Entwicklung eines Informationssystems für präventive Sicherheitsanalysen an Maschinen und Anlagen

Beisheim, N.

Die Entwicklung neuer Maschinen und Anlagen basiert größtenteils auf dem Erfahrungswissen von bereits realisierten Konstruktionen. Um die dabei gemachten Erfahrungen bei der Neukonstruktion verwendet zu können, müssen diese in geeigneter Form strukturiert, gespeichert und aufbereitet werden. Der Artikel beschreibt ein System zur Verknüpfung der Informationen aus dem Entwicklungsprozess, der Sicherheitsanalyse und der Simulation von verfahrenstechnischen Anlagen. Mit diesem Informationssystem können präventive begleitende Sicherheitsanalysen während der Entwicklung neuer Anlagen durchgeführt werden.

The engineering process of new machines and systems is mainly the result of experiences from constructions, which have been made some time before. The experiences and their data have to be managed and saved in a useful structure to get the needed information at the right time. This paper shows a knowledge based system to deal with information from the engineering process, the hazard analysis and the simulation of process machinery. With this knowledge based system it is possible to make preventive hazard analysis in the engineering process of new plants.

1 Einleitung

Die Komplexität der zu entwickelnden Systeme, Komponenten und Anlagen hat in der Vergangenheit stetig zugenommen und wird auch in der Zukunft weiter ansteigen. Die Ingenieure und Techniker greifen deshalb bei der Entwicklung neuer Systeme weitgehend auf ihr Erfahrungswissen zurück. Dieses Erfahrungswissen soll aber nicht nur die Informationen zum Zeitpunkt der Planung und Entwicklung beinhalten sondern alle Phasen des Produktlebenszykluses umfassen, also auch Fertigung, Montage, Betrieb etc. Während aller Lebensphasen fallen große Mengen an Informationen an, die für neue Konstruktionen von Interesse sein können.

Die Aufgabe besteht nun darin, diese Informationen so zu strukturieren, zu speichern und aufzubereiten, dass sie bei der Neukonstruktion effizient wiederverwendet werden können.

2 Konzept

Das in dem Teilprojekt A2 des SFB 180 entwickelte Konzept der "**Wi**ssensbasierten **Si**cherheitsanalyse (WISI)" hat zum Ziel, die Schwachpunkte der im Rahmen des Projekts untersuchten Sicherheitsanalysen im Bereich Verfahrenstechnik und Maschinenbau zu verringern und die Vorteile der Methoden in einem Informationssystem zusammenzufassen. Dieses Informationssystem soll letztendlich alle Produktlebensphasen von der Entwicklung, Fertigung, Montage, Betrieb, Wartung bis zum Recycling eines Entwicklungsobjekts begleiten. Die dabei entstehenden Informationen sollen den in den Entwicklungsprozess integrierten sicherheitstechnischen Analysen übergeben werden, um deren Ergebnisse in den nachfolgenden Phasen zu berücksichtigen, wie in **Bild 1** dargestellt.

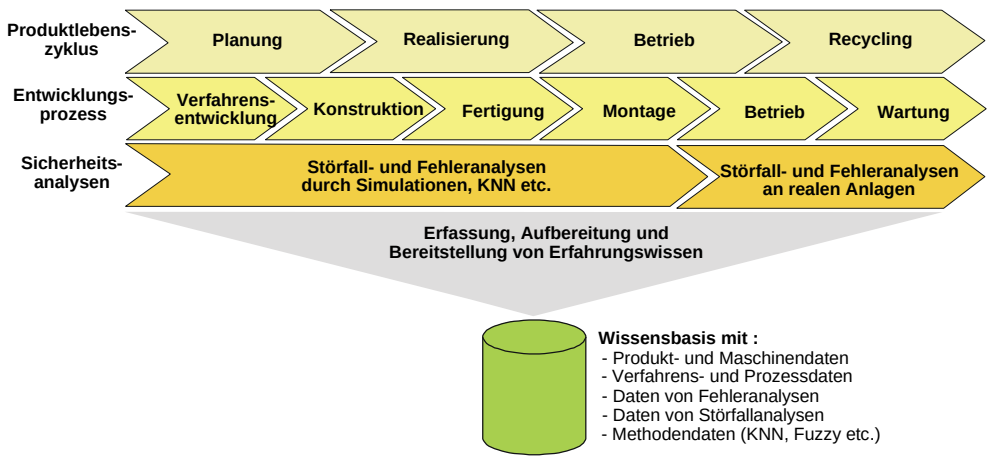

Bild 1: Daten- und Informationsfluss zur Wissensbasis während der Produktlebensphasen einer verfahrenstechnischen Anlage oder Maschine

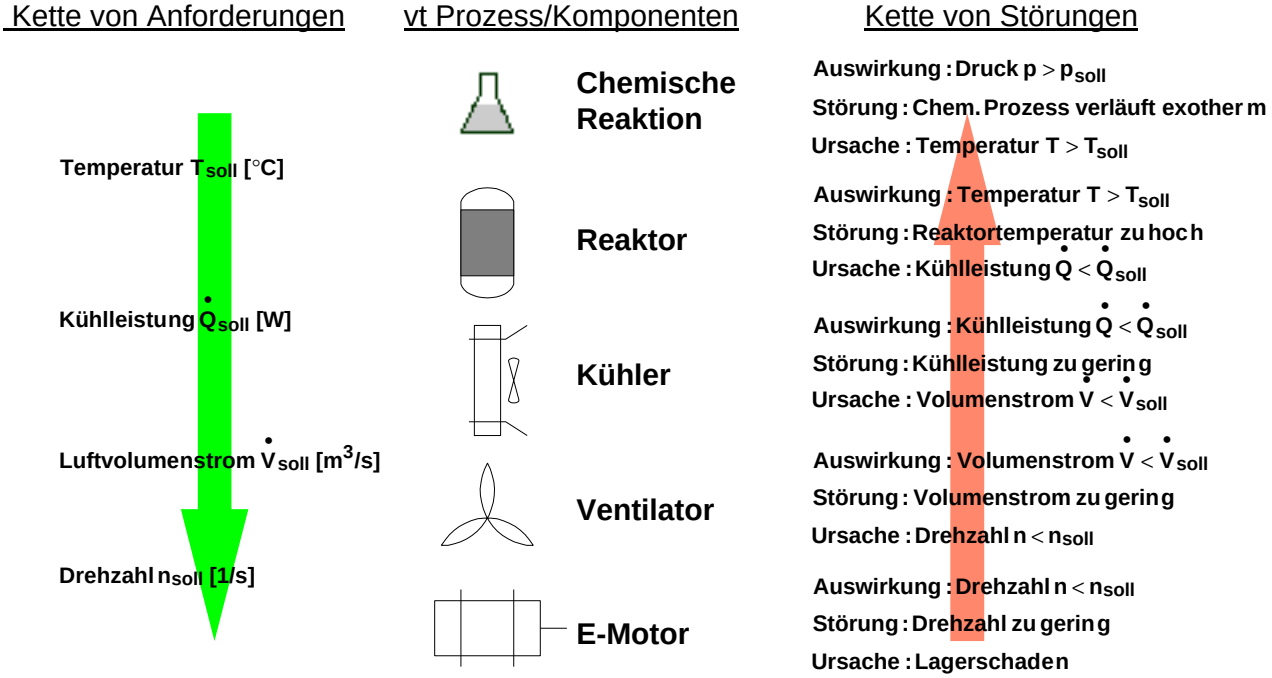

Bild 2: Kette von Störungen basierend auf der Struktur der Komponenten und ihrer Anforderungen

2.1 Funktions-Anforderungsstruktur

Das hier vorgestellte Konzept der Sicherheitsanalyse WISI beruht auf folgendem Zusammenhang /1/:

"Störungen sind Zustände, bei denen die Eigenschaften einer Komponente oder Anlage die an sie gestellten Anforderungen nicht erfüllen."

Denn so wie es eine Verbindung zwischen den Anforderungen der einzelnen Komponenten einer Anlage gibt, so gibt es auch einen Zusammenhang zwischen Störungen der Komponenten untereinander, wie **Bild 2** für einen Anwendungsfall zeigt: Es soll eine Lauge mit bestimmter Konzentration erzeugt werden. Die dabei stattfindende chemische Reaktion ist exotherm. Damit die Temperatur im Reaktor konstant bleibt, muss dieser von einem Kühler gekühlt werden. Der Kühler hat einen Ventilator, der mit einem E-Motor angetrieben wird.

Um nun das Konzept der Sicherheitsanalyse in einem wissensbasierten Informationssystem umzusetzen, werden die bei der Entwicklung von verfahrenstechnischen Systemen anfallenden Anforderungen systematisch erfasst, dokumentiert und gespeichert. Sie bilden die Grundlage der Sicher-

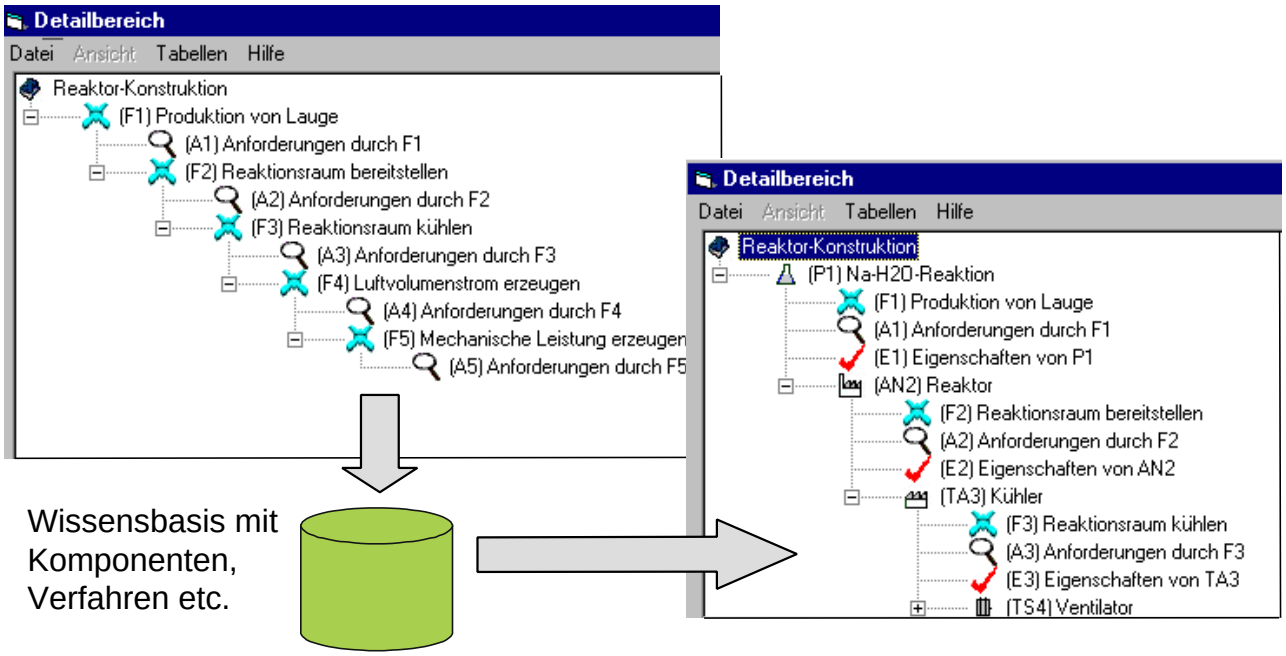

Bild 3: Aufbau der Struktur der Komponenten und ihrer Eigenschaften, Funktionen und Anforderungen

heitsanalyse und werden deshalb zusammen mit den Funktionen als erstes in dem Informationssystem WISI festgehalten. Es entsteht eine Kette von Funktionen und Anforderungen wie sie in **Bild 3** (linker Bereich) dargestellt ist.

2.2 Erweiterung der Struktur mit Anlagen, Komponenten und ihren Eigenschaften

Die Anforderungen stehen bei der Realisierung einer Anlage in Relation zu bestimmten Eigenschaften von Einzelkomponenten und Anlagenteilen. Deswegen ist es notwendig, neben den definierenden Anforderungen die resultierenden Eigenschaften der Komponenten, Anlagen und Baugruppen zu dokumentieren und in der Wissensbasis abzulegen. **Bild 3** (rechter Bereich) zeigt die sich daraus ergebene Informationsstruktur.

2.3 Zuordnung der Störungen, Ursachen, Auswirkungen und Maßnahmen

Durch Festlegen des Konstrukteurs auf Verfahren, Komponenten und deren Zuordnung zu Funktionen und Anforderungen sind auch die in der Datenbank gespeicherten Störungen und Fehler dieser Komponenten bestimmt, die in der bisherigen praktischen Verwendung des Verfahrens oder der Komponente aufgetreten sind. Die daraufhin durchgeführten Maßnahmen zur Beseitigung der Störung, sowie die Ursachen und Auswirkungen der Störung sind durch das Wartungs- und Instandhaltungspersonal im Informationssystem zu erfassen. In einer späteren Entwicklung stehen diese Daten dann als Erfahrungswissen über bereits verwendete Komponenten, Anlagen und Prozesse im Informationssystem zur Verfügung.

Werden die Daten für die Verfahren, Anlagen und Komponenten aber zum ersten Mal angelegt, so sind jetzt mögliche Fehler und Störungen an Hand der im Informationssystem vorliegenden Anforderungen bzw. Funktionen und deren theoretisch möglichen Abweichungen zu ermitteln. Die Informationen sind im System dahingehend zu kennzeichnen, ob es sich um im Team **überlegte** Aktivitäten zur Vorbeugung von Störungen und zur Beseitigung von Störfällen handelt oder ob diese Maßnahmen bei Störfällen bereits realisierter Anlagen und Maschinen bereits **angewendet** wurden.

2.4 Methode einer Sicherheitsanalyse basierend auf der Semantik der Anforderungen

Um aus der Kette von Anforderungen und Eigenschaften eine Methode zur präventiven Analyse möglicher Fehlerquellen zu erhalten, müssen die Informationen von vorbeugend oder den nach einer Störung durchgeführten Störfall- und Fehleranalysen mit den bereits gespeicherten Entwicklungsdaten in der Wissensbasis verknüpft werden. Mit der Verknüpfung der Störungen an die Komponenten können die Auswirkungen der Störung der Komponente A als potentielle Ursachen für Störungen anderer Komponenten B, C, D über die vorliegende Komponentenstruktur untersucht werden. **Bild 4** zeigt einen Aufbau der Struktur zur Untersuchung komponentenübergreifender und interdisziplinärer Auswirkungen von Störungen zwischen chemischer Reaktion und physikalischen Komponenten. Für das Beispiel aus **Bild 2** ergibt sich durch Abweichungen von den Anforderungen folgende theoretische Störungskette, **Bild 4**: Durch einen Lagerschaden am E-Motor K5 als Ursache kommt es zu einer Verringerung des Luftvolumenstroms des Ventilators TS4 und somit einer Verringerung der Kühlleistung des Kühlers TA3. Dadurch steigt die Temperatur im Reaktor AN 2 und die chemische Reaktion P1 verläuft unkontrolliert exotherm.

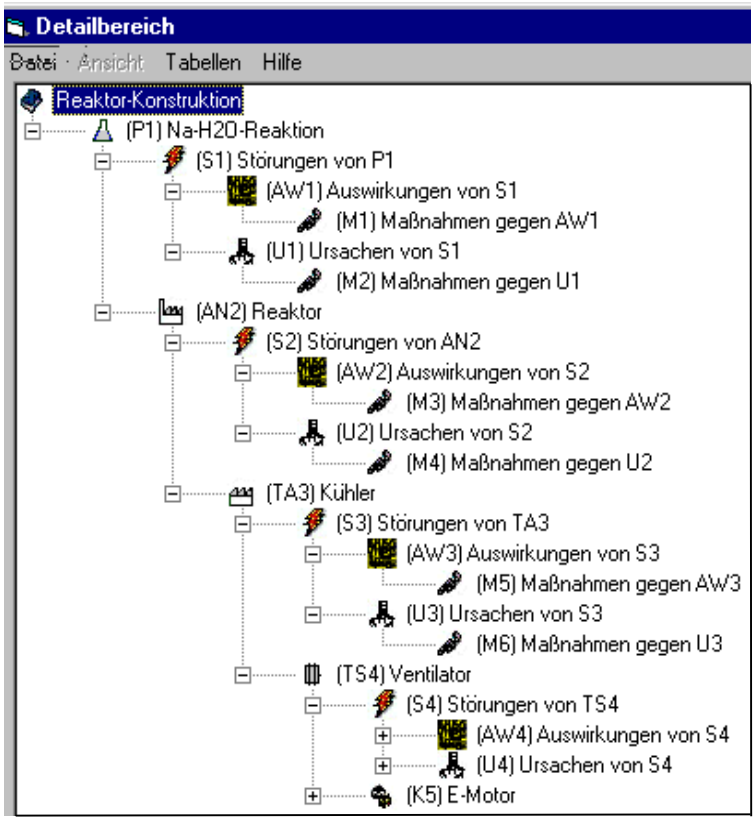

Bild 4: Abbildung der Störungen, Ursachen, Auswirkungen und Maßnahmen im Informationssystem

2.5 Präventive Sicherheitsanalysen

Mit den vorliegenden Daten von bereits realisierten Anlagen können durch das Informationssystem präventive Sicherheitsanalysen mit hoher Zuverlässigkeit für neue Anlagen durchgeführt werden, obwohl diese noch in der Entwicklungsphase sind. Mit den im Informationssystem abgespeicherten Datenstrukturen von Komponenten, Anlagen etc. lassen sich Ursachen von Störungen simulieren. Die sich daraufhin ergebende Störungskette kann nach gefährlichen Auswirkungen durchsucht werden. Gegen die Ursachen oder Auswirkungen werden dann präventive Maßnahmen ergriffen.

Aufgrund des modularen Aufbaus ist das Informationssystem geeignet, interdisziplinäre Zusammenhänge zwischen einzelnen Fachbereichen wie Verfahrenstechnik und Maschinenbau nicht nur beim Entwicklungsprozess sondern auch bei der Sicherheitsanalyse zu berücksichtigen. Es ist dadurch möglich, Ursache-Störung-Auswirkung-Zusammenhänge über chemische Verfahren, physikalische Komponenten und softwaretechnische Programme hinweg zu untersuchen, wie bereits in **Bild 4** in der Störungskette zwischen chemischer Reaktion (Bezeichnung P1) und der physikalischer Komponente Reaktor (AN2) gezeigt wurde.

In das Informationssystem wurden die Analysemethoden nach HAZOP "Hazard and Operability Study" (auch PAAG-Verfahren genannt) /4/ und FMEA "Fehler-Möglichkeits- und -Einfluß-Analyse" /5/ integriert.

Mit der HAZOP-Methode werden systematisch Gefahrenquellen durch Abweichung der Funktion einer Komponente von der Sollfunktion mit Hilfe von Leitworten in interdisziplinärer Teamarbeit ermittelt. Die potentielle Gefahr wird hinsichtlich ihrer Bedeutung bewertet und bei Relevanz werden Maßnahmen zur Risikominimierung ausgearbeitet.

Durch die FMEA-Analyse können die Störungen hinsichtlich ihres Risikos quantitativ beurteilt werden. Dazu werden die Kriterien "Bedeutung B" einer Auswirkung, "Entdeckungswahrscheinlichkeit E" einer Ursache und "Auftrittswahrscheinlichkeit A" einer Ursache mit einem Wert im Bereich von 1 bis 10 bewertet. Das Produkt der drei Einzelwerte ergibt dann die Risikoprioritätszahl RPZ = AxBxE. Je größer RPZ ist, desto höher ist das Risiko dieser Störung.

Bild 5 (unterer Bereich) zeigt das Ergebnis der Si-

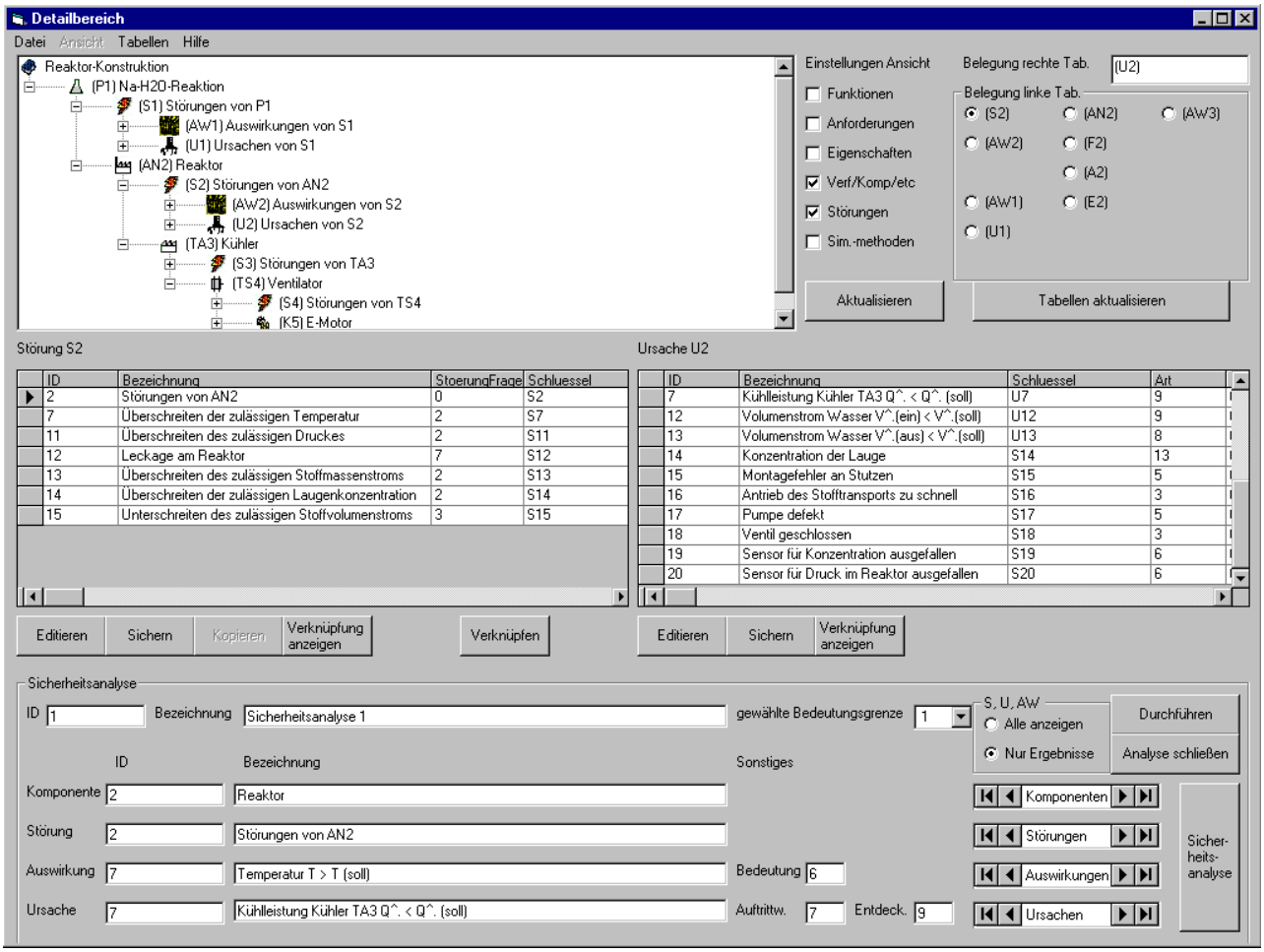

Bild 5: Oberfläche des Informationssystems "**Wi**ssensbasierte **Si**cherheitsanalyse" (WISI)

cherheitsanalyse an der Struktur aus **Bild 2**, durchgeführt mit dem Informationssystem WISI. Dabei wurde die Ursache Lagerschaden einer Störung des E-Motors (K5) ausgelöst. Das Informationssystem ermittelt alle Störungen, Ursachen und Auswirkungen, die sich daraufhin bei den anderen Komponenten (TS4, TA3, AN2) und der chemischen Reaktion (P1) ergeben und zeigt sie an.

3 Integration von Simulationstechniken in das Informationssystem WISI

Um noch genauere Aussagen über Fehler- oder Störungspotentiale und ihre möglichen Auswirkungen gerade bei neuen Anlagen und ihren Prozessen zu machen, müssen die Prozessgrößen jeder Komponente im Betrieb mit dem zulässigen Wert der dazugehörigen Eigenschaft für diese Komponente verglichen werden. Wird dieser Vergleich an realen Anlagen durchgeführt, handelt es sich um eine Prozessüberwachung, die bei erkannten Abweichungen eine Störungsmeldung oder Gegenmaßnahme auslöst. Damit diese Analyse schon präventiv durchgeführt werden kann, muss ein Vergleich zwischen den zulässigen, in der Wissensbasis gespeicherten Werten und simulierten Prozessgrößen vorgenommen werden.

3.1 Abbildung von Anlagen und Komponenten durch Simulationsmodelle

Zur Ermittlung dieser Werte sind Simulationsmodelle nötig, die das reale Verhalten der Anlage und ihrer Komponenten sehr genau abbilden. Werden diese Simulationsmodelle in den Regelkreis zwischen Operateuren und der realen Anlage eingefügt, so können die zu erwartenden Prozessgrößen aus den Stellgrößen vorherbestimmt werden. Die Überprüfung auf Prozesssicherheit kann dann an Hand der zulässigen Werte aus der Wissensbasis vorgenommen werden. Sollte das Informationssystem das Überschreiten der zulässigen Werte und damit das potentielle Auftreten von Störungen feststellen, kann es den Operateur darauf hinweisen und ihn zum Korrigieren der Stellgrößen auffordern bevor tatsächlich an der Anlage etwas verändert wird /2/.

Damit computergestützte Methoden wie Neuronale Netze, Fuzzy-Technologie und numerische Algorithmen in das Informationssystem "Wissensbasierte Sicherheitsanalyse" integriert werden können, ist die datenbanktechnische Zuordnung der einzelnen Methode zu der durch sie zu simulierenden Komponente in der Wissensbasis nötig /3/. Außerdem sind die für eine Abbildung ermittelten Methodenparameter dort zu speichern. Dabei ist die benötigte Genauigkeit einer Abbildung vom jeweiligen Anwendungsfall abhängig. Auf diese Weise wird das Erfahrungswissen über das Betriebsverhalten von Prozessen und Anlagen im Informationssystem erfasst. Wegen der Relationen zwischen den Simulationsmethoden und einzelnen Komponenten stimmen die Ergebnisse einer präventiven Sicherheitsanalyse für eine neuzuentwickelnde Anlage, durchgeführt an ihrem Modell, mit hoher Wahrscheinlichkeit mit dem zukünftigen Verhalten der realen Anlage überein. Die Zuordnung einzelner Methoden zur jeweiligen Komponente zeigt **Bild 6**.

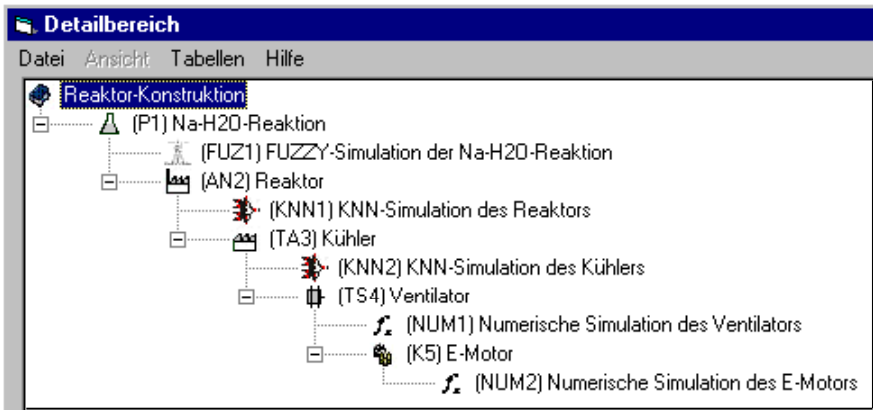

Bild 6: Integration der Simulationsmethoden in die Struktur des Informationssystems

Durch die Integration der Simulationsmethoden einzelner Komponenten können die Auswirkungen von angenommenen Fehlern quantifiziert werden. Die ermittelten Werte werden als neue Anforderungen mit den zugehörigen zulässigen Eigenschaften einer Komponente oder Anlage im Informationssystem verglichen. Bei Überschreiten von Eigenschaften sind geeignete Maßnahmen zu ergreifen.

3.2 Verknüpfung einzelner Simulationsmodelle zu einem Simulationsnetzwerk

Um nun eine Sicherheitsanalyse an einer ganzen Anlage durchzuführen, muss die Struktur ihrer physikalischen, energietechnischen, signaltechnischen und sonstigen Verbindungen der Komponenten innerhalb dieser Anlage erfasst sein. Dazu kann die

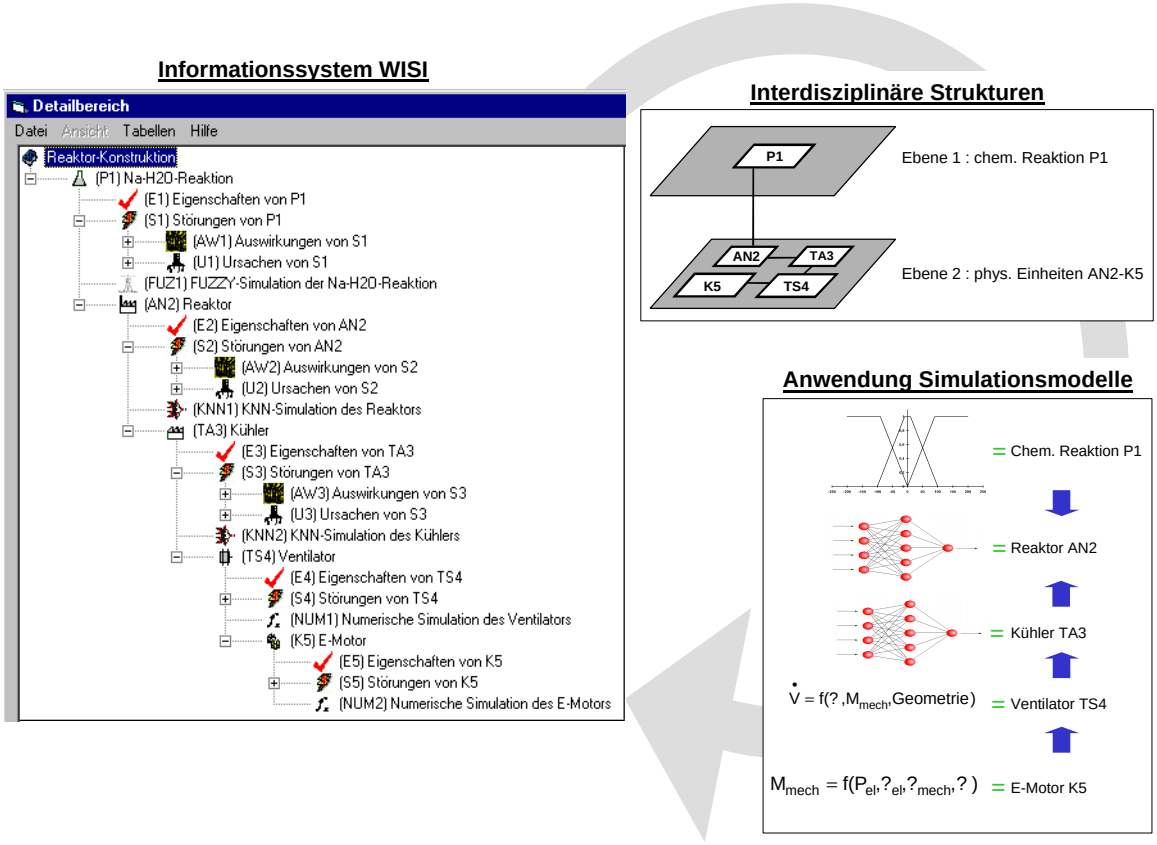

Bild 7: Untersuchung der Störungen an Hand der Komponentenstruktur und Simulationsmodelle

bereits im Entwicklungsprozess modellierte interdisziplinäre Struktur benutzt werden. Anhand dieser erkennt das Informationssystem, welche Datenobjekte miteinander in Verbindung stehen. In **Bild 7** ist schematisch eine solche interdisziplinäre Untersuchung an den Simulationsmodellen der einzelnen Objekte dargestellt.

4 Zusammenfassung

Der Artikel beschreibt ein Informationssystem zur Erfassung, Speicherung und Aufbereitung von Informationen aus allen Produktlebensphasen von Maschinen und Anlagen. Dabei wird besonders auf die Bereiche Entwicklungsprozess, Simulationstechnik und Sicherheitsanalysen eingegangen. Das Informationssystem verknüpft die Daten aus einzelnen Fachbereichen des Entwicklungsprozesses von der Planung bis zur Stilllegung. Die erfassten Daten können nicht nur für einen optimalen Betrieb der Anlagen oder Maschinen hinsichtlich Sicherheit genutzt werden, sondern stehen auch bei der Neukonstruktion als Erfahrungswissen über bereits verwendete Verfahren, Prozesse, Teilanlagen und Komponenten zur Verfügung. Durch die zusätzliche Integration der Simulationstechnik in das Informationssystem wird der Entwicklungsprozess umfassend unterstützt und die Durchführung von zuverlässigen, quantitativen und präventiven Sicherheitsanalysen ermöglicht.

5 Literatur

/1/ Dietz, P. (Hrsg.): Konstruktion verfahrenstechnischer Maschinen; Springer Verlag, Berlin 2000

/2/ Beisheim, N.: Einsatz von neuronalen Netzen und Fuzzy-Technologie in der vorbeugenden Störfallsimulation; Institutsmitteilung Nr. 24, IMW Clausthal 1999

/3/ Rosendahl, R.: Wissensbasierte Simulationstechnik bei verfahrenstechnischen Maschinen und Anlagen, Diplomarbeit am Institut für Maschinenwesen der TU Clausthal, Clausthal 2000

/4/ DIN IEC 56/581/CD: Leitfaden zur Gefährdungs- und Betreibbarkeitsuntersuchung (HAZOP) Deutsches Institut für Normung e.V.,Beuth Verlag GmbH, Berlin 1998

/5/ DIN 25448: Ausfalleffektanalyse (Fehler-Möglichkeits- und -Einfluß-Analyse) Deutsches Institut für Normung e.V.,Beuth Verlag GmbH, Berlin 1990