Modellbasierte Diagnose in der Schiffsleittechnik

A. Bäcker, S. Kockskämper, B. Neumann, H. Reetmeyer und **G. Nicklas,** Hamburg

Zusammenfassung

Maritime Einrichtungen im weitesten Sinn, sowohl stationäre Einheiten wie z.B. Offshore-Einrichtungen als auch nichtstationäre Einrichtungen wie z.B. Handelsschiffe sind komplexe, sicherheitsrelevante Anlagen. Im Falle einer Störung bergen diese Systeme ein Risikopotential in sich, von dem erhebliche Gefahren nicht nur für Menschen und Material, sondern auch für die gesamte Umwelt ausgehen.

Der vorliegende Beitrag stellt ein Prozeßmanagement-System vor, das modellgestützte Verfahren zur Störfallentdeckung, Ursachenfindung und Störfallbehandlung in derartigen Anlagen einsetzt. In diesem System wird eine Fehlerdiagnose im wesentlichen durch eine rechnerinterne Simulation des Systemverhaltens geleistet auf der Basis eines strukturierten Modells der Anlage. Es wird gezeigt, daß dieser Ansatz ideal geeignet ist, der großen Komplexität derartiger Anlagen Rechnung zu tragen.

1. Einleitung

Die Weiterentwicklung technischer Systeme führt in zunehmendem Maße zum Entwurf von Anlagen erheblicher Komplexität. Um den Menschen in die Lage zu versetzen, die Anlage auch bei auftretenden Störungen sicher zu bedienen, werden Schutzeinrichtungen in das Anlagenkonzept integriert. Die entsprechenden Zusatzeinrichtungen sind bisher überwiegend derart konzipiert, daß sie zwar auf Störungen in Anlagenteilen sinnvoll reagieren, eine möglicherweise komplexe Gesamtsituation jedoch meist nicht korrekt erfassen und klassifizieren können. Dies gilt um so mehr, wenn es nicht nur auf die genaue Anzeige einer Störung sondern auch auf die Empfehlung und Einleitung geeigneter korrektiver Maßnahmen ankommt. Hier ist die Grenze der Leistungsfähigkeit von Schutzmaßnahmen herkömmlicher Art erreicht.

Das hiermit gegebene Restrisiko ist von großer Relevanz, wenn die Anlage im Störfall ein erhebliches Gefahrenpotential für Umwelt, Mensch oder Maschine darstellt. Die

bekanntesten Beispiele für solche Ereignisse sind mit den Namen Harrisburg, Tschernobyl oder Valdez verbunden.

Dieser Beitrag befaßt sich mit Störsituationen in komplexen Anlagen, bei denen der Mensch in seiner Prozeßmanagement-Funktion überfordert sein kann und Hilfsmittel zur Störfallentdeckung, Ursachenfindung und Störfallbehandlung wünschenswert sind. Derartige Hilfsmittel können heute in Gestalt von komplexen informationsverarbeitenden Systemen entwickelt werden, die sich auf Forschungsergebnisse der Künstlichen Intelligenz stützen und die Leistungsfähigkeit moderner Hardware und Software ausnutzen. Wir bezeichnen ein solches System im folgenden als Prozeßmanagement-System (PMS).

Nach einer kurzen Übersicht über die Anforderungen, die an das PMS gestellt werden, wird die Systemarchitektur vorgestellt.

2. Anforderungen

Um einen Menschen beim Prozeßmanagement wirksam unterstützen zu können, muß das PMS eine Reihe von Aufgaben ausführen:

- Der Prozeß ist permanent zu beobachten. Dies erfolgt durch das regelmäßige Abtasten von Sensoren.
- Die Entwicklung abnormaler Systemzustände und abnormalen Systemverhaltens muß möglichst frühzeitig erkannt werden.
- Die Ursachen für abnormales Systemverhalten, also mögliche Defekte von Komponenten oder Fehleinstellungen, müssen ermittelt werden.
- Abnormales Systemverhalten ist daraufhin zu klassifizieren, inwieweit es den technischen Prozeß und die Prozeßumgebung gefährdet.
- Im Falle von abnormalem Systemverhalten sind Strategien zu ermitteln, wie in der aktuellen Situation weiter zu verfahren ist. Dabei müssen je nach Klassifizierung der Situation Prioritäten entsprechend gesetzt werden.
- Geplante korrektive Prozeßsteuerungsmaßnahmen sind hinsichtlich ihrer voraussichtlichen Auswirkungen auf das Gesamtsystem zu analysieren.

3. Systemarchitektur

Der Systementwurf, der diesen Anforderungen entspricht, ist in Abbildung 1 dargestellt und soll folgend kurz diskutiert werden.

Systembeobachtung und eine robuste, aber nur begrenzt aussagefähige Verhaltensanalyse werden durch das Prozeßsteuerungs-Interface (PCI) durchgeführt, hinter dem sich ein konventionelles Prozeßdaten-Akquisitions-System verbirgt.

Die frühzeitige Fehlererkennung erfolgt durch eine prädiktive Fehlerdetektion. Diese beruht auf dem Prinzip, den Prozeß zu beobachten und mit Erwartungswerten zu vergleichen, die aus einem simulierten Modellprozeß gewonnen werden. Die Prädiktion wird also wesentlich durch die Simulator-Komponente getragen.

Die spezielle Aufgabe der Diagnose ist es, Fehlverhalten einer oder mehrerer Komponenten des technischen Prozesses zu ermitteln. Dies geschieht, indem das interne Prozeßmodell des PMS entsprechend der Meßdaten angepaßt wird, bis die Simulation mit der Realität übereinstimmt. Das so gewonnene Prozeßmodell erlaubt die gewünschten Aussagen über fehlerhafte Komponenten.

Gleichzeitig ist das PMS auch in der Lage, eine Prädiktion über das zukünftige Verhalten des realen, gestörten Prozesses anzustellen.

Auf der Basis der Fehlerdiagnose schließlich entwickelt der als Therapie bezeichnete Baustein Strategien, um mit den verfügbaren Mitteln die Auswirkungen des aufgetretenen Fehlers auf ein Minimum zu reduzieren. Die Verifikation der vorgeschlagenen Strategien kann wiederum durch Simulation am gestörten Prozeßmodell erfolgen.

Jede der genannten Software-Komponenten hat Zugriff auf ein Prozeßmodell, das die erforderlichen Informationen über den realen Prozeß in Form einer deklarativen Wissensbasis enthält. Da der Aufbau dieses Modells von zentraler Bedeutung für die Leistungsfähigkeit des PMS ist, werden wir im nächsten Kapitel explizit darauf eingehen.

Da an das PMS Echtzeitanforderungen zu stellen sind, ist eine flexible Ablaufsteuerung erforderlich, die es gestattet, zeitkritische Berechnungen vorzuziehen und generell den Rechenaufwand der zur Verfügung stehenden Zeit anzupassen. Dies wird durch die dargestellten Komponenten Agenda, Scheduler und Strategien erreicht.

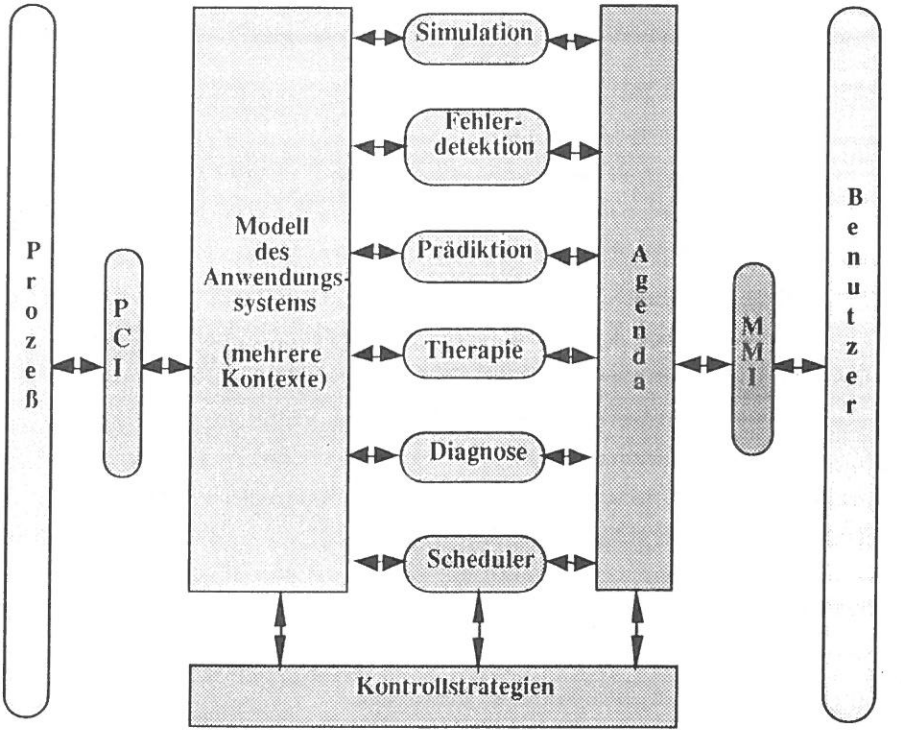

Abb. 1: Die Systemarchitektur

4. Modellbasierte Diagnose

Bisherige Ansätze auf dem Gebiet der technischen Diagnose sind wesentlich durch das regelbasierte Paradigma geprägt. Es beruht auf einer rechnerinternen Modellierung von regelhaftem Expertenwissen über Fehlersymptome und ihre wahrscheinlichen Ursachen. In den letzten Jahren sind die Grenzen dieses Ansatzes zunehmend deutlich geworden. Ein wesentlicher Grund für die Probleme ist die Tatsache, daß der regelbasierte Ansatz, der für die Modellierung kognitiver Phänomene, insbesondere empirischer Assoziationen, nicht aber für die Beschreibung technischer Zusammenhänge geeignet ist. Daraus resultieren zahlreiche Schwierigkeiten: Größere regelbasierte Systeme sind schwer zu warten und zu modifizieren; eine Lösung läßt sich nicht leicht von einer Anwendung auf eine andere übertragen; regelbasierte Systeme können nur Fehler diagnostizieren, auf die sie explizit vorbereitet wurden; es können keine tiefergehenden Erklärungen zu einer Fehlerdiagnose gegeben werden; es gibt keine abgesicherten

Verfahren zur systematischen, ingenieursmäßigen Konstruktion regelbasierter Diagnosesysteme [3].

Zur Überwindung dieser Schwierigkeiten wurden von der KI-Forschung in den letzten Jahren neuartige Architekturen für Diagnosesysteme vorgeschlagen, in denen "tiefe Modelle" [1,2,4] der zu diagnostizierenden Systeme eine entscheidende Rolle spielen.

Folgende Abbildung veranschaulicht die Vorgehensweise bei der modellbasierten Diagnose:

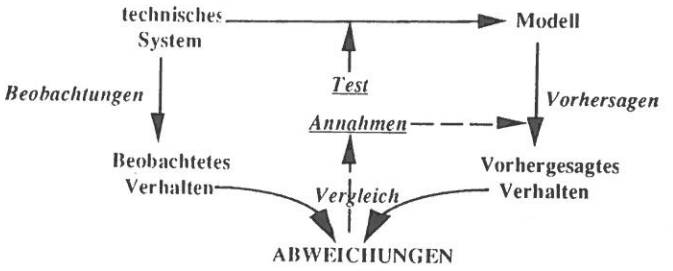

Abb. 2: Vorgehensweise bei der modellgestützten Diagnose

Durch ein tiefes Modell wird versucht, wesentliche Eigenschaften eines technischen Systems rechnerintern nachzubilden, so daß korrektes wie auch fehlerhaftes Verhalten simuliert werden kann. Vorhergesagtes und tatsächliches Verhalten werden permanent verglichen. Tritt eine Abweichung auf, so können ausgehend von diesen Daten (und evtl. weiteren Tests) Vermutungen über Fehlfunktionen von Komponenten untersucht werden. Hypothesenüberprüfungen werden wiederum mithilfe des Simulators vorgenommen, in dem unter geänderten Verhaltensannahmen (z.B. Ventil klemmt) für die Komponenten simuliert wird.

Im weiteren Verlauf dieses Abschnittes werden wir einen kurzen Überblick über die für die tiefe Modellierung erforderliche Wissensrepräsentation geben und anschließend mithilfe eines Beispiels die Vorgehensweise bei der Diagnose veranschaulichen.

4.1. Wissensrepräsentation

Das konzeptuelle Domänenwissen wird in einer Komponentenhierarchie vorstrukturiert, die eine taxomomische und eine kompositionelle (Zerlegungs-)Hierarchie umfaßt (Abbildung 3). Hier werden alle Komponenten mit ihren Eigenschaften konzeptuell, d.h. als Komponentenklassen beschrieben, ähnlich einem Typenverzeichnis. Als *elementar* werden solche Komponenten bezeichnet, die nicht weiter in Unterkomponenten zerlegt werden. Ihre geschickte Auswahl spielt eine wichtige Rolle sowohl beim Modellierungsaufwand als auch bei der späteren Effizienz. Es bietet sich

z.B. an, Komponenten, die bei Defekt ohnehin komplett ausgetauscht werden, als elementare Komponenten zu modellieren.

Da Komponenten dem Aufbau von Wirkungsketten dienen sollen, muß jede Komponentenklasse folgende Informationen speichern:

- **Schnittstellen nach außen (ports):** Die Ports einer Komponente bilden die einzigen Verbindungen zur Außenwelt. Jeder Port besitzt einen Typ, der angibt, mit welchem Porttyp er verbunden sein kann. Zusätzlich wird für jeden Port angegeben, ob er ein Input- oder Output-Port ist oder bidirektional verwendet wird.
- **Korrektes Verhalten und mögliche Fehlverhalten:** Das Verhalten einer Komponente geht für die Außenwelt nur aus den Beziehungen zwischen seinen Ports hervor. Diese Funktionalität läßt sich intern z.B. durch Constraints zwischen den Ports und Zustandsparametern, Regeln oder Tabellen etc. darstellen.
- **Interne Parameter:** Eine Komponente kann interne Parameter besitzen, z.B. haben Leitungen einen Strömungswiderstand. Der (Gesamt-)Zustand einer Komponente setzt sich aus den konkreten Belegungen der Ein- und Ausgangsvariablen und der internen Parametern zusammen.
- **Bestandteile (Zusammensetzung):** Für jede Komponente ist angegeben, aus welchen Teilkomponenten sie besteht ("part-of-Kanten" Abbildung 3b) und welche Verbindungsstruktur zwischen den Ports dieser Teilkomponenten untereinander und zu der strukturell übergeordneten Komponente selbst bestehen. Die Ports der einzelnen Teilkomponenten sind untereinander durch "connected-to-Kanten" (Abbildung 3b) verbunden. Die Ports der strukturell übergeordneten Komponente werden mit den entsprechenden Ports der Teilkomponenten *identifiziert*.

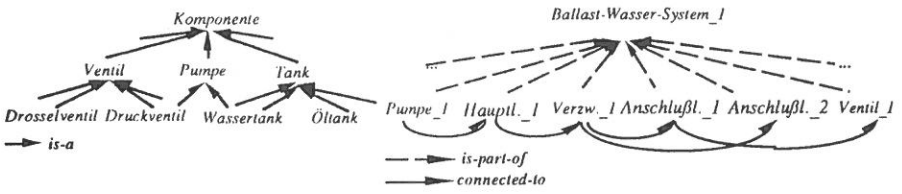

Abb. 3: a) Die konzeptuelle Komponentenhierarchie b) Zerlegungshierarchie und funktionale Abhängigkeiten

4.2. Qualitative Beschreibungsebenen

Bei der Modellierung technischer Systeme spielt die Auswahl geeigneter Modellierungsebenen eine große Rolle. Einerseits besteht der Wunsch, möglichst weitgehende Informationen über das Systemverhalten aus dem Modell ableiten zu

können. Dazu müssen funktionale Zusammenhänge, interne Parameter und Port-Variablen quantitativ und präzise beschrieben werden. Andererseits wächst mit dem Umfang des Modells auch der Rechenaufwand für eine Simulation des Systemverhaltens. Es kann daher sinnvoll sein, eine Komponente nur qualitativ durch grobe Wertebereiche, ungefähre Zusammenhänge etc. zu beschreiben.

Wir verfolgen den Ansatz, mehrere qualitative Detaillierungsebenen einer Komponente zu berücksichtigen. Diese Lösung ist sehr flexibel, da die Ebene der Betrachtung nicht vorab feststeht, sondern je nach Bedarf variieren kann. Solange Modell und reales System keine Abweichungen in ihrem Verhalten aufweisen, kann der Prozeß auf einer relativ hohen (qualitativen und/oder strukturellen) Ebene beobachtet werden. Treten Diskrepanzen auf, kann ein Abstieg in eine tiefere Ebene erfolgen, um den Fehler zu lokalisieren.

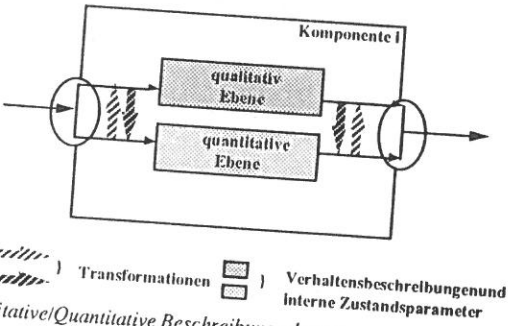

Abb.4: Qualitative/Quantitative Beschreibungsebenen

4.3. Diagnose im Ballastwasser-System

Wir demonstrieren im folgenden anhand eines Beispiels, wie der modellbasierte Ansatz im Problembereich der Schiffsleittechnik realisiert werden kann. Wir beschränken uns in der Darstellung auf Teile eines Ballastwasser-Systems (Abb. 5).

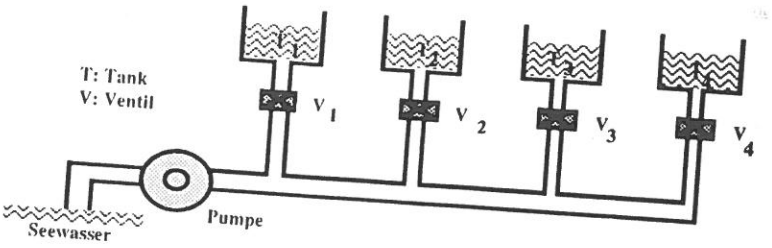

Abb. 5: Das Ballastwasser-System

Vier Tanks sind je über ein Ventil mit einer Pumpe verbunden. Die eingeschaltete Pumpe erzeugt einen konstanten Wasserstrom, der die Tanks in Abhängigkeit von den jeweiligen Ventilstellungen und Füllhöhen auffüllt. Aufgabe des Diagnosesystems ist es, von den Meßwerten (Füllstände Q_i, Ventilstellungen R_i, Pumpenstrom A_P, Pumpenspannung E_P) auf mögliche Fehlerbedingungen (verklemmte oder gebrochene Ventile, Rohrbrüche, Pumpendefekte, u.a.) zu schließen. Kern des Diagnosesystems ist ein Simulationsmodell, mit dem das Füllen der Tanks sowie Fehlersituationen simuliert werden können.

Das Simulationsmodell besteht, wie bereits im letzten Abschnitt erwähnt, aus individuell beschriebenen Komponenten sowie einer Spezifikation ihrer Verbindungsstruktur (Abb.6).

Pumpe(P): I_p = konstant
Hauptleitung: $I_p = \Sigma I_{i1}$, $i \in \{1,...,3\}$

$U_p = U_{i1}$
Ventile(V): $I_{i2} = I_{i3}$
$U_{i3} = U_{i2} + R_i * I_{i2}$

Anschluß-leitungen(A): $I_{i1} = I_{i2}$
$U_{i1} = U_{i2}$
Tanks(T): $U_0 = U_{i3} - Q_i \backslash C$
$Q_i(t+dt) = Q_i(t) + I$
*dt

Fehlverhalten Anschlußleitungen:
verstopft: $I_{i1} = I_{i2} = 0$
U_{i2}, U_{i1} unkorreliert
undicht: $I_{i2} <> I_{i1}$, $U_{i2} = U_{i1}$

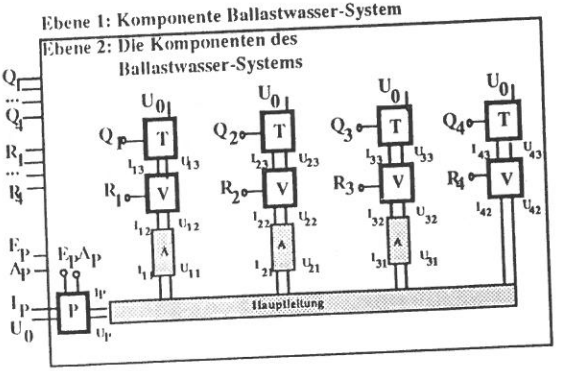

Abb. 6: *Das Ballastwasser-System, seine Komponenten und deren Verhalten im fehlerfreien Zustand und mögliches Fehlverhalten (beispielhaft für die Anschlußleitungen). Aus Gründen der Übersichtlichkeit wurde auf die Verbindungen zwischen den Ports des Ballastwasser-Systems und den entsprechenden Ports der Subkomponenten verzichtet.*

Verzweigungen (VZ): $I_i = I_{i+1} + I_{i+2}$
$U_i = U_{i+1} = U_{i+2}$

Haupt-leitungen(H): $I_i = I_{i+1}$
$U_i = U_{i+1}$

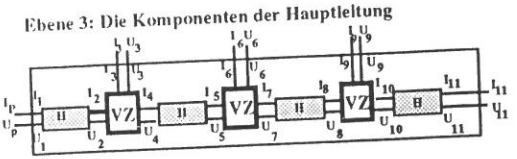

Abb. 7: *"Innenansicht" der Hauptleitung als Beispiel für verschiedene strukturelle Ebenen*

Gegeben sei nun folgende Ausgangssituation:

Es wird beobachtet, daß der Wasserpegel des zweiten Tanks (im Gegensatz zu den Pegeln der anderen Tanks) immer weiter fällt, obwohl vom Simulator (unter der Annahme, daß alle Komponenten korrekt arbeiten) ein steigender Wasserpegel für alle

Tanks vorausgesagt wurde. Hier liegt also eine Diskrepanz zwischen beobachtetem und vorhergesagtem Verhalten vor. Diese Diskrepanz läßt sich nur durch einen Wasserverlust erklären. Ein Nivellierungsvorgang, als Auswirkung einer Störung, erklärt zwar das beobachtete Verhalten, kann jedoch ausgeschlossen werden, aufgrund der Tatsache, daß der Pegel des zweiten Tanks niedriger ist als die der anderen Tanks.

Diese Information wird auf der (strukturellen) Ebene 1 (Abbildung 6: Komponente Ballastwasser-System) abgeleitet.

In ersten Schritt wird versucht, diejenigen Verhaltensannahmen zu identifizieren, die für die Abweichung in Frage kommen können, d.h. die das abweichende Verhalten erklären.

Als wahrscheinlichste Fehlerkandidaten kommen ein Leck in einem der Tanks oder ein Rohrbruch in Frage. Weitere Störungen können nicht ausgeschlossen werden, jedoch kommen sie nur in Verbindung mit den erstgenannten Defekten in Frage, da sie alleine einen Wasserverlust nicht erklären.

Als Fehlerhypothesen werden Defekte folgender Komponenten angenommen:

{Pumpe, Hauptleitung, Anschlußleitung, Ventil, Tank2}

Weiterhin liegen folgende (qualitative) Informationen vor, die die Pumpe und das Ventil als Fehlerkandidaten ausschließen.

Pumpe_liefert_Wasser ($I_p > 0$ und konstant) , Ventil1_Offen ($R_1 \approx 0$)

Als Hypothesen verbleiben somit: *{Hauptleitung, Anschlußleitung1;Tank2}*

Nach einer qualitativen Simulation auf Ebene 2 (unter geänderten Verhaltensannahmen für die Komponenten) wird festgestellt, daß ein Leck im Tankboden als einziger Kandidat für einen Störung in Frage kommt, die von einer einzelnen Komponente verursacht wurde. Ein Bruch in der Hauptleitung und/oder der Anschlußleitung konnte durch die Simulation ausgeschlossen werden, da sich in diesem Falle alle Tanks gleichmäßig entleeren würden. Es besteht weiterhin die Möglichkeit, daß auch andere Defekte vorliegen, jedoch nur in Kombination mit diesem Fehler.

Aufgrund der qualitativen Analyse (und da keine weiteren Messungen vorgenommen werden können), würde der Operateur in diesem Fall - um zu verhindern, daß zuviel Flüssigkeit unkontrolliert entweicht - die Ventile der intakten Tanks schließen und die Pumpe so umsteuern, daß der defekte Tank möglichst schnell entleert wird.

Wird das System jedoch einer weiteren, jetzt quantitativen Analyse unterzogen, zeigt sich, daß auch das geänderte Verhaltensmodell (Annahme: Leck im Tank) nicht mit der Realität übereinstimmt, da die Flüssigkeitszunahme in den intakten Tanks exakt dem

Pumpenstrom entspricht. Ein erheblicher Teil des geförderten Wassers müßte aber in Tank2 und von dort durch das Leck strömen. Das bedeutet also, daß ein Leck im Boden des zweiten Tanks nicht der alleinige Verursacher des beobachteten Verhalten sein kann.

Nach einer quantitativen Simulation stellt sich heraus, daß erst die zusätzliche Annahme - eine Verstopfung der Anschlußleitung zum zweiten Tank - das beobachtete Verhalten vollständig erklärt.

Zur Behebung dieses Problems muß nun eine vollkommen andere Strategie entwickelt werden als dies beim Ergebnis der qualitativen Analyse der Fall war. Aufgrund der verstopften Leitung ist ein Abpumpen der Flüssigkeit aus dem Tank nicht mehr möglich.

Dieser Schluß, der in der Realität erhebliche Konsequenzen haben kann, ist hier nur durch die modellgestützte Analyse des Systems möglich geworden. Von großem Vorteil haben sich hierbei auch die verschiedenen qualitativ/quantitatven und strukturellen Modellierungsebenen gezeigt: Auf strukturell und/oder qualitativ hoher Ebene kann der Fehler relativ schnell eingekreist werden. Mit Hilfe einer sich daran anschließenden quantitativen Analyse kann die Störung schließlich exakt lokalisiert werden.

5. Zusammenfassung und Ausblick

Die Weiterentwicklung von Methoden der Informationsverarbeitung, insbesondere die Technologie der wissensbasierten Systeme, beinhaltet ein weitreichendes Potential für Systeme, mit Hilfe derer das Restrisiko kritischer technischer Prozesse reduziert werden kann.

Der modellbasierte Ansatz erscheint als eine geeignete Möglichkeit, komplexe technische Anlagen sinnvoll zu beschreiben und Aufgaben der Prädiktion, Diagnose und Therapie zu unterstützen.

6. Literatur

[1] J. de Kleer, B.C.Williams: Diagnosing Multiple Faults
aus: Artificial Intelligence 32 (1987) S. 97-130

[2] J. de Kleer, B.C.Williams: Diagnosis With Behavioral Modes
aus: Proc. IJCAI '89 (11th International Joint Conference on Artificial Intelligence), S. 1324-1330

[3] P.Struß: Model-Based Diagnosis - Progress and Problems
aus: Proc. 3. Interner GI-Kongreß Wissensbasierte Systeme, München, S.320-331, Oktober 1989

[4] P.Struß, O.Dressler : 'Physical Negation' - Integration Fault Models into the General Diagnostic Engine
aus: Proc. IJCAI '89 (11th International Joint Conference on Artificial Intelligence), S. 1318-1324