Risikobasiertes statistisches Testen

Fabian Zimmermann, Robert Eschbach, Johannes Kloos, Thomas Bauer
{fabian.zimmermann, robert.eschbach, johannes.kloos, thomas.bauer}@iese.fraunhofer.de

***Abstract*— In dieser Arbeit stellen wir erste Ideen für eine Methode zur automatischen Ableitung risikoreicher Testfälle vor. Diese Testfälle werden aus Modellen abgeleitet, die speziell zum Testen erstellt wurden. Das hier vorgestellte Verfahren ist eine Anpassung des modellbasierten statistischen Testens für risikoreiche Systeme. Dabei verwenden wir Markov-Ketten, die das Nutzungsverhalten beschreiben. Diese Markov-Ketten werden so verändert, dass nur risikoreiche Testfälle, die eine realistische Nutzung des Systems darstellen, erzeugt werden. Dadurch kann die Zuverlässigkeit des Systems in kritischen Situationen ermittelt werden.**

1. Motivation

Die weite Verbreitung von sicherheitskritischen Systemen macht es notwendig, die Risiken, die von diesen Systemen ausgehen, zu ermitteln und zu beherrschen. Dafür müssen schon während der Entwicklung potentielle Gefährdungen aufgedeckt und ihnen entgegengewirkt werden. Die Analyse von Risiken darf aber nicht auf die Entwicklungsphase beschränkt bleiben. Vielmehr ist es auch Sache der Qualitätssicherung, nachzuweisen, dass ein System gewisse erforderliche Sicherheitsfunktionen erfüllt. Dazu müssen Testfälle abgeleitet werden, die alle potentiellen Risiken des Systems adressieren. Mit steigender Komplexität und steigenden Qualitätsanforderungen erhöht sich auch der Aufwand des Testens, so dass manuelles Testen nicht mehr praktikabel ist. Aus Modellen lassen sich Testfälle automatisch erzeugen. Dabei sollen vor allem solche Testfälle erzeugt werden, die besonders kritische Situationen im System hervorrufen sollen. Diese risikoreichen Situationen lassen sich durch gängige Risikoanalysetechniken bestimmen. In dieser Arbeit werden erste Ansätze zur Veränderung von Testmodellen vorgestellt. Aus diesen neuen Testmodellen lassen sich nur noch risikoreiche Testfälle ableiten.

2. Related Work

Verschiedene Arbeiten verwenden den Begriff risikobasiertes Testen. Dabei werden nicht immer nur Risiken, die durch das zu testende System verursacht werden, sondern auch Management-Risiken betrachtet [1],[2]. Bei unserem Ansatz wird dagegen ausschließlich das Sicherheitsrisiko betrachtet, das von einem Produkt ausgeht. In [3] werden Testfälle für den Regressionstest nach Risiko priorisiert. Im Gegensatz dazu wollen wir Risiko schon als Kriterium für die Generierung und nicht erst zur Priorisierung von Testfällen verwenden. In [4] wird ein Ansatz beschrieben, der Risiko als Kriterium für die Generierung von Testfällen aus Testmodellen verwendet. Unsere Arbeit ist eine Verfeinerung dieses Ansatzes.

3. Modellbasiertes statistisches Testen

Unsere Arbeit ist eine Erweiterung des modelbasierte statistischen Testens (MBST). MBST [5] ist ein funktionsorientierter Ansatz, der zur Validierung des Systems dient. Die dort abgeleiteten Tests werden verwendet, um Aussagen über die erwartete Zuverlässigkeit des getesteten Systems zu treffen. Dabei wird ausgehend von den Anforderungen ein Modell des Systems mit allen möglichen Eingaben und den zu erwarteten Ausgaben auf einem gewissen Abstraktionsniveau erstellt. Dies kann beispielsweise mit Hilfe der sog. sequenzbasierten Spezifikation geschehen[6].
Dieses Modell lässt sich zu einem Testmodell erweitern. Das Testmodell besitzt ausgezeichnete Zustände für Initialisierung (START) und Ende (EXIT). START ist der Initialzustand, in dem sich das System zu Beginn der Ausführung eines Testfalls befindet. Der Endzustand EXIT markiert das Ende eines Testfalls. Er kann von allen Zuständen, in denen das Beenden eines Testfalls möglich sein soll, über eine Kante mit dem Stimulus *Exit* erreicht werden. Ein Testfall ist ein beliebiger Pfad durch das Modell von START nach EXIT.
Indem an alle Transitionen im Modell Wahrscheinlichkeiten annotiert werden, erhält man ein Markov-Benutzungsmodell. Dadurch wird eine Wahrscheinlichkeitsverteilung auf allen möglichen Stimuli-Sequenzen induziert. Aus ihr lassen sich zufällige Testfälle bezüglich dieser Verteilung ableiten. Ein Testfall ist ein zufälliger Pfad von START nach EXIT durch die Markov-Kette. Nach der Durchführung derart abgeleiteter Testfälle lassen sich statistische Aussagen über die Zuverlässigkeit des gestesteten Systems treffen[7]. Sobald das Testmodell erstellt ist, können Ableitung, Durchführung und Auswertung der Testfälle automatisiert erfolgen. Hierbei wird allerdings Risiko nicht als Auswahlkriterium für die Testfallableitung beachtet.

4. Beispiel

Als kurzes Beispiel zur Veranschaulichung dient eine einfache Alarmanlage.

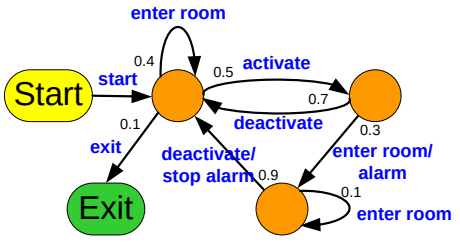

Abbildung 1: Testmodell der Alarmanlage

Die Anlage soll einen Alarm auslösen, falls sie aktiviert ist und jemand den überwachten Raum betritt. Das Testmodell dieser Anlage (Abb. 1) enthält alle möglichen

Eingaben und die zu erwartenden Ausgaben. Jede Transition ist mit einer Wahrscheinlichkeit aus einem Nutzungsprofil versehen. Dadurch können realistische Testfälle abgeleitet werden.

5. Unser Ansatz

Unser Ziel ist es, Testfälle abzuleiten, die ein bestimmtes Risiko adressieren. Trotzdem sollen die meisten Testfälle eine realistische Benutzung des Systems darstellen. Dadurch sind Zuverlässigkeitsaussagen für die risikoreichen Transitionen möglich. Es hat sich gezeigt, dass ein bestimmtes Risiko in unseren Modellen häufig an ganz bestimmten Transitionen auftaucht.
Um Testfälle abzuleiten, die dieses Risiko adressieren, verändern wir unser Modell *M*, so dass nur risikoreiche Testfälle abgeleitet werden können. Die Idee dabei ist, dass im neuen Modell *M'* nur Pfade nach EXIT zugelassen sind, die eine als risikoreich identifizierten Transitionen enthalten. Des Weiteren verlangen wir, dass jeder Pfad von *M'* auch ein Pfad im alten Modell *M* ist. Dies garantiert, dass das neue Modell *M'* eine echte Verfeinerung von *M* ist.

Der folgenden Algorithmus berechnet aus *M* das neue Testmodell *M'* erstellen:

1. *M* wird zweimal kopiert. Dadurch erhält man die Modelle *A* und *B*
2. In *A* werden alle *Exit*-Transitionen und in *B* wird START entfernt
3. Alle risikoreiche Transitionen in *A* werden ersetzt durch Transitionen mit dem entsprechenden Endzustand in *B*
4. Alle Zustände in *A*, aus denen kein Pfad nach EXIT führt, werden entfernt
5. Alle Wahrscheinlichkeiten werden normiert

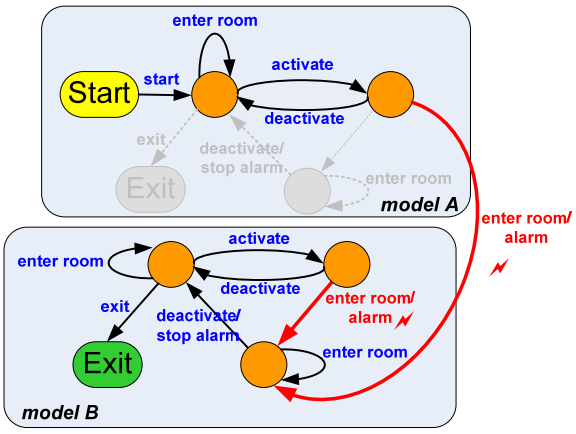

Abbildung 2: Neues Testmodell

Da sich in *A* keine Exit-Kanten befinden und Modell *B* nur über eine kritische Transition erreicht werden kann, muss jeder abgeleitete Testfall einen kritischen Testschritt enthalten.
Im Alarmanlagenbeispiel wollen wir das Risiko betrachten, dass kein Alarm ausgelöst wird, obwohl er eigentlich müsste. Dabei haben wir die Transition, die den Alarm auslösen soll, haben wir als kritisch identifiziert. Das Testmodell wird so verändert, dass jeder Testfall diese Transition mindestens einmal enthält. Abb. 2 zeigt das neue Modell, aus dem nur noch risikoreiche Testfälle abgeleitet werden können.

6. Zusammenfassung und Ausblick

In diesem Beitrag wurden erste Ideen zur Ableitung risikoreicher Testfälle beim modellbasierten statistischen Testen durch eine Modelltransformation entwickelt. Andere Heuristiken zur Ableitung ganz bestimmter risikoreicher Testfälle sind möglich. Als eine mögliche weitere Weiterentwicklung dieses Verfahrens könnten die Risiken verschiedener Transitionen klassifiziert werden. Bisher wird nur zwischen risikoreichen und risikolosen Transitionen unterschieden. Außerdem soll eine allgemeine Transformationstheorie für Testmodelle inkl. verschiedener Erhaltungssätzen entwickelt werden. So muss genauer untersucht werden welche Modellveränderungen erlaubt sind, um weiterhin gültige Zuverlässigkeitsaussagen zu erhalten. Hierfür sollen auch andere Transformationsoperatoren betrachtet werden. Die verschiedenen neuen Transformationsoperatoren sollen in Hinblick auf Effizienz und Effektivität hinsichtlich einer risikoorientierten Fehlersuche untersucht werden.

7. Danksagung

Diese Arbeit ist mit Unterstützung der BMBF/DLR-Projekte ViERforES (Förderkennzeichen: 01 IM08003 B) und D-Mint (Förderkennzeichen: 01 IS07001 E) entstanden.

8. Referenzen

[1] Bach, J., James Bach on Risk-Based Testing – How to conduct heuristic risk analysis, Software Testing & Quality Engineering November/December 1999, p. 23-28

[2] Redmill, F. 2004. Exploring risk-based testing and its implications: Research Articles. *Softw. Test. Verif. Reliab.* 14, 1 (Mar. 2004), 3-15.

[3] Chen, Y., Probert, R. L., and Sims, D. P. 2002. Specification-based regression test selection with risk analysis. In *Proceedings of the 2002 Conference of the Centre For Advanced Studies on Collaborative Research* (Toronto, Ontario, Canada, September 30 - October 03, 2002).

[4] Bauer, T., Stallbaum, H., Metzger, A., Eschbach, R. Risikobasierte Ableitung und Priorisierung von Testfällen für den modellbasierten Systemtest, SE09 München, 2008.

[5] S. Prowell, C. Trammell, R. Linger, J. Poore, *Cleanroom Software Engineering: Technology and Process, Addison-Wesley-Longman*, 1999.

[6] S. Prowell, J. Poore, "Foundations of sequence-based software specification", *IEEE Transactions of SoftwareEngineering*, Vol. 29, No. 5, May 2003, 417--429.

[7] S. Prowell, J. Poore, "Computing system reliability using Markov chain usage models", *Journal of Systems and Software*, Vol. 73, No. 2, October 2004, 215 - 225.