Automatisierung und Kreativität

Ist die Grenze beherrschbarer Komplexität in sicherheitskritischen Systemen erreicht?

Dr. Robert Hilbrich

1 Einführung

Das Ende der Ära der Lochkarten zur manuellen Programmierung war zugleich auch der Beginn eines deutlich erweiterten Aufgabenspektrums der Computersysteme. Neben ihrer Rolle als Laufzeitplattform und Ressourcenlieferant zur Ausführung von manuell entwickelten Codes, konnten sie im Zuge ihrer zunehmenden Leistungsfähigkeit auch die *Entwicklung* von Codes unterstützen. Mittlerweile ist die Softwareentwicklung ohne die Unterstützung von Computern nicht mehr sinnvoll durchzuführen. Computer transformieren manuell entwickelten Code aus Hochsprachen in Maschinensprache, sie analysieren die Codes auf Speicherlecks oder ungültige Ressourcenzugriffe und validieren deren Korrektheit mit Hilfe einer Vielzahl von Testfällen - alles weitgehend automatisch.

Nicht nur bei der Entwicklung von Software konnten sich Computersysteme als hilfreiche Assistenten emanzipieren. Mittlerweile ist auch die Entwicklung von Hardware zwingend auf den Einsatz von Computern angewiesen. So werden die komplexen Steuerungs- und Assistenzsysteme in Fahrzeugen und Flugzeugen beispielsweise nur noch mit Hilfe von Computersystemen entworfen. Dies ist notwendig, um die Komplexität der zu entwickelnden Systeme zu beherrschen und zugleich auch ökonomischen Randbedingungen zu genügen.

Obwohl sich die Leistungsfähigkeit der Rechentechnik und damit auch ihr Nutzen bei der der Unterstützung von Entwicklungstätigkeiten seit den Lochkarten deutlich erhöht hat, ist die grundlegende Arbeitsteilung zwischen dem Menschen und der Maschine erhalten geblieben. Während der menschliche Entwickler die *kreativ-konstruktiven* Tätigkeiten bei der Synthese von Komponenten und Artefakten übernimmt, sind die *analytischen* und *automatisierbaren* Tätigkeiten dem Computer vorbehalten. So übernimmt der Mensch die schöpferischen Tätigkeiten, durch die er etwas Neues und Originelles erschafft. Die stupiden und repetitiven Tätigkeiten der Entwicklung werden dagegen durch den Computer übernommen und von ihm entsprechend einer vordefinierten Art und Weise in identischer Manier ausgeführt. Aufgrund dieser Arbeitsteilung ist die Komplexität der zu entwickelnden Systeme durch die menschliche Verarbeitungskapazität begrenzt, denn

jedes Entwicklungsvorhaben ist zunächst auf die Durchführung von kreativ-konstruktiven Tätigkeiten angewiesen.

Bei der Entwicklung von komplexen sicherheitskritischen Systemen, zum Beispiel der Steuerungssysteme an Bord eines modernen Flugzeugs, sehen sich Entwickler mittlerweile mit der Herausforderung konfrontiert, auch kreativ-konstruktive Tätigkeiten automatisieren zu müssen. Dies ist einerseits die Folge einer stark gestiegenen Komplexität in den funktionalen Anforderungen der Systeme in Verbindung mit einer exponentiell gestiegenen Komplexität der technologischen „Bausteine“, die für die Synthese zur Verfügung stehen. Die vollständige und fehlerlose Berücksichtigung aller Anforderungen bei der Verwendung der technologischen Bausteine übersteigt bereits heute in vielen Fällen die menschliche Verarbeitungskapazität der Entwickler.

Andererseits ist der Drang zur Automatisierung der kreativ-konstruktiven Tätigkeiten auch eine Folge der hohen Anforderungen an die funktionale Korrektheit und Zuverlässigkeit dieser Systeme. In der Praxis lässt sich die vollständige Korrektheit eines derartigen Systeme mittlerweile nicht mehr allein durch die extrinsische Beobachtung und Analyse von dessen Verhalten überprüfen. Aufgrund der Vielzahl der zu prüfenden Systemzustände ist ein derartiges Vorgehen zum vollständigen Analyse in der Praxis nicht länger ökonomisch sinnvoll. Daher muss die Korrektheit eines Systems verstärkt auf der Grundlage seines *Konstruktionsprozesses* nachgewiesen werden. Die Automatisierung des Konstruktionsprozesses kritischer Artefakte ist daher eine zentrale Herausforderung für die ingenieurwissenschaftliche Forschung in diesem Bereich, um die Weiterentwicklung dieser Klasse von Systemen zu ermöglichen und zugleich auch zukünftig deren Zuverlässigkeit und Korrektheit zu gewährleisten.

Die zugrunde liegende Dissertation befasst sich mit der automatisierten Konstruktion eines zentralen Artefakts sicherheitskritischer Systeme: der Zuweisung von Ressourcen, zum Beispiel der Rechenzeit auf einem Prozessor oder einem Teil des Arbeitsspeichers, zu den einzelnen Softwarekomponenten – oder anders formuliert: der Platzierung der Softwarekomponenten auf den Ressourcen des Systems. Diese Zuweisung ist scheinbar unspektakulär, doch dieser Eindruck trügt. Eine „richtige“ und „ausreichende“ Zuweisung von Ressourcen, ist für das Gesamtsystem *essentiell*. Sie ist die Grundvoraussetzung dafür, dass zeitkritische Steuerungsmodule, zum Beispiel das Airbagsteuergerät im Auto, zum „richtigen“ Zeitpunkt über „genügend“ Ressourcen zur Abarbeitung ihrer Steuerungslogiken verfügen.

Mit der Einführung von modernen „Mehrkern-“ Prozessoren, die eine parallele Ausführung von Softwarekomponenten erlauben, wurde die Möglichkeit zu einer starken Funktionsverdichtung in der Architektur von sicherheitskritischen Systemen geschaffen. Ein Mehrkern-Prozessor kann – im Gegensatz zu einem klassischen Ein-Kern-Prozessor – verschiedene Softwarekomponenten zur gleichen Zeit ausführen, so dass Geräte eingespart und damit die Effizienz des Systems gesteigert werden können. Die Ressourcenzuweisung ist damit nicht nur eine Grundvoraussetzung für die korrekte Funktionsweise des Systems, sondern zugleich auch der zentrale Ansatzpunkt für Optimierungen zur Steigerung der Ressourceneffizienz.

Die Synthese einer solchen Zuweisung erfordert eine vollständige Koordination aller Ressourcenzugriffe der Softwarekomponenten bereits zum Zeitpunkt der Entwicklung. Ihre Erstellung ist äußerst aufwändig und fehlerträchtig, denn sie ist sowohl mit der Komplexität der Anforderungen *aller* Softwarekomponenten als auch der Komplexität *aller* Ressourcen der Hardwareplattform konfrontiert. Während die Ressourcenzuweisung bei realen Systemen in der Vergangenheit noch manuell konstruiert werden konnte, ist spätestens mit der Einführung von Mehrkern-Prozessoren ein Komplexitätsniveau erreicht, bei dem eine Fortsetzung tradierter Vorgehensweisen nicht länger zielführend ist.

Vor dem Hintergrund dieser Herausforderung wird in der zugrunde liegenden Dissertation ein automatisiertes Verfahren zur Konstruktion einer solchen Ressourcenzuweisung für Mehrkernprozessoren entwickelt und anhand von zwei Fallbeispielen für komplexe Systeme aus der Luft- und Raumfahrt erprobt.

Mittlerweile wird dieses Verfahren in leicht angepasster Form bei einem Hersteller ziviler Flugzeuge für die Optimierung der Systemarchitektur eines Flugzeugtyps eingesetzt. Durch die Verwendung dieses Verfahrens konnte die benötigte Zeitdauer für die Konstruktion einer vollständigen und fehlerfreien Zuweisung von ca. 12-15 Monaten auf einen Zeitraum von etwa 5 Minuten reduziert werden. Die Kürze der Konstruktionsdauer ermöglichte erstmals die Synthese einer Vielzahl unterschiedlicher Zuweisungen, so dass erstmalig auch Entwurfsalternativen zur Optimierung verglichen und letztendlich Geräte eingespart werden konnten.

In den folgenden Abschnitten ...

2 Ergebnisse der Dissertation

Hier kommt der Inhalt der Dissertation etwas stärker im Detail; dazu die Ergebnisse ...

3 Gesellschaftliche Bedeutung

- Zunächst kann damit die Entwicklung von Systemen beschleunigt werden
- Systeme können optimiert werden, so dass weniger Ressourcen benötigt werden
- Weniger Fehler im System
- ...

Aber, diese Arbeit ist ein guter Gegenstand, um Fragen nach der Beherrschbarkeit heutiger Technologien zu stellen und zu diskutieren

- Was sind die Nachteile die sich daraus ergeben?

- Ist es nicht sinnvoll, wenn sich Menschen so lange mit den Anforderungen beschäftigen?
- Sollten wir Dinge konstruieren und nutzen, deren Aufbau das Verständnis des Menschen übersteigt?
- ...

4 Zusammenfassung