Kurzfassung der Dissertation

Fehlertolerante Steuerung von nichtdeterministischen Eingangs-Ausgangsautomaten

Yannick Nke
Lehrstuhl für Automatisierungstechnik und Prozessinformatik

Bei ereignisdiskreten Systemen existieren, im Gegensatz zu kontinuierlichen und hybriden Systemen, im Wesentlichen nur heuristische Ansätze zur Verbesserung der Verlässlichkeit technischer Systeme. Der hier vorgestellte Ansatz ist modellbasiert und beruht auf einer ereignisdiskreten Betrachtung des fehlertoleranten Regelkreises in dem die Regelstrecke und die Steuerung mittels nichtdeterministischer Eingangs-Ausgangsautomaten modelliert werden. Beide Komponenten reagieren auf Eingangsereignisse mit Ausgangsereignissen und internen Zustandswechseln. Die konsistenzbasierte Diagnose ermittelt den aufgetretenen Fehler anhand der gemessenen Eingaben und Ausgaben der Regelstrecke. Wird ein Fehler identifiziert, so erfolgt durch die Rekonfiguration eine Anpassung bzw. ein Neuentwurf der Steuerung unter Berücksichtigung struktureller und analytischer Freiheitsgrade, sodass der rekonfigurierte Regelkreis die Spezifikation des nominellen Regelkreises erfüllt.

In dieser Dissertation wird eine Methode vorgestellt, mit der eine ereignisdiskrete Steuerung so angepasst werden kann, dass der fehlerbehaftete Regelkreis eine an ihn gestellte Spezifikation weiterhin einhält.

Ein wichtiges Ergebnis dieser Dissertation ist die Entwicklung und Erprobung einer neuen Steuerungsentwurfsmethode für ereignisdiskrete Systeme. Dabei wird anfänglich eine Spezifikation in Form eines Endzustands, einer Zustands- oder einer Ausgangsfolge formuliert. Alle Transitionen und Zustände des Automaten der Strecke, die mit der Spezifikation inkonsistent sind, werden entfernt. Daraus entsteht ein reduzierter Automat, dessen Eingangs-Ausgangsverhalten invertiert wird um die maximal zulässige Steuerung zu erhalten. Für die Analyse des Regelkreises im nominellen Fall sowie im Fehlerfall wird eine geeignete Struktur eingeführt, die eine implementierungsfreundliche Umsetzung des Steuergesetzes erlaubt.
Weiterhin wird das Verhalten der fehlerbehafteten Strecke durch die Einführung von Fehlerfunktionen für Aktor-, Sensor- und systeminterne Fehler und Ausfälle modelliert. Damit ist es möglich das Systemverhalten unter dem Einfluss von gleichzeitig wirkenden Fehlern systematisch abzuleiten.

Die Hauptergebnisse dieser Dissertation sind die Methoden der formalen Trajektorieänderung und Eingangs-Ausgangsanpassung mit denen Fehler verdeckt werden können und die Bedingungen unter denen dies möglich ist. Diese formalen Rekonfigurationsmethoden lassen sich sowohl off-line als auch on-line durchführen. Für den on-line Betrieb hat sich eine Unterteilung in eine Vorwärts- und Rückwärtsrekonfiguration als zweckmäßig erwiesen. Je nach Rekonfigurationsrichtung sucht der Algorithmus in polynomialer Komplexität nach Transitionen zu zukünftigen oder zu früheren fehlerfreien Zuständen.

Es wurden notwendige und hinreichende Bedingungen zur Steuerbarkeit einer fehlerbehafteten Strecke jeweils für Aktorausfälle, sowie Aktor- und Sensorfehler hergeleitet. Bei Aktorausfällen konnte gezeigt werden, dass die Erfüllbarkeit der Spezifikation, gekoppelt mit einem redundanzbasierten Kriterium, die Rekonfigurierbarkeit der vorhandenen Steuerung gewährleistet. Bei Aktor- und Sensorfehlern hängt die Rekonfigurierbarkeit lediglich von der verklemmungsfreien Erfüllbarkeit der Spezifikation im fehlerbehafteten Regelkreis ab. Die Forderung nach Lebendigkeit des Regelkreises ist mittels des eingeführten Wohldefiniertheitskonzeptes untersucht worden. Die Methoden dieser Dissertation sind an verfahrenstechnischen Prozessen, an emulierten und realen Fertigungsanlagen des Lehrstuhls sowie an Pilotanlagen in der Industrie erprobt worden.