.	Ursache(n) der konkreten Abweichung	Erkennungs- bzw. Abweichungs-Punkt	Abweichungs-Folgen im System	Auftritts-Häufigkeit	Fehler-Kompensation Geplante Maßnahmen	Einzel-Auswirkung(en)	Folgen im Gesamtsystem	Umsetzung der Maßnahmen
-----------	-------------------------------------	------------------------------------	------------------------------	----------------------	--	-----------------------	------------------------	-------------------------

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25
- 26
- 27
- 28
- 29
- 30
- 31

Abb. 2.4 Tabelle zur Darstellung der Risiken

Aus den bisherigen Erfahrungen mit Risikoanalysen haben sich bereits Stichwort-„Pools“ herausgebildet. Diese sind nicht in Standards verankert, denn dafür ist die Vielfalt der möglichen technischen Systeme zu groß. Sie liegen jedoch bei darauf spezialisierten Firmen (wie TÜV, DEKRA usw.) sowie den Fachabteilungen großer Firmen vor. Je nach Analyse-Ziel sind sie verschieden; hier sollen die der Funktionalität von Systemen zugeordneten Begriffe herangezogen werden. Eine geeignete Aufstellung der Stichworte ist in Abb. 2.3 gelistet.

Aus dieser Auswahl können nicht benötigte Suchbegriffe gestrichen und weitere ergänzt werden. Dies sollte jedoch im Team abgestimmt werden. Als Regel gilt: Lieber ein Stichwort zu viel als eines vergessen! Die Stichworte können in eine entsprechende Tabellenform eingefügt werden, die beispielhaft in Abb. 2.4 dargestellt ist.

2.3.4 Durchführung der Risikoanalyse

Sind die genannten Vorbereitungen erfolgt, kann die eigentliche Analyse durchgeführt werden (analog zu [14]). Aus praktischen Erfahrungen heraus sind verschiedene Schritte abzuarbeiten, und zwar für jede Funktion separat (auch wenn dies u. U. Wiederholungen impliziert):

1. Der Moderator
erläutert anhand des Fließbilds oder der Schrittfolge die technischen Abläufe incl. aller Schnittstellen, wechselseitigen Beeinflussungen, der Arbeitsplätze und Gefährdungen, ggf. der Verriegelungen. Seitens des Betreibers sollten Ergänzungen folgen zur Bedienung/Handhabung sowie zu allen Bediener-Eingriffen und –Steuerungen.
2. Der Moderator
stellt das erste Stichwort in den Raum.
3. Alle Beteiligten
betrachten das System, ob dieses Stichwort auf Probleme bei der jeweiligen Funktion hinweist. Dazu sollte das System von Anfang bis Ende sowie an allen Schnittstellen systematisch durchgesprochen werden. Wenn das Stichwort zutrifft (einmal oder mehrfach), wird jede einzelne, zutreffende Ursache separat bis hin zu ihren Auswirkungen betrachtet und festgehalten wie in Abb. 2.4 dargestellt, und zwar dies für alle auftretenden Ursachen nacheinander.
4. Alle Beteiligten
beraten über die Gegenmaßnahmen, die technischer oder organisatorischer Art sein können. Hierbei ist zu beachten, ob diese Maßnahmen gravierende Auswirkungen auf das System haben (z. B. ein größerer Platzbedarf oder veränderte Regelungs-Struktur).
5. Der Moderator
schlägt Rahmenbedingungen für die Planung und Umsetzung jeder Modifikation vor mit Verantwortlichkeiten und Terminen, die im Team diskutiert und letztendlich festgelegt werden (entfällt für die vorliegende Publikation, da sie ein theoretischer Ansatz ist).

Dieser Arbeitsschritt gliedert sich also auf in mehrere bis viele Einzel-Analysen. Diese sind durchzuführen für jede Funktion des betrachteten Systems, für jedes Stichwort sowie für alle kritischen Zustände eines Stichpunktes.

Bei der Erarbeitung der Gegenmaßnahmen sind derartige Planungswerkzeuge wie Simulationen oder 3D-Raumbelagungen zu empfehlen. Hier kann direkt während der Risikoanalyse die Wirksamkeit bzw. Machbarkeit der Modifikationen geprüft werden.

Ist jeweils eine Funktion durchgearbeitet, sollte dies mittels Unterschrift aller Beteiligten und möglichst mit Ausdruck der geänderten oder Rot-Eintrag in den zugrundeliegenden Planungsdokumenten festgeschrieben werden.

2.4 Möglichkeiten und Grenzen bei komplexen Risikoanalysen

Wie bereits ausgeführt, ist bei sehr komplexen Systemen eine einzelne Risikoanalyse nicht ausreichend. Hierfür sind mehrere Analysen anzusetzen. Dies trifft insbesondere zu, wenn ein System zahlreiche Steuerungs-Ebenen beinhaltet oder wenn die betrachtete Herstell-Kette sehr lang bzw. sehr komplex ist (z. B. schwierige An- und Abfahr-Zyklen aufweist) oder wenn das System mehrere, z. T. stark differierende Prozessfunktionen hat.

Hierfür gelten auch die Kriterien für Systeme mit verschiedenen Funktionen, wie sie in Tab. 2.1 dargestellt sind. Insbesondere sind die Übergänge und Schnittstellen zwischen den Teilsystemen, Hierarchie-Ebenen und differierenden Prozess-Schritten im Detail zu prüfen. Denn hierbei traten in der betrieblichen Praxis bereits zahlreiche, z. T. schwerwiegende Gefahrenmomente auf.

Beispiel

In einer Fertigungsstraße laufen nacheinander verschiedene Grundoperationen ab. Folgt z. B. auf eine Klebe-Verbindung eine heißgehende Verarbeitung, kann folgendes Risiko auftreten: Das beim Kleben freiwerdende Lösungsmittel befindet sich teilweise noch als Gas in den Werkzeugteilen. Beim anschließenden Erhitzen kann der Flammpunkt des Gases überschritten werden und sich dieses entzünden. Hier liegt ein Risiko sowohl für Mensch als auch Maschine vor. Betrachtet man ausschließlich die zwei Grundoperationen, wird dieser Zusammenhang ausgeblendet. Das Beispiel zeigt, dass auch die Übergänge bzw. die Vorbedingungen jedes Prozess-Schrittes im Detail zu betrachten sind. Derartige Risiken sind besonders bei stoffumwandelnden Prozessen zu beobachten, da hier zum einen die Betriebsparameter (Druck, Temperatur, Menge) stark variieren können und zum anderen chemische und physikalische Stoffumwandlungen stattfinden, d. h. andere Stoffe entstehen können mit komplett anderen Eigenschaften.

Bei der Risikoanalyse eines komplexen Systems (wie es bei der Thematik „Industrie 4.0“ hochgradig der Fall ist) können zwar viele kritische Punkte erkannt werden, jedoch hat diese Betrachtungsweise auch Grenzen bzw. birgt eigene Risiken in sich.

Tab. 2.1 Datenbasis für eine Risikoanalyse, bezogen auf die Kriterien des analysierten Systems. (Siehe auch [20])

Kriterien	Erforderliche minimale Datenbasis	Bemerkungen
Einfaches System	Aufstellung, Begehrbarkeit/Bedienbarkeit	Diese Basis ist auch für alle weiteren aufgeführten Kriterien erforderlich
Komplexes System	Beschreibung der Abläufe/Prozesse Fließschemata Energie- & Mengenbilanzen, ggf. inclusive der Stoffdaten Größe & Kapazität der Ausrüstungen Sicherheitseinrichtungen Werkstoff-/Material-Daten Regelungs-Struktur(en) & Verriegelungen Andienungs- und Entsorgungswege	Diese Basis ist auch für alle weiteren aufgeführten Kriterien erforderlich
Systeme mit mehreren Funktionen	Reinigungsabläufe Umrüstungen Referenz-Stoffe (mit den Stoffdaten, die am problematischsten sind)	
Systeme mit Gefahrenpotenzial	Abschalt-Regimes während Bedienung (z. B. Toter-Mann-Drücker), Wartung und Störfall Bedienabstände Sicherheits-Datenblätter für gefährliche Stoffe Ex-Einstufung raum- oder anlagenbezogen Zonen-Abtrennung(en) bzgl. Gefahrstoffe und/oder Brand- & Explosionsgefahr Angrenzende räumliche Bereich und mögliche gegenseitige Beeinflussungen (durchlaufende Rohrleitungen/Lüftungen?)	
Temporäre Prozesse	Je nach Bedarf: Genaue Abmaße der Geräte; Anschlagpunkte oder Kranhöhen; Transportwege in Gebäuden; provisorische Arbeitsmittel, Medien und deren Entsorgungs-Produkte; Arbeits- und Bedienabläufe an benachbarten Anlagen	Betrifft z. B. Montagen und Inbetriebnahmen

Diese wurden bereits in den bisherigen Betrachtungen angedeutet und sollen jetzt im Detail benannt werden.

1. „Vergessene“ bzw. übersehene Zustände und Übergänge
2. Fehl-Diagnosen/-Interpretationen
3. Falsche oder unzureichend wirksame Gegenmaßnahmen
4. Zu geringe Prozesskenntnis in frühem Stadium (ist besonders bei komplexen Systemen zu beachten)
5. Keine durchgängige Umsetzung der erforderlichen Änderungen

Diese Risiken traten bisher in jeder Planungsphase für ein technisches System auf. Bedingt durch die nunmehr auftretende höhere Komplexität bei I4.0 sind sie in stärkerem Maße zu beachten sowie klar zu benennen, da sie auch für die in dieser Publikation angestrebte Analyse zu beachten sind.

Ein weiteres Manko der hier durchgeführten Betrachtung ist nicht zu unterschätzen:

6. Die hier vorliegende Risikoanalyse wird nicht im Team durchgeführt, sondern als Betrachtung einer Einzelperson.

Der Autor ist sich dieses Umstands bewusst und erhebt keinen Anspruch auf 100 %ige Treffsicherheit. Im Wesentlichen geht es um die Darstellung der Methodik sowie ihre theoretische Einführung und praktische Erprobung für I4.0, um sie als Hilfestellung anzubieten. In der weiteren Ausgestaltung des Gesamtvorhabens wäre ihre Anwendung als Teamarbeit wünschenswert und sicher auch zielführend für das Gelingen. Dies muss nicht unbedingt nur die Analyse „über alles“ sein, sondern kann ebenso für Teilbereiche genutzt werden, von den Fertigungslinien bis zum Datentransfer zwischen den Clouds (siehe auch Kap. 4).

Wenn für ein komplexes System mehrere Analysen erstellt werden, ist die exakte Abgrenzung zwischen ihnen von großer Bedeutung. Die bisherigen Erfahrungen mit Risikoanalysen haben gezeigt, dass eine praktikable Bearbeitung eines technischen Systems möglich ist, wenn die folgende Reihenfolge angewandt wird:

1. Risikoanalysen direkt für die technischen Systeme (z. B. Fertigungslinien)
 - a. Analyse des/der Normal-Betriebsweisen
 - b. Analyse der An- und Abfahr-Prozesse
 - c. Analyse der Reparaturen und Wartungen und Reinigungen
 - d. Analyse für Montagen und Demontagen im technischen System (bei Bedarf)
 - e. Analyse für Havarie-Zustände wie Brand, Totalausfall u. ä. (bei Bedarf)

Das Vorhaben I4.0 geht über den Rahmen eines oder mehrerer Fertigungslinien weit hinaus. Es ist absehbar, dass die Kopplungen dieser Linien nicht mit bisherigen Steuerungen vergleichbar sind, sondern wesentlich umfangreicher und komplexer sein werden. Aus diesem Grund wird vorgeschlagen, die übergeordneten Abläufe (Auftragsverwaltung, Datentransfer und -speicherung, Abgleich zwischen den untergeordneten Systemen, Steuerung/Verfolgung der Logistik usw.) separat mit Risikoanalysen zu betrachten. Dies sollen sein:

2. Risikoanalysen für die übergeordneten Steuerungen
 - a. Analyse für Schnittstellen und Kommunikationen zwischen den technischen Systemen
 - b. Analyse für Rohstoff-/Produkt-/Medien-Ströme incl. Logistik (Transport, Umschlag und Lagerung), Zwischenpuffer, Aufreinigung und Entsorgung

- c. Analyse für Datensammlung, -speicherung, -verarbeitung und -wiederabruf
- d. Analyse für Auftragsverwaltung incl. Annahme und Prüfung, Modellierung der Ablauf-Änderungen in der Fertigung, Beschaffung von Rohstoffen, Übergangsfahrweisen und Reinigungen zwischen verschiedenen Aufträgen usw.
- e. Analyse für Änderungen der Prozessabläufe incl. Planung, Montage, Umschlüsse mit „Alt“-Systemen, Inbetriebnahme
- f. Analyse für Notzustände wie Transfer- oder Cloud-Ausfall.

Wie die Umfänge der einzelnen Risikoanalysen sein werden und wie die Abgrenzung zwischen ihnen im Detail verläuft, wird in Kap. 3 und 4 herausgearbeitet.

Gemäß Kap. 1 liegt dabei der Fokus nicht auf der Funktionalität der Herstellungs-Kette, sondern darüber hinaus auf einer flexiblen Auslastung der betreffenden Produktionsanlagen sowie auf der bestmöglichen Kunden-Zufriedenheit. Diese Anforderung ist Bestandteil der Gesamt-Zielstellung, die an Industrie 4.0 gestellt wird (siehe Abschn. 1.1), und soll nachfolgend im Komplex aller Anforderungen betrachtet werden (Kap. 3).