Informatik 11
Embedded Software

RWTH AACHEN UNIVERSITY

Bachelorarbeit

Konsistenzprüfung von Gefährdungsanalysen

In Kooperation mit dem Ford Research and Innovation Center Aachen

Problemstellung

Gefährdungen, die in der Gefährdungsanalyse und Risikoabschätzung (engl. Hazard Analysis and Risk Assessment – HARA) identifiziert werden, werden in der Automobilindustrie anhand des sogenannten Automotive Safety Integrity Levels (ASIL) eingestuft. Je sicherheitskritischer die Funktionalität ist, die entwickelt werden soll, desto höher ist das ASIL. In welches ASIL eine Gefährdung eingestuft wird hängt von vielen Faktoren ab. Bei dieser Menge von Faktoren kann es zu inkonsistenten Beschreibungen und Einstufungen führen.

Im Rahmen des HARA-Projekts am Lehrstuhl Informatik 11 wird ein Tool zur Unterstützung bei der Durchführung der Gefährdungsanalyse entwickelt. Das Werkzeug soll die Anwender nicht nur bei der Eingabe unterstützen, sondern auch automatisiert die eingegebenen Daten auf Konsistenz überprüfen.

KONSISTENZPRÜFUNGSPROZESS

Eine Gefährdung wird anhand von drei Parametern eingestuft: Schwere der Auswirkung (engl. Severity), Häufigkeit der Fahrsituation (engl. Exposure) und Beherrschbarkeit der Fehlfunktion (engl. Controllability). Für jede Einstufung wird zusätzlich eine Begründung (engl. Rationale) erstellt. In dem unten abgebildeten Beispiel wurde die Schwere der Auswirkungen unterschiedlich eingestuft, obwohl die Begründung die selbe ist, was eine Form von Inkonsistenz darstellt.

S	Severity	E	Exposure	C	Controllability	ASIL
Category	Rationale *(description of reasonable expected consequences, if not obvious)*	Category	Rationale *(including description of accident trigger, if not obvious)*	Category	Rationale *(including action to avoid harm)*	
S2	Potential lane departure	E3	All normal driving situations	C3	Difficult to control or uncontrollable for an average driver.	B
S3	Potential lane departure	E2	AEB intervention occurs a few times a year for the great majority of drivers	C3	Difficult to control or uncontrollable for an average driver.	B

VEREINFACHTES BEISPIEL FÜR EINE INKONSISTENTE EINGABE

Aufgabenstellung

- Literraturrecherche zum aktuellen Stand der Forschung über Konsistenzprüfung von Gefährdungsanalysen
- Entwicklung einer Methodik zur Bewertung der Konsistenz der Gefährdungsanalysen
- Implementierung der Konsistenzprüfung
- Einbindung in ein vorhandenes Tool
- Evaluation mit Hilfe geeigneter Methoden und industriellen Fallbeispielen

Ansprechpartner

Paul Chomicz, M.Sc. RWTH
chomicz@embedded.rwth-aachen.de