

# Integration domänenspezifischer Modellierung in der Diagnose von Automatisierungssystemen

Dennis Klar

Michaela Huhn

Institut für Informatik, Technische Universität Clausthal, D-38678 Clausthal-Zellerfeld  
{Dennis.Klar | Michaela.Huhn}@tu-clausthal.de

## Zusammenfassung

Wir diskutieren die Verwendung einer domänen- und aufgabenspezifischen Modellierung im Rahmen der Anlagendiagnose von Bahnautomatisierungssystemen. Aus Randbedingungen wie der Variabilität der Prozesse, der Komplexität und Exponiertheit der Anlagen und den geforderten Kennzahlen für die Instandsetzung ergibt sich die Notwendigkeit, spezifische Diagnosemodelle zu erstellen, die sich auf Fehler, Symptome und ihre Wandlung konzentrieren.

**Schlüsselwörter** Anlagendiagnose, domänenspezifische Modellierung, Diagnoseprozess

## 1 Einleitung

In der Automatisierungstechnik finden modellbasierte Software-Entwicklungs- und Analysemethoden breite Verwendung. In der chemischen Industrie bilden Entwicklungsmodelle mit funktionalem Charakter, die das Schalt- oder Flussverhalten im Normalbetrieb in der Produktionsanlage beschreiben, auch die Basis für die Diagnose. Die traditionelle, konsistenzbasierte Diagnose [1] ‚simuliert‘ diese Modelle mit dem Ziel, durch Vergleichswerte aus der laufenden Anlage Abweichungen zu detektieren. Lassen sich die Prozesse kompakt modellieren und aus den Sensorwerten der Anlage präzise Aussagen über den Ursprung möglicher Abweichungen ableiten, besteht dieser Ansatz durch den geringen Modellierungsaufwand.

Bahnautomatisierungsanlagen, aber auch z.B. moderne Energieversorgungsnetze, zeichnen sich hingegen durch ausgedehnte und exponierte Anlagen, komplexe Komponenten, eingeschränkte Beobachtbarkeit und eine große Prozess-Variabilität aus, sodass wesentliche Voraussetzungen der traditionellen Diagnose nicht erfüllt sind. Speziell die prädiktive Simulation des Normal- und Sicherheitsverhaltens skaliert in diesem Szenario nicht aufgrund der Berechnungskomplexität („state space explosion“). Diese Probleme werden durch separate Diagnosemodelle mit erhöhtem Abstraktionsgrad umgangen, was jedoch Auswirkungen auf den Modellierungsprozess hat.

## 2 Diagnose als Prozess

Das Konzept einer *Anlagendiagnose* von Automatisierungssystemen geht weit über die Anwendung einer diagnostischen Methode hinaus. Der Diagnoseprozess integriert Aufgaben und Ergebnisse aus vielen Phasen, u.a. Komponentenentwicklung und Anlagenerstellung, Erzeugung und Verwaltung von Diagnosemodellen, technische Dokumentation, Laufzeitdiagnose, Verteilung und Visualisierung von Ergebnissen, Ableitung und Unterstützung von Instandsetzungsmaßnahmen und Feedback von Erkenntnissen. Es können verschiedene Kompetenzbereiche identifiziert werden [2], die durch entsprechende Fachleute besetzt sind und auf die sich die einzelnen Teilschritte der Beschaffung, Verwaltung und Verarbeitung von diagnoserelevanten Daten verteilen (s. Abb. 1).

Bei der Einführung modellbasierter Methoden entstehen oft aufgabenoptimierte Modell- und Werkzeugsammlungen. („Insellösungen“). Für einen durchgängigen Diagnoseprozess müssen jedoch auch die Lücken zwischen den Modellierungseinseln überbrückt werden, von der Datenbeschaffung bis zur Online-Auswertung von Diagnosemeldungen.

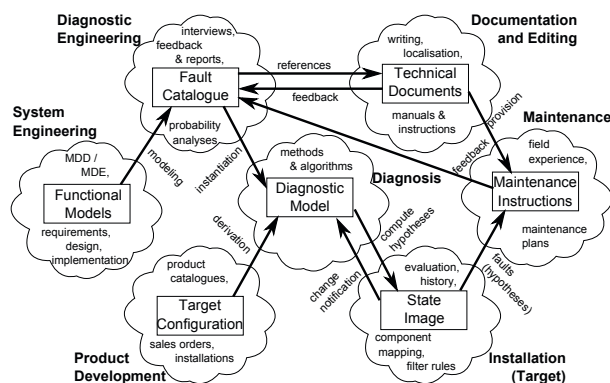


Abbildung 1: Diagnoseprozess und Kompetenzzentren (vgl. [2])

Die Nutzung von Daten und Prozessartefakten zu Diagnosezwecken kann prinzipiell auf zwei Wegen verbessert werden. Zum Einen durch Vielseitigkeit, d.h. durch die Vereinheitlichung von Konzepten und Daten-

modellen. Zum Anderen durch bewusste Abgrenzung und Schaffung dokumentierter Schnittstellen entlang identifizierter Abhängigkeiten.

In unserem Plädoyer für domänenspezifische Modellierung und abgegrenzte Schnittstellen stellen wir fest: Für verschiedene Zielsetzungen braucht es verschiedene Modelle mit einem dem Modellierungszweck angepassten Fokus und Abstraktionsgrad.

### 3 Erstellung von Diagnosemodellen

Bei der Komponentenentwicklung steht die Implementierung der geforderten Funktion und die lokale, sichere Reaktion auf mögliche Fehler und Ausfälle im Vordergrund. Eine *vorauseilende* Erweiterung von Entwurfsmodellen um Informationen, die möglicherweise für eine Anlagendiagnose relevant sind, stellt aus Entwicklersicht einen signifikanten Overhead dar.

Aus Sicht der Diagnose beinhalten Entwurfsmodelle für Komponenten viele Details, die gemäß den Diagnoseanforderungen auf Anlagenebene nicht relevant sind oder aufgrund der eingeschränkten Systembeobachtbarkeit nicht erkennbar bzw. unterscheidbar sind.

Insgesamt ist die Übernahme von Entwicklungsdaten für die Anlagendiagnose praktisch schwer umsetzbar. Schon die Betrachtung der Entitäten offenbart Unterschiede in den Anliegen: Diagnose reduziert die Betrachtung auf tauschbare Einheiten, nimmt aber andererseits betriebliche Faktoren hinzu, insbesondere laufende Betriebsprozesse und -konfigurationen, deren Abbildung über die technische Funktion hinausgeht (z.B. Einbindung „virtueller“ Komponenten).

In einem Projekt zur Anlagendiagnose in der Bahnautomatisierung setzen wir daher auf eine aufgabenspezifische Modellierung. Entwurfsmodelle und Dokumentation dienen als Referenz, aber diagnoserelevante Daten (Fehlerlisten/-modelle, Störungsverhalten und Reaktionen) werden separiert. Der zusätzliche Modellierungsaufwand kann durch die Wahl einer geeigneten Modellart minimiert werden. Dafür kommen symptom-basierte, modulare Kausalmodelle [3] zum Einsatz, die im Wesentlichen auf das Störungsverhalten beschränkt bleiben. Aus Prozesssicht wird eine Schnittstelle zur Systementwicklung und den anderen mit Diagnose und Wartung befassten Kompetenzzentren benötigt.

### 4 Kausale, symptom-basierte Diagnose

Um den Anforderungen im industriellen Umfeld gerecht zu werden, konzentrieren wir uns auf die Dokumentation des Diagnosewissens und die deduktive (erklärende) Analyse von abnormalen Verhalten, Systembeobachtungen und kausaler Beziehungen. Durch azyklische Modellstrukturen bleibt der Analyseaufwand zur Laufzeit beherrschbar.

Die Analyse der *Symptom-Propagation und Transformation* (SPT) [3, 4] beruht auf der Annahme, dass lokale Fehler und Störungen einer Komponente zu beobachtbaren Abweichungen an den Schnittstellen führen. An den medizinischen Begriff angelehnt, können

technische Symptome für jede Art von abnormalem Verhalten stehen, z.B. Hardwareausfälle, Softwarefehler, Eigendiagnosemeldungen oder physikalische Effekte. Durch die funktionale oder physische Kopplung beeinflussen diese Symptome benachbarte Komponenten (Propagation), welche ihrerseits auf Störungen an eingehenden Schnittstellen mit neuen Symptomen an ausgehenden Schnittstellen reagieren können (Transformation). So ergeben sich verzweigte Kausalketten in einem Netzwerk aus Komponenten. Auch wenn der unmittelbare Fehler bereits lokal behandelt wird, so erlaubt das Wissen über die sekundären Systemreaktionen die schnelle Fehlereingrenzung und -behebung.

In der Entwurfsphase wird die Erzeugung und Transformation von Symptomen separat für jeden Komponententyp durch logische Regeln beschrieben (vgl. [4]). Die an einer Schnittstelle sichtbaren Symptome richten sich nach der Art der Abhängigkeit, wobei auch hier diagnostische Schnittstellen über die Betrachtung der (Daten-) Kommunikation an physikalischen Schnittstellen hinausgehen. Symptome lassen sich aus den Anforderungen und Erwartungen an die Schnittstelle bzw. aus der Verletzung derselben ableiten. Sie zählen die Modi auf, wie die Bereitstellung bestimmter Funktionen, Daten, Eigenschaften, Mittel usw. eingeschränkt, gestört oder eingestellt werden könnte. Die formale Dokumentation des abnormalen Komponentenverhaltens und beobachtbarer Symptome ist die Basis für automatisierte Analysen und wird durch einen *Xtext*-basierten Editor [3] unterstützt.

### 5 Schlussfolgerung

Die domänen- und aufgabenspezifische Modellierung eignet sich gut zur Unterstützung des mehrstufigen Prozesses einer Anlagendiagnose, da der Effizienzgewinn die Nachteile überwiegt. In Fallstudien zur Diagnostizierbarkeit von Subsystemen (Weichensteuerung, Achszähler) konnte die industrielle Anwendbarkeit erfolgreich gezeigt werden.

### Literatur

- [1] DAVIS, Randall ; HAMSCHER, Walter: Model-based reasoning: Troubleshooting. (1988)
- [2] KLAR, Dennis ; HUHN, Michaela ; GRÜHSER, Jochen: Diagnosis in Rail Automation: A Case Study on Megamodels in Practice. In: *7. MBEES Dagstuhl-Workshop*, 2011
- [3] KLAR, Dennis ; HUHN, Michaela ; GRÜHSER, Jochen: Symptom Propagation and Transformation Analysis: A Pragmatic Model... In: *ETFA, 16th IEEE Int. Conf.* Toulouse, 2011
- [4] KLAR, Dennis ; HUHN, Michaela: Diagnosis and Diagnosability Based on a Symptom Propagation and Transformation Model. In: *ICIT, 13th IEEE Int. Conf.* Athen, 2012