Nachweis von Sicherheitseigenschaften in modellbasierten Entwurfsprozessen

Thomas Peikenkamp

Bereich Sicherheitskritische Systeme, OFFIS,
Escherweg 2, 26121 Oldenburg
peikenkamp@offis.de

Abstract: Mit der zunehmenden Modellbildung und modellbasierten Entwicklung im Bereich sicherheitskritischer Systeme gewinnt die Frage Bedeutung, wie effizient und zeitgerecht der Nachweis der Sicherheit für Systeme geführt werden kann, die über lange (und zunehmend länger werdende) Entwicklungszeiträume hinweg (nur) als Modell vorliegen.

Ein modellbasierter Ansatz zur Führung des Nachweises von Sicherheitseigenschaften unterliegt dabei folgenden Rahmenbedingungen:

1. Während früher vor allem Hardware Gegenstand der Modellierung war, gibt es heute praktisch keine Technologien mehr, für die nicht entsprechende Modellierungsmethoden etabliert sind. Im Hinblick auf die zunehmende Integration dieser Technologien müssen die auf ihnen basierenden Systeme mit den ihnen eigenen Modellierungsmethoden erfassen werden können.
2. Die notwendige Ersetzbarkeit von Komponenten eines Systems erfordert, dass die Gleichwertigkeit nicht nur im Hinblick auf funktionale, sondern auch auf nicht-funktionale Eigenschaften bewertet werden kann.
3. Wiederverwendbarkeit als erklärtes Ziel des komponentenbasierten Entwurfs führt zum Einsatz von Komponenten, für die Sicherheitsanforderungen nicht oder nur in anderem Kontext nachgewiesen sind.
4. Die zunehmende Integration von Komponenten unterschiedlicher Zulieferer erfordert eine Entwurfmethodik, die gestattet, den Nachweis der Sicherheit auch über eine Vielzahl von Entwurfsschritten, verteilt auf nicht-triviale Supply-Chains zu führen.
5. Die Methodik muss adaptierbar sein im Hinblick auf die unterschiedlichen Durchdringungsgrade modellbasierter Entwicklungsmethoden im industriellen Entwicklungsprozess, wobei anzumerken ist, dass dieser Faktor nicht allein unternehmensabhängig ist, sondern aufgrund der Heterogenität der involvierten Teilsystem die Modellbildung für diese unterschiedlich stark ausgeprägt ist.
6. Mit der gerade durch die modellbasierte Entwicklung vorangetriebenen Verwendung von Entwicklungswerkzeugen und automatisierten Entwicklungsschritten muss der Nachweis der Sicherheit auch die Rolle dieser „Komponenten“ bei der Validation erfassen.

Dieser Beitrag zeigt auf, wie der Sicherheitsnachweis im modellbasierten Entwurfsprozess unter Berücksichtigung der obigen Rahmenbedingungen er-

folgen kann: Ein um nicht-funktionale Eigenschaften erweitertes Komponentenmodell für heterogene Systeme in Verbindung einer auf den modellbasierten Ansatz zugeschnittenen Erweiterung traditioneller Sicherheitsanalysetechniken garantieren dabei zu jedem Zeitpunkt des Entwurfs eine kohärente Sicht auf die Sicherheitseigenschaften eines Systems und seiner Komponenten.

1 Etablierung einer Safety-Sicht

Als eine Maßnahme zur Komplexitätsreduktion im modellbasierten Entwurf hat sich die sichtenorientierte Modellierung bewährt. Typische Sichten, die dabei unterstützt werden, sind etwa Daten, Struktur/Architektur, Verhalten/Funktion, Ablauf/Szenarien. Die Bewertung der Sicherheit eines Systems stützt sich dabei typischerweise auf *alle* diese Sichten ab, so dass sich die Frage stellt, wie hier trotzdem eine „Sicherheitssicht“ etabliert werden kann. Der hier vorgeschlagene Ansatz besteht darin, eine Sicht auf das System eigenschaftsorientiert zu definieren, so dass etwa alle funktionalen Eigenschaften die funktionale Sicht, Performanceeigenschaften die Performance-Sicht oder die Gesamtheit aller Sicherheitseigenschaften die Safety-Sicht auf ein System liefern. Der Vorteil einer solchen Aufteilung ist, dass semantische Abhängigkeiten der Safety-Sicht von anderen Sichten (z.B. Echtzeiteigenschaften, Performanceeigenschaften) – zusammen mit den entsprechenden Validierungsanforderungen - früh explizit identifiziert werden können. So kann etwa überprüft werden, ob die Verletzung einer funktionalen Anforderung die Verletzung einer Sicherheitseigenschaft nach sich ziehen kann. Derzeit werden im Rahmen des SPEEDS Projektes die hierfür erforderlichen Analysetechniken entwickelt. Voraussetzung hierfür ist ein gemeinsames semantisches Modell für funktionale und nicht-funktionale Eigenschaften, welches in [S07] beschrieben ist.

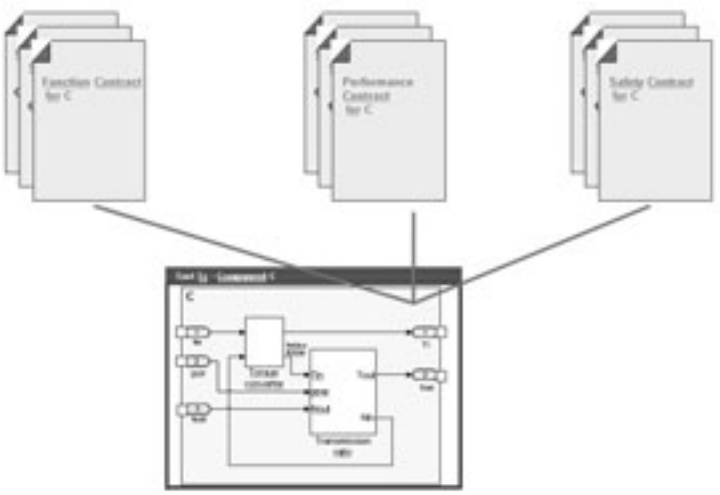

Abbildung 1: Contracts für 3 Sichten

2 Gleichwertigkeit/Ähnlichkeit von Komponenten aus Safety-Sicht

Zentrales Ziel beim komponentenbasierten Entwurf ist, erstens, die Wiederverwendbarkeit von Komponenten auf Basis definierter (und in der Regel bereits nachgewiesener) schnittstellen-orientierter Eigenschaften der Komponenten und, zweitens, die Ersetzbarkeit von Komponenten durch andere, bezüglich ihrer Schnittstellen „gleichwertiger" Komponenten. Die Gleichwertigkeitsanforderungen der Schnittstellen sind dabei abhängig von der jeweiligen Entwurfssicht. Für die Safety-Sicht bestimmen solche Gleichwertigkeitsanforderungen etwa, dass Teilsysteme nur durch Systeme *mit gleichem Safety Integrity Level* ersetzt werden dürfen. Da solche Anforderungen in der Regel nur unter bestimmten Umgebungsbedingungen und häufig auch nur unter Annahmen über den Bedienkontext eingehalten werden, sind sie als „Vertrag" (Contract) aufzufassen, der „Gegenleistung" für das Einhalten einer Umgebungsbedingung (Assumption) die Bereitstellung eines definierten Sollverhaltens verspricht (Promise). Beim Ersetzen einer Komponente durch eine neue (Implementierung der) Komponente kann dann überprüft werden, ob die ursprünglich vereinbarten Verträge noch eingehalten werden.

3 Kompositionelle Validierung

Um das obige Ersetzungsszenario auch (formal) validieren zu können müssen die Contracts einer Komponente aus den Contracts der Teilkomponenten ableitbar sein. Im Unterschied zur kompositionellen Validierung von funktionalen Eigenschaften [Dw98] muss hier auch das Fehlverhalten der Komponente aus dem Fehlverhalten der Teilkomponenten ableitbar sein.

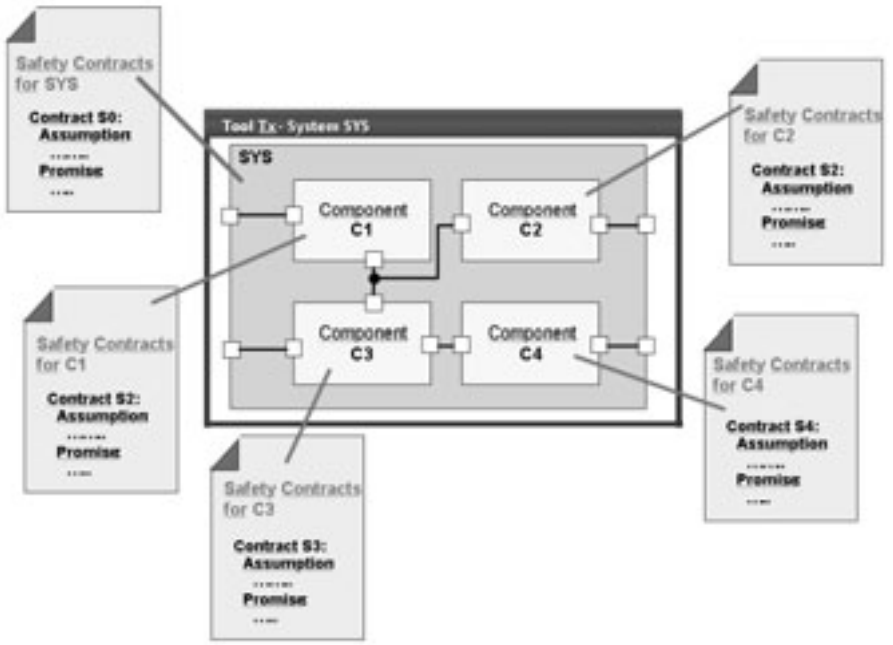

Abbildung 2: Ableitung von Contracts

Die hierfür erforderliche, ebenfalls im SPEEDS Projekt realisierte Analyse (Dominance-Check) stellt sicher, dass jedes Fehlverhalten welches durch die Safety-Contracts der Komponenten C1,...,C4 erlaubt ist auch durch den Safety-Contract von SYS erlaubt ist. Insoweit wird sichergestellt, dass auch komplexe Fehlersituationen, die durch das Zusammenspiel von u.U. defekten Komponenten C1,...,C4 entstehen durch den Safety-Contract von SYS erfasst sind. Typischerweise wird im frühen Entwurf der Safety-Contract von SYS gegeben sein und im Rahmen der Entwurfsverfeinerung sind dann entsprechende Sicherheitsanforderungen für die Teilkomponenten zu allokieren. Der Dominance-Check erlaubt dann diese Eigenschafts-Dekomposition abzusichern.

4 Untersuchung von detaillierten Systemmodellen: Fehlerinjektion

Ziel einer detaillierten Sicherheitsanalyse ist insbesondere die Identifikation von zusätzlichen Fehlern, die durch die Wahl einer Implementierung zustande kommen [Jp00]. Liegen detaillierte Modelle für einzelne Komponenten vor, so lassen sich diese durch eine Injektion von Fehlern um Fehlverhalten anreichern (Failure Mode Capturing) und erlauben somit eine Evaluierung der Fehlerfolgen in dem angereicherten Modell (Extended System Model), wobei die Modellanalyse dann das ursprüngliche, nominale Verhalten mit dem angereicherten Verhalten vergleichen muss um etwa Ursächlichkeit von Fehlern festzustellen.

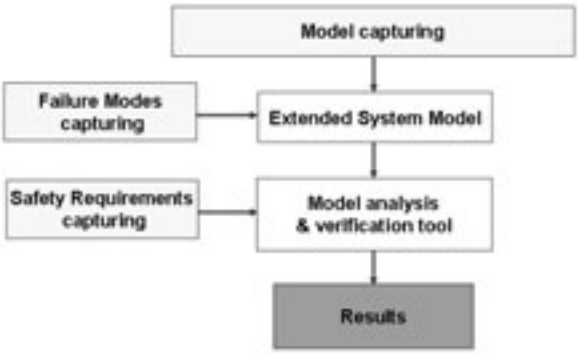

Abbildung 3: Modellbasierte Sicherheitsanlyse von Komponenten

Die Analysephase (Model analysis & verification tool) kann dann mit simulationsbasierten Techniken durchgeführt werden, wobei allerdings eine entsprechende Fehlerabdeckung sicherzustellen ist, wozu z.B. Techniken aus der automatischen Testgenerierung zum Einsatz kommen können. Eine neuere Methode mit erheblich höherer Zuverlässigkeit (bis zu 100% Abdeckung) wurde aus formalen Verifikationstechniken abgeleitet und gestattet etwa bei den obigen Ausgangsdaten die Erzeugung eines vollständigen (bezüglich der injizierten Fehler) Fehlerbaums aus einem Systemmodell heraus. In [Pt04] wurde damit ein Hochauftriebssystem eines Flugzeuges untersucht. In [Pt06] werden Erweiterungen dieser Methode im Hinblick auf Sicherheit von Diagnosesystemen, Berücksichtigung von *Common Causes* und Betriebsbedingungen vorgestellt.

5 Zusammenfassung

Das hier beschriebene Vorgehen erlaubt die Führung des Nachweises von Sicherheitseigenschaften inkrementell in bestehende modellbasierte Entwicklungsprozesse zu integrieren. Durch die Wahl eines Komponentenmodells, in dem Sicherheitseigenschaften unabhängig von dem (Entwurfs-)Modell der Komponente erfasst werden können, werden dabei auch Entwicklungsprozesse unterstützt bei denen etwa nur in frühen Entwurfsphasen oder nur teilweise (z.B. auf Komponentenebene oder Teilsystemebene) modellbasiert entwickelt wird. Für die technologische Unterstützung werden Integrationsplattformen benötigt, die insbesondere die um Contracts angereicherten Komponentemodelle unterstützen [Be05] und eine Einbindung von COTS Tools gestatten. Derzeit wird eine solche bus-basierte Plattform z.B. im SPEEDS Projekt entwickelt.

Literaturverzeichnis

[Be05] E. Brinksma, G. Coulson, I. Crnkovic, A. Evans, S. Gérard, S. Graf, H. Hermanns, J.-M. Jézeqél, B. Jonsson, N. Plouzeau, A. Ravn, Ph. Schnoebelen, F. Terrier, and A. Votintseva. Part ii: Component-based design and integration platforms. In B. Bouyssounouse and J. Sifakis, editors, *Embedded Systems Design: The ARTIST Roadmap for Research and Development*, number 3436 in LNCS, pages 103-214. Springer, 2005.

[Be06a] Böde, E., Herbstritt, M., Hermanns, H., Johr, S., Peikenkamp, T., Pulungan, R., et al. (2006). Compositional Performability Evaluation for STATEMATE. Proc. of QEST.

[Be06b] Böde, E., Damm, W., Hoyem, J., Josko, B., Niehaus, J., and Segelken, M.; Adding Value to Automotive Models, In Broy, M., Krüger. I.H., and Meisinger, M., Automotive Software - Connected Services in Mobile Networks. First Automotive Software Workshop (ASWSD 2004) San Diego. Revised Selected Papers, Lecture Notes in Computer Science 4147, Springer-Verlag, pp. 86-102, 2006.

[Dw98] W. Damm, B. Josko, H. Hungar, A. Pnueli: A Compositional Real-time Semantics of STATEMATE Designs, In de Roever, W.-P. , Langmaack, H., and Pnueli, A. (Edts.), Compositionality: The Significant Difference; International Symposium COMPOS '97, Lecture Notes in Computer Science 1536, Springer-Verlag, pp. 186-238, 1998.

[JMM08] B. Josko, Q. Ma, A. Metzner: Designing Embedded Systems using Heterogeneous Rich Components, 2008 (submitted).

[Jp00] P.H. Jesty, K.M. Hobley, R. Evans, I. Kendall, Safety Analysis of Vehicle-Based Systems. Proceedings of the 8th Safety-critical Systems Symposium, 2000.

[Pt04] T. Peikenkamp, E. Böde, I. Brückner, H. Spenke, M. Bretschneider, and H.-J. Holberg. Model-based Safety Analysis of a Flap Control System. In *Proceedings of the INCOSE 2004 -- 14th Annual International Symposium*, Toulouse, 2004.

[Pt06] Peikenkamp, T., Cavallo, A., Valacca, L., Böde, E., Pretzer, M., & Hahn, E. M. (2006). Towards a Unified Model-Based Safety Assessment.

[S07] SPEEDS Core Meta-model Syntax and Draft Semantics. SPEEDS internal Deliverable D.2.1.c, 2007.