Wissensbasierte Fehler- und Störfallanalyse bei der Entwicklung von verfahrenstechnischen Maschinen

Große, A.; Heimannsfeld, K.

Im Rahmen des Sonderforschungbereichs 180 "Konstruktion verfahrenstechnischer Maschinen bei besonderen mechanischen, thermischen oder chemischen Belastungen" ist das Teilprojekt A2 "Rechnerunterstützte Anforderungsermittlung und Funktionsanalyse verfahrenstechnischer Maschinen" im Bereich der übergreifenden Forschung angesiedelt. Das Projekt befaßt sich seit Beginn der Arbeiten mit der Unterstützung des interfakultativen Entwicklungsprozesses (Verfahrenstechnik, Maschinenbau, Chemie, Werkstoffwissenschaften). Der Artikel soll Probleme bei der Entwicklung verfahrenstechnischer Prozesse und ihrer Maschinen, mögliche Lösungswege und geplante Arbeiten aufzeigen.

Within the special research project 180 "Design of process engineering machinery with special reference to exceptional mechanical, thermal or chemical application of stress" the subproject A2 "Computer-Aided Requirement and Functional Analysis for Processing Machines" is engaged in general research. Since the beginning of the investigations this project works on supporting the development process involving several specialities: process engineering, mechanical engineering, chemistry and material science. This article describes problems in the development of processes and their machines and possible solutions as well as work in the planning.

1 Einführung

Eines der wesentlichen Ergebnisse aus den vergangenen Arbeiten dieses Projekts ist die Erkenntnis, daß in fortgeschrittenen Konstruktionsphasen (Dimensionierung und Gestaltung) bei vorliegenden, aus rein verfahrenstechnischen Überlegungen herrührenden konstruktiven Randbedingungen, der Gestaltungsprozeß durch rechnergestützte Methoden nach dem Prinzip der Konstruktionskataloge oder der Variation bekannter Lösungen unterstützt werden kann. Der entscheidende Nachteil dabei ist aber, daß eine solche Vorgehensweise die integrierte Entwicklung von Prozeß und Maschine verhindert und damit die Innovationsmöglichkeiten einschränkt. Insbesondere in den frühen Phasen der Entwicklungstätigkeit – d.h. von der Erstellung der Anforderungsstruktur bis hin zu dem, was in VDI 2221 im Bereich der verfahrenstechnischen Entwicklung "verfahrenstechnisches Fließbild", in der maschinenbaulichen Entwicklung "Konzept" genannt wird – kann dagegen eine Informationsbasis Potentiale zur Entwicklung neuer Prozesse und Maschinenanlagen freisetzen. Bei den Lösungsansätzen ist nicht daran gedacht, dem Verfahrenstechniker die Entwicklungsmethodik des Maschinenbauers "überzustülpen" (oder umgekehrt). Die unterschiedlichen Vorgehensweisen von Verfahrenstechnikern und Maschinenbauern können aber durch gemeinsame Methoden zur Beschreibung von Anforderungen, Funktionen, Ergebnisdarstellungen der jeweiligen Entwicklungsschritte, Produkt- und Prozeßdaten entscheidend angereichert werden.

2 Informationssystem zur rechnergestützten Anforderungsermittlung und Funktionsanalyse

Auf der Basis eines integrierten Produktmodells wurde ein Konstruktionsinformationssystem zur rechnergestützten Entwicklung verfahrenstechnischer Maschinen erstellt. Mit der prototypischen Implementierung eines rechnergestützten Werkzeugs zur Anforderungsermittlung und Funktionsanalyse wurde die Realisierbarkeit und Verwendbarkeit des spezifizierten Produktmodells gezeigt. Es wurden Wege dargelegt, die Anforderungs- und Funktionsanalyse durch Verfahrenstechniker und Maschinenbauer auf eine einheitliche Sicht abzubilden und zu formalisieren.

Begleitend wurde ein Modell des Entwicklungsvorgangs erstellt, das – unter Verwendung der in VDI 2221 getroffenen Definitionen für die Einzelschritte – eine Beschreibung des aktuellen Zustands der Entwicklung liefert und so die Anwendung fachspezifischer Vorgehensweisen einer schrittweisen Weiterentwicklung ermöglicht.

2.1 Modell zur Beschreibung des Konstruktionsprozesses

Für eine umfassende Unterstützung des Konstrukteurs müssen ihm die Produktdaten in geeigneter Form zugänglich gemacht werden. Dazu werden Modelle zur Beschreibung des Konstruktionsprozesses und der Konstruktionsergebnisse genutzt. Die Integration dieser Modelle ermöglicht es, die Eingangs- und Ausgangsgrößen der Konstruktionsschritte zu beschreiben und zu klassifizieren. Weiterhin definiert ein Konstruktionsraum mit seinen Dimensionen die Grundfunktionen der Konstruktionsaktivitäten. Dadurch werden ebenfalls die einzelnen Aktivitäten beschrieben. Das Modell des Konstruktionsraums stellt somit eine Verbindung zwischen der Gedanken- und Handlungswelt des Konstrukteurs und den Daten- und Informationsmodellen dar, **Bild 1**.

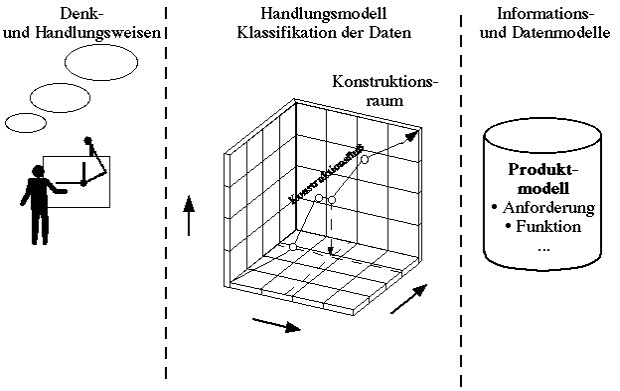

Bild 1: Der Konstruktionsraum als Schnittstelle

Die Integration des Konstruktionsraumes in einen rechnerunterstützten Konstruktionsarbeitsplatz dient folgenden Zielen:

- Orientierung im Konstruktionsprozeß ("Wo befinde ich mich? Welche Möglichkeiten habe ich?"),
- detaillierte Dokumentation und Bereitstellung von Konstruktionsabläufen,
- Integration von Auslegungs- und Auswahlmethoden in Abhängigkeit vom Zustand des Konstruktionsobjektes.

2.2 Systemkonzept

Für die Realisierung eines rechnergestützten Konstruktionsinformationssystems, das das Modell des Konstruktionsraumes nutzt, wird ein modulares System vorgeschlagen, **Bild 2**. Bei den einzelnen Modulen handelt es sich um:

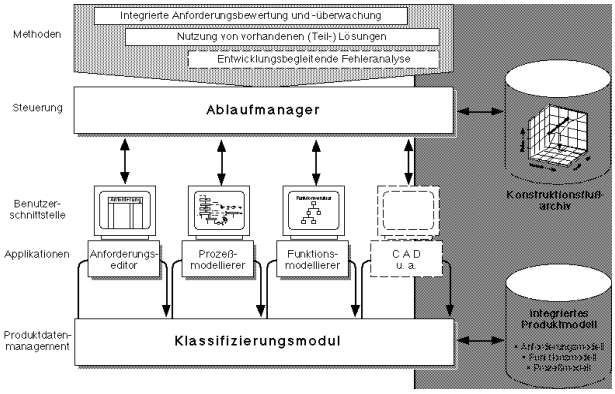

Bild 2: Systemkonzept

- Klassifizierungsmodul,
- Konstruktionsflußarchiv,
- Ablaufmanager,
- integriertes Produktmodell mit relevanten Partialmodellen.

Das Klassifizierungsmodul erfaßt die ein- und ausgehenden Informationen und ordnet sie einer Koordinate des Konstruktionsraumes zu. Die Klassifizierung erfolgt entsprechend der Definition der Dimensionen des Konstruktionsraumes. Dies kann sowohl interaktiv durch Befragen des Benutzers als auch automatisch erfolgen. Für eine automatische Klassifizierung der Daten ist ihre Semantik eindeutig festzulegen.

Das Konstruktionsflußarchiv dokumentiert und verwaltet die Klassifizierung der einzelnen Ein- und Ausgangsgrößen der Konstruktionsschritte. Zusätzlich stellt es die Verbindung zu den Instanzen, die im Produktmodell abgelegt sind, her. Auf diese Weise kann der gesamte Konstruktionsprozeß einschließlich des jeweiligen Standes der Produktdefinition weiteren Betrachtungen zugänglich gemacht werden.

Der Ablaufmanager steuert die Funktionen und Applikationen, die dem Konstrukteur angeboten werden. Dies geschieht in Abhängigkeit vom Zustand des Konstruktionsobjektes, d.h. seiner Lage im Konstruktionsraum. Entsprechend den Dimensionen des Konstruktionsraumes und den zwei unterschiedlichen Bewegungsrichtungen ergeben sich verschiedene Klassen von Konstruktionsschritten. Aufgabe des Ablaufmanagers ist die Auswahl und Zusammenstellung der jeweils detaillierten Systemfunktionen der beteiligten Subsysteme und Applikationen. Bei

diesen Klassen von Konstruktionsschritten handelt es sich um:

- Konkretisieren / Abstrahieren,
- Spezialisieren / Generalisieren
- Dekomponieren / Zusammensetzen
- Variieren

Diese Oberklassen werden durch die Unterteilung der Dimensionen noch weiter detailliert. Zusätzlich kann der Ablaufmanager anwendungs- oder unternehmensspezifische Abläufe vorgeben und diese auch um organisatorische Gesichtspunkte ergänzen. So kann er bestimmte Zustände des Konstruktionsobjektes als Fixpunkte festlegen. Die Vorgabe dieser Fixpunkte entspricht einer Konstruktionsablaufplanung, sie umfaßt Freigabeprozeduren und kann um Termin- und Kapazitätsaspekte ergänzt werden.

Weiterhin dient der Ablaufmanager zur Integration von rechnergestützten Methoden für einzelne Konstruktionsschritte. So werden beim Übergang von den funktionalen Anforderungen zur Festlegung der Gestalt eines Bauteiles Methoden der Bauteildimensionierung bereitgestellt. Zu derartigen Methoden gehört ebenfalls die später in diesem Artikel vorgestellte Systematik zur konstruktionsbegleitenden Fehleranalyse. Im folgenden soll der bereits realisierte Anforderungseditor bzw. -modellierer (vgl. **Bild 2**) vorgestellt werden.

2.3 Der Anforderungsmodellierer

Für die Realisierung eines Werkzeuges zur Erfassung und Analyse von Anforderungen wurde das in **Bild 3** dargestellte Systemkonzept gewählt. Basis der Entwicklung des Anforderungswerkzeugs ***demanda*** ist ECCO Toolkit zum Rapid Prototyping von Informationsmodellen nach ISO 10303-11 (EXPRESS). Ausgehend von dem in der Datenmodellierungssprache EXPRESS formulierten Produktmodell wird mit Hilfe eines EXPRESS-Compilers ein RUNTIME-System generiert. Das RUNTIME-System enthält die Grundfunktionalitäten zum Zugriff auf die einzelnen Teile des Produktmodells und Funktionen zum Datenaustausch nach ISO 10303-21 (STEP Physical Files). Die Kommunikationsschicht und die EXPRESS-Abstraktionsschicht bilden den modellunabhängigen Teil der Zugriffsfunktionen auf das Produktmodell. Alle Softwaremodule zur Realisierung von ***demanda*** wurden in der Programmiersprache Tcl/Tk und der objektorientierten Erweiterung [incr Tcl] implementiert. Tcl/Tk ist eine Programmiersprache die insbesondere zum schnellen Entwickeln von graphischen Benutzerschnittstellen entworfen wurde und schnell und leicht erlernbar ist.

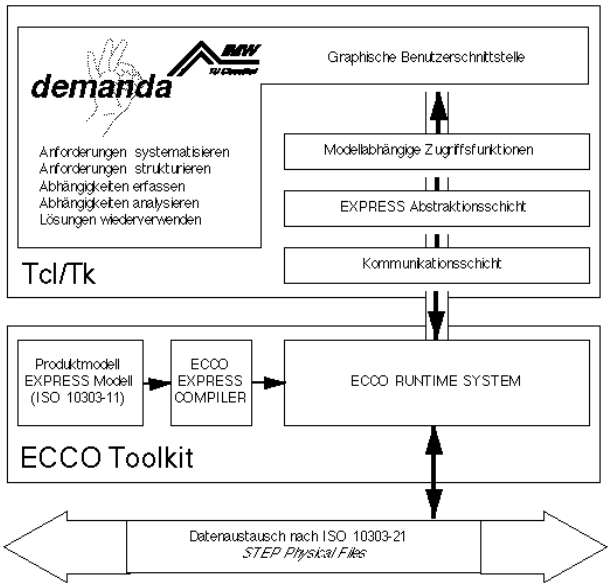

Bild 3: Systemarchitektur des Anforderungswerkzeugs ***demanda***

Bild 4 zeigt die graphische Benutzeroberfläche des Anforderungsmodellierers. ***demanda*** gliedert sich in die drei Teilbereiche Anforderungen, Produktkategorien und Eigenschaften. Anforderungen werden immer einer Produktkategorie oder einem Produkt zugeordnet. Eigenschaften und deren Darstellungselemente sind die formalisierte Beschreibung von Anforderungen, die zur Analyse und späteren Bewertung von Lösungen eingesetzt werden.

Neben den eigentlichen Anforderungen wird durch Strukturierung auch weitergehendes Konstruktionswissen erfaßt und der rechnergestützten Auswertung und Wiederverwendung zugänglich gemacht. Ausgehend von den definierten Anforderungen kann der Produkt- oder Verfahrensentwickler auf bestehende Lösungen aus anderen Konstruktionsphasen zurückgreifen.

Aus Benutzersicht bieten sich dem Produktentwickler mehrere Vorgehensmöglichkeiten, die dem kreativen Vorgang des Konstruierens Rechnung tragen. Zur Systematisierung der Anforderungserfassung bietet ***demanda*** vordefinierte Anforderungskataloge, die der Produktentwickler als Schablonen benutzen

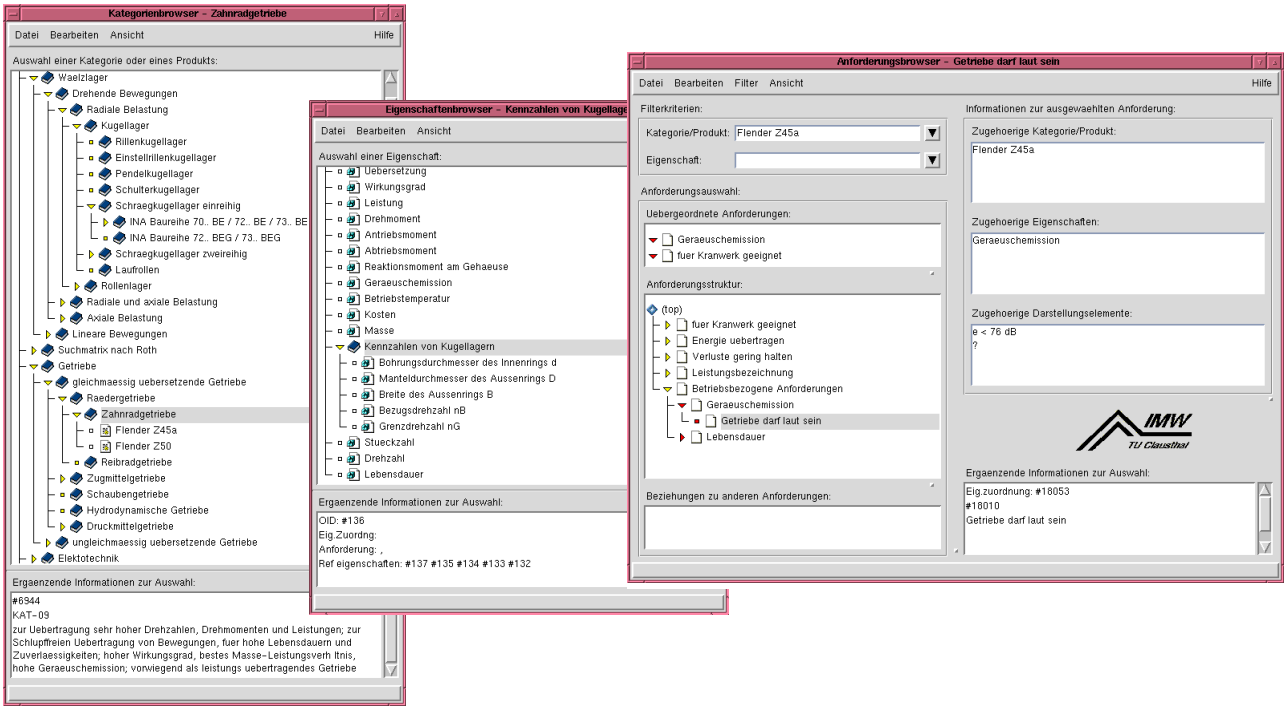

Bild 4: Graphische Benutzerschnittstelle des Anforderungswerkzeuges ***demanda***

kann. Neben der eigentlichen Strukturierung der Anforderungen, können auch Beziehungen zwischen Anforderungen modelliert werden. Hierdurch kann der Produktentwickler rechtzeitig auf konkurrierende oder sich im schlimmsten Fall sogar ausschließende Anforderungen aufmerksam werden.

Zusammenfassend bietet ***demanda*** dem Produktentwickler die folgenden Möglichkeiten:

- Wiederverwendung von Konstruktionswissen aus ähnlichen Produkten
- Systematisierung der Anforderungserfassung durch Anforderungskataloge
- Teilautomatisierte Erfassung und Analyse von Beziehungen zwischen Anforderungen
- Konsistenzprüfung der Anforderungen ähnlicher Produkte

3 Geplante Arbeiten

Im Verlauf der bisherigen Arbeiten wurde auch erkannt, daß bei der Entwicklung verfahrenstechnischer Maschinen insbesondere die in den Phasen der Fertigung, der Inbetriebnahme und des Betriebes gewonnenen Erfahrungen selten in die bereits erfaßten Anforderungen und Teillösungen der neuen Produkte zurückfließen. Die Erfahrungen aus dem Lebenszyklus der verfahrenstechnischen Maschine oder des erzeugten Produkts stehen somit bei der nächsten Neukonstruktion oder Variantenkonstruktion nicht mehr zur Verfügung. Auch die während der Neukonstruktion von verfahrenstechnischen Maschinen gemachten negativen Erfahrungen stehen am Projektende selten vollständig zur Verfügung, obwohl sie wichtiger sein können als die konkrete Lösung.

Im Mittelpunkt der weiterführenden Arbeiten soll daher die Entwicklung von Methoden zur Unterstützung des Konstrukteurs bei der Fehler- und Störfallanalyse in den frühen Phasen der Konstruktion verfahrenstechnischer Maschinen stehen. Dazu ist die Erfassung, Analyse und Rückführung von Fehlerinformationen aus allen späteren Phasen in einem Produktleben in die Entwicklung erforderlich.

3.1 Rechnergestützte Fehler- und Störfallanalyse

Es ist vorgesehen auf Basis von Fehlerinformationen ein System zur Fehleranalyse in den bestehenden Konstruktionsarbeitsplatz zu integrieren. Die Fehlerinformation kann dabei realen oder virtuellen Charakter haben. Als reale Fehlerinformation werden Informationen über Fehler bezeichnet, die in späteren Produktlebensphasen "real" aufgetreten sind. Virtuelle Fehlerinformationen sind hingegen Fehler, die sich der Verfahrensentwickler, der Konstrukteur oder ein

Projektteam vorstellt, um so präventiv Fehlerquellen zu erkennen, ihre Auswirkungen zu beurteilen und die Ursachen zu vermeiden.

Bild 5 zeigt das grundsätzliche Vorgehen bei der wissensbasierten Fehler- und Störfallanalyse. Zum Auffüllen der Wissensbasis stehen am Anfang zwei Möglichkeiten zur Verfügung. Einerseits fließt durch die Fehler- und Störfallanalyse disziplininternes Fehlerwissen in die gemeinsame Wissensbasis. Das gespeicherte Fehlerwissen steht von diesem Zeitpunkt an auch den anderen Teildisziplinen oder Abteilungen zur Verfügung. Andererseits wird die Fehlerinformation aus den späten Phasen des Produktlebenszyklusses erfaßt, den Ursachen zugeordnet und in die Wissensbasis eingebracht. Ziel des Systems ist es, mit steigendem Wissen die Regelkreise zwischen der Verfahrensentwicklung, Konstruktion und den späten Phasen des Produktlebenszyklusses zu verkürzen und somit zu kürzeren Entwicklungszeiten und einer qualitativ besseren, kostengünstigeren verfahrenstechnischen Maschine oder Anlage für einen stabilen und sicheren Prozeß zu kommen.

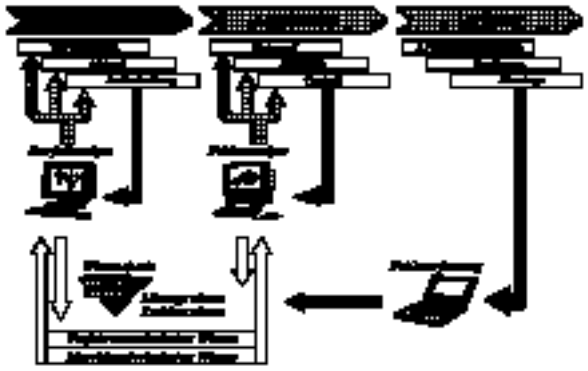

Bild 5: Wissensbasierte Fehler- und Störfallanalyse

Innerhalb des Projekts sollen daher vorrangig drei Ziele verfolgt werden:

a) Konzept zur Integration der maschinentechnischen Fehleranalyse in die verfahrenstechnische Störfallanalyse

Zur Umsetzung einer disziplinübergreifenden Fehleranalyse auf Basis von Erfahrungswissen ist es zunächst nötig, die Auswirkung von maschinentechnisch bedingten Fehlern auf den Prozeß einer verfahrenstechnischen Maschine oder Anlage zu untersuchen, zu systematisieren und zu beschreiben. Dazu ist das entwickelte integrierte Produktmodell so zu erweitern, daß die in verfahrenstechnischen Maschinen ablaufenden Prozesse in einem funktionalen Zusammenhang mit den Parametern der maschinentechnischen Realisierung beschrieben werden können.

Dieses Modell stellt später die Grundlage für die Rückkopplung von Erfahrungen zwischen dem Maschinenbau und der Verfahrenstechnik dar. Dabei muß das Modell flexibel und erweiterbar angelegt werden, um den Entwicklungen in der Forschung und in der Neuentwicklung verfahrenstechnischer Maschinen Rechnung zu tragen. Gleichzeitig muß das Modell eine verständliche Repräsentation der enthaltenen Informationen erlauben, um so dem Verfahrensentwickler und dem Konstrukteur Expertenwissen der jeweils anderen Disziplin verständlich in einer aufgaben- und situationsgerechten Darstellung zugänglich zu machen.

b) Erfassung und Wiederverwendung von Erfahrungswissen aus späten Phasen des Produktlebenszyklusses

Durch präventive Fehleranalyse sollen Fehler erkannt und beseitigt werden, bevor sie zu höheren Kosten und negativen Auswirkungen auf die Produktqualität führen. In der Praxis und insbesondere im Umfeld der Forschung und Neuentwicklung lassen sich allerdings oftmals die Parameter einer Entwicklung nur schwer vorhersehen. Im Gegensatz zu den häufig in der Industrie angewandten Variantenkonstruktion, deren Entwicklung "überschaubarer" ist, werden hier viele Erfahrungen erstmals gesammelt. Daher muß die Integration von Fehlerwissen in einer möglichst aufgegliederten Darstellung erfolgen und die damit zu erreichende Übertragbarkeit und Wiederverwendbarkeit einen Schwerpunkt in der Untersuchung und Entwicklung eines disziplinübergreifenden Fehleranalysewerkzeuges für Verfahrensentwickler und Konstrukteur darstellen. Dies erfordert zunächst eine Klassifizierung und Rückführung von Fehlern, Ausfällen und Ursachen und ihre Darstellung in dem Produktmodell.

Ein besonderer Schwerpunkt muß auch hier auf die sichtengerechte Darstellung des Wissens gelegt werden, denn nur so kann garantiert werden, daß der Verfahrensentwickler oder Konstrukteur

die Chance hat die Zusammenhänge zwischen seinen Aktivitäten und den Auswirkungen in späteren Produktlebensphasen zu erfassen, um seine Handlungen und Ideen anzupassen und zu korrigieren.

c) Integration von verfahrens- und maschinentechnischem Erfahrungswissen in die präventive Fehleranalyse

Nach der Erfassung des disziplinübergreifenden Erfahrungswissens kann dieses Wissen benutzt werden um den Konstrukteur bei der Generierung und Verfolgung einer Fehleridee zu unterstützen. Dies erfordert aber eine durchgängige und konsistente Formalisierbarkeit, die oftmals nicht oder nur sehr schwer realisierbar ist. Ein Schwerpunkt bei der Integration des disziplinübergreifenden Wissens muß folglich in der Untersuchung der Modellierbarkeit von unscharfem und unsicherem Wissen liegen. Neben der Untersuchung zur rechnergerechten Abbildung des unsicheren Wissens müssen auch die Mechanismen zur Bereitstellung in der Benutzerschnittstelle untersucht werden, denn nur wenn die Kommunikation des Benutzers mit dem Konstruktionsinformationssystem und der implementierten Datenaufbereitung harmonisiert, kann die angebotene optimale Information genutzt werden.

3.2 Methoden der Fehler- und Störfallanalyse

Zuverlässigkeit und *Sicherheit* sind zwei wesentliche Qualitätsmerkmale einer verfahrenstechnischen Maschine oder Anlage. Dabei hängen beide eng zusammen und bedingen sich gegenseitig. Die Abgrenzung von Zuverlässigkeit und Sicherheit kann durch die beiden Begriffe *Versagen* und *Unfall* erfolgen /1/. Ein Versagen eines unzuverlässigen Maschinenteils kann, soweit die ausgefallene Funktion sicherheitsrelevant ist, zu einem Unfall führen, muß allerdings nicht Voraussetzung für einen Unfall sein. Eine andere qualitative Definition von Sicherheit findet man in /2/: "*Safety is the freedom from those conditions that can cause death, injury, or occupational illness; damage to the enviroment; or damage to or loss of equipment or property* ".

Nach /3/ können Methoden zur Fehler-, Unfall- und Störfallanalyse in drei Klassen unterteilt werden. Diese Klassifizierung wird auf Grund der Art von Beziehung zwischen den Ursachen und Konsequenzen vollzogen, die von den Methoden während der Analysephase untersucht werden. Man unterscheidet:

- Eine-zu-Viele Methoden
- Viele-zu-Einer Methoden
- Viele-zu-Viele Methoden

Beispiele für die Klasse der Eine-zu-Viele Methoden sind die FMEA (Failure Mode and Effects Analysis), die FMCEA (Failure Mode, Effects and Criticality Analysis, die AEA (Action Error Analysis) und die ETA (Event Tree Analysis). Alle diese Ansätze gehen von einem einzelnen Ereignis aus und versuchen systematisch die möglichen Folgen durchzuspielen und zu untersuchen. Andere Autoren beschreiben diese Vorgehensweise als vorwärtsgerichtete Analyse oder induktive Methoden /4/.

Bei diesen Methoden wird das zu untersuchende System in eine Anzahl von Elementen (z.B. Bauteile, Unterfunktionen) zerlegt. Danach werden für diese Elemente mögliche Abweichungen von Sollwerten vorgegeben und durch das Gesamtsystem propagandiert und in Bezug auf die sicherheitsrelevanten Aspekte bewertet. Eine ausführlichere Beschreibung der einzelnen Methoden findet sich in /5-7/.

Die Viele-zu-Eine Methoden versuchen für eine Folge die möglichen Gründe zu ermitteln. Deswegen spricht man auch oftmals von rückwärtsgerichteten oder deduktiven Analysemethoden. Die FTA (Fault Tree Analysis) ist ein typischer Vertreter der deduktiven Fehleranalyseverfahren. Die FTA beginnt bei einem vorgegebenen Startereignis und verfolgt in zeitlich inverser Folge die Ereignisse, die als Ursachen für das Startereignis in Frage kommen. Die Auswahl eines geeigneten Startereignisses ist ein oftmals kritischer Faktor bei der FTA und wird häufig durch eine weniger detaillierte Methode der Fehleranalyse oder durch Erfahrungswissen bestimmt. Die Durchführung der FTA kann auf Grund einer formalisierten Beschreibung von Fehlerbäumen automatisiert werden. Weitere Informationen zu der FTA und Fehlerbäumen finden sich z.B. in /8, 9/.

Viele-zu-Viele Methoden sind oftmals Mischformen aus den beiden vorhergehend beschriebenen Klassen. Wählt man ein Zwischenereignis einer Unfallsequenz als Startereignis einer FTA und als Auslöseereignis einer ETA, so erhält man eine bidirektionale

Methode, die als CCA (Cause-Consequence Analysis) bezeichnet wird. Oftmals werden auch die induktiven Methoden der FMEA und FMECA durch eine deduktive Suche nach Versagensursachen bidirektional angewendet. Eine ausführliche Beschreibung der CCA findet sich in /10/.

Ein weitere Unterklasse der Viele-zu-Viele Methoden wird in /4/ als *morphologische Analyse* bezeichnet und konzentriert sich von Anfang an auf potentielle Gefahrenstellen eines Systems. Die Analyse beginnt meistens mit der Suche nach Startereignissen die oftmals mit Energieschwerpunkten, gefährlichen Stoffen oder potentiellen Zielen wie Menschen und gefährdeten Gegenständen zusammenhängen. Diese wird in der Regel durch die Anwendung einer Menge von Leitworten bewerkstelligt. Für jedes dieser Leitworte wird nun in einer bidirektionalen Vorgehensweise auf die Konsequenzen und die Ursachen hin untersucht. Beispiele dieser morphologischen Analysen sind z.B. die in der chemischen Industrie weitverbreitete PAAG (engl. HAZOP - Hazard and Operability Study), MORT (Management Oversight and Risk Tree), OHA (Operating Hazard Analysis, PHA (Preliminary Hazard Analysis). Eine ausführliche Beschreibung dieser Methoden findet man in /4, 7, 9-11/.

4 Ausblick

Aus der Rückführung von Erfahrungswissen mit Methoden der Fehler- und Störfallanalyse leiten sich folgende Arbeitsschritte ab:

Konstruktive Begleitung anderer Teilprojekte

Zur Überprüfung und Weiterentwicklung der vorgeschlagenen Methodik zur wissensbasierten Fehleranalyse wird aktiv in anderen Teilprojekten des Sonderforschungsbereichs mitgearbeitet. Die durch die Mitarbeit gewonnenen Erfahrungen der Teilprojekte können direkt genutzt werden um die Methoden und Modelle zu validieren. Auf Basis der realen Erfahrungswerte soll eine Optimierung der Fehleranalysemethoden und Modelle vollzogen werden. Andererseits sollen die Daten genutzt werden, um präventive Fehleranalysen in den Teilprojekten durchzuführen und somit neben einer aktiven Erprobung auch einen eigenen Beitrag in den Teilprojekten zu leisten. Durch den Aufbau eines derartigen Regelkreises "Erfahrungen sammeln - Anwendung - Überprüfung - Optimierung" ist ein effizienter Abgleich zwischen Theorie und Praxis zu erwarten. Außerdem sind Rückschlüsse auf organisatorische Aspekte in der Anwendung der Methodik möglich. Ergebnis ist die kritische Überprüfung der Methodik und des Modells anhand realer Daten. Dazu soll der bestehende Prototyp um ein Fehlererfassungsmodul erweitert werden.

Aufbereitung und Evaluierung von Ansätzen zur präventiven Fehleranalyse

Zu Beginn der Arbeiten ist eine intensive Untersuchung der verschiedenen Methoden der präventiven Fehleranalyse notwendig. Dazu ist es erforderlich, die Ansätze in Bezug auf die Anwendbarkeit in dem interdisziplinären Umfeld der Entwicklung verfahrenstechnischer Maschinen hin zu untersuchen. Ein weiterer Aspekt wird die Formalisierbarkeit und damit verbunden die Automatisierbarkeit der Ansätze sein. Neben dem Vergleich und der Bewertung der bereits existierenden Ansätze zur Fehleranalyse soll ein Vorgehensmodell ausgearbeitet werden, daß hinreichend formalisierbar ist, gleichzeitig aber flexibel genug, um vom Anwender akzeptiert zu werden.

Modellbildung zur Beschreibung der Ursache/ Folge-Beziehung

Basierend auf dem zu entwickelnden Vorgehensmodell muß eine Datenmodellierung der Fehlerinformation erfolgen. Dazu soll ein Modell zur Repräsentation der Ursache/Folge-Beziehung entwickelt werden. Dieses Modell ist der Eingangsparameter zur manuellen Erfassung von Fehlern in den späteren Phasen des Produktlebenszyklusses und wird zur Modellierung des Fehlerzustandes (Fehleridee) in der präventiven Fehleranalyse benötigt. Ein Schwerpunkt in der Modellierung liegt dabei auf der Berücksichtigung der speziellen Anforderungen an die Schnittstelle zwischen verfahrenstechnischer Störfallanalyse und der maschinentechnischen Fehleranalyse.

Integration der Ursache/Folge-Beziehung in das Referenzmodell

Das zu entwickelnde Modell soll nicht als Partialmodell abgebildet werden, sondern in das bestehende Referenzmodell integriert werden. Dazu muß das bestehende Referenzmodell um die Konstrukte zur Abbildung der Ursache/Folge-Beziehung und der dazu inversen Beziehung in allen möglichen Produktzuständen erweitert werden.

Aufbereitung von Methoden der künstlichen Intelligenz

Die Anwendung von Methoden der künstlichen Intelligenz für die Fehler- und Störfallanalyse soll zwei Ziele erfüllen: Einerseits soll der Konstrukteur im Auffinden von für ihn relevantem Wissen unterstützt werden und andererseits soll versucht werden, aus den vorliegenden Erfahrungen Schlüsse zu ziehen, die den Konstrukteur bei seinen Entwurfsentscheidungen unterstützen. Dazu sollen besonders hybride Methoden (z.B. Explanation Based Learning der künstlichen Intelligenz, die die Vorteile verschiedener Formen des Lernens verbinden) hinsichtlich der Anwendbarkeit untersucht werden.

5 Zusammenfassung

Im Mittelpunkt des Projektes steht die Unterstützung des interdisziplinären Entwicklungsprozesses von verfahrenstechnischen Maschinen und Anlagen im Sinne des Concurrent Engineering. Basierend auf dem beschriebenen Modell des Konstruktionsraumes wurde ein rechnergestütztes Konstruktionsinformationssystem entwickelt und umgesetzt. Des weiteren wurde die Realisierung des Anforderungsmodellierers vorgestellt.

Mit dem Ziel einer präventiven Fehlervermeidung werden in den geplanten Arbeiten Methoden zur Fehler- und Störfallanalyse in das bestehende Gesamtkonzept (Produktmodell, Systemkonzept) eingebunden. Durch das in frühen Phasen des Entwicklungsprozesses bereitgestellte Erfahrungswissen kann der Konstrukteur die Produktqualität aufgrund kürzerer Regelkreise verbessern und die Sicherheit der verfahrenstechnischen Maschinen und Anlagen erhöhen.

Literatur

/1/ Shen, K.-C.: On the exploratory study of reliability and safety engineering techniques and their implementation in the machine design process. Lund, LUTMDN /(TMKT-1001) (1986)

/2/ Toola, A.: Safety Analysis in the conceptual design of process control. Espoo, Technical Research Center of Finland, VTT Publications 117 (1992)

/3/ Hollnagel, E.; Cacciabue, C.: Reliability assement of interactive systems with system response generator. In Safety and Reliability ´92, London P 140-150 (1992)

/4/ Suokas, J.: On the reliability and validity of safety analysis. Espoo, Technical Research Center of Finland, VTT Publications 25 (1985)

/5/ ESA: Requirements for failure modes, effects and criticality analysis, and associated activities, on ESA space systems. PSS-01-303, Issue 1 Draft 7, Noordwijk, ESA-ESTEC Safety Section (1988)

/6/ Guidelines for hazard evaluation procedure . Second Edition with Worked Examples, New York, American Institute of Chemical Engineers (1992)

/7/ Reunanen, M.; Suokas, J.: Saftey analysis of a black liquor recovery boiler plant. Espoo, Technical Research Center, Finland, VTT Research Notes 551(1986)

/8/ Hammer, W.: Product safety management and engineering. Englewoods Cliff, N.J., Prentice-Hall, Inc. (1980)

/9/ Roland H.E.; Moriarty B.: System safety engineering and management. New York, John Wiley & Sons (1983)

/10/ Daling, P.M.; Geffen, C.A.: Evaluation of safety assessment methods for the mining industry. Vol. I, Washington, DC, Bureau of Mines, BuMines OFR195(1)-83 (1983)

/11/ ESA: Hazard Analysis and Safety Risk Assessement, Methods and Procedures. ESA PSS-01-403 Issue 1 (Jan 1994)