Informatiker testen Airbag \\

Prof. Stefan Leue hat mit seinem Team die Gefahrenwahrscheinlichkeit für ein Airbag-System berechnet

Ein „gutes Beispiel für Technologietransfer“ nennt Prof. Stefan Leue die Zusammenarbeit seiner Arbeitsgruppe mit der Firma TRW Automotive GmbH. Der Konstanzer Informatiker und sein Team untersuchen für den weltweit fünftgrößten Automobilzulieferer, der im benachbarten Radolfzell ein Technologiezentrum betreibt, die Gefahrenwahrscheinlichkeit für das von TRW entwickelte und vertriebene Airbag-System. Mit einem eigens zu diesem Zweck angepassten Modellierungssystem konnte seine Arbeitsgruppe herausfinden, was alles schief laufen kann mit diesem Sicherheitssystem und mit welcher Wahrscheinlichkeit solche Gefahrensituationen eintreten können. Die Studie wurde im September auf der 6th International Conference on Quantitative Evaluation of SysTems (QEST) 2009 vorgestellt.

Airbags können auf verschiedene Weise versagen. Man denke daran, dass sie bei einem Zusammenstoß ihren Dienst verweigern und nicht aufgehen. Was aber noch viel fataler sein kann: Dass sie im falschen Moment losgehen, ohne dass ein Unfall stattgefunden hat. Und das mit 180 auf der Autobahn noch dazu auf der Fahrerseite. Die sicherheitsrelevante Gefahreneinschätzung solcher „eingebetteter Systeme“, wie ein Airbagsystem es ist, wird dabei immer wichtiger. Diese technischen Informatiksysteme, die die Hardware kontrollieren sollen, sind vom Handy angefangen allgegenwärtig. In den Autos haben sie schon jetzt ein Großteil der mechanischen und elektromechnischen Steuerungselemente, so beispielsweise den Zündverteiler, ersetzt. Neueste Technologie ermöglicht es darüber hinaus, dass keine mechanische Verbindung mehr zwischen Lenkrad und Rädern notwendig ist. Sensoren im Lenker messen die Lenkbewegung, die Daten werden zu kleinen Motoren in den Rädern weitergegeben, die diese entsprechend in Stellung bringen.

Sicherheit wird da großgeschrieben. Natürlich ist es für den Zulieferer TRW wichtig zu wissen, wie zuverlässig seine Produkte sind. Dabei ist TRW auf Angaben seiner Zulieferer über die Zuverlässigkeit der verwendeten Bauteile

angewiesen. Aber wie kann man daraus auf die Zuverlässigkeit des Gesamtsystems schliessen, das ja aus einer komplizierten Komposition von unterschiedlichen Bauteilen besteht? Wegen der Seltenheit der Komponentenfehler lässt sich diese Zuverlässigkeit weder durch Testen noch durch Beobachtung bestimmen. Da müssen die Informatiker ran. Leue und seine Leute haben die Architektur der „Electronic Control Unit" (ECU), eines Bauteils des realen TRW-Airbagsystems, mit Hilfe von einem stochastischen Prozessenmodell nachmodelliert. Das heißt: Sie haben nachvollzogen, wie die einzelnen Komponenten des Airbagsystems bzw. des ECU-Bauteils miteinander vernetzt und verschaltet sind, von der Stromzufuhr für die Zündung bis hin zum Mikroprozessor selbst. Und sie haben mithilfe von Prozessmodellen rekonstruiert, wie sich dieses System als ganzes verhält.

Dieses Modell wird mit Daten zur Ausfallwahrscheinlichkeit jeder einzelnen Komponente versehen. „Wir berechnen mit unserem Modell die Gesamtwahrscheinlichkeit", stellt der Informatikprofessor fest. Konkret: Wie wahrscheinlich es ist, dass die Signale der Beschleunigungssensoren, die an unterschiedlichen Orten im Fahrzeug angebracht sind, falsch verarbeitet werden. Dass das System zum Beispiel ein einfaches über den Bordstein Fahren oder starkes Abbremsen fälschlicherweise etwa als Auffahrunfall interpretiert. Oder dass es die Airbags nicht optimal einsetzt. „Bei einem Frontalcrash werden andere Airbags gesteuert als bei einem Überrollcrash", erklärt Leue die verschiedenen Herausforderungen. Failure Mode and Effects Analysis, kurz FMEA, heißt die Methode, mit der die Auswirkungen der Fehler von Einzelteilen auf das Gesamtsystem und damit dessen wahrscheinliches Versagen numerisch berechnet werden.

Für ein Unternehmen wie TRW, das weltweit 60.000 Mitarbeiter hat, ist diese Art der Gefahrenabschätzung von größter Bedeutung. Nicht nur, um die geforderten Mindeststandards an Sicherheit zu erfüllen. Stefan Leue weist auch auf die moralisch-ethische Verantwortung eines Industrieunternehmens wie TRW hin. Wie etwa bei dem Unfall, als vor längerem ein Baby durch ein falsch programmiertes Airbagsystem eines anderen Herstellers zu Tode kam. Die Eltern waren in der Werkstatt, um die Airbag-Kontrollsoftware für die Beifahrerseite abschalten zu lassen, da sie den Babysitz auf dem Frontsitz montieren wollten. Es kam zum Unfall, der Airbag zündete trotzdem und tötete das Baby. „Wenn wir sicherheitskritische Systeme bauen, die immer mehr unser Leben bestimmen, dann müssen wir aus moralischen Gründen sicherstellen, dass nach Möglichkeit keine Fehlfunktionen eintreten", stellt Stefan Leue fest. Selbstverständlich sind auch handfeste

*Prof. **Stefan Leue** (2.v.l.), Inhaber des Lehrstuhls Software Engineering, und seine Mitarbeiter: v.l. Post-Doc Dr. **Matthias Kuntz**, Doktorand **Husain Aljazzar** und **Florian Leitner-Fischer**, Masterstudent Information Engineering, der seit dem Abitur Werkstudent bei TRW ist. Nicht auf dem Bild sind der Ingenieur Manuel Fischer von TRW sowie Prof. Lars Grunske von der Swinburne University in Australien, die ebenfalls am Projekt mitwirkten.*

Die Airbag Electronic Control Unit (AECU), die für die Steuerung des Airbags verantwortlich ist. In der Mitte der quadratische Mikroprozessor, auf dem die Steuersoftware läuft. Die hellen quadratischen Bauteile sind die Beschleunigungssensoren, die größeren zylindrischen Bauteile sind Kondensatoren, welche die elektrische Spannung für den Zündfunken liefern.

finanzielle Gründe im Spiel. Eine Rückrufaktion, die pro Wagen vielleicht 500 Euro kostet, kann einen gesamten Jahresgewinn eines Automobilunternehmens auffressen. Das Ergebnis der Analyse fasst Leue so zusammen: „Wir konnten zeigen, dass die Architektur zu einem Teil diese Mindestanforderungen erfüllt, und zu einem Teil eben nicht." Eine der Konsequenzen des Zulieferers war, dass nun anstatt einem zwei Mikrocontroller ins Airbagsystem eingebaut werden. Nur wenn beide die Anweisung zum Zünden des Airbags geben, darf auch gezündet werden. Durch die teilweise Anpassung des verwendeten Modelliersystems PRISM, das von Kollegen in Birmingham und Oxford entwickelt wurde, konnte das Konstanzer Informatikteam auch zeigen, warum eine gewisse Sicherheitswahrscheinlichkeit nicht erreicht wurde. Zudem kann der Autozulieferer sicher sein, dass keine Möglichkeit vergessen wurde. Während es früher letztlich vom Zufall abhing, ob jemand durch gedankliche Antizipation, was passieren kann, auf die richtige Konsequenz stieß, werden hier durch Automatisierung alle sicherheitskritischen Konsequenzen abgedeckt.

Die Kooperation besteht nicht nur im gelungenen Technologietransfer, sondern liefert auch einen Forschungsbeitrag. Zum einen konnten die Informatiker zeigen, dass das erweiterte Modellierungssystem PRISM auf solch einen konkreten und komplexen Fall erfolgreich anwendbar ist. Dennoch verstehen sie ihre Arbeit nicht ausschließlich als Anwendung von existierenden Methoden, sondern sehen eine wichtigen methodischen Beitrag ihrer Arbeit.. Publiziert wurde die Studie auf der QEST, der renommiertesten Konferenz zum Thema Wahrscheinlichkeits- und Zuverlässigkeitsanalyse von Systemen. „Der Forschungsbeitrag besteht im Prinzip darin, dass wir eine Methode beschreiben, wie diese Technologie auf reale Szenarien anzuwenden ist", erklärt Leue. Das Ziel einer wissenschaftlichen Publikation ist also erreicht. Das allein sei schon mal gut, so der Informatiker, der in die Zukunft schaut: „Langfristig hoffen wir, dass es von Seiten der Industrie Ressourcen gibt, die uns zur Verfügung gestellt werden."

msp.