Positionsstatement: Zertifizierungsargumentationen mit mathematischer Präzision

Hardi Hungar

F&E-Bereich SC
OFFIS – Institut für Informatik
Escherweg 2
26121 Oldenburg
hungar@offis.de

Abstract: In gegenwärtiger Praxis haben Argumentationen, mit denen Zertifizierungen sicherheitskritischer Systeme begründet werden, die Qualität juristischer Beweise. Hier wird die Meinung zum Ausdruck gebracht, dass diese langfristig in einer stärkeren, mathematischen Präzision zu erbringen sein werden.

1 Ausgangslage

In den der Zertifizierung unterliegenden Bereichen erreicht die Qualität der Produkte unter Sicherheitsgesichtspunkten bereits heute eine sehr hohe Qualität: Unfälle sind weit seltener auf technisches Versagen zurückzuführen als auf Unzulänglichkeiten des Systemzusammenhangs oder der Bedienung. Gleichwohl ist vom rigorosen Standpunkt aus die Qualität der Zertifizierungszusicherung als eingeschränkt zu bewerten. Dies wird auch in der Formulierung von Normen deutlich, wo schwächere Argumentationen in Ermangelung anwendbarer formalerer Methoden zugelassen werden. Vor dem Hintergrund der enormen Fortschritte, welche es in der Anwendung rigoroser Techniken auf Systeme nichttrivialer Größenordnung in den letzten Jahrzehnten gegeben hat, wird deutlich, dass der Druck auf die Entwicklung, ein noch höheres Qualitätsargument zu liefern, zunehmen wird: Weil es möglich (und wirtschaftlich vertretbar) sein wird, werden in ferner, jedoch absehbarer Zukunft, ein großer Teil von Sicherheitsargumentationen im mathematischen Sinn formal geführt werden müssen.

2 Indikationen

Es gibt eine Vielzahl von Beispielen, welche den Fortschritt exakter Methoden bei der Sicherheits- oder Zuverlässigkeitsanalyse dokumentieren. So werden im Hardwarebereich formale Methoden schon routinemäßig angewendet. Ein herausragendes Beispiel ist die Verifikation des Prozessorkerns des Tricore 2 der Firma Infineon innerhalb des Verisoft-Projektes.

Aber auch auf Anwendungsebene haben Verifikationsmethoden Einzug gehalten, wie der erfolgreiche Einsatz von modelcheckbasierten Analysewerkzeugen etwa der Firma OSC für die Entwurfswerkzeuge Statemate, Stateflow und ASCET zeigt.

3 Wege zur Präzision

An der prinzipiellen Machbar formaler Verifikation besteht schon lange kein Zweifel mehr. Jedoch ist genauso klar, dass als unrealistisch anzusehen ist, mit Hilfe automatischer Beweiser die Ergebnisse heute gängiger Entwurfsprozesse behandeln zu können. Eine Vielzahl von Maßnahmen erscheinen erforderlich, um die Vision kompletter Verifikation Wirklichkeit werden zu lassen. Der Verfasser dieser Zeilen erhebt nicht den Anspruch, den Weg zu kennen und anderen aufzeigen zu können. Jedoch lassen sich etliche Maßnahmen aufzählen, die mit einiger Wahrscheinlichkeit einen wichtigen Beitrag liefern können.

- Verwendung abgesicherter Architekturen, etwa für Redundanzkonzepte, Zeitverteilung, zuverlässige Kommunikation
- Dedizierte Programmiersprachen und Modellierungswerkzeuge, welche die Beherrschbarkeit der Artefakte und nicht die Mächtigkeit und Vielfalt der Konzepte in den Vordergrund stellen.
- Hardwarearchitekturen und Betriebssysteme mit vorhersagbarem Ressourcenverbrauch und insbesondere zuverlässigem Zeitverhalten
- Komponenten mit zugesicherten Eigenschaften (Wiederverwendung, Modularisierung)
- Verzahnung automatischer und interaktiver Beweismethoden
- Evidenzproduzierende Verifikation (z.B. Modelchecker, welche Fehlerfreiheit nicht nur feststellen, sondern auch begründen)
- Verifikation von Codegenerierung und Übersetzung (z.B. Übersetzer**lauf**verifikation für Produktcode, im Gegensatz zu schwieriger zu verifizierenden Übersetzern)

4 Zeithorizont

Eine Voraussage zu treffen ist sicherlich wenig mehr als schlichtes Raten, jedoch erscheinen zwanzig Jahre als nicht unrealistischer Zeitraum für die weitgehende Ablösung heutiger Vorgehensweisen durch formal abgesicherte, wenn dieses Thema eine Gemeinschaft von Forschern findet, welche sich ihres annehmen und welche für ihre Arbeiten Rückhalt bei öffentlichen und privaten Organisationen finden.