Bild: © depositphotos.com/chesky_w

Gedanken zu einer greifbar nahen Zukunftsvision

Das vernetzte E-Auto als IoT-Gerät

Wie wäre Straßenverkehr ohne Unfälle und Staus, ohne gesundheitsschädliche Abgase, verstopfte Innenstädte und lange Warteschlangen an roten Ampeln? Auf dem Weg zur Arbeit lieber mit dem frischen Kaffee statt mit dem Lenkrad hantieren? Mit dem Einzug des digitalen Wandels auch in den Verkehr und in das Automobil sind dies keine utopischen Wunschvorstellungen mehr. Die Machbarkeit des „Smart Traffic" ist bereits erwiesen – grundlegende Technologien wie das Internet of Things (IoT) und Elektromobilität müssen nun noch zur praktischen Verkehrstauglichkeit mit der erforderlichen Sicherheit weiterentwickelt werden. Hierzulande sorgt die politische Situation auch für den nötigen Anschub für die Automobilindustrie.

Das IoT als Ableger des Internet-Zeitalters bezeichnet abstrakt die Vernetzung von virtuellen und physischen Gegenständen. Das Ziel ist die Verfügbarkeit und Kontrolle von Informationen aus Kontext und Umgebung, in die Dinge jeweils eingebettet sind. Es ist praktisch ein großes und komplexes Netzwerk von eingebetteten IT-Systemen, welches die Dinge unseres Alltags intelligent miteinander verbindet.

Die Vernetzung bringt eine Menge Vorteile mit sich. Zum einen können auf der Basis dieser Informationen Umwege und nicht mehr notwendige Handlungen vermieden werden, zum anderen können Abläufe effizienter, kostengünstiger und umweltschonender geplant und ausgeführt werden. Ein Beispiel ist die Messung von Windstärke und Temperatur auf Windkraftanlagen, auf erhöhten Gebäuden oder Masten, die für Wettervorhersagen interessant sind. Ein weiteres Beispiel wäre das Programm einer Waschmaschine im Privathaus, das abhängig vom aktuellen Strompreis auf den kostengünstigsten Zeitpunkt für das Starten des Waschprogramms wartet. Dies hätte den Vorteil der Energiekosteneinsparung für die Privatperson auf der einen Seite und eine gleichmäßigere Stromnetzbelastung für den Netzbetreiber auf der anderen Seite. In der Industrie ergibt sich die Möglichkeit, dass beispielsweise Zulieferfirmen ihre Auftraggeber über den aktuellen Stand der Fertigung ihres Auftrags automatisiert informieren können, der Auftraggeber hingegen kann den Auftrag überwachen und jederzeit auch anpassen. Ziel ist immer, hier ebenfalls eine bessere und effizientere Planung zu erreichen und damit Ressourcen einzusparen.

Die Schlagworte, unter welchen die genannten Beispiele prominent subsummiert werden, heißen Smart Factory, Industrie 4.0, Smart Home und Smart Grid. Smart Traffic hingegen ist derzeit noch nicht so geläufig. Autonomes Fahren ist für viele noch Jahre entfernt, intelligentes Verkehrsmanagement präsentiert sich in den täglichen Praxiserfahrungen vieler Autofahrer allein etwa bei der Ampelschaltung als Utopie. Doch auch beim Smart Traffic stehen die Zeichen mittlerweile klar auf „Go". Für diesen sehr entscheidenden Schritt sind verschiedene Stellschrauben in der Entwicklung eines Autos entscheidend, die nachfolgend erläutert werden.

Vehicle-to-X-Kommunikation

Die erste Stellschraube ist die Einführung von neuen Kommunikationsmodellen in den aktiven Straßenverkehr. Damit ist die Kommunikation zwischen Fahrzeugen untereinander und zwischen Fahrzeugen und der Verkehrsinfrastruktur gemeint, die sogenannte Car-to-X- oder Vehicle-2-X- (V2X-) Kommu-

nikation. Für die Einführung dieses neuen Kommunikationskonzeptes spricht eine ganze Reihe von Gründen.

Allein im Jahr 2015 gab es in Deutschland über 300.000 Verkehrsunfälle mit Personenschaden. Eine der am häufigsten vorkommenden Unfallursachen ist zu dichtes Auffahren, das in einem Auffahrunfall endet. Bereits Technologien wie Distanzkontrolle oder ein Notbremsassistent wirken dieser Statistik nachweislich entgegen. Im Stadtverkehr ist der häufigste Unfall jedoch die Kollision beim Abbiegen oder beim Kreuzen der Fahrbahn des Gegenverkehrs. Diese Art von Unfällen lässt sich mit den bisherigen Technologien nicht verhindern, denn das Fahrzeug ist mit den heute verbauten Systemen nicht in der Lage, Gefahren außerhalb des Sichtbereiches des Fahrers zu erkennen. Die Lösung, die V2X hier bietet, nennt sich Vehicle to Infrastructur oder V2I. Diese Infrastruktur besteht aus sogenannten Road Site Units (RSU), die entlang der Straßen an Schildern oder Ampeln montiert sind.

Wenn zwei Fahrzeuge aus verschiedenen Richtungen auf eine Kreuzung zufahren ohne einander sehen zu können, sind sie in der Lage, über die RSU miteinander zu kommunizieren und sich so aufeinander vorzubereiten. Weiterhin können RSUs große Entfernungen zwischen Fahrzeugen überbrücken. Dies ist beispielsweise sinnvoll, um Fahrzeuge in Gebieten mit wenig Verkehrsaufkommen vor Gefahrenstellen wie Glatteis, Ölspur oder Straßenschäden rechtzeitig zu warnen. Die kommunikationstechnische Grundlage für die V2X-Kommunikation bietet die Technologie Dedicated Short Range Communication (DSRC). Mit DSRC sind die technischen Voraussetzungen auf physischer Ebene der Kommunikationstechnik geschaffen. DSRC ist im Bereich der Mautgebührenabbuchung auf Autobahnen bereits erprobt. Im Bereich der V2X-Kommunikation wird DSRC aktuell schon in Baustellensituationen praktisch eingesetzt. Neuere Fahrzeuge werden darüber bereits heute in einigen Baustellengebieten über die aktuelle Verkehrssituation mit Informationen versorgt.

Für die Kommunikation zwischen den Fahrzeugen müssen idealerweise alle Verkehrsteilnehmer mit entsprechender Technik ausgestattet werden, was aktuell noch nicht absehbar ist. Eine Möglichkeit wäre, dass ältere Fahrzeuge nachträglich zumindest in dem Grad ausgestattet werden, dass sie den visuellen Kontakt zwischen den V2X-fähigen Fahrzeugen nicht behindern, sondern ähnlich wie RSUs, als Hop dienen.

Anders als bei den mobilen Netzwerken, ist bei V2X eine der größten Herausforderungen das Routing und die gesamte Selbstorganisation der Netzwerkstruktur. Diese muss auch bei Netzwerkteilnehmern, die sich mit sehr hohen Geschwindigkeit bewegen, immer noch funktionieren. Bei einer durchschnittlichen Fahrtgeschwindigkeit von 100 km/h und bei einer Reichweite der Funkmodule von etwa 100 Metern, besteht eine Verbindung gerade mal etwa vier Sekunden. In dieser Zeit müssen Verbindungsaufbau und Informationsübertragung über die Bühne gegangen sein. Bei der Übertragung von sicherheitskritischen Informationen sollen auch Geschwindigkeiten bis zu 250 km/h unterstützt werden. Eine weitere Anforderung ist die Aufrechterhaltung des Netzwerks bei wechselnden Umgebungsbedingungen. Es muss sichergestellt werden, dass eine Verbindung bei überlastetem Verkehr und somit auch bei überlastetem und kollisionsreichem Luft-Medium ebenso stabil ist wie in Situationen mit wenigen Verkehrsteilnehmern. Auch ist die unterschiedliche Signalausbreitung in ländlichen oder urbanen Gebieten zu berücksichtigen. In letzteren kann es aufgrund von Reflexion durch Gebäude einerseits zu einem verstärkten Signal kommen, andererseits aber auch vermehrt zu Kollisionen, die das Signal verfälschen.

Bordnetz

Die Einführung von V2X und die damit verbundenen zusätzlichen Anforderungen an

die Kommunikation innerhalb des Fahrzeuges, drängen die Autohersteller auf die ohnehin schon lang ersehnte Reformation des Bordnetzes. Die Zunahme von Antriebs-, Komfort- und Infotainmentfunktionen haben dazu geführt, dass das Gewicht allein des Kabelbaums schon etwa 40 Kilogramm erreicht hat. Das entspricht einen halben Liter mehr Kraftstoff pro 100 Kilometer. Deshalb ist eine zusätzliche Belastung durch V2X-Komponenten bezüglich des Gewichts nicht mehr vertretbar. Neben dem Gewicht ist die große Zahl der Steckverbinder ein weiteres Problem: Korrosion an den Steckerkontakten bringt ein erhöhtes Fehlerpotenzial. Zusätzliche Kosten entstehen durch die Montage von Einzelkabeln zum Kabelbaum, was zusätzliche Abschlusstests nach der Montage erfordert, was wiederum zur Komplexität beiträgt. Damit verbunden ist das Risiko eines Imageschadens, der durch teure Werkstattsaufenthalte entsteht und den Kunden abschrecken könnte.

Eine ebenfalls große Herausforderung ist das Management beim Entwicklungsprozess aufgrund der Vielzahl an Zulieferfirmen, da der Autohersteller heute im Grunde nur noch als Systemintegrator von Zulieferkomponenten auftritt. Jeder Zulieferer hat seine eigene Mentalität und Philosophie bei Entwicklung und Test der Komponenten. Zwar gibt es Rahmenbedingungen und Standards, trotzdem kommt es bei der Montage häufig zu Inkompatibilitäten zwischen Bauteilen unterschiedlicher Zulieferer. Dadurch entstehen in der Entwicklung immer wieder Verzögerungen. Hinzu kommt, dass unter dem enormen Preisdruck und Konkurrenzkampf zwischen den Autoherstellern die Qualität der Fahrzeuge leidet und die Fehleranfälligkeit weiter ansteigt. Entschädigungskosten für Fehler oder Bandstillstände fallen meistens auf die Zulieferer zurück, was oft ihre Existenz bedroht.

Eine Lösung für all diese Probleme ist eine einheitliche Bordnetzstruktur mit Automotive Ethernet als einziges Netzwerkprotokoll und einer zentralen und leistungsstarken Backbone-Recheneinheit, die alle ECUs (Electronic Control Units, Steuergeräte) ersetzt. Diese Lösung würde das Fahrzeug weiter zu einem IoT-Gerät transformieren und gleichzeitig Komplexität und Gewicht des Bordnetzes deutlich reduzieren. Es gäbe auf der einen Seite neue Herausforderungen an die Softwareentwicklung, die aufgrund der Multicore-Architektur des Zentralrechners komplexer werden wird. Hier könnten die Hersteller aber auf bewährte Technologien aus der Softwarebranche zurückgreifen. Auf der Seite von Automotive Ethernet sind zwar im Bereich der industriellen Automatisierungstechnik schon etablierte Lösungen verfügbar, diese müssten aber noch für den Einsatz im Automobil evaluiert und an die neuen Anforderungen des Energieverbrauchs angepasst werden.

Trotzdem überwiegen die Vorteile. Ziel ist es, abhängig von Klasse und Ausstattung des Fahrzeugs, das Netzwerk beliebig nach Anzahl der Steuergeräte zu skalieren. Somit könnte eine Grundnetzwerkstruktur in alle Fahrzeuge verbaut werden, und entsprechend der Modellreihe nach den speziellen Anforderungen an die Ausstattung erweitert werden. Zudem wären Gateway-Komponenten zwischen den verschiedenen Netzwerken nicht mehr erforderlich, was die Entwicklung vereinfachen und die Fehleranfälligkeit reduzieren würde. Ein weiterer Vorteil von Ethernet ist die große Marktdurchdringung in der IT-Welt. Entwicklungswerkzeuge sind bereits im großen Maß vorhanden und Entwickler müssten nicht neu angelernt werden. Ethernet bietet hohe Datenraten und kann über ein ungeschirmtes, zweiadriges Kabel realisiert werden. Damit würde es die Anforderungen hinsichtlich Gewicht, Systemkosten und Bandbreite bedienen.

E-Antrieb

Im Zuge der Reformation des Bordnetzes und der daraus resultierenden Reduzierung des Gewichts wird zeitgleich auch der Weg in die Elektrifizierung des Automobils geebnet. Sowohl Verbraucher als auch die gesamte deutsche Autoindustrie zögern diesen Schritt so weit wie nur möglich heraus. Doch ähnlich wie beim Übergang von Handys zu Smartphones in der Mobilfunkbranche stellt sich hier die Frage, welche Player die Zukunft des Autos entscheidend mitgestalten werden. Um nicht das gleiche Schicksal wie Nokia in der Handybranche zu erleben, bedarf es zum einen Mut und zum anderen die Bereitschaft, die momentan sehr lukrative Branche der Verbrennungsmotorkomponenten zu transformieren. Denn sollten sich Tesla und Co. durchsetzen, würden dem neuen Trend nicht nur einige mittelständische Unternehmen zum Opfer fallen, die Komponenten für den Verbrennungsmotor herstellen, sondern es wäre der nach Dieselskandal und Kartellvorwürfen bereits angeschlagene Automobilstandort Deutschland gefährdet. Die

Das vernetzte Fahrzeug als IoT-Gerät (Quelle: ifis)

aufstrebende Konkurrenz aus der Elektroautoindustrie kommt den deutschen Weltmarktführern des Automobilbaus gefährlich nahe. Es bleibt abzuwarten, ob Elon Musk mit seinem Tesla Model 3 den deutschen und internationalen Bürger begeistern kann und inwiefern sich der deutsche Automarkt dazu bewegen lässt, endlich deutlichere Schritte zu wagen, um das Auto elektrisch anzutreiben.

IoT

Das V2X-fähige Auto mit Automotive Ethernet als Netzwerkprotokoll integriert die Automobilität weiter in das Internet of Things. Die Vernetzung aller Verkehrsteilnehmer miteinander und mit der Infrastruktur eröffnet eine ganze Reihe weiterer Geschäftsfelder – von den Vorteilen im Verkehr ganz abgesehen. Da sich die RSUs auch als Internet-Zugangspunkt nutzen lassen könnten, wäre es möglich, abhängig von der Ortschaft, durch die das Auto gerade fährt, den Passagieren auf Wunsch Angebote und Möglichkeiten aus den Bereichen Gastronomie, Sport oder Unterhaltung zu unterbreiten oder die Insassen, ähnlich wie in einem Touristenbus, mit Kultur und Geschichte der Ortschaft zu unterhalten. Car-Sharing-Angebote, Paket-Lieferungen in den Kofferraum, oder, um einen kleinen Blick weit in die Zukunft zu wagen, das vollständig autonome Auto, das eigenständig fährt und auf Bedienelemente und Lenkrad vollständig verzichtet. All das kann durch das Fahrzeug als Teil des Internet of Things effizient erreicht werden.

Alle genannten Geschäftsfelder sind auf eine schnelle und kontaktlose Bezahlung angewiesen. Gerade für Fahrer von Elektroautos ist dies eine selbstverständliche Forderung. Denn aufgrund der zu niedrig ausfallenden Reichweite steht der E-Mobilität der große Durchbruch noch bevor. Das induktive Laden der Fahrzeuge an Ampeln während der Rotphase oder an Parkplätzen könnte interessant werden – ein entsprechendes, kontaktloses Mikro-Payment inklusive.

Eine mögliche Antwort für solche Bezahlsystemanforderungen ist die Blockchain-Technologie, die es erlaubt, eine Bezahlung schnell und sicher abzuwickeln. Unternehmen wie ZF, UBS und der Innogy Innovation Hub von RWE haben mit „Car eWallet" bereits ein Bezahlsystem auf Basis der Blockchain-Technologie vorgestellt. Car eWallet kann, analog zur Brieftasche, mit Geld aufgefüllt werden. Während der Fahrt lassen sich automatisiert Bezahlungen zu tätigen. An Mautstellen, auf Parkplätzen oder an E-Tankstellen ist für die Bezahlung kein extra Gang an die Kasse oder den Bezahlautomaten erforderlich. Dabei legt der Inhaber des Kontos, das mit der eWallet verknüpft

ist, fest, in welcher Höhe Zahlungen automatisch getätigt werden dürfen, und ab wann der Nutzer der Zahlung zuzustimmen hat. Auch die Anwendung der Paketlieferung in den Kofferraum oder die Inanspruchnahme eines Car-Sharing-Angebots können mit dem Car eWallet realisiert werden. Alle Transaktionsdaten werden bei jeder Transaktion in einem Block gespeichert, und der Blockchain angehängt. Somit ist jede Transaktion für alle beteiligten Instanzen einsehbar, die somit verifizierbar ist und auf Korrektheit überprüft werden kann.

Anforderungen an die IT-Infrastruktur

Mit der Integration des Autos in dieses komplexe Netzwerk von eingebetteten IT-Systemen werden ganz neue Herausforderungen zunächst an die technische Umsetzung, dann aber auch an die IT-Sicherheit dieser Infrastruktur gestellt. Die Konsequenzen von Fehlern halten sich beim Einschalten einer Waschmaschine zum richtigen Zeitpunkt oder beim Auslesen der Temperatur eines Sensors für Wettervorhersagen in vertretbaren Grenzen, da dies in den meisten Fällen nicht mit Personenschaden oder größeren Sachschäden verbunden ist. Ob die Information der Temperatur oder des Strompreises einige Sekunden früher oder später eintrifft, ist wenig von Belang. Doch wie sieht es mit der Steuerung von Fahrzeugen aus? Man braucht an dieser Stelle gar nicht über das Ausmaß von beispielsweise fehlgeleiteten Güter,- oder Verkehrszügen zu sprechen. Es reicht die Vorstellung von Unfällen innerhalb eines Parkhauses, in welchem sich die Fahrzeuge selbstständig einparken. Selbst kleine Unfälle zur Zeit der Einführung des vernetzten Verkehrs würden das Vertrauen der Bürger in die Technik nachhaltig zerstören.

Wenn heute ein Unfall auf menschliches Versagen zurückzuführen ist, wird dies von der Allgemeinheit normalerweise akzeptiert. Menschen machen Fehler. Doch wenn Menschenleben aufgrund von technischen Fehlern gefordert werden, denkt keiner an menschliches Versagen auf der Seite des Ingenieurs. Die einzige Reaktion ist die Ablehnung der neuen Technologie. Genau das hat der tödliche Unfall eines Teslafahrers im Mai 2016 bestätigt. Heute wird die Auffassung vertreten, dass die Technik des autonomen Fahrens einfach noch nicht ausgereift ist.

Doch ist eine ausgereifte Technologie ein Garant für Fehlerfreiheit? Aus der Sicht der IT-Sicherheit wird diese Frage klar mit einem Nein beantwortet. Denn die Erfahrung aus der jungen Geschichte des Internets zeigt, ein funktionierendes aber vernetztes System gilt als von außen angreifbar und ist damit nie hundertprozentig sicher. Deshalb wird für das Internet of Things, das dann auch aus Personentransportmitteln besteht und somit einen direkten Einfluss auf das Wohlbefinden des Menschen hat, ein neues Sicherheitsniveau gefordert. Es wird eine neue, vertrauenswürdige Infrastruktur in Europa benötigt, die primär für die Vernetzung von Autos und andere Verkehrsmittel konzipiert worden ist. Doch wer stellt diese vertrauenswürdige Infrastruktur zur Verfügung? Wer verantwortet die IT-Sicherheit? Wer kommt für Schäden auf, die beispielsweise von Hackerangriffen ausgehen? Ist es überhaupt möglich, ein ausreichend sicheres Netzwerk zu erschaffen, um die vielen Vorteile der Vernetzung in Anspruch zu nehmen?

Da beispielsweise die Einführung der V2X-Technologie auch ein politisches Thema ist, könnte die höchste verantwortende Instanz ein neues Bundesamt für „IT-Sicherheit im Verkehr" sein. Denn wenn die V2X-Technologie mit autonomen Fahrzeugen auf den Straßen erst einmal Gestalt annimmt, wird spätestens mit dem ersten Unfall die Frage der Verantwortung beantwortet werden müssen. ■

PROF. DR. NORBERT POHLMANN
ist Professor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco.

MARKUS REIMER
studiert im Master Internet-Sicherheit am Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen und beschäftigt sich im Rahmen des Studiums mit der IT-Sicherheit von vernetzten Autos.