Ein Aufruf – Praktische Standards für autonomes Fahren

Die Autoindustrie bewegt sich auf Level 3 und Level 4 der Fahrzeugautomatisierung zu. Jüngste Erfahrungen mit der Systemsicherheit des Levels 2 haben allerdings bereits gezeigt, dass selbst etablierte Systeme unter Annahmen arbeiten, die im Störungsfall zu extrem gefährlichen Situationen führen können. Die ISO 26262 und Erweiterungen wie „Safety of the Intended Functionality“ bieten höchste Anforderungen an die Sicherheit der automatisierten Systeme, aber keine Anleitung, wie diese Anforderungen erreicht werden können. Elektrobit ist der Meinung, dass es notwendig ist, branchenweit Diskussionen bezüglich der Best Practices für algorithmische und architektonische Konfigurationen einzuleiten, die den Stand der Technik für sichere selbstfahrende Systeme definieren.

© Elektrobit

AUTOR

Dr. Ing. Björn Giesler
ist Leiter Fahrerassistenz bei der Elektrobit Automotive GmbH in Erlangen.

AUSGANGSSITUATION

Hochautomatisierte Fahrfunktionen des Levels 3 und 4 erfordern einen menschlichen Fahrer im Fahrzeug, sowohl aus technischer als auch aus rechtlicher Sicht, aber sie erlauben es dem Fahrer, seine Aufmerksamkeit von der Fahraufgabe wegzulenken. Das bedeutet, dass sie zumindest in der Lage sein müssen, sicher festzustellen, ob die augenblickliche Situation automatisch gehandhabt werden kann oder vom Fahrer übernommen werden muss. In Level 4 müssen sie darauf vorbereitet sein, dass der Fahrer nicht übernehmen kann, also müssen sie auf alle Situationen sicher reagieren können. In Level 5 kann die Anwesenheit eines Fahrers nicht mehr angenommen werden. Aber auch bereits in den unteren Levels kann das automatisierte Fahrzeug als fahrerlos gelten, solange es unter der Kontrolle der Automatisierung ist.

Funktionale Sicherheit, wie sie von der ISO 26262 gefordert wird, beruht auf der grundsätzlichen Annahme, dass alle Gefahren in den folgenden Kategorien beschrieben werden können: Exposition (Wie wahrscheinlich wird eine Gefahr eintreten?), Schwere der Auswirkungen (Wie gefährlich ist die Gefahr für das Leben und die Gesundheit, falls sie eintritt?) und Beherrschbarkeit der Fehlfunktion in der jeweiligen Fahrsituation (In welchem Maß kann vom Menschen erwartet werden, dass er auf die Gefahr reagiert und sie abwendet?). Die letzte Kategorie ist für automatisierte Systeme problematisch. Da der Fahrer, selbst wenn er körperlich anwesend ist, der Situation keine Aufmerksamkeit geschenkt hat, kann nicht davon ausgegangen werden, dass er die Situation im Griff hat. Daher ist die Frage berechtigt, ob die ISO 26262 auf fahrerlose Systeme anwendbar ist. Zumin-

dest sollten alle Gefahren unter der Kontrolle der Automatisierung als C3 behandelt werden, also praktisch unkontrollierbar. Diese Einschätzung führt zu hohen funktionalen Sicherheitsanforderungen für die automatisierte Fahrhardware und -software; ASIL-D (Automotive Safety Integrity Level) für den Hauptsicherheitspfad ist üblich. Vereinfacht ausgedrückt bedeutet dies, dass keine Komponente auf dem sicherheitsrelevanten Ausführungspfad des Systems eine höhere Fehlererwartung als 10 bis 8 pro Stunde haben darf beziehungsweise statistisch nicht häufiger versagen darf als einmal in 11.704 Jahren. Das bedeutet, dass eine Person, die 50 Jahre lang täglich 2,5 Stunden Auto fährt, mit einer Wahrscheinlichkeit von rund 0,1 % einer solchen Gefahr begegnet, was sicherlich ein ehrenwertes, aber auch sehr hohes Ziel ist. ISO 26262 gibt einige Empfehlungen, wie dieses Ziel auf elektrischer, elektronischer und Software-Qualitätsebene erreicht werden kann. Hoch automatisierte Fahrzeuge basieren ihre Entscheidungen allerdings auf Sensoren und Algorithmen. Die Erfahrung zeigt, dass die meisten Gefahren häufig nicht durch elektrische oder elektronische Probleme verursacht werden und noch nicht einmal durch Softwarefehler (obgleich diese immer noch wesentlich häufiger auftreten als Hardwarefehler). Manche Algorithmen ziehen die falschen Schlüsse daraus, was den Sensordaten zu entnehmen ist. Wenn die Automatisierung einen Fehler macht, der nicht auf einen elektrischen/elektronischen oder Softwarefehler zurückzuführen ist, aber die Algorithmen schwerwiegende Fehler machen, dann ist dies für Level-3+-Systeme nicht hinnehmbar.

Neuere Entwicklungen konzentrieren sich daher nicht nur auf die funktionale Sicherheit, sondern auf die „Safety of the Intended Functionality“ (SOTIF). Dies kann als eine Erweiterung von ISO 26262 betrachtet werden, die algorithmische und wahrgenommene Gefahren mit berücksichtigt. Elektrobit (EB) glaubt, dass dies zwar der richtige Ansatz zur umfassenden Beurteilung eines automatisierten Systems ist, aber auch SOTIF beschreibt nicht, wie die notwendige Sicherheit tatsächlich zu erreichen ist. Dies ermöglicht eine maximale Freiheit in der Umsetzung, spricht aber nicht den aktuellen Stand der Technik in der eigentlichen Systemumsetzung an. Elektrobit ist der Meinung, dass nicht nur die Ziele für sicheres automatisiertes Fahren erörtert werden sollten, sondern auch, wie sich diese praktisch erreichen lassen.

ALGORITHMISCHE REDUNDANZ

Es gibt viele Wege, ein System sicher zu machen, zumindest theoretisch. Ein verbreiteter Ansatz auf Makrosystemebene ist es, eine „Hauptfunktion“ und eine „Supervisor-Funktion“ zu entwickeln. Beide Funktionen werden mit gegenseitig redundanten Umweltmodellen versorgt und beide bestätigen sich gegenseitig, dass die augenblickliche Situation korrekt eingeschätzt wird, **BILD 1**.

Diese Methode ermöglicht es, die funktionalen Sicherheitsanforderungen auf zwei ECUs (beziehungsweise an zwei CPUs und eine ECU) und zwei Software-Entwicklungsteams zu verteilen.

DIE MODELLIERUNG DER WELT

Es gibt großes Potenzial für diese Art von Redundanz auf einer wesentlich tieferen und detaillierteren Ebene. Betrachten wir beispielsweise die „Time to Collision“-(TTC)-Zeit bis zur Kollision, die ein automatisiertes Fahrsystem berechnen muss. Die wichtigste Angabe einer sicherheitsrelevanten Fahrzeugkontrollfunktion wird immer Folgende sein: „In x Sekunden wird eine Kollision stattfinden.“ In vielen aktuellen Konfigurationen wird die TTC durch ein Umfeldmodell berechnet, das als Objektfusion bekannt ist.

Der Gedanke hinter der Objektfusion ist der, dass die meisten potenziellen Kollisionspartner im Umfeld des Autos entweder statisch oder dynamisch sind und ihre Bewegung (falls es eine gibt) durch eine bestimmte mathematische Funktion modelliert werden kann. Beispielsweise hat ein anderes Fahrzeug normalerweise eine gelenkte Achse und eine Antriebsachse und bewegt sich entsprechend der Achse ersterer und der Geschwindigkeit letzterer. Damit kann es zum Beispiel nicht plötzlich zur Seite springen oder sofort stoppen, sondern es wird erwartet, dass es sich entsprechend einem spezifischen Bewegungsmodell bewegt. Diese Eigenschaft kann genutzt werden, um die Bewegung des Objekts vorauszusagen und um Messfehler herauszufiltern. Daher ist der typische Zyklus einer Objektfusionskomponente folgendermaßen, **BILD 2**:

- Prädiktion der Position eines Objekts
- Verknüpfung des prädizierten Objekts mit einer neuen Messung des Sensors
- Aktualisierung des Bewegungsmodells des Objekts in Übereinstimmung mit den neuen Sensorinformationen.

Diese Art des Modells wird typischerweise mit einem Kalman-Filter [1] beziehungs-

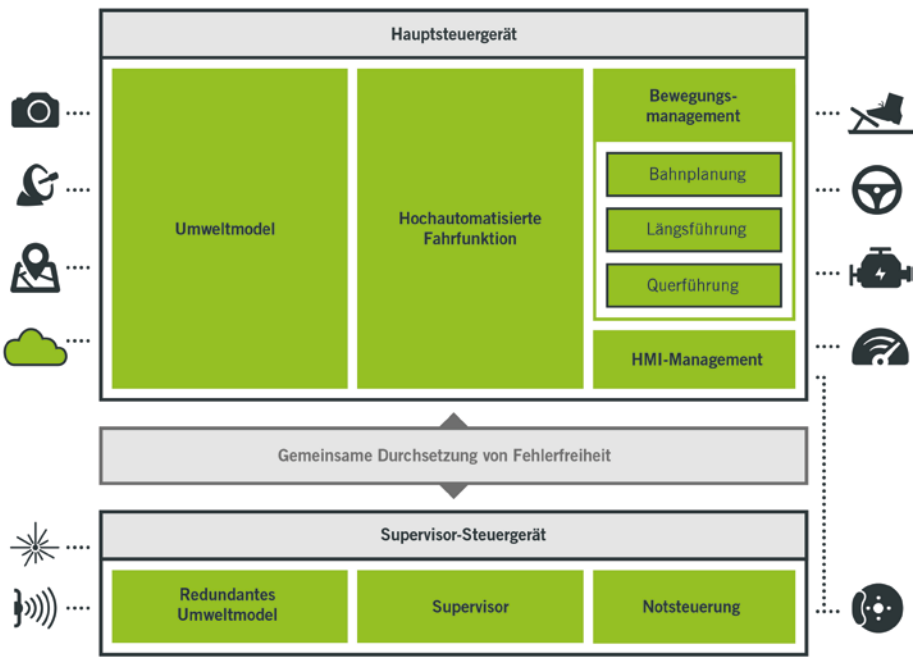

BILD 1 Die Aufteilung in Hauptfunktion und Supervisor-Funktion verteilt die funktionalen Sicherheitsanforderungen auf zwei Steuergeräte (© Elektrobit)

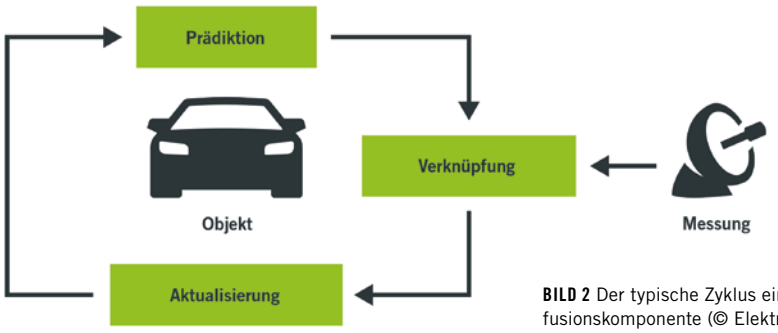

BILD 2 Der typische Zyklus einer Objektfusionskomponente (© Elektrobit)

weise einer Variante davon ausgeführt, einer Methode aus dem Jahr 1960, die in der Robotikforschung seit den 1980er Jahren für Objektbewegungsmodelle angewandt wird. Sie kann als bewährte und dem Stand der Technik entsprechende Methode angesehen werden, und sie wird in nahezu allen Umweltsensoren im Automobilbereich eingesetzt. Wenn die Annahmen bezüglich des gewählten Bewegungsmodells richtig sind und alle Fehlerquellen im System korrekt abgebildet werden, ist das Ergebnis nachweislich die bestmögliche Art der Objektbeschreibung. Wenn der Algorithmus korrekt umgesetzt wird, kann das System daher die größtmögliche Sicherheit erreichen. Oder?

Nicht unbedingt. Die Objektmodellierung gründet auf einer Reihe von Annahmen. Das Bewegungsmodell muss das richtige sein. Zum Beispiel dürfen wir das Auto, das wir darstellen, nicht mit einem anderen Objekt verwechseln; falls es sich um einen Fußgänger handelt, könnte die Person plötzlich zur Seite springen. Da wir dies nicht abgebildet haben, würde es unseren Algorithmus vollkommen überraschen; es würde als Fehler betrachtet und unserer Funktion nicht mitgeteilt werden. Die Zuordnung muss ebenfalls richtig sein. Falls wir fälschlicherweise die Erfassung einer Straßenlaterne unserem abgebildeten Auto zuordnen, würde dies eine vom Kurs abkommende Bewegung einleiten, die das Auto nicht wirklich aufweist. Alle Fehler im System müssen korrekt abgebildet werden. Und so weiter.

Dies heißt nicht, dass Objektmodellierung das falsche Instrument in dieser Situation ist. Da es aber auf Annahmen basiert, die nicht immer zutreffen, kann es dennoch gelegentlich falsche Ergebnisse liefern. Keine dieser Annahmen ist durch funktionale Sicherheitsstandards abgedeckt. Die logische Schlussfolgerung für dieses Problem ist, dies mit einem redundanten Algorithmus abzusichern, der ebenfalls auf dem neuesten Stand der Technik ist und der die gleichen Informationen auf eine andere Art liefert.

Eine weitere Möglichkeit, die Umgebung des Autos abzubilden, ist die, dass man sich die Umgebung des Fahrzeugs als Netz einzelner Zellen einer bestimmten Größe vorstellt, von denen jede entweder besetzt, frei oder unbekannt ist, da sie noch nicht durch die Fahrzeugsensoren erfasst wurde, **BILD 3**. Wenn ein Sensor ein Hindernis in einer bestimmten Entfernung und einem bestimmten Winkel zum Fahrzeug erkennt, wird die Gitterzelle des entsprechenden Standorts als besetzt gekennzeichnet, und für bestimmte Sensortypen werden die Gitterzellen zwischen dem Sensor und dem wahrgenommenen Hindernis als frei markiert.

Diese Art der Umweltmodellierung wurde 1985 eingeführt [2]. Auch sie hat sich in vielen Umgebungssensoren in Fahrzeugen bewährt, wenn sie auch vielleicht nicht so häufig verwendet wird wie das Kalman-Filter. Sie kann ebenfalls Informationen zur TTC zur Verfügung stellen, da sie auch Hindernisse auf der Fahrspur des Fahrzeugs abbildet. Ebenso beruht sie aber auf Annahmen, zum Beispiel, dass ein Bereich frei ist, wenn die Sensorstrahlen hindurchdringen können (was, in Abhängigkeit des Sensors und des Objekttyps, nicht der Fall sein muss), und der Dynamik der Umgebung, das heißt wie viele Messungen an einer einzelnen Zelle vorgenommen werden müssen, bevor diese als frei oder besetzt erkannt wird. Diese Annahmen unterscheiden sich jedoch grundsätzlich von denen, die in der Objektmodellierung verwendet werden, **BILD 4**.

ALGORITHMISCHE REDUNDANZ ERZEUGT SICHERERE SYSTEME

Als ein Beispiel haben wir soeben zwei weitverbreitete Mechanismen zur Abbildung der Umwelt untersucht. Beide sind erfolgreich praxiserprobt und können zu beliebig hoher funktionaler Sicherheit entwickelt werden (allerdings zu beliebig hohen Entwicklungskosten). Keine von beiden wird in allen Fällen korrekte Ergebnisse liefern. Wenn die funktionale Sicherheit und SOTIF eine Fehlerrate von weniger als einmal pro 108 Betriebsstunden verlangen, ist es sicher anzunehmen, dass während dieser Betriebszeit einer dieser beiden Algorithmen Fehler hervorruft, für deren Verhinderung weder die funktionale Sicherheit noch

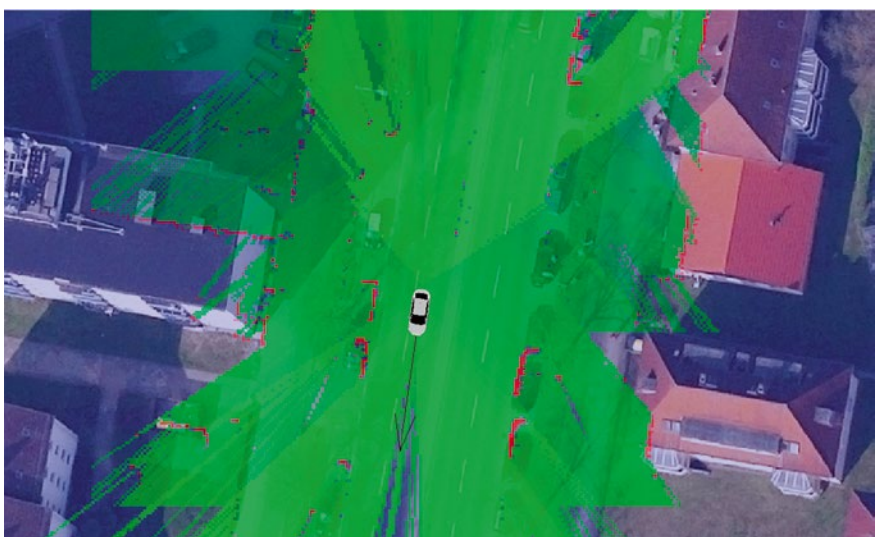

BILD 3 Ein Netz aus freien, besetzten oder unbekannten Zellen bildet die Umgebung des Fahrzeugs ab (© Elektrobit)

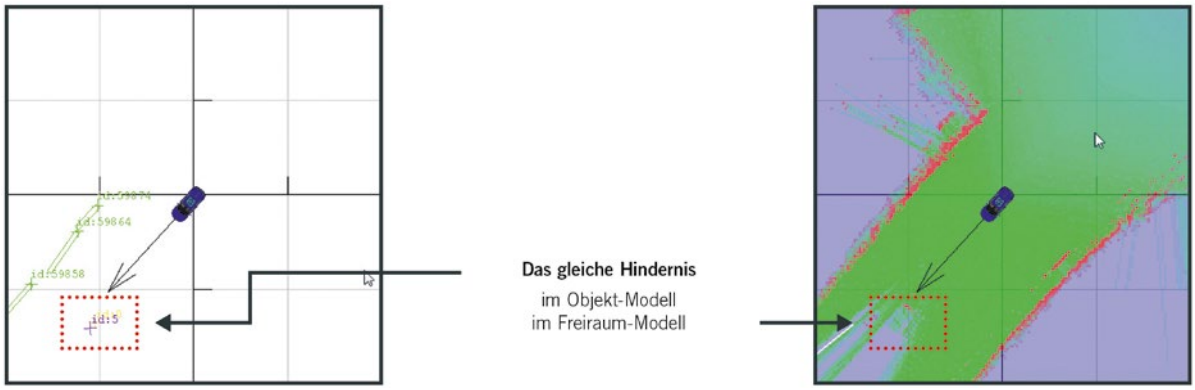

BILD 4 Unterschiede in der Objekterkennung im Objektmodell und Freiraummodell (© Elektrobit)

SOTIF eine Orientierungshilfe bieten. Das ganze System hat viele solcher Beispiele. Dies ist ein großes Problem für ein automatisiertes System, das Personenschaden verursachen kann, wenn es Situationen falsch einschätzt.

Ein Weg, diese Fehleinschätzungen zu vermeiden, ist der gleichzeitige Einsatz mehrerer Methoden zur Modellierung der Umgebung darin, und eine Aktion nur dann zuzulassen, wenn alle diese Methoden die Aktion übereinstimmend als sicher beurteilen. Im obigen Beispiel fährt unser Fahrzeug vielleicht nur weiter, wenn beide, das „Objekt"-Modell und das „Freiraum"-Modell der Umgebung übereinstimmen, dass sich kein Hindernis auf der Fahrspur befindet. Da die diesen beiden Methoden zugrundeliegenden Annahmen sich fundamental unterscheiden, besteht die Hoffnung, dass nicht beide gleichzeitig falsch sind.

DIE NOTWENDIGKEIT ZUR BEGUTACHTUNG IM PEER-REVIEW

Aber von einem autonomen Fahrzeug sollte man nicht hoffen, sondern wissen, dass es sicher ist. SOTIF legt keine Dekompositionsregeln für algorithmische Annahmen fest, aber doch, dass diese für ein ASIL-D-System nicht häufiger als einmal alle 108 Stunden falsch sein dürfen. Dies trifft auch für andere Systeme (zum Beispiel Bremsmechanismen) zu, aber in unserem Fall ist das Problem weit weniger gut verstanden und kann nicht im Labor getestet werden. Daher kann die notwendige Sicherheit derzeit nur durch Feldversuche erreicht werden, die eine Anzahl statistischer Test benötigen würden, von denen einer allein 108 Stunden dauern müsste. Es ist nicht finanzierbar, auch nur ein Fallbeispiel durch Testfahrten mit einem Auto zu untersuchen, ganz zu schweigen von der Anzahl an Beispielen, die für eine statistische Sicherheit notwendig wären. Testfahrten sind somit, im wissenschaftlichen Sinne, ein Stochern im Nebel. Für assistiertes Fahren hat dies gut funktioniert, aber angesichts der Höhe der ISO-Anforderungen an die Systemsicherheit kann augenblicklich nicht garantiert werden, dass die entsprechende Testtiefe erreicht wird. Dies bedeutet, dass es momentan keine technische Möglichkeit gibt, die Sicherheit einer algorithmischen Lösung für automatisierte Fahrzeuge zu garantieren.

Es gibt Wege, dies zu umgehen. In der Wissenschaft ist ein Ansatz hierfür das

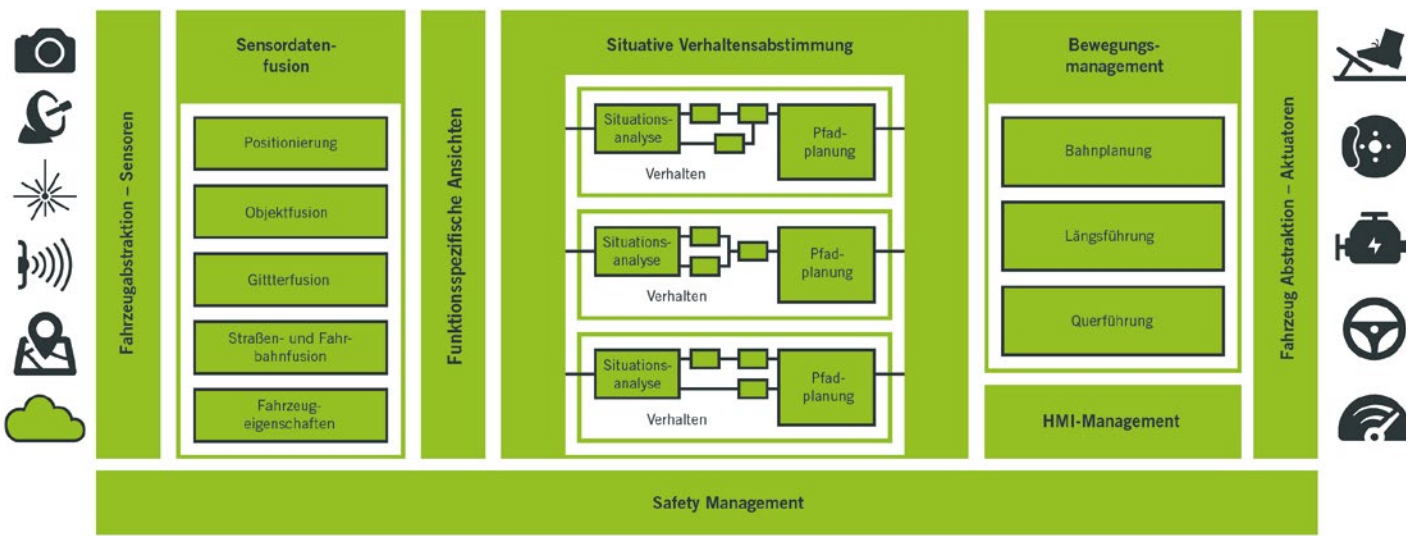

BILD 5 Die Softwarelösung EB robinos basiert auf „open robinos", EBs mit offenen Schnittstellen versehener Architektur für hochautomatisierte Fahrsysteme (© Elektrobit)

Peer-Review: Eine bestimmte Methode, von der angenommen wird, dass sie ein Problem lösen kann, wird detailliert veröffentlicht und beschrieben. Sie wird von anderen untersucht, und Fehler werden durch theoretische Untersuchungen und praktische Prüfungen entlarvt. Verbesserungen werden gefunden, erneut veröffentlicht und wieder getestet. Das ist der typische Zyklus für einzelne Lösungen, gegen deren Ende hin es häufig viele leicht unterschiedliche Varianten gibt, die dann verglichen werden. Am Schluss ergibt sich ein Goldstandard, der eine Zeit bestehen bleibt, bis neue Ideen oder der Fortschritt in anderen Gebieten neue Impulse auf den Tisch bringen und der Zyklus von vorne beginnt. Beide oben beschriebenen Algorithmen haben diesen Zyklus durchlaufen und gelten als Goldstandard-Lösung für ihr spezifisches Problem. Der Peer-Review garantiert keine 100 % sichere Lösung, aber er attestiert, dass zu einem bestimmten Zeitpunkt niemand eine bessere Lösung zur Verfügung hat.

Im Wettbewerb, der Erste auf dem Markt zu sein, geht die Entwicklung des hochautomatisierten Fahrens scheinbar einen anderen Weg. Bestimmte Goldstandard-Lösungen für spezifische Probleme werden verwendet, aber deren Verbindung in Gesamtsystemen wird als intellektuelles Firmeneigentum behandelt und geheim gehalten. Neuerdings scheint die öffentliche Vermarktung der neuesten Fortschritte in der neuronalen Netzwerkforschung nahezulegen, dass selbst die Verwendung von Goldstandard-Algorithmen nicht mehr à la mode ist und dass stattdessen die künstliche Intelligenz das Problem durch bislang unveröffentlichte Magie lösen wird.

Dies ist eine sehr kurzsichtige Lösung. Mit Sicherheit wird irgendwann ein Mensch in einem Unfall mit einem hochautomatisierten System verletzt werden, ob dies nun der Fehler des Systems ist oder nicht. In diesem Fall wird eine Gerichtsverhandlung dann herausfinden wollen, ob das System auf dem neuesten Stand der Technik entwickelt wurde. Falls zu dieser Zeit noch kein Stand der Technik etabliert ist, kann davon ausgegangen werden, dass viele unangenehme Diskussionen folgen werden. Je nach Urteil des Gerichts und möglicherweise folgender Gesetzgebungsverfahren, kann dies nicht nur die betroffenen Firmen schädigen, sondern die gesamte Branche des automatisierten Fahrens, die bis 2025 auf 42 Milliarden US-Dollar geschätzt wird.

DIE NOTWENDIGKEIT VON STANDARDS

Daher schlägt EB vor, in der Branche eine Diskussion über Best Practices für die Konstruktion von hochautomatisierten Fahrsystemen auf einer hochtechnischen Ebene zu beginnen. Es ist nicht notwendig, dass Hersteller ihre eigenen Lösungen detailliert offenlegen (obwohl das schlussendlich wünschenswert wäre), sondern, dass es eine veröffentlichte Lösung gibt, die begutachtet und mit der Zeit verbessert werden kann. Dies birgt keinerlei Gefahr für das geistige Eigentum der Hersteller.

Im Juni 2016 veröffentlichte EB eine Beschreibung ihrer eigenen Lösung unter dem Namen „open robinos“ [4], die für den Betrieb auf Standard-PCs und einigen ECUs der Autoindustrie implementiert wurde, **BILD 5**. Die Spezifikation (das heißt die Systembeschreibung, die im Peer Review begutachtet werden soll) ist unter einer Creative-Commons-Lizenz erhältlich und die Anwendung ist frei verfügbar. Augenblicklich baut EB eine Arbeitsgemeinschaft im Zusammenhang mit dieser Spezifikation auf, die das Review-Verfahren einleiten und Verbesserungen der Spezifikation veröffentlichen soll: mit dem Ziel, eine Referenzimplementierung zu erstellen, mit der andere Systeme verglichen und geprüft werden können, um letztendlich einen offenen Standard für die Konstruktion selbstfahrender Systeme aufzubauen.

Ein Standard hat noch weitere Effekte als das Begutachten von sicherheitskritischen Algorithmen im Peer-Review. Er öffnet die Tür für Software-, Hardware- und Fahrzeughersteller, Teile des Standards zu nutzen und andere mit ihren eigenen Lösungen zu ersetzen. Er eröffnet einen Weg, eigene IP- beziehungsweise markengebende Funktionen zu entwickeln, ohne ein komplettes System entwickeln zu müssen. Er schafft einen Markt für Systemmodule, so dass Wettbewerb auf Modulbasis und nicht auf Systembasis stattfindet. Dies schafft bessere technologische Lösungen und verteilt Entwicklungs- und Testkosten über eine Branche, anstatt lediglich über ein einzelnes Automodell. Ein Standard kann mit dem Gesetzgeber erörtert werden, um Testverfahren für Behörden wie die NHTSA oder den TÜV zu erstellen, und dazu verwendet werden, dem Kunden zu garantieren, dass ein Produkt diesem Standard entspricht und es daher als sicher in der Anwendung betrachtet werden kann.

FAZIT

In diesem Artikel wurde keine neue technische Lösung veröffentlicht. Im Gegenteil, die Autoren haben eine sehr alte Lösung für das Problem vorgestellt, um die richtigen technologischen Weiterentwicklungen zu finden. Im Wettrennen um selbstfahrende Autos wird diese Lösung außerhalb der Hochschulforschung allerdings derzeit nicht genutzt. EB glaubt, dass das Problem hochautomatisierten Fahrens nicht ausreichend verstanden wird, um von einer einzelnen Firma oder einem Konglomerat allein gelöst zu werden. Aber selbst wenn dies so wäre, würde es das Problem, sichere selbstfahrende Autos zu entwickeln, nicht in seiner Gesamtheit lösen. Denn wenigstens die Prinzipien des automatisierten Fahrens müssen von der Branche überprüft, getestet, genehmigt und letztendlich standardisiert werden.

Dieser Vorschlag wird nicht das Geschäft der Unternehmen oder die Entwicklungsgeschwindigkeit selbstfahrender Autos mindern. Im Gegenteil, EB ist davon überzeugt, dass hiermit Geld- und Personalressourcen besser genutzt werden können, der Entwicklungsprozess beschleunigt wird und sicherere Systeme geschaffen werden können. Wenn Sie am Begutachtungs- und Spezifikationsprozess teilhaben möchten und Algorithmen und die Architektur für selbstfahrende Autos diskutieren möchten, registrieren Sie sich bitte: www.open-robinos.com.

LITERATURHINWEISE

[1] Welsh, G.; Bishop, G.: A Gentle Introduction to the Kalman Filter. In: Proc. SIGGRAPH, August 2001

[2] Moravec, H.; Elfes, A.E. : High Resolution Maps from Wide Angle Sonar. In: Proc. ICRA, March 1985

[3] Green, J.: Driverless-Car Global Market Seen Reaching $42 Billion by 2025. Online: https://www.bloombergcom/news/articles/2015-01-08 driverless-car-global-market-seen-reaching-42-billion-by-2025

[4] Elektrobit GmbH. Open robinos specification. Online: https://www.elektrobit.com/products/eb-robinos/eb-robinos-specification/