Fahrerassistenzsysteme: Eine Herausforderung an Sachverständige und Juristen – Teil 2

*von Dipl.-Ing. Axel Tenzer, Hannover**

Fortsetzung aus VRR 2009, 214 ff.

III. Mögliche Fehlfunktionen und deren Detektion durch den technischen Sachverständigen

1. Allgemeines

Wie in Teil 1 (VRR 2009, 214 ff.) gezeigt, sind moderne Fahrerassistenzsysteme **technisch in der Lage**, über Eingriffe in Lenkung, Drosselklappenstellung und Bremsen fahrerwunschunabhängige **Abbremsungen**, **Beschleunigungen** oder **Lenkmanöver einzuleiten**. Die Herausforderung für den Sachverständigen wird sein, den Vortrag einer solchen Fehlfunktion zu prüfen.

Grds. ist aufgrund der Sorgfalt in der Produktentstehungskette (Entwurf über Entwicklung bis hin zur Produktion und Serienüberwachung) eine Fehlfunktion relativ unwahrscheinlich. Auch wenn bei einer Wahrscheinlichkeitsbetrachtung **Systemfehler vs. Fehlbedienung oder allgemeine Fahrfehler** die größere Wahrscheinlichkeit eindeutig auf dem Fahrfehler liegen wird, ist ein technischer Defekt nie à priori auszuschließen. Dies zeigt allein die hohe Anzahl von Rückrufen der Fahrzeughersteller.

Die ISO 26262 („Road vehicles – Functional safety") ist eine entstehende ISO-Norm (ISO = Internationale Organisation für Normung [engl. International Organization for Standardization]) für sicherheitsrelevante Systeme in Kfz. Ihr Einsetzen als Norm wird für etwa 2011 erwartet. Der Normentwurf sieht vor, dass auf Basis des Systemkonzepts die potenziell gefährlichen Situationen (hazards) ermittelt werden. Anschließend wird jede Gefahr mit einer Sicherheitsanforderungsstufe von A bis D klassifiziert (automotive safety integrity level – ASIL), bzw. als nicht sicherheitsrelevant eingeordnet (quality management – QM). Dazu muss für jede identifizierte Gefahr einzeln der Verletzungsgrad (severity – S), die Häufigkeit der Situation (exposure – E) und die Beherrschbarkeit der Situation durch den Fahrer (controllability – C) abgeschätzt werden. Aus einer vorgegebenen Tabelle lässt sich dann für jede Gefahr die Einstufung QM oder ASIL A bis D ablesen.

Mit steigendem ASIL steigen auch die Anforderungen an die Sicherheit, die in den nachfolgenden Teilen spezifiziert sind. An Gefahren der Klasse QM sind keine Anforderungen gestellt, die über das übliche Qualitätsmanagement des Systemherstellers hinausgehen (Quelle: *http://de.wikipedia.org/wiki/ISO_26262*). Für sicherheitsrelevante Systeme und Systemkomponenten, die eine ASIL A Einstufung oder höher erhalten haben, sind bestimmte Prozesse und Anforderungen an die Entwicklung und das fertige Produkt definiert, die z.B. in einer Ausfallrate von $1*10^{-8}$/h nicht überschreiten dürfen. Das kann über bestimmte Anforderungen an die Programmierung als auch die Hardware des Systems bis hin zu redundanten Bauteilen führen (z.B. zwei unabhängig voneinander arbeitende Steuergeräte für die gleiche Funktion). Weiterhin werden Ausfallstrategien vorgeschrieben. Eine der bekanntesten ist „Fail-safe". Dies bedeutet, dass bei einem Ausfall des Systems oder einzelner Komponenten ein (möglichst) sicherer Zustand erzeugt wird. Ein Beispiel ist hier die Federspeicherbremse bei Nutzfahrzeugen. Die Bremsbeläge werden mittels Federkraft auf eine Bremsscheibe oder -trommel gedrückt. Um die Bremse zu lösen, muss daher eine Kraft aufgewendet werden, was i.d.R. durch Druckluft (Pneumatikzylinder) oder durch Hydraulikpumpen erreicht wird. Versagt das System z.B. durch Bruch in der Druckluftleitung, nimmt die Bremse automatisch einen sicheren Zustand ein, in dem sie gebremst wird. Auch wenn die Norm noch nicht in Kraft gesetzt ist, so werden bei allen (deutschen) Fahrzeugherstellern die Risikoanalysen bei der Entwicklung von Fahrerassistenzsystemen bereits durchgeführt.

Es ist jedoch i.d.R. davon auszugehen, dass Entwicklungsprozesse und Algorithmen von Fahrerassistenzsystemen und deren Parameter von den Herstellern als schutzbedürftig angesehen werden. Dies führt in einigen Fällen soweit, dass der Zwischenkunde, der Automobilhersteller, der das System einbaufertig von dem Zulieferer kauft, selber keinen Einblick in diese Daten hat.

Eine retrospektive Ermittlung einer Fehlfunktion ist nicht trivial. Sie kann im Einzelfall bis hin zu einem **Ausbau von Sensorik und Aktuatorik** führen. Eine überragende Hilfestellung seitens der Hersteller ist aus o.g. Gründen nicht zwingend zu erwarten.

Insbesondere von Bedeutung ist, dass der Sachverständige einen zeitnahen Zugang auf das nach Möglichkeit nach dem Auftreten des Fehlers unveränderte Fahrzeug hat. Hier wäre ein selbstständiges Beweisverfahren oder zumindest eine Asservierung des betroffenen Fahrzeugs oder der relevanten Komponenten hilfreich.

Bei einer vorgetragenen Fehlfunktion eines Assistenzsystemes ist der Sachverständige gehalten, die Wahrscheinlichkeiten einer technischen Ursache oder einer menschlichen Ursache durch eine Fehlbedie-

* Der Autor ist Gesellschafter des Ingenieurbüros Lange + Tenzer in Hannover und Mitglied der Schimmelpfennig + Becke-Gruppe.

nung oder, insbesondere im Fall eines Unfalles, einem Fahrfehler gegenüberzustellen.

Im Folgenden werden die einzelnen Punkte einer Fehleranalyse in der Reihenfolge der Herangehensweise besprochen.

2. Vortrag

Für die Sachverständigenanalyse einer möglichen Fehlfunktion eines Fahrerassistenzsystems ist zunächst ein möglichst **präziser und detaillierter Vortrag des Fehlers** erforderlich. Dieser sollte sich nicht nur auf den Fehler selber beschränken sondern auch die Situation und Häufigkeit des Auftretens und die Folgen beinhalten.

Leitfragen sind:

- In welcher Fahrsituation (Geschwindigkeit, Lenk-, Brems- oder Beschleunigungsverhalten) ist der Fehler aufgetreten und wie oft?
- An welchem geografischen Ort trat der Fehler auf?
- Wie ist der Fehler bemerkt worden (Kontrollleuchte, Fahrzeugverhalten)?
- Ist das Fahrzeug nach Auftreten des Fehlers noch bewegt/genutzt worden, wenn ja, wie oft/lange?
- Ist es im Rahmen der Fehlfunktion zu einem Unfallereignis gekommen? Welche Spuren (auf der Fahrbahn/an anderen Fahrzeugen oder Objekten) konnten dabei gesichert werden?

3. Fehlerspeicher

Der erste Schritt in der Analyse ist das Auslesen des Fehlerspeichers des betroffenen Fahrzeugs. Der **Fehlerspeicher** ist **Teil eines jeden Steuergeräts** moderner Fahrzeuge, die eine OBD-Schnittstelle (OBD = On Board Diagnostics) besitzen. Er speichert die Aufzeichnung von Störungen oder technischen Defekten im Kfz. Dazu prüfen die Steuergeräte die bei ihnen einlaufenden Messwerte auf mögliche Fehler wie bspw. Sensorunterbrechung, Kurzschluss, unplausible Größen oder fehlerhafte Prüfsummen. Abb. 10 zeigt ein Auslesen des Fehlerspeichers über OBD Schnittstelle bei einem Kia Carnival.

Dabei erkannte Fehler werden nichtflüchtig i.d.R. in EEPROMs (EEPROM = Electrically Erasable Programmable Read-Only Memory, wörtlich: elektrisch löschbarer, programmierbarer Nur-Lese-Speicher) gespeichert. Häufig wird ein Zeitstempel oder die Höhe des letzten plausiblen Wertes und einiger Randinformationen gespeichert. Jedes Steuergerät speichert dabei nur seine eigenen Fehler, es existieren in einem Fahrzeug also in Wirklichkeit eine ganze Reihe voneinander unabhängige Fehlerspeicher. Bei den zu speichernden Fehlern wird zwischen statischen und **sporadischen Fehlern** unterschieden. Der Unterschied ist, dass sporadische Fehler automatisch gelöscht werden, wenn sie über eine bestimmte Anzahl (z.B. 50) von Fahrzyklen (Einschalten der Zündung) nicht mehr auftraten. Im Fehlerspeicher werden dazu entsprechend individuell für jeden möglichen Fehler **Fahrzykluszähler** mitgeführt (Quelle: *http://de.wikipedia.org/wiki/Fehlerspeicher*). Wichtig ist somit für eine möglichst umfassende Analyse, dass das betroffene Fahrzeug zeitnah einer Untersuchung durch den Sachverständigen zugeführt wird.

Ist das Fahrzeug durch Gewalteinwirkung ganz oder teilweise zerstört, können die noch erhaltenen Steuergeräte ausgebaut und ausgelesen werden.

Abb. 10 Auslesen des Fehlerspeichers über OBD-Schnittstelle

4. Event Data Recording EDR

Diese juristisch umstrittene Methode der **ereignisbezogenen Datenspeicherung** geht deutlich über die Funktion des Fehlerspeichers hinaus. Eine bekannte Version des EDR ist der Unfalldatenspeicher UDS. Dieser zeichnet mehrkanalig Fahrzeuggeschwindigkeit, Beschleunigungen in der Ebene sowie verschiedene Schaltzustände von Fahr- und Bremslicht, Blinker etc. auf. Die Aufzeichnung erfolgt in einem Ringspeicher, der wieder überschrieben wird. Erst wenn ein bestimmtes Triggerereignis wie bspw. ein Stoß erfolgt, werden die Daten etwa 30 s vor bis 15 s nach diesem Triggerereignis festgeschrieben und können ausgelesen und ausgewertet werden. Die Abb. 11 zeigt eine solche Aufzeichnung eines Pkw/Fußgängerunfalls.

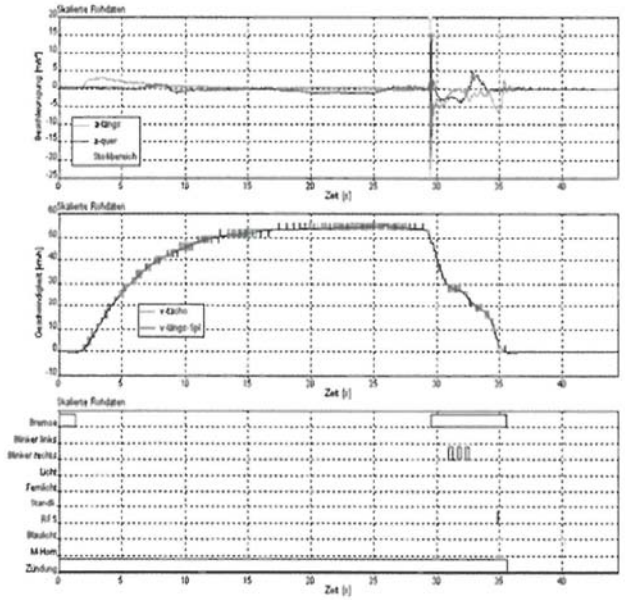

Abb. 11 UDS-Aufzeichnung eines Fußgängerunfalls[1]

Während das UDS als autarkes Gerät mit eigenen Sensoren arbeitet, zeichnet der EDR Teile des CAN-Verkehrs zwischen Sensoren, Steuergeräten und Aktuatoren auf.

Die Grenze zwischen einem Fehlerspeicher und einem EDR ist fließend. Hauptunterscheidungsmerkmal ist,

1 Quelle: *http://www.unfallanalyse.de/unfallgutachten/uds_gutachten/uds_detail_01.html.*

dass der Fehlerspeicher nur das Auftreten des Fehlers für Wartungs- und Reparaturzwecke dokumentieren soll. Ein EDR zeichnet jedoch auch Daten auf, die zeitlich im Umfeld des Auftretens dieses Fehlers erzeugt wurden und den Sachverständigen in die Lage versetzen, die Situation zu rekonstruieren, in der der Fehler aufgetreten ist. Tritt bspw. im Vorfeld eines ESP-Eingriffs keine Lenkaktivität durch den Lenkradwinkelsensor auf, so ist mit großer Wahrscheinlichkeit von einer Fehlfunktion auszugehen. Im Umkehrschluss lässt sich über den Lenkwinkel, die Fahrzeuggeschwindigkeit und Drehzahlunterschiede der Räder der fahrdynamische Zustand des Fahrzeugs rekonstruieren. Wird nun im Rahmen eines Unfallgeschehens von einer Partei ein unberechtigter ESP-Eingriff als auslösendes Moment vorgetragen, so lässt sich dieser Vortrag anhand des fahrdynamischen Zustands des Fahrzeugs bei Unfalleinleitung bestätigen oder widerlegen.

Ein EDR wäre hier also in der Lage, Rechtssicherheit zu schaffen. Leider wird dies nicht immer so gesehen. Datenschützer als auch Automobilhersteller wie Zulieferer wehren sich gegen einen verpflichtenden Einbau. Dies ist aus technischer Sicht insofern unverständlich, da i.d.R. nur die belastende Seite einer solchen Datenspeicherung hervorgehoben wird. Sie hat jedoch auch deutlich entlastenden Charakter. Mithilfe eines EDR ist es dem Kläger in einem zivilen Rechtsstreit häufig erst möglich, eine Fehlfunktion eines Assistenzsystems zu beweisen.

Hierzu hat der Arbeitskreis VII „Die Auswertung von Fahrzeugdaten bei der Unfallanalyse" auf dem 45. Deutschen Verkehrsgerichtstag 2007 empfohlen:

1. In der Betriebsanleitung des Kfz sollte darüber aufgeklärt werden, welche relevanten Daten gespeichert werden und unter welchen Voraussetzungen die Speicherung erfolgt.
2. Daten, die anlässlich eines Verkehrsunfalls gespeichert werden, müssen nachvollziehbar aufgezeichnet werden, sodass eine standardisierte Auswertung möglich ist. Eingriffe der Fahrerassistenzsysteme und Auslösen von Rückhaltesystemen sind zu protokollieren.
3. Die Datenauswertung setzt nach geltendem Recht die Einwilligung des Fahrzeugeigentümers/Fahrers oder eine richterliche Anordnung voraus.
4. Der Serieneinbau eines Speichermoduls für unfallrelevante Daten („Unfallrekorder"), das die vorhandene Sensorik des Fahrzeugs nutzt und deshalb außerordentlich preiswert sein kann (unter 10 € in einfacher Ausführung), sollte gesetzlich vorgeschrieben werden (Quelle: *http://www.versicherung-und-verkehr.de/index.php/5.0.236*).

4. Rekonstruktion des Unfallablaufs und Plausibilitätsprüfung

Ein fehlerhaftes Eingreifen eines Assistenzsystems in den Fahrprozess führt unter bestimmten Randbedingungen zu einem Unfall. Dies gilt insbesondere für **unberechtigte Brems- und Lenkeingriffe**.

Eine weitere Möglichkeit der Verifikation des Vortrags über einen technischen Defekt ist eine ganzheitliche Betrachtung des Fahrvorgangs, bei dem es zur Fehlfunktion gekommen ist. Hierzu sind eine profunde Kenntnis der Funktion des Assistenzsystems und seiner Einwirkdauern und Übersteuerungsmöglichkeiten erforderlich. Weiterhin ist die Kenntnis des Vorfallsortes und der bei dem Unfall gezeichneten Spuren erforderlich.

Der Sachverständige wird das Schadensereignis wie einen klassischen Verkehrsunfall rekonstruieren und ein Toleranzband der Fahr- und Giergeschwindigkeit am vorgetragenen Schadensort angeben. Im Kontext der Unfallörtlichkeit kann dann angegeben werden, ob es sich um einen Fahrfehler mit einer bspw. dem Kurvenradius unangepassten Geschwindigkeit wie bei dem Unfallbeispiel in Abb. 12 handelt.

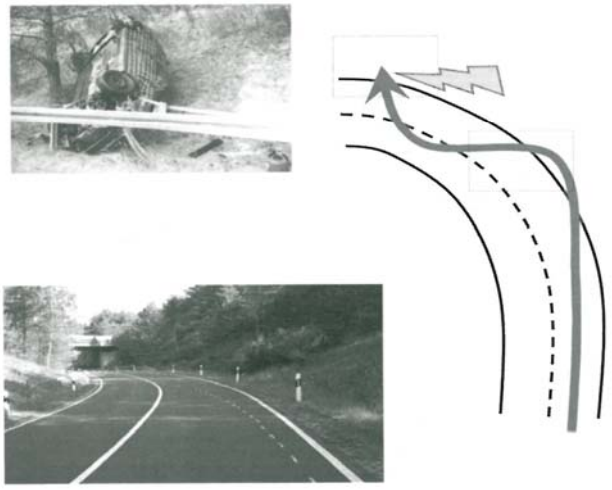

Abb. 12: Fahrunfall durch Fahrerfehler in der Längs- und Querführung[2]

Andererseits ist der Sachverständige in der Lage, einen vorgetragenen Unfallablauf zu simulieren, wenn ihm die Randbedingungen des Vorfalls bekannt sind, oder er sich diese aus dem Kontext des Unfallgeschehens erarbeiten kann. Hierfür bieten sich neben **Fahrdynamiksimulationsprogrammen** auch eine **Unfallrekonstruktionssoftware** wie bspw. PC-Crash an, welche über ein gutes Fahrdynamikmodell verfügt. Abb. 13 zeigt eine Simulation einer ESP-Fehlfunktion, bei der dem unteren Fahrzeug aus einer Geschwindigkeit von 100 km/h auf trockener Straße das linke Hinterrad selektiv bis zum Blockieren abgebremst wurde. Ein lediglich etwa 150 ms dauernder Eingriff führt hier zu einem etwa 4 m langen Blockierspurast. Die Simulation wurde in diesem Falle „open loop" durchgeführt, also ohne einen gegensteuernden Eingriff des Fahrers. Das Fahrzeug bricht nicht, wie möglicherweise erwartet, sofort aus, sondern bleibt auf einem vergleichsweise stabilen Kurs. Der Abstand der Fahrzeugpositionen in Abb. 13 beträgt ca. 1 s.

2 Quelle: Giebel, T., et al. „Current Trends in vehicle active safety and driver assistance development" 24. VDI/VW-Gemeinschaftstagung Integrierte Sicherheit und Fahrerassistenzsysteme, Oktober 2008

Man erkennt anhand der ersten Fahrzeugposition nach dem Blockierspurenast, dass nach Ablauf einer Reaktionszeit der Fahrer durchaus in der Lage gewesen wäre, gegenzulenken. Ein Abkommen von der Fahrbahn ist also nicht zwangsweise die Folge eines solchen ESP-Fehlers.

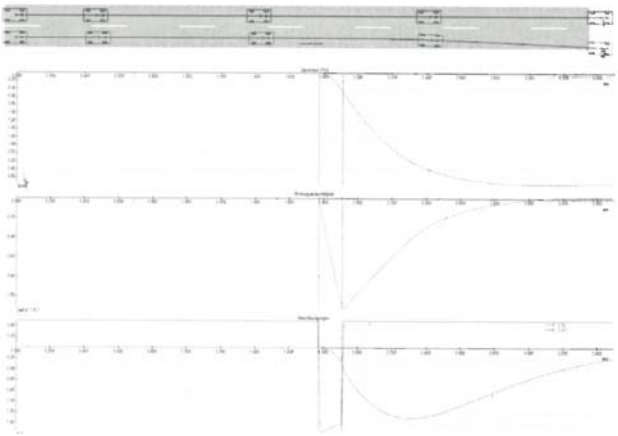

Abb. 13 Simulation eines fehlerhaften ESP-Eingriffs bei 100 km/h mit PC-Crash

6. Hardware-/Software-in-the-Loop

Die letzte Eskalationsstufe bei der Detektion von Fehlern in Fahrerassistenzsystemen ist die Durchführung von Hardware bzw. Software-in-the-loop Tests. Hierbei werden einzelnen Komponenten des Assistenzsystems freigelegt und in einen Hardware-in-the-loop (HiL) Prüfstand eingebaut. Ein HiL-Prüfstand besteht aus folgenden Komponenten (s. Abb. 14):

- Hardware (reales Bauteil)
- Echtzeitfähige Simulationsumgebung
- Ausgabe- und Analyseeinheit

Die Eingangsgrößen werden von einer Simulationsumgebung in Echtzeit zur Verfügung gestellt und an einer Schnittstelle dem realen Bauteil übergeben, das es zu überprüfen gilt. Art und Ausprägung der Signale entsprechen genau denen, wie sie auch im Fahrzeug vorkommen. Die Komponente wiederum erzeugt Stellgrößen, die über eine zweite Schnittstelle dem HiL-Prüfstand zurückgegeben werden, der diese als Eingangsgröße in die Simulationsumgebung leitet. Auf diese Weise entsteht ein **geschlossener Regelkreis** („in the loop"), der eine **realitätsnahe Überprüfung** des Bauteils **im Labor** ermöglicht, die sonst nur in aufwändigen und nicht immer ungefährlichen Fahrversuchen möglich ist. Der weitere Vorteil ist, dass man durch einfache Parametervariation systematisch eine ganze Testreihe des Bauteils durchführen kann, die es erlaubt Fehlfunktionen des Bauteils offenzulegen.

Der Nachteil ist, dass man für die Anwendung dieses Verfahrens das fehlerhafte Bauteil bereits identifiziert haben sollte, da sonst eine kostenintensive Prüfung aller Komponenten des Assistenzsystems erforderlich ist.

Neben der Hardware lässt sich in einer vergleichbaren Versuchsanordnung, nur ohne die Hardwarekomponenten, auch die Software überprüfen. Spätestens hier ist eine intensive Zusammenarbeit mit dem Hersteller erforderlich, da sich der Programmcode im Gegensatz zu den einzelnen Hardwarekomponenten nicht ohne Weiteres extrahieren lässt.

Eine HiL/SiL Überprüfung sollte jedoch aufgrund ihres technischen Aufwands und damit verbundenen Kostenintensität immer die ultima ratio sein, dann, wenn alle anderen Eskalationsstufen durchlaufen wurden und es bereits deutliche Hinweise auf Fehlfunktion des Assistenzsystems gibt.

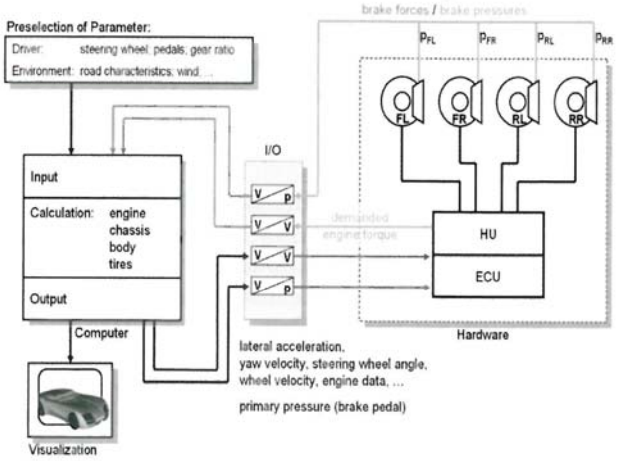

Bild 14: Hardware-in-the Loop Schema

IV. Zusammenfassung

Die zunehmende Einbaurate von Fahrerassistenzsystemen und die Komplexität der Systeme werden Juristen und damit auch Sachverständige zunehmend beschäftigen.

Allen diesen Systemen gemein ist ein Aufbau, bei dem eine Sensorik Kenngrößen von Fahrzeug-, Fahrer- und Verkehrszuständen misst. Diese werden an ein Steuergerät geleitet, in dem ein hinterlegter Programmcode die Signale interpretiert und Steuerbefehle an ein oder mehrere Aktuatoren sendet. Diese Aktuatoren greifen dann bei einigen Assistenzsystemen in die Fahrzeuglenkung, das Bremssystem oder die Drosselklappensteuerung ein. I.d.R. wird ein auftretender Fehler dazu führen, dass das System in einen sicheren Zustand zurückfällt. Mit einer sehr geringen Wahrscheinlichkeit kann ein Fehler dazu führen, dass das Fahrzeug zum Selbstbremser, Selbstlenker oder Selbstbeschleuniger wird.

Um einen solchen Fehler festzustellen und ihn ggf. auch gegenüber einem Fahrfehler des Fahrzeugführers abzugrenzen, ist zunächst einmal ein dezidierter Parteivortrag über Art und Weise des Auftretens des Fehlers und den Kontext der Fahrsituation, in der er aufgetreten ist, hilfreich. In der Folge wird sich der Sachverständige in einer Eskalationsstrategie der Aufklärung des Fehlers nähern, indem er zunächst den Fehlerspeicher des betroffenen Fahrzeugs ausliest und dessen Inhalt analysiert. In diesem Zusammenhang wäre ein Event Data Recording (EDR) äußerst hilfreich,

3 Quelle: *http://www.fahrzeugtechnik-muenchen.de.*

da es nicht nur den Fehler selber aufzeichnet, sondern auch weitere Messgrößen, die es erlauben, die Situation, in der der Fehler aufgetreten ist, zu rekapitulieren. Bedauerlicherweise sind bislang nur eine sehr geringe Anzahl von Fahrzeugen mit einem EDR ausgerüstet.

Mit Kenntnis des Parteivortrags und den Informationen über den Fehlerspeicher kann der Sachverständige die Situation nachbilden, in der der Fehler aufgetreten ist und so i.d.R. unterscheiden, ob es sich hierbei um einen Fahrfehler oder um einen Systemfehler des Assistenzsystems handelt. Abschließend besteht die (kostenintensive) Möglichkeit, einzelne Komponenten eines Assistenzsytems in einem Hardware-in-the-Loop Test auf Fehlfunktionen zu prüfen.