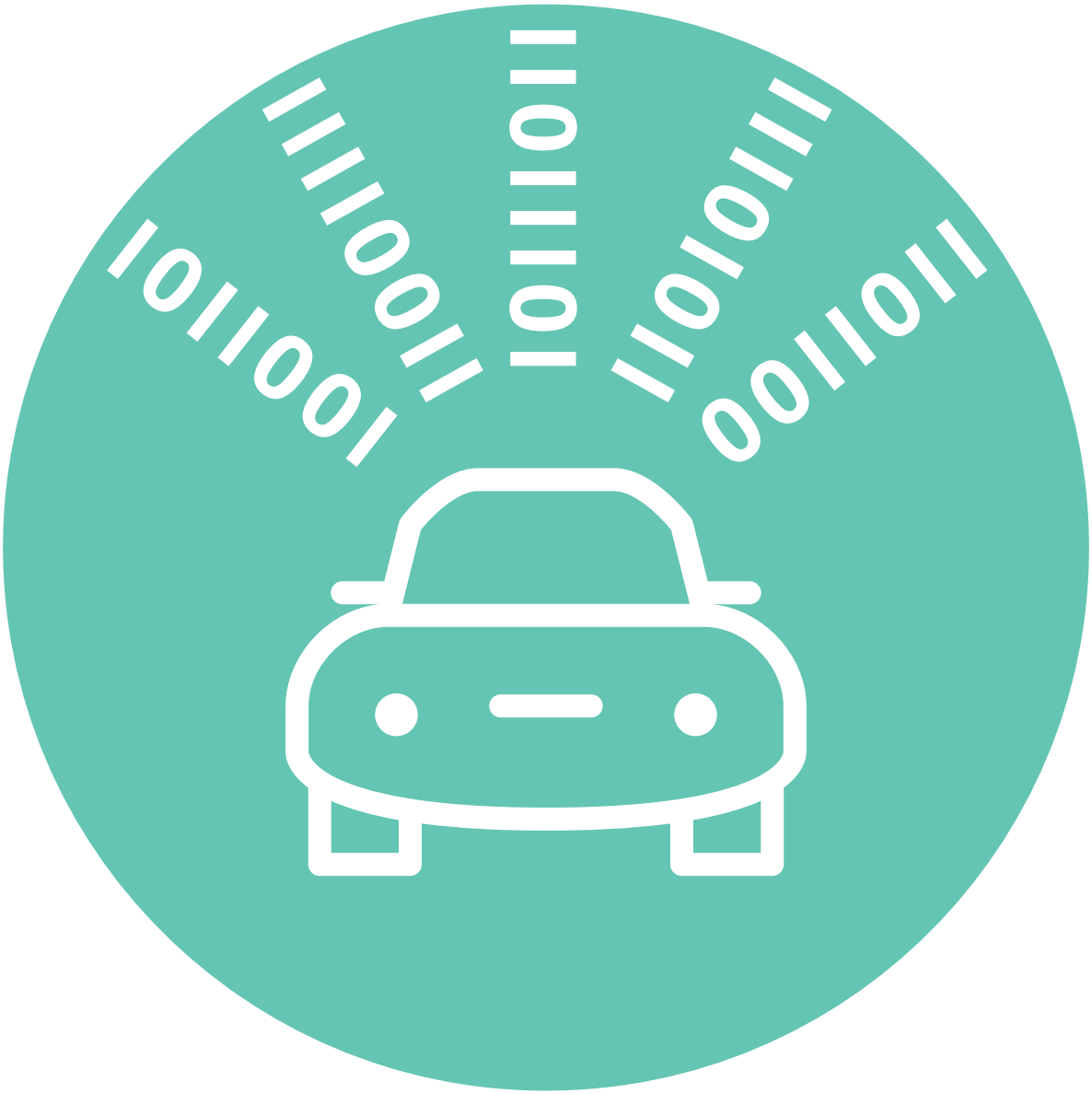
Deloitte.



Automotive Software Quality

Was OEMs heute
für morgen beachten müssen

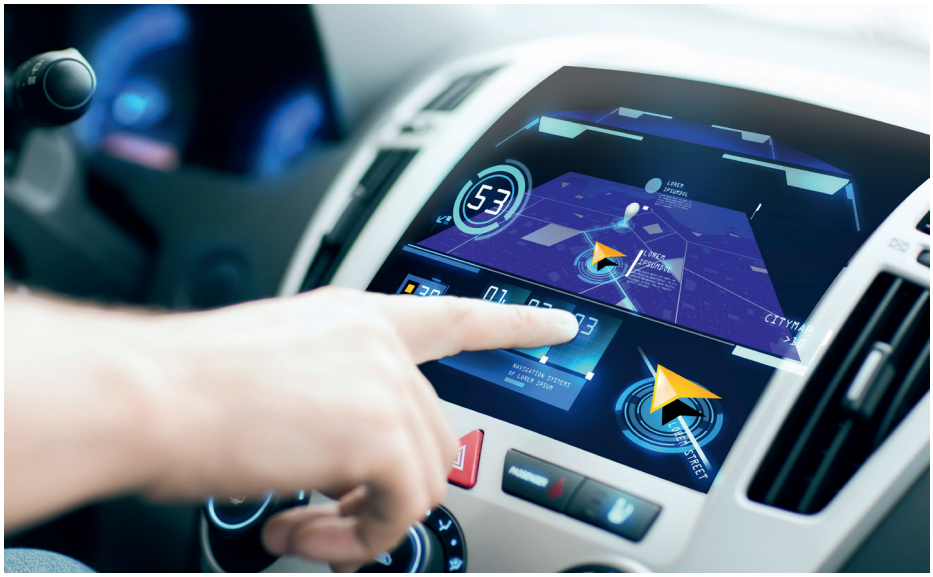
Die Automobilindustrie befindet sich in einem tiefgreifenden Wandel. Hersteller, Branchenverbände und Politik müssen möglichst schnell auf technische und gesellschaftliche Megatrends reagieren und sich auf veränderte rechtliche und wirtschaftliche Rahmenbedingungen einstellen. Das wirklich Neue daran ist, dass erstmals Software eine wettbewerbsentscheidende Rolle spielt.

Aus einer globalen Sicht des Mobilitätsmarktes ist die Entwicklung selbstfahrender Fahrzeuge alternativlos.

Die Entwicklung hochautomatisierter Fahrzeuge für den Straßenverkehr erfordert enorme Investitionen. Die globalen F&E-Ausgaben der deutschen Automobilindustrie wachsen jährlich mit deutlich zweistelligen Raten und haben im Jahre 2015 die Marke von 39 Mrd. Euro überschritten – in den nächsten Jahren ist aufgrund der anstehenden Herausforderungen mit weiteren Steigerungen zu rechnen. Damit sich diese Investitionen lohnen, müssen hochautomatisierte Fahrzeuge im Markt akzeptiert und nachgefragt werden. Um den Markterfolg zu sichern, sind zwei Faktoren entscheidend:

- Der Bedarf zum Beispiel durch mehr Komfort und Zeitgewinn sowie durch höhere Sicherheit muss geschaffen werden. Prestige und technologischer Führungsanspruch treten bei künftigen Käuferschichten gegenüber Mobilität und ökologischen Aspekten etwas in den Hintergrund.
- Neben der Vermittlung des Nutzens ist das nachhaltige Schaffen von Vertrauen in die neue Technologie ein wesentlicher Punkt, um langfristig erfolgreich zu sein. Hochentwickelte und kreative Technologie für sich allein kann nur kfr. Nachfrage erzeugen. Wenn Qualität und Zuverlässigkeit nicht gewährleistet sind, sind die anschließende Enttäuschung und die negative Marktreaktion deutlich ausgeprägter als ohne vorangegangenen Technik-Hype. Fehlende Qualität im Falle hochautomatisierter Fahrzeuge ist nicht nur ärgerlich – sie ist gefährlich. Und das ist wohl die größte Herausforderung: Wer kein Lenkrad in der Hand hat, neigt zunächst einmal dazu, sich ausgeliefert zu fühlen und Risiken als sehr hoch einzuschätzen. Das Beispiel des Tesla-Autopiloten, der im Sommer 2016 die weiße Seitenwand eines kreuzenden Lkw für Freiraum hielt und in die Kreuzung hineinfuhr – der Tesla-Fahrer starb –, dürfte diese Wahrnehmung verstärkt haben.

Die Ausgangssituation wird anhand einiger Zahlen einer aktuellen Studie von Deloitte[1] deutlich: Hochautomatisierte Fahrzeuge (teilautonomes und autonomes Fahren) finden nur in China und Indien bei deutlich über der Hälfte der Befragten Akzeptanz. In den traditionellen Auto-Ländern wie USA, Japan, Südkorea und Deutschland liegt dieser Wert deutlich unter 50 Prozent – mit knapp unter 25 Prozent in Deutschland sogar mit Abstand am niedrigsten. Die gute Nachricht ist, dass das Interesse am teilautonomen und autonomen Fahren über alle einbezogenen Länder bei den jüngeren Generationen (Generation Y/Z) am höchsten ist. Der wichtigste Grund für diese möglicherweise unerwartet geringe Akzeptanz ist das Gefühl der Konsumenten, dass selbstfahrende Autos nicht sicher sind. Die Anzahl der Studienteilnehmer mit dieser Meinung schwankt hier zwischen 62 (China) und 81 Prozent (Südkorea). Deutschland liegt mit 72 Prozent in etwa in der Mitte. Etwas zuversichtlicher werden die potenziellen



[1] What´s ahead for fully autonomous driving – Consumer opinions on advanced vehicle technology – Perspectives from Deloitte´s Global Automotive Consumer Study (22.000 Befragte aus 17 Ländern).

Steigende Anforderungen hinsichtlich Performance, Kompatibilität und Wartbarkeit erzwingen eine zunehmende Standardisierung der IT in Fahrzeugen.

Kunden, wenn über eine gewisse Zeit der Nachweis geführt werden kann, dass selbstfahrende Fahrzeuge sicher sind. Unter diesen Umständen wären von 47 (Deutschland) bis zu 81 Prozent (China) der Befragten bereit, solche Fahrzeuge zu nutzen.

Es wird deutlich, dass mehr Sicherheit und Komfort im Vergleich zu herkömmlichen Pkw nicht ausreichen werden, um autonome Fahrzeuge zum Markterfolg zu führen. Es müssen Wege gefunden werden, das Vertrauen in diese Technologie zu entwickeln und zu erhalten. Wenn dies den traditionellen Automobilherstellern nicht gelingt, dann stehen andere Unternehmen bereits in den Startlöchern, um deren Rolle zu übernehmen.

Aus einer globalen Sicht des Mobilitätsmarktes ist die Entwicklung selbstfahrender Pkw alternativlos: Sie brauchen – und haben –das Potenzial, den Individualverkehr von Grund auf zu verändern, besonders im urbanen Raum. Verkehrs- und Parkflächen werden knapper und teurer, die Ownership-Kosten eines Autos steigen. Alternative Formen der persönlichen Mobilität, mit Fahrzeugen, die im öffentlichen Raum für die geteilte Nutzung zur Verfügung stehen, ergeben auf Dauer wesentlich mehr Sinn – sowohl hinsichtlich der Kosten als auch, was Komfort und Sicherheit angeht. Selbstfahrende Autos sind hierfür wesentlich besser geeignet als herkömmliche Individualfahrzeuge.

Der Marktwandel spielt sich in vier wesentlichen Bereichen ab:

- Im Fokus stehen emissionsfreie Fahrzeuge samt Lade-Infrastruktur, die hohe Leistungen und Reichweiten ermöglichen, und das zu Preisen, die den Umstieg von fossiler auf elektrische Energie attraktiv machen.
- Assistenzsysteme gewinnen an Bedeutung, bis hin zum autonomen Fahren; die Fahrzeuge müssen zu diesem Zweck miteinander, aber auch mit den sie umgebenden Infrastrukturkomponenten kommunizieren.
- Schließlich wachsen den Fahrzeugen immer mehr digitale Funktionen zu, die es ihren Nutzern ermöglichen, während der Fahrt zu kommunizieren, zu arbeiten oder multimediale Unterhaltung zu genießen.
- Die Zunahme von autonomen Fahrfunktionen in Verbindung mit den Möglichkeiten, Fahrzeuge auch softwaregesteuert zu individualisieren, bedeutet eine immer höhere Attraktivität von „Shared Cars“. In diesen Fällen werden Fahrzeuge von spezialisierten Mobilitätsdienstleistern ständig bereitgehalten und sind dadurch im Gegensatz zu herkömmlichen Mietfahrzeugen auch für sehr kurze Strecken in der Stadt eine interessante Mobilitätsalternative – nicht zuletzt dadurch, dass sie flächendeckend verfügbar sind und die Suche nach knappem und teurem Parkraum durch reservierte Stellflächen für die Shared Cars entfällt.

In allen vier Domänen nehmen Daten sowie Software zu ihrer Übermittlung und Verarbeitung zentrale Funktionen ein. Alle Marktakteure müssen sich darum vier Fragen stellen, deren Beantwortung die Rolle der Software im Auto definieren wird. Zu den Akteuren zählen vor allem Entwicklung, Produktion und Qualitätssicherung aufseiten der Autohersteller, aber auch IT-Bereiche der OEMs und IT-Service-Anbieter (z.B. Cloud, Telekommunikation) sowie der Gesetzgeber und Standardisierungsgremien. – Die Fragen:

1. Wie wird die Qualität softwarebasierter Funktionen in Autos definiert und sichergestellt?
2. Wie können Autohersteller ihre Marken vor Schaden durch Qualitätsprobleme und ihre rechtlichen Folgen schützen und welche Rolle spielt dabei die Softwareentwicklung?
3. Welche Herausforderungen für die OEMs ergeben sich aus den Sicherheits- und Datenschutzanforderungen durch Vernetzung von Fahrzeugen und Infrastruktur (z.B. Cyber-Security-Anforderungen) und wie können die Hersteller ihnen begegnen?
4. Sind zusätzliche gesetzliche Regulierungen (z.B. weitere Zulassungsvoraussetzungen/-prüfungen) erforderlich, um den Änderungen im Fahrzeug sowie im Verkehr insgesamt Rechnung zu tragen?

Bei der Auseinandersetzung damit stützen wir uns auf Erfahrungen aus vergangenen und aktuellen Projekten im Automobilsektor.

1. Wie wird die Qualität softwarebasierter Funktionen in Autos definiert?

Hier gibt es noch viel zu tun: Es sind weder umfassende und allgemeingültige regulatorische Normen, die zum Beispiel als Anforderungen an eine Typenzulassung aufgesetzt sein könnten, noch eingespielte Software(!)-Qualitätssicherungsmaßnahmen und -prozesse bei den Autoherstellern verfügbar. Aktuelle Entwicklungsrichtlinien wie ISO 26262 oder Auditierungsstandards wie Automotive Spice, CMMI oder Misra setzen lediglich auf die unstrittige Tatsache, dass ein gut strukturierter und zuverlässiger Prozess auch ein gutes Ergebnis erzeugt. Inhaltliche Prüfungen jedoch, wie sie für Komplexität und Funktionsumfang von Software zur Steuerung von Fahrzeugen angemessen wären, sind nicht Bestandteil dieser Standards und werden nur im Ausnahmefall durchgeführt.

Aktuelle Tests beruhen auf Risikoszenarien und Testverfahren, die je OEM und Zulieferer unterschiedlich sind. ISO 26262 sieht dabei richtigerweise vor, dass die Tests je nach Risikoeinschätzung für die zu entwickelnden Funktionen und Module unterschiedlich genau und intensiv sind. Die Verfahren hängen jedoch von den Einschätzungen einzelner Personen sowie von den Prozessen ab, die in einem Unternehmen etabliert sind; oftmals auch vom aktuellen Zeitdruck bis zum SoP (Start of Production). Was es nicht gibt, ist ein allgemeingültiges und verpflichtendes Set an Risiko- und Testszenarien.

Solche – zusätzlichen – Tests wären teuer und würden Entwicklungen verzögern. Um dem gegenzusteuern, könnte der Gesetzgeber für Entlastung sorgen, indem er Mindestanforderungen an Sicherheit und Zuverlässigkeit formuliert und dies über die Typenzulassung durchsetzt. Ein deutscher Alleingang wäre dabei freilich weder sinnvoll noch zulässig; die Anforderungen deutscher Gesetze müssten jedoch unbedingt auf europäischer-Ebene, bei der UN sowie im G7-Rahmen nachdrücklich vertreten werden. Beispiele dafür gibt es aus der Luftfahrtindustrie sowie der medizinischen Apparatetechnik.

Steigende Anforderungen hinsichtlich Performance, Kompatibilität und Wartbarkeit erzwingen eine zunehmende Standardisierung der IT in Fahrzeugen. Auch dadurch rückt das Thema Cyber Security immer stärker in den Fokus der Fahrzeugsicherheit und wird damit zum festen Bestandteil des Themas Softwarequalität. Denn während gegenwärtige Fahrzeuge zwar einzeln angegriffen werden können, sind sie durch ihre proprietären, individuellen Architekturen vor massenhaften Hacker-Attacken oder Virenbefall zu einem gewissen Grad geschützt. Das wird sich durch die Standardisierung ändern; Maßnahmen zur Sicherung der rollenden Rechenzentren sowie der von ihnen online genutzten Backbones (Cloud-Services) sind deshalb dringend erforderlich und müssen Bestandteil künftiger Risikoszenarien und Testanforderungen sein. Entsprechende Hinweise beziehungsweise Richtlinien existieren bereits, nicht nur von der deutschen, sondern auch von der amerikanischen und der japanischen Regierung.

In der Zukunft der Automobilentwicklung wird Software der dominante Faktor sein.

Automobilhersteller und ihre Lieferanten sind an höchster Qualität orientiert, was sich in der Zuverlässigkeit und Langlebigkeit heutiger Fahrzeuge bei immer höherer Leistung und Funktionalität zeigt. Rostende Karosserien, häufige Reifenpannen, permanentes Nachfüllen von Motoröl, hakelnde Getriebe – das und mehr sind weitgehend Probleme von gestern. Sie haben jedoch eines gemeinsam: Es geht um Hardware. In der Zukunft der Automobilentwicklung wird jedoch Software der dominante Faktor sein. Hier sind neue Qualitätsmechanismen gefragt. Das hat eine Reihe von Gründen:

Dynamik

Im Gegensatz zu Karosserie- oder Motorteilen, die sich über den Lebenszyklus eines Fahrzeugs nicht verändern, unterliegt Software einer hohen Dynamik. Diese entsteht durch geänderte beziehungsweise neue Funktionen sowie durch Updates zur Fehlerbehebung oder zur Risikominderung, etwa hinsichtlich potenzieller Risiken durch Cyber-Angriffe.

Lebenszyklus

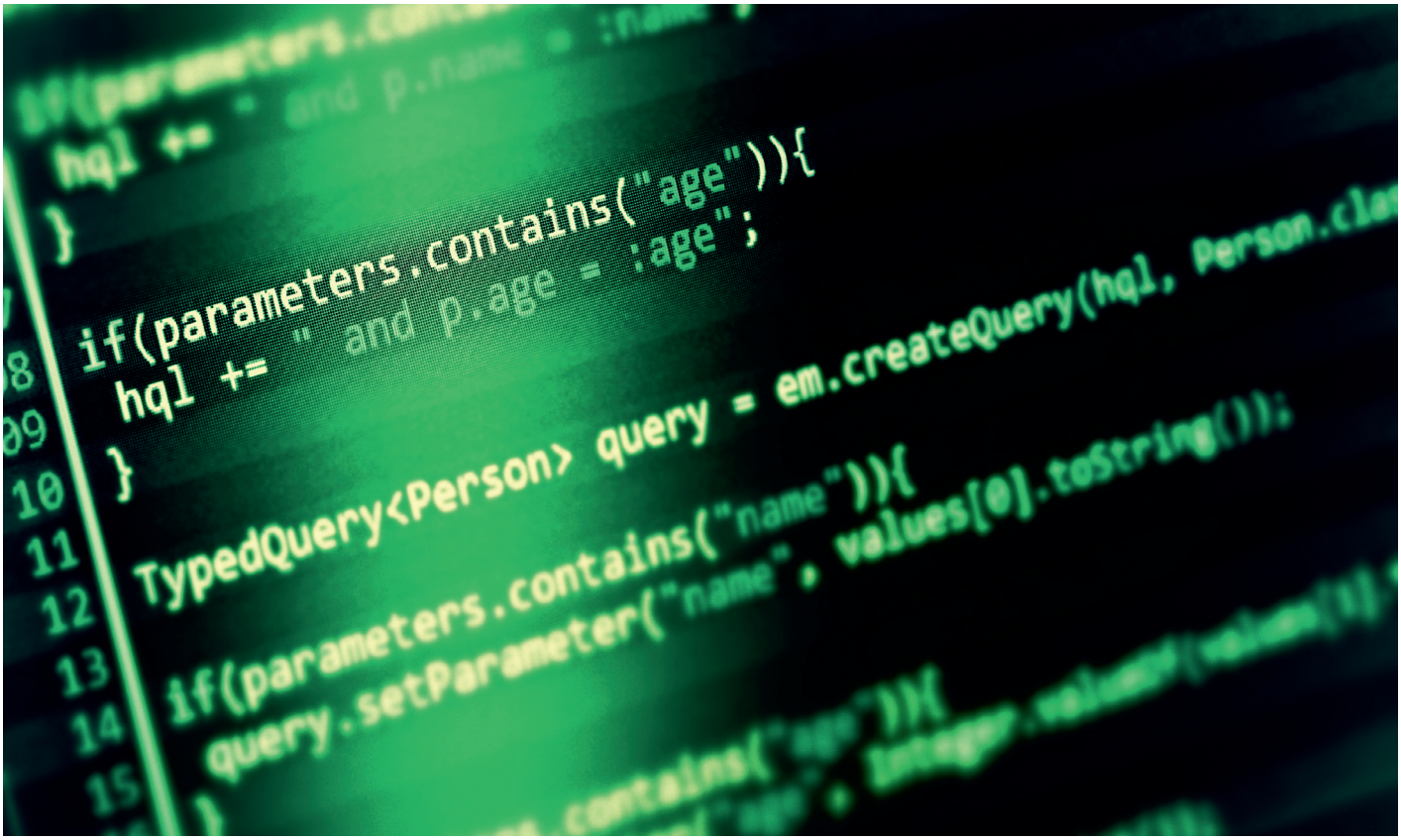
Der Lebenszyklus von Software im Sinne von Entwicklung, Herstellung, Nutzung, Weiterverkauf und Verschrottung ist nicht vergleichbar mit entsprechenden Hardware-Zyklen. Nutzungsbedingungen (Lizenzierung), Nutzungsübergang, eventuell im Fahrzeug installierte Zusatzfunktionen, Übertragung von Datenschutzregelungen auf verschiedene Fahrzeugnutzer, Datenlöschung bei Weiterverkauf oder Nutzungsende sowie die Sicherstellung der langfristigen Kompatibilität von Formaten zum Datenaustausch: Das sind nur einige Beispiele, die die Notwendigkeit einer differenzierten Handhabung deutlich machen.

Komplexität

Software ist nicht als ein Teil oder Modul im Fahrzeug vorhanden, sondern steckt in einer Vielzahl von Bauteilen (ECUs) mit unterschiedlichsten Aufgaben. Selbst Reifen und Stoßdämpfer sowie Querlenker haben bei neueren Fahrzeugen Sensoren und melden bestimmte Zustände – entweder fest verdrahtet oder über integrierte Softwaremodule. In jedem Fall entsteht durch eine Vielzahl von Sensoren, Aktoren und Control Units im Fahrzeuge umfangreicher Datenverkehr, der empfangen, verstanden und interpretiert werden muss. Auch Informationen von außerhalb des Fahrzeugs tragen zunehmend zu diesem Datenvolumen bei. Derzeit betrifft das vor allem Informationen zur Navigation (inklusive Telematik-Services); mit Kurzstreckenfunkverbindungen zwischen Fahrzeugen (Car to Car) beziehungsweise von Fahrzeugen zu externen Komponenten (Car to Infrastructure) werden jedoch bereits weitere Verbindungen diskutiert. Datenmengen und Verarbeitungsmechanismen befinden sich dadurch auf einer steil ansteigenden Kurve mit immer höherer Komplexität und damit neuen Herausforderungen; eine Entwicklung, die es so bei Hardware nicht gibt.

Testverfahren

Die Funktionalitäten der Hardware eines Fahrzeugs – auch in komplettierter Interaktion miteinander – sind endlich und können nach sorgfältiger Qualitätssicherung einzelner Komponenten virtuell sowie im praktischen Einsatz auf Teststand, -strecke oder Straße umfassend geprüft werden. Software dagegen ist für umfassende Tests zu komplex in ihrer möglichen Funktionalität und kann darum auch niemals als vollständig fehlerfrei angesehen werden. Testverfahren werden daher an bestimmten Risiken ausgerichtet: Durch maschinelle Lösungen wie HIL, SIL oder VIL[2] wird eine möglichst hohe Abdeckung angestrebt und erreicht. Dabei kommt es darauf an, dass die abzudeckenden Risikoszenarien und entsprechende Tests bereits in der Konzeptionsphase der Software mit entwickelt werden (Security by Design), da ein rückwirkendes Aufrollen der aufgesetzten komplexen Funktionen mit hoher Sicherheit zu Fehlern und Lücken führt. Je zentraler die Fahrzeugarchitektur ist, desto besser können Test vorbereitet und durchgeführt werden; dezentrale Module müssen gemäß ihres Funktionsumfangs vollständig getestet sein, bevor sie in einen Integrationstest aufgenommen werden.



[2] Hardware in the Loop, Software in the Loop, Vehicle in the Loop.

Supply Chain
Einem integrierten Vorgehen bei der Softwareentwicklung und koordinierten Tests steht derzeit die branchentypische Komplexität der Supply-Chain-Struktur entgegen. Der Löwenanteil von Software in Fahrzeugen wird von Drittanbietern zugeliefert. Entwicklungs- und Testverfahren sowie der Quellcode sind für den Fahrzeughersteller oft intransparent. Bereits genannte Verfahren zur Qualitätssicherung (Spice, CMMI, Misra etc.) werden in Form vertraglicher Zusicherungen von Lieferanten eingefordert und oft in Stichproben überprüft. Inhaltliche Prüfungen, der Nachweis erfolgter Tests sowie die stichprobenartige Überprüfung von Quellcodes finden dagegen nur selten statt.

Vernetzung von Kompetenzen
Bei den Autoherstellern arbeiten die für Fahrzeug- beziehungsweise Datensicherheit zuständigen Stellen nicht systematisch zusammen – oder sie verstehen einander nur unzulänglich. Mehr noch: Autos sind künftig Teile eines Hochleistungsnetzwerks, zu dem auch Plattformtechnologie und Komponenten von Drittanbietern gehören. Künftige Security-Konzepte müssen diesen hohen Vernetzungsgrad berücksichtigen. Heute tun sie es noch nicht.

IT-Kompetenzaufbau
Die klassischen Autohersteller sind noch nicht dafür aufgestellt, IT-relevante Kriterien – vor allem Datenintegrität sowie Verlässlichkeit und Verfügbarkeit der Software – auch für ihre Produkte sicherzustellen. Sie müssen hier Kompetenz aufbauen und einschlägige Testverfahren entwickeln. Es gilt wie in der Flugzeug- oder der medizinischen Apparate-Industrie, eine Datenbank aller denkbaren Risikoszenarien aufzubauen und ständig zu aktualisieren, sobald neue Risiken erkennbar werden. Für künftige Typenzulassungen ganz oder teilweise automatisierter Fahrzeuge werden erweiterte Sicherheitsprüfungen und auch praktische Tests erforderlich. Darauf sollten sich die Autohersteller vorbereiten.

Mehr als 100 Millionen Codezeilen stecken in den Steuer-, Assistenz- und Multimediafunktionen von unterschiedlichen Zulieferern, über die ein Luxusauto heute verfügt.

2. Wie können Autohersteller ihre Marken vor Schaden durch Qualitätsprobleme und ihre rechtlichen Folgen schützen und welche Rolle spielt dabei die Softwareentwicklung?

Fahrer hochautomatisierter Fahrzeuge wollen sicher sein; Qualitätsanforderungen für Software müssen das berücksichtigen. Kommt es zu einem Unfall, den sie selbst nicht herbeigeführt haben, stellt sich zudem die Haftungsfrage. Wenn Fahrer für Softwarefehler haften müssen, die ihnen nicht einmal bekannt waren, dann findet das sicherlich keine Akzeptanz. Darum muss jede Softwareentscheidung dokumentiert werden, denn auch eine richtige Entscheidung kann zum Unfall führen – die Alternative hätte ja noch schlimmer sein können. Beispiel: Ein Fahrzeug weicht einem Menschen aus und stößt dadurch mit einem anderen Fahrzeug zusammen.

Die Diskussion im Folgenden dreht sich letztendlich vor allem um eine wesentliche Frage: Können die Kunden Vertrauen zu den OEMs und deren Produkten haben? Hinsichtlich Software und Datenschutz sind dafür zwei wesentliche Aspekte zu betrachten:

Blackbox vs. offene Systeme
Besonders schwierig werden die Sicherung eines umfassenden Qualitätsversprechens der OEMs und die Dokumentation von automatisierten Entscheidungen in Fahrzeugen dadurch, dass Software in Fahrzeugen meist von Komponenten-Drittanbietern (die Bandbreite reicht hier von globalen Großunternehmen bis zu kleinen innovativen Start-ups) stammt und dass in ihr schützenswertes geistiges Eigentum steckt. Der Quellcode wird deshalb bislang

nur in wenigen Fällen offengelegt, sondern bleibt eine Blackbox. Dadurch bleibt zwangsläufig unklar, wo Qualitätsrisiken bestehen oder wie eine Softwareentscheidung in einer autonomen Fahrsituation zustandekommt. Autohersteller müssen das in künftigen Verträgen mit ihren Komponenten- und Softwarelieferanten berücksichtigen und ändern – mit tiefgreifenden Auswirkungen auf die Test-, Review- und Audit-Prozesse.

Vertrauensvorsprung bewahren

Fahrzeughersteller genießen hinsichtlich der Produktqualität und des sensiblen Umgangs mit Daten einen Vertrauensvorsprung gegenüber IT-Konzernen. Hardware und Systemsoftware kommen aus einer, nämlich ihrer Hand. Die extrem hohen Qualitätsansprüche in der Automobilbranche sind bekannt und haben zu sehr hochwertigen und zuverlässigen Fahrzeugen auf unseren Straßen geführt. Diese Qualitätsansprüche auf die Entwicklung und Wartung von Software auszudehnen, ist ein kritischer Erfolgsfaktor zum Erhalt oder gar Ausbau des Vertrauensvorsprungs gegenüber IT-Konzernen oder andere Newcomern auf dem Mobility-Spielfeld.

Die Kunden vertrauen den OEMs, was deren Umgang mit personenbezogenen Daten betrifft. Dass Fahrzeughersteller mit Daten vertraulich umgehen – anders als Microsoft, Google, Apple etc. – hat die Vergangenheit gezeigt. Kaum ein einschlägiger Skandal hat diese Branche bislang erschüttert. Das Problem jedoch: Eine intensive Nutzung von Daten befindet sich bei den OEMs auch erst in den Kinderschuhen. Kommunikations- und Media-Apps werden aber immer wichtiger, besonders in selbstfahrenden Fahrzeugen. Damit eine individualisierte und integrierte Funktionalität, wie man sie vom Smartphone gewohnt ist, realisiert werden kann, müssen Daten jedoch ausgetauscht und miteinander verknüpft werden. Die Herausforderung besteht nun darin, eine Balance zwischen minimaler Nutzung personenbezogener Daten und der bestmöglichen Customer Experience zu finden und die verwendeten Daten bestmöglich zu schützen. Dieser Schutz muss auch auf Apps von Dritten sowie potenzielle Plattformen zum Verkauf der Apps und andere von den Fahrzeugen verwendete Backbones ausgedehnt werden.

Zur Verwaltung von Fahrzeugdaten könnte beispielsweise ein unabhängiges „Trust Center“ eingerichtet werden, das alle im Fahrzeug erzeugten Daten verwaltet, hinsichtlich Relevanz für den Datenschutz überprüft und auf Anfrage in einer gesetzeskonformen Ausführung bereitstellt sowie dabei natürlich auch Datensicherheitsstandards einhält. Das Trust Center als vertrauenswürdiger Dritter nimmt damit eine Vermittlerposition zwischen Dateninhabern und (potenziellen) Nutzern der Daten ein. Datenanfragen werden hier geprüft und datenschutzgerecht beantwortet, wenn deren Berechtigung festgestellt wurde.

Mehr als 100 Millionen Codezeilen stecken in den Steuer-, Assistenz- und Multimediafunktionen von unterschiedlichen Zulieferern, über die ein Luxusauto heute verfügt. Um diesen Umfang und diese Komplexität auf Dauer handhaben und gleichzeitig Entwicklungszyklen beschleunigen sowie rasche Software-Updates bereitstellen zu können, werden neue Entwicklungsmethoden und Formen der Zusammenarbeit über die gesamte Supply Chain benötigt. Im Folgenden werden einige der wesentlichen Punkte zu diesem Thema diskutiert.

Nur eine offene Systemarchitektur kann umfassend getestet und ständig verbessert werden

Bisher werden Softwarefunktionen im Auto nach der ISO-Norm 26262 entwickelt. Autohersteller und Zulieferer arbeiten dabei jedoch selten so zusammen, wie es für die Entwicklung und ständige Verbesserung von Software notwendig wäre; Zulieferteile samt Software werden als Blackbox behandelt. Die Anwendung traditioneller Supply-Chain-Prozesse aus der Automobilindustrie führt bei Software in eine Sackgasse, da wesentliche Ziele der Entwicklungsgeschwindigkeit, -sicherheit/-integrität und -nachvollziehbarkeit nicht in ausreichendem Maß realisierbar sind; mithin also aus einer ganzheitlichen Sicht die Softwarequalität des Produkts auf der Strecke bleibt. Obwohl die meisten Fahrzeuge im Detail unterschiedliche Kommunikationsnetze aufweisen, werden große Teile der Information über die CAN-Bus-Architektur und verteilte elektronische Steuereinheiten (ECU) für unterschiedliche Funktionen übertragen. Eine offene Systemarchitektur, mutmaßlich unter einem gängigen und performanten Betriebssystem – z.B. auf Linux basierend – wird die proprietäre Architektur auf Dauer ablösen. Die Entwicklung bewegt sich hin zu einer wesentlich stärkeren Zentralisierung der IT-Architektur im Fahrzeug, durch die auf einem standardisierten Betriebssystem bestimmte Funktionalitäten oder Apps zum Einsatz kommen. Der Zugriff auf die Hardware bleibt – wie in heutigen modernen IT-Architekturen – dem Betriebssystem vorbehalten.

Mittel- bis langfristig ergeben sich aus einer solchen Architektur wesentliche Vorteile in der Wartbarkeit und der Erweiterung von Funktionen. Zudem können Entwicklungsprozesse auf die eigentliche Funktionalität innerhalb vorgegebener Standards fokussieren und dadurch schneller und ablaufen. Tests und Dokumentation sowie eine Zusammenarbeit in der Lieferkette werden ebenfalls erleichtert. Hier leistet die Entwicklungspartnerschaft AUTOSAR wesentliche Pionier- und Grundlagenarbeit durch die Entwicklung eines künftigen Industriestandards für Systemsoftware in Fahrzeugen.

Bereits jetzt hat eine Reihe von Herstellern angekündigt, ihre Architekturen offenzulegen. Dahinter steckt oft der Wunsch, sich gegen mächtige Wettbewerber aus dem Bereich der Betriebssysteme und des Geschäfts mit Daten (Apple, Microsoft, Google etc.) durch eine übergreifende Zusammenarbeit zu wappnen. Indes: Für diese öffentlichkeitswirksam angekündigten Initiativen fehlen den betreffenden Herstellern und Herstellergruppen aus dem Automobilmarkt jedoch meist entscheidende Grundlagen:

1. Das geistige Eigentum an den über die gesamte Automobil-Wertschöpfungskette verteilten Komponenten. Deshalb können immer nur Teile eine (Betriebs-)Systems tatsächlich für Dritte geöffnet werden, ohne das geistige Eigentum anderer zu verletzen.
2. Agile und dennoch sehr zuverlässige Methoden zur Softwareentwicklung, die mit den über Jahrzehnte entwickelten Verfahren der IT- und Internet-Riesen konkurrieren können.

Es überrascht darum nicht, dass ausgerechnet ein – aus der Betrachtung des Marktanteils heraus völlig unbedeutendes – Unternehmen derzeit die gesamte Automobilbranche aufmischt und in Sachen Technik die Trends setzt: Tesla. Im Gegensatz zu den traditionellen Herstellern mit ihren wenig flexiblen Strukturen hatte Tesla die Möglichkeit, ein Unternehmen auf der grünen Wiese aufzubauen und es auf die kommenden technologischen Herausforderungen auszurichten. Ein Schwerpunkt ist dabei die rasche und zuverlässige Entwicklung von Software, die – wie bei den Wettbewerbern aus dem IT- und Internet-Umfeld – mit einer Basisfunktionalität und -sicherheit auf den Markt kommt und über fortwährende Updates in beiden Bereichen ständig verbessert wird. Wie bei den Betriebssystemen auf PCs und Handys sind es die User (hier: Fahrer) selbst, die die Daten für die Verbesserungen liefern. Das geschieht meist nicht aktiv, sondern durch automatisch übersandte Protokolle aus dem Betriebssystem der Fahrzeuge. Dass die wesentlichen Teile des geistigen Eigentums bei Tesla liegen und agile Entwicklungsmethoden angewandt werden, leuchtet darum ein. Nicht umsonst sehen einige der großen traditionellen Fahrzeughersteller bereits jetzt vor allem Tesla als Wettbewerber. Sie wissen, warum.

Es ist keine Frage, dass die großen OEMs überall auf der Welt (noch) die besseren Fahrzeuge bauen können. Aber während bei den traditionellen Autobauern Qualität noch an traditionellen Parametern wie den Spaltmaßen gemessen, ein Fahrzeug zu 100 Prozent fertig gebaut, dann auf den Markt gebracht und möglichst nicht mehr angefasst wird, stellt Tesla seine Software-Qualität durch allein 200 Online-Updates im letzten Jahr sicher und hält dabei die Funktionalität seiner Fahrzeuge stets auf dem neuesten Stand beziehungsweise erweitert sie sogar. Das geschieht zum Teil auch als optionales Angebot an die Fahrzeugeigentümer; das Geschäft der Zukunft ist hier schon Realität. Produktpflege bei den klassischen OEMs bedeutet vor allem die Entwicklung der nächsten Fahrzeuggeneration bzw. der Facelift in einer Baureihe, während Tesla die auf dem Markt befindlichen Produkte permanent weiter pflegt. Das kannten wir bislang v.a. von IT- und TK-Endgeräten. Dies heißt nicht, dass der Weg, den Tesla beschreitet, der beste Weg ist – es ist aber ein anderer. Fahrer und deren Fahrzeuge als Beta-Tester einzusetzen, kann mitunter zu gefährlichen Situationen führen. Die Vorteile beider Varianten – d.h. umfassende Qualitätsansprüche und der Wunsch, ausgereifte Funktionalitäten auf den Markt zu bringen, in Verbindung mit agilen Entwicklungsmethoden und ausgefeilten Vorgehensweisen für stufenweise Tests, Online-Update-Fähigkeiten und ein permanenter Verbesserungsanspruch auch zur Laufzeit des Fahrzeugs – sind der bessere Weg in die Zukunft.

Erste Schritte der OEMs, kleine und bewegliche – auch rechtlich selbstständige – Geschäftseinheiten aufzubauen und die wesentliche Entwicklungsverantwortung in deren Hände zu legen, gehen in die richtige Richtung. Zur Umsetzung der dort entwickelten Vorgaben werden aber meist noch die bisherigen Strukturen benutzt. Und spätestens hier sind alle innovativen Ideen in der Gefahr, ins Stocken zu geraten. Mittelfristig führt daher kein Weg an einer neuen Organisation sowohl der OEMs selbst als auch der zugehörigen Supply Chain vorbei.

3. Welche Herausforderungen für die OEMs ergeben sich aus den Sicherheits- und Datenschutzanforderungen durch Vernetzung von Fahrzeugen und Infrastruktur (z.B. Cyber-Security-Anforderungen) und wie können die Hersteller ihnen begegnen?

Autos werden zunehmend intern vernetzt und immer enger mit dem Internet verbunden sein, aber sie sind heute weniger wirksam geschützt als Bürocomputer, Handys und Tablets. Um das zu ändern, muss der gesamte Qualitäts- und Safety-Prozess, wie er in der ISO-Norm 26262 vorgeschrieben ist, angepasst werden. Was die Branche braucht, sind Cyber-spezifische Risikoszenarien, und sie müssen sowohl in der Softwareentwicklung als auch bei der Komponentenfertigung zum Tragen kommen.

Wartungsplattformen für den Online-Zugriff von Herstellern und Werkstätten auf Fahrzeuge müssen zwingend Bestandteil dieser Szenarien und somit Teil einer umfassenden Security Governance sein mit dem Ziel, Fahrzeuge widerstandsfähig gegen Cyber-Angriffe zu machen.

An dieser Stelle könnte der in Entwicklung befindliche Standard ISO 21434 für Automotive Cyber Security weiterhelfen: Die daraus resultierenden Vorgaben müssen aber auch zunächst in Entwicklungsverfahren in der gesamten Supply Chain umgesetzt und – ganz wichtig! – im Weiteren überwacht werden. Außerdem ist heute noch nicht sichergestellt, dass künftige Anforderungen an die Typenzulassung samt gegebenenfalls zusätzlicher Tests der technischen Dienste zu 100 Prozent im Einklang mit diesem ISO-Standard stehen werden, da sich alle diese Dinge derzeit parallel entwickeln. Sicher ist lediglich, dass sich regulatorische Anforderungen auf weit mehr als allein auf die Cyber Security beziehen werden. Die Qualität der in Fahrzeugen verwendeten Software sowie der Schutz personenbezogener Daten werden eine ebenso wichtige Rolle spielen und müssen in die Risiko- und Testszenarien der Fahrzeughersteller und ihrer Lieferanten einfließen.

Online-Updates der Autosoftware ohne Werkstattbesuch sind sowohl im Safety- als auch im Security-Sinne unverzichtbar.

Fernwartung und Online-Updates

Online-Updates der Autosoftware ohne Werkstattbesuch sind sowohl im Safety- als auch im Security-Sinne unverzichtbar. Aber sie müssen so geregelt werden, dass Fehler nicht vorkommen oder sich nicht auswirken können – etwa dann, wenn eine Datenübertragung unversehens abbricht, ein Fahrzeug nicht erreichbar ist oder sein Eigentümer den Online-Eingriff ablehnt. Wie etwa soll sich ein Hersteller oder eine Werkstatt verhalten, wenn er/sie per Fernüberwachung feststellt, dass ein kritischer Safety-Fehler am Auto vorliegt, der Eigner aber nicht reagiert? Einige Hersteller haben heute bereits die Möglichkeit, das Fahrzeug online in so einem Fall stillzulegen. Die Frage wäre dann, ob das juristisch akzeptabel ist oder in Zukunft vielleicht sogar verpflichtend sein soll.

Die Möglichkeit zu Online-Updates ist auch eine wesentliche Voraussetzung für die erwähnten Methoden zur schnellen und agilen Softwareentwicklung sowie zur Aktualisierung und (kostenpflichtigen) Erweiterung der Fahrzeugfunktionalität. Dabei sind die Anforderungen an Updates hinsichtlich Qualität und Security genauso hoch wie an die mit dem Fahrzeug ausgelieferte Basissoftware. Schnittstellen für Online-Updates sowie die dahinterstehenden Backbones der Fahrzeughersteller im Sinne weltumspannender Cloud-Systeme sind ebenfalls ein relativ neues Betätigungsfeld für OEMs. Die hohen Anforderungen an Security und Datenschutz dieser Systeme können auch mithilfe vertrauenswürdiger Dritter sichergestellt werden.

Safety-relevant oder nicht?

Alle elektronischen Komponenten müssen danach klassifiziert werden, ob und in welchem Ausmaß sie die Fahrzeugsicherheit beeinflussen oder nicht. Prinzipiell sieht die ISO-Norm 26262 Ähnliches bereits vor, nämlich die Zuordnung jeder Komponente zu einem „Automotive Safety Integrity Level" (ASIL). Aber die Kriterien der Klassifizierung und der entsprechende Prozess müssen verbindlich und branchenübergreifend festgelegt werden. Multimedia- und Businessanwendungen sind hier eher unkritisch zu betrachten und können folglich über APIs (Programmierschnittstellen) auch für Dritte geöffnet werden. Systeme mit Einfluss auf das Fahrverhalten müssen aber klar getrennt bleiben.

Das heißt: Jedes Fahrzeug wird zwei Systemplattformen aufweisen. Trotzdem wird eine Datenschnittstelle gebraucht für Anwendungen, die auf beide Bereiche zugreifen. Beispiel: Ein (natürlich nicht Safety-relevanter) Reiseführer nutzt Daten aus dem Navigationssystem, das für die Betriebssicherheit speziell von autonomen Fahrzeugen dagegen extrem wichtig ist.

Von kontrollierten Veränderungen in diesem Bereich hängen neben Safety und Security auch Effizienz und Agilität bei der Softwareentwicklung ab. Die Möglichkeit, Third Parties sicher einzubinden, kann großen Einfluss auf Komfort, Leistung und Features eines Autos haben und wird damit zu einem wichtigen Wettbewerbsfaktor.

Verschärfter Wettbewerb durch niedrigere Markteintrittsbarrieren

Im Wettbewerb treffen die Autohersteller künftig nicht nur auf Ihresgleichen, sondern auch auf IT- und Internet-Konzerne. Die Markteintrittsbarrieren im Automobilsektor sinken, vor allem durch die Elektromobilität: Der extrem komplexe Antriebsstrang vom Motor über Kupplung, Getriebe, Differenzial und Antriebswellen bis zum Rad ist die Domäne der klassischen Autohersteller und Zulieferer, einschließlich elektronischer Komponenten wie ABS und ESP. Wenn jedoch jedes Rad direkt von einem Elektromotor angetrieben wird, übernimmt eine Software den Großteil der Funktionen des Antriebsstrangs.

Der Markt wird sich langfristig in einen Hardware-, einen Software- und einen Dienstleistungsmarkt aufspalten. Wie in der klassischen Datenverarbeitung sowie bei mobilen Endgeräten wird der Hardwaremarkt durch geringe Margen und – zumindest anfänglich – durch Überkapazitäten gekennzeichnet sein. Margen und das echte Geschäft mit den Endkunden liegen dagegen im Bereich Software und Dienstleistungen. Neue Wettbewerber, deren eigentliche Kernkompetenzen weitab von der Konstruktion und dem Bau von Fahrzeugen liegen, erhalten dadurch Marktzutritt. Neben Apple, Microsoft und Google sind das im Dienstleistungsbereich Unternehmen wie Uber und Lyft. Während sich einige OEMs hier bereits aufstellen, sind ihre Rückstände hinsichtlich agiler und rascher Softwareentwicklung sowie der notwendigen Umstellung der Supply Chain noch ganz erheblich. Hier haben Apple, Google und Microsoft einen klaren Kompetenzvorsprung vor den klassischen Fahrzeugherstellern. Dem können OEMs nur noch durch das schnelle und konsequente Abschneiden von alten Zöpfen und umfassende vertikale und horizontale Kooperationen – der Kartendienst HERE ist dazu ein gutes Beispiel – begegnen. Geschieht das nicht, wird der Rückstand zu groß, um noch mit bezahlbarem Aufwand aufgeholt werden zu können.

Der Markt wird sich langfristig in einen Hardware-, einen Software- und einen Dienstleistungsmarkt aufspalten.

4. Sind zusätzliche gesetzliche Regulierungen (z.B. weitere Zulassungsvoraussetzungen/-prüfungen) erforderlich, um den Änderungen im Fahrzeug sowie im Verkehr insgesamt Rechnung zu tragen?

Regulierung verhindert vernünftiges ökonomisches Verhalten und bremst Innovation – dieser Glaubenssatz stimmt nicht immer. Die Gemengelage in der Autoindustrie ist durch dynamisch hinzustoßende Akteure, teils disruptive technologische Veränderungen und die Bedeutung der Branche wegen ihrer schieren Größe extrem herausfordernd. Regulatorische Eingriffe mit Vision und Fingerspitzengefühl können hier dazu führen, dass Kräfte gebündelt, Entwicklungen angestoßen oder gestärkt und damit Innovationen gefördert werden.

Einige Themen sind sogar zwingend zu regulieren, weil sie Entscheidungen auf ethischer statt technischer oder ökonomischer Grundlage erfordern. Einen zentralen Beitrag dazu leistet die Ethikkommission des Bundesverkehrsministeriums, zusammengesetzt aus Rechts-, Gesellschafts-, Ethik-, Technik- und Wirtschaftsexperten. Diese Kommission und andere Arbeitsgruppen in den Ministerien befassen sich mit grundlegenden Fragen im Zusammenhang mit dem autonomen Fahren – einige Beispiele:

- Welche Fahrsituationen dürfen maschinell entschieden werden, welche nicht?
- Sollten Safety und Security in einem verbindlichen Standard gesetzlich geregelt werden – etwa, um zu verhindern, dass das Maß an Fahrsicherheit vom Preis eines Autos und damit vom Einkommen der Käufer abhängt?
- In welchem Umfang müssen Versicherungen unter den Bedingungen des autonomen Fahrens künftig Haftung übernehmen?
- Wem gehören die Daten (Big Data), die beim Betrieb autonomer Fahrzeuge anfallen?
- Was sollte im Vordergrund stehen: Datenschutzanforderungen oder die Speicherung und damit langfristige Verfügbarkeit von Daten, etwa zur Klärung der Schuldfrage bei Unfällen oder für die immer wichtiger werdende Kommunikation zwischen Auto und Infrastruktur?

Diese Fragen sind freilich nicht allein ethischer Natur; ihre Beantwortung wirkt sich massiv auf die Wettbewerbssituation aus. Weil sich die Rollenverteilung in der Autobranche grundlegend ändert – Software und Daten sind auf Dauer wichtiger als die Fertigung der Fahrzeuge –, stehen die Autokonzerne vor einer riesigen Herausforderung: Sie müssen eine Systemsoftware – alle Software, die Fahrzeugeinheiten direkt steuert sowie das Betriebssystem zur übergreifenden Steuerung – entwickeln, die nicht nur vom Markt akzeptiert wird, sondern auch im Wettbewerb mit den neuen Playern aus der IT-Industrie bestehen kann.

Zusätzliche Regulierung wird kommen. Bisherige Regulierungen zum Beispiel der Druckkräfte elektrisch schließender Fenster, um Einklemmverletzungen zu vermeiden, können nicht ignorieren, dass Fahrzeuge künftig in immer mehr Situationen von Software gesteuert werden. Versagt diese, geht es nicht nur um eingeklemmte Finger. Gewisse Anforderungen können nicht dem Preis- und Kostenwettbewerb überlassen werden. Hier muss eine Regulierung Standards setzen und kontrollieren. Damit wird eine Basissicherheit festgelegt, die nicht dem Wettbewerbsdruck am Markt unterliegt – sie ist durch die Hersteller schlichtweg verpflichtend sicherzustellen.

Der größte Hebel, den der Regulator für diesen Fall hat, ist die Typenzulassung. Da der Kfz-Verkehr längst globale Ausmaße angenommen hat, kann kein Land hier einen Alleingang machen – alle Maßnahmen sind auf den Ebenen der EU, der G7 und der UN (Wiener Übereinkommen über den Straßenverkehr) abzustimmen. Es ist im Interesse der Bevölkerung sowie der Fahrzeugindustrie, dass hier hohe Sicher-

heitsstandards angelegt werden. Nicht nur, weil die deutschen OEMs in Sachen Sicherheit und Qualität einen guten Ruf zu verlieren haben, sondern auch wegen des dichten Verkehrs in Deutschland, der ohne Einhaltung hoher Standards für ganz oder teilweise automatisiertes Fahren nur bedingt geeignet wäre. Werden hohe Standards angelegt und sind die Hersteller in der Lage, selbst im dichten und komplexen Verkehrsgewirr Deutschlands zuverlässiges (teil-)automatisiertes Fahren zu demonstrieren, kann das sogar einen Wettbewerbsvorteil auf den globalen Märkten ergeben.

Verbindlicher Systemsoftware-Standard

Gemeinsame Bemühungen aller Autohersteller dürften die Chancen, dass das gelingt, verbessern. Sie werden aber unter nicht regulierten Konkurrenzbedingungen kaum zustandekommen. Zu stark ist der aktuelle Wettbewerb und zu groß die berechtigte Furcht vor kartellrechtlichen Konsequenzen. Die Schaffung eines Safety- und Security-Standards – ob gesetzlich oder im Rahmen existierender Standardisierungsorganisationen wie ISO oder SAE – würde sich mit hoher Sicherheit förderlich auswirken. Ein Betriebssystem, das zentral für einen Großteil der OEMs entwickelt würde, benötigte nur einmal Updates, etwa wenn Security-Risiken neu aufträten. Schnittstellen müssten nur einmal definiert werden, eine zulassungsrelevante Zertifizierung wäre nur einmal erforderlich und letztendlich wäre durch den geringen Wettbewerbs- und Zeitdruck eine höhere Fokussierung auf Qualität und Zuverlässigkeit möglich.

Datenschutz

Auch beim Schutz persönlicher Daten wird es nicht ohne Regulierung gehen. Einerseits besteht das Risiko, dass die strengen europäischen Datenschutzregeln Innovationen bei der im autonomen Verkehr erforderlichen Kommunikation zwischen mehreren Autos sowie zwischen Fahrzeugen und Infrastruktur blockieren. Andererseits gewährleistet nur strikter, nachvollziehbarer Datenschutz das Verbrauchervertrauen, das erforderlich ist, um technologische Umbrüche wie gegenwärtig in der Autoindustrie möglich zu machen. Zumindest in Europa bestehen darum in diesem Feld gute Aussichten, mit sensibler Regulierung die Entwicklung moderner Fahrzeuge und einer zukunftsweisenden Verkehrsinfrastruktur zu fördern.

Ein wesentlicher Beitrag kann auch durch die Konzeption und Entwicklung von Software und Schnittstellen in Fahrzeugen geschaffen werden. Das Zauberwort lautet hier Privacy by Design. Die meisten Aufgaben, die Daten beim autonomen Fahren sowie für zusätzliche Anwenderservices zu erfüllen haben, können ohne die Weitergabe personenbezogener Daten erfüllt werden. Das gilt zumindest dann, wenn dies bereits in der Konzeption entsprechender Funktionalitäten berücksichtigt ist. Für alle anderen Datenverwendungen ist entweder das Einverständnis des Anwenders erforderlich (wie vom Smartphone bekannt) oder eine gesetzliche Regelung, die dem Datenschutz übergeordnet ist (etwa eine Blackbox zur Aufzeichnung der Fahrbewegungen). Die Initiative sollte von den OEMs selbst kommen und könnte über externe Dritte – Trustees für die gesetzeskonforme Verwaltung und Verwendung von Daten – zusätzlich abgesichert werden. Passiert das nicht, wird der Gesetzgeber den Rahmen setzen – möglicherweise enger, als es im Sinn aller Akteure in der Automobilindustrie wäre.

Derzeit gibt es in der Branche viele parallele Entwicklungsstränge, die Fragen bezüglich der künftigen Ordnung in diesem weltweit wichtigen Wirtschaftszweig aufwerfen. Neue Akteure werden den Markt betreten, traditionelle Akteure werden vom Markt verschwinden. Disruptive Technologien sind für diese Entwicklungen wie ein Katalysator. Wichtig in diesem technologischen Entwicklungskampf ist, dass die Kunden stets im Mittelpunkt der Betrachtung stehen, denn auch die fahrenden Rechenzentren der (teil)autonomen Fahrzeuge müssen von jemandem gekauft und eingesetzt werden.

Wesentliche Themen sind und bleiben daher die Zuverlässigkeit, Sicherheit und Qualität der Fahrzeuge sowie das Nutzenversprechen der Hersteller, das in einem ausgewogenen Verhältnis zu den Anschaffungs- und Unterhaltskosten stehen muss. Diese Gleichung kann natürlich – wie auch heute schon – für verschiedenen Kundengruppen auch unterschiedlich aussehen.

Eins ist sicher: Es bleibt spannend!

Safety und Security – wo liegt der Unterschied?

Beide Begriffe stehen für Sicherheit – aber mit unterschiedlichen Bedeutungen im Automobilsektor.

Der Begriff **Safety** – Fahrzeugsicherheit – fasst Bestrebungen zusammen, Fehler in den Kernfunktionen eines Autos zu verhindern und dafür zu sorgen, dass im schlimmsten Fall Schäden für Insassen und andere Beteiligte verhindert werden. Safety-kritisch sind Bremsen, Lenkung, Airbags und die Knautschzonen eines Fahrzeugs, aber auch elektronische Assistenten wie ESP oder ABS.

Security bezeichnet dagegen die Sicherheit von Softwaresystemen vor Fehlfunktionen und Angriffen Dritter. Software in Autos spielt mehrere Rollen: bei der Motorsteuerung, der externen Kommunikation , aber auch der Fahrzeugsicherheit.

Ihre Ansprechpartner

Andreas Herzig
Partner Risk Advisory
Tel: +49 (0)711 16554 7160
aherzig@deloitte.de

Peter Wirnsperger
Partner Risk Advisory
Tel: +49 (0)40 32080 4675
pwirnsperger@deloitte.de

Ingo Dassow
Director Risk Advisory
Tel: +49 (0)30 25468 451
idassow@deloitte.de

Deloitte.

Stand 8/2017