AUTOREG 2011, 22. – 23. November 2011, Baden-Baden

Titel des Beitrags	Praktische Durchführung von Gefährdungsanalysen und Risikobewertungen nach ISO 26262 für Gesamtfahrzeuge
Name des Autors	Dr.-Ing. Tobias Ständer[(1)]
Namen der Co-Autoren	Dr.-Ing. Uwe Becker[(1)] Peter Spies[(1)] Dipl.-Phys. Udo Steininger[(2)] Dipl.-Ing. Sven Hille[(2)]
Organisation / Firma	[(1)] Institute for Quality, Safety and Transportation Tel. 0531/31732636 Fax: 0531/20856711 {t.staender | u.becker}@iqst.de [(2)] TÜV SÜD Automotive, TÜV SÜD Gruppe Daimlerstr. 11, 85748 Garching udo.steininger@tuev-sued.de
Zuordnung zum thematischen Schwerpunkt	B.6: Sicherheits- und Diagnosekonzepte E: Entwicklungsmethoden und Softwaretools
Inhaltsangabe mit spezifischen Informationen	s. unten
Innovationsgrad	Aktuellste Praxiserfahrungen → neu
Bevorzugte Beitragsart	Vortrag
Angabe von Veröffentlichungen zum Thema	Ständer, T., Becker, U., Bartels, A., Steininger, U., Weidl, T. *Eine funktionsorientierte semi-quantitative Methode zur Entwicklung sicherer Fahrzeug-Systeme*, autoreg 2008, Baden-Baden Ständer, T. *Eine modellbasierte Methode zur Objektivierung der Risikoanalyse nach ISO 26262*, Dissertation 2010

Inhaltsangabe:

Dieser Beitrag behandelt die praktische Umsetzung der Gefährdungsanalyse und Risikobewertung (GuR) nach ISO 26262 im Entwicklungsprozess von elektrischen und elektronischen Fahrzeugsystemen. Besonderes Augenmerk wird auf die Einordnung der Systementwicklung in den Gesamtfahrzeug-Entwicklungsprozess gelegt.
Die GuR ist per Definition in der frühen Konzeptphase (s. Abb. 1) angesiedelt und soll vollkommen losgelöst von der technischen Realisierung durchgeführt werden. Mit ihr sollen potenzielle Gefährdungen identifiziert werden, welche im Zusammenhang mit der zu

entwickelnden Funktion stehen. Die Gefährdungen werden unter Bezugnahme auf sich ergebende mögliche Konsequenzen hinsichtlich Ihres Risikopotenzials bewertet. Für eine gesamthafte Risikobewertung ist es unerlässlich, die Betrachtungen auf der Ebene des Gesamtsystems – bestehend aus Fahrer, Fahrzeug und Fahrumgebung – zu beginnen und anschließend auf System- und Komponenten-Ebene herunter zu brechen. Dabei kann der Detaillierungsgrad auf Gesamtsystemebene zunächst noch gering sein, hier geht es im Wesentlichen um die Vollständigkeit der Betrachtung.

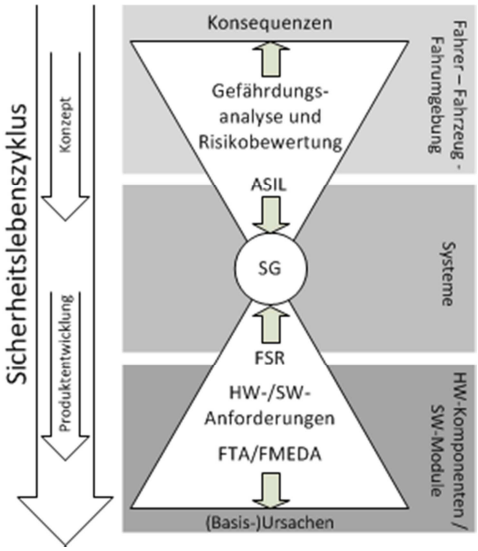

Abbildung 1: Eingliederung der GuR im Sicherheitslebenszyklus

Die GuR geht von einer rein funktionalen Sichtweise aus und stellt auf Basis der Ableitung von Automotive Safety Integrity Levels (ASIL), Safety Goals (SG) und Functional Safety Requirements (FSR) Anforderungen an die Entwicklung von Hardware (z.B. Redundanzen, Diversitäten etc.) und Software (z.B. SW-Architektur, Programmierrichtlinien etc.). Mit der Dokumentation dieser SG und FSR ist die GuR zunächst abgeschlossen. Im nächsten Schritt wird basierend auf den SG und den FSR ein funktionales Sicherheitskonzept abgeleitet.
Die tatsächliche Umsetzung dieser Anforderungen und die zu Ihrer Erfüllung anzuwendenden sicherheitsanalytischen Methoden (z.B. Fault Tree Analysis (FTA), Failure Modes, Effects and Diagnostic Coverage Analysis (FMEDA)) sind Bestandteil der Produktentwicklungs-Phase. Mit ihnen wird der Nachweis erbracht, dass das zu entwickelnde System die funktionalen Sicherheitsanforderungen erfüllt, und die die vorhersehbaren Gefährdungen initiierenden (Basis-)Ursachen mit einer hinreichend niedrigen Wahrscheinlichkeit eintreten.
TÜV SÜD Automotive GmbH (TÜV) und Institute for Quality, Safety and Transportation GmbH (iQST) führen im Auftrag ihrer Kunden sowohl GuR als auch Reviews dieser

Analysen durch. Dabei wird immer wieder deutlich, dass die ISO 26262 zwar einen guten Leitfaden zur Durchführung einer GuR bietet, dem Anwender aber von der Norm keine Struktur an die Hand gegeben wird. Vor diesem Hintergrund wurde von TÜV und iQST ein strukturierter auf verschiedenen Matrizen basierender Ansatz (s. Abb. 2) entwickelt, mit welchem ein sehr hohes Maß an Vollständigkeit und Nachvollziehbarkeit erreicht werden kann.

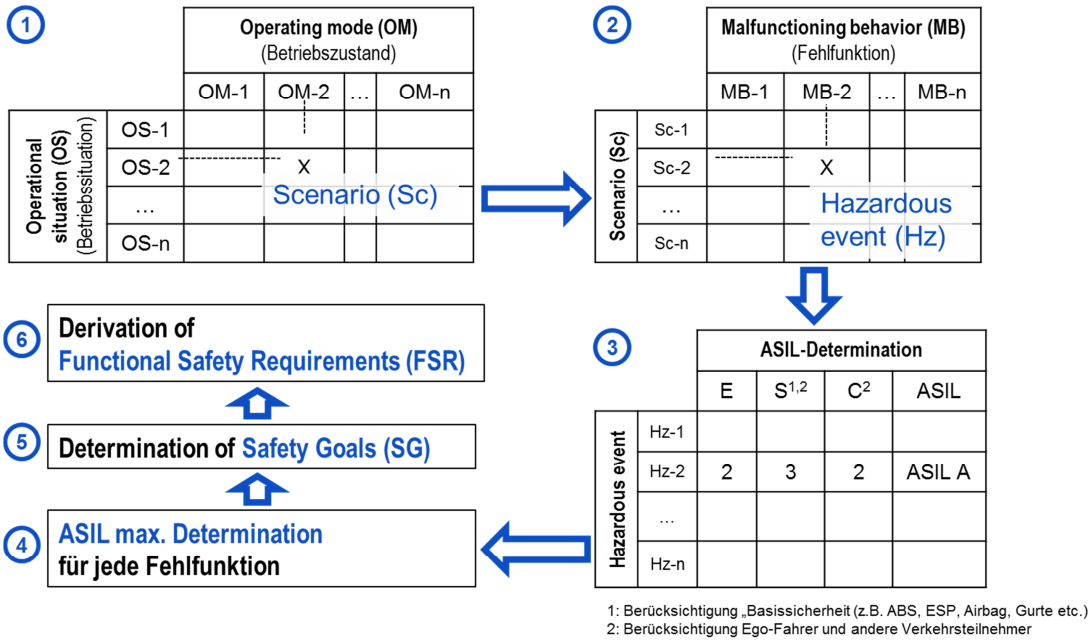

Abbildung 2: Schematische Darstellung des GuR-Prozedere gemäß ISO 26262

Die ASIL-Bewertung in Schritt 3 von Abbildung 2 basiert in hohem Maße auf subjektiven - meist konservativen - (Experten-) Einschätzungen der den ASIL charakterisierenden Parameter (s. Abb. 2) Expositionswahrscheinlichkeit (E), Schadensausmaß (S) und Kontrollierbarkeit (C), weswegen Sicherheitsfunktionen häufig überdimensioniert werden. Im Beitrag wird kurz auf eine Methode eingegangen, welche diesen subjektiven Einflüssen durch Simulation und Analyse von Modellen begegnet und so die Ergebnisse der GuR objektiviert.

Zur praktischen Umsetzung der in Abbildung 2 dargestellten Phasen der GuR haben TÜV SÜD Automotive und iQST ein Excel-basiertes Tool entwickelt. Dieses Tool wird in dem Beitrag vorgestellt. Darüber hinaus wurden und werden allgemeingültige Kataloge von Betriebssituationen erarbeitet. Derzeit liegen solche Kataloge für zukünftige Fahrerassistenzsysteme (FAS) und für batterie- bzw. hybrid-elektrische Antriebe vor. Das methodische Vorgehen lässt sich uneingeschränkt auf beliebige Fahrzeugsysteme anwenden.