TU Clausthal

Abschlussvortrag Masterarbeit Jan Toennemann

„Evaluation einer Toolkette zur modellbasierten Entwicklung mit automatisierter Testfallgenerierung basierend auf den Anforderungen“

Durch die zunehmende Realisierung des vollständig autonomen Fahrens werden die Sicherheitsanforderungen für elektrische/elektronische Systeme und Software von Kraftfahrzeugen immer strenger und auch schwieriger zu überprüfen. In Umgebungen, in denen eine Fehlfunktion schwerwiegende Auswirkungen haben kann und möglicherweise auch Menschenleben kosten könnte, ist die Gewährleistung der Gesamtsicherheit kritischer Systeme im Fahrzeug von größter Bedeutung. Seit der Einführung der ISO 26262 „Road vehicles – Functional safety“ werden dem gesamten Entwicklungsprozess umfangreiche und sehr strikte Regeln auferlegt und mit der ISO/PAS 21448 „Road vehicles – Safety of the intended functionality“ (SOTIF) muss noch mehr als nur die funktionale Sicherheit eines Systems gründlich validiert werden.

Auf der Suche nach einemtool-gestützten Entwicklungsansatz, der die Arbeit mit geforderten Standards erleichtert, fallen besonders mehrere Toolhersteller auf, die die Integration formaler Methoden in einer für den Industriegebrauch angemessenen Entwicklungsumgebung bewerben. Im Rahmen dieser Arbeit wird eine Toolkette evaluiert, die CATIA STIMULUS für die Spezifikation der Anforderungen und die ANSYS SCADE Suite für die modellbasierte Entwicklung einsetzt. Beide Werkzeuge bauen auf einem formalen Backend auf und bieten einen vergleichsweise zugänglichen Ansatz zur Modellerstellung sowie umfangreiche Möglichkeiten zur Verifikation & Validierung.

Wir stellen einen systematischen Ansatz zur Übertragung der vorhandenen Artefakte in die neuen Umgebungen vor, wobei zugrundeliegende Unterschiede hervorgehoben und sowohl die Benutzerfreundlichkeit als auch die bereitgestellten Werkzeuge mit dem aktuellen Ansatz verglichen werden. Es werden Praktiken für die Entwicklung innerhalb der Entwicklungsumgebungen empfohlen und Richtlinien für die Übertragung ähnlicher Projekte vorgestellt. Die Test-, Verifikation- und Validierungsfähigkeiten der Werkzeuge werden unter die Lupe genommen und mit der aktuellen Toolkette verglichen.

Es wird untersucht, wie Tests mit den bereitgestellten Werkzeugen automatisch generiert werden können und wie sich dieser Prozess mit dem derzeitigen Ansatz der manuellen Testfallerstellung vergleichen lässt. Die entwickelten Verfahren können dazu verwendet werden, die im Gesamtprozess erforderliche manuelle Arbeit stark zu reduzieren und so wertvolle Ressourcen sowie Arbeitsstunden einzusparen. Die derzeitigen Grenzen des Ansatzes werden detailliert beschrieben und Erweiterungen der Toolkette vorgeschlagen, welche den Weg für einen vollständig integrierten und möglichst automatisierten modellbasierten Entwicklungsprozess für sicherheitskritische Steuerungssoftware ebnen.

Betreuer der Arbeit: Prof. Dr. Andreas Rausch, Prof. Dr. Rüdiger Ehlers

TU Clausthal

Datum:	Dienstag, 01. September 2020, 14:30 Uhr
Ort:	Online-Meeting über BBB
	Link: https://webconf.tu-clausthal.de/b/sim-uc9-rvy