Bachelorprojekt
Wintersemester 2013/2014 – Sommersemester 2014

HPI Hasso Plattner Institut
IT Systems Engineering | Universität Potsdam

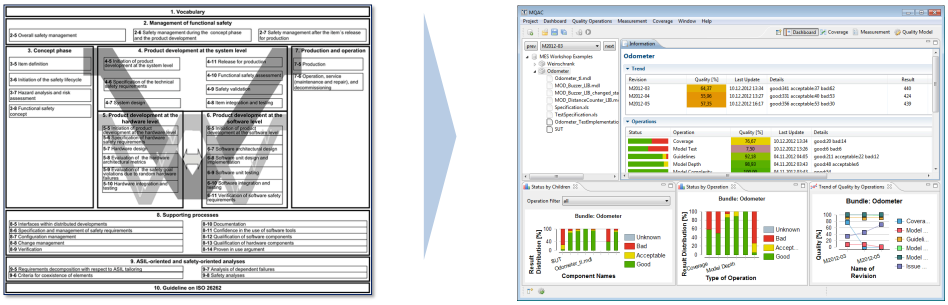
# Safety Process Guidance for Automotive Software Development

## Projekthintergrund

Software-basierte Systeme im Automobil realisieren häufig sicherheitsrelevante Funktionen. Elektronische Lenksysteme oder radargestützte Fahrerassistenzsysteme sind bekannte Beispiele. Die Gewährleistung von Sicherheit ist dabei oberstes Ziel für die Umsetzung der Funktionen. Auswirkungen von Fehlern im System müssen so begrenzt werden, dass durch diese Fehler keine Personen zu Schaden kommen. Im günstigsten Fall wird das Auftreten dieser Fehler durch die Wahl geeigneter Maßnahmen sogar ganz ausgeschlossen.

Der State-of-the-Art in der Entwicklung sicherheitsrelevanter Software wird durch den internationalen Standard ISO 26262 beschrieben. Dieser deckt den gesamten Entwicklungsprozess ab: beginnend bei der Beschreibung der Systemfunktion Funktionsidentifikation über die Risikoanalyse bis hin zur Prüfung des Codes, der zur Realisierung der Funktion im Automobil ausgeführt wird. Der Standard stellt eine Vielzahl von Anforderungen auf, die je nach Gefährdungsklasse des entwickelten Systems Anwendung finden sollen. Die ISO 26262 gibt zudem Empfehlungen und nennt Maßnahmen, die für die Umsetzung der Anforderungen geeignet sind.

Die ISO 26262 fordert neben der Anwendung von Qualitätssicherungsmaßnahmen auch deren umfassende Dokumentation: In einem Sicherheitsnachweis sind die Durchführung und das Ergebnis der Ausführung der Maßnahmen zu dokumentieren. Gerade bei umfangreichen Funktionen ist die Erstellung des Sicherheitsnachweises mit hohen Aufwänden verbunden. Viele Artefakte müssen geprüft werden. Die Nachweise sind zu organisieren und strukturiert abzulegen. Im Falle von Änderungen an Artefakten muss eindeutig erkennbar sein, welche Absicherungen neu erfolgen müssen. Die Überwachung des kompletten Sicherheitsprozesses ist daher eine zentrale Aufgabe in der Entwicklung sicherheitsrelevanter Funktionen.



## Projektgegenstand

Das Bachelorprojekt hat das Ziel auf der Basis von MQAC, einer Werkzeugumgebung zum Qualitätsmonitoring, die Erstellung und Pflege eines Sicherheitsnachweises für eine Beispielfunktion umzusetzen. Das zu bearbeitende Szenario sieht vor, dass die sicherheitsrelevante Funktion bereits in einer ersten Version umgesetzt ist. So liegen spezifische Systemanforderungen vor und eine Systemarchitektur ist entworfen, die auch die technischen Sicherheitsfunktionen definiert. Die Realisierung ausgewählter Sicherheitsfunktionen ist als Simulink-Modell vorgenommen, aus dem darüber hinaus Code generiert wurde. Diese Artefakte sind durch die unterschiedlichen Verfahren, die durch die ISO 26262 gefordert werden, zu untersuchen und der Sicherheitsnachweis ist aufzubauen.

Das Konzept für das Qualitätsmonitoring soll so aufgesetzt werden, dass es die Überarbeitung einer sicherheitsrelevanten Funktion geeignet erfasst und ausstehende Qualitätsmaßnahmen herausgearbeitet werden. Weiterhin sind die Umsetzung des Sicherheitsprozesses zu begleiten und der Sicherheitsnachweis zu erstellen. Im Einzelnen sind folgende Use Cases zu realisieren:
a) automatische Ableitung eines Safety Case zum Ende der Entwicklung,
b) Identifikation der noch ausstehenden Schritte für die vollständige Umsetzung der Sicherheitsanforderungen,

c) Bewertung möglicher nächster Schritte für die effiziente Umsetzung der Sicherheitsanforderungen,
d) Kontinuierliche Beobachtung des Umsetzungsgrads der Sicherheitsanforderungen.

## Umsetzung

Die Umsetzung beruht auf dem Einsatz realer Entwicklungsartefakte und Entwicklungs- und Prüfverfahren. Die Durchführung der Verfahren ist im Qualitätsmonitoring zu überwachen mit dem Ziel, die Ergebnisse in einen finalen Sicherheitsnachweis aufzunehmen.
Es sind mehrere Aufgaben zu bearbeiten:
1) Identifikation der erforderlichen und Anwendung der ausgewählten Absicherungsmaßnahmen
2) Gestaltung des integrierten Qualitätsmodells als Struktur des Sicherheitsnachweises
3) Anbindung der Verfahren zur automatischen Ergebnisaufnahme in das Qualitätsmonitoring
4) Exemplarische Überarbeitung von vorliegenden Artefakten, um ??????
5) Ableitung der erforderlichen nachträglichen Absicherungsmaßnahmen aus dem Qualitätsmodell
Die Arbeiten sind unter Einsatz realer Entwicklungswerkzeuge durchzuführen. Deren Leistungsfähigkeit ist zu evaluieren und deren Ergebnisse sind in das Qualitätsmonitoring zu integrieren. Eine Automatisierung ist vorzulegen. Die Anbindung der Entwicklungswerkzeuge erfolgt auf der Basis von XML-basiertem Datenaustausch. Die tiefergehende Integration soll bei Vorliegen geeigneter Schnittstellen mit Java als Realisierungssprache erfolgen.

## Projektumfeld

Das Projekt wird in Zusammenarbeit mit Model Engineering Solutions GmbH (MES) durchgeführt. MES ist spezialisiert auf die integrierte Qualitätssicherung eingebetteter Software im Automobil. MES entwickelt und vertreibt Werkzeuge, die die Entwicklung und Qualitätssicherung eingebetteter Software im Fahrzeug konstruktiv und analytisch unterstützen. Die Studierenden werden, im Rahmen der Kooperation mit MES, als Auftragnehmer interagieren. Dies gilt insbesondere für die Erfassungen der Anforderungen aber auch für die Evaluierung der Ergebnisse des Projekts. Die für die Durchführung der Qualitätssicherung erforderlichen Werkzeuge werden für die Laufzeit des Bachelorprojekts zur Verfügung gestellt. Es ist zu erwarten, dass bei erfolgreicher Bearbeitung des Projekts auch eine studentische Beschäftigung in thematisch naheliegenden Projekten nach Abschluss möglich ist.

## Organisation

In der Vorbereitungsphase werden fachliche Grundlagen zur Entwicklung sicherheitsrelevanter Systeme nach ISO 26262, modellbasierter Softwareentwicklung und Echtzeitsystemen vermittelt und es werden vorhandene Modelle und Werkzeuge entsprechend auf die geplante Aufgabe hin betrachtet. Dazu werden beispielhaft ausgewählte Aufgabenstellungen einzeln oder in kleineren Teams bearbeitet und allen Teilnehmern vorgestellt. Studierende, die in diesem Projekt teilnehmen wollen, sollten Interesse an der modellbasierten Entwicklung und an technischen Systemen haben. Es wird weiter erwartet, dass man sich in die zum Einsatz kommenden Methoden der Softwaretechnik während des Projekts einarbeitet.

## Teilnehmer und Projektbeginn

Zwischen 4 und 8 Teilnehmer können in diesem Bachelorprojekt mitwirken. Aufgaben und Organisation werden bei Projektbeginn mit den Projektmitgliedern erarbeitet. Projektbeginn ist der 1.10.2013.

## Informationen

Für ausführliche Informationen zu dem Projekt stehen Regina Hebig (Regina.Hebig@hpi.uni-potsdam.de) und Prof. Holger Giese (A-2.5, holger.giese@hpi.uni-potsdam.de) zur Verfügung. Ansprechpartner seitens der Model Engineering Solutions GmbH wird während des Projekts Dr. Elke Salecker (elke.salecker@model-engineers.com) sein.

MES
MODEL ENGINEERING SOLUTIONS

HPI Hasso Plattner Institut
IT Systems Engineering | Universität Potsdam
FG Systemanalyse und Modellierung