Technische Universität Dresden

Fakultät Elektrotechnik und Informationstechnik

Professur für Prozessleittechnik

Diplomarbeit

Thema

vorgelegt von: Marius Müller

Matrikelnummer: 3661272

geboren am: 29. September 1989 in Dresden

zum Erlangen des akademischen Grades

Diplomingenieur

(Dipl.-Ing.)

Betreuer:

Dipl.-Ing. Annett Pfeffer (PLT/TUD)

Verantwortlicher Hochschullehrer:

Prof. Dr.-Ing. Leon Urbas

Tag der Einreichung:

12.07.2017

Bibliografischer Nachweis

Marius Müller

Thema der Diplomarbeit

Diplomarbeit: Anzahl Seiten, Anzahl Abbildungen, Anzahl Literaturangaben

Datum

Technische Universität Dresden

Fakultät Elektrotechnik und Informationstechnik

Professur für Prozessleittechnik

Autorenreferat:

Zusammenfassung der Arbeit

Bitte ersetzen Sie diese Seite vor dem Binden mit der Aufgabenstellung.

Selbstständigkeitserklärung

Hiermit versichere ich, dass ich die vorliegende Arbeit ohne unzulässige Hilfe Dritter und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe; die aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht. Bei der Auswahl und Auswertung des Materials sowie bei der Herstellung des Manuskripts habe ich Unterstützungsleistungen von folgenden Personen erhalten:

- Person 1
- Person 2

Weitere Personen waren an der geistigen Herstellung der vorliegenden Arbeit nicht beteiligt. Mir ist bekannt, dass die Nichteinhaltung dieser Erklärung zum nachträglichen Entzug des Diplomabschlusses führen kann.

Dresden, 12. Juli 2017 Marius Müller

Inhaltsverzeichnis

Abkürzungsverzeichnis

EG	Europäische Gemeinschaft
EU	Europäische Union
EWR	Europäische Wirtschaftsraum
MTP	Module Type Package
OPC	Open Platform Communications
UA	Unified Architecture
OPC-UA	Open Platform Communications Unified Architecture
HAZOP	Verfahren zur Prognose, Auffinden der Ursache, Abschätzen der Auswirkungen, Gegenmaßnahmen (Hazard and Operability Analysis)
FTA	Fehlerbaumanalyse (Fault Tree Analysis)
FMEA	Fehlermöglichkeits- und -einflussanalyse (Failure Mode and Effects Analysis)
FDI	Fehlererkennung und Fehlerisolation (fault detection and isolation)
LQM	Methode der kleinsten Fehlerquadrate (Least Squares Method)
DBN	Deep Belief Network
BBN	Bayesian Belief Network
RBN	Restricted Boltzmann Machine
TEB	Tennessee Eastman Benchmark
SDG	Signed Directed Graph
P&ID	Rohrleitungs– und Instrumentenfließschema (Piping and

	instrumentation diagram)
HFPM	hierarchical fault propagation model
IRML	Infrastructure Resilience-Oriented Modeling Language
PCA	Principle component analysis
DTW	Dynamic time warping
DAE	Differential–algebraische Gleichung (Differential Algebraic Equation)
GHS	global harmonisierte System zur Einstufung und Kennzeichnung von Chemikalien
SEVESO III	Richtlinie 2012/18/EU
CLP	Verordnung Nr. 1272/2008/EG
IED	Industrieemissionsrichtlinie 2010/75/EU
DGRL	Druckgeräte–Richtlinie 2014/68/EU
MRL	Maschinen–Richtlinie 2006/42/EG
BImSchG	Bundes–Immissionsschutzgesetz
BImSchV	Bundes–Immissionsschutzverordnung
4. BImSchV	Verordnung über genehmigungsbedürftige Anlagen
12. BImSchV	Störfall–Verordnung
BetrSichV	Betriebssicherheitsverordnung
UVPG	Umweltverträglichkeitsprüfungsgesetz
GefStoffV	Verordnung zum Schutz vor Gefahrstoffen
TRAS	Technische Regeln für Anlagensicherheit
TRBS	Technische Regeln für Betriebssicherheit
TRGS	Technische Regeln für Gefahrstoffe
TRwS	Technische Regeln für wassergefährdende Stoffe
TRBA	Technische Regeln für biologische Arbeitsstoffe

Verzeichnis der verwendeten Formelzeichen

α	m^2/s	Temperaturleitfähigkeit

Verzeichnis der verwendeten Indizes

l	liquid/flüssig

Symbolverzeichnis

Notation	Bedeutung

Abbildungsverzeichnis

Tabellenverzeichnis

Thesen der Diplomarbeit

1. Erste These

Einleitung 1

1.1 Herausforderungen der deutschen Chemie- und Pharmaindustrie

Das reale Bruttoinlandsprodukt Deutschlands wuchs von 1995 bis 2013 im Mittel weniger als 2% und wurde damit von den teils zweistelligen Wachstumsraten der Schwellenländer und insbesondere China deutlich übertroffen. Um international erfolgreich zu bleiben, sind die schnell wachsende Pharmazeutische Industrie und die exportlastige Chemische Industrie für die deutsche Wirtschaft von besonderer Bedeutung.

Noch eine aktuelle Quelle zur wirtschaftl. Lage suchen und einen Überleitungssatz zu der meist verwendeten Quelle [11] erstellen

Die Chemische Industrie und die Pharmazeutische Industrie sind Schlüsselbranchen der deutschen Wirtschaft. Sie exportierten im Jahr 2013 Waren im Wert von über 150 Milliarden €. Dies entspricht 15% der deutschen Gesamtexporte des verarbeitenden Gewerbes. Der Export von pharmazeutischen Erzeugnissen wuchs in den Jahren 1995 bis 2013 jährlich im Durchschnitt 11,3% und damit schneller, als der jeder anderen Branche. Im gleichen Zeitraum entwickelte sich die Chemische Industrie nur unterdurchschnittlich – im globalen Wettbewerb verlor sie sogar Marktanteile. Als Ursache hierfür wird die besonders hohe Abhängigkeit der Branche von den in diesem Zeitraum in Deutschland stark gestiegenen Energiepreisen angesehen. Es müssen geeignete Maßnahmen entwickelt und angewandt werden, um die Standortnachteile auszugleichen. Nur so kann die Pharmazeutische Industrie ihre Wachstumsdynamik beibehalten und die Chemische Industrie ihre Entwicklungschancen realisieren.
Eine wichtige Grundlage für den Erfolg der Chemischen und Pharmazeutischen Industrie ist die beständige Weiterentwicklung und Erschaffung innovativer Pro-

dukte. Die allein im Jahr 2013 über 7500 in Deutschland neu angemeldeten Patente belegen die bereits aufgebrachte Innovationskraft. Die größten deutschen Industriezweige Maschinen- und Fahrzeugbau meldeten im gleichen Zeitraum in Summe nur circa Dreihundert Patente mehr an. Die Entwicklungsleistung im Chemie- und Pharmabereich ist in Relation zu den übrigen Gewerbezweigen offensichtlich bereits überdurschnittlich hoch. Es erscheint daher sinnvoll andere Faktoren zu untersuchen, welche die Entwicklung der betrachteten Industriezweige maßgeblich beeinflussen. [11]

Im aktuellen Bericht des Verbands der Chemischen Industrie untersucht Jan Limbers die Lage und Entwicklungsmöglichkeiten der chemisch-pharmazeutischen Industrie und prognostiziert die Entwicklung bis zum Jahr 2030. Durch die schnellere Verbreitung von Technologie und Wissen und den damit verbundenen gesteigerten globalen Wettbewerb ist ein weiter ansteigender Innovationsdruck zu erwarten. Wird die umfangreiche Forschungsarbeit auf die Bereiche Spezialchemikalien und Pharmazeutika fokussiert, so können die Standortnachteile, welche durch hohe Energiekosten entstehen, ausgeglichen werden und ein überdurchschnittliches Wachstum ist möglich. Dies erfordert jedoch insbesondere ein insgesamt höheres Innovationstempo. Der Entwicklungsfaktor Innovationstempo soll daher im Folgenden weiter betrachtet werden. [86]

Das Innovationstempo ist mit der benötigten „Time to market“ eines Produktes gleichzusetzen. Darunter versteht man in diesem Zusammenhang den Zeitraum von der ersten Idee für ein neues Produkt bis zum Zeitpunkt der Inbetriebnahme der Produktionsanlagen im marktangepassten Maßstab. Die dazu erforderlichen Schritte umfassen die notwendige Forschungsarbeit zur Produkt- und Prozessentwicklung, die Planung und den Bau der Produktionsanlagen. Der Zeitraum nach erfolgter Produktentwicklung bis zum Produktionsbeginn umfasst in etwa 5 – 10 Jahre, wobei davon circa die Hälte der Zeit auf Anlagenplanung und Konstruktion entfallen. [13]

Dieser Zeitraum muss reduziert werden, um die von J. Limbers prognostizierte Entwicklung der chemisch-pharmazeutischen Industrie zu ermöglichen.
Die prinzipielle Notwendigkeit einer schnelleren und vor allem auch flexibleren Produktentwicklung beziehungsweise Produktion ist seit langem bekannt. Die Arbeit von I. E. Grossmann zu den Herausforderungen für die Forschung im Bereich der Verfahrens- und Anlagentechnik aus dem Jahr 2000 weist beispielsweise

auf diese Herausforderungen hin [53].

Es wurden bereits zahlreiche Untersuchungen durchgeführt, um zu ermitteln wie das Ziel einer flexibleren und beschleunigten Produktentwicklung erreicht werden kann. Auf ausgewählte Ansätze wird im folgenden Abschnitt eingegangen.

Der Übersichtsbeitrag von WACHSEN u. a. [144] fasst die genannte Problemstellung mit Hinblick auf die Spezialchemie zusammen und bietet einen geeigneten Einstieg in aktuelle Untersuchungen zu dieser Thematik.

1.2 Beschleunigung des Innovationstempo

In Abschnitt 1.1 wurde die Relevanz der chemisch-pharmazeutischen Industrie für die deutsche Wirtschaft dargelegt und die Notwendigkeit eines erhöhten Innovationstempos begründet. In diesem Abschnitt werden Methoden zur Realisierung dieses Ziels vorgestellt. Der Fokus liegt auf der Idee der Modularisierung von Anlagenkomponenten.

Ein Ansatz zur Verbesserung des Produktentwicklungsprozesses wurde über ein Jahrzehnt hinweg an der Universität Clausthal untersucht. Anhand eines neu entworfenen Apparates zur Herstellung von Chlorsilanen aus Ferrosilicium und Chlorwasserstoff wurde von DIETZ und NEUMANN in [40] gezeigt, wie durch eine frühzeitige Parallelisierung von Prozessplanung und dem Entwurf der notwendigen Maschinen die Entwicklungszeit verkürzt werden kann. Die Parallelisierung wird erreicht, indem die zu realisierenden Prozessschritte in Teilsysteme geringer Komplexität so weit zerlegt werden, dass sich deren Funktion durch naturwissenschaftliche Grundoperationen darstellen lässt. Durch die so erhaltene Darstellung wird ein Blick für die mögliche Zusammenfassung von mehreren Teilsystemen in einer einzigen Maschine ermöglicht. Eine derart entworfene Maschine kann auf innovative Weise einen Prozess optimal erfüllen. Prozessschritte wie Zerkleinern, Reagieren und Mischen können beispielsweise in einem Apparat vereint werden. Es wird bei diesem Entwicklungsprozess bewusst auf Standardlösungen verzichtet, was die Wiederverwendbarkeit der erhaltenen Lösungen erschwert. Das Innovationstempo kann jedoch auf diesem Weg erfolgreich gesteigert werden und es wird eine hocheffiziente Umsetzung für einen Produktionsprozess gefunden.

Neben der Parallelisierung von Prozessplanung und Anlagenentwicklung gibt es weitere Methoden zur Verkürzung der Entwicklungszeit. Dazu zählen unter anderem der verstärkte Einsatz von mathematischen Modellen beispielsweise in Simulationen, das Verwenden von Mini- und Mikroplants und der Gebrauch von standardisierten Modulen.

Zahlreiche Vertreter aus Wissenschaft und Wirtschaft haben sich 2009 zum 48. Tutzing Symposium getroffen. Diskussionsschwerpunkt war die „50% – Idee Vom Produkt zur Produktionsanlage in der halben Zeit“ . Es sollte analysiert werden, welche Methoden besonders dazu geeignet sind, um die „Time to Market“ auf die Hälfte zu reduzieren. Als Ergebnis wurden unter anderem die Thesen von Tutzing [38], ein Positionspapier [39] und ein Übersichtsvortrag [13] veröffentlicht. Es wurden die notwendigen Forschungsschwerpunkte herausgearbeitet, um das Ziel eines signifikant erhöhten Innovationstempos zu erreichen.

In diesen Arbeiten wurde als Kernthema die Modularisierung von Anlagen und deren Komponenten identifiziert. Durch die Verwendung von Standardlösungen sollen umfangreiche Detailarbeiten entfallen und Anlagenkomponenten durch erneuten Einsatz perfektioniert werden. Dies bedeutet eine bewusste Abkehr von dem in [40] vorgestellten Vorgehen einer parallelisierten Prozess- und Anlagenentwicklung in Verbindung mit einer optimal ausgelegten Anlage. Statt dessen werden wiederverwendbare Module in diskreten Größen erzeugt, welche skalierbar und vielseitig einsetzbar sein sollen. Die Skalierbarkeit ermöglicht dabei eine flexible Veränderung von Produktionsvolumina und damit eine schnelle Anpassbarkeit an Marktveränderungen. Module können dezentral vorgefertigt und am Standort der Gesamtanlage schnell zusammengefügt werden. Dies beschleunigt die Konstruktion der Gesamtanlage.

Die Verwendung von Modulen bedeutet eine signifikante Änderung im Entwicklungsprozess. Es wurden mehrere Themenschwerpunkte identifiziert, welche die notwendigen Anpassungen beschreiben sollen. Die hier aufgeführten Schwerpunkte sind dem bereits aufgeführten Positionspapier zur 50 % – Idee entnommen [39]. Die Reduktion der Entwicklungszeit auf die Hälfte durch den Einsatz von Modulen ist nur möglich, wenn die im Folgenden genannten Themen erfolgreich bearbeitet werden.
Ein Themenschwerpunkt ist die Entwicklung von Modellen zur Beschreibung von Modulen. Module sollen abgeschlossene Funktionseinheiten bilden. Für einzelne

Prozessschritte sind Apparate zu entwickeln, die diese realisieren können. Sie sollen skalierbar und getrennt von anderen Anlagenteilen testbar sein.
Die Funktion eines Moduls und die Dokumentation in verschiedenen Detaillierungsgraden sowie entwickelte Skalierungsvarianten und alle weiteren relevanten Informationen sollen für Anlagenbauer, Zulieferer, Prozessplaner und alle übrigen am Produktentwicklungszyklus Beteiligten abrufbar sein. Dazu sind geeignete Informationsmodelle notwendig. Diese sollten in Verbindung mit bestehenden Softwarelösungen verwendet werden können. [39]
Das Konzept der Modularisierung soll in allen Phasen eines Projektes zur Entwicklung neuer Produkte eingesetzt werden. Die Projektplanung muss dazu umstrukturiert werden. Die notwendigen Anpassungen der etablierten Projektabläufe sind zu erarbeiten und zu testen. [39]
Um ein durchgängiges Modulkonzept zu etablieren ist die Definition von Standards und Schnittstellen zwischen Modulen unumgänglich. Dazu ist eine firmenübergreifende Kooperation und die Zusammenarbeit mit der Wissenschaft notwendig. [39]
Weiterhin muss die Automatisierungstechnik an die modulare Bauweise angepasst werden. Insbesondere ist zu erörtern, wie autonom einzelne Module gesteuert werden sollen und wie die Kommunikation zwischen Modulen im Rahmen einer Gesamtanlage konzipiert werden kann. [39]

Diese Themen wurden weitreichend untersucht. Die prinzipielle Anwendbarkeit der modularen Anlagenbauweise konnte anhand mehrerer Fallstudien im Rahmen des Projektes F^3–Factory gezeigt werden. Die Ergebnisse wurden im Abschlussbericht dieses Projektes [17] veröffentlicht.
Weitere Untersuchungen wurden beispielsweise im Projekt CoPIRIDE [126] durchgeführt.

Die wichtigsten Ergebnisse vom F3 noch zusammenfassen.

Die Anwendbarkeit von Modulen konnte demnach bereits erfolgreich gezeigt werden. Es sind aber noch einige Forschungsschwerpunkte offen. Ein wichtiger Gesichtspunkt wurde bisher noch nicht umfassend betrachtet: die Auswirkung der Modularisierung auf notwendige Sicherheitsbetrachtungen.
Bei der Planung und Inbetriebnahme einer neuen prozessleittechnischen Anlage ist die Gewährleistung des sicheren Betriebs von höchster Wichtigkeit. Dazu sind geeignete Sicherheitsuntersuchungen durchzuführen. Die Auswirkung der

Modularisierung von Anlagen auf Sicherheitsuntersuchungen findet in den direkten Veröffentlichungen zum Tutzing Symposium keine gesonderte Beachtung. Im Abschnitt 1.3 wird auf die prinzipielle Problemstellung von Sicherheitsuntersuchungen eingegangen und im daran anschließenden Abschnitt 1.4 das Thema dieser Arbeit herausgearbeitet.

1.3 Notwendigkeit von Sicherheitstechnik

Sicherheit ist ein menschliches Grundbedürfnis. Wird dieses Bedürfnis nicht in ausreichendem Maße erfüllt, so hat dies gravierende Auswirkungen. Die massenweise Flucht aus Kriegsgebieten ist beispielsweise ein solcher Extremfall.
Unter normalen Umständen können Risiken durch geeignete Mittel reduziert werden. Dazu kann entweder die Eintrittswahrscheinlichkeit eines Schadensfalles oder dessen schädliche Auswirkung gemindert werden. Um eine dieser Methoden anzuwenden ist jedoch entweder die Aufwendung von Kapital oder die Einschränkung von möglichem Nutzungsumfang notwendig. Typische Beispiele des Alltags sind die Verwendung von Versicherungen, um die Auswirkungen eines Schadens zu reduzieren oder die Einschränkung der erlaubten Fahrtgeschwindigkeit in Städten zur Reduktion von Schadenseintrittswahrscheinlichkeiten. Es gibt offensichtlich einen Interessenkonflikt zwischen Risikominimierung und der Aufwendung von Kapital oder der Einschränkung von Nutzungsumfang.
Es ist eine gesellschaftliche Aufgabe, einen Kompromiss zwischen dem Wunsch nach hoher Sicherheit und den notwendigen Maßnahmen zu finden. Diese Aufgabe soll in erster Linie von der Politik gelöst werden.

Ein geeignetes Mittel dieses Ziel zu erreichen ist die Verwendung einer Risikoanalyse. Diese soll Aufschluss über mögliche Schadensereignisse, deren Auswirkungen und mögliche Präventionsmethoden liefern. Die Verwendung von Risikoanalysen ist kein Konstrukt der Neuzeit, sondern existiert bereits seit mehreren hundert Jahren. Das Buch von Peter L. Bernstein „Against the Gods: The Remarkable Story of Risk“ [9] zeigt die geschichtliche Entwicklung von Risikobetrachtungen auf. Die zweite Auflage des Werkes von Bilal M. Ayyub ist eine aktuelle umfassende Referenz zum Thema Risikoanalyse [2].

Im Bereich der chemischen Industrie gab es lange Zeit keine verbindlichen Richtli-

nien, wie die Sicherheit von Anlagen zu bewerten ist und welches Sicherheitslevel als von der Gesellschaft akzeptiert angesehen werden kann. In Folge einer Reihe schwerer Chemieunfälle wurden die aktuellen Gesetze zum Betrieb sicherheitsrelevanter Anlagen entworfen und weiterentwickelt.
Maßgeblich für die Forderung und Entwicklung von einheitlichen Regeln waren insbesondere die Unfälle in Seveso – Italien im Jahr 1976, Bhopal – Indien im Jahr 1984, Enschede – Niederlande und Baia Mare – Rumänien im Jahr 2000 sowie Kolontár – Ungarn im Jahr 2010. Diese Unfälle waren allesamt mit gravierenden Humanschäden verbunden. In Folge des Unfalls in Seveso 1976 entstand das erste europaweite Regelwerk – die Seveso I Richtlinie. Dieses wurde weiterentwickelt und gilt heute in Form der Seveso III Richtlinie 2012/18/EU. Die Seveso III Richtlinie wurde in den Mitgliedsstaaten der Europäische Union (EU) in Form nationaler Gesetzte, Verordnungen und Richtlinien umgesetzt. In Deutschland dient dazu unter anderem das Bundes–Immissionsschutzgesetz (BImSchG) in der derzeitig aktuellen Fassung vom 05.04.2017.

Entsprechend der aktuellen deutschen Gesetze sind geeignete Methoden anzuwenden, um den sicheren Betrieb von sicherheitstechnisch relevanten Anlagen zu gewährleisten. Dazu gehören chemische Anlagen, welche potentiell gefährliche Stoffe lagern, verarbeiten, erzeugen oder anderweitig verwenden. Das aktuelle Grundlagenwerk „*Prozess–und Anlagensicherheit*“ von HAUPTMANNS gibt einen umfassenden Überblick zu rechtlichen Rahmenbedingungen und wie diese konkret umzusetzen sind [57].
Neben konventionell geplanten Anlagen unterliegen auch Anlagen, welche in Modulbauweise entsprechend den im Abschnitt 1.2 dargelegten Konzepten entworfen werden, diesen gesetzlichen Bestimmungen. Modulare Anlagen müssen daher in geeigneter Weise auf die Erfüllung von Sicherheitsanforderungen untersucht werden. Dieser gesonderten Problematik wurde bisher wenig Beachtung geschenkt. Die Arbeit von FLEISCHER u. a. [45] setzt sich als eine der wenigen Veröffentlichungen mit dieser Problematik auseinander. Darin konzentrieren sich FLEISCHER u. a. auf die Sicherheitsbetrachtung von Modulen in Containerbauweise, wie sie im Projekt F^3 erfolgreich eingesetzt wurden. Sie weisen auf die prinzipiellen Probleme einer Sicherheitsbetrachtung von modularen Anlagen hin. Zum einen ist mit den aktuellen Methoden eine Wiederverwendung von bereits durchgeführten Sicherheitsanalysen beispielsweise derer von einzelnen Modulen

nicht möglich. Weiterhin wird die Flexibilität beim Einsatz von Modulen, welche einen der größten Vorteile dieses Konzeptes bildet, stark eingeschränkt. Die Ursache dafür ist, dass bei Änderungen an einer genehmigungspflichtigen Anlage eine erneute Sicherheitsüberprüfung der gesamten Anlage durchzuführen ist. Dies ist sehr kosten– und zeitintensiv und daher ein Problem, welches gelöst werden sollte.
Der Ansatz von FLEISCHER u. a. sieht eine Zweiteilung der Sicherheitsanalyse vor. Die Wechselwirkung zwischen Modulen soll mit Hilfe einer HAZOP analysiert werden. Dies ist aber erst möglich, wenn die Anlagenplanung weit fortgeschritten ist, und eine konkrete Auswahl der einzubindenden Module stattgefunden hat. Die Untersuchung einzelner Module soll unter Verwendung von Checklisten und Heuristiken durchgeführt werden. Diese Untersuchung liefert dann Aufschluss über die Verwendbarkeit der Module für einen bestimmten Prozess. Um die Einsetzbarkeit prinzipiell bewerten zu können, wird die Definition von Stoffklassen, Reaktionsklassen und zulässigen Betriebsfenstern vorgeschlagen. Einem Modul wird dann anhand seiner Eigenschaften jeweils eine diskrete Stufe dieser Kategorien zugeordnet und durch diese Zuordnung kann die Einsetzbarkeit eines Moduls für einen Prozess schnell und frühzeitig bewertet werden. Auf die konkrete Verwendbarkeit dieser intramodularen Sicherheitsanalyse für eine nachfolgende HAZOP wird nicht im Detail eingegangen. Das Problem der Wiederverwendbarkeit von durchgeführten Sicherheitsbetrachtungen von einzelnen Modulen für eine anschließende Analyse der Gesamtanlage ist Motivation für die vorliegende Arbeit. Das konkrete Thema der Arbeit wird im folgenden Abschnitt 1.4 detailliert formuliert.

1.4 Problemstellung dieser Arbeit

Es ist zu beachten, dass eine zeitaufwendige Sicherheitsbetrachtung nach erfolgter Auswahl von Modulen die Zeit bis zur Erteilung der Betriebserlaubnis und damit der Entwicklungszeit maßgeblich verlängern kann. Es ist daher wünschenswert, die Sicherheitsanalyse der geplanten Gesamtanlage so zügig wie möglich durchzuführen.
Ein einzelnes Modul sollte bereits einer Sicherheitsuntersuchung unterzogen werden. Dazu ist die in Abschnitt 1.3 vorgestellte Methode von FLEISCHER u. a.,

welche auf dem Einsatz von Checklisten und Heuristiken basiert, geeignet. Es stellt sich daher die Frage, inwiefern die Erkenntnisse aus der Sicherheitsbetrachtung eines einzelnen Moduls für die Sicherheitsbetrachtung der Gesamtanlage verwendet werden können.
Ein geeignetes Mittel zur Sicherheitsuntersuchung von Gesamtanlagen ist die Durchführung einer HAZOP. Im Rahmen dieser Analyse wird geprüft, wodurch Anlagenparameter vom Normbetrieb abweichen können und mit welchem Risiko eine solche Abweichung verbunden ist. Dazu werden Fehler identifiziert, welche ungewollte Schwankungen von Prozessparametern zur Folgen haben können. Zur Bewertung des Risikos muss die Auswirkung des Fehlers auf die Gesamtanlage betrachtet werden. Dazu ist eine Analyse der Fehlerfortpflanzung notwendig.

Das Ziel der vorliegenden Arbeit ist es zu untersuchen, welche Algorithmen geeignet sind, um eine automatisierte Untersuchung der Fehlerfortpflanzung in modularen Anlagen durchzuführen. Als Basis für die Algorithmen sollen die Beschreibung der Module, die HAZOP–Studien der Module und die Beschreibung der modularen Gesamtanlage dienen.
Anhand eines geeigneten Beispiels soll überprüft werden, welche Auswirkungen von Fehlern, die in einem Modul auftreten, mit der vorgegebenen Instrumentierung in den anderen Modulen der Anlage erkannt und beherrscht werden können. Ein solche automatisierte Bewertung der Fehlerfortpflanzung auf Basis der Sicherheitsuntersuchung von Anlagenmodulen kann die HAZOP einer Gesamtanlage maßgeblich beschleunigen und damit das Innovationstempo erhöhen.

Stand der Technik 2

2.1 Modularisierung

Im Kapitel 1 wird erläutert, dass die Zukunftsfähigkeit der Chemischen und Pharmazeutischen Industrie von Flexibilität und Geschwindigkeit der Entwicklung und Herstellung von Produkten maßgeblich abhängig ist. Als geeignete Mittel um diese Ziele zu erreichen gelten der Einsatz von Mikro- und Millianlagen, sowie die Verwendung von modularen Komponenten. Diese beiden Planungsansätze sind eng miteinander verbunden und werden im folgenden Abschnitt beschrieben.

Die Entwicklung eines neuen Produktes besteht üblicherweise aus vier Phasen. Zu Beginn wird die Herstellbarkeit eines neuen Produktes in einer Laboranlage in Form eines Batchprozesses untersucht. Darauf erfolgt der Entwurf einer Minianlage. Die Produktionsmengen werden dann durch Konstruktion einer Pilotanlage erhöht und der Produktionsprozess umfassend getestet und verfeinert. Auf Basis der Pilotanlage wird zuletzt die Produktionsanlage geplant und das neue Produkt in industriellen Mengen gefertigt. Je nach prognostiziertem Verkaufsvolumen des entwickelten Produktes geschieht die industrielle Produktion als kontinuierlicher oder Batchprozess. [54]

Dieser Entwicklungsprozess ist stark beschleunigbar, wenn die Produktionsmengen der Laboranlage ohne großen Konstruktionsaufwand hoch skaliert werden können. Die Konstruktion einer Pilotanlage ist dann nicht notwendig.

Das Hochskalieren eines entwickelten Batchprozesses ist kompliziert und nicht uneingeschränkt möglich. Dies betrifft insbesondere stark exotherme Reaktionen, da die Wärmeabfuhr in einem Reaktor begrenzt ist. [16]
Durch den Einsatz von Mikro- und Millireaktoren wird das Hochskalieren von Prozessen jedoch ermöglicht und der Entwicklungsprozess somit stark beschleunigt. [54, 16, 58, 72, 60]

Solche Reaktoren sind durch einen kontinuierlichen Betrieb, Strömungskanäle mit Durchmessern im Mikro- bis Millimeterbereich und Wärmeaustauschflächen pro Volumeneinheit, welche im Vergleich zu klassischen Anlagen etwa um den Faktor 100 höher sind, gekennzeichnet. Dies ermöglicht eine hohe Energieableitung, was inhärente Sicherheit zur Folge hat und Scale-Up Faktoren von zehntausend und darüber ermöglicht. [16, 73, 8]

Der Einsatz dieser Reaktoren zur Produktentwicklung erfordert die Umwandlung des Batchprozesses der Laboranlage in einen kontinuierlichen Prozess. Diese Problematik ist seit dem Durchbruch der Mikroprozesse zu Beginn der neunziger Jahre bekannt und wurde weitreichend untersucht. [58] Die Arbeit „*Umwandlung diskontinuierlicher chemischer Prozesse in eine kontinuierliche Prozessführung unter Verwendung mikrostrukturierter Reaktoren - Reaktionstechnik und Sicherheit*“ von HUGO und LOPEZ widmet sich dieser Problematik. HUGO und LOPEZ führen darin aus, dass langsame Reaktionen schlechter als schnelle Reaktionen für die Überführung in einen kontinuierlichen Prozess geeignet sind. Als Grund dafür wird vor allem die lange Verweilzeit angegeben, welche bei langsamen Reaktionen in kontinuierlicher Fahrweise notwendig ist. Eine Erhöhung der Prozesstemperatur kann die Verweildauer reduzieren, sie mindert aber gegebenenfalls die Produktqualität und ist daher nicht unbedingt geeignet. Die zu beachtenden Regeln bei der Überführung eines Semi-Batchprozesses in einen kontinuierlichen Prozess werden von den Autoren für schnell ablaufende, stark exotherme Reaktionen allgemein dargelegt und anhand eines Beispiels konkret angewandt. Der Fokus liegt dabei auf der Dimensionierung der Mikroreaktoren mit dem Ziel einer sicheren Anlagenführung.[64]

Die wirtschaftlichen Vorteile und die mögliche Zeitersparnis bei der Produktentwicklung wurden anhand zahlreicher Fallbeispiele erfolgreich nachgewiesen. [16, 8, 54, 123] Neben Reaktoren sollen auch andere Prozessschritte mittels Mikro- und Millianlagen realisiert werden. Insbesondere die Trennung von Stoffen ist ein aktueller Forschungsschwerpunkt [58]. Die aktuelle Arbeit von YANG u. a. gibt den Kenntnisstand zur Verwendung von Mikroanlagen zur Destillation wieder [155]. LIER u. a. führen im Übersichtsbeitrag weitere modulare Apparate auf. Diese realisieren die Prozessschritte Wärmeaustausch, Reaktion, Mischen von Stoffen und Stofftrennung. Die vorgestellten Apparate sind dabei nicht auf Konstruktionen in Mikro- oder Millibauweise beschränkt. [85]

Mikro- und Millireaktoren sind ein bewährtes Mittel der Chemischen und Pharmazeutischen Industrie, um Produkte schneller und kostengünstiger zu entwickeln. Insbesondere die Skalierbarkeit durch Parallelisierung von vielen Reaktoren der gleichen Bauart ist ein großer Vorteil. Diese Wiederverwendbarkeit ist ein wichtiger Aspekt der Tutzing Thesen [38]. Mikro- und Millireaktoren können als eine Ausprägung modularer Anlagenkomponenten angesehen werden und sind daher geeignete Beispiele, um die erfolgreiche Verwendung von modularen Anlagen zu belegen. Weitere Beispiele stellen die Modularisierung eines Gaswäschers [102] und die Modularisierung einer Anlage zur Hochleistungsflüssigkeitschromatographie [118] dar.
Da Mikro- und Millireaktoren einen Spezialfall modularer Komponenten bilden wird auf ihre Besonderheiten im weiteren Verlauf der Arbeit jedoch nicht weiter eingegangen. Statt dessen liegt der Fokus im weiteren Verlauf dieser Arbeit auf der allgemeinen Verwendung von modularen Anlagenkomponenten und deren Sicherheitsbetrachtungen.
Im Folgenden werden der Forschungsstand zu modularen Anlagen grob wiedergegeben und die offenen Schwerpunkte benannt. Dazu werden Übersichtsarbeiten zu diesem Thema ausgewertet und die Entwicklung der Forschung wiedergegeben, ohne jedoch eine zu ausgeprägte Detailtiefe zu erreichen.

Das Gebiet der Modularisierung von Anlagenkomponenten ist ein verhältnismäßig junges Forschungsgebiet. In Folge der in Kapitel 1 dargelegten hohen Relevanz wird diese Thematik intensiv untersucht.
Ein Nachweis der wirtschaftlichen Sinnhaftigkeit von kleinskaligen Anlagen wurde von SEIFERT u. a. in „*Small scale, modular and continuous: A new approach in plant design*“ erfolgreich erbracht. [122]
Drei Jahre nach Veröffentlichung der Tutzing Thesen [38] wurde von zwei der Teilnehmern des 48. Tutzing Symposiums eine grundlegende Arbeit zur Verwendung von Modulen im Planungsprozess einer verfahrenstechnischen Anlage veröffentlicht. Die Autoren BRAMSIEPE und SCHEMBECKER betrachten in ihrer Arbeit „*Die 50 % – Idee: Modularisierung im Planungsprozess*“ [14] Sichtweisen auf die Modularisierung, definieren verschiedene Typen von Modulen, erläutern deren Einsatzzweck und -zeitpunkt im Planungsprozess und gehen weiterhin auf offene Forschungsfragen ein.
Als besondere Vorteile der Modularisierung werden die hohe Flexibilität und eine

schnelle Anpassung der Produktionskapazität an Marktveränderungen genannt. Weitere Vorteile sind die Möglichkeit einer räumlichen Trennung der Produktion verschiedener Zwischenprodukte zur Einsparung von Transportkosten und die Möglichkeit, einen Großteil der Anlagenmontage an einem beliebigen Ort unter optimalen Bedingungen vornehmen zu können. Am Aufstellungsort der Anlage müssen die Module dann nur noch verbunden werden, was insbesondere bei klimatisch anspruchsvollen Anlagenstandorten sehr vorteilhaft ist.
BRAMSIEPE und SCHEMBECKER fordern eine Moduldefinition derart, dass ein Modul einen hohen Grad an Wiederverwendbarkeit besitzt und losgelöst von einer Gesamtanlage getestet werden kann. Module sollten außerdem nach ihrem Detaillierungsgrad unterschieden werden. Die Aufteilung in Planungsmodule und Variantenmodule wird daher als sinnvoll erachtet. Planungsmodule stellen in erster Linie einen Wissensspeicher dar und dienen der Darstellung der Vielfalt von Variantenmodulen. Sie bieten Ansätze zu Auswahl, Funktionsumfang, Auslegung und Dimensionierung von Variantenmodulen. Ein Variantenmodul soll als 2D und als 3D Version entwickelt werden. Ein 2D Variantenmodul soll Informationen enthalten, welche am Ende des Basic Engineering vorhanden sind. Dies umfasst alle Informationen, welche zum Entwurf eines R&I Fließbildes für ein Modul notwendig sind. Ein 3D Variantenmodul ist um Auslegungsgrößen derart erweitert, dass die Modulfertigung möglich ist, wobei eine genaue Definition der Schnittstellen notwendig ist.
Im Planungsprozess hat der Detaillierungsgrad der verwendeten Variantenmodule maßgeblichen Einfluss. 2D Module erleichtern die Erzeugung von Fließbildern einer Gesamtanlage. Insbesondere ermöglichen sie einen direkten Vergleich verschiedener Anlagenstrukturen. Mit Hilfe von Simulationen können in Kombination mit Planungsmodulen geeignete 3D Module für einen Prozess ausgewählt und die Gesamtanlage entworfen werden. BRAMSIEPE und SCHEMBECKER verweisen auf Literatur, in welcher die zur Erlangung von 2D und 3D Modulen notwendigen Arbeitsschritte dargelegt werden.
Bei der Entwicklung von Regelungs- und Sicherheitskonzepten muss betrachtet werden, welche Aufgaben ein einzelnes Modul losgelöst vom Gesamtsystem erfüllen kann und welche Aufgaben nur im Zusammenspiel mehrerer Module gelöst werden können. Die implementierten Fähigkeiten des Moduls bestimmen also maßgeblich den Entwicklungsaufwand neuer Sicherheitsfunktionen einer Gesamtanlage.

Um Module verwenden zu können, nennen BRAMSIEPE und SCHEMBECKER die folgenden Forschungsschwerpunkte:

- Systematischer Entwurf von 2D, 3D Variantenmodulen und Planungsmodulen, wobei besonders eine Systematik des Modulentwurfs zu definieren ist.
- Die Verbesserung von Ansätzen, wie Module konkret in den Planungsprozess integriert werden können.
- Entwicklung von Berechnungsmodellen zum Scale-Up von Modulen.
- Erstellung von Simulationsmodellen von Modulen, um deren Variantenauswahl und konkrete Auslegung durchführen zu können.
- Entwicklung eines Datenmodells, um Datenanreichung und Datenaustausch zu ermöglichen.

Ein weiterer Übersichtsbeitrag zum Thema Modularisierung stammt von URBAS u. a. . Die Autoren legen ihren Fokus dabei auf die Prozessführung mit Hilfe modularer Anlagenkomponenten. Ein besonderer Schwerpunkt stellt die Zusammenarbeit von internen Komponenten eines Moduls, wie der Automatisierung und implementierten Sicherheitsfunktionen, mit den externen Komponenten, wie dem übergeordneten Prozessleitsystem, dar.
Zum Zeitpunkt der Veröffentlichung der Arbeit „*Modularisierung und Prozessführung*“ von URBAS u. a. gab es noch keine einheitliche Definition des Begriffs „Modul“ . Die Autoren definieren den Begriff Modul in Anlehnung an die Konstruktionslehre als „abgeschlossene und wiederverwendbare Einheiten zur Erfüllung einer oder mehrerer Prozessfunktionen, die im Prozessführungskontext sinnvoll zusammengefasst werden können.“ [131, S. 2] Die für die Implementierung der Prozessfunktion notwendigen Equipments, Instrumente und Automatisierungsfunktionen sollen im Modul enthalten sein. Weiterhin benötigt ein Modul klar definierte Schnittstellen zu seiner Umgebung. [131, S. 2]. Als Umfang eines Moduls wird eine beliebige Ebene zwischen Teilanlage und Einzeloperation eines Prozesses vorgeschlagen. Der Mangel einer klaren Methodik zur Definition von Modulen hat Forschungsbedarf zur Folge. Als besonderer Schwerpunkt wird die von BRAMSIEPE und SCHEMBECKER ebenfalls geforderte Entwicklung von gewerkeübergreifenden formalen Informationsmodellen empfohlen. [131]

Als dritte Übersichtsarbeit zum Thema Modularisierung soll auf die Arbeit „*Multikriterielle Aspekte der Modularisierung bei der Planung verfahrenstechnischer Anlagen*“ von HADY und WOZNY [55] verwiesen werden. Diese Arbeit betrachtet zum einen allgemeine Fragestellungen, wie die Definition von Modulen und deren Abgrenzung zum Baukastenprinzip und zum anderen Aspekte der modularen Anlagenplanung. Weiterhin wird ein Modularisierungskonzept im Detail vorgestellt, welches die Beschreibung und Verwendung von Modulen ermöglichen soll. Die Autoren gehen ebenfalls auf die Anwendbarkeit der Modularisierung für die in diesem Kapitel bereits genannten Minianlagen ein und legen außerdem die Auswirkungen der Modularisierung auf die Kostenschätzung eines Anlagenbaus dar.
HADY und WOZNY bekräftigen die bereits ausgeführte Notwendigkeit und die Vorteile einer modularen Anlagenplanung. Im Rahmen einer Industriebefragung stellen sie jedoch fest, dass die modulare Anlagenplanung nur in geringem Maße eingesetzt wird. HADY und WOZNY erläutern den Begriff der Modularisierung und ziehen Parallelen zur Automobilindustrie und den dort ebenfalls etablierten Baukastensystemen. Ein Modul wird in Abgrenzung zu Bausteinen als eine Einheit charakterisiert, welche eine definierte Funktionalität allgemein abdecken soll. Ein Baustein deckt lediglich in Bezug auf das System, dessen Bestandteil er ist, die gewünschte Funktionalität ab.
Den Vorteil einer möglichen Vormontage von modularen Anlagen belegen die Autoren anhand mehrere Quellen, weisen aber darauf hin, dass die in diesem Zusammenhang verwendeten Module eher als Einzelstücke anzusehen sind, da die konzipierten Anlagen zumeist nur in sehr wenige Einzelmodule zerlegt wurden. An dieser Stelle zeigt sich besonders deutlich, dass die Verwendung von Modulen Kosten reduzieren kann, ohne zwangsläufig einen hohen Grad an Wiederverwendbarkeit zur Folge zu haben. Als besonders wichtig gilt daher die bereits genannte systematische Entwicklung von Modulen und deren Darstellung in einer Form, welche Weiterentwicklungen und Austausch begünstigt.
Zur Ablage von bereits entwickelten Modulen schlagen die Autoren die Verwendung einer Bibliothek von Modulen und Dokumenten vor, welche von allen am Anlagenplanungsprozess beteiligten Personen verwendet werden kann. Eine solche Datenbank wurde entwickelt und wird von HADY und WOZNY entsprechend referenziert. Die entwickelte Datenbank wurde an der TU Berlin erfolgreich eingesetzt und liefert in Kombination mit dem vorgestellten Vorgehen

zum Einsatz von Modulen in der Anlagenplanung einen detaillierten Ansatz für die Industrie und weitere Forschungsvorhaben. [55]

Die Auswahl eines geeigneten Moduls sollte besonders bei großen Datenbanken rechnergestützt erfolgen. OBST, DOHERR und URBAS stellen einen Algorithmus vor, mit Hilfe dessen die Eignung eines Moduls für einen gegebenen Einsatzzweck bewertet werden kann. [98]

Ein vergleichbarer Ansatz zum von HADY und WOZNY vorgestellten Vorgehen zur Verwendung von Modulen wurde von UZUNER in [133, 132] erarbeitet. In „*Ein wissensbasiertes System zur Unterstützung von R&I-Fließbild Designprozessen auf der Grundlage eines modulbasierten Ansatzes*“ wird gezeigt, wie die Erstellung eines Rohrleitungs– und Instrumentenfließschema (Piping and instrumentation diagram, P&ID) durch Unterteilung einer Gesamtanlage in wiederverwendbare Funktionsgruppen und die Verwendung einer wissensbasierten Software geeignet beschleunigt werden kann. Module sollen laut UZUNER derart definiert werden, dass sie prozesstechnisch sinnvoll sind und einen möglichst hohen Grad an Wiederverwendbarkeit aufweisen. Der Autor folgt damit dieser etablierten Anforderung an ein Modul. Ein Modul soll Standard-Prozesseinheiten wie Pumpen, Verdichter, Wärmeübertrager, Behälter, Reaktoren oder Kolonnen umfassen und weiterhin die notwendigen Elemente der Sicherheitstechnik, Regelungstechnik, Nahverrohrung und Instrumentierung enthalten. Die damit verbundene Vereinfachung und Beschleunigung der Planungsarbeit wird aufgezeigt und best-practise Lösungen präsentiert.

Eine Weiterentwicklung und Konkretisierung der von BRAMSIEPE und SCHEMBECKER, UZUNER und SCHEMBECKER und HADY und WOZNY [14, 133, 55] vorgestellten modularen Planungsansätze findet sich in der Arbeit „*Planungsansatz für modulare Anlagen in der chemischen Industrie*“ von FLEISCHER-TREBES u. a. [46]. Die Autoren stützen sich dabei schwerpunktmäßig auf das Projekt F^3–Factory [17]. Sie legen ausführlich dar, wie mit Hilfe einer Datenbank bestehend aus Modulen und zugehörigen Planungsdokumenten wie Berechnungen, Fließbildern, Betriebsanleitungen und Apparatelisten während der Planung einer neuen Anlage geeignete Module ausgewählt werden können. Module gelten als geeignet, wenn sie zuvor definierte Prozessparameter und Funktionen direkt erfüllen, oder wenn sie durch geringfügige Modifikationen dazu in die Lage versetzt werden können. Prozessparameter sind dabei beispielsweise geforderte

Durchflussmengen, Drücke und Temperaturen; als Funktionen gelten Prozessschritte wie Pumpen oder Rühren. Die Datenbank dient als wachsender Speicher an Engineeringleistung und bietet für alle an der Planung beteiligten Personen eine Planungsgrundlage und Wissensablage.

Der Forschungsschwerpunkt der Simulation ist ein weiterhin intensiv zu untersuchendes Feld. Die Arbeit „*Towards an integrated use of simulation within the life-cycle of a process plant*“ von OPPELT, WOLF und URBAS betrachtet die bisherige Verwendung von Simulationen bezogen auf den gesamten Lebenszyklus einer prozessleittechnischen Anlage. Die Autoren kommen zu dem Schluss, dass Simulationen zwar bereits verwendet werden, die Leistungsfähigkeit von bereits vorhandener Software aber nicht ausgenutzt wird. Die Integration in den Lebenszyklus einer Anlage bedarf weiterer Forschung wobei besonders der Vereinheitlichung von Schnittstellen eine große Bedeutung beigemessen wird. Eine Bereitstellung von Simulationsmodellen von Komponentenlieferanten wird als sehr nützlich erachtet. [103] Im Rahmen der Modularisierung könnte genau diese Aufgabe erfolgreich gelöst werden. Dazu sind die von BRAMSIEPE und SCHEMBECKER in [14] formulierten Arbeiten zur Erstellung von Simulationsmodellen für Module durchzuführen.

Im Bereich der Darstellung von Daten wurden bereits wichtige Fortschritte erzielt. Für die Beschreibung von Modulen wurde das Module Type Package (MTP) entwickelt, welches in [100] und [101] vorgestellt wird. Es dient als Informationsträger, welcher alle Modulinformationen beinhaltet, die zur Integration eines Moduls benötigt werden [100, S. 2]. Wird dieser Informationsträger erfolgreich verwendet, so kann ein Modullieferant das gesamte Modulengineering durchführen und der Betreiber mit wenig Aufwand ein geliefertes Modul in seine Anlage integrieren, ohne das Modul selbst detailliert zu kennen. Ein wichtiger Schritt zur Integration eines Moduls ist die Transformation des MTP auf ein Modell, welches von der Gesamtanlage genutzt werden kann. Ein solches Informationsmodell kann auf Basis von Open Platform Communications Unified Architecture (OPC-UA) entworfen werden. In [151] beziehungsweise [150] zeigen WASSILEW u. a., wie die in einem MTP gespeicherten Modulinformationen in einem OPC-UA Gesamtmodell abgebildet werden können. Auf einem OPC-UA Server können die Modulinformation dadurch online durchsucht werden, was eine wichtige Grundlage für Plug-and-Produce Lösungen darstellt.

In der aktuellen Arbeit „*Transformable Production Concepts: Flexible, Mobile, Decentralized, Modular, Fast*“ [84] wird erneut die Notwendigkeit modularer Anlagen dargelegt und die bereits erprobten Konzepte der Modularisierung bewertet. Es werden die im Abschnitt 1.1 bereits benannten Projekte F^3–Factory [17] und CoPIRIDE [126] sowie der daraus hervorgegangene „Evotrainer“ beziehungweise „EcoTrainer“ [79] betrachet. Die Autoren stellen fest, dass mit Ausnahme von Modulen in Containerbauweise der große Durchbruch der modularen Strategie noch immer nicht erfolgt ist. Weiterhin werden Arbeiten zur Wirtschaftlichkeit von modularen Ansätzen ausgewertet (unter anderem [122, 16]). LIER, WÖRSDÖRFER und GRÜNEWALD kommen zu dem Schluss, dass modulare Anlagen in Folge einer deutlich verkürzten Amortisierungszeit für wechselnde Marktverhältnisse bestens geeignet sind. Für längere Produktlebenszyklen sind derzeit konventionell geplante Anlagen die wirtschaftlich bessere Wahl. Die Ursache dafür sind geringere Betriebskosten und eine auf den Prozess genauer abgestimmte Anlage. Die in [14] geforderten Berechnungsmodelle für die Skalierung von modularen Anlagen wurden bisher noch nicht entwickelt. Die Arbeiten von BRODHAGEN u. a. [16] und GRUNDEMANN, SCHOENITZ und SCHOLL [54] zeigen aber ein mögliches Vorgehen auf. Die Verfasser bestätigen den von URBAS u. a. in [131] genannten akuten Bedarf nach Forschungsarbeit zur Automatisierung von Modulen und deren Einbindung in ein übergeordnetes Prozessleitsystem. Zusätzlich verweisen sie auf die Notwendigkeit von anpassbaren, modularen Logistiklösungen.

Die ebenfalls aktuelle Arbeit „*Modules in process industry - A life cycle definition*“ von HOHMANN u. a. [61] bestätigt ebenfalls diese Aussagen. Die Autoren geben einen groben Überblick zur Entwicklung der Modularisierung von Anlagen und nennen eine Reihe an Herstellern, welche bereits modulare Anlagen für die Chemische und Pharmazeutische Industrie zum Kauf anbieten.
Sie verdeutlichen die Unterschiede von konventioneller Anlagenplanung und modularen Ansätzen und werten neben den bereits aufgeführten Ansätzen ([14, 133, 55, 46]) noch weitere aus. Sie kommen zu dem Schluss, dass die bisher entwickelten Vorgehen jeweils nur einen Spezialfall oder einen Teil einer kompletten Anlagenplanung bezogen auf den gesamten Lebenszyklus betrachten. Die Konzepte sind laut Aussage von HOHMANN u. a. nicht zu einem Gesamtkonzept kombinierbar, da die Begrifflichkeit eines Moduls im Rahmen der Prozessleittechnik noch immer nicht standardisiert ist und weil einheitliche Arten der

Informationsdarstellung nicht vorhanden sind oder zumindest nicht verwendet werden.
Die organisatorischen Konsequenzen der Modularisierung auf den Lebenszyklus wurden bereits von OBST u. a. in [99] betrachtet. Eine Weiterentwicklung dieser Arbeit wurde durch den Namur Arbeitskreis 1.12 in Form der „*NE 148: Anforderungen an die Automatisierungstechnik durch die Modularisierung verfahrenstechnischer Anlagen*“ [10] veröffentlicht. Darin wird ein prinzipieller Leitfaden für Anlagenbauer, Lieferanten und Betreiber zu Entwicklung und Einsatz von modularen Anlagen präsentiert. Der Fokus liegt dabei auf der Automatisierung von Modulen und deren Einbindung in übergeordnete Systeme.
HOHMANN u. a. präsentieren einen konkreten Planungsansatz, welcher den gesamten Lebenszyklus einer modular aufgebauten Anlage abdeckt. Da für die Automatisierung von Modulen noch kein einheitlicher Standard gefunden wurde gehen sie jedoch nicht im Detail auf die in [10] vorgestellten Methoden ein.
Ein Modul wird in diesem Ansatz definiert als „ein während der Planung und Fertigung von modularen Anlagen unveränderbares Element, welches eine bestimmte Funktion für einen Prozess erfüllt und welches im Rahmen weiterer Entwicklungen im Rahmen der Prozessindustrie wiederverwendbar ist“ [61, S. 2]. Durch Verwendung einer Blockdarstellung („block representation frame“) werden die Entwicklungsstadien einer Anlage abgebildet. Ein Block enthält dabei Felder für Informationen, deren Anzahl und Umfang bei Fortschreiten der Planung zunimmt und welche durch Engineeringleistungen gefüllt werden. Die Felder beschreiben beispielsweise Kostenschätzungen, Massenbilanzen, notwendige Drücke und Temperaturen, entwickelte Simulationsmodelle und konkrete 3D Layouts.

Zusammenfassend lässt sich feststellen, dass die Modularisierung von Anlagen ein intensiv erforschtes Themengebiet darstellt. Der Nachweis der Notwendigkeit von modularen Anlagen und deren erwartete Verwendungsmöglichkeiten ist erbracht. Trotz zahlreicher Studien, die großes Entwicklungspotenzial belegen, gibt es weiterhin großen Forschungs- und Entwicklungsbedarf, um eine Steigerung der Akzeptanz und eine umfangreiche Anwendung in der Industrie zu erreichen.

2.2 Gesetzliche Rahmenbedingungen zur Genehmigung von Chemischen Anlagen

Abschnitt 1.3 erläutert, dass in Folge schwerer Unfälle in Industrieanlagen eine Vereinheitlichung von Sicherheitsstandards in der EU angestrebt wird. Dies geschieht durch europäische Richtlinien, welche von den Mitgliedstaaten in nationales Recht umzusetzen sind.

In diesem Zusammenhang ist vor allem die Richtlinie 2012/18/EU (SEVESO III) relevant. Diese wird in Deutschland in den Regelungen des Bundes-Immissionsschutzgesetzes (BImSchG), des Umweltverträglichkeitsprüfungsgesetzes (UVPG), und in der Störfall–Verordnung (12. BImSchV) umgesetzt. Weitere europäische Richtlinien, welche fü verfahrenstechnische Anlagen zu beachten sind, sind die Maschinen–Richtlinie 2006/42/EG (MRL), die Industrieemissionsrichtlinie 2010/75/EU (IED) und die Druckgeräte–Richtlinie 2014/68/EU (DGRL).
Zusätzlich zu den Richtlinien der EU haben sich zahlreiche Nationen auch auf globale Regeln geeinigt. Dazu zählt beispielsweise das global harmonisierte System zur Einstufung und Kennzeichnung von Chemikalien (GHS), welches europaweit durch die Verordnung Nr. 1272/2008/EG (CLP) umgesetzt ist.

Das BImSchG wird durch zahlreiche Verordnungen ergänzt und präzisiert.
Für den Betrieb von verfahrenstechnischen Anlagen ist vor allem die Verordnung über genehmigungsbedürftige Anlagen (4. BImSchV) von Interesse, in der geregelt wird, welche Anlagen einer immissionsschutzrechtlichen Genehmigung bedürfen.
Darüber hinaus dient die 12. BImSchV der Verhütung schwerer Unfälle, die durch bestimmte Industrietätigkeiten hervorgerufen werden könnten und der Begrenzung der Unfallfolgen für die menschliche Gesundheit und die Umwelt. Weiterhin sind die Bestimmungen der Verordnung zum Schutz vor Gefahrstoffen (GefStoffV) sowie der Betriebssicherheitsverordnung (BetrSichV) bei Industrieanlagen einzuhalten.

Die genannten Richtlinien, Gesetze und Verordnungen werden durch Technische Regeln und Leitfäden ergänzt. Diese definieren den Stand der Technik und geben Empfehlungen für die Umsetzung von Gesetzen und Verordnungen. Wichtige technische Regeln sind beispielsweise die Technische Regeln für Anlagensicherheit

(TRAS), die Technische Regeln für Betriebssicherheit (TRBS), die Technische Regeln für Gefahrstoffe (TRGS), die Technische Regeln für wassergefährdende Stoffe (TRwS) und die Technische Regeln für biologische Arbeitsstoffe (TRBA).

Bei Überschreitung von festgelegten Mengenschwellen für verschiedene gefährliche Stoffe sind die Bestimmungen der 12. BImSchV von Anlagenbetreibern einzuhalten. Es werden Anlagen mit Betriebsbereichen „der unteren“ und „der oberen Klasse“ (§1 Abs. 1 S. 1 12. BImSchV) definiert. Die Einordnung in eine Klasse basiert auf der vorhandenen Menge von gefährlichen Stoffen, wobei das Über- oder Unterschreiten festgelegter Grenzwerte zu einer Klassifikation führt (§2 Nr. 1 f. 12. BImSchV). Die gefährlichen Stoffe und deren Mengenschwellen sind im Anhang I 12. BImSchV aufgeführt. Entsprechend §3 Abs. 1 12. BImSchV hat der Betreiber „. . . die nach Art und Ausmaß der möglichen Gefahren erforderlichen Vorkehrungen zu treffen, um Störfälle zu verhindern . . .“ . Als Störfall gilt nach §2 Nr. 7 12. BImSchV „ein Ereignis, das unmittelbar oder später innerhalb oder außerhalb des Betriebsbereichs zu einer ernsten Gefahr oder zu Sachschäden . . . führt“ . Ein „Ereignis“ ist eine „Störung des bestimmungsgemäßen Betriebs in einem Betriebsbereich unter Beteiligung eines oder mehrerer gefährlicher Stoffe“ (§2 Nr. 6 12. BImSchV). Eine „ernste Gefahr“ ist nach §2 Nr. 8 12. BImSchV definiert als „eine Gefahr, bei der das Leben von Menschen bedroht wird oder schwerwiegende Gesundheitsbeeinträchtigungen von Menschen zu befürchten sind, die Gesundheit einer großen Zahl von Menschen beeinträchtigt werden kann oder die Umwelt, insbesondere Tiere und Pflanzen, der Boden, das Wasser, die Atmosphäre sowie Kultur oder sonstige Sachgüter geschädigt werden können, falls durch eine Veränderung ihres Bestandes oder ihrer Nutzbarkeit das Gemeinwohl beeinträchtigt würde.“ Der Anlagenbetreiber, dessen gefährliche Stoffe die Mengenschwellen der Spalte 5 des Anhangs I der 12. BImSchV überschreiten und der damit eine Anlage der „oberen Klasse“ betreibt, hat darüber hinaus die erweiterten Pflichten der 12. BImSchV zu erfüllen. Dazu zählt unter anderem das Verfassen eines Sicherheitsberichtes (§9 Abs. 1 12. BImSchV), in dem dargelegt wird, dass „die Gefahren von Störfällen und mögliche Störfallszenarien ermittelt, sowie alle erforderlichen Maßnahmen zur Verhinderung derartiger Störfälle und zur Begrenzung ihrer Auswirkungen auf die menschliche Gesundheit und die Umwelt ergriffen wurden“ (§9 Abs. 1 Nr. 2 12. BImSchV). Der erstellte Sicherheitsbericht muss eine „Beschreibung der Szenarien möglicher Störfälle nebst

ihrer Wahrscheinlichkeit oder den Bedingungen für ihr Eintreten ...“ (Anhang II Abschnitt IV S. 1 12. BImSchV) und eine „Abschätzung des Ausmaßes und der Schwere der Folgen der ermittelten Störfälle ...“ (Anhang II Abschnitt IV Nr. 2 12. BImSchV) enthalten. In Folge dieser Formulierung können deterministische oder probabilistische Methoden zum Einsatz kommen. Eine Reihe akzeptierter Methoden wird in „*Der Sicherheitsbericht nach Störfall–Verordnung – Eine Handlungshilfe für Behörden und Betreiber – Stand 01.03.2009*“ [37, S. 20 f.] aufgeführt. Eine der genannten Methoden ist die weit verbreitete HAZOP. Auf diese Methode wird im folgenden Abschnitt 2.3 weiter eingegangen.

2.3 Sicherheitsuntersuchung in Form einer HAZOP

Eine Sicherheitsuntersuchung soll sicherstellen, dass eine Anlage ein toleriertes Risiko nicht überschreitet. Dazu sind einige Begriffe zu definieren. Die Definitionen sind noch zu ergänzen!
„Risiko“ : DIN EN 61511-1
„Schaden“ : DIN EN 61511-1
„Fehler“ : DIN EN 61511-1

Die Anwendung eines Verfahrens zur Prognose, Auffinden der Ursache, Abschätzen der Auswirkungen, Gegenmaßnahmen (HAZOP) ist ein bewährtes Mittel, um die in der 12. BImSchV geforderte Gefahrenanalyse durchzuführen. Die Methode wurde 1973 erstmals von LAWLEY auf dem AICHE Loss Prevention Symposium öffentlich vorgestellt und ein Jahr später publiziert [80]. Seit dem wurde die Methode vielfach angewandt und weiterentwickelt.
KLETZ gibt in „*Hazop—past and future*“ einen kurzen historischen Überblick über die Entstehung und Entwicklung dieser Methode [71]. DUNJÓ u. a. arbeiten in „*Hazard and operability (HAZOP) analysis. A literature review*“ [43] 166 Veröffentlichungen zur HAZOP aus dem Zeitraum 1974 bis 2009 auf, fassen die grundlegenden Gedanken der untersuchten Veröffentlichungen zusammen, teilen sie in verschiedene Gruppen ein und ermitteln den Stand der Technik. Sie stellen fest, dass die Anzahl der Veröffentlichungen zur HAZOP vom Jahr ihrer Vorstellung bis zur zweiten Hälfte der neunziger Jahre stark zugenommen hat. Der Themenschwerpunkt hat sich dabei stark verschoben. Die ersten Arbeiten

erarbeiten mögliche Anwendungsfälle der HAZOP, analysieren den abgedeckten Anlagenumfang und versuchen diesen durch Anpassungen der Methode zu erweitern. Der größte Teil der Arbeiten untersucht Möglichkeiten eine HAZOP zu automatisieren. Die aktuellsten Arbeiten versuchen die HAZOP mit anderen Methoden wie beispielsweise Simulationen zu kombinieren (siehe beispielsweise [82]). DUNJÓ u. a. kommen zu dem Schluss, dass HAZOP zwar bereits die am meisten untersuchte Methode zur Analyse von Gefahren in Prozessen ist, dass aber weiterhin Verbesserungen notwendig sind. Der Mensch als Gefahrenquelle für eine Anlage wird noch nicht hinreichend im Rahmen einer HAZOP untersucht, weiterhin wird eine HAZOP in weiten Teilen von Menschen durchgeführt, was zu Ungenauigkeiten und Fehlern führen kann. Darüber hinaus sind Störungen und Ausfälle von speicherprogrammierbaren Steuerungen, welche eine wichtige Rolle bei der Steuerung und Regelung von Anlagen haben, derzeit nur ungenügend durch eine HAZOP abgebildet. Diese Punkte erfordern weitere Forschung.

Eine Hazop kann durch Automatisierung beschleunigt werden. Fehlerfortpflanzung in ein wichtiger Teil einer Hazop. System zur Automatisierung einer hazop sind daher geeignete Suchstellen für Verfahren zur Fehlerfortpflanzung für die hazop einer Gesamtanlage, welche hazops von Teilanlagen kennt.

2.3.1 Durchführung einer HAZOP

Eine ausführliche Anleitung zur konkreten Durchführung einer HAZOP findet sich beispielsweise in „*HAZOP: Guide to Best Practice*“ [35].
Eine HAZOP wird von einem interdisziplinären Team in Form einer kreativen Analyse der Anlage durchgeführt. Das Ziel ist es mögliche Abweichungen eines Prozesses vom Sollverhalten zu untersuchen. Dazu wird die Gesamtanlage zuerst in kleinere Funktionsgruppen die sogenannten „nodes“ untergliedert. Die „nodes“ werden dann nacheinander untersucht. Dazu wird die Sollfunktion beziehungsweise der Sollwert einer betrachteten Variable oder eines Prozesses innerhalb der „node“ definiert. Anschließend wird dafür eine Reihe an Leitworten wie „kein/nicht“ ,„mehr“ ,„weniger“ ,„teilweise“ ,„Umkehrung“ ,„anders als“ oder „sowohl als auch“ ausgewählt, mit Hilfe derer eine physikalisch sinnvolle Abweichung vom Sollverhalten beschrieben wird. Darauf folgend werden mögliche Ursachen und Konsequenzen der betrachteten Abweichung abgeschätzt. Ursachen und Aus-

wirkungen können dabei sowohl innerhalb als auch außerhalb der betrachteten „node“ entstehen beziehungsweise wirksam werden. Danach wird das Risiko der ermittelten Auswirkungen unter der Annahme, dass keine Gegenmaßnahmen bestehen, abgeschätzt. Im Anschluss werden die vorhandenen Gegenmaßnahmen ermittelt und bewertet. Dazu wird das sich ergebende Restrisiko ermittelt, welches bei Vorhandensein der Gegenmaßnahmen zu erwarten ist. Sind ungenügende Schutzeinrichtungen zur Einhaltung des tolerierten Risikos vorgesehen, so soll durch das HAZOP–Team eine zur Senkung des Risikos geeignete Maßnahme vorgeschlagen werden.

2.3.2 Automatisierung einer HAZOP

Die Durchführung einer HAZOP ist kompliziert, zeitaufwendig und arbeitsintensiv. Außerdem ist die Verlässlichkeit der erarbeiteten Ergebnisse einer HAZOP maßgeblich von der Erfahrung der durchführenden Experten abhängig. Durch den hohen Zeitaufwand und die wiederkehrende Anwendung der gleichen Leitworte stellt sich schnell eine ermüdende Routine eine, welche das Übersehen wichtiger Zusammenhänge begünstigt. In Folge dieser Tatsachen wurden zahlreiche computergestützte Systeme entwickelt, um die Durchführung einer HAZOP zu unterstützen. Diese Expertensysteme sollen die Wiederverwendbarkeit von gewonnenem Expertenwissen ermöglichen, die Anwendung der Leitworte vereinfachen und die Wahrscheinlichkeit von übersehenen Zusammenhängen reduzieren. Insgesamt sollen also die Kosten der Durchführung einer HAZOP gesenkt und die Qualität der Ergebnisse gesteigert werden.

Eine erste Arbeit zur Automatisierung von HAZOPs wurde von PARMAR und LEES veröffentlicht [107, 108]. Die untersuchte Anlage zur Trennung von Wasser und Kohlenwasserstoffen wird basierend auf dem P&ID in Einheiten unterteilt. Durch auslösende und terminierende Ereignisse wird die Fortpflanzung von Fehlern beschrieben. Mit Hilfe eines regelbasierten Algorithmus können die Ursachen und Auswirkungen der Abweichung von Prozessvariablen ermittelt werden. Die Analyse ist dabei auf jeweils benachbarte Einheiten begrenzt und eine anlagenweite Untersuchung ist nicht möglich, obwohl eine solche Betrachtung ein wichtiger Teil einer HAZOP ist. Das System ist in den Programmiersprachen Fortran 77 and Prolog umgesetzt. Das implementierte Expertenwissen ist nur

ungenügend abstrahiert, wodurch eine Wiederverwendbarkeit erschwert wird. Die Anwendbarkeit für Anlagen im großindustriellen Maßstab konnte bisher nicht gezeigt werden. Eine Weiterentwicklung dieses Ansatzes wird daher als nicht sinnvoll erachtet.

CATINO und UNGAR stellen in „*Model-based approach to automated hazard identification of chemical plants*“ ein System mit dem Namen „Qualitative Hazard Identification (QHI)“ vor [19]. Die Autoren definieren in einer Bibliothek allgemeine Fehler wie Lecks oder verstopfte Filter und je nach Struktur der untersuchten Anlage werden diese untersucht. Das Vorliegen eines Fehlers wird mit Hilfe automatisch generierter Prozessmodelle simuliert und die Auswirkung der Fehler bewertet. Der dazu notwendige Code ist unabhängig von einer konkreten Anlage formuliert, benötigt zur Simulation aber eine weitere Bibliothek mit Prozessmodellen. QHI ist flexibel einsetzbar, benötigt aber aktualisierte Bibliotheken. In Folge der sehr rechenintensiven Algorithmen konnte sich dieses System nicht in der Industrie etablieren. Im Rahmen modularer Anlagen müssten die Bibliotheken aufwendig aktualisiert werden, weswegen die Möglichkeit einer Weiterentwicklung von QHI für die Sicherheitsuntersuchung modularer Anlagen nicht weiter analysiert wird.

KHAN und ABBASI präsentieren in „*OptHAZOP — an effective and optimum approach for HAZOP study*“ eine Adaption des konkreten Vorgehens bei der Durchführung einer HAZOP [68]. Durch Verwendung einer Wissensbasis wollen die Autoren die notwendige Arbeitszeit einer HAZOP in etwa halbieren. Die konkrete Implementierung der Wissensbasis bezeichnen die Autoren als TOPHAZOP, welche sie in „*TOPHAZOP: a knowledge-based software tool for conducting HAZOP in a rapid, efficient yet inexpensive manner*“ vorstellen [69]. Als Implementierungsumgebung nutzen KHAN und ABBASI die Software „G2“ der Firma „gensym“ . Die Wissensbasis ist in einen allgemeinen Teil und den Prozess spezifischen Teil untergliedert. Der allgemeine Teil enthält generische Fehlerursachen und Fehlerauswirkungen, der Prozess spezifische Teil umfasst für bestimmte Prozesse spezifische Kombinationen aus Ursache und Wirkung, sowie die Fortpflanzung von Auswirkungen auf andere Prozesseinheiten. Die Software wurde durch KHAN und ABBASI weiterentwickelt, zu EXPERTOP umbenannt und in Visual C++ neu implementiert [70]. Die Anwendung von EXPERTOP kann die Durchführung einer HAZOP erfolgreich beschleunigen, wenn die zu

untersuchende Anlage durch die vorhandene Wissensbasis adäquat beschrieben werden kann. Das Werkzeug ist jedoch nicht in der Lage abstrakt definiertes Wissen auf neue Anlagen zu übertragen. Aus diesem Grund wird EXPERTOP im Rahmen der vorliegenden Arbeit als nicht geeignet bewertet.

Die besonders umfangreiche Veröffentlichung von MCCOY u. a. beschreibt das computergestützte Werkzeug HAZID [90, 92, 91, 93, 94]. HAZID besteht aus einer Reihe von Werkzeugen, welche auf Basis von Wissensdatenbanken durch qualitative Fehlerfortpflanzung die Ursachen und Auswirkungen von Prozessfehlern bestimmen. Als Eingangsdaten wird ein P&ID benötigt, welches in der Software „SmartPlant P&ID“ entweder entworfen oder in diese importiert werden muss. Der „Hazard Import Wizard“ erstellt auf Basis des P&ID ein Modell der Anlage. Das Modell wird mit Hilfe von zwei Bibliotheken erweitert, welche Stoffeigenschaften, mögliche Fehlerursachen und Fehlerauswirkungen sowie Informationen zur Fortpflanzung von Fehlern enthalten. Die „HAZID Analysis Engine“ führt dann eine hochgradig automatisierte Analyse der Anlage durch und liefert einen umfassenden Bericht im XML Format. Dieser kann mit Hilfe des „HViewer Results Browser“ betrachtet werden, wobei der Nutzer vielfältige Einstellmöglichkeit hat, um die Anzeige anzupassen und den XML Bericht gezielt zu durchsuchen. Zusätzlich wird der Bericht in einem Format generiert, welcher auf die Empfehlungen zur Notation eines HAZOP–Berichts (vgl. [35]) angepasst ist.
Die erste Bibliothek beschreibt „Unit Models“ , welche in einer hierarchischen Struktur gespeichert werden, wodurch das Vererben von Eigenschaften unterstützt wird. Unit Models sind wohl unterscheidbare Einheiten, welche Prozessfunktionen erfüllen. Je nach Detaillierungsgrad dieser Einheiten sind die erfüllbaren Funktionen mehr oder weniger umfassend. Die konkrete Definition eines Unit Models kann durch den Nutzer mit Hilfe des „Model Generation Tool“ erfolgen. Ein Unit Model umfasst unter anderem Informationen zu den Ein– und Ausgängen und zu möglichen Fehlerfortpflanzungen, welche mit Hilfe von Signed Directed Graph (SDG) modelliert werden. (vlg. [92])
Die zweite Bibliothek umfasst Eigenschaften von Flüssigkeiten. Deren Analyse zeigt beispielsweise eine Brandgefahr oder Toxische Wirkung auf, welche durch das ungewollte vermischen zweier Substanzen entsteht. (vgl. [91])
Die HAZID Analysis Engine führt auf Basis der Unit Models und der Eigenschaf-

ten der verwendeten Stoffe eine umfassende Fehleranalyse durch. Dazu wird für eine gegebene Prozessabweichung ein SDG konstruiert, welcher die Abweichung mit allen möglichen Auswirkungen verbindet. Die Pfade zu jeder möglichen Auswirkung werden dann mit Hilfe der zuvor definierten Eigenschaften in den Unit Models und den Stoffeigenschaften auf Gültigkeit geprüft und die ungültigen Pfade werden entfernt. Die verbleibenden Pfade werden abgespeichert und in den Ergebnisreport übernommen. (vgl. [91, 94])
HAZID wurde seit seiner Veröffentlichung erfolgreich weiter entwickelt und ist kommerziell über die Website (`https://www.hazid.com/` zu erwerben.
Die der Fehlerfortpflanzung zugrunde liegenden Algorithmen werden in den genannten Veröffentlichungen oberflächlich beschrieben. Weiterhin gehen die Autoren davon aus, dass die Bibliothek der Model Units durch einzeln durchgeführte HAZOPs um wichtige Details ergänzt werden kann. Bei der Sicherheitsuntersuchung modularer Anlagen ist davon auszugehen, dass die Durchführung einer HAZOP für einzelne Module sinnvoll ist. Wenn es gelingt einzelne Module in Form von Model Units zu beschreiben, so ist HAZID nach dem aktuellen Forschungsstand ein vielversprechendes Mittel, um die Sicherheitsuntersuchung einer aus Modulen bestehenden Anlage zu beschleunigen. Da der verwendete Code jedoch nicht frei verfügbar ist, wird HAZID im Rahmen dieser Arbeit nicht weiter im Detail betrachtet.

Eines dieser Expertensysteme wurde von VENKATASUBRAMANIAN und VAIDHYANATHAN in „*A knowledge-based framework for automating HAZOP analysis*“ [139] erstmals vorgestellt. Das wissensbasierte System HAZOPExpert wurde auf Basis der Software „G2“ der Firma „gensym“ implementiert. HAZOPExpert sieht eine Aufteilung des Expertenwissens in Prozess spezifisches und allgemein gültiges Wissen vor. Das allgemein gültige Wissen wird in einer Datenbank hinterlegt und kann bei jeder neuen HAZOP wiederverwendet werden, wobei die Darstellung nach einem objektorientierten Ansatz erfolgt. Dadurch wird eine Erweiterung der Datenbank vereinfacht. Es werden HAZOP Modelle für verschiedene Prozesseinheiten entworfen, sowie Methoden zur Fehlererkennung, Auswirkungsanalyse und Fehlerfortpflanzung implementiert. Mit Hilfe des Prozess spezifischen Wissens wie konkreten Stoffeigenschaften und einem P&ID wird das allgemeine Wissen konkretisiert und spezifiziert und die Durchführung

einer HAZOP teilweise automatisiert. Insbesondere können Ursachen und Auswirkungen einer betrachteten Abweichung einer Prozessvariablen anlagenweit analysiert werden
Die Fehleranalyse in HAZOPExpert wurde durch den Einsatz von erweiterten SDGs verbessert [135], die Bewertung von Fehlerauswirkungen durch Wichtungsmethoden ergänzt [134], die Anwendbarkeit von kontinuierlichen Prozessen auf Batchprozesse erweitert [140] und die industrielle Nutzbarkeit des Systems anhand von Fallbeispielen verifiziert [139, 136, 140].

2.4 Nachtrag

Die Einordnung dieses Abschnitts in die Gesamtarbeit steht noch nicht fest. Verweis auf die zwei Arbeiten von Fleischer-Trebes, es gibt quasi keine Arbeiten zu dem Thema, Darum ist meine Arbeit wichtig. Verweis auf andere Varianten der Fehleruntersuchung noch bringen. Dazu gehören Fehlerbaumanalyse (Fault Tree Analysis, FTA), Fehlermöglichkeits- und -einflussanalyse (Failure Mode and Effects Analysis, FMEA), LOPA und weitere.

Im Rahmen modularer Konzepte wird teilweise davon ausgegangen, dass Module funktional eigensicher sind und das durch modulinterne Maßnahmen eine Fehlerfortpflanzung verhindert wird. [130, S. 4] Ob dieser Zustand erfolgreich erreicht wurde, kann aber erst geprüft werden, wenn sämtliche Stoff- und Prozessdaten bekannt sind und die Gesamtanlage geplant ist. Daher kann erst nach dem Detailengineering eine Sicherheitsuntersuchung der Gesamtanlage durchgeführt werden. Im Rahmen dieser ist der Nachweis zu erbringen, dass die Module eigensicher sind. Ist dies nicht der Fall, so sind geeignete Sicherheitsmaßnahmen zu entwickeln, um einen sicheren Betrieb zu gewährleisten.

Fehlerursachenermittlung 3

Definitionen: DIN EN 61511-1: Risiko(risk), Schaden(harm), Gefährdung(hazard), Störung, fault, basic event(s)/root cause(s)/malfunction/failure, sicherheit(safety), DIN EN 61511

In Verfahrenstechnischen Anlagen kommt es immer wieder zu Abweichungen des Prozesses vom Sollzustand. Es ist Aufgabe der Anlagenfahrer auf diese Abweichungen geeignet zu reagieren, um den Prozess wieder in den sicheren Sollzustand zu überführen. Diesen Vorgang können Menschen nicht allein bewältigen, da sie in Folge des Umfangs moderner Anlagen nicht mehr in der Lage sind, den kompletten Zustand einer Anlage zu erfassen. Zu dem enormen Umfang an Prozessvariablen kommt erschwerend hinzu, dass Abweichungen in Folge von Sensorfehlern und Messungenauigkeiten teilweise erst spät erkannt werden. Dies erschwert das rechtzeitige Initiieren notwendiger Prozesskorrekturen. Durch verspätetes ergreifen notwendiger Maßnahmen kommt es immer wieder zu Störungen und kleinen Unfällen. Der dadurch entstehende Schaden beträgt jährlich mehrere Milliarden Euro. Es wurden umfangreiche Forschungen durchgeführt, um zu ermitteln wie Abweichungen frühzeitig erkannt und zugrunde liegende Ursachen identifiziert werden können. Dieses Vorgehen nennt man Fehlererkennung und Fehlerisolation (fault detection and isolation, FDI). Zur Ermittlung der Ursachen einer Prozessabweichung werden erfolgreich Methoden der Fehlerfortpflanzung (engl. fault propagation methods) eingesetzt. [141, S. 2]
Eine kompakte Einführung in die FDI findet sich im Abschnitt „Fault Detection and Diagnosis“ des Buches „*Encyclopedia of Systems and Control*“ [4, S. 417 ff.].

Die Fortpflanzung von Störungen beim Betrieb chemischer Anlagen ist ein intensiv erforschtes Problem. Von Interesse sind Abweichungen der Prozessvariablen von einem definierten Sollwert und Abweichungen des Betriebszustandes von Geräten, Instrumenten und Gewerken vom Optimalzustand und daraus resultierende Auswirkungen auf den Prozess.

Die Abweichung einer Prozessvariable vom Sollwert kann vielfältige, verkettete Ursachen haben. Am Beispiel einer stark exothermen Reaktion zweier flüssiger Stoffe A und B soll dies verdeutlicht werden. Die Reaktion sei dabei noch in der Erprobungsphase, weswegen keine Erfahrungswerte in der gegebenen Anlage bestehen.
Ein Reaktionsbehälter mit Rührer habe zwei über Pumpen gesteuerte Zuflüsse. Um die gewünschte Reaktion zu starten, wird der Stoff A eindosiert. Durch langsame Zugabe von Stoff B soll unter Vermischung der Reaktanten die Reaktion gestartet werden. Sei nun der Rührer durch Alterung deutlich langsamer als im optimalen Zustand und außerdem der im Reaktor befindliche Temperatursensor defekt. Trotz Zugabe von Stoff B und Einschalten des Rührers findet die Reaktion dann nicht zu dem erwarteten Zeitpunkt statt, da keine ausreichende Vermischung der Stoffe A und B zustande kommt. Eine Ursachenanalyse ist in Folge fehlender Erfahrungswerte sehr kompliziert. Ein mögliches Vorgehen besteht in der vermehrten Zugabe von Stoff B in der Annahme so die Reaktion starten zu können. Durch die vermehrte Zugabe und das langsame Vermischen der Reaktanten beginnt die Reaktion. Dies wird durch den defekten Temperatursensor jedoch nicht bemerkt. Der Stoff B wird daher weiter zudosiert. Die stark exotherme Reaktion geht in Folge dessen durch. Dies wird jedoch erst durch einen Druckanstieg im Behälter erkannt, welcher durch Verdampfen der Reaktanten zustande kommt. Aus Sicht der Anlagenfahrer hat die Reaktion jedoch noch immer nicht begonnen, da die Temperatur im Reaktor nicht gestiegen ist. Der Druckanstieg könnte also einem fehlerhaften Drucksensor oder einer nicht erkannten Reaktion geschuldet sein. Die Ursachenanalyse für den erhöhten Druck ist zu diesem Zeitpunkt in Folge einer möglichen Verkettung von Fehlfunktionen sehr kompliziert. Eine durchgehende Reaktion ist hochgradig gefährlich. Wird die Gefahr nicht unmittelbar erkannt, so kann dies verheerende Folgen für die Anlage, die Betreiber und die Umwelt haben.

Das Auffinden möglicher Ursachen eines vorliegenden Fehlers ist eine Aufgabe, welche mit Hilfe der Analyse von Fehlerfortpflanzungen gelöst werden soll. Weitere Aufgaben sind die Bewertung und Auslegung von Systemen, welche das Betriebsrisiko einer Anlage auf ein gewünschtes Level bringen sollen. Die Planung optimaler Wartungsintervalle ist eine Aufgabe, welche direkt auf deren Ergebnissen aufbauen kann.

Im Rahmen einer Fehlerfortpflanzungsanalyse wird je nach Verfahren der Einfluss von Prozessgrößen, die räumliche Positionierung von Anlagenteilen, die Alterung von Anlagenkomponenten oder eine Kombination dieser Faktoren betrachtet. Je nach Art der verwendeten Informationen unterscheidet man in

- modellbasierte qualitative Verfahren,
- modellbasierte quantitative Verfahren und
- auf historischen Messdaten basierende Verfahren.

Die modellbasierten Verfahren sind solche, welche Wissen über die Struktur und Funktion einer Anlage auswerten. Zur Durchführung eines solchen Verfahrens werden meist Experten eingesetzt. Die datenbasierten Verfahren analysieren hingegen Messwerte, welche durch den Betrieb der Anlage oder Simulation der Anlage verfügbar werden. Die Auswertung findet dann beispielsweise mit Hilfe statistischer Methoden oder Verfahren zur Mustererkennung statt.
In der dreiteiligen Veröffentlichung von VENKATASUBRAMANIAN u. a. ([141, 138, 142]) wird eine umfassende Einordnung der bis zum Jahr 2002 veröffentlichen Methoden zur Analyse von Fehlerfortpflanzungen in diese drei Kategorien und eine Bewertung der Eignung der Methoden vorgenommen. Für zahlreiche Anwendungsfälle erörtern die Autoren geeignete Methoden, wodurch sie Nicht–Experten der Fehlerfortpflanzungsanalyse ein Hilfsmittel zur Evaluierung der Anwendbarkeit bestimmter Methoden für weitere Fälle bieten. Diese Veröffentlichung ist daher bei der Suche nach einer anwendbaren Methode zur Fehlerfortpflanzungsanalyse ein besonders zweckmäßiger Startpunkt. Es gibt neben den Arbeiten von VENKATASUBRAMANIAN u. a. weitere Literaturanalysen, diese haben aber einen geringeren Umfang und konzentrieren sich zumeist auf eine der drei genannten Kategorien. Eine hervorzuhebende Ausnahme bildet die zweiteilige Arbeit von GAO, CECATI und DING, in welcher ein umfangreicher, aktueller Literaturüberblick zum Thema FDI präsentiert wird [49, 50].
In den folgenden Abschnitten 3.3, 3.1 und 3.2 werden die einzelnen Kategorien detailliert betrachtet, weiter untergliedert und anhand von Beispielmethoden wird die Einsetzbarkeit einiger Methoden für modulare Anlagen bewertet.

Als Alternative zu den drei Kategorien nach VENKATASUBRAMANIAN u. a.[141] ist eine Einteilung in off-line und on-line Verfahren möglich [67]. Ersteres sind Verfahren, die losgelöst vom Betrieb einer Anlage durchgeführt werden. Ein

solches Verfahren kann beispielsweise vor der Erstinbetriebnahme auf Basis von Expertenwissen durchgeführt werden. Dann ist ein solches Verfahren gleichzeitig ein modellbasiertes Verfahren. Off-line Verfahren können aber auch datenbasierte Verfahren sein. Dies ist dann der Fall, wenn Messwerte durch zeitintensive Rechenoperationen ausgewertet werden. Ist dies nicht mehr in Echtzeit möglich, so kann nur eine off-line Analyse durchgeführt werden.
Ist ein Verfahren in Echtzeit berechenbar und basiert es auf aktuellen Messdaten einer Anlage, so wird es als on-line Verfahren kategorisiert. Ein solches Verfahren ist zwangsläufig frühestens nach der Erstinbetriebnahme einer Anlage durchführbar.

Eine klare Abgrenzung der Einteilung in off-line und on-line Verfahren beziehungsweise in modell- und datenbasierte Verfahren ist offensichtlich kompliziert. Im Rahmen dieser Arbeit liegt der Fokus auf den notwendigen Daten, welche zur Durchführung eines Verfahrens zur Analyse von Fehlerfortpflanzungen notwendig sind. Die Einteilung, ob es sich um on-line oder off-line Verfahren handelt, ist hingegen nebensächlich. Daher wird im Folgenden nur noch in modellbasierte qualitative, modellbasierte quantitative, auf historischen Messdaten basierende und Hybride dieser Verfahren unterschieden.

3.1 Modellbasierte Quantitative Fehlerfortpflanzungsmethoden

Als modellbasierte quantitative Verfahren zur FDI werden im Rahmen dieser Arbeit Verfahren bezeichnet, welche auf Basis von „analytischer Redundanz“ Residuen generieren, die wiederum zur Fehleridentifikation und Isolation genutzt werden. Die Ausführungen im Abschnitt 3.1 basieren in weiten Teilen auf der Arbeit von VENKATASUBRAMANIAN u. a. [141].

Verfahren dieser Art bestehen aus zwei grundlegenden Schritten. Im ersten Schritt werden mit Hilfe eines analytischen Prozessmodells und gemessenen Größen durch Einsatz mathematischer Verfahren Residuen generiert. Diese werden im zweiten Schritt analysiert, um das Vorliegen eines Fehlers zu erkennen und diesen eindeutig zu identifizieren.

Ein analytisches Prozessmodell kann entweder durch einen Satz an Gleichungen

oder in Form einer Black Box beschrieben werden. Analysiert man die physikalischen und chemischen Gesetze welchen ein Prozess unterliegt, so kann man Massen-, Energie-, Impuls- und Reaktionsbilanzen formulieren. Diese lassen sich allgemein als Differential–algebraische Gleichungen (Differential Algebraic Equations) (DAEs) darstellen. Betrachtet man hingegen Messwerte der Ein- und Ausgangsgrößen eines Prozesses, so kann man beispielsweise durch den Einsatz stochastischer Methoden ein Ein-Ausgangsmodell für den Prozess erstellen. Diese Art der Modellbildung bezeichnet man als „Systemidentifikation". Zahlreiche Veröffentlichungen der Regelungstechnik behandeln dieses Thema. UNBEHAUEN bietet in „*Regelungstechnik III: Identifikation, Adaption, Optimierung*" [129] einen Einstieg in die Systemidentifikation. Fortgeschrittene Verfahren zur Identifikation nicht–linearer Systeme werden beispielsweise von SCHRÖDER in „*Intelligente Verfahren: Identifikation und Regelung nichtlinearer Systeme*" [121] vorgestellt.
Physikalische Modelle zeichnen sich durch die Interpretierbarkeit der Prozessvariablen und eine genau abschätzbare Güte aus, haben aber einen hohen Entwurfs– und Berechnungsaufwand zur Folge.
Es existieren zahlreiche computergestützte Hilfsmittel, welche die Entwicklung eines Black Box Modells unterstützen und damit stark beschleunigen. Ein Beispiel dafür ist die „System Identification Toolbox™" der Firma „Mathworks". Black Box Modelle sind daher weniger aufwendig in der Formulierung und der Berechnung als die analytische Beschreibung eines Prozesses. Die Erstellung eines solchen Modells benötigt aber Messdaten, welche alle möglichen Betriebsbedingungen abdecken. Nur so kann ein genaues Modell erstellt werden. Die Erzeugung dieser Daten ist besonders an den Auslegungsgrenzen einer Anlage und für transiente Bedingungen kompliziert und kostspielig eventuell sogar überhaupt nicht möglich.
Ein analytisches Modell lässt sich prinzipiell durch

$$y(t) = f(u(t), w(t), x(t), \theta(t)) \tag{3.1}$$

formulieren, wobei die Systemausgangsgrößen $y(t)$ in Abhängigkeit von den Systemeingangsgrößen $u(t)$, den auf das System wirkenden Störungen $w(t)$, den Zustandsvariablen des Systems $x(t)$ und den Prozessparameter $\theta(t)$ berechnet werden.

Ein vorhandener Prozessfehler wirkt sich bei einer Systembeschreibung nach

Gleichung (3.1) direkt auf die Zustandsvariablen und beziehungsweise oder auf die Prozessparameter aus. Diese können aber häufig nicht direkt gemessen werden. Die Systemein- und Systemausgangsgrößen können hingegen in der Regel entweder durch Sensoren direkt erfasst oder mit Hilfe mathematischer Modelle beobachtet werden. Die Zustandsvariablen und Prozessparameter können daher mit Hilfe geeigneter mathematischer Methoden aus Messwerten von $u(t)$ und $y(t)$ geschätzt werden. Typische Methoden der Zustands- beziehungsweise Parameterschätzung sind die Methode der kleinsten Fehlerquadrate (Least Squares Method, LQM), die Verwendung von Kalman Filtern, die Formulierung von geeigneten Beobachterstrukturen oder der Einsatz von Paritätsgleichungen.

Die zur Berechnung der Residuen notwendigen Redundanzbeziehungen basieren auf Ein- und Ausgangsgrößen, welche voneinander nicht unabhängig sind. Die Abhängigkeiten können durch zusätzliche Hardware oder analytische Beziehungen erzeugt werden. Lässt sich die Redundanz als Gleichung formulieren und werden die Redundanzbeziehungen mit den Modellgleichungen zu einem Gleichungssystem kombiniert, so ist dieses Gleichungssystem überbestimmt. Der entstehende Freiheitsgrad der Lösung wird zur Entwicklung der Residuen genutzt.
Redundanz durch Hardware entsteht beispielsweise durch mehrere Sensoren, welche die gleiche Größe erfassen. Bei sicherheitstechnisch besonders anspruchsvollen Anwendungen wie der Luft- und Raumfahrt ist dieses Vorgehen trotz der damit verbunden gesteigerten Kosten und dem erhöhten Raumbedarf üblich. Analytische Redundanz wird erreicht, wenn sich bestimmte Sensorwerte algebraisch aus anderen Sensorwerten berechnen lassen, oder wenn es einen zeitlichen Zusammenhang zwischen der Änderung von Messwerten gibt, welcher sich analytisch beschreiben lässt. Ein Beispiel für eine solche Größe ist der Füllstand in einem Tank. Werden der Zufluss und der Abfluss durch Sensoren erfasst, so kann der Füllstand direkt berechnet werden. Wird trotzdem ein Füllstandssensor verbaut, so führt dies zu nutzbarer Redundanz, da die zeitlichen Änderungen der drei Messwerte zueinander verträglich sein müssen. Ist dies nicht der Fall, so kann auf einen Sensordefekt, ein Leck oder auf einen anderen Fehler geschlossen werden.

Die auf Basis der analytischen Redundanzen ermittelten Residuen sollen zur Fehlerdiagnose eingesetzt werden können. Es ist daher zweckmäßig, wenn die Residuen bei Vorliegen einer Abweichung vom Sollverhalten des Prozesses si-

gnifikante Werte annehmen. Liegt keine Störung vor, so sollten die Residuen Werte nahe Null annehmen. Weiterhin ist es günstig, wenn die Residuen robust gegen zufällige Fehler wie Sensorrauschen und systematische Fehler wie Modellungenauigkeiten sind.

Als ersten Verfahrenstyp zur Residuenberechnung stellen VENKATASUBRAMANIAN u. a. die Diagnose mit Beobachtern[1] vor ([141, S. 11 ff.]). Methoden dieser Art entwickeln eine bestimmte Menge an Beobachtern, welche Residuen generieren. Jeder dieser Beobachter wird so definiert, dass er bezüglich einer definierten Menge an Fehlern sensitiv und bezüglich den restlichen Fehlern und unbekannten Größen unempfindlich ist. Die Menge der Beobachter ist derart zu strukturieren, dass jeder Fehler ein eindeutiges Muster an Residuen zur Folge hat. Wird dies erreicht, so kann das Vorliegen eines Fehlers durch stark von null abweichende Werte der Residuen erkannt und mit Hilfe der bekannten Residuenmuster identifiziert werden. Eine wichtige Besonderheit dieses Verfahren ist es, dass die Schätzung der Zustandsvariablen $x(t)$ nicht notwendig ist, statt dessen muss nur der Systemausgang durch Messung oder Schätzung ermittelt werden.

Die Formulierung von Paritätsgleichungen ist ein alternatives Vorgehen zur Generierung von Residuen (vgl. [141, S. 13 f.]). Bei diesem Vorgehen werden die Modellgleichungen geeignet umgestellt, sodass Residuenvektoren entstehen, die orthogonal zueinander sind. Die Residuenvektoren sind dann linear unabhängig und das Auftreten jedes betrachteten Fehlers wird durch genau einen Residuenvektor beschrieben. Voraussetzung zur Einsetzbarkeit dieser Methode ist, dass die Anzahl der Ausgangsgrößen größer als die der Zustandsgrößen ist. Dieser Zusammenhang wird in Definition 1 verdeutlicht.

Definition 1 (Systemredundanz)**.** *Sei ein System nach Gleichung (3.1) beschrieben und gelten die Eigenschaften*

$$\dim(y(t)) = n, \qquad \dim(x(t)) = m, \qquad n > m, \tag{3.2}$$

dann ist das System redundant mit dem Freiheitsgrad

$$f = n - m, \tag{3.3}$$

da das System mehr erfassbare Ausgangsgrößen als Zustände umfasst.

1 im englischen spricht man von „diagnostic observer“ oder „unknown input observer“ (UIO)

Mit Hilfe des Freiheitsgrades f kann dann eine Projektionsmatrix $\boldsymbol{V}$ derart entworfen werden, dass für Abweichungen von jedem redundant vorhandenen Ausgangswert ein Vektor berechenbar ist, der zu den anderen Vektoren dieser Art orthogonal ist.
Paritätsgleichungen und die Verwendung von Beobachtern zur Residuenerzeugung ähneln sich sehr stark. Beide Verfahren sind ohne eine Schätzung von $x\,(t)$ anwendbar. Man kann sogar zeigen, dass beide Verfahren unter Verwendung der gleichen Designziele zu äquivalenten Residuen für ein fehlerbehaftetes System führen. Die Methoden der Auswertung von Residuen zur Diagnose von Fehlern sind für diese beiden Verfahren ebenfalls gleich. Üblich ist die Definition von Schwellwerten für die Residuen, bei deren Überschreiten ein Fehler als vorliegend erkannt wird.

Es gibt weitere Methoden, welche Residuen auf Basis quantitativer Modelle berechnen um so Fehler zu diagnostizieren und zu isolieren. Dazu zählen Methoden, welche die Zustandsvariablen oder Prozessparameter schätzen, um auf Basis derer Residuen zu generieren. Dies sind beispielsweise Kalman Filter und LQM (vgl. [141, S. 14 f.]). Außerdem gibt es fortgeschrittene Methoden zur Residuenberechnung wie der Entwurf von gerichteten oder strukturierten Residuen[2] (vgl. [141, S. 15 f.]).

3.1.1 Bewertung modellbasierter quantitativer Methoden der FDI für modulare Anlagen

Modellbasierte quantitative Methoden bieten den großen Vorteil, dass der Anwender bei der Wahl eines Verfahrens zur Residuengenerierung viele Freiheiten hat. Auch die Verfahren selbst bieten Möglichkeiten, um sie hinsichtlich der Erkennung bestimmter Fehler gezielt zu entwerfen. Werden entkoppelte Beobachterstrukturen geeignet entworfen, so kann jeder betrachte Fehler durch einen gesonderten Beobachter gezielt diagnostiziert werden. Dem gegenüber steht der große Nachteil der Notwendigkeit von möglichst genauen Prozessmodellen. Der Entwurf dieser Modelle ist aufwendig und häufig mit Ungenauigkeiten verbunden. Dies gilt für analytische Modelle und Black Box Modelle gleichermaßen. Weiterhin sind Analysemethoden, welche auf quantitativen Modellen basieren, in

2 engl. directional residuals and structured residuals

aller Regel auf die Erkennung von Fehlern, welche additiv auftreten, beschränkt. Die Erkennung von multiplikativ auftretenden Fehlern wie einem Drift von Prozessparametern ist nur in Sonderfällen möglich. Darüber hinaus müssen die Residuen zur Erkennung von Fehlern vorab definiert werden. Das Auftreten von vorab unbekannten Fehlern ist dadurch nur stark eingeschränkt möglich. Auch die Ursachenanalyse ist zumeist nicht möglich – nur das Vorliegen eines Fehlers wird diagnostiziert und der konkrete Fehler ermittelt. [141, S. 17 f.]

In Hinblick auf modular konstruierte Anlagen lässt sich feststellen, dass Methoden dieser Kategorie nicht geeignet sind, um die zur Genehmigung einer aus Modulen bestehenden Anlage notwendige Sicherheitsuntersuchung zu beschleunigen oder anderweitig zu vereinfachen.
Für die Analyse eines einzelnen Moduls könnten jedoch solche Verfahren zum Einsatz kommen. Module sollen entsprechend ihrer Definition einzeln komplett testbar sein. Daher ist die Erstellung von Ein-/Ausgangsdaten und darauf aufbauend die Entwicklung eines Black Box Modells prinzipiell möglich. Die Erstellung eines analytischen Modells durch den Modullieferanten ist ebenfalls möglich und sollte ohnehin ein Ziel dessen sein, denn auf Basis eines analytischen Modells können die im Abschnitt 2.1 geforderten Simulationsmodelle geeignet entworfen werden. Die notwendige Grundlage für modellbasierte quantitative Verfahren wäre damit zumindest auf Modulebene gegeben, jedoch verbleiben zwei bedeutende Probleme:

- der aufwendige Entwurf eines analytischen Modells der Gesamtanlage ist notwendig und
- nicht erkannte Fehler können nicht verlässlich identifiziert werden.

Zum einen ist zu erwarten, dass die Modelle der einzelnen Module noch keine ausreichenden Informationen über die möglichen Wechselwirkungen, welche im Rahmen der Gesamtanlage auftreten können, enthalten. Ein Modell der Gesamtanlage müsste daher vor dem Einsatz von Verfahren der betrachteten Kategorie noch erstellt werden. Dies wäre nur durch analytische Ansätze möglich. Die zur Generierung von Black Box Modellen notwendigen Ein-/Ausgangsdaten müssten von der Gesamtanlage stammen, diese ist zum Zeitpunkt der durchzuführenden Sicherheitsbetrachtung aber noch gar nicht betriebsfähig. Die Durchführung praktischer Tests und die Erstellung von Messdaten ist daher keine zur Verfügung

stehende Option und die Erstellung von Black Box Modellen nicht möglich. Die Erstellung von analytischen Modellen ist mit den bereits genannten Problemen des hohen Aufwands und der entstehenden Ungenauigkeiten verbunden. Die notwendige Entwicklungsleistung eines analytischen Modells reduziert damit mögliche Zeiteinsparungen bei der Sicherheitsbetrachtung maßgeblich.
Zum anderen werden vorab unbekannte Fehler durch modellbasierte quantitative Verfahren nicht verlässlich identifiziert. Das Auffinden von bisher nicht betrachteten Fehlern wird also bereits auf der Betrachtungsebene einzelner Module durch Methoden dieser Kategorie nicht ermöglicht. Durch das Verbinden von Modulen zu einer Gesamtanlage ist mit neuen Fehlerquellen und für die Anlage spezifischen möglichen Auswirkungen zu rechnen. Die Erkennung dieser neuen Fehler ist nicht möglich. Die durch Kopplung der Module potentiellen neuen Fehler sind aber genau die Fehler, welche durch die Sicherheitsuntersuchung der Gesamtanlage aufgedeckt werden müssen. Eine Vereinfachung dieser Aufgabe durch die Verwendung von modellbasierten quantitativen Verfahren zur Fehlerdiagnose ist damit nicht zu erwarten.

Im Rahmen der vorliegenden Arbeit soll davon ausgegangen werden, dass die vorhandene Datenbasis aus für die einzelnen Module durchgeführten HAZOPs, Beschreibungen der Module und einer Beschreibung der Gesamtanlage besteht. Auf dieser Basis lässt sich nicht ohne großen Aufwand ein analytisches Modell der Gesamtanlage formulieren. Selbst wenn quantitative modellbasierte Verfahren der FDI potentielle Einsparungen bei der Sicherheitsbetrachtung der Gesamtanlage bieten würden, was wie dargelegt wird, nicht der Fall ist, so wäre die notwendige Datenbasis in keiner weise vorhanden. Im Rahmen dieser Arbeit ergibt sich daher zwangsläufig, dass der Einsatz von modellbasierten quantitativen Verfahren nicht geeignet ist, um die Fehlerfortpflanzung innerhalb einer aus Modulen bestehenden Anlage zu untersuchen.

3.2 Modellbasierte Qualitative Fehlerfortpflanzungsmethoden

Modellbasierte qualitative Verfahren unterscheiden sich von den modellbasierten quantitativen dadurch, wie das vorab vorhandene Wissen über den betrachteten Prozess formuliert wird. Im Fall der quantitativen Verfahren dienen dazu mathematische Gleichungen, bei den qualitativen Methoden werden die bekannten Beziehungen zwischen Prozessvariablen als relative Aussagen formuliert. Diese relativen Aussagen beschreiben zumeist eine Abhängigkeit der Wertentwicklung von Prozessvariablen zueinander. Ein solche Beziehung besteht beispielsweise zwischen dem Druck und der Temperatur in einem geschlossenen Behälter. Als qualitative Aussage kann formuliert werden, dass ein Ansteigen der Temperatur einen Druckanstieg zur Folge hat. Die Aussage lässt jedoch keinen Schluss über das Ausmaß der Änderung zu und wird daher als qualitativ bezeichnet.
Aufbauend auf qualitativen Aussagen kann ein System entworfen werden, welches zur FDI genutzt werden kann.
Die Formulierung eines qualitativen Modells wird vorwiegend durch Experten vorgenommen. Soll eine Methode zur FDI auf Basis eines qualitativen Modells angewandt werden, so ist eine Untersuchung des Modellverhaltens im Sollzustand und im fehlerbehafteten Zustand notwendig. Die Beschreibung des Sollzustandes wird im Rahmen der Prozessentwicklung durchgeführt. Eine geeignete qualitative Beschreibung des Prozesses bei Vorliegen von Fehlern wird in Folge der im Abschnitt 2.3 beschriebenen HAZOP erlangt. Es sind aber auch andere Methoden zur qualitativen Beschreibung von Fehlzuständen möglich. Verweis auf Abschnitt, in welchem andere Methoden genannt werden.

Zur Darstellung einer qualitativen Systembeschreibung gibt es mehrere Möglichkeiten. Ein umfassend untersuchter Ansatz in die Verwendung von wissensbasierten Expertensystemen [3]. Ein solches System definiert in einer für einen PC analysierbaren Weise eine vorgegebene Menge von Aussagen, welche das Systemverhalten beschreiben. Dies geschieht zumeist durch den Einsatz von verschachtelten wenn–dann–sonst Formulierungen. Das Expertensystem kann auf Basis von vorgegebenen Zuständen die Gültigkeit der zuvor definierten Aussagen prüfen und dadurch Schlussfolgerungen ziehen. Als vorgegebener Zustand

3 engl. knowledge-based expert systems

kann beispielsweise die Abweichung einer Prozessvariable vom Sollverhalten definiert werden, deren Auswirkung zu untersuchen ist. Das Expertensystem imitiert auf Basis der wenn–dann–sonst Zusammenhänge die Gedankengänge eines Menschen und ermittelt die möglichen Auswirkungen. Ein großer Vorteil des Expertensystems ist es, dass keine zuvor definierten Auswirkungen übersehen werden können. Jedoch ist das Expertensystem stets auf die zuvor definierten Systemeigenschaften beschränkt und kann keine komplett neuen Erkenntnisse entwickeln.

Das Ziehen von Schlussfolgerungen basiert in aller Regel auf der Auswertung von vorhandenem Wissen. Dieses Vorgehen geschieht unter der Anwendung von „Inferenzmechanismen“ . Diese schließen das Prüfen von bekannten Aussagen auf Erfülltheit durch Analyse eines aktuellen Zustands ebenso wie das Herleiten von neuen Aussagen (Konklusionen) auf Basis von bekannten, wahren Aussagen (Prämissen) ein. Man unterscheidet dabei die drei Inferenzmechanismen

1. deduktives Schließen,
2. abduktives Schließen und
3. induktives Schließen .

Als deduktives Schließen bezeichnet man die Formulierung einer logischen Konsequenz, welche auf Basis von mehreren festgelegten Prämissen formuliert wird. Dabei findet zumeist eine Ableitung vom Allgemeinen auf einen Einzelfall statt. Als Beispiel dienen die Prämissen ein Zufluss erhöht das Volumen im Lagertank und Flüssigkeit A strömt in den Lagertank. Als Konklusion erhält man die Aussage, dass die Flüssigkeit A das Tankvolumen erhöht.
Beim abduktiven Schließen folgert man aus einer Prämisse und einem beobachteten Resultat die Gültigkeit einer Voraussetzung. Eine Abduktion liefert bei Betrachtung gewisser Effekte eine plausible Ursache für deren Eintreten, die durchgeführte Schlussfolgerung muss jedoch nicht notwendigerweise korrekt sein. Trotzdem ist dieses Vorgehen bei der Suche nach möglichen Erklärungen für einen beobachteten Effekt sehr hilfreich. Der Zusammenhang „das Öffnen des Abflussventils senkt das Tankvolumen“ in Verbindung mit der Beobachtung, dass das Tankvolumen sinkt, lässt den abduktiven Schluss zu, dass das Abflussventil geöffnet ist. Eine alternative Begründung ist aber auch, dass der Tank ein Leck aufweist. Die abduktive Schlussfolgerung ist demnach zwingend auf Gültigkeit

zu prüfen.
Die Induktion ist in ihrem Vorgehen in etwa das Gegenteil der Deduktion. Im Rahmen induktiver Schlussfolgerungen wird aus mehreren Beobachtungen eine allgemeine Regel abstrahiert. Deren Gültigkeit ist aber nicht zwangsläufig gegeben. Werden in einem Reaktor zwei Stoffe mit hoher Temperatur zugeführt und zu einer endothermen Reaktion gebracht so könnte man schließen, dass das Zusammenführen von zwei Reaktanten prinzipiell ein Absinken der Temperatur zur Folge hat. Diese Aussage ist für exotherm reagierende Stoffe aber offensichtlich falsch und mit einem hohem Risiko verbunden.
Im Gegensatz zu Induktion und Abduktion ist die Deduktion wahrheitserhaltend und daher die zu bevorzugende Inferenzmethode. Ist Deduktion jedoch nicht möglich oder zu aufwendig, so ist der Einsatz von Induktion oder Abduktion aber möglich, um neue Aussagen zum Systemverhalten zu generieren. (vgl. [36, S. 28 ff.])

Um die Durchführung einer HAZOP zumindest teilweise zu automatisieren wurden zahlreiche Expertensysteme entwickelt.

3.3 auf historischen Messdaten basierende Fehlerfortpflanzungsmethoden

Diese Verfahren beruhen auf der Verwendung von historischen Messdaten konkreter Anlagen. Je nach Verfahren werden Messdaten zum Normalbetrieb oder beziehungsweise und Daten zum Störbetrieb benötigt. Manche Methoden benötigen weiterhin ein P&ID. Ziel der Verfahren ist es zum einen Störungen der Anlage frühzeitig zu erkennen und zum anderen deren Ursache oder Ursachen zu ermitteln. Dazu werden Ursache–Effekt Beziehungen zwischen untersuchten Parametern ermittelt.

Die Auswertung historischer Messdaten basiert zumeist auf statistischen Methoden. Die kausalen Zusammenhänge, welche mit Hilfe dieser Methoden ermittelt werden sollen, können dann geeignet als Graphen dargestellt werden. Wie man aus statistischen Größen kausale Zusammenhänge ermitteln kann wird in den frühen Werken HOLLAND [62] und PEARL [110] aufgezeigt. Ein umfassendes Lehrbuch zu dieser Thematik wurde von PEARL veröffentlicht, welches

mittlerweile in der zweiten Auflage verfügbar ist [111].

Datenbasierte Methoden sind hervorragend für die Erstellung von quantitativen Modellen geeignet. Eine Erstellung von qualitativen Modellen ist ebenfalls möglich. Beispiele

Nennung von Verfahren [158], [127]

3.4 Vorstellung ausgewählter Algorithmen

3.5 Bewertung der Verwendbarkeit für modulare Anlagen

Wichtige Gesichtspunkte:

- Welche Daten sind notwendig
- Automatisierbarkeit der Berechnung
- Dokumentationsfähigkeit der Ergebnisse
- Sind die Ergebnisse für eine HAZOP nutzbar

Literatursichtung 4

4.1 Sicherheit

[116] Erklärungen zu **quantitativen** Risikoanalysen anhand zweier Beispiele.

Alles nur zitiert!

Im internationalen Anlagenbau wird in zunehmendem Maße die Durchführung einer quantitativen Risikoanalyse gefordert. Die Methodik kann nicht nur zum Nachweis der Einhaltung übergeordneter Akzeptanzkriterien dienen, sondern auch als eine qualifizierte Entscheidungsgrundlage z. B. zu Sicherheitsabständen und -barrieren verwendet werden. Dies kann von nicht probabilistischen quantitativen Verfahren (z. B. HAZOP)) nicht geleistet werden. Durch die Identifizierung der Hauptrisikoquellen in der Anlage ermöglicht eine quantitative Risikoanalyse (QRA) zudem die Ableitung von Risikominderungsmaßnahmen, deren Wirksamkeit sich mit Hilfe von Sensitivitätsberechnungen analysieren und bewerten lässt. Quantitative Sicherheitsanalyse

[75] Noch lesen!

[15] Probleme bei der Anwendung von LOPA (Layer of Protection Analysis) (vereinfachte quantitative Sicherheitsbetrachtung ausgewählter Probleme, wenn eine HAZOP o. ä zur Identifikation risikoreicher Szenarien bereits durchgeführt wurde)
Ein erstes Zusammenhängendes Buch zur Anwendung von LOPA ist 2001 erschienen. Die Methode hat vielerlei Anwendung in der Industrie gefunden, wurde

jedoch häufig auch zweckentfremdet. Die gemachten Erfahrungen und Probleme wurden gesammelt und 2010 eine neue Richtlinie Richtlinie zur Anwendung der Methode veröffentlicht (zum Zeitpunkt dieses Papers stand dieses 2. Buch noch aus). **Absicht von LOPA:** Risikobewertung eines bekannten Szenarios mit Hilfe unabhängiger Schutzschichten (independent Protection Layers IPL), welche durch strenge Regeln definiert werden, und Auslösungsereignissen (initiating events IEs). Durch korrekte Anwendung der Methode ist eine vereinfache Risikobewertung eines Ursache-Wirkung Paares (=Szenario) möglich. Das Auffinden von möglicher Störungen ist nicht Teil der Methode, nur die Bewertung von bekannten Szenarien! Die Methode eignet sich besser als eine FMEA für komplexe Probleme, ohne für simple Probleme viel zu aufwendig zu sein (wie es bei einer Fehlerbaumanalyse der Fall wäre). Der aktuelle Nutzen einer LOPA liegt in der Bewertung, ob eine SIF notwendig ist und ob sie die richtige Wahl zur Risikoreduktion darstellt (es existieren auch andere Methoden, welche diesen Zweck erfüllen). Wird eine SIF als Lösung gewählt, so kann LOPA das notwendige SIL liefern. **Vorteile LOPA**

- Konsistente Definition von Schutzschichten, was die Filterung der entscheidenden Schutzeinrichtungen vereinfacht und somit ein umfassendes Sicherheitsmanagement vereinfacht.
- Die Detailbetrachtung mit LOPA kann überflüssige Schutzeinrichtungen identifizieren
- Durch die anhand klarer Regeln definierten Schutzschichten kann ein gefordertes SIL besser auf Erfüllung überprüft werden, eine Übererfüllung durch zu viele SIS wird dadurch weniger wahrscheinlich
- LOPA braucht weniger Aufwand als eine QRA, wodurch insbesondere komplexe, schwerwiegende Risikoszenarien schneller quantifiziert werden können (Arbeitsaufwand von Stunden statt Tagen)
- Durch die konsistenten Bewertungsregeln für Risiken und das vereinfachende Vorgehen können durch verschiedene Expertengruppen gewonnene Analyseergebnisse komplexer Risikoszenarien besser verglichen werden
- LOPA ermöglicht das Festlegen eines geeigneten Vorgehens, wenn Schutzschichten z. B. wegen Wartung deaktiviert werden müssen.

Nachteile/Probleme LOPA

- Die Regeln der LOPA werden missachtet. Beispiele
  - Es wird nicht geprüft, dass Schutzschichten wirklich unabhängig von einander sind (Ein Anlagenfahrer darf beispielsweise nur in max. einer Schicht vorkommen!)
  - Die Werte von Ausfallraten und anderen statistischen Größen werden ungefiltert aus der Literatur übernommen und nicht das konkrete Umfeld angepasst (z. B. konkrete Betriebsbedingungen)
  - Die Sicherheitswerte (richtiger Begriff?) von Schutzschichten und IEs werden während dem Betrieb einer Anlage nicht aufrecht erhalten, da Wartungen und Tests nicht ausreichend (Umfang und Frequenz) geplant werden. Ursache ist fehlende Erfahrung und der Mangel eines standardisierten Vorgehens bei der Wartungs-/ Testplanung, um konkrete Zahlenwerte von IPLs zu erreichen und zu halten. Die Ergebnisse von Tests/Wartung werden nicht ausreichend dokumentiert, insbesondere wird bei nicht-erreichen und fast-nicht-erreichen geforderter IPLs nicht ausreichend weiterverfolgt, wie dies zustande kam. Solche Untersuchungen sind aber notwendig, um statistische Verfügbarkeit genauer mit Zahlenwerten belegen zu können.
  - Die durch IPLs verhinderten Auswirkungen werden zu ungenau spezifiziert. Dadurch kommt es zu Über- und Unterschätzen von Risiken. Die Erfahrung hat gezeigt, dass Risiken eher Überschätzt werden, wodurch unnötig viel Geld für Schutzmaßnahmen ausgegeben wird.
  - Überverwendung von LOPA. Angedacht ist die Methode für eine einzige Person im Anschluss an eine HAZOP für 1-5% der gefundenen Szenarien. Die Person sollte Teil des Risikobewertungsteams sein, oder mit diesem einfach kommunizieren können. LOPA wurde teilweise mit dem gesamten Analyseteam im Rahmen der Risikoanalyse gemacht. Dafür ist die Methode nicht ausgelegt. Der Brainstormingprozess des Teams wird durch das analytische Vorgehen einer LOPA gestört. Mögliche Risikoszenarien werden dadurch leicht übersehen. Qualitative und quantitative Betrachtungen sollten zeitlich getrennt ablaufen. Weiterhin ist die Bestimmung der Notwendigkeit und des Grades eines

SIL durch das Expertenteam zulässig für SIL-1 und SIL-2. Nur für Szenarien, welche für das Expertenteam zu komplex sind, sollte eine LOPA unter SIL-3 angewandt werden. LOPA wird aber teilweise prinzipiell zur Bestimmung der Notwendigkeit/ des Grades von SIL genutzt. Insbesondere die Entscheidung über die Notwendigkeit eines SIL sollte aber dem Expertenteam im Rahmen der HAZOP überlassen werden.

– Überverwendung von Software: LOPA soll ein Szenario im Detail erklären, eine IPL definieren/ das Szenario einer IPL zuordnen und die Aufrechterhaltung einer IPL belegen. Dies geschieht in Textform und Software kann daher die Arbeit nur geringfügig unterstützen.

Abschluss: LOPA ist ne dolle Sache zur quantitativen Betrachtung. Aktuelle Richtlinie: [23] fertig

[128] Supporting the selection of process and plant design options by Inherent Safety KPIs

[119] Reliability and safety analysis of the process plant

[82] Risk identification and assessment of modular construction utilizing fuzzy analytic hierarchy process (AHP) and simulation

[3] Literaturübersicht zum Thema „Fault Tree Analysis“ .
Fehlerbaumanalyse entstammt der Luftfahrtbranche und wurde zunächst auch zur Bewertung der Sicherheit von Atomkraftwerken verwendet. Durch die guten Erfahrungen in Bereich der Stromerzeugung ist dieser Ansatz auch in der chemischen Industrie sehr beliebt geworden. Es handelt sich um eine Top-Down Analyse, bei welcher die Ursachen für einen Fehler ermittelt werden. Insbesondere die Einwirkung von Geräteversagen, menschlichem Versagen und externen Einflüssen wird betrachtet. Ausgehend von einem unerwünschten Ereignis wie beispielsweise einem Unfall werden Ereignisse mit Hilfe logischer Gatter verknüpft, um die Ursache fr eben dieses Unfall zu ermitteln. Die Ursachen-Ereignisse werden dabei Stufenweise in Sublevel unterteilt und erhalten je nach Leveltiefe

eine andere Symbolik. Eine Fehlerbaumanalyse lässt sich in mehrere Schritte einteilen. Siehe dazu beispielsweise [2].

- Vorteile:
  - sehr effektiv bei der Risikobewertung von System moderater Größe
  - die möglichen Ursachen eines vom Nutzer vorgegebenen Ereignisses lassen sich detailliert ermitteln und darstellen
  - Eine Fehlerbaum kann mit Hilfe von Software erstellt und ausgewertet werden
  - sind empirische Daten vorhanden, so kann eine quantitative Aussage über die Eintrittswahrscheinlichkeit für ein Ereignis gemacht werden
- Nachteile:
  - Bei grßen Systemen ist die Herleitung des Fehlerbaumes sehr zeitaufwendig.
  - Vollständigkeit kann nicht garantiert werden
  - keine Beachtung von Teilausfällen möglich. Ein System ist entweder komplett funktionsfähig oder garnicht.
  - die konkrete Struktur einer Fehlerbaumes hängt vom Entwickler und dessen Erfahrung/ Vorlieben ab. Das Untersuchungsergebnis eines Systems ist also nicht generisch.
  - Die Eintrittwahrscheinlichkeit eines Ereignisses einer höheren Ebene ist nur möglich, wenn die Eintrittswahrscheinlichkeiten aller Elemente der Subebene verfügbar sind, welche einen Pfad zum Ereignis bilden. Diese Unterwahrscheinlichkeiten sind oft nicht konkret bekannt. Dies ist das mit Abstand größte Problem dieser Methode.

Die Arbeit zeigt einige konkrete Anwendungsfälle der Fehlerbaumanalyse auf. Genannte Anwendungsgebiete sind Nuklearreaktoren, schienengebundene Verladestationen für chemische Stoffe (Analyse der Gefahren beim Be- und Entladen), Verhinderungsmaßnahmen von Suiziden im Bahnverkehr und Analysen zur Verhinderung von Arbeitsunfällen durch z. B. Ausrutschen.
Weiterhin listet die Arbeit einige Ansätze auf, mit Hilfe derer die Nachteile der FTA kompensiert werden sollen. Ziel ist zumeist eine vereinfachte Erstellung

des Fehlerbaumes durch gezielte Betrachtung von Subproblemen und die Computer gestützte Auswertung. Dadurch wird beispielsweise die Betrachtung der dynamischen Entwicklung der Eintrittswahrscheinlichkeit einer Störung durch dynamische Änderung der Eintrittswahrscheinlichkeiten der Ursachen möglich (z. B. durch Alterung ändert sich die Ausfallwahrscheinlichkeit eines Gerätes, durch steigende Erfahrung eines Anlagenbedieners sinkt dessen Fehleranfälligkeit, durch geeignete Wartungsintervalle sinken Ausfallwahrscheinlichkeiten; diese Auswirkungen können bezogen auf eine Zeitskala berücksichtigt werden). Weiterhin wird beschrieben, wie die Wirkung menschlicher Fehler und deren psychologische Ursachen untersucht werden können. Es wird weiterhin auf Arbeiten verwiesen, welche den Umgang mit einer bekannten Schwankungsbreite für eine Ausfallwahrscheinlichkeit darlegen (Nutzung von Fuzzy-Logik).
Fertig.

[32] Die Verwendung der aus der Computerwissenschaft bekannten Methode des „model checking“ wird verwendet, um die Anlagensicherheit eines Crackers zu bewerten.
Traditionelle Methoden zur Sicherheitsbetrachtung wie HAZOP betrachten die verwendeten Sicherheitseinrichtungen nicht explizit. Um dieses Problem zu lösen wurde die graphenbasierte Darstellung einer Anlage durch „Process Control Event Diagrams = PCED“ eingeführt. Diese stellt den Informationsfluss zwischen Komponenten eines Systems dar (z. B. Anlagenfahrer, Sensor und Regeleinrichtung). Mit Hilfe dieser Beschreibungsform und ein geeigneten Beschreibung der Regellogik der Anlage kann eine Sicherheitsanalyse im Stile einer HAZOP durchgeführt werden. Dieser Prozess ist jedoch sehr zeitaufwendig. Die Methode des „model checking“ soll nun genutzt werden, um durch Modellverifikation diesen Analyseprozess automatisierbar zu machen. Das System muss dazu als Zustandsgraph mit Transitionen beschrieben werden. Ein solches Modell kann dann durch geeignete Software (z. B. Symbolic Model Verifier = SMV) mit Hilfe symbolischer Operationen automatisch untersucht werden. Verwendet man PCEDs, so kann die Modellstruktur teil-automatisiert in ein von SMV lesbares Format umgewandelt werden. Es existieren aber alternative Ansätze, um eine Anlage in ein von SMV lesbares Format zu bringen, beziehungsweise komplett andere Formalismen (Condition/Event Systems). Weiterhin existieren Methoden,

welche statt symbolischer Operationen mit Hilfe mathematischer Programmierung eine Modellbeschreibung vornehmen. Die Analyse geschieht dann mit Hilfe von „Integer Programming“ . Diese Arbeit zeichnet sich durch die frühe Anwendbarkeit im Entwicklungsprozess aus. PCED haben 5 Schichten zur Beschreibung des Informationsflusses. Die PCEDs werden im Detail definiert und die Symbolik wird erläutert. Notwendige Grundlage zur Verwendung ist das ausgearbeitete Fließbild der Anlage. Mit dessen Hilfe kann der Entwurf einer Sicherheitsfunktion auf Erreichen der gewünschten Wirkung untersucht werden. Die referenzierte Beschreibungssprache von SMV ist modular aufgebaut. Sie kann die Wechselwirkung zwischen Modulen abbilden. Es existiert eine Bibliothek zur Beschreibung von PLT Einrichtungen/ Funktionen in SMV. Ein Modulverhalten wird durch diskrete Zustandsvariablen beschrieben. Ein Modul im Sinne von SMV ist aber ziemlich low-level! Beispielsweise beschreibt ein Modul das Verhalten eines Sensor. Das Modul kann Sensordefekte, korrekte Messung und Unter-/Überschreiten von Grenzwerten modellieren. Es ist für Sicherheitsbetrachtungen also durchaus geeignet. Es wird auf weitere Module der Bibliothek eingegangen (Aktoren, Regler/Controller. Die Wechselwirkung zwischen Modulen wird in einem Main-Modul beschrieben. Als „sicher“ angesehene Zustände können gezielt definiert werden (durch SPEC). Die Anwendung der Methode wird anhand der Temperaturregelung eines Crackers dargelegt. Für diesen existiert angeblich eine veröffentlichte Sicherheitsbetrachtung! Verschiedene Szenarien können getestet werden, indem man Modulen konkrete Zustände zuweist. Ob dies automatisch gemacht werden kann wird nicht beleuchtet. Es scheint, als ob Fehlerszenarien manuell vorgegeben werden müssen.
fertig. Wenn SMV verwendet wird, so kann die Modellbildung entsprechend dieser Arbeit hier geschehen. Die auf Seite 3 zitierten Arbeiten mal anschauen! Die Modellierung mit SMV im Detail prüfen.

[45] Die wichtigste Arbeit bisher.
Sicherheitstechnische Aspekte bei Planung und Bau modularer Produktionsanlagen

[113] Vorstellung verschiedener Architekturen, wie Sicherheitsfunktionen (SIF) erfüllt werden können. Im Hinblick auf Modularisierung ist es von großer

Wichtigkeit, wie SIF implementiert werden. Sind SIF in jedem Modul einzeln implementiert, so muss bei Wechsel eines Moduls in erster Linie das Modul selbst validiert sein/werden. Das gleich gilt bei Einführung oder Änderung einer SIF. Werden SIF durch übergeordnete Sicherheitsregler implementiert, so muss für eine neue/geänderte SIF nicht nur das Modul selbst, sondern auch eben diese übergeordnete Einheit erneut geprüft werden. Der Aufwand steigt also maßgeblich an, wenn SIF nicht direkt im Modul implementiert sind.

[51] Ein modellbasierter Ansatz zur rechnergestützten Sicherheitsbetrachtung von Chemieanlagen während der Planungsphase

[52] Early hazard identification of chemical plants with statechart modelling techniques

[87] SDG-based hazop and fault diagnosis analysis to the inversion of synthetic ammonia

[147] SDG-based HAZOP analysis of operating mistakes for PVC process

[47] Risk and Hazard Control the new process control paradigm

[34] A preliminary study of thermal hydraulic models for virtual hazard and operability analysis and model-based design of rotating machine packages

[161] Hazard rate models for early detection of reliability problems using information from warranty databases and upstream supply chain

[1] This book contains the proceedings of a NATO Advanced Research Workshop on the Reliability and Safety Analysis of Dynamic Process Systems. Ziemlich alt, trotzdem mal reinschauen.

[2] Scheinbar ein Grundlagenbuch zum Thema Risikoanalyse und Reduktion von Risiken
Wird bereits im Text zitiert.
Auf jeden Fall noch mal reinschauen!.

[28] Buch, nachlesen

[27] Buch, nachlesen

[29] Buch, nachlesen

[22] Buch, nachlesen

[30] Buch, nachlesen

[20] Buch, nachlesen

[26] Buch, nachlesen

[25] Buch, nachlesen

[21] Buch, nachlesen

[24] Buch, nachlesen

[23] Buch, nachlesen

[97] Safety and Security Review for the Process Industries: Application of Hazop, Pha, What-If and Sva Reviews

[33] Mit Hilfe von Automaten wird durch Anwendung von Erreichbarkeitsanalyse gezeigt, wie durch eine automatisch ermittelte, sichere Folge an Prozessschritten ein gewünschter Modellzustand erreicht werden kann. Fokus dieser und ähnlicher Arbeiten liegt auf Batchprozessen.
Im Rahmen sicherheitstechnisch kritischer Prozesse muss sicher gestellt werden, dass ein geplantes Prozedere zur Beeinflussung einer Prozessvariable keine Sicherheitsbestimmungen verletzt - es muss verifiziert werden. Konkret muss sichergestellt werden, dass physikalische Größen innerhalb definierter Grenzen verbleiben, maximale Aktorstellgrößen nicht überschritten werden und dass Einschränkungen bezüglich der Verfügbarkeit von benötigten Subsystemen nicht verletzt werden(es werden keine Subsysteme für das Prozedere angefordert, welche nicht verfügbar sind). Folgende Begriffe sind in dieser Arbeit wichtig: **Aktionssequenz:** Führt ein System von einer Istsituation in eine Sollsituation. Die Sollsituation muss durch die Aktionssequenz erreicht werden. Sie besteht aus mehreren, einzelnen Aktionen, welche manuell oder automatisch ausgeführt werden können. Aktionen verändern den Zustand von Equipment und verändern dadurch physikalische Kennwerte. **Situation:** Zustand des Systems und Verfügbarkeit von Komponenten. Diese Arbeit will automatisch generierte Aktionssquenzen auf Sicherheit überprüfen. Dazu wird ein Systemmodell entsprechend **ISA88-Standard** als Kommunikations-Automat entworfen. Dieses Modell wird mit einer Erreichbarkeitsanalyse (mit Hilfe von Modell-überprüfungssoftware) untersucht. An einem Beispiel wird gezeigt, wie auf Basis eines R& I Fließbildes und anhand von zusätzlichen Überlegungen (z.B. Verriegelungen und andere sicherheitsrelevante Funktionen) ein Modell in der geforderten Form entworfen werden kann. Der dazu notwendige Prozess ist nur teilautomatisiert. Das entworfenen Modell kann dann auf Erreichbarkeit von Zuständen geprüft werden. Für erreichbare Zustände kann dann eine Aktionssequenz generiert werden. Die Aktionssequenzen führen zu gewünschten Situationen und halten (die vorher von Hand definierten) Sicherheitsbestimmungen ein. Sie sind jedoch nicht optimal (sinnloses öffnen/ schließen von Ventilen möglich). Weiterhin ist insbesondere für komplexe Systeme der notwendige Automat riesig (die Anzahl notwendiger Zustände wächst exponentiell mit der Anzahl der untersuchten Objekte). Es soll in Zukunft untersucht werden, ob Modelle abstrakter formuliert werden können, welche sich genauso wie die Detailmodelle verhalten. Ziel ist die Reduktion notwendiger Zustände.

Die Arbeit verweist auf andere Ansätze, welche automatisiert eine sichere Aktionssequenz zum erreichen eines Zustandes ermitteln sollen. Die zitierten Arbeiten sind jedoch alle schon recht alt. Es werden unter anderem grafische Methoden, Petrinetze und Statecharts genannt. Die Methoden liefern jedoch entweder nur nicht-ideale Sequenzen, können Hierarchien nicht gut abbilden, oder sind nicht in der Lage ein Equipment gleichzeitig mehreren Ebenen einer Hierarchie/ mehreren Funktionen zuordnen. Fertig. Der Ansatz hat mit meiner Arbeit nicht viel zu tun, zeigt aber die Verwendung von Graphen/Automaten/Zuständen zur Sicherheitsbetrachtung von Systemen. Die Suche nach aktuellen Arbeiten zu diesem Thema könnte noch etwas bringen. die zitierten Ansätze zur Modellbildung könnten noch interessant sein. Diese werden am Ende markiert.

[120] Why do verification approaches in automation rarely use HIL-test?

[59] A Tool for Hazard Detection in Hybrid Systems

[31] Wissensgestütztes Diagnosekonzept durch Kombination von Anlagenstruktur und Prozessmodell Dissertation. Später noch mal anschauen

[105] The focus of this book is the emerging topic of dynamic risk analysis, as opposed to traditional risk analysis. Research on how to dynamically assess risk has been carried out in several chemical and petroleum companies, but no real implementation has been attempted. This book is not aimed to be an exhaustive review of dynamic risk analysis; it is rather a concrete support for the application of new risk analysis techniques.

[152] Grundlagenbuch zur Sicherheitsbetrachtung von Chemischen Anlagen

4.2 HAZOP

[43] HAZOP Literaturübersicht
Die Arbeit liefert eine Übersicht zur Entwicklung der HAZOP von den ersten Arbeiten, welche die Methode konkret beschrieben haben 1974 bis hin zu aktuellen

Arbeiten (2007). Die Veröffentlichungen werden in verschiedene Themengebiete eingeteilt. Diese sind:

- Einführung in verschiedene Themen zur Risikoanalyse
- Einführung in HAZOP; konkrete Guidelines und Erfahrungsberichte zur Anwendung der Methode
- Vergleich von HAZOP mit anderen Methoden zur Risikoanalyse; jeweils Stärken und Schwächen der Methoden
- Erweiterungen der HAZOP (Quantifizierung, Einfluss des Menschen, Erfahrungsaustausch mit gemachten HAZOPs welcher immerhin 18% der untersuchten Arbeiten zum Thema hat...)
  - Erweiterung durch Kombination mit FMEA oder LOPA soll die Qualität der HAZOP verbessern, eine Kombination mit FTA liefert zusätzliche, quantitative Aussagen
- HAZOP für programmierbare Steuerungen, SIL - Zuweisung (ungefähr 22% der untersuchten Arbeiten)
- Automatisierung der HAZOP (durch Software); 40% der untersuchten Arbeiten (insgesamt etwas mehr als 160 Stück) zum Thema HAZOP beschäftigen sich mit dieser Thematik
- HAZOP und dynamische Simulationen

Siehe für noch aktuellere Entwicklungen [109]. Insbesondere der Abschnitt 3.5 verweist auf Arbeiten zur Automatisierbarkeit der HAZOP und ist daher für mich relevant. Die Arbeit noch mal lesen und ausführlicher wiedergeben.

[109] Aktueller Untersuchungen zur Automatisierbarkeit von HAZOP. Wird bereits im Text zitiert

[115] Methodology for the generation and evaluation of safety system alternatives based on extended Hazop

[44] Combining HAZOP with dynamic simulation — Applications for safety education

[78] Model-based HAZOP study of a real MTBE plant

[42] New trends for conducting hazard & operability (HAZOP) studies in continuous chemical processes

4.3 automatisierte HAZOP

[6] Entwurf einer Ontologie um die Informationen, welche im Rahmen einer HAZOP gewonnen werden, in einer Art darzustellen, dass sie von einem PC leicht weiter verarbeitet oder wieder verwendet werden können.

[159] PHASuite: An Automated HAZOP Analysis Tool for Chemical Processes Part I

[160] PHASuite: An Automated HAZOP Analysis Tool for Chemical Processes Part II

[114] ExpHAZOP+: Knowledge-based expert system to conduct automated HAZOP analysis

[104] An automated system for batch hazard and operability studies

[117] A functional HAZOP methodology

[145] A new intelligent assistant system for HAZOP analysis of complex process plant

[12] A systematic formulation for HAZOP analysis based on structural model

4.4 Fehlerfortpflanzung

4.4.1 modellbasiert, qualitativ

[107]

Eine Computer basierte Methode zur Identifizierung von Gefahren in kontinuierlich betriebenen Anlagen wird vorgestellt. Das Vorgehen der Gefahridentifizierung orientiert sich dabei stark am Vorgehen in einer HAZOP. Die Methode soll bei einer HAZOP als Ergänzung einsetzbar sein.

Als Basis der Gefahridentifikation dient die Menge alle Prozessvariablen – ergänzt um die Menge aller Guide-Wörter (mehr, weniger, zu viel, zu wenig...), die im Rahmen einer HAZOP angewandt werden. Die Gesamtanlage wird in Basis Einheiten zerlegt. Eine Basiseinheiten ist durch ihr Verhalten bezüglich der Weiterleitung von Gefahren beschrieben. Gefahren können entstehen, verstärkt, gedämpft, weitergeleitet oder aufgehoben werden. Physisch werden Basis Einheiten in Leitungselemente („lines“) (Pumpen, Rohre Ventile...) und Gefäße („vessels“) (Tanks, Reaktoren, Kolonnen...) unterschieden. Ob ein Fehler durch eine Einheit weitergereicht wird, oder nicht, wird durch definierte Regeln beschrieben. Die Aufstellung dieser Regeln wird im Detail genannt. Außerdem wird auf die Funktion des erstellten Computer Programms eingegangen.

Die Anwendbarkeit der Methode wird an einem konkreten Beispiel gezeigt: [108]

Methode ist als Grundlage sinnvoll. Weiterentwicklung der Methode suchen!

[153]

Ziel ist die Fortpflanzung von Fehler zu ermitteln. Einerseits um während der Entwurfsphase die Auswirkungen eines Fehlers besser abschätzen und in Folge dessen Gegenmaßnahmen in geeignetem Umfang entwerfen zu können und andererseits um im Betrieb die genau Ursache bzw. die Verkettung von Ursachen ermitteln zu können, welche zu einem Alarm geführt haben. Dazu werden gerichtete Graphen (SDG) verwendet.

Gerichtete Graphen bestehen aus Knoten und gerichteten Kanten, welche die Beziehung zwischen den Knoten darstellen. Die Knoten umfassen bspw. Pro-

zessgrößen, Arbeitspunkte, Stellgrößen und bekannte Störungen. Die Erstellung eines solchen Graphen ist auf Textbasis mit Hilfe von Grapheditoren/ Werkzeugen wie Graphviz (http://www.graphviz.org/) möglich. Dies ermöglicht eine Automatisierung.

Die historische Entwicklung von SDG wird kurz benannt. Der Aufbau von SDG kann auf Basis von DAEs oder auf Grundlage von Wissen über den Prozess geschehen. Für Standardkomponenten oder Module kann bereits vorab ein SDG erstellt werden. Die Informatio n der Kopplung kann aus dem P&ID gewonnen werden. Wird die Struktur des P&ID z. B. als XML oder als Verbindungs- und Adjazenzmatrix abgebildet, so können Modul-SDGs korrekt gekoppelt werden.

- Vorteile einer wissensbasierten Erstellung von SDGs:
  - teilautomatisiert durch Softwareunterstützung möglich
- Nachteile:
  - Graph wird nicht plausibilisiert, kein Test auf Kausalität
  - Kanten werden nicht gewichtet -> extrem unwahrscheinliche Fehlerfortpflanzungen sind nicht von wahrscheinlichen zu unterscheiden
  - Wechselwirkungen zwischen mehreren Eingangsparametern werden nicht abgebildet
  - Zeithorizont wird nicht abgebildet, in Folge dessen sind transiente Vorgänge nicht von Stationären zu unterscheiden

Die Arbeit empfiehlt daher einen Übergang zu datenbasierter Graphenentwicklung. Dadurch wird das schon wieder Mist.. Durch die Verwendung von Messdaten und den Einsatz gezielter Verzögerungen kann die Korrelation zwischen Größen bestimmt und der Graph konstruiert werden. Die Korrelation muss dabei mit Hilfe geeigneter Verfahren auf Signifikanz untersucht werden.

- Vorteile einer datenbasierten Erstellung von SDGs:
  - Ergebnis ist kausal und enthält Zeitbezug (Verzögerungen)
- Nachteile:
  - nur messbare Größen werden untersucht
  - Verfahren zum Signifikantest von Korrelationen sind nicht eindeutig

Fazit: Kombination der beiden Methoden. Wissensbasierter Ansatz schafft komplettes Netz, datenbasierter Ansatz verfeinert den Graphen. Anhand einer Fallstudie kann wird der Erfolg der Methode gezeigt.

Fazit: Ansatz der Graphen sieht vielversprechend aus, die Verfeinerung und Verifizierung des SDG mit Messdaten wird aber nicht möglich sein. **Weitere Suche in die Richtung lohnt sich.**

4.4.2 datenbasiert

[158]

Als datenbasierte Risikoanalyse wird Deep Learning vorgeschlagen. Genau genommen wird die Verwendung eines Deep Belief Network (DBN) vorgeschlagen. Dessen Schichten bestehen aus Restricted Boltzmann Machine (RBN). Ziel ist eine verbesserte Erkennung von Fehlern.

Übersicht über aktuelle Methoden der datenbasierten Risikoanalyse (als Alternative zu quantitativen oder qualitativen modellbasierten Methoden):

1. statistische Methoden
    - principal component analysis (PCA)
    - partial least squares (PLS)
    - independent component analysis (ICA)
    - fisher discriminant analysis (FDA)
    - subspace aided approach (SAP)
    - correspondence analysis (CA)
    - $\rightarrow$ Vergleich der Methoden anhand des Tennessee Eastman Benchmark (TEB) durch (Yin, et al., 2012)
    - Bayesian diagnosis
2. Methods based on pattern classification
    - artificial neural network (ANN)
    - k-nearest neighbor (KNN)

- self-organizing map (SOM)
- support vector machine (SVM)
- artificial immune system (AIS)

Weitere Übersichtsarbeit zum Thema Datenbasierte Fehlerfortpflanzung findet sich in [127].

Die vorgestellte Methode erweist sich bei Anwendung auf den TEB als sehr erfolgreich. Jedoch wird zum Training der Struktur (wie auch bei allen anderen Risikoanalysemethoden, welche auf Daten basieren) eine große Mengen an Messdaten erfordert. Insbesondere eine große Anzahl an Daten zu Fehlfunktionen in der Anlage ist erforderlich um die Fortpflanzung von Fehlern im Netz beschreiben zu können.

Fazit: Methode ist wenig Erfolg versprechend für den Einsatz in modularen Anlagen, bevor die Gesamtanlage bestehen aus Modulen in Betrieb genommen wurde.

[83]

Der Einfluss von Alterungserscheinungen in Mehrkomponentensystemen wird untersucht. Besteht ein Systemen aus sicherheitsrelevanten und nicht sicherheitsrelevanten Systemen, so kann die Alterung/ der Verschleiß der nicht sicherheitsrelevanten Systemen die Alterung der sicherheitsrelevanten Systeme durch Fortpflanzung der Alterungserscheinung beschleunigen/ beeinflussen. Setzt sich durch Alterung beispielsweise ein Filter langsam zu, so muss eine Pumpe immer mehr Druck auf eine Flüssigkeiten aufbauen, um einen konstanten Volumenstrom hinter dem Filter zu gewährleisten. Die Pumpe verschleißt dadurch schneller. Eine solche Wechselwirkung kann geeignet durch Verwendung einer multi-layered vector-valued continuous-time Markov chain abgebildet werden. Dazu werden statistische Daten benötigt.

Fazit: Die Fortpflanzung „normaler“ Fehler in Sinne der HAZOP kann dadurch nicht ohne aufwendige Umformungen/ Adaptionen abgebildet werden.

[7]

Die vorgestellte Methode verwendet historische Daten um die Fehlerfortpflanzung zu untersuchen. Mit Hilfe von Kreuzkorrelation wird die Zeitverzögerung zwischen Prozessgrößen berechnet und daraus eine Struktur der Abhängigkeiten abgeleitet. Aus der Kreuzkorrelation wird eine kausale Abfolge von Ereignissen konstruiert, dass die Fortpflanzung eines Fehlers in einem Graphen dargestellt werden kann.

Die Methode benötigt Messdaten der Gesamtanlage und kann daher nicht verwendet werden.

[148]

Die Methode basiert auf der Auswertung von Residuen und einer „contribution plot analysis“ . Die Residuen werden durch Identifikation von Paritäts- und Unterräume berechnet. Die optimalen Residuen werden dann genutzt, um ein Fehleridentifikationsschema zu erstellen. Auf Basis des Durchschnitts aktueller und historischer Residuen wird ein Index definiert. Die Fehlerfortpflanzung kann dann anhand dieses Index ermittelt werden. Anhand eines TEB wird die Wirksamkeit des Verfahrens demonstriert.

Die Einleitung gibt einen umfassenden Überblick über datenbasierte Methoden und referenziert zahlreiche Quellen.

Die Methode ist für meine Zwecke nicht geeignet, das Einleitungskapitel lohnt sich aber wegen der vielen datenbasierten Verfahren noch mal anzusehen.

[56]

Datenbasierter Ansatz welcher ein qualitatives Modell mit Hilfe statistischer Entropien liefert. Das Verfahren wurde erfolgreich eingesetzt, um einen gerichteten Ursache-Wirkungsgraphen zu erstellen (Quellen werden genannt). Das Verfahren wird derart erweitert, dass einzeln auftretende Fehler, welche eine erkannte Störung verursacht haben, identifiziert werden können.

[149]

Verwendung von Principle component analysis (PCA) in Verbindung mit einer angepassten Variante von Dynamic time warping (DTW) um insbesondere in der schwierigen Phase des Starts einer verfahrenstechnischen Anlage Fehler erkennen zu können. Die Einleitung liefert zahlreiche Verweise zur Verwendung von PCA. Es kommt die Software „SymCure“ der Firma „GenSym“ zum Einsatz, mit Hilfe derer umfangreiche Entwicklungen zum Thema Fehlererkennung und -behebung möglich sind. Die vorgestellte Methode vergleicht online den aktuellen Signalverlauf mit bekannten Verläufen von Fehlerzuständen und Normverläufen. Auf diese Weise wird das Auftreten bekannter Fehler diagnostiziert. Neue Fehler werden durch die eingesetzte Software „SymCure“ erkannt, deren Ursache bestimmt und der Verlauf anschließend der Signaldatenbank hinzugefügt. Die Methode zeichnet sich vor allem durch hohen Recheneffizienz aus.

Der Verweis auf viele Arbeiten zu PCA und auf die verwendete Software ist hilfreich. Außerdem kann die Arbeit als Beispiel verwendet werden.

[81]

Komplettes Framework zum Erkennen von Fehlern und Identifikation der zugrunde liegenden Ursachen.

Das erste Kapitel verweist auf viele Arbeiten zum Thema datenbasierte Analyse und benennt bekannte Probleme.

4.4.3 hybride Methoden

[63]

modellbasiert qualitativ und datenbasiert Fehlerfortpflanzung mit Hilfe von Dynamischen Bayesschen Netzen. Grundlage bietet die HAZOP der Gesamtanlage. Ziel ist es während dem Betrieb einer Anlage bei Auftreten eines Fehlers (eines Alarms) dessen wahrscheinlichste Ursache oder Ursachen schnell zu ermitteln und den Pfad von der Ursache oder den Ursachen zum Fehler/Alarm einfach lesbar (grafisch) darstellbar zu machen. Dem

Operator wird so die Wahl, welche Aktion zum Beheben des Fehlers notwendig ist, maßbeglich vereinfacht.

Grundlage des Netzes sind eine Struktur, welche die Entwicklung von Fehlern abbildet und eine Menge von Messdaten, welche das Netz verfeinert. Die statischen Knoten des Netzes werden aus einer voran gegangen HAZOP ermittelt. Jeder Knoten entspricht dabei einer in der HAZOP untersuchten Prozessvariable. Alternative Verfahren dazu sind die Durchführung einer FTA oder die Anwendung der **Bow Tie Methode**. Insbesondere eine FTA würde die Fortpflanzung von Fehlern genauer beschreiben und wäre daher zu bevorzugen. Die Informationen, welche aus einer HAZOP entstehen, werden aber als ausreichend betrachtet. Die statischen Knoten werden um dynamische Knoten ergänzt. Sie repräsentieren (versteckte) Fehler-Modi des Systems. Ihre genauen Werte werden aus Messdaten aus dem Live-Betrieb ermittelt. Neben der Festlegung der Knoten muss die Struktur bestimmt werden. Der Lösungsaufwand dieses Problems wächst exponentiell mit der Anzahl an Knoten. Mit dem Wissen aus der HAZOP (dem Wissen, wie sich ein Fehler fortpflanzt) kann der Lösungsraum bei der Strukturberechnung des Netzes aber stark eingeschränkt werden. Zu beachten ist dabei, dass im Rahmen der HAZOP in der Regel nur direkt benachbarte Bauteile (Knoten, definierte Untersuchungseinheiten) auf Wechselwirkung hin untersucht werden. Weiterführende Fortpflanzungen werden nicht betrachtet. Die Berechnung der optimalen Struktur eines Dynamischen Bayesschen Netzes kann durch verschiedene Algorithmen erfolgen. Eine Variante ist der **K2 Algorithmus** von Cooper und Hersovits, 1992. Dazu werden jedoch Messdaten benötigt, welche die zeitliche Entwicklung eines Fehlers abbilden (aus Simulation gewinnbar?). Die Aufstellung der Conditional probability tables (CPT) erfordert weiterhin große Mengen an Messdaten. Das erhaltene Netz kann dann aber die Entwicklung von Fehlern über mehrerer Ebenen hinweg ermitteln / untersuchen. Eine Darstellung der Netzentstehung findet sich in Abbildung 4.1.

Fazit: Methode sieht schick aus, Datenbasis ist bei neuer Anlage aber nicht gegeben. Nur eine bestehende (Komplett-!) Anlage mit historischen Messdaten kann mit dieser Methode tiefgreifend analysiert werden. Eine Sicherheitsanalyse kann dann damit verbessert werden.

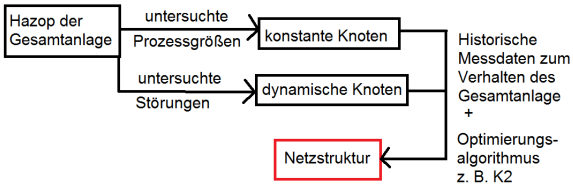

Abbildung 4.1: Erstellung eines Dynamischen Bayesschen Netzes

[18]

Resiliente Systeme, Verwendung eines hierarchical fault propagation model (HFPM) als Erweiterung der Infrastructure Resilience-Oriented Modeling Language (IRML). Ziel des Modells ist die Beschreibung des dynamischen Verhaltens und die dynamische Fortpflanzung von Fehlern. Des neue Modell hat zwei Teile: statische Analyse der Struktur und dynamische Analyse für Fehlerfortpflanzung. Untersucht werden Fehler durch Abweichungen von Stoffparametern und Geräteausfälle. Der Fokus liegt auf der Analyse der Resilienz (Fähigkeit des Systems trotz Fehler in definierten Zustand zu gelangen).

Wird eine HAZOP um ein Strukturmodell ergänzt, so kann eine Fehleranalyse systematisch durchgeführt werden (Boonthum et al., 2014). Eine HAZOP erfasst aber nur die Abhängigkeit von Prozessgrößen und nicht die der Komponenten eines Systems, eine makroskopische Betrachtung von Fehlerfortpflanzungen ist daher nicht möglich. Die folgenden Methoden zur makroskopischen Betrachtung werden genannt:

- Utne et al. (2011): cascade diagram
- Johansson and Hassel (2010): agent based approach $\mapsto$ benötigt detaillierte Prozesskenngrößen und Messwerte, quantitativ
- Kjølle et al. (2012) across-sector approach $\mapsto$ benötigt vielseitiges Wissen und umfangreiche Daten über den Prozess, diese sind oft nicht vorhanden
- Haimes and Jiang (2011) Framework basierend auf Leontief's input-output model $\mapsto$ ungeeignet für die Analyse von Verknüpfungen auf Komponentenebene
- SDG insbesondere in Verbindung mit HAZOP

- Functional Resonance Analysis Method (FRAM) $\mapsto$ emphasizes the functional relationship between components and provides a way to describe the fault evolution
- fault semantic network (FSN) using genetic programming (GP) and neural networks (NN) $\mapsto$ braucht viele Daten und Prozesswissen
- Petrinetze
- hierarchical Bayesian model (HBM)
- Markov network combined with Bayesian theory

Vorteile HFPM:

1. Fehleranalyse auf Systemebene (statt Komponentenebene)
2. durch Simulation können im vorweg geeignete Sicherheitsmaßnahmen ermittelt werden, um gewünschte Sicherheitslevel zu erreichen

Systemaufbau:

- basierend auf IRML
- ein System wird in Subsysteme gegliedert, die Struktur durch ein hierarchisches Framework dargestellt, die Gliederung in mehrere Ebenen von Subsystemen stellt die Prozessstruktur und Fehlerszenarien dar
- statische Analyse: zeigt den Grad der Abhängigkeit von Subsystemen auf, das System wird auf die Teile mit den stärksten Wechselwirkungen reduziert und diese Teilsysteme werden im Detail weiter untersucht
- dynamische Analyse: Anwendung von Testfällen; durch Wenn–dann Analyse werden die Fortpflanzung eines bekannten Fehlers und die Operationen des Systems, welche notwendig sind, um in einen stabilen Zustand zurück zu kehren, im Modell so eingestellt, dass das Verhalten dem Testfall entspricht, mit Hilfe geeigneter Parameter, welche vor allem das zeitliche Verhalten widerspiegeln, wird das Verhalten gekennzeichnet und darauf aufbauen ein Zustandsgraph ermittelt

Fazit: statische Analyse ist hilfreich, bietet aber keinen besonderen Mehrwert, dynamische Analyse erforderte historische Messdaten, Aufteilung auf Module ist fragwürdig, Analyse der anfälligsten Subsysteme ist hilfreich, Fokus liegt auf Resilienz und Berechnungen zum Sicherheitslevel insbesondere während ein

Fehler sich im System verbreitet und das System darauf reagiert, für meine Arbeit eher nicht zu gebrauchen die verwiesenen Methoden zur makroskopischen Betrachtung könnten hilfreich sein.

[88]

Entwicklung einer echtzeitfähigen Methode zum Erkennen des Vorliegen eines Fehlers und Identifikation der Grundursache. Verwendung von PCA in Kombination mit Bayesian Belief Network (BBN). Aus Daten zum Normalbetrieb wird das PCA aufgebaut. Im laufenden Betrieb kann dann damit das Vorliegen eines Fehlers erkannt werden. Mit Hilfe historischer Daten zur Prozessdynamik oder durch Formulierung von Differentialgleichungen oder durch Expertenwissen wird das BBN aufgestellt. Auf Basis des BBN kann bei vorliegen eines Fehlers dessen Ursache ermittelt werden. Das initiale BBN wird mit fortschreitender Betriebszeit durch Informationen aus der PCA verbessert um die Ursachenanalyse genauer zu machen.

Schöne Methode, welche statische Verfahren (PCA) mit Prozesswissen (BBN) vereint, die benötigten Daten zum Gesamtprozess, welche für PCA notwendig sind, liegen bei modularen Anlagen aber nicht vor ↦ bringt nichts

4.4.4 Rezensionen

- Einführung in [158]: Übersicht datenbasierte Methoden
- Einführung in [153]: Entwicklung von Methoden zu SDG
- Einführing in [88]: Verweise auf mehrere Methoden/Anwendungen von SDG
- Einführung in [18] Methoden zur makroskopischen Fehlerfortpflanzung ↦ genau das will ich eigentlich
- Einführung in [148]: Datenbasierte Fehlerfortpflanzung
- [127]: Datenbasierte Fehlerfortpflanzung
- [156]: Datenbasierte Fehlerfortpflanzung
- [137]: Datenbasierte Fehlerfortpflanzung
- [65]: Modellbasierte und stochastische Methoden der Fehlerfortpflanzung;

Reglerneueinstellung nach Fehlererkennung

- [96]
- [157] Umfassende Übersicht zum Thema Fehlerfortpflanzung und Fehleridentifikation
- [154]
- [41]: Ursachenanalyse von anlagenweiten, schwingenden Fehlern
- Einführung in [81]: Übersicht zu datenbasierten Methoden
- [141]: quantitative modellbasierte Methoden
- [138]: qualitative modellbasierte Methoden
- [142]: datenbasierte Methoden

4.4.5 unsortiert

[5] Qualitative models of equipment units and their use in automatic HAZOP analysis

Wichtige Begriffe 5

Package Unit aus Wikipedia:
Eine Package Unit (aus dem Englischen package und unit entlehnt; wörtlich Paketeinheit[1][2] oder [ab]gepackte sinngemäß auch abgegrenzte Einheit ist eine von einem Fremdunternehmen geplante und gefertigte Anlage. Die Anforderungen und Voraussetzungen für eine Package Unit sind in einem Lastenheft genannt. Spezielle Anforderungen an eine Package unit sind z. B. Leistungsparameter, Abmessungen und der Steuerungsumfang.

SIF Safety Integrated Function: Ein Zusammenschluss von Komponenten um das Risiko durch eine bestimmte Gefahrenquelle (Hazard) zu reduzieren.

SIL Der Safety Integrity Level bzw. Sicherheitsintegritätslevel, kurz SIL, ist eine Maßeinheit zur Quantifizierung von Risikoreduzierung im Bereich von 1 bis 4. Je größer die Zahl ist, desto mehr muss ein erkanntes Risiko reduziert werden.

IPL An independent protection layer (IPL) is a device, system, or action that is capable of preventing a scenario from proceeding to its undesired consequence independent of the initiating event or the action of any other layer of protection associated with the scenario.

QRA Quantitative Risk Analysis:

IEs initiating events: Zu einem risikobehafteten Zustand führende Ursachen/ Ereignisse

PHA Process Hazard Analysis: Untersuchung von Prozessrisiken.

Entropy Entropies are an information theoretical concept to characterize the amount of information needed to predict the next measurement with a certain precision.

Literaturverzeichnis

[1] Tunc Aldemir u. a. *Reliability and Safety Assessment of Dynamic Process Systems*. 1. Aufl. NATO ASI Series 120. Springer-Verlag Berlin Heidelberg, 1994.

[2] Bilal M. Ayyub. *Risk Analysis in Engineering and Economics*. 2. Aufl. Chapman und Hall/CRC, 2014.

[3] Ahmed Ali Baig, Risza Ruzli und Azizul B. Buang. „Reliability Analysis Using Fault Tree Analysis: A Review“. In: *International Journal of Chemical Engineering and Applications* (2013), S. 169–173.

[4] John Baillieul und Tariq Samad, Hrsg. *Encyclopedia of Systems and Control*. Springer London, 2015.

[5] V Bartolozzi u. a. „Qualitative models of equipment units and their use in automatic HAZOP analysis“. In: *Reliability Engineering & System Safety* 70.1 (2000), S. 49–57.

[6] Rafael Batres. „An ontology approach to support HAZOP studies“. In: *Asian Pacific Confederation of Chemical Engineering congress program and abstracts*. The Society of Chemical Engineers, Japan. 2004, S. 466–466.

[7] Margret Bauer und Nina F. Thornhill. „A practical method for identifying the propagation path of plant-wide disturbances“. In: *Journal of Process Control* 18.7 (2008), S. 707–719.

[8] Arno Behr, Henning Witte und Michael Zagajewski. „Scale-up durch Miniplant-Technik: Anwendungsbeispiele aus der homogenen Katalyse“. In: *Chemie Ingenieur Technik* 84.5 (2012), S. 694–703.

[9] Peter L. Bernstein. *Against the Gods: The Remarkable Story of Risk*. Wiley, 1998.

[10] Sanofi-Aventis Bleuel u. a. *NE 148: Anforderungen an die Automatisierungstechnik durch die Modularisierung verfahrenstechnischer Anlagen.* Techn. Ber. NAMUR, 2013.

[11] Dr. Michael Böhmer u. a. *Lage und Zukunft der deutschen Industrie (Perspektive 2030).* 2016.

[12] Narapan Boonthum, Unchalee Mulalee und Thongchai Srinophakun. „A systematic formulation for HAZOP analysis based on structural model". In: *Reliability Engineering & System Safety* 121 (2014), S. 152–163.

[13] Thomas Bott und Gerhard Schembecker. *Die 50 % – Idee Vom Produkt zur Produktionsanlage in der halben Zeit.* Vortrag zum Jahrestreffen der PAAT-Fachgemeinschaft in Weinheim. 2009. URL: `http://processnet.org/processnet_media/die+50prozent_idee+vortrag+bott_schembecker-p-1158.pdf` (besucht am 23. 04. 2017).

[14] Christian Bramsiepe und Gerhard Schembecker. „Die 50 % – Idee: Modularisierung im Planungsprozess". In: *Chemie Ingenieur Technik* 84.5 (2012), S. 581–587.

[15] William Bill Bridges und Tony Clark. „Key issues with implementing LOPA". In: *Process Safety Progress* 29.2 (2010), S. 103–107.

[16] Andreas Brodhagen u. a. „Erhöhung der Wirtschaftlichkeit durch beschleunigte Produkt- und Prozessentwicklung mit Hilfe modularer und skalierbarer Apparate". In: *Chemie Ingenieur Technik* 84.5 (2012), S. 624–632.

[17] Dr. Sigurd Buchholz. *The F3 Factory Project – Flexible, Fast and Future Production Processes.* Final Report. 2014. URL: `http://www.f3factory.com/scripts/pages/en/newsevents/F3_Factory_final_report_to_EC.pdf` (besucht am 23. 04. 2017).

[18] Zhansheng Cai u. a. „Hierarchical fault propagation and control modeling for the resilience analysis of process system". In: *Chemical Engineering Research and Design* 103 (2015), S. 50–60.

[19] Catherine A. Catino und Lyle H. Ungar. „Model-based approach to automated hazard identification of chemical plants". In: *AIChE Journal* 41.1 (1995), S. 97–109.

[20] CCPS. *Guidelines for Developing Quantitative Safety Risk Criteria*. 1. Aufl. JOHN WILEY & SONS INC, 2009.

[21] CCPS. *Guidelines for Engineering Design for Process Safety*. JOHN WILEY & SONS INC, 2012.

[22] CCPS. *Guidelines for Hazard Evaluation Procedures*. JOHN WILEY & SONS INC, 2008.

[23] CCPS. *Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis*. JOHN WILEY & SONS INC, 2015.

[24] CCPS. *Guidelines for Managing Process Safety Risks During Organizational Change*. JOHN WILEY & SONS INC, 2013.

[25] CCPS. *Guidelines for Process Safety Acquisition Evaluation and Post Merger Integration*. JOHN WILEY & SONS INC, 2010.

[26] CCPS. *Guidelines for Process Safety Metrics*. 1. Aufl. JOHN WILEY & SONS INC, 2009.

[27] CCPS. *Guidelines for Risk Based Process Safety*. JOHN WILEY & SONS INC, 2007.

[28] CCPS. *Guidelines for Safe and Reliable Instrumented Protective Systems*. JOHN WILEY & SONS INC, 2007.

[29] CCPS. *Guidelines for the management of change for process safety*. JOHN WILEY & SONS INC, 2008.

[30] CCPS. *Inherently Safer Chemical Processes: A Life Cycle Approach*. JOHN WILEY & SONS INC, 2008.

[31] Lars Christiansen. „Wissensgestütztes Diagnosekonzept durch Kombination von Anlagenstruktur– und Prozessmodell“. ger. Diss. Holstenhofweg 85, 22043 Hamburg: Helmut-Schmidt-Universität, 2015.

[32] Paul W.H. Chung und Shuang H. Yang. „Safety Analysis of Process Plant Control Systems Based on Model Checking“. In: *Safety and Reliability* 23.1 (2002), S. 19–34.

[33] Thomas Cochard, David Gouyon und Jean-Francois Petin. „Generation of safe plant operation sequences using reachability analysis“. In: *2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA)*. Institute of Electrical und Electronics Engineers (IEEE), 2015, S. 1–8.

[34] R. Conti u. a. „A preliminary study of thermal hydraulic models for virtual hazard and operability analysis and model-based design of rotating machine packages“. In: *Proceedings of the Institution of Mechanical Engineers, Part E: Journal of Process Mechanical Engineering* 228.4 (2013), S. 255–271.

[35] Frank Crawley und Brian J. Tyler. *HAZOP: Guide to Best Practice*. Elsevier - Health Sciences Division, 2015. 168 S.

[36] Andreas Dengel. *Semantische Technologien*. Springer Spektrum, 2011.

[37] *Der Sicherheitsbericht nach Störfall–Verordnung – Eine Handlungshilfe für Behörden und Betreiber – Stand 01.03.2009*. 2009.

[38] *Die 50 % – Idee Vom Produkt zur Produktionsanlage in der halben Zeit*. Thesen Tutzing. 2009. URL: `http://processnet.org/processnet_media/die+50prozent_idee-p-1159.pdf` (besucht am 23. 04. 2017).

[39] *Die 50 % – Idee Vom Produkt zur Produktionsanlage in der halben Zeit*. Positionspapier zu bestehendem Forschungsbedarf und Empfehlungen an die Forschungsförderung. 2010. URL: `http://processnet.org/processnet_media/Positionspapier+50+_+Idee+final-p-1296.pdf` (besucht am 23. 04. 2017).

[40] Peter Dietz und Uwe Neumann. „Verfahrenstechnische Maschinen — Chancen der gleichzeitigen Prozeß- und Maschinenentwicklung“. In: *Chemie Ingenieur Technik* 72.1-2 (2000), S. 9–16.

[41] Ping Duan u. a. „Methods for root cause diagnosis of plant-wide oscillations“. In: *AIChE Journal* 60.6 (2014), S. 2019–2034.

[42] Jordi Dunjó Denti. „New trends for conducting hazard & operability (HAZOP) studies in continuous chemical processes“. Diss. Universitat Politècnica de Catalunya, 2010.

[43] Jordi Dunjó u. a. „Hazard and operability (HAZOP) analysis. A literature review“. In: *Journal of Hazardous Materials* 173.1-3 (2010), S. 19–32.

[44] Shimon Eizenberg, Mordechai Shacham und Neima Brauner. „Combining HAZOP with dynamic simulation — Applications for safety education“. In: *Journal of Loss Prevention in the Process Industries* 19.6 (2006), S. 754–761.

[45] Christoph Fleischer u. a. „Sicherheitstechnische Aspekte bei Planung und Bau modularer Produktionsanlagen“. In: *Chemie Ingenieur Technik* 87.9 (2015), S. 1258–1269.

[46] Christoph Fleischer-Trebes u. a. „Planungsansatz für modulare Anlagen in der chemischen Industrie“. In: *Chemie Ingenieur Technik* (2016).

[47] Gheorghe Florea und Radu Dobrescu. „Risk and Hazard Control the new process control paradigm“. In: *Systems, Control, Signal Processing and Informatics II, Prague* (2014).

[48] Hossam A. Gabbar. „Improved qualitative fault propagation analysis“. In: *Journal of Loss Prevention in the Process Industries* 20.3 (2007), S. 260–270.

[49] Zhiwei Gao, Carlo Cecati und Steven X Ding. „A Survey of Fault Diagnosis and Fault-Tolerant Techniques—-Part I: Fault diagnosis with model-based and signal-based approaches“. In: *IEEE Transactions on Industrial Electronics* 62.6 (2015), S. 3757–3767.

[50] Zhiwei Gao, Carlo Cecati und Steven X Ding. „A Survey of Fault Diagnosis and Fault-Tolerant Techniques–Part II: Fault Diagnosis With Knowledge-Based and Hybrid/Active Approaches“. In: *IEEE Transactions on Industrial Electronics* 62.6 (2015), S. 3768–3774.

[51] Holger Graf. „Ein modellbasierter Ansatz zur rechnergestützten Sicherheitsbetrachtung von Chemieanlagen während der Planungsphase“. Diss. Technische Universität Dortmund, 2000.

[52] Holger Graf und H. Schmidt-Traub. „Early hazard identification of chemical plants with statechart modelling techniques“. In: *Safety Science* 36.1 (2000), S. 49–67.

[53] Ignacio E. Grossmann und Arthur W. Westerberg. „Research challenges in process systems engineering“. In: *AIChE Journal* 46.9 (2000), S. 1700–1703.

[54] Laura Grundemann, Martin Schoenitz und Stephan Scholl. „Shorter Time-to-Market with Micro-Conti Processes“. In: *Chemie Ingenieur Technik* 84.5 (2012), S. 685–693.

[55] Łukasz Hady und Günter Wozny. „Multikriterielle Aspekte der Modularisierung bei der Planung verfahrenstechnischer Anlagen“. In: *Chemie Ingenieur Technik* 84.5 (2012), S. 597–614.

[56] Payman Hajihosseini, Karim Salahshoor und Behzad Moshiri. „Process fault isolation based on transfer entropy algorithm“. In: *ISA Transactions* 53.2 (2014), S. 230–240.

[57] Ulrich Hauptmanns. *Prozess–und Anlagensicherheit*. Springer, 2013.

[58] Christoph Helling u. a. „Fundamentals towards a Modular Microstructured Production Plant“. In: *Chemie Ingenieur Technik* 84.6 (2012), S. 892–904.

[59] Peter Herrmann und Peter Grannas. „A Tool for Hazard Detection in Hybrid Systems“. In: *Proceedings of the 4th International Conference on Automation of Mixed Processes: Hybrid Dynamic Systems (ADPM2000)*. 2000, S. 225–230.

[60] Volker Hessel u. a. „Potenzialanalyse von Milli- und Mikroprozesstechniken für die Verkürzung von Prozessentwicklungszeiten - Chemie und Prozessdesign als Intensivierungsfelder“. In: *Chemie Ingenieur Technik* 84.5 (2012), S. 660–684.

[61] Lukas Hohmann u. a. „Modules in process industry - A life cycle definition“. In: *Chemical Engineering and Processing: Process Intensification* 111 (2017), S. 115–126.

[62] Paul W. Holland. „Statistics and Causal Inference“. In: *Journal of the American Statistical Association* 81.396 (1986), S. 945–960.

[63] Jinqiu Hu u. a. „Fault propagation behavior study and root cause reasoning with dynamic Bayesian network based framework“. In: *Process Safety and Environmental Protection* 97 (2015), S. 25–36.

[64] P. Hugo und F. Lopez. „Umwandlung diskontinuierlicher chemischer Prozesse in eine kontinuierliche Prozessführung unter Verwendung mikrostrukturierter Reaktoren - Reaktionstechnik und Sicherheit“. In: *Chemie Ingenieur Technik* 81.1-2 (2009), S. 145–152.

[65] I. Hwang u. a. „A Survey of Fault Detection, Isolation, and Reconfiguration Methods“. In: *IEEE Transactions on Control Systems Technology* 18.3 (2010), S. 636–653.

[66] B. Kampczyk u. a. „Effizientere Anlagenplanung durch Modularisierung?“ In: *Chemie Ingenieur Technik* 75.5 (2003), S. 540–543.

[67] Mateja Kavčič und Dani Juričić. „CAD for fault tree–based diagnosis of industrial processes“. In: *Engineering Applications of Artificial Intelligence* 14.2 (2001), S. 203–216.

[68] Faisal I. Khan und S.A. Abbasi. „OptHAZOP — an effective and optimum approach for HAZOP study“. In: *Journal of Loss Prevention in the Process Industries* 10.3 (1997), S. 191–204.

[69] Faisal I. Khan und S.A. Abbasi. „TOPHAZOP: a knowledge-based software tool for conducting HAZOP in a rapid, efficient yet inexpensive manner“. In: *Journal of Loss Prevention in the Process Industries* 10.5-6 (1997), S. 333–343.

[70] Faisal I. Khan und S.A. Abbasi. „Towards automation of HAZOP with a new tool EXPERTOP“. In: *Environmental Modelling & Software* 15.1 (2000), S. 67–77.

[71] Trevor A Kletz. „Hazop—past and future“. In: *Reliability Engineering & System Safety* 55.3 (1997), S. 263–266.

[72] Norbert Kockmann. „Scale-up-fähiges Equipment für die Prozessentwicklung“. In: *Chemie Ingenieur Technik* 84.5 (2012), S. 646–659.

[73] Norbert Kockmann. „Sicherheitsaspekte bei der Prozessentwicklung und Kleinmengenproduktion mit Mikroreaktoren“. In: *Chemie Ingenieur Technik* 84.5 (2012), S. 715–726.

[74] Norbert Kockmann u. a. *Micro Process Engineering: Fundamentals, Devices, Fabrication, and Applications*. 1. Aufl. Wiley-VCH, 2014.

[75] Norbert Kockmann u. a. „Safety assessment in development and operation of modular continuous-flow processes“. In: *Reaction Chemistry & Engineering* (2017).

[76] Zdravko Kravanja und Miloš Bogataj, Hrsg. *26th European Symposium on Computer Aided Process Engineering*. Elsevier Science & Technology, 2016.

[77] Jörg Krekel und Gerd Siekmann. „Die Rolle des Experiments in der Verfahrensentwicklung“. In: *Chemie Ingenieur Technik* 57.6 (1985), S. 511–519.

[78] Juraj Labovský u. a. „Model-based HAZOP study of a real MTBE plant“. In: *Journal of Loss Prevention in the Process Industries* 20.3 (2007), S. 230–237.

[79] Jürgen Lang, Frank Stenger und Rüdiger Schütte. „Chemieanlagen der Zukunft - Unikate und/oder Module“. In: *Chemie Ingenieur Technik* (2012), S. 883–884.

[80] H. G. Lawley. „Operability studies and hazard analysis“. In: *Chemical Engineering Progress* 70 (1974), S. 45–56.

[81] Gang Li, S Joe Qin und Tao Yuan. „Data-driven root cause diagnosis of faults in process industries“. In: *Chemometrics and Intelligent Laboratory Systems* 159 (2016), S. 1–11.

[82] Hong Xian Li u. a. „Risk identification and assessment of modular construction utilizing fuzzy analytic hierarchy process (AHP) and simulation“. In: *Canadian Journal of Civil Engineering* 40.12 (2013), S. 1184–1195.

[83] Zhenglin Liang u. a. „On fault propagation in deterioration of multi-component systems“. In: *Reliability Engineering & System Safety* 162 (2017), S. 72–80.

[84] Stefan Lier, Dominik Wörsdörfer und Marcus Grünewald. „Transformable Production Concepts: Flexible, Mobile, Decentralized, Modular, Fast“. In: *ChemBioEng Reviews* 3.1 (2016), S. 16–25.

[85] Stefan Lier u. a. „Modulare Verfahrenstechnik: Apparateentwicklung für wandlungsfähige Produktionssysteme“. In: *Chemie Ingenieur Technik* 88.10 (2016), S. 1444–1454.

[86] Jan Limbers. *AKTUALISIERUNG: DIE DEUTSCHE CHEMISCHE INDUSTRIE 2030*. 2016.

[87] Ning Lü und Xiong Wang. „SDG-based hazop and fault diagnosis analysis to the inversion of synthetic ammonia“. In: *Tsinghua Science and Technology* 12.1 (2007), S. 30–37.

[88] Md Raihan Mallick und Syed A Imtiaz. „A Hybrid Method for Process Fault Detection and Diagnosis“. In: *IFAC Proceedings Volumes* 46.32 (2013), S. 827–832.

[89] P.K. Marhavilas, D. Koulouriotis und V. Gemeni. „Risk analysis and assessment methodologies in the work sites: On a review, classification and comparative study of the scientific literature of the period 2000–2009“. In: *Journal of Loss Prevention in the Process Industries* 24.5 (2011), S. 477–523.

[90] S.A. McCoy u. a. „HAZID, a computer aid for hazard identification: 1. The STOPHAZ Package and the HAZID Code: An Overview, the Issues and the Structure“. In: *Process Safety and Environmental Protection* 77.6 (1999), S. 317–327.

[91] SA McCoy u. a. „HAZID, a computer aid for hazard identification: 2. Unit model system“. In: *Process Safety and Environmental Protection* 77.6 (1999), S. 328–334.

[92] SA McCoy u. a. „HAZID, a computer aid for hazard identification: 3. The fluid model and consequence evaluation systems“. In: *Process Safety and Environmental Protection* 77.6 (1999), S. 335–353.

[93] SA McCoy u. a. „HAZID, a computer aid for hazard identification: 4. Learning set, main study system, output quality and validation trials“. In: *Process Safety and Environmental Protection* 78.2 (2000), S. 91–119.

[94] SA McCoy u. a. „HAZID, a computer aid for hazard identification: 5. future development topics and conclusions“. In: *Process safety and environmental protection* 78.2 (2000), S. 120–142.

[95] Peter Meier. „Risikomanagement in Großprojekten“. In: *Chemie Ingenieur Technik* 84.5 (2012), S. 727–729.

[96] Yew Seng Ng und Rajagopalan Srinivasan. „Multi–agent based collaborative fault detection and identification in chemical processes“. In: *Engineering Applications of Artificial Intelligence* 23.6 (2010), S. 934–949.

[97] Dennis P. Nolan. *Safety and Security Review for the Process Industries: Application of Hazop, Pha, What-If and Sva Reviews*. ELSEVIER LTD, 2014. 192 S.

[98] Michael Obst, Falk Doherr und Leon Urbas. „Wissensbasiertes Assistenzsystem für modulares Engineering“. In: *at - Automatisierungstechnik* 61.2 (2013), S. 103–108.

[99] Michael Obst u. a. „Automatisierung im Life Cycle modularer Anlagen“. In: *atp edition - Automatisierungstechnische Praxis* 55.01-02 (2013), S. 24.

[100] Michael Obst u. a. „Beschreibung von Prozessmodulen“. In: *atp edition - Automatisierungstechnische Praxis* 57.01-02 (2015), S. 48.

[101] Michael Obst u. a. „Semantic description of process modules“. In: *2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA)*. Institute of Electrical und Electronics Engineers (IEEE), 2015.

[102] Andrea Ohle u. a. „Modularisierung von Gaswäschern für die CO 2 -Entfernung aus Biogas“. In: *Chemie Ingenieur Technik* 86.5 (2014), S. 640–648.

[103] M. Oppelt, G. Wolf und L. Urbas. „Towards an integrated use of simulation within the life-cycle of a process plant“. In: *Proc. IEEE 20th Conf. Emerging Technologies Factory Automation (ETFA)*. 2015, S. 1–8.

[104] C. Palmer und P.W.H. Chung. „An automated system for batch hazard and operability studies“. In: *Reliability Engineering & System Safety* 94.6 (2009), S. 1095–1106.

[105] Nicola Paltrinieri und Faisal Khan. *Dynamic Risk Analysis in the Chemical and Petroleum Industry*. Elsevier Science & Technology, 2016. 284 S.

[106] Y. Papadopoulos u. a. „Analysis and synthesis of the behaviour of complex programmable electronic systems in conditions of failure“. In: *Reliability Engineering & System Safety* 71.3 (2001), S. 229–247.

[107] J.C. Parmar und F.P. Lees. „The propagation of faults in process plants: Hazard identification“. In: *Reliability Engineering* 17.4 (1987), S. 277–302.

[108] J.C. Parmar und F.P. Lees. „The propagation of faults in process plants: Hazard identification for a water separator system“. In: *Reliability Engineering* 17.4 (1987), S. 303–314.

[109] Hans J. Pasman und William J. Rogers. „How Can We Improve HAZOP, Our Old Work Horse, and Do More with Its Results? An Overview of Recent Developments“. In: *CHEMICAL ENGINEERING* 48 (2016).

[110] Judea Pearl. „Causal diagrams for empirical research“. In: *Biometrika* 82.4 (1995), S. 669.

[111] Judea Pearl. *Causality*. Cambridge University Pr., 2009. 484 S.

[112] JD Perkins. *Interactions between process design and process control*. Department of Chemical Engineering, Imperial College, 1992.

[113] Annett Pfeffer und Leon Urbas. „Architectures for integrating functional safety into modular process plants“. In: *IFAC-PapersOnLine* 48.21 (2015), S. 1321–1326.

[114] Shibly Rahman u. a. „ExpHAZOP+: Knowledge-based expert system to conduct automated HAZOP analysis“. In: *Journal of Loss Prevention in the Process Industries* 22.4 (2009), S. 373–380.

[115] Naveed Ramzan, Fred Compart und Werner Witt. „Methodology for the generation and evaluation of safety system alternatives based on extended Hazop“. In: *Process Safety Progress* 26.1 (2007), S. 35–42.

[116] S. Rath, Ü. Can und E. Leimer. „Quantitative Risikoanalyse (QRA) - Anwendungsbeispiele aus dem Großanlagenbau“. In: *Chemie Ingenieur Technik* 81.1-2 (2009), S. 53–62.

[117] Netta Liin Rossing u. a. „A functional HAZOP methodology“. In: *Computers & Chemical Engineering* 34.2 (2010), S. 244–253.

[118] Johannes Rottke u. a. „Efficient Engineering by Modularization into Package Units“. In: *Chemie Ingenieur Technik* 84.6 (2012), S. 885–891.

[119] J Savkovic-Stevanovic. „Reliability and safety analysis of the process plant“. In: *Petroleum & Coal* 52.2 (2010), S. 62–68.

[120] N. Schetinin u. a. „Why do verification approaches in automation rarely use HIL-test?“ In: *2013 IEEE International Conference on Industrial Technology (ICIT)*. Institute of Electrical und Electronics Engineers (IEEE), 2013, S. 1428–1433.

[121] Dierk Schröder. *Intelligente Verfahren: Identifikation und Regelung nichtlinearer Systeme*. Springer-Verlag, 2010.

[122] Tim Seifert u. a. „Small scale, modular and continuous: A new approach in plant design“. In: *Chemical Engineering and Processing: Process Intensification* 52 (2012), S. 140–150.

[123] Ina Sell, Denise Ott und Dana Kralisch. „Lebenszykluskostenanalyse zur Entscheidungsunterstützung in der chemischen Prozessentwicklung“. In: *Chemie Ingenieur Technik* 85.4 (2013), S. 447–454.

[124] Uwe Strauch. „Modulare Kostenschätzung in der chemischen Industrie - Konzept eines integrierten Systems zur Abschätzung und Bewertung des Kapitalbedarfes für die Errichtung einer chemischen Anlage“. Diss. Technische Universität Berlin, 2009.

[125] Aarne Sundberg. „Micro-scale Distillation and Microplants in Process Development“. Diss. Aalto University, 2014.

[126] *The CoPIRIDE Project*. 2010. URL: `http://www.copiride.eu/` (besucht am 23. 04. 2017).

[127] Nina F. Thornhill und Alexander Horch. „ADVANCES AND NEW DIRECTIONS IN PLANT-WIDE CONTROLLER PERFORMANCE ASSESSMENT“. In: *IFAC Proceedings Volumes* 39.2 (2006). 6th IFAC Symposium on Advanced Control of Chemical Processes, S. 29–36.

[128] Alessandro Tugnoli u. a. „Supporting the selection of process and plant design options by Inherent Safety KPIs“. In: *Journal of Loss Prevention in the Process Industries* 25.5 (2012), S. 830–842.

[129] Heinz Unbehauen. *Regelungstechnik III: Identifikation, Adaption, Optimierung*. 6. Aufl. Vieweg +Teubner Verlag, 2010.

[130] Leon Urbas u. a. „Automatisierung von Prozessmodulen“. In: *atp edition - Automatisierungstechnische Praxis* 54.01-02 (2012), S. 44.

[131] Leon Urbas u. a. „Modularisierung und Prozessführung“. In: *Chemie Ingenieur Technik* 84.5 (2012), S. 615–623.

[132] Hülya Uzuner. „Ein wissensbasiertes System zur Unterstützung von R&I-Fließbild Designprozessen auf der Grundlage eines modulbasierten Ansatzes“. Diss. Technische Universität Dortmund, 2012.

[133] Hülya Uzuner und Gerhard Schembecker. „Wissensbasierte Erstellung von R&I-Fließbildern“. In: *Chemie Ingenieur Technik* 84.5 (2012), S. 747–761.

[134] Ramesh Vaidhyanathan und Venkat Venkatasubramanian. „A semi-quantitative reasoning methodology for filtering and ranking HAZOP results in HAZOPExpert“. In: *Reliability Engineering & System Safety* 53.2 (1996), S. 185–203.

[135] Ramesh Vaidhyanathan und Venkat Venkatasubramanian. „Digraph-based models for automated HAZOP analysis“. In: *Reliability Engineering & System Safety* 50.1 (1995), S. 33–49.

[136] Ramesh Vaidhyanathan, Venkat Venkatasubramanian und Frederick T Dyke. „HAZOPExpert: An expert system for automating HAZOP analysis“. In: *Process Safety Progress* 15.2 (1996), S. 80–88.

[137] Andreas Varga. „New computational paradigms in solving fault detection and isolation problems“. In: *Annual Reviews in Control* 37.1 (2013), S. 25–42.

[138] Venkat Venkatasubramanian, Raghunathan Rengaswamy und Surya N. Kavuri. „A review of process fault detection and diagnosis: Part II: Qualitative models and search strategies“. In: *Computers & Chemical Engineering* 27.3 (2003), S. 313–326.

[139] Venkat Venkatasubramanian und Ramesh Vaidhyanathan. „A knowledge-based framework for automating HAZOP analysis“. In: *AIChE Journal* 40.3 (1994), S. 496–505.

[140] Venkat Venkatasubramanian, Jinsong Zhao und Shankar Viswanathan. „Intelligent systems for HAZOP analysis of complex process plants“. In: *Computers & Chemical Engineering* 24.9-10 (2000), S. 2291–2302.

[141] Venkat Venkatasubramanian u. a. „A review of process fault detection and diagnosis: Part I: Quantitative model-based methods“. In: *Computers & chemical engineering* 27.3 (2003), S. 293–311.

[142] Venkat Venkatasubramanian u. a. „A review of process fault detection and diagnosis: Part III: Process history based methods“. In: *Computers & chemical engineering* 27.3 (2003), S. 327–346.

[143] Valeria Villa u. a. „Towards dynamic risk analysis: A review of the risk assessment approach and its limitations in the chemical process industry“. In: *Safety Science* 89 (2016), S. 77–93.

[144] Olaf Wachsen u. a. „Anforderungen der zukunftsorientierten Spezialchemie an die angewandte Reaktionstechnik“. In: *Chemie Ingenieur Technik* 87.6 (2015), S. 683–693.

[145] Feng Wang, Jinji Gao und Huaqing Wang. „A new intelligent assistant system for HAZOP analysis of complex process plant“. In: *Journal of Loss Prevention in the Process Industries* 25.3 (2012), S. 636–642.

[146] Hangzhou Wang u. a. „Open source signed digraph inference framework“. In: *CIESC Journal* 61.7, 1829 (2010), S. 1829.

[147] Hangzhou Wang u. a. „SDG-based HAZOP analysis of operating mistakes for PVC process“. In: *Process Safety and Environmental Protection* 87.1 (2009), S. 40–46.

[148] Jing Wang u. a. „Fault isolation based on residual evaluation and contribution analysis“. In: *Journal of the Franklin Institute* (2016).

[149] Zhenheng Wang, Jinsong Zhao und Helen Shang. „A hybrid fault diagnosis strategy for chemical process startups“. In: *Journal of Process Control* 22.7 (2012), S. 1287–1297.

[150] Sachari Wassilew u. a. „Abbildung des NAMUR Module Type Package auf OPC UA“. In: *at - Automatisierungstechnik* 65.1 (2017), S. 49–59.

[151] S. Wassilew u. a. „Transformation of the NAMUR MTP to OPC UA to allow plug and produce for modular process automation“. In: *Proc. IEEE 21st Int. Conf. Emerging Technologies and Factory Automation (ETFA)*. 2016, S. 1–9.

[152] Klaus H. Weber. *Inbetriebnahme verfahrenstechnischer Anlagen*. Springer-Verlag GmbH, 2015.

[153] Fan Yang, Sirish L. Shah und Deyun Xiao. „SDG (Signed Directed Graph) Based Process Description and Fault Propagation Analysis for a Tailings Pumping Process“. In: *IFAC Proceedings Volumes* 43.9 (2010), S. 50–55.

[154] Fan Yang und Deyun Xiao. „Progress in root cause and fault propagation analysis of large–scale industrial processes“. In: *Journal of Control Science and Engineering* 2012 (2012).

[155] Ruey-Jen Yang u. a. „A comprehensive review of micro-distillation methods“. In: *Chemical Engineering Journal* 313 (2017), S. 1509–1520.

[156] S. Yin u. a. „A Review on Basic Data-Driven Approaches for Industrial Process Monitoring“. In: *IEEE Transactions on Industrial Electronics* 61.11 (2014), S. 6418–6428.

[157] Youmin Zhang und Jin Jiang. „Bibliographical review on reconfigurable fault-tolerant control systems“. In: *Annual Reviews in Control* 32.2 (2008), S. 229–252.

[158] Zhanpeng Zhang und Jinsong Zhao. „A deep belief network based fault diagnosis model for complex chemical processes“. In: *Computers & Chemical Engineering* (2017).

[159] C. Zhao, M. Bhushan und V. Venkatasubramanian. „PHASuite: An Automated HAZOP Analysis Tool for Chemical Processes Part I“. In: *Process Safety and Environmental Protection* 83.6 (2005), S. 509–532.

[160] C. Zhao, M. Bhushan und V. Venkatasubramanian. „PHASuite: An Automated HAZOP Analysis Tool for Chemical Processes Part II“. In: *Process Safety and Environmental Protection* 83.6 (2005), S. 533–548.

[161] Chongwen Zhou, Ratna Babu Chinnam und Alexander Korostelev. „Hazard rate models for early detection of reliability problems using information from warranty databases and upstream supply chain“. In: *International Journal of Production Economics* 139.1 (2012), S. 180–195.

Anhang

Anhang von Bildern

A

Anhang von Tabellen

B