Absicherungsprozesse für automatisierte Fahrzeuge

Johannes Mitterbauer
Professionelle Textsatzsysteme
Technische Hochschule Ingolstadt
Ingolstadt, Deutschland

***Zusammenfassung*—Automatisierte Fahrzeuge werden immer verbreiteter und vielseitiger. Zunächst werden automatisierte Fahrzeuge nach ihrem Automatisierungsgrad und weiteren Eigenschaften eingeteilt. Für deren problemlosen Einsatz werden zudem bestimmte Absicherungsprozesse für Hardware und Software benötigt. In diesem Text werden die beiden Arten der Sicherheit beim automatisierten Fahren, funktionale Sicherheit und Sicherheit in Gefahrensituationen, besprochen. Danach wird darauf eingegangen, wie Redundanz und Codequalität zur Sicherung der funktionalen Sicherheit eingesetzt werden können und wie es möglich ist, ein automatisiertes Fahrzeug aus einer Gefahrensituation wieder in eine sichere Situation zu bekommen. Zusätzlich wird die Bedeutung von Sicherheit automatisierter Fahrzeuge im Rahmen der rechtlichen Situation in Deutschland und der Einstellung von Verbrauchern behandelt. Letztendlich ist ausreichende Sicherheit die letzte Hürde, die autonome Fahrzeuge überwinden müssen.**

***Index Terms*—automated vehicles, autonomous vehicles, safety**

I. Einleitung

Automatisierte Fahrfunktionen sind heutzutage in mehr Fahrzeugen, als je zuvor. Diese haben auch mehr Einsatzmöglichkeiten als je zuvor. Der Traum der selbstfahrenden Fahrzeuge scheint immer näher zu rücken. Tatsächlich gab es vor nicht einmal zwei Jahrzehnten das erste kommerziell erhältliche Fahrzeug mit Einparkassistent und heute schon Fahrzeuge mit Autopilot-Funktion. Durch neue Technologien wie Deep Learning und den generellen technischen Fortschritt sind wir dem autonomen Fahren näher denn je. Ein Thema, dass aber rechtliche Instanzen und öffentliche Wahrnehmung vom autonomen Fahren abschreckt, ist Sicherheit. Da mit Abstand die meisten Unfälle aufgrund von menschlichem Versagen verursacht werden, haben selbstfahrende Fahrzeuge das Potential, deutlich sicherer zu sein, als herkömmliche Fahrzeuge. Zu aktuellen Unfallraten selbstfahrender Fahrzeuge gibt es leider noch keine verlässlichen Daten, nur Behauptungen der Hersteller selbst. Es ist gut möglich das selbstfahrende Fahrzeuge bereits sicherer sind als herkömmliche. Die öffentliche Wahrnehmung ist dem gegenüber aber noch kritisch. Berichte von Unfällen von Fahrzeugen mit Selbstfahrfunktionen werden weit verbreitet und schockieren Leser. Gesetzgeber sehen den Einsatz von als unsicher wahrgenommenen Technologien ebenfalls kritisch. Eine teilweise sogar bergündete Skepsis gegenüber dem Neuen könnte so eine Annahme autonomer Fahrzeuge verhindern. So gilt es, automatisierte Fahrzeuge so sicher wie möglich zu machen. Im Folgenden Text wird behandelt, was Sicherheit bei automatisierten Fahrzeugen bedeutet und wie diese verbessert werden kann.

II. Arten des automatisierten Fahrens

Automatisierte Kraftfahrzeuge bestehen aus zwei Teilen, dem Fahrzeug selbst und dem Fahrsystem, welches das Fahrzeug steuern kann. Der Überbegriff der automatisierten Fahrsysteme schließt alle Systeme mit ein, die selbstständig Fahraufgaben übernehmen können. Die automatisierten Fahrsysteme lassen sich je nach Automatisierungsgrad, Aufgabenbereich und erforderlicher Benutzereingabe unterteilen. [1][2, S. 9]

A. Assistierte Fahrsysteme

Meist einfach als Assistenzsysteme bezeichnet, sind Fahrsysteme, bei denen der Fahrer ausschließlich unterstützt wird. Sie übernehmen entweder die Querführung, also das Lenken, oder die Längsführung, das Beschleunigen und Abbremsen. Der Fahrer muss das Fahrsystem während dieses eingesetzt wird durchgehend überwachen. Die bekanntesten assistierten Fahrsysteme sind Einparkassistenten, bei denen das Fahrsystem das Lenken in eine Parklücke übernimmt, während der Fahrer Gas gibt bzw. bremst. Spurhalteassistenten zählen ebenfalls zu den Assistenzsystemen, da diese den Fahrer bloß unterstützen und auch nur die Quer- und nicht die Längsführung übernehmen.

B. Teilautomatisierte Fahrsysteme

Manchmal auch nur automatisierte Fahrsysteme genannt oder weiter in teilautomatisierte und hochautomatisierte Fahrsysteme unterteilt, sind Fahrsysteme, die sowohl Quer- als auch Längsführung übernehmen können, aber nur für einen bestimmten Zeitraum oder eine bestimmte Situation. Auch wie bei Assistenzsystemen muss der Fahrer während dem Einsatz des Fahrsystems dieses durchgehend überwachen. Die bekanntesten teilautomatisierten Fahrsysteme sind Autobahnassistenten. Diese sind oft eine Kombination und Weiterentwicklung verschiedener Assistenzsysteme, wie etwa Spurhalteassistenten und Abstandsregeltempomaten. So kann ein Autobahnassistent sowohl die Quer- als auch die Längsführung übernehmen. Mittlerweile gibt es auch Parkassistenten, die auch die Längsführung übernehmen und so auch als teilautomatisiert kategorisiert werden können.

C. Autonome Fahrsysteme

Sind Fahrsysteme, die vollkommen selbstständiges Fahren ermöglichen. Es wird lediglich die Eingabe eines Ziels, einer Route oder ähnlicher Parameter benötigt. Eine dauerhafte Überwachung durch den Fahrer ist nicht mehr nötig, vor allem da bei Fahrzeugen mit autonomen Fahrsystemen oft Steuerelemente für menschliche Fahrer, wie zum Beispiel Lenkrad und Pedale, fehlen.

D. Vollautomatisierte Fahrsysteme

Eine Sonderform, die vom Automatisierungsgrad zwischen teilautomatisierten und autonomen Fahrsystemen liegt, sind vollautomatisierte Fahrsysteme. Diese sind den autonomen Fahrsystemen sehr ähnlich und werden oft fälschlicherweise als solche bezeichnet. Vollautomatisierte Fahrsysteme unterscheiden sich von autonomen Fahrsystemen dadurch, dass diese durchgehend von einem Fahrer überwacht werden müssen. Somit sind sie nicht autonom. Aufgrund diverser Gründe, welche im Folgenden noch besprochen werden, werden diese in bestimmten Fällen autonomen Fahrsystemen vorgezogen.

III. Arten der Absicherung automatisierter Fahrsysteme

Bei den Absicherungsprozessen ist zwischen zwei verschiedenen Arten zu unterscheiden, den Prozessen zur Absicherung der funktionalen Sicherheit und den Prozessen zur Absicherung der Sicherheit in Gefahrensituationen.

A. Funktionale Sicherheit

Der TÜV SÜD bezeichnet funktionale Sicherheit als "[...] die zuverlässige Erbringung der Sicherheitsfunktionen eines Systems. [...] wenn ein elektrisches oder elektronisches Schutzsystem im Ernstfall seine Funktion erfüllt." [3] Um also zu gewährleisten, dass ein Fahrsystem in jeder Situation so funktioniert, wie es soll, müssen Maßnahmen zur Absicherung ergriffen werden.

B. Sicherheit in Gefahrensituationen

Für die Sicherheit in Gefahrensituationen ist zunächst die Unterscheidung zwischen Gefahrensituationen und nicht gefährlichen Situationen, auch 'Safe States' genannt, zu machen. Als Safe State werden hier Zustände und Situationen bezeichnet, in denen keine unangemessene Gefahr vorliegt. Im Straßenverkehr besteht immer eine gewisse Gefahr, liegt diese aber unter einer bestimmten gesellschaftlich anerkannten Schwelle, so gilt eine Situation als sicher genug. Liegt die Gefahr einer Situation aber über dieser Schwelle, so redet man von einer Gefahrensituation. Die Gefahr einer Situation muss während der Nutzung eines Fahrsystems andauernd aus Umwelt- und Fahrzeugfaktoren berechnet werden. So muss sich ein Fahrsystem über die Eigenschaften der Umgebung und des eigenen Systems bewusst sein. Ein Umweltfaktor, der die Gefahr einer Situation erhöht, wäre zum Beispiel eine kalte Außentemperatur. Unter einer bestimmten Temperatur besteht ein Risiko auf Winterglätte, allgemein bekannt als Glatteis. Ein autonomes Fahrsystem könnte zum Beispiel durch Verringerung der maximalen Fahrgeschwindigkeit und der Fahrgeschwindigkeit in Kurven reagieren. Das Fahrzeug geht so von einer Situation mit zu hoher Gefahr, schnelles Fahren mit der Möglichkeit von Glatteis, zu einer Situation mit akzeptabler Gefahr. Welche Faktoren für ein Fahrsystem relevant zur Gefahrenanalyse sind, hängt von den Fahrsystemen, deren Automatisierungsgrad und Einsatzgebiet ab. Fahrsysteme, welche zum Fahren im öffentlichen Straßenverkehr Straßenmarkierungen über Bilderkennung erkennen müssen, werden in der Nacht mehr beeinträchtigt werden wie Parkassistenten, welche über Ultraschall in Parklücken lenken.

IV. Massnahmen zur Absicherung der funktionalen Sicherheit

A. Redundanz

Eine simple und effektive Maßnahme zur Absicherung der funktionalen Sicherheit ist Redundanz. Systeme werden hier mehrfach implementiert, um die Funktionalität auch bei Ausfall einzelner Teilsysteme zu garantieren. Automatisierte Fahrsysteme können aus anderen Bereichen mit kritischen Anwendungszwecken Maßnahmen übernehmen. So sind etwa Flugzeugsysteme immer dreifach redundant. Dreifache Redundanz ist in der Praxis ein guter Kompromiss aus Aufwand und Praktikabilität.

Konkret können durch Redundanz die beiden Faktoren Zuverlässigkeit und Datenintegrität verbessert werden. Die Zuverlässigkeit eines Systems gibt an, wie wahrscheinlich es ist, dass ein System in einem bestimmten Zeitraum korrekt funktioniert. Systemausfälle, welche die Zuverlässigkeit senken, sind generell eher selten, können aber durch redundante Backupsysteme weiter drastisch verringert werden. Bei kritischen Anwendungen wie autonomen Fahrsystemen ist dies von hoher Bedeutung.

Betrachtet wird ein Teilsystem eines autonomen Fahrsystems, das eine Ausfallwahrscheinlichkeit von 1% pro Fahrt hat. Wird davon ausgegangen, dass das Fahrzeug mit diesem Fahrsystems ein Jahr lang täglich eine Fahrt tätigt, so ergibt sich eine Wahrscheinlichkeit von bloß 2,6%, dass das Fahrzeug ohne Systemausfall funktioniert. Bei kritischen Teilsystemen, wie zum Beispiel der Erkennung von anderen Verkehrsteilnehmern, ist diese Wahrscheinlichkeit viel zu niedrig.

Die Ausfallwahrscheinlichkeit p eines n-Fach redundanten Systems, bei der die einzelnen Teilsysteme eine Ausfallwahrscheinlichkeit von p_i haben, kann mit der Formel

$$p = \prod_{i=1}^{n} p_i$$

berechnet werden. [4] Da davon ausgegangen werden kann, dass die einzelnen Teilsysteme die gleiche Ausfallwahrscheinlichkeit p_0 haben, kann die Formel zu

$$p = p_0^n$$

vereinfacht werden. Wird das Teilsystem von vorhin nun dreifach redundant implementiert, haben die einzelnen Untersysteme zwar immer noch eine Ausfallwahrscheinlichkeit p_0

von 1% pro Fahrt, das gesamte Teilsystem aber damit eine Ausfallwahrscheinlichkeit p von nur 0,0001% pro Fahrt, da nun alle drei Untersysteme ausfallen müssten. Somit hätte das Fahrzeug mit diesem Fahrsystem bei einem Jahr mit einer Fahrt pro Tag eine Wahrscheinlichkeit von 96,4% ohne Systemausfall zu funktionieren. Die verwendeten Werte sind frei gewählt und damit nicht unbedingt realitätsnah, sollen aber bloß anschaulich zeigen, dass durch Redundanz die Zuverlässigkeit enorm verbessert werden kann. Im Allgemeinen lässt sich der Faktor c, um den sich die Ausfallwahrscheinlichkeit verbessert, durch die Formel

$$c = \frac{p_0}{p} = \frac{p_0}{p_0^n} = p_0^{-n+1}$$

berechnet werden. So kann in dem Beispiel die Ausfallwahrscheinlichkeit um den Faktor 10000 verringert werden.

Datenintegrität bezeichnet die Korrektheit und Vollständigkeit von Daten. Bei automatisierten Fahrzeugen konkret die Daten, die von Fahrsystemen gesammelt und verarbeitet werden. Bei Sensoren und Software, die die Daten der Sensoren verarbeiten, besteht immer eine gewisse Wahrscheinlichkeit, dass diese einen falschen Wert weitergeben. Durch Redundanz bei diesen Systemen kann diese Wahrscheinlichkeit verringert werden.

Implementiert wird Redundanz zur Datenintegrität meist durch n redundante, parallele Teilsysteme und einen Mehrheitsentscheider. Ein solches System mit dreifacher Redundanz ist in Abbildung 1 zu sehen. Die Teilsysteme A, B und C messen bzw. berechnen dieselben Daten und geben ihre Ergebnisse nach jeder atomaren Operation an den Mehrheitsentscheider M weiter. Dieser gibt dann den Wert weiter, der von den Teilsystemen mehrheitlich genannt wurde. Sollten A und C den Wert 1 und B den Wert 0 an M weitergeben, so entscheidet sich M den Wert 1 weiterzugeben. Der Mehrheitsentscheider kann nicht wissen welcher Wert korrekt ist. Werden von den Teilsystemen mehrheitlich falsche Werte weitergegeben, so gibt der Mehrheitsentscheider auch einen falschen Wert weiter. Die Wahrscheinlichkeit, dass ein Teilsystem einen korrekten Wert weitergibt ist allerdings im Vergleich zu der Wahrscheinlichkeit, dass ein falscher Wert weitergegeben wird, viel höher. Somit ist die Korrektheit von Daten zwar nicht in allen Fällen garantiert, aber trotzdem wahrscheinlicher.

Die Wahrscheinlichkeit p_m eines solchen n-fach redundanten Systems mit Mehrheitsentscheider, den richtigen Wert weiterzugeben, kann mit der Formel

$$p = (1 - p_0)^m$$

berechnet werden, wobei angenommen wird dass alle Teilsysteme dieselbe Fehlerwahrscheinlichkeit p_0 haben. Die Mehrheitsanzahl m gibt die Anzahl an Werten an, die gleich sein müssen um zu einer Mehrheit führen. Diese kann mit der Formel

$$m = \frac{n - n \bmod 2}{2} + 1$$

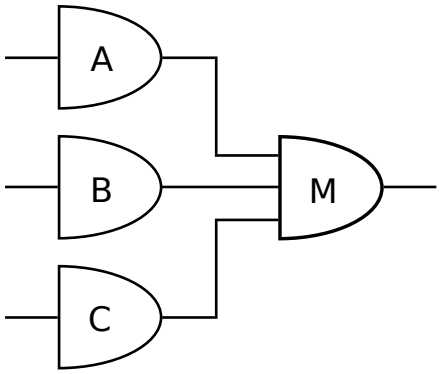

Abbildung 1. Mehrheitsentscheider

berechnet werden. Da bei Mehrheitsentscheidern normalerweise eine ungerade Anzahl an Teilsystemen verwendet wird, kann bei diesen Fällen die Formel

$$m_u = \frac{n_u + 1}{2}$$

verwendet werden.

Angenommen wird nun, dass die Teilsysteme A, B und C identisch sind und alle eine Fehlerwahrscheinlichkeit p_0 von 1% pro Operation haben. Die Teilsysteme einzeln hätten so bei bereits 100 Operationen bloß eine Wahrscheinlichkeit von 36,6%, immer die richtigen Werte weiterzugeben. Das in Abbildung 1 dargestellte System hat im Gegensatz dazu eine Fehlerwahrscheinlichkeit p_m von nur 0,01% pro Operation, da bei einer Operation mindestens zwei der drei Teilsysteme Fehlerhaft sein müssten, sodass M einen falschen Wert ausgibt. Damit ergibt sich für dieses System bei 100 Operationen eine Wahrscheinlichkeit von 99,0%, dass jedes mal am Ende die richtigen Werte von M weitergegeben werden. Genauso wie beim Beispiel davor sind die hier verwendeten Werte frei gewählt und dienen nur zur Veranschaulichung.

Es ist zu erkennen, dass die Datenintegrität durch Redundanz enorm verbessert werden kann. Bei kritischen Anwendungen wie etwa automatisierten Fahrsystemen ist dies von hoher Bedeutung, da gewisse Systeme praktisch immer richtige Daten liefern müssen. Ein einzelnes Bilderkennungssystem eines autonomen Fahrzeugs, dass einen Fußgänger übersieht, kann durch parallele Bilderkennungssysteme korrigiert, eine Kollision verhindert und somit ein Leben gerettet werden.

Diversität kann auch als eine Form der Redundanz betrachtet werden. Bei automatisierten Fahrzeugen werden so meist verschiedene Sensoren implementiert. Bei autonomen Fahrzeugen werden Kameras mit Bilderkennungssystemen zur Wegfindung und Gefahrenerkennung eingesetzt. Als zusätzliche Absicherung haben diese Fahrzeuge aber in fast allen Fällen noch Radar- oder Ultraschallsensoren, die Objekte in der nahen Umgebung des Fahrzeugs erkennen können. Bilderkennung bei automatisierten Fahrzeugen geschieht heutzutage meist durch den Einsatz von künstlicher Intelligenz. Diese Black-Box-Systeme liefern Ergebnisse, ohne dass völlig bekannt ist, wie diese exakt berechnet werden.

Bei perfekt trainierten KI-Systemen werden jedes mal richtige Ergebnisse geliefert. Da dies in der Realität aber nicht möglich ist, kann es in einzelnen Fällen zu Fehlern kommen. Sollte so ein Hindernis von der Bilderkennung nicht erkannt werden, kann eine Kollision aber trotzdem durch Radar- oder Ultraschallsensoren verhindert oder wenigstens vermindert werden.

Redundanz hat allerdings auch einige Nachteile, die ebenfalls beachtet werden müssen. Bei n-fach redundanter Hardware fallen auch n-fach viele Kosten für diese an. Bei einzelnen Teilsystemen können diese Kosten noch relativ trivial sein. Bei automatisierten Fahrsystemen entstehen dadurch bei dreifacher Redundanz dreifache Hardwarekosten für das gesamte Fahrsystem, was sich deutlich auf die Kosten und somit den Preis des Fahrzeugs auswirkt. Zusätzlich ergeben sich durch Hardwareredundanz auch noch ein erhöhter Platzverbrauch, erhöhte Komplexität und ein erhöhter Stromverbrauch. Dies sind aber alles Faktoren, die in kauf genommen werden müssen. Bei Fahrsystemen sind praktisch alle Teilsysteme direkt oder indirekt kritisch, weshalb Redundanz des kompletten Fahrsystems unumgänglich ist, um die funktionale Sicherheit zu gewährleisten.

B. Codequalität

Bei Fahrzeuganwendungen ist qualitativ hochwertiger Code von extremer Wichtigkeit. Kontrollverlust oder Fehlverhalten eines Fahrsystems ist besonders kritisch. Ein einzelner Fehler könnte schon der Unterschied zwischen Leben und Tod sein.

Qualitativ hochwertiger Code hat eine geringe Komplexität, hohe Überprüfbarkeit, hohe Lesbarkeit und die Richtigkeit des Kontroll- und Datenflusses. Software mit qualitativ hochwertigem Code hat somit im Idealfall bestimmte Eigenschaften, die bei kritischen Anwendungen, wie etwa dem automatisierten Fahren, erfordert werden. Zuverlässigkeit, dass etwas jedes mal so funktioniert, wie es sollte, ist ein wichtiger Bestandteil der funktionalen Sicherheit und ergibt sich in einer Anwendung aus qualitativ hochwertigem Code. Die Zuverlässigkeit wird weiterhin durch die Testbarkeit, Wartbarkeit und Portierbarkeit sichergestellt. Ohne Testbarkeit ist es nur erschwert möglich Fehler im Code zu finden, wodurch diese im Falle der automatisierten Fahrsysteme vielleicht erst im Verkehr auffallen und womöglich Verkehrsteilnehmer gefährden oder sogar verletzen. Wartbarkeit ist deshalb auch wichtig, um gefundene Fehler zu beheben. Zusätzlich ist Portierbarkeit auch wichtig, da eine ansonsten Fehlerfreie Anwendung auf einem System auf einem anderen System zu Fehlern führen könnte. Bei Fahrzeugsoftware, die von Drittanbietern oder für verschiedene Fahrzeugmodelle entwickelt wird, wäre dies eine realistische Gefahr.

Um die Qualität von Code bei automatisierten Fahrsystemen sicherzustellen, werden unter anderem Coding Standards verwendet. Coding Standards sind Richtlinien, die Softwareentwickler beim Schreiben ihres Codes befolgen müssen, um dessen Qualität zu verbessern. Coding Standards gibt es für Code im Allgemeinen und für Code für bestimmte Anwendungszwecke. Für Straßenfahrzeuge gibt es den ISO 26262 Standard, welcher neben generellen Richtlinien zur funktionalen Sicherheit auch Coding Standards und Richtlinien für Code festlegt. Diese Codings Standards gelten für digitale aber auch für automatisierte und autonome Fahrsysteme.

C und C++ sind die in der Fahrzeuginformatik meistgenutzten Sprachen. Für diese gibt es für kritische Anwendungen die konkreten Coding Standards MISRA C und CERT C. C und C++ werden aufgrund ihrer Hardwarenähe und daraus resultierenden Performanz verwendet, haben aber auch den Nachteil, dass sie in bestimmten Situationen undefiniertes Verhalten zeigen, was zu Fehlern führen kann. Meist werden diese Problemstellen auch nicht von den Compilern gefunden oder behoben. Ein Beispiel für eine solche Situation ist im C-Codefragment 2 zu sehen.

```
INPUT = 4

int numbers[4] = {1, 2, 3, 4};

numbers[INPUT] = 7;
```

Abbildung 2. Array out of Bounds Problem

'INPUT' stellt hierbei vereinfacht als Konstante den eingegebenen Wert eines Benutzers dar. Das Integer Array $numbers$ hat nur die Indizes 0 bis 3. Wird versucht auf einen Index außerhalb dieses Bereichs zuzugreifen, wird versucht auf einen Bereich im Speicher zuzugreifen, der nicht für die aktuelle Anwendung reserviert wurde. Bei Schreiboperationen führt dies meist dazu, dass der Schreibvorgang vom System verweigert wird, bei Leseoperationen dazu, dass entweder der Lesevorgang verweigert wird oder ein zufälliger Wert, der für die Operation unbrauchbar ist, gelesen wird. Eine Möglichkeit, wie dieses Problem gelöst werden kann, ist im C-Codefragment 3 zu sehen.

```
int numbers[4] = {1, 2, 3, 4};

if(INPUT < 0 || INPUT > 3) {
    handleError();
} else {
    numbers[INPUT] = 7;
}
```

Abbildung 3. Lösung für das Array out of Bounds Problem

Indem vor dem indizierten Zugriff überprüft wird, ob der gewählte Index zulässig ist, können Ausnahmen, die zu Fehlern führen würden, behandelt werden. In C++ wäre es so zum Beispiel möglich Exceptions einzusetzen. Diese explizite Fehlerbehandlung ist auch wichtig, da bestimmt Fehler, wie zum Beispiel Division durch null, die ganze Anwendung zum Absturz bringen können, was bei kritischen Anwendungen nicht passieren darf.

Die korrekte Verwendung von Coding Standards muss auch überprüft werden. Dies geschieht über manuelle und statische Überprüfung. Manuelle Überprüfung ist die Überprüfung von Code durch Entwickler oder Entwicklerteams. Sie ist zeit- und kostenaufwendig und kann nicht für dem gesamten Code verwendet werden. Die Systeme eines nicht autonomen Fahrzeugs

haben heutzutage bereits ungefähr 100 Millionen Zeilen Code, was eine komplette manuelle Überprüfung unmöglich macht. Dafür gibt es die statische Überprüfung. Hierbei überprüft eine Software Code auf Coding Standards, ähnlich wie IDEs den Syntax von Code überprüfen. Statische Überprüfung hat einen enorm geringeren Kosten- und Zeitaufwand als manuelle Überprüfung und kann somit den kompletten Code überprüfen. Die statische Überprüfung ist aber kein Ersatz für die manuelle Überprüfung, da die statische Überprüfung Sonderfälle nicht erkennen und selbst Fehler übersehen kann. Sie wird deshalb ergänzend zur manuellen Überprüfung benutzt.

V. Massnahmen zur Absicherung der Sicherheit in Gefahrensituationen

Um von einer Gefahrensituation in einen Safe State zu gelangen gibt es je nach Situation und Fahrsystem drei Möglichkeiten.

A. Anpassen der Fahrparameter

Bei Gefahrensituationen mit einem eher geringen Risiko ist es möglich und sinnvoll, Fahrparameter anzupassen. Automatisierte Fahrsysteme können so unter anderem die Fahrgeschwindigkeit verringern, Abstand zu anderen Autos erhöhen oder bestimmte Fahrmanöver, wie etwa das Überholen, blockieren. Welche Fahrparameter vom Fahrsystem angepasst werden können hängt natürlich davon ab, welche Fahrparameter ein automatisiertes Fahrsystem beeinflussen kann. Ein Spurhalteassistent, welcher nur die Querführung beeinflussen kann, kann zum Beispiel das hohe Risikolevel einer Situation nicht verringern, wenn dieses dadurch entsteht, dass der Fahrer zu schnell fährt. Als Situation, in der das Anpassen der Fahrparameter die sinnvollste Möglichkeit ist, um in einen Safe State zu gelangen, ist ein autonomes Fahrzeug mit zu wenig Abstand zum vorausfahrenden Fahrzeug zu nennen. Durch eine Anpassungen der Fahrgeschwindigkeit kann ein Ausreichender Abstand wiederhergestellt werden, bei dem es im Falle einer Vollbremsung nicht zu einer Kollision kommen würde.

B. Kontrolle an den Fahrer zurückgeben

Die einfachste Möglichkeit ist, dem Fahrer die Kontrolle über das Fahrzeug zurückzugeben. Über eine audiovisuelle Meldung wird der Fahrer aufgefordert, die Kontrolle des Fahrzeugs zu übernehmen. Das automatisierte Fahrsystem kann dann die Kontrolle über das Fahrzeug auf Software- bzw. Hardwareebene aufgeben. So wird in einigen automatisierten Fahrzeugen das Fahrsystem physisch von der Schnittstelle, mit der es das Fahrzeug steuern kann, getrennt. Der menschliche Fahrer kann dann das Fahrzeug wieder in einen Safe State bringen.

Dies funktioniert allerdings nur bei nicht autonomen Fahrzeugen, da ein menschlicher Fahrer und Steuerelemente für diesen im Fahrzeug vorausgesetzt werden. Bei autonomen Fahrzeugen ist diese Möglichkeit so nicht möglich. Hier ergibt sich einer der vermeintlichen Vorteile vollautomatisierter Fahrzeuge gegenüber autonomen Fahrzeugen, da bei vollautomatisierten Fahrzeugen ein menschlicher Fahrer im Notfall eingreifen kann. Bei längeren Fahrten mit vollautomatisierten Fahrsystemen können menschliche Fahrer diese aber nur schlecht überwachen. Fahrer passen aufgrund der Abwesenheit von Aufgaben, wie Lenken, Bremsen, Gas Geben und Beobachten des Verkehrs, nach einer gewissen Zeit nicht mehr auf und werden abgelenkt, etwa von den Multimediasystemen des Fahrzeugs. Sollte sich das Fahrzeug nun plötzlich in einer kritischen Situation befinden, können abgelenkte menschliche Fahrer nur verspätet oder gar nicht eingreifen, auch wenn diese rechtzeitig eine audiovisuelle Meldung vom Fahrzeug bekommen.

C. Fahrzeugstillstand

In bestimmten Situationen mit einer schwerwiegenderen Gefahr ist es am sinnvollsten, das Fahrzeug zum Stillstand zu bringen. Falls es nicht möglich sein sollte, dem Fahrer die Kontrolle über das Fahrzeug oder rechtzeitig die Kontrolle über das Fahrzeug zurückzugeben, ist der Fahrzeugstillstand vorzuziehen. Dies trifft vor allem bei autonomen Fahrzeugen zu, da diese nicht von menschlichen Fahrern gesteuert werden können, und in Situationen, bei denen der Fahrer nicht schnell genug reagieren kann, wie etwa einer Notbremsung.

Bei dieser kann ein automatisiertes Fahrsystem beinahe ohne Reaktionszeit abbremsen, wodurch der Anhalteweg gegenüber des Anhalteweges eines menschlichen Fahrers in der gleichen Situation verkürzt wird. Der Anhalteweg d_A, die Distanz die ein Fahrzeug bis zum Erreichen des Stillstands benötigt, besteht aus dem Reaktionsweg d_R und dem Bremsweg d_B. Der Reaktionsweg d_R ist die Distanz, die das Fahrzeug zurücklegt, während der Fahrer reagiert und kann mit der Formel

$$d_R = \frac{v}{10} \cdot 3$$

für menschliche Fahrer angenähert werden, wobei v die Fahrgeschwindigkeit zu Beginn des Anhaltevorgangs ist. [5] Bei einer Geschwindigkeit v von 50 km/h hätte ein automatisches Fahrsystem bereits einen um bis zu 15 m kürzeren Anhalteweg. Jeder Meter, um den der Anhalteweg verkürzt werden kann, verringert die Wahrscheinlichkeit einer Kollision oder zumindest die Geschwindigkeit, mit der diese passiert.

In Situationen, bei denen es mittel- bis langfristig zu gefährlich wäre, auch mit angepassten Fahrparametern weiterzufahren und bei denen kein menschlicher Fahrer übernehmen kann oder dies keinen Sinn machen würde, gilt der Fahrzeugstillstand auch unter bestimmten Voraussetzungen als Safe State. Steht ein Fahrzeug auf dem Standstreifen oder am Straßenrand und blockiert den Verkehr nicht, so befindet es sich in einem Safe State.

Sollte es nicht möglich sein den Straßenrand oder Standstreifen mit annehmbarer Gefahr zu erreichen, befindet sich ein Fahrzeug in einem Safe State, wenn die relative Geschwindigkeit zu anderen Fahrzeugen nicht zu groß ist, Notfallfahrzeuge, wie Krankenwagen und Feuerwehrautos, nicht blockiert werden und das Fahrzeug in kurzer Zeit von der Fahrbahn entfernt werden kann.

Ein Beispiel für eine Situation, in der der Fahrzeugstillstand auf der Fahrbahn als Safe State zu betrachten ist, wäre ein autonomes Fahrzeug auf einer Bundesstraße, bei dem die Sensorsysteme ausgefallen sind, zu sehen in der Abbildung 4.

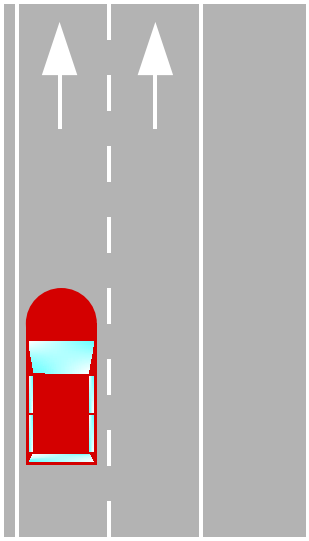

Abbildung 4. Situation 1

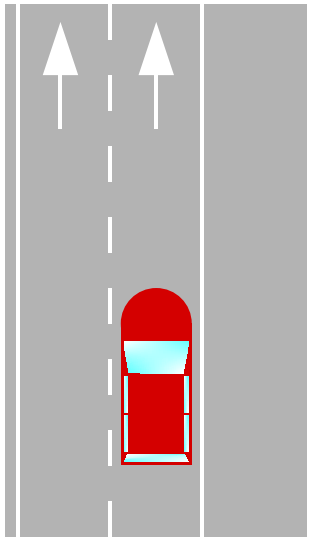

Abbildung 5. Situation 2

Das rote Fahrzeug befindet sich auf der linken Fahrspur und ein Weiterfahren ist nicht möglich. Zudem kann die Steuerung nicht von einem menschlichen Fahrer übernommen werden, da es sich um ein autonomes Fahrzeug handelt. Ohne funktionierende Sensorsysteme ist es für das rote Fahrzeug nicht möglich wahrzunehmen, ob sich ein anderes Fahrzeug auf der rechten Fahrspur befindet oder wo der Standstreifen und anderen Fahrspuren überhaupt sind. Somit ist es zu gefährlich oder sogar gar nicht möglich, den Standstreifen rechts zu erreichen. Hier ist nun die sicherste Möglichkeit, einen Safe State zu erreichen, das Fahrzeug auf der aktuellen Fahrspur zum Stillstand zu bringen. Dies wäre auch in der Situation in Abbildung 5 der Fall. Es wirkt zunächst, als ob das rote Fahrzeug einfach auf den Standstreifen fahren könnte, vor allem da dafür keine andere Fahrspur überquert werden muss wie in Abbildung 4, jedoch kann das Fahrsystem nicht wahrnehmen, wo sich der Standstreifen befindet und ob auf diesem bereits ein anders Fahrzeug steht. Deshalb ist es auch in dieser Situation am sichersten auf der aktuellen Fahrspur zum Stillstand zu kommen.

VI. Rechtliche Situation automatisierter Fahrsysteme in Deutschland

Automatisierte Fahrzeuge im Straßenverkehr sind eine relativ neue Entwicklung. Erst seit Anfang der 2000er Jahre sind kommerzielle Fahrzeuge mit wenn auch nur niedrigem Automatisierungsgrad verbreitet. So ist die rechtliche Lage automatisierter Fahrzeuge, insbesondere automatisierter Fahrzeuge mit hohem Automatisierungsgrad, im Straßenverkehr in vielen Ländern noch ungeklärt, da Regierungen oft lange Zeit brauchen, um auf neue Techniktrends zu reagieren.

Das weltweit erste Gesetz zur Regulierung von Fahrzeugen mit hohem Automatisierungsgrad gilt in Deutschland seit 2017. Das sogenannte “Gesetz zum automatisierten Fahren” erlaubt den Einsatz von Fahrzeugen mit bis zu vollautomatisierten Fahrsystemen. Es werden Rechte und Pflichten für Fahrer, Besitzer sowie Hersteller, aber auch technische Voraussetzungen für die Fahrzeuge und Fahrsysteme festgelegt, welche den Einsatz automatisierter Fahrzeuge im Straßenverkehr ermöglichen sollen. So müssen Fahrer von automatisierten Fahrzeugen präsent sein, müssen aus rechtlicher Sicht aber während der automatisierten Fahrfunktion diese nicht durchgehend überwachen. Bei Unfällen haftet weiterhin der Fahrer, auch wenn dieser während des Unfalls das Fahrzeug nicht gesteuert hat. Bei Soft- oder Hardwarefehlern kann der Hersteller des automatisierten Fahrzeugs aber auch mithaften.

2021 soll nun das “Gesetz zum autonomen Fahren” folgen, welches dann einen rechtlichen Rahmen für autonome Fahrzeuge festlegt. Das Ziel ist es, den Einsatz komplett autonomer Fahrzeuge ohne Fahrer zu ermöglichen. Das Gesetz wird sich hauptsächlich auf Richtlinien und Voraussetzungen für die Fahrsysteme und Fahrzeuge, Betreiber und Hersteller fokussieren, da Fahrer im Vergleich zu vollautomatisierten Fahrzeugen komplett wegfallen. Zunächst sollen autonome Fahrzeuge nur als alternative öffentliche Verkehrsmittel oder in der Industrie eingesetzt werden, als eine Art Test, um sicherzustellen, dass autonome Fahrsysteme sicher genug sind, bevor diese für Privatpersonen frei auf dem Markt verfügbar sind.

Zudem ergibt sich ohne einen Fahrer bei autonomen Fahrzeugen das Problem der Haftung. Bei schwerwiegenden Soft- oder Hardwarefehlern haftet wie beim Gesetz zum automatisierten Fahren weiterhin auch der Hersteller des Fahrzeugs. Im aktuellen Gesetzesentwurf ist aber vorgesehen, dass hauptsächlich der Halter eines autonomen Fahrzeugs für dieses haftet. Diese Regelung wurde von Verbraucherschützern stark kritisiert, da die Schuld bei einem Unfall eines autonomen Fahrzeugs eigentlich beim Fahrzeug selbst liegt und somit beim Hersteller. Deshalb wird auch zunächst der Einsatz autonomer Fahrzeuge im öffentlichen und industriellen Raum vorgesehen, da öffentliche Betreiber und Firmen mit der Haftung besser umgehen können. Kritisch ist deshalb zu betrachten, ob sich so mit der aktuellen Gesetzeslage autonome Fahrzeuge bei Verbrauchern überhaupt durchsetzen können.

Aufgrund der in Kürze bestehenden Gesetzeslage werden voraussichtlich viele Verbraucher, die ansonsten bereit wären, sich ein autonomes Fahrzeug anzuschaffen, davon abgeschreckt. Mit der schon angesprochenen Regelung, außer in bestimmten Fällen den Halter eines autonomen Fahrzeugs und nicht den Hersteller für das Fahrzeug haften zu lassen, als Hauptgrund. Der Halter eines autonomen Fahrzeuges hat kaum bis keinen Einfluss auf dessen konkretes Fahrverhalten. Viele Verbraucher werden so wahrscheinlich nicht dazu bereit sein, potentiell für Unfälle zu haften, die sie nicht verursacht haben und auf die sie keinen Einfluss hatten. Mit genügender

Absicherung könnte so die Anzahl an Unfällen, die autonome Fahrzeuge verursachen, auf ein Niveau gebracht werden, das niedrig genug ist, dass Verbraucher genug Vertrauen haben, dass sie für keinen Unfall haften werden und somit bereit wären sich ein autonomes Fahrzeug anzuschaffen.

Die Haftung für autonome Fahrzeuge kann aber auch anders Verstanden werden. Da die Hersteller eines autonomen Fahrzeugs im Falle von Soft- oder Hardwarefehlern für dieses Haften, könnte es sein, dass Hersteller so in den meisten Fällen für ihre Fahrzeuge haften. So können autonome Fahrzeuge eigentlich nur im Falle von Soft- oder Hardwarefehlern überhaupt Unfälle verursachen. Absicherung der Fahrzeuge spielt hiermit auch wieder eine extrem wichtige Rolle, da so Hersteller von autonomen Fahrzeugen ihre Haftung bei Unfällen und somit ihren zu zahlenden Schadensersatz minimieren. Autonome Fahrzeuge könnten nämlich Unfälle verursachen, deren Schaden deutlich über dem Gewinn, den der Hersteller durch den Verkauf erzielte, liegt. Ein autonomes Fahrzeugmodell könnte so dadurch unrentabel sein, da Kosten für Schadensersatz im Vergleich zu Gewinnen durch Fahrzeugverkäufe zu hoch sind. Auch dadurch, dass ein als unsicher wirkendes Fahrzeug zu einer geringeren Nachfrage von Verbrauchern führt. Dies kann auch gelten, wenn die Unfallquote autonomer Fahrzeuge niedriger ist, als die Unfallquote nicht autonomer Fahrzeuge, da Sicherheit im Verkehr oft sehr subjektiv ist und Verbraucher so nicht unbedingt objektive Kaufentscheidungen treffen. Außerdem gibt es noch keine zuverlässigen Statistiken oder Studien, die Unfälle automatisierter Fahrzeuge behandeln, weshalb informierte Entscheidungen auch erschwert werden.

VII. Fazit

Ausreichende aber vor allem überzeugende Sicherheit ist die letzte Hürde, die autonome Fahrzeuge überwinden müssen, um Verbraucher, Gesetzgeber und Automobilhersteller vom autonomen Fahren zu überzeugen. Fahrzeuge mit niedrigem bis hohem Automatisierungsgrad sind bereits weit verbreitet. Die meisten Neuwägen bieten viele verschiedene Assistenzsysteme entweder als Standard- oder als optionale Zusatzfeatures. Seit noch nicht allzu langer Zeit sind auch für Verbraucher Softwareerweiterungspakete für bestimmte Modelle des Automobilherstellers Tesla verfügbar, die hoch- bzw. vollautomatische Fahrfunktionen ermöglichen. Bis autonome Fahrzeuge jedoch für Verbraucher erhältlich sind, kann es aber noch lange Zeit dauern. Sicherheit wird von vielen als höchstes Gut betrachtet und solange diese bei autonomen Fahrzeugen noch nicht ausreichend garantiert ist, ist eine Annahme autonomer Fahrzeuge nicht möglich.

Literatur

[1] Bundesamt für Straßenwesen.
Selbstfahrende Autos – assistiert, automatisiert oder autonom?
11. März 2021. URL:
https://www.bast.de/BASt_2017/DE/Presse/Mitteilungen/2021/06-2021.html.

[2] Tom M Gasser u. a.
"Rechtsfolgen zunehmender Fahrzeugautomatisierung". In:
Wirtschaftsverlag N.W. Verlag für neue Wissenschaft GmbH, 2012.
ISBN: 978-3-86918-189-9. URL: https://bast.opus.hbz-nrw.de/opus45-bast/frontdoor/deliver/index/docId/541/file/F83.pdf.

[3] TÜV SÜD. *FUNKTIONALE SICHERHEIT VON PRODUKTEN, MASCHINEN UND ANLAGEN*. URL:
https://www.tuvsud.com/de-de/indust-re/funktionale-sicherheit-info.

[4] *Redundancy (engineering)*.
URL: https://en.wikipedia.org/wiki/Redundancy_(engineering).

[5] ADAC Redaktion. *Anhalteweg berechnen: Mit dieser Formel geht's*.
26. Apr. 2021. URL: https://www.adac.de/verkehr/rund-um-den-fuehrerschein/erwerb/anhalteweg-berechnen/.

[6] Andreas Reschka. "Safety Concept for Autonomous Vehicles". In:
Autonomous Driving: Technical, Legal and Social Aspects.
Hrsg. von Markus Maurer u. a.
Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, S. 473–496.
ISBN: 978-3-662-48847-8. DOI: 10.1007/978-3-662-48847-8_23.

[7] Presse- und Informationsamt der Bundesregierung.
Autonomes Fahren in die Praxis holen.
URL: https://www.bundesregierung.de/breg-de/suche/faq-autonomes-fahren-1852070.

[8] Jill Britton und Frank van den Beuken.
Role of Coding Standards in Autonomous Vehicles.
Hrsg. von Inc. Perforce Software. 26. Apr. 2021.
URL: https://www.perforce.com/webinars/qac/role-coding-standards-autonomous-vehicles.

[9] Markus Hörwick und Karl-Heinz Siedersberger.
"Strategy and architecture of a safety concept for fully automatic and autonomous driving assistance systems".
In: *2010 IEEE Intelligent Vehicles Symposium*. 2010, S. 955–960.
DOI: 10.1109/IVS.2010.5548115.

[10] Tasuku Ishigooka, Shinya Honda und Hiroaki Takada.
"Cost-Effective Redundancy Approach for Fail-Operational Autonomous Driving System". In: *2018 IEEE 21st International Symposium on Real-Time Distributed Computing (ISORC)*. 2018, S. 107–115. DOI: 10.1109/ISORC.2018.00023.

[11] Jack Karsten und Darrell West.
The state of self-driving car laws across the U.S.
Hrsg. von The Brookings Institution. 1. Mai 2018.
URL: https://www.brookings.edu/blog/techtank/2018/05/01/the-state-of-self-driving-car-laws-across-the-u-s/.

[12] Bundesministerium für Verkehr und digitale Infrastruktur.
Deutschland wird international die Nummer 1 beim autonomen Fahren. 21. Mai 2020.
URL: https://www.bmvi.de/SharedDocs/DE/Artikel/DG/gesetz-zum-autonomen-fahren.html.

[13] Gerald Traufetter.
Hersteller sollen bei Unfällen mit autonomen Fahrzeugen haften.
7. Mai 2020. URL: https://www.spiegel.de/auto/autonomes-fahren-hersteller-sollen-bei-unfaellen-haften-fordern-verbraucherschuetzer-a-78df0b3a-0002-0001-0000-000177426963.