Effiziente Safety-Analysen durch Kombination von Methoden

Prof. Dr. Bettina Buth
Department Informatik
HAW Hamburg

Durchgängige Methoden für Entwicklung und Analyse von Systemen und speziell Software sind ein wesentliches Ziel des Systemengineering. Dies gilt insbesondere für den Bereich der Analysen von sicherheitskritischen Aspekten eines Systems, also dort wo ein Systemfehler zu ernsthaften Gefährdung von Menschenleben oder Firmeninteressen führen kann. State-of-the-Art Entwicklungsstandards wie etwa die im Luftfahrt- oder Raumfahrtbereich oder in der Automobilindustrie, der Medizintechnik oder dem Eisenbahnwesen definieren Risikokategorien und Modelle für Sicherheitsebenen (SIL) und leiten daraus Anforderungen an die Entwicklung wie auch die Qualitätssicherung ab. Dennoch fehlen heute noch an vielen Stellen durchgängige Methoden zur einheitlichen Sicherstellung dieser Anforderungen auf System- und Softwareebene.

Analysen für Systemzuverlässigkeit (Reliability, Safety, Availability) und die Einstufung der Kritikalität eines System und seiner Komponenten liefern Informationen, die rückwirkend in die Architektur und das Design eines Systems einfließen sollen und müssen. Aus diesem Grunde ist eine frühzeitige und entwicklungsbegleitende Analyse empfohlen, wird aber noch selten durchgeführt. Der hier vorgestellte Ansatz zielt auf eine solche entwicklungsunterstützende Qualitätssicherung und speziell auf fokussierte Verifikations-, Valdiations- und Testaktivitäten durch die Kombination verschiedener etablierter Methoden. Eine starke Motivation für diese Kombination von Methoden sind die im allgemeinen relativ beschränkten Ressourcen für die angesprochenen Tätigkeiten, die bestmöglich verwendet werden sollen.

Exemplarisch wird hier die Weiterverfolgung von systemseitigen Fehlerbaumanalysen (FTA) in der Software und ihre Ergänzung durch Failure Modes and Effects Analysis (FMEA) vorgestellt. Entgegen der gängigen Meinung, dass Fehlerbaumanalysen für Software wegen der großen Komplexität nicht praktikabel sind, konnte in diesem Fall ein Ansatz, der SW FTA und SW FMEA kombiniert, erfolgreich für die Sicherheitsanalyse im Rahmen einer Bahnanwendung durchgeführt werden. Diese Analyse erlaubt neben der Anknüpfung an den Systemfehlerbaum auch eine Fokussierung von Verifikations-, Validations- und Testaufgaben auf die so identifizierten kritische Bereiche der Software.

Der Vortrag soll zunächst eine Motivation für den Ansatz der Methodenkombination liefern und zeigt dann anhand eines Beispiels wie die Methode angewandt werden kann. Abschließend wird ein Ausblick darüber gegeben welche weiteren Methodenkombinationen in dem Zusammenhang denkbar sind und welche Werkzeuge in dem Rahmen eingesetzt werden können.

Autor	Prof. Dr. Bettina Buth
Firma	Hochschule für Angewandte Wissenschaften Hamburg (HAW), Fakultät Technik und Informatik, Department Informatik
Anschrift	Berliner Tor 7, 20099 Hamburg
Email	buth@informatik.haw-hamburg.de
Telefon	++49-421-3491946 oder ++49-40-42875-8150