

SPECifIC

Durchgängige qualitätsorientierte bidirektionale Transformation

Spezifikation

Modellierung

Implementierung



Sicherheit im Entwurf komplexer Systeme

Beim Entwurf hochkomplexer Systeme ist trotz stetig steigender Sicherheitsanforderungen eine natürlichsprachliche Spezifikation als zentrales Ausgangsdokument unverzichtbar. Nur so können alle Beteiligten, d.h. Entwickler, Projektleiter und Kunden zu einem gemeinsamen Verständnis des Produktes kommen. Um die entworfenen Systeme letztendlich jedoch als Produkt fertigen zu können, müssen sie in mehreren Phasen in immer konkreter werdende Modelle überführt werden. Diese Transformationen sind besonders sicherheitskritisch und ihre Analyse ist daher von zentraler Bedeutung. Dabei liefert das Projekt SPECifIC des Forschungsbereichs Cyber-Physical Systems (CPS) am DFKI Lösungen zu drei Herausforderungen, die im Folgenden beschrieben werden.

Assistierte Übersetzung der Spezifikation

Mit den in SPECifIC entwickelten Methoden wird ein erstes formalisiertes Modell bereits beim Schreiben der Spezifikation automatisiert erstellt. Mensch und Computer arbeiten dabei als Team und Unklarheiten in der Spezifikation werden im Dialog zwischen beiden geklärt. Dieses Vorgehen weist den Entwerfer auf unpräzise und missverständliche Abschnitte in der Spezifikation hin. Somit wird sichergestellt, dass die natürlichsprachlich formulierten Anforderungen richtig verstanden werden.

Frühzeitige Verifikation

Auf dem Modell, das aus der Übersetzung der Spezifikation resultiert, lassen sich bereits erste automatische Verfahren zur Überprüfung der Korrektheit anwenden.

Dadurch werden Fehler frühzeitig im Entwurfsablauf erkannt und korrigiert. Dies führt zu Zeit- und Kosteneinsparungen, die bei heutigen „Time-to-Market“ Anforderungen ausschlaggebend sein können. Insbesondere ist die Verifikation der Transformation wichtig, die Beschreibungen von einer Ebene in die nächst konkretere übersetzt. Das Projekt SPECifIC untersucht Methoden, die eine korrekte Transformation ermöglichen und somit sicherstellen, dass die Anforderungen vom Produkt korrekt umgesetzt werden.

Nachvollziehen von Änderungen

Um nichtfunktionalen Anforderungen wie beispielsweise Ausführungszeit und Energieverbrauch nachzukommen, ist es üblich, dass Modelle späterer Phasen händisch verändert werden. Da diese Schritte oft nicht transparent sind, ist dieses Vorgehen besonders sicherheitskritisch. Das SPECifIC-Projekt entwickelt eine intelligente Verfolgung dieser Änderungen und macht sie in vorhergehenden Modellen bis hin zur Spezifikation sichtbar.

Das SPECifIC-Projekt wird gefördert durch das Bundesministerium für Bildung und Forschung (BMBF).

GEFÖRDERT VOM



Förderkennzeichen: 01IW13001

Kontakt:

DFKI GmbH, Cyber-Physical Systems
Leitung: Prof. Dr. Rolf Drechsler

Dr. Mathias Soeken
Telefon: 0421-218-63955
E-Mail: mathias.soeken@dfki.de
Internet: www.dfki.de/cps