

Zuverlässige Systemidentifikation moderner Kraftfahrzeugarchitekturen

Dipl.-Ing. Michael Grimm, IVK - Universität Stuttgart;
Prof. Dr.-Ing. Hans-Christian Reuss, IVK - Universität Stuttgart;

Kurzfassung

Mit der Anzahl der elektronischen Systeme im Kraftfahrzeug und ihrem Variantenreichtum steigt die Fehlerwahrscheinlichkeit des Gesamtsystems überproportional an. Insbesondere fehlende Wartung, Manipulation und nicht fachgerechte Instandsetzung verschärfen diese Problematik bei Kraftfahrzeugen. Von besonderer Bedeutung ist hierbei der Trend, mechanische Komponenten in sicherheitsrelevanten Systemen, wie der Lenkung, durch elektronische Komponenten zu ersetzen. Die am öffentlichen Straßenverkehr teilnehmenden Fahrzeuge befinden sich teilweise in einem nicht verkehrssicheren Zustand. Heutige Prüf- und Überwachungsverfahren stoßen bereits bei bestehenden Elektronikarchitekturen an ihre Grenzen und können die Systemintegrität nicht feststellen, obwohl sie gesetzlich dazu verpflichtet sind.

Um diesen Zustand künftig zu verlassen wurde das Verfahren der erweiterten Integritätsprüfung, im Rahmen einer Promotion, am Institut für Verbrennungsmotoren und Kraftfahrwesen der Universität Stuttgart entwickelt. Mit dem Verfahren ist man in der Lage, das elektronische Gesamtsystem qualitativ und quantitativ zweifelsfrei zu identifizieren und bezüglich seiner Integrität zu bewerten.

Nach der Definition des sicheren und integeren Zustandes von elektronischen Kfz – Systemen wird im Rahmen dieses Beitrages das Verfahren einer erweiterten Integritätsprüfung vorgestellt. Es wird die Frage beantwortet, welche Eigenschaften einer Elektronikarchitektur zu überprüfen sind, um eine eindeutige Prüfaussage bezüglich der Integrität des Gesamtsystems ermitteln zu können. Die beiden Kernthemen der erweiterten Integritätsprüfung, der Lebendtest und der Manipulationsschutz, werden detailliert vorgestellt. Der Lebendtest ist Teil der erweiterten Integritätsprüfung und stellt die Anwesenheit der Einzelkomponenten, auch bei verteilter Software, fest. Identifikationsverfahren aus der Informationstechnik erlauben, mit den Methoden der Diagnose, die Integration aller Subsysteme mit deren Regelkreisen. Signalbasierte und modellgestützte Diagnosefunktionen erhöhen die Prüftiefe und erlauben die Integration

von den elektrischen, elektronischen und mechanischen Bereichen eines Regelkreises. Damit ist die Funktionalität eines Systems erfassbar.

Ist ein Prüfergebnis unter Ausnutzung fahrzeugeigener Infrastruktur erzeugt worden, muss die Integrität des Ergebnisses sichergestellt werden. Der Manipulationsschutz der erweiterten Integritätsprüfung stellt dies mit modernen Verschlüsselungen unter Berücksichtigung der Kommunikationsmedien, dem Implementierungsaufwand und dem Aspekt der Praxistauglichkeit sicher. Die Referenzdatenhaltung und die Fahrzeug-Tester-Kommunikation spielen bei der Feststellung der Integrität eine wichtige Rolle und werden heute nicht entsprechend berücksichtigt. Die notwendigen technischen Maßnahmen werden im Kontext des ganzheitlichen mechatronischen Kfz – Systems erläutert.

Neben der gesteigerten Verkehrssicherheit entstehen durch die Anwendung der erweiterten Integritätsprüfung Vorteile, wie die Verbesserung der Kontrolle des Herstellers über das Produkt seines Zulieferers, eine Stärkung des Kundenvertrauens im Gebrauchtfahrzeughandel durch Manipulationssicherheit oder die Steigerung der Erfolgsquote von Rückrufaktionen.

Abstract

With the growing number of electronic subsystems and their numerous versions built in a motor vehicle the error margin of the entire system is increasing. In particular missing maintenance, manipulation or non-professional corrective maintenance contributes to the decline of safety and security in road traffic. The trend to introduce electronics in security relevant systems such as steering and braking systems underlines the importance of error-free electronics and their continuous safety. According to the present state of technology it cannot be proven that a motor vehicle is secure or not. Even the term 'safety' allows interpretation and therefore a new definition is required for this work.

The motor vehicles that are part of the public road traffic might therefore not be in a roadworthy condition. In order to address this problem the method of the extended integrity check was developed in the context of a dissertation at the Institute of Combustion Engines and Automotive Engineering (IVK) at the University of Stuttgart.

With the extended integrity check a method will be introduced, which identifies the condition of electronic motor vehicles systems in a practicable, doubtless and tamper-proof way. For this the relevant elements of vehicle diagnosis, encryption of electronic data and internal motor vehicle communication are introduced. The existing E/E - infrastructure of a vehicle will be checked as well as the existing software regarding the

diagnosis and the self diagnosis of a motor vehicle. Particular attention will be given to the fact, that both the check itself and the results of the check will be transmitted tamper-proof from the inspection report of the vehicle to the tester. Fundamentally new is the approach to combine available methods of automobile mechatronics and computer science in a way, that the resulting tamper-proof method is suited for the everyday life of motor vehicle evaluation.

An agreement between the legislator, the motor companies and the technical supervisory association to test motor vehicles according to the guidelines of the extended integrity check would come as a big step in advancing road safety and security. The method introduced could be part of the mandatory main technical check up. Before an implementation of the extended integrity check however a considerable standardization effort concerning the content, the encoding methods, the provision of reference value and the inspection process would be necessary.

1. Motivation

Das elektronische Stabilitätsprogramm ESP gehört bei knapp der Hälfte aller in Deutschland erhältlichen Fahrzeugmodelle zum Serienstandard. Bei 58 Prozent der Autos ist laut [1] der elektronische „Schleuderverhinderer“ serienmäßig an Bord.

Bei Störungen oder Ausfällen dieser Systeme sind Fahrzeugführer schnell überfordert. Fehlermeldungen werden durch Unwissenheit oder Überheblichkeit nach dem Motto „Das System wird schon funktionieren“ oft nicht beachtet oder sogar absichtlich ignoriert. Dies verdeutlicht folgender Unfallbericht [2]:

„Die Daten zum Unfallhergang: Autobahn HH - Berlin, kurz vor der Auffahrt Kremmen. Meine Geschwindigkeit: ca. 200 km/h (vom Sachverst. ermittelt) war aber etwas höher. Gegner: LKW mit Anhänger, Geschwindigkeit lt. Tachoscheibe ca. 83 kmh. LKW zog ohne Vorwarnung oder Anzeige kurz vor der Einmündung auf die linke Spur. 87m Blockierspur (ABS hat nämlich den Dienst versagt) dann Buff. Differenzgeschwindigkeit ca. 60 - 70 km/h!!! Die defekten Teile für das ABS System hatte ich schon gekauft, aber eben noch nicht eingebaut. ... Daher vielleicht eine Warnung an eigentlich alle, die ABS haben: Wenn bei höheren Geschwindigkeiten die gelbe ABS-Lampe leuchtet, der Störung sofort nachgehen.“

Es ist festzustellen, dass die elektronischen Helfer in ihrer Wirkung oft unterschätzt oder das eigene Können oft überschätzt wird, Teile aus dem privaten Teilemarkt nicht fachmännisch verbaut werden und defekte elektronische Systeme im öffentlichen Straßenverkehr anzutreffen sind.