Sven Söhnlein: **Quantitative Bewertung der Softwarezuverlässigkeit komponentenbasierter Systeme durch statistische Auswertung der Betriebserfahrung**

Promotion: Friedrich-Alexander-Universität Erlangen-Nürnberg, Technische Fakultät
Erstgutachter: Prof. Dr. Francesca Saglietti, Friedrich-Alexander-Universität Erlangen-Nürnberg
Zweitgutachter: Prof. Dr. Dr. h.c. Mario Dal Cin, Friedrich-Alexander-Universität Erlangen-Nürnberg
Datum der Prüfung: 10. September 2010
Veröffentlichung: Arbeitsberichte des Department Informatik, Friedrich-Alexander-Universität Erlangen-Nürnberg, Band 43, Nummer 1, Oktober 2010. ISSN 1611-4205.

Kurzfassung:

Angesichts der schwerwiegenden Folgen eines Versagens ist für den Einsatz von Softwaresystemen in sicherheitskritischen Anwendungsbereichen ein rigoroser Nachweis hoher Zuverlässigkeit angebracht und oft auch vorgeschrieben. Prinzipiell bieten hier statistische Testverfahren einen adäquaten Ansatz zur quantitativen Zuverlässigkeitsbewertung solcher Systeme. Die praktische Anwendung (vor allem im Bezug auf neue Systeme) ist jedoch nicht frei von Kritik, denn die Probleme in der konkreten Umsetzung liegen in erster Linie am enormen Testaufwand zum Nachweis domänenspezifischer Vorgaben. Für bereits erprobte Komponenten kann dieser Aufwand durch die Auswertung vorliegender Betriebserfahrung zumindest theoretisch stark verringert werden. Hierzu mag die während einer vorangegangenen Test- oder Betriebsphase beobachtete fehlerfreie Funktionsweise intuitiv auf ein verlässliches Produkt hindeuten, jedoch fehlten bisher Methoden, um einen quantitativen Nachweis auf Basis der gewonnen Betriebserfahrung zu erbringen, bzw. um komponentenspezifische Zuverlässigkeitskenngrößen zu systembezogenen Gesamtaussagen zu kombinieren. Vor dem Hintergrund dieser Problematik wurden im Rahmen dieser Arbeit mehrere Beiträge geliefert: Zum einen wurden Ansätze und Verfahren hergeleitet, die eine weitestgehend verlustfreie, architekturspezifische Kombination der mit Komponenten gewonnenen Zuverlässigkeitskenngrößen erlauben, wobei darüber hinaus auch Techniken zur Sensitivitätsanalyse und zur Optimierung des Nachqualifizierungsprozesses erarbeitet wurden. Zum anderen wurde eine allgemeine Leitlinie zur Erfassung, Analyse und Auswertung statistisch relevanter operationaler Daten erstellt, welche die wesentlichen Schritte zur Bestimmung von Zuverlässigkeitskenngrößen auf Grund der beobachteten Betriebserfahrung beschreibt. Darüber hinaus wurde die Umsetzung dieser Leitlinie anhand einer Getriebesteuerungssoftware im Rahmen einer industriellen Forschungskooperation praktisch erprobt.