4. VDA AUTOMOTIVE SYS

Vernetztes Fahrzeug – Risiken durch Sicherheitslücken

Im Juli fand zum vierten Mal die Konferenz VDA Automotive SYS in Berlin statt. In drei Tagen konnten sich die Besucher über die neuesten Trends zum Thema Qualitäts- und Sicherheitsmanagement informieren. Leitthema waren Qualitäts- und Sicherheitsstandards in der Praxis und im Kontext zukünftiger Entwicklungen.

Die Workshops am ersten Tag der Veranstaltung boten Praxisseminare zur funktionalen Sicherheit und zum Anforderungs- und Variantenmanagement. Besonderes Interesse fand die angekündigte Version 3.0 des Standards Automotive SPICE, welche von Mitgliedern des VDA-QMC-Arbeitskreises 13 vorgestellt wurde.

Während der folgenden zwei Tage kreisten viele Vorträge um die Frage, wie eine sicherheitsorientierte Entwicklung im Rahmen der Qualitätssicherungsprozesse im Unternehmen integriert werden kann. Stellvertretend dafür war die kontrovers diskutierte Frage, wie sich Automotive SPICE als Prozessmodell mit den Prozessanforderungen der Sicherheitsnorm ISO 26262 harmonisieren lässt. Dies ist notwendig, da die Bewertung von Entwicklungsprozessen sicherheitskritischer Systeme ein wesentlicher Bestandteil des Nachweises der funktionalen Sicherheit ist.

Mit dem Sicherheitsnachweis beschäftigte sich auch die Keynote von Prof. Tim Kelly von der Universität York in Großbritannien. In ihr zeigte er anhand weniger Grundprinzipien auf, wie schlüssig nachvollziehbar dokumentiert werden kann, dass ein System die notwendige Sicherheit bietet. Dabei warb er eindringlich dafür, sich nicht mit der puren Erfüllung der Anforderungen der einschlägigen Normen zufrieden zu geben, sondern eine einfach nachvollziehbare Argumentation auf Basis geeigneter Einzelnachweise aufzubauen. Dieser überzeugende Ansatz berücksichtigt den „gesunden Menschenverstand“ und fand viel Anklang bei den Teilnehmern der Konferenz.

Neue Risiken durch IT-Vernetzung

Während die Experten noch einen gemeinsamen Prozessbewertungsansatz auf Basis von Automotive SPICE und ISO 26262 diskutieren, steht mit dem Thema Informationssicherheit schon die nächste Herausforderung an.

In der Vergangenheit waren Systeme im Kraftfahrzeug kaum oder nur im Servicefall mit ihrer Umgebung vernetzt. Heute ist die Anbindung an verschiedenste Dienste über das Internet eine in vielen Fahrzeugen verfügbare Option. Diese Vernetzung von Fahrzeugfunktionen mit der Umgebung über bekannte Informationstechnologien wird in der Zukunft zunehmen.

Der Anspruch des Kunden ist natürlich, dass diese Kommunikation sicher erfolgt. Kennt die deutsche Sprache nur den Überbegriff Sicherheit, so bezeichnet im Englischen der Begriff „Safety“ die Betriebssicherheit eines Systems. Der Begriff „Security“ steht dagegen für den Schutz eines Systems gegen den Eingriff von außen (Informationssicherheit). Dabei ist ein System im Sinne der funktionalen Sicherheit „safe“, wenn die Gefährdung von Personen durch Fehlverhalten des Systems mit ausreichend hoher Wahrscheinlichkeit ausgeschlossen ist. „Secure“ ist es, wenn das Risiko einer Beeinflussung des Systems durch außen minimiert ist. Für eine unzureichende Informationssicherheit gibt es in unserer hochvernetzten Welt bekanntlich genügend Beispiele (Hackerangriffe, gestohlene Passwörter, Datenspionage etc.).

Zunehmend beschäftigen sich die Referenten daher auch mit dem Zusammenwirken von „Safety“ und „Security“. Dabei sind die Themen durchaus verzahnt, denn ein vernetztes System kann durch einen

Foto: 123 rf © Ivan Mikhaylov und Fotolia

Autor

Dr. Jan Morenzin ist als freiberuflicher Experte für das Qualitäts Management Center im Verband der Automobilindustrie e. V. (VDA QMC) verantwortlich für das Thema Automotive SPICE und Software-Entwicklungsprozesse.

Kontakt

Dr. Jan Morenzin
morenzin.extern@vda-qmc.de

Veranstaltungshinweis

Die nächste VDA-Automotive-SYS wird von 15.–17. Juli 2015 in Potsdam stattfinden.
www.automotivesys.org

QZ-Archiv

Diesen Beitrag finden Sie online:
www.qz-online.de/921998

Prof. Tim Kelly warb für den Einsatz des „gesunden Menschenverstands".

Prof. Peter Gutzmer betonte die Integration von IT- und Automotive-Standards.

Dr. Alois Seewald erklärte die Bedingungen für ein automatisiertes Fahren in Zukunft.

Eingriff von außen negativ beeinflusst werden. Die Erfahrungen in der Vergangenheit zeigen dabei, dass eine beeinträchtigte Informationssicherheit sehr häufig auf mangelnder Prozessdefinition oder Prozessdurchführung beruht. Bei der Entwicklung einer softwarebasierten elektronischen Funktion werden zusätzlich zu den bereits bestehenden Qualitäts- und Safety-Anforderungen in Zukunft auch Security-Anforderungen eine entscheidende Rolle spielen.

Die Auswirkungen dieser Trends auf die Qualitätssicherung für softwaregestützte elektronische Systeme beleuchteten Jang Tik Siem, Leiter Konzern Qualitätssicherung Kaufteile Elektrik/Elektronik bei der Volkswagen AG, und Ulrich Schrickel, Senior Vice President der Robert Bosch GmbH, in ihren Keynotes.

Keine Sicherheit ohne Datenschutz

Ein prägnantes Beispiel für die zu erwartende Verzahnung zwischen Qualität, Safety und Security und die damit verbundene Komplexität der Aufgaben zeigt sich in einem weiteren intensiv auf der Konferenz diskutierten Trend. Zurzeit gehen die Experten davon aus, dass sich über die nächsten zwanzig Jahre eine Entwicklung vom assistierten zum voll automatisierten Fahren einstellen wird. Um sich diesem Thema zu nähern, ist eine Begriffsdefinition hilfreich, die sich danach gliedert, wie viel Kontrolle der Fahrer an das Fahrzeug abgibt.

Dabei versteht man unter assistiertem Fahren Funktionen, die den Fahrer bei Lenk-, Brems- und Beschleunigungsmanövern unterstützen. Aktuelle Beispiele dafür sind eine abstandsgesteuerte Geschwindigkeitsregelung oder eine elektronische Lenkunterstützung. Dabei muss der Fahrer jederzeit in der Lage sein, Gefahrensituationen durch eigenen Eingriff zu beherrschen. Beim teilautomatisierten Fahren übernimmt die Elektronik sowohl die Kontrolle über die Richtung als auch über die Geschwindigkeit des Fahrzeugs, jedoch muss der Fahrer wie beim assistierten Fahren jederzeit eingreifen können. Im letzten Schritt – dem voll automatisierten Fahren – ist dieser Eingriff in bestimmten oder allen Fahrsituationen nicht mehr erforderlich. Die elektronischen Systeme sind selbst in der Lage, Gefahrensituationen zu beherrschen, und der Fahrer kann Zeitung lesen, arbeiten oder einfach schlafen.

Dr. Alois Seewald, Technical Director Integrated Active & Passive Safety Technologies der TRW Automotive GmbH, gab zu diesem Thema einen Überblick über die Anforderungen an ein teil- oder sogar voll automatisiertes Fahren. Dabei wurde schnell klar, welche Vielfalt an Informationsverarbeitung und Situationsbeherrschung das System leisten muss. Dazu sind abgesicherte Informationen über den Straßenverlauf und alle statischen und dynamischen Hindernisse (andere Fahrzeuge, Personen etc.) in der Umgebung unabdingbar. Diese können nur zum Teil über optische oder radarbasierte Sensoren des Fahrzeugs ermittelt werden, der andere Teil muss durch externe Quellen zur Verfügung gestellt werden.

Ein vernetztes Fahrzeug ist dafür eine wesentliche Voraussetzung. Dabei werden in der Regel über die vorhandenen Mobilfunktechnologien Daten entweder mit der Infrastruktur der Umgebung (Car2X) oder mit anderen Fahrzeugen (Car2Car) ausgetauscht. Wo jedoch Informationen ausgetauscht werden, ist auch immer die Gefahr von Manipulation oder Störung des Flusses oder der Integrität der Daten gegeben. Die zu beherrschenden Risiken sind offensichtlich und reichen von wirtschaftlichen Schäden durch äußere Einwirkung (beispielsweise durch gezielte Blockierung des Verkehrsflusses) bis hin zur Gefährdung von Leib und Leben durch Eingriff auf die Fahrsicherheit des Autos.

Ständiger technischer Wandel bleibt Herausforderung

Eine wesentliche Herausforderung für viele Unternehmen ist dabei die Integration von allgemein bekannten Informationstechnologien unter Beibehaltung der automobilspezifischen Qualitäts- und Sicherheitsstandards. Dieser Wandel zur Integration neuer Technologien bedingt eine ständige technologische Weiterentwicklung der Unternehmen.

Ein eindrucksvolles Beispiel für einen solchen vollzogenen Wandel schilderte Prof. Peter Gutzmer, Mitglied des Vorstands und Chief Technology Officer der Schaeffler AG, anhand des eigenen Unternehmens. Dieses entwickelte sich in den vergangenen Jahren von einem Produzenten rein mechanischer Teile zu einem Systemlieferanten für mechatronische Systeme. Die Fähigkeit der Unternehmen, diese durch Technologiewandel erzeugten technologischen und organisatorischen Herausforderungen zu meistern, ist in seinen Augen ein wichtiger Faktor für die Zukunftssicherung des Technologiestandorts Deutschland.

Die Auswertung des Teilnehmerfeedbacks zeigte eine durchgängige Steigerung der Bewertung von Workshops und Fachvorträgen im Vergleich zum bereits guten Niveau des Vorjahres. Aufgrund der Relevanz von „Security" hat das VDA QMC entschieden, den Fokus der Konferenz künftig um dieses Thema zu erweitern. □

Jan Morenzin, Berlin