

Modellierung von Funktionsnetzen mit UML-RT:

Erfahrungen aus einem Automobilprojekt zur Entwicklung sicherheitsrelevanter Systeme

Michael von der Beek

BMW AG, München

Beschreibung

Dieser Vortrag stellt die SW-Entwicklung für sicherheitsrelevante Systeme anhand eines Beispielprojektes aus der Automobilindustrie vor. Dieses BMW-Vorentwicklungsprojekt aus der Domäne der Fahrwerksregelelektronik beschäftigt sich mit der Entwicklung von HW- und SW-Architekturen, mit einer neuen Bustechnologie (FlexRay) zur sicheren Datenkommunikation, mit der Realisierung einer sicheren Energieversorgung und schliesslich – und dies ist der Fokus dieses Vortrags - mit der Definition und Realisierung eines sicherheitsgerichteten SW-Entwicklungsprozesses.

In einem Gesamtüberblick werden die einzelnen Prozessschritte, -resultate und eingesetzten SW-Werkzeuge dieses Entwicklungsprozesses vorgestellt. Dabei wird insbesondere die Orientierung an dem Sicherheitsstandard IEC 61508 erläutert. Einen zentralen Bestandteil des Entwicklungsprozesses nimmt die Funktionsnetzmodellierung ein: Hierbei handelt es sich um eine graphische, relativ abstrakte Darstellung der Gesamtheit der zu realisierenden Fahrzeugfunktionen unter Verwendung der UML-RT. Diese Funktionsnetzmodellierung stellt im wesentlichen eine Modellierung von Strukturinformation, also keine Verhaltensmodellierung dar. Dabei werden zwei Sichten präzise unterschieden: Die logische Sicht verwendet die Strukturdiagramme der UML-RT, um möglichst unabhängig von (späteren) SW/HW-Designentscheidungen modellieren zu können. Designentscheidungen werden erst in der SW/HW-Sicht gefällt – hierbei werden die Komponenten- und Deploymentdiagramme der UML-RT eingesetzt. Die Erstellung der Funktionsnetzmodelle ist innerhalb des Entwicklungsprozesses methodisch und werkzeugtechnisch eng mit anderen Aktivitäten integriert: Mit dem Anforderungsmanagement, der Verhaltensmodellierung und der Codegenerierung sowie dem Versions- und Konfigurationsmanagement. Im Anschluss an die Beschreibung dieser Integrationen wird noch ein Ausblick auf zukünftig geplante Integrationen mit Testaktivitäten, mit der Architektursimulation sowie dem Änderungsmanagement gegeben. Schliesslich werden Probleme der Funktionsnetzmodellierung beschrieben und mögliche Problemlösungen erörtert.