



Das Auto als forensischer Datenspeicher – Technische Hilfsmittel und Möglichkeiten einer forensischen Auswertung von Kfz-Elektroniksystemen

Heiko Polster

Forensic Science Investigation Lab, Hochschule Mittweida – University of Applied Sciences, D-09648 Mittweida, heiko.polster@hs-mittweida.de

Dirk Labudde

Fraunhofer SIT Darmstadt, Rheinstraße 75, D-64295 Darmstadt, dirk.labudde@hs-mittweida.de

1	Einleitung.....	271
2	Grundstruktur der Kfz-Elektronik, Versuchsaufbau	271
3	Tools zum Auslesen von klassischen Kraftfahrzeugen	274
4	Diagnose aktueller Kraftfahrzeuge	278
5	Verwendung von ermittelbaren Daten aus klassischen Kraftfahrzeugen.....	279
6	Diskussion / Zusammenfassung	284
7	Literaturverzeichnis	285

Abstract:

Heutige Kraftfahrzeuge beinhalten eine große Anzahl an elektronischen Komponenten. Die Steuergeräte sind sowohl intern miteinander über Bussysteme als auch extern vernetzt. In diesen Steuergeräten werden eine Vielzahl an Daten gespeichert, die aus Ermittlersicht zur Aufklärung von Unfällen oder sogar Straftaten herangezogen werden können. In diesem Paper wird die Akquise von Daten aus Kraftfahrzeugen anhand ausgewählter Beispiele dargestellt. Es werden neben der grundlegenden Architektur der in Kraftfahrzeugen verbauten Bus-Systeme verschiedene technische Hilfsmittel aufgezeigt, die zur Datenextraktion Verwendung finden können. Eine besondere Rolle spielen extrahierbare Fehlermeldungen in Steuergeräten, wobei diese Daten via On-Board-Diagnose oder auch direkt aus Steuergeräten auslesbar sind. Es wird dargestellt, welche Informationen diese Fehlermeldungen beinhalten und wie diese für Ermittler verwendbar sind. Im weiteren Verlauf wird dargestellt, wie aus Schlüsseltranspondern Informationen gewonnen werden können, sodass diese Daten mit anderen forensischen Informationen verknüpfbar sind. Ein weiteres Ziel des Papers ist die Darstellung der Analyse von Infotainmentsystemen, die unter anderem Positionsdaten, gespeicherte Routen, Telefondaten oder auch genaue Abstellorte eines Fahrzeugs zu einem definierten Zeitpunkt beinhalten können.

JEL Classification: C83, C88, C93, I23, L62, Y5, Y50

Keywords: Car-Forensik, Kraftfahrzeug-Datenextraktion, forensische Werkzeuge.

1 Einleitung

Der digitale Wandel hat das Kraftfahrzeug von einem isoliert zu betrachtenden Fortbewegungsmittel zu einem unablässig mit seiner Umwelt kommunizierendem System verändert. Dank der Vernetzung von Fahrzeugfunktionen (Antrieb, Lenkung, Bremsen, Komfort und Infotainment) durch Bussysteme sowie der Kommunikation des Fahrzeugs mit seiner Umgebung durch Mobilfunk, eCall oder Car2X sind Fahrzeuge heute effizienter, komfortabler und sicherer geworden. Ein modernes Fahrzeug besteht dabei heute aus ca. 100 Millionen Zeilen Programmcode [Kfz-Betrieb Vogel (2019)], verteilt auf mindestens 50 verbaute Steuergeräte. In der Statistik aus [Statista (2021)] wird ein prognostizierter Anteil an vernetzten Kraftfahrzeugen in den USA, China und der Europäischen Union bis in das Jahr 2035 dargestellt. So werden im Jahr 2035 in der Europäischen Union etwa 72 % der Kraftfahrzeuge vernetzt sein.

In [JUNIPER (2018)] wird dargestellt, dass es im Jahr 2023 Schätzungen zufolge 775 Millionen vernetzte Fahrzeuge geben wird, die mittels fahrzeugeigener Telematik oder über eine Smartphone-App verbunden sind. Diese stark steigende Zahl vernetzter Fahrzeuge gepaart mit der ständigen Erweiterung um neue Schnittstellen mit der Umwelt eröffnet die Möglichkeit, dass Unbefugte das System des vernetzten Fahrzeugs kompromittieren.

In den zahlreichen Software-Komponenten vernetzter Fahrzeuge finden Sicherheitsforscher immer wieder Schwachstellen. So lassen sich die meisten Softwarefehler in Mobilfunk-Anbindungen sowie in Ortungs- oder Notrufsystemen aufzeigen mithilfe derer in Infotainmentsysteme eingedrungen werden kann, um anschließend die Steuerelektronik zu kompromittieren. Teilweise ist es für die Funktionalität der Komfortanwendungen im Fahrzeug aber notwendig, Fahrzeugdaten an das Infotainmentsystem zu senden. Hier ist es wichtig, den Datenfluss in die andere Richtung zu unterbinden, um eine Kompromittierung der Steuerelektronik zu verhindern. [IEEE (2010)], [KASPERSKY (2015)], [INGENIEUR.DE (2015)]

Diese Arbeit befasst sich mit Techniken und Methoden, um Daten aus Kraftfahrzeugen und deren Steuergeräten extrahieren zu können. Es wird an Beispielen dargestellt, wie man diese Daten interpretieren kann, um forensische Informationen zu erhalten.

2 Grundstruktur der Kfz-Elektronik, Versuchsaufbau

2.1 Grundstruktur der Kraftfahrzeug-Elektronik und Datenquellen

Ausgehend von der Grundstruktur der Elektronik in Kraftfahrzeugen können verschiedene Steuergeräte im Fahrzeug oder auch Schlüssel zur Untersuchung herangezogen werden. Aus Steuergeräten ist eine Datenextraktion möglich, da diverse Daten

elektronisch gespeichert sind. Abbildung 1 zeigt exemplarisch die klassische Grundstruktur der On-Board-Elektronik eines Kraftfahrzeugs.

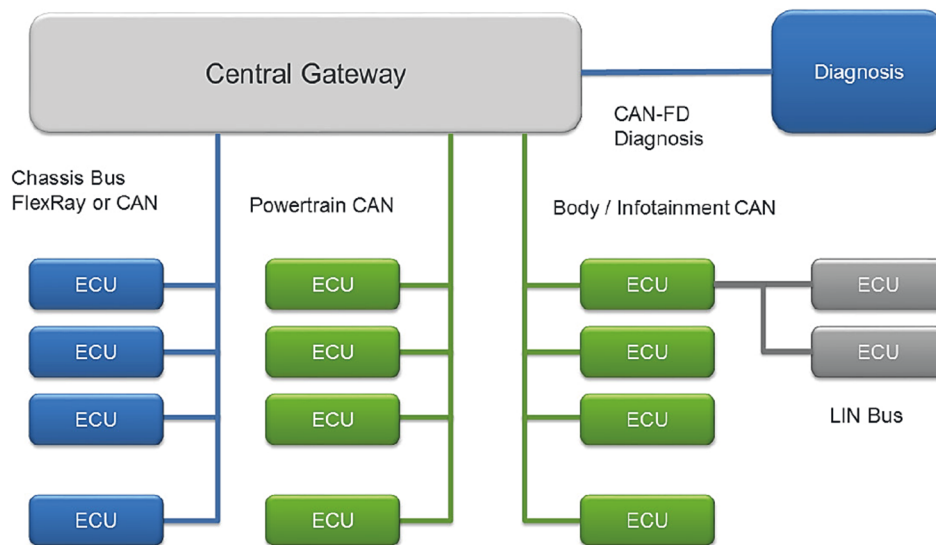


Abbildung 1: Grundstruktur Kraftfahrzeug-On-Board-Elektronik eines Kraftfahrzeugs

Quelle: Lieder, 2017

Wichtigstes Element der On-Board-Elektronik ist das zentrale Gateway, an dem alle Bus-Systeme angeschlossen sind. Das zentrale Gateway selbst übersetzt elektronische Informationen von einem System in andere Bus-Systeme. Dies ist notwendig, um beispielsweise Daten zur gefahrenen Wegstrecke vom zugehörigen Sensor an das Navigationssystem zu übermitteln. Die Daten werden dabei von einem CAN-System über das Gateway an das Multimediasystem gesendet. Je nach Ausstattung des Fahrzeugs können mehrere CAN-Bus-Systeme (CAN: Controller Area Network), z. B. Antriebs-CAN, Komfort-CAN, Diagnose-CAN, Abstands-CAN, FlexRay oder auch der Infotainment Bus (MOST: Media Oriented Systems Transport) verbaut sein. Zusätzlich zum CAN-Bus ist der Einsatz eines weiteren Subbussystems möglich, das als LIN (Local Interconnect Network) ausgeführt ist und für einfache Sensor- Aktor-Anwendungen Verwendung findet.

In den einzelnen Steuergeräten ist ein Speicher integriert, in dem Fehlermeldungen zu auftretenden Störungen während des Betriebs abgelegt werden. Diese Meldungen werden auch als Diagnostic Trouble Codes bezeichnet und helfen in der Werkstatt, Defekte schnell erkennen und beheben zu können. Aus diesen Daten können Informationen zu Fehlern selbst, als auch Umgebungsinformationen, z. B. Zeitpunkt des Auftretens, Kilometerstand, Umgebungstemperaturen etc., gewonnen werden.

Aktuellere Kraftfahrzeuge beinhalten zusätzlich Automotive Ethernet als Bus-Komponente, wobei sich die Struktur der On-Board-Elektronik wie in Abbildung 2 darstellt.

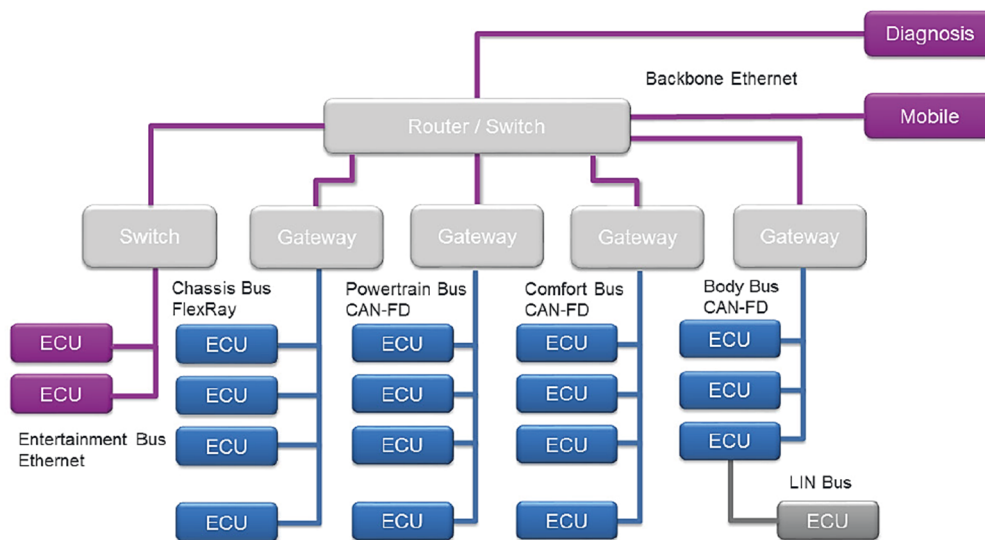


Abbildung 2: Struktur der On-Board-Elektronik mit Automotive Ethernet

Quelle: Lieder, 2017

Das zentrale Gateway ist durch einen Backbone-Router ersetzt. Dieser verteilt die Nachrichten an Domänen-Gateways, an denen klassische Fahrzeugbussysteme angeschlossen sind. Gemeinsam haben beide Systeme, dass jeweils ein Diagnoseinterface zur Verfügung steht. Dieses ist bei klassischen Kraftfahrzeugen der Diagnose-CAN und in aktuellen Fahrzeugen ab ca. 2017 als Ethernet-Verbindung realisiert.

2.2 Versuchsaufbauten zur Datenextraktion

In einigen Fällen ist es notwendig, einzelne Steuergeräte auszulesen. Dies können Motorsteuergeräte, Wegfahrsperrern etc. sein. Prinzipiell eignen sich dazu die in Abschnitt 3 vorgestellten Tools. Zum exemplarischen Auslesen einzelner Steuergeräte wurde ein Board realisiert, das mit den relevanten Kommunikationsanschlüssen OBD-2, CAN-Leitungen, K-Line sowie Masse und Bordspannung ausgestattet war.

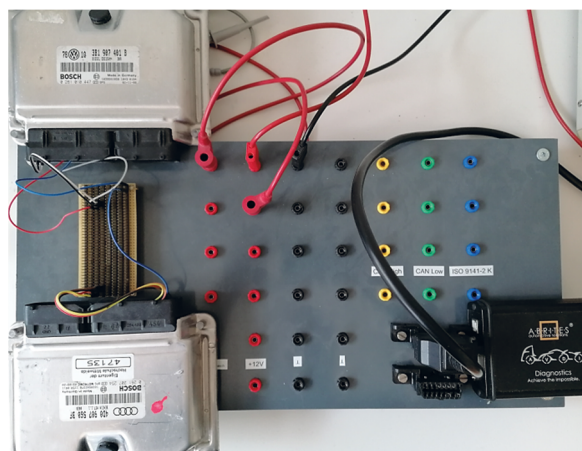


Abbildung 3: Versuchsboard zum Auslesen einzelner Steuergeräte

Quelle: Eigene Abbildung

An diese Anschlüsse wurden verschiedene Steuergeräte aus klassischen Fahrzeugen angeschlossen. Dies waren das EDC15-Diesel-Motorsteuergerät, ein ME7-Benzin-Motorsteuergerät mit jeweils einem K-Line-Diagnoseinterface sowie ein Car Access-System CAS3 von BMW mit Can-Interface.

Zum exemplarischen Auslesen der Diagnoseinformationen eines Kraftfahrzeugs wurde ein Ford Focus mk3 aus dem Baujahr 2011 verwendet.

3 Tools zum Auslesen von klassischen Kraftfahrzeugen

Die Datenextraktion in Form von Fehlermeldungen aus einem kompletten Kraftfahrzeug ist über das Diagnoseinterface möglich, das als OBD-2 (On-Board-Diagnose) in jedem Kraftfahrzeug verbaut ist, wobei in den Normen SAE J2012 und der ISO-Norm 15031 die Fehlercodes für OBD-2 spezifiziert sind. An dieses Interface können diverse Diagnosetools angeschlossen werden.

Zur OBD-2-Diagnose können kommerzielle Tools, wie z. B. Werkstatttester, aber auch Tools von Drittanbietern, z. B. VAGdashCAN, EDIABAS oder das Abrites Vehicle Diagnostic Interface Verwendung finden.

3.1 Werkstatttester

Eine der zahlreich verfügbaren Werkstatttester ist das Diagnosesystem Bosch KTS 980 [Bosch (2021)].



Abbildung 4: Bosch KTS 980 Diagnosesystem mit Kfz-Interface und Notebook

Quelle: Bosch, 2021

Dieses System ermöglicht die Kommunikation über OBD-2 mit den Protokollen ISO 15031, ISO 22900, SAE J2534-1 und -2 (PassThru), ISO 9141-2 (K und L), SAE J1850 VPW und PWM, CAN High Speed ISO 11898, ISO 15765-4 (OBD), CAN Single Wire, CAN Low Speed, ISO 13400 (Diagnose über IP).

3.2 VAGdashCAN

VAG-Kraftfahrzeuge können beispielsweise mit VAGdashCAN diagnostiziert werden, wobei u. a. aber auch die Anpassung oder Wiederherstellung des km-Standes vorgenommen werden kann. Weiterhin gibt es eine Schlüsselanlernfunktion sowie die Möglichkeit, Tachos über die Typenklassen hinweg anzulernen. Es gibt einen vollständigen Zugriff auf den EEPROM (Variablen- und Parameterspeicher) von EDC15-Diesel-Steuergeräten, sowie ME7-Benzin-Motorsteuergeräten. Sämtliche Programmfunktionen sind über die OBD2-Buchse realisierbar.

3.3 EDIABAS

Speziell für BMW-Kraftfahrzeuge kann das Tool Set EDIABAS verwendet werden. Mit EDIABAS ist es möglich, die Diagnose über K-Line und CAN durchzuführen. Weitere Funktionen sind der Start der Regeneration des Dieselpartikelfilters, das Auslesen von Fehlerspeichern aus Steuergeräten, VIN-Änderung vorzunehmen, Batteriewechsel zu registrieren, und Schlüssel im CAR-Access-System zu sperren bzw. zu entsperren.

3.4 Abrites Vehicle Diagnostic Interface (AVDI)

Als herstellerübergreifendes Diagnosetool wird von ABRITES das Vehicle Diagnostic Interface (AVDI) angeboten [ABRITES (2021)].

Das Tool Set unterstützt eine Vielzahl an Herstellern zur Diagnose entsprechender Kraftfahrzeug-Modelle per K-Line ISO 9141 [ISO9141] oder auch CAN-Bus nach ISO14229 [ISO14229], ISO15765 [ISO15765], J1939 [J1939] und ISO22901 [ISO22901]. AVDI kann u. a. Motorsteuergeräte für viele Marken und Modelle anpassen und umprogrammieren, Getriebesteuergeräte für die gängigsten Mercedes, VW, Audi, Seat und Skoda Fahrzeuge kodieren. Zusätzlich kann man EDC15, EDC16 und EDC17 Steuergeräte anpassen sowie programmieren, elektronische Zündschlosssysteme bei vielen Mercedes Fahrzeugen anpassen und programmieren, Wegfahrsperren für Opel, VW, Audi, Seat, Skoda, BMW u.v.a. programmieren sowie Fehlercodes der meisten Marken und Modelle auslesen.

3.5 Bluetooth OBD-Dongle

Durch den Privatanwender können zur Fahrzeugdiagnose im Internet verschiedene OBD-Bluetooth-Adapter erworben werden. Diese basieren zum großen Teil auf dem OBD2-Interpreterchip ELM327. [Elmelectronis (2021)] Dieser Chip beinhaltet u. a. die Kommunikation per CAN mit 11 Bit und 29 Bit IDs und unterstützt die Protokolle ISO 15765-4 mit 500 kbps und 250 kbps.



Abbildung 5: Beispielhafte Darstellung eines handelsüblichen OBD Dongle

Quelle: OBDII, 2021

Diese Adapter können mit entsprechenden Android-Apps kommunizieren, um beispielsweise aktuelle Daten zu Geschwindigkeit, Beschleunigung, Kühlwassertemperatur etc. im Livebetrieb anzeigen zu können. Mit der Carly App kann das eigene Fahrzeug diagnostiziert werden, oder auch ein Tachometerbetrug an Gebrauchtfahrzeugen aufgedeckt werden [MYCARLY (2021)].

3.6 Tool zum Auslesen von Infotainmentsystemen

Zur forensischen Datenextraktion aus Infotainmentsystemen ist Spezialhardware und Software notwendig. Die Firma Berla stellt dazu das Forensik-Tool für Fahrzeugsysteme iVe kostenpflichtig zur Verfügung. Derzeit werden Infotainmentsysteme von BMW, Chevrolet, Chrysler, Fiat, Ford, Jeep, Maserati, Pontiac, Toyota und Volkswagen unterstützt. Das Auslesen der Daten erfolgt am ausgebauten System per USB oder JTAG (Joint Test Action Group, IEEE-Standard 1149.1). Daten können logisch oder physikalisch extrahiert werden. In Abhängigkeit des Infotainmentsystems können Daten zu Applikationen, Verbindungen, Geräten, Events und Navigation ermittelt werden. In Bezug auf die aktive Nutzung des jeweiligen Systems sind Verbindungsdaten von Smartphones, z. B. Bluetoothadressen, Gerätenamen, Gerätehersteller, Kontaktdaten, Anruflisten, Nachrichten, Kalendereinträge sowie Navigationsdaten mit letzten Zielen, gespeicherten Favoriten und abgefahrenen Routen auslesbar.

3.7 Chip-Off

In einigen Fällen sind Steuergeräte durch Defekte nicht mehr über eine elektronische Kommunikation ansprechbar. An dieser Stelle kann der Versuch unternommen werden, Speicherchips aus der Platine zu entnehmen, um anschließend mithilfe eines Lesegeräts die enthaltenen Daten zu extrahieren. Exemplarisch wird an dieser Stelle auf das Reworksystem ERSA IR 500 [KURTZERSA (2021)] und das Lesegerät GALEP der Firma Conitec [CONITEC (2021)] verwiesen.

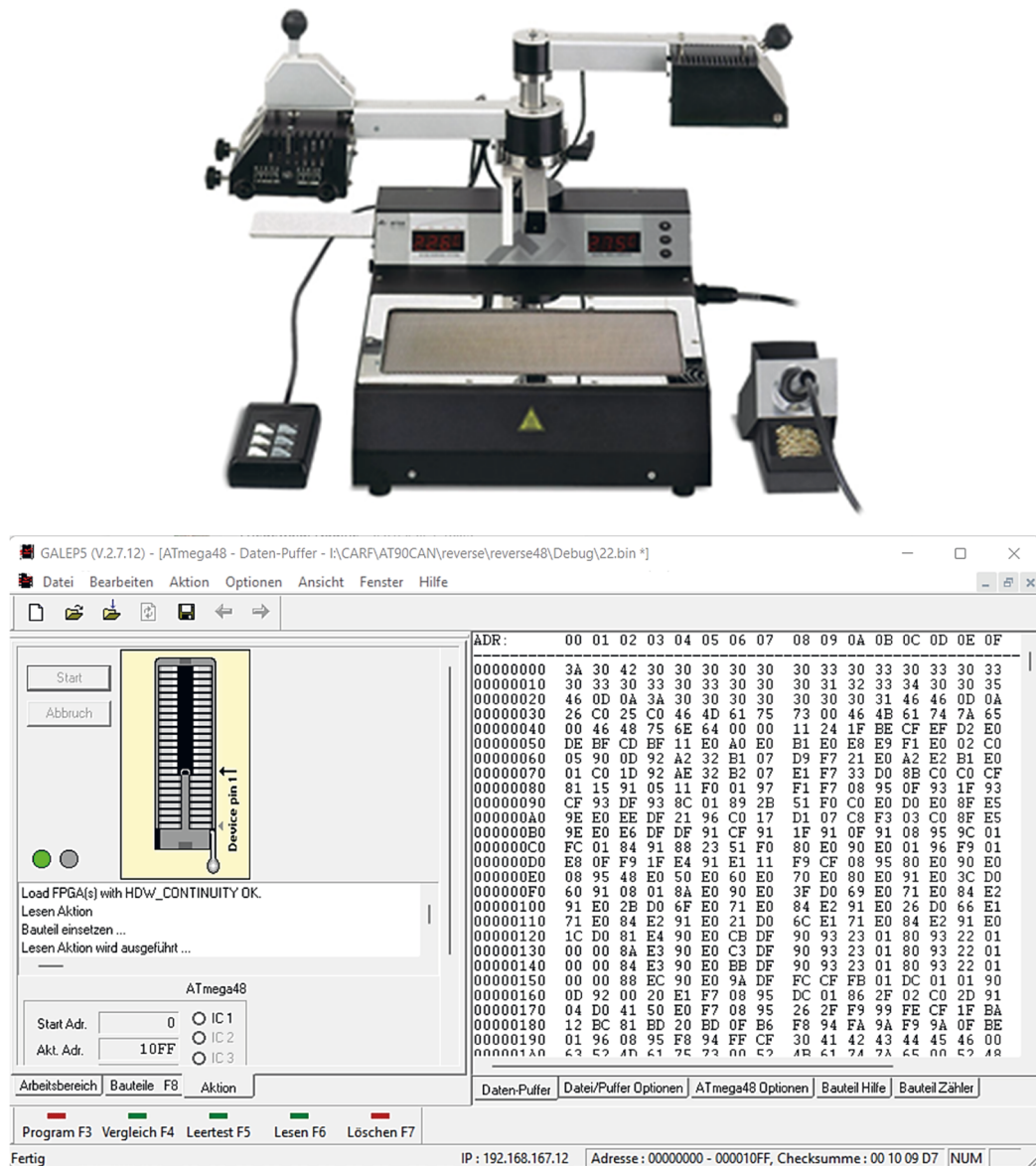


Abbildung 6: ERS IR 500 (Quelle: KURTZER, 2021) und Software GALEP-Programmer mit ausgelesenen Daten (Quelle: Eigene Abbildung)

Mithilfe des Rework-Systems können Chips selektiv aus Elektronikplatinen entfernt werden. Das GALEP-System unterstützt derzeit mehr als 62.000 Bauteile verschiedener Hersteller. Es können u. a. EPROM, EEPROM, FLASH, FPGA und auch Speicher aus unterschiedlichsten Mikrocontrollern gelesen werden.

3.8 Tool zum Auslesen von Kraftfahrzeug-Schlüsseln

Kontaktlose Schlüssel für Fahrzeuge sind Teil moderner Fahrzeugausrüstung. Sie unterstützen die Sicherung des Fahrzeugs gegenüber Zugang vor Fremden. In diesen Schlüsseln ist ein passiver RFID-Transponder (RFID: Radio Frequency Identification) integriert, der über ein Nahfeld per Funk mit dem Wegfahrsperrensteuergerät

kommuniziert. Unter passiven Transpondern versteht man Systeme, die zur Kommunikation und zur Abarbeitung interner Prozesse benötigte Energie ausschließlich aus dem Feld der Sende-Empfangseinheit beziehen. Passive Transponder benötigen keine eigene Stromversorgung, können daher nur auf kurze Distanzen arbeiten. Verwendete Frequenzbereiche sind 125–134 kHz, 13,56 MHz, 433 MHz und 850–950 MHz. Diese Transponder besitzen teilweise Userdatenspeicherbereiche, in denen die Fahrzeugidentifikationsnummer, Kilometerstände und Wartungsdaten abgelegt sein können. Zum Auslesen von Transponderdaten sind eine Reihe an Lesegeräten verfügbar. Exemplarisch soll an dieser Stelle der Tango-Programmer vorgestellt werden.



Abbildung 7: Hardware des Tango Key Programmers
Quelle: Eigene Abbildung

Dieser Programmer ist mit einer proprietären Grundsoftware ausgestattet, die es ermöglicht, Inhalte aus den Transpondertypen MEGAMOS, PCF79XX, TEMIC und TIRIS zu lesen. Unterstützte Krypto-Algorithmen sind HITAG, HITAG2, HITAG3 und weitere. Mit zusätzlichen käuflichen Optionen ist der User in der Lage, Key Marker zu erwerben, mit denen Schlüsseltransponder verschiedener Hersteller kopiert und vervielfältigt werden können.

4 Diagnose aktueller Kraftfahrzeuge

Aktuelle Kraftfahrzeuge werden immer häufiger mit zusätzlichen Komfort- und Assistenzsystemen ausgestattet. Damit steigt aber auch die Gefahr, offen gegenüber Hackerangriffen, beispielsweise über das OBD-2-Diagnose-Interface des Fahrzeugs, ausgeliefert zu sein. Aus diesem Grund setzen immer mehr Hersteller ab ca. 2017 Security Gateways ein, um unautorisierte Zugriffe via Diagnoseinterface zu unterbinden [AUTOSEVICEPRAXIS (2020)], [AUTOSEVICEPRAXIS (2021)], [HERTH&BUSS (2021)]. Die Kommunikation mit Steuergeräten über das Diagnoseinterface wird erst nach Öffnen der Verbindung per Zertifikat, Token oder Keys bzw. Seed-und-Key-Verfahren ermöglicht. Zusätzlich ist eine Verbindung des Testequipments zum Hersteller-IT-Backend notwendig. Hersteller, die solche

Security Gateways einsetzen, sind unter anderem Fiat Chrysler Automobiles N.V., Mercedes-Benz, Renault, Nissan, Audi und Volkswagen. Durch Drittanbieter werden schon jetzt verschiedene Diagnosesysteme angeboten, die dies kostenpflichtig auch ohne herstellerspezifisches Equipment ermöglichen. Vertreter sind beispielsweise die Diagnose on Demand VCI (Vehicle Communication Interface) [HERTH&BUSS (DoD)] von HERT+BUSS oder auch das Euro5/6 Diagnose- und Flash-Tool (EuroDFT) [ADIS] der Firma ADIS Technology.

5 Verwendung von ermittelbaren Daten aus klassischen Kraftfahrzeugen

5.1 Daten aus Kraftfahrzeug-Schlüsseln

Mit Daten aus Kraftfahrzeug-Schlüsseln lässt sich beispielsweise ein vorgetäuschter Diebstahl ermitteln. Eine ausführliche Vorgehensweise ist in [GÖTH (2017)] Seite 3 ff dargestellt. Wie in Abschnitt 3.8 erläutert, werden in Schlüsseltranspondern Großteils Wegstrecken bei letzter Benutzung gespeichert.

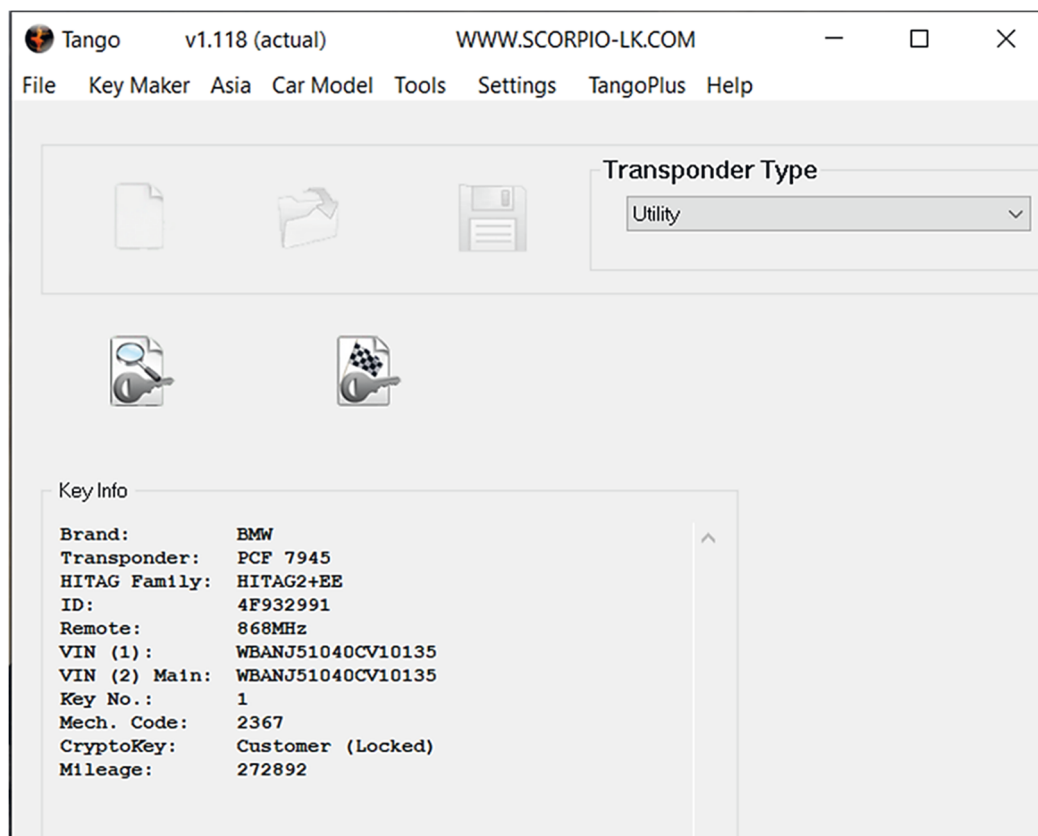


Abbildung 8: Daten eines BMW-Transponders

Quelle: Eigene Abbildung

Wenn die Kilometerangaben in den Originalschlüsseln des zugehörigen Kraftfahrzeugs bei Wiederauffinden des Fahrzeugs übereinstimmen bzw. nah beieinanderliegen, kann davon ausgegangen werden, dass das Kraftfahrzeug mit dem Originalschlüssel bewegt wurde.

In einem Fall aus der Schweiz [Feusi (2019)] wird ein vorgetäuschter Kraftfahrzeug-Diebstahl beschrieben, bei dem Daten aus Schlüsseltranspondern in Bezug auf Zeitstempel zur Aufklärung der Vortäuschung führte, indem festgestellt wurde, dass der Täter das Kraftfahrzeug mit einem Drittschlüssel benutzt hat.

5.2 Daten aus Infotainmentsystem

Aus einem realeren Fall wurde bekannt, dass bei einer allgemeinen Verkehrskontrolle ein Kraftfahrzeug mit auffälligen Insassen überprüft wurde. Im Fahrzeug befand sich augenscheinlich Diebesgut. Die Insassen führten keine Smartphones oder andere elektronischen Kommunikationssysteme mit. Im Kraftfahrzeug war ein Infotainmentsystem verbaut. Dieses Infotainmentsystem konnte mithilfe des in Abschnitt 5 beschriebenen Berla-Systems ausgewertet werden.

Date/Time	Bearing	TrackName	Distance	Latitude	Longitude
21.11.2015 07:54:00	18°	Recovered0057	5,65 m	50,143650000	8,555770000
21.11.2015 07:54:01	18°	Recovered0057	11,31 m	50,143670000	8,555830000
21.11.2015 07:54:02	26°	Recovered0057	11,98 m	50,143700000	8,555890000
21.11.2015 07:54:03	23°	Recovered0057	13,61 m	50,143730000	8,555960000

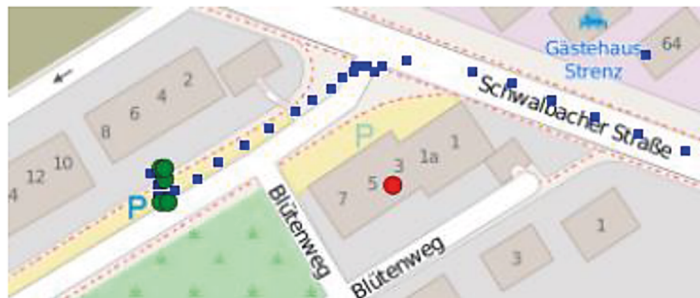


Abbildung 9: Abgefahrte Routen ermittelt mit Berla iVe

Quelle: Born, 2016

Im Navigationssystem wurden unwissentlich Routen geloggt, aus denen abgefahrte Routen und längere Standzeiten des Fahrzeugs ermittelt werden konnten. An diesen ermittelten Aufenthaltsorten konnten die Beamten Diebesgutlager entdecken und somit weitere Straftaten nachweisen.

5.3 Daten aus Fehlermeldungen

Daten aus einem Park Distance Control Fehler

Aus Daten, die in Fehlermeldungen als Umgebungsbedingungen gespeichert sind, lassen sich Zuordnungen zu Zeit, Kilometerstand und Temperaturen im und außerhalb des Fahrzeugs treffen. In Abbildung 10 ist ein Park Distance Control (PDC) Fehler dargestellt, der aus einem Ford Focus mk3 mithilfe des Tools AVDI von Abrites ausgelesen wurde.

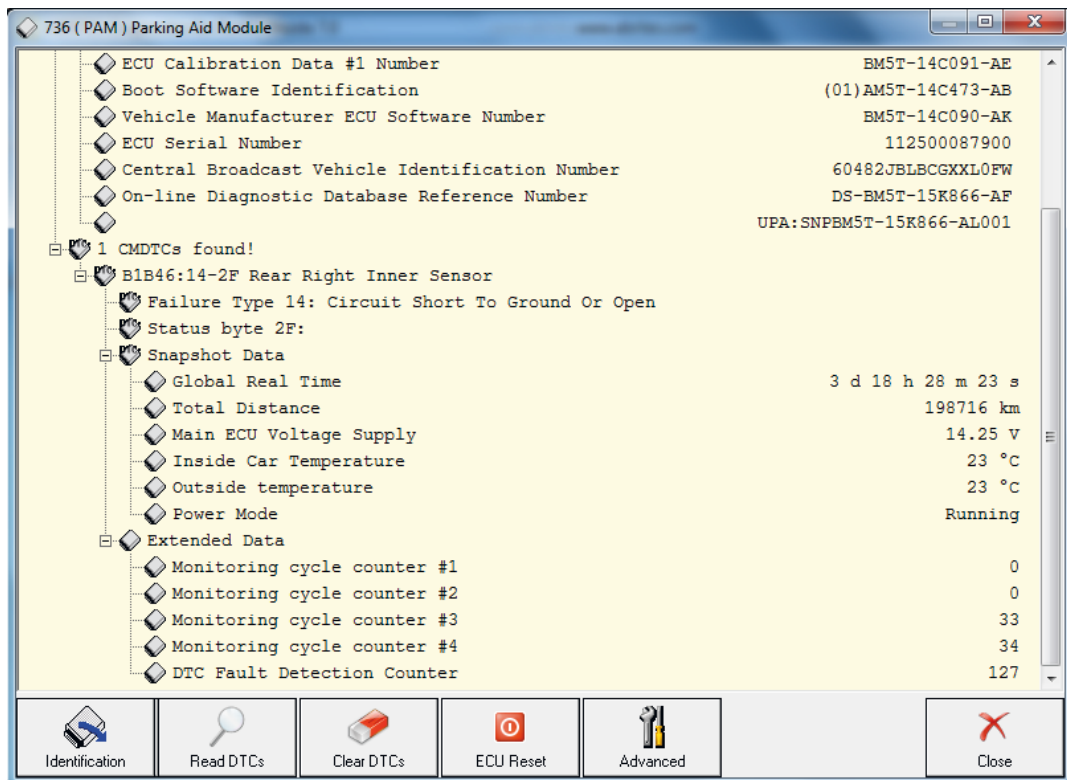


Abbildung 10: Mit Abrites ausgelesener PDC-Fehler

Quelle: Eigene Abbildung

Zur eigentlichen Information, dass der rückwärtige, rechte innere Sensor einen Defekt aufweist, können zusätzlich Kilometerstand und die Zeit des Eintretens des Fehlers abgelesen werden. Der Zeitpunkt der Fehlermeldung ist relativ angegeben, d. h. es ist die reale Zeit vom Zeitpunkt des Auslesevorgangs dargestellt. Eine weitere Information ist in der Angabe der Temperaturen im und außerhalb des Fahrzeugs auswertbar. Diese könnte beispielsweise in der kälteren Jahreszeit auf den Abstellort des Kraftfahrzeugs hinweisen, also z. B. ob sich das Fahrzeug in einer warmen Garage oder im Außenbereich befunden hat.

Daten aus einem Car Access System

Mit dem AVDI von Abrites wurde ein Car Access System CAS3 von BMW ausgelesen. Abbildung 11 zeigt die grundlegenden Informationen des CAS3-Systems zu aktivierten Schlüsseln, dem Fräscod für den mechanischen Schlüssel sowie die Frequenz der Fernbedienung. Im Verlauf der Systemanalyse konnten Fehlermeldungen extrahiert werden. Abbildung 12 stellt die ausgelesenen DTCs dar. In den Fehlermeldungen ist nur der Fehler selbst sowie der Kilometerstand des Fahrzeugs, an dem der Fehler aufgetreten ist, angegeben.

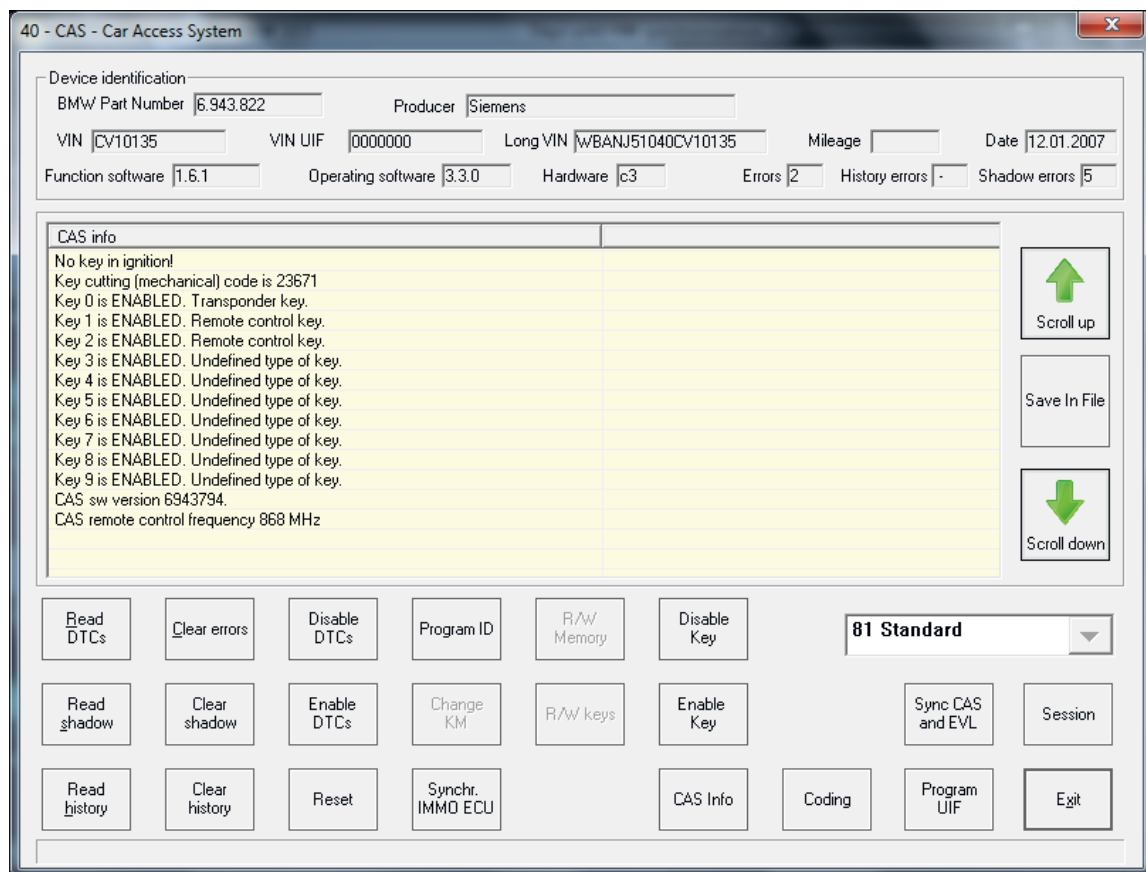


Abbildung 11: Mit AVDI ausgelesenes CAS3-System

Quelle: Eigene Abbildung

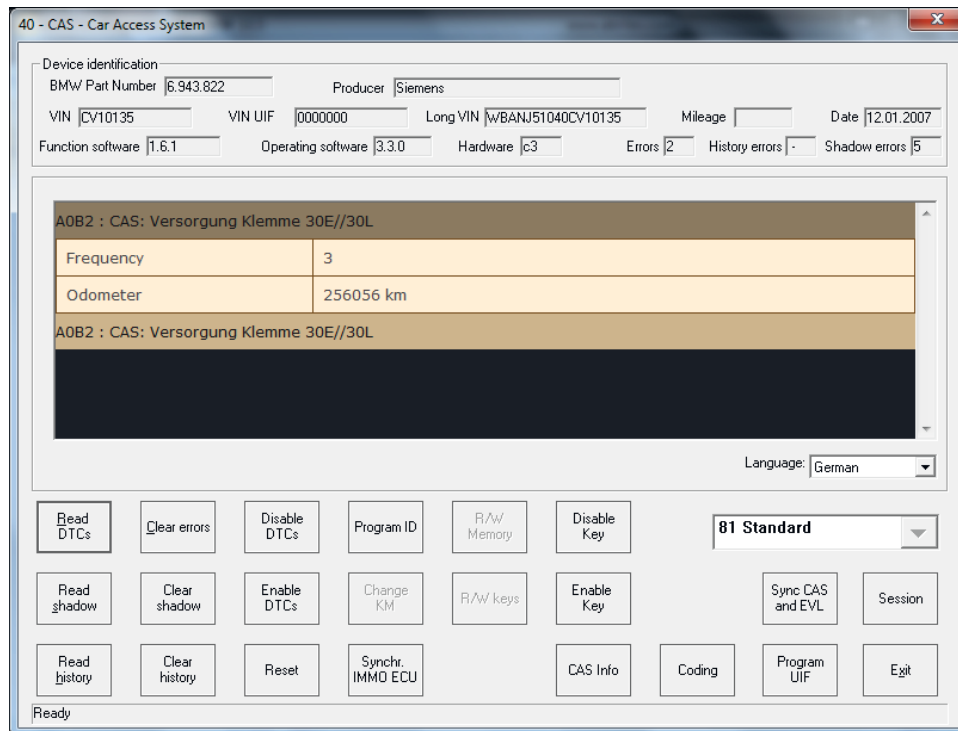


Abbildung 12: Mit AVDI ausgelesene DTCs des CAS3-Systems

Quelle: Eigene Abbildung

Daten aus einem ME7-System

In einem weiteren Versuch wurde mithilfe des AVDI ein ME7-Benzin-Motorsteuergerät von Audi per K-Line ausgelesen.

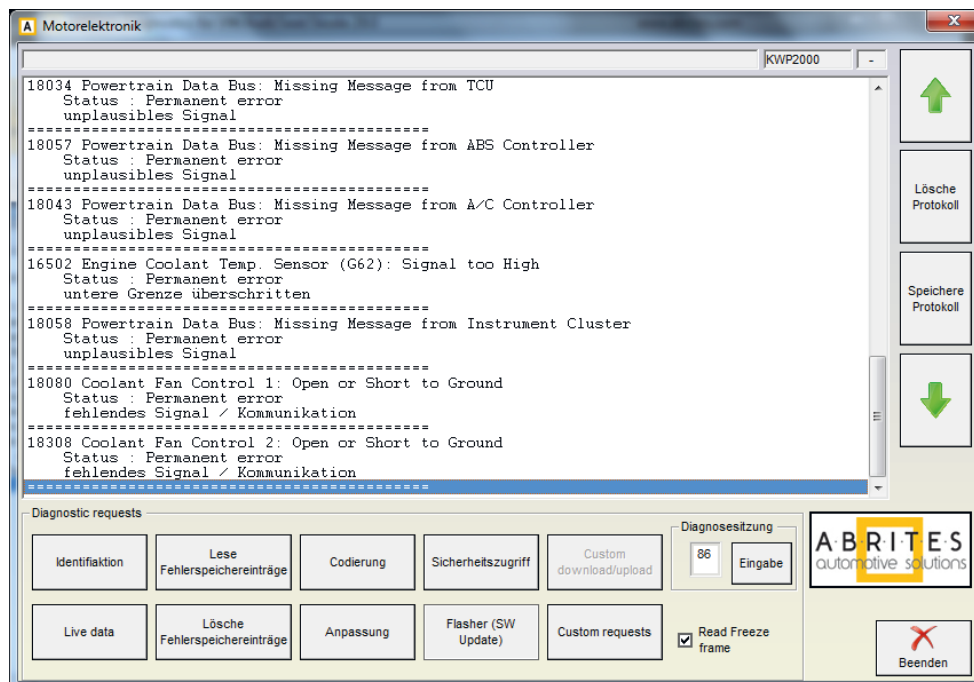


Abbildung 13: Mit AVDI ausgelesene DTCs des ME7-Systems

Quelle: Eigene Abbildung

Anhand dieser ermittelten Daten konnte nur die Fehlerbeschreibung extrahiert werden. Weitere Zusatzinformationen zu Zeit des Auftretens oder auch zum Kilometerstand waren nicht verfügbar, da das ME7-System diese Informationen nicht als Umgebungsbedingungen speichert.

Daten aus Airbag-Steuergeräten

Im Handbuch Verkehrsunfallrekonstruktion [Burg und Moser (2009)] Seite 745 ff. wird „Der Airbag als Sicherheitsbestandteil heutiger Automobile“ beschrieben. Im Verlauf stellt sich die Frage, „Welche Aufzeichnungen können bei (Gurtstraffer- und/oder) Airbag-Auslösung erwartet werden?“

Es wird festgestellt, dass diese Daten hersteller- und typabhängig sind [Larl]. Aufgezeichnete Werte beziehen sich auf:

- Vorgelegene Störungen vor der aktuellen Kollision nach Art und Zeitpunkt,
- Auslösefreigabe bei der aktuellen Kollision auf niedrigem Verzögerungsniveau,
- Verzögerungsverlauf vor und nach der Kollision,
- aus der Verzögerung errechnete Geschwindigkeitsänderung,
- Zündsignale nach Zeit und Größe für die Airbags (und für die Gurtstraffer) sowie
- Bestätigung der Auslösung von Airbags (und Gurtsystemen).

Zusätzlich können die Parameter Bremsdaten, Raddrehzahlen, Gierrate, Motordrehzahl, Außentemperatur gespeichert sein. Prinzipiell dienen diese gespeicherten Daten der Fahrzeugdiagnose in einer Vertragswerkstatt des Fahrzeugherstellers, können aber teilweise zur Unfallrekonstruktion herangezogen werden.

6 Diskussion / Zusammenfassung

Im Paper wurde die Akquise von Daten aus Kraftfahrzeugen unter Verwendung verschiedenster technischer Hilfsmittel aufgezeigt. Grundlegend wurde dargestellt, welche elektronischen Systeme in Kraftfahrzeugen verbaut sind. Zusätzlich konnte gezeigt werden, wie diese Systeme forensisch angesprochen bzw. ausgewertet werden können und welche Analysewerkzeuge eine Datenauswertung ermöglichen. Es konnte veranschaulicht werden, dass Positionsdaten, gespeicherte Routen, Telefondaten, Fehlermeldungen, Zeitstempel, km-Stände oder auch genaue Abstellorte eines Fahrzeugs zu einem definierten Zeitpunkt ermittelbar sind. Diese Daten aus Infotainmentsystemen, einzelnen Steuergeräten und Schlüsseltranspondern können bei Bedarf einem Fall zugeordnet werden, um bei der Aufklärung von Straftaten oder bei der Unfallrekonstruktion zu helfen. Kritisch ist an dieser Stelle anzumerken, dass nicht jeder Hersteller alle Funktionen in den Steuergeräten implementiert. Dies be-

zieht sich auf die Umgebungsdaten wie z. B. Zeitinformationen innerhalb von Fehlermeldungen. Diese können gespeichert sein, müssen aber nicht. Zusätzlich ist die Plausibilität von gespeicherten Umgebungsvariablen zu prüfen. Es wurden teilweise fehlerhafte Einträge festgestellt, da analysierte Steuergeräte beispielsweise Wegstrecken doppelt gezählt haben. Zum Berla-System gibt es in [Born (2016)] auf Seite 21 Hinweise, dass auch in Infotainmentsystemen Zeitstempel nicht immer korrekt abgespeichert sind.

7 Literaturverzeichnis

- ABRITES (2021): ABRITES Vehicle Diagnostic Interface (AVDI). Abgerufen am 19.05.2021 von <https://abrites.com/page/avdi>.
- ADIS: ADIS Technology EuroDFT. Abgerufen am 09.07.2021 von <https://www.eurodft.com/?s=eurodft>.
- AUTOSEVICEPRAXIS (2020): Diagnosesoftware: Zugang auch in geschützte Systeme. Abgerufen am 09.07.2021 von <https://www.autoservicepraxis.de/nachrichten/autobranche/diagnosesoftware-zugang-auch-in-geschuetzte-systeme-2542598>.
- AUTOSEVICEPRAXIS (2021): Security Gateway: Auf sicheren Wegen. Abgerufen am 09.07.2021 von <https://www.autoservicepraxis.de/nachrichten/autobranche/security-gateway-auf-sicheren-wegen-2832594>.
- Born, J. (2016): Automobil-Forensik mit Berla iVe. Abgerufen am 20.05.2021 von https://www.fh-aachen.de/fileadmin/people/fb05_schuba/IT-Forensik/download/workshop2016/2016_07_Born_Workshop.pdf.
- Bosch (2021): KTS 980 – Diagnoselösung mit DCU 220 und KTS 590. Abgerufen am 19.05.2021 von <https://www.boschaftermarket.com/de/de/werkstattausrustung/steuergeraetediagnose/diagnosegeraete/kts-980/>.
- Burg, H. und Moser, A. (2009): Handbuch Verkehrsunfallrekonstruktion. 2. Aufl., Springer Vieweg, Wiesbaden.
- CONITEC (2021): GALEP-5D. Abgerufen am 20.05.2021 von <http://www.conitec.net/german/galep5d.php>.
- Elmelectronics (2021): ELM327DS. Abgerufen am 19.05.2021 von <https://www.elmelectronics.com/wp-content/uploads/2016/07/ELM327DS.pdf>.
- Feusi, A. (2019): Vorgetäuschter Autodiebstahl: Elektronische Autoschlüssel taugen wenig als Belastungszeugen. Abgerufen am 20.05.2021 von <https://www.nzz.ch/zuerich/vorgetaeuschter-autodiebstahl-elektronische-autoschluesssel-taugen-wenig-als-belastungszeugen-ld.1494058>.
- GÖTH (2017): Göth GmbH: Der Kraftfahrzeug-Diebstahl in der Praxis. Abgerufen am 20.05.2021 von <https://www.goeth.com/wp-content/uploads/2017/03/Artikel38.pdf>.

- HERTH&BUSS (2021): OBD-Schnittstelle: Wie freier Werkstatt-Zugang zu Fahrzeugdaten erschwert wird. Abgerufen am 09.07.2021 von <https://herthundbuss.com/branche-mehr/obd-schnittstelle-erschwerter-zugang-fuer-freie-werkstaetten/>.
- HERTH&BUSS (DoD): Diagnose on Demand –Das ideale Kfz Diagnosegerät. Abgerufen am 09.07.2021 von <https://herthundbuss.com/produkte/highlights/diagnose/>.
- IEEE (2010): Experimental Security Analysis of a Modern Automobile. Abgerufen am 03.06.2021 von <https://ieeexplore.ieee.org/document/5504804>.
- INGENIEUR.DE (2015): Hacker Samy Kamkar öffnet Garagentore und Autotüren. Abgerufen am 03.06.2021 von <https://www.ingenieur.de/technik/fachbereiche/ittk/hacker-samy-kamkar-oeffnet-garagentore-autotueren/>.
- ISO9141: Road vehicles — Diagnostic systems — Part 2: CARB requirements for interchange of digital information. Abgerufen am 03.06.2021 von <https://www.iso.org/obp/ui/#iso:std:iso:9141:-2:ed-1:v1:en>.
- ISO14229: Road vehicles — Unified diagnostic services (UDS) — Part 1: Application layer. Abgerufen am 03.06.2021 von <https://www.iso.org/obp/ui/#iso:std:iso:14229:-1:ed-3:v1:en>.
- ISO15765: Road vehicles — Unified diagnostic services (UDS) — Part 1: Application layer. Abgerufen am 03.06.2021 von <https://www.iso.org/obp/ui/#iso:std:iso:15765:-2:ed-3:v1:en>.
- ISO22901: Road vehicles — Open diagnostic data exchange (ODX) — Part 1: Data model specification. Abgerufen am 03.06.2021 von <https://www.iso.org/obp/ui/#iso:std:iso:22901:-1:ed-1:v1:en>.
- J1939: SAE J1939 Standards Collection on the Web: Content. Abgerufen am 03.06.2021 von <https://www.sae.org/standardsdev/groundvehicle/j1939a.htm>.
- JUNIPER (2018): In-Vehicle Commerce Opportunities Drive Total Connected Cars to Exceed 775 Million by 2023. Abgerufen am 21.05.2021 von <https://www.juniperresearch.com/press/in-vehicle-commerce-opportunities-exceed-775mn>.
- KASPERSKY (2015): Shock at the wheel: your Jeep can be hacked while driving down the road. Abgerufen am 03.06.2021 von <https://www.kaspersky.com/blog/remote-car-hack/9395/>.
- Kfz-Betrieb Vogel (2019): 100 Millionen Codezeilen: Das kann der Golf 8. Abgerufen am 24.09.2021 von <https://www.kfz-betrieb.vogel.de/100-millionen-codezeilen-das-kann-der-golf-8-a-824084/>.
- KURTZERSA (2021): IR 550. Abgerufen am 20.05.2021 von <https://www.kurtzesa.de/electronics-production-equipment/rework-inspektionssysteme/rework-systeme-stationen/produkt-details/ir-550.html>.

- Larl, W.: Digitale Spuren - Neue Möglichkeiten in der Sachbeweissführung am Beispiel der Kfz-Airbag-Steuerung. Abgerufen am 21.05.2021 von http://www.jpcity.de/digitale_spuren.htm.
- Lieder, R. (2017): Gateway processor evolution in automotive networks. Abgerufen am 24.09.2021 von https://www.can-cia.org/fileadmin/resources/documents/conferences/2017_lieder.pdf.
- MYCARLY (2021): Die beste App für deine Auto-Diagnose, Kodierung und Wartung. Abgerufen am 19.05.2021 von <https://www.mycarly.com/de>.
- OBDII (2021): OBDII Interface Lescars. Abgerufen am 19.05.2021 von https://images-na.ssl-images-amazon.com/images/I/811dSmBKHfL._AC_SL1300_.jpg.
- Statista (2021): Prognostizierter Anteil von vernetzten Automobilen (connected cars) in den USA, China und der EU von 2020 bis 2035. Abgerufen am 03.06.2021 von <https://de.statista.com/statistik/daten/studie/757547/umfrage/prognostizierter-absatz-von-vernetzten-automobilen-in-regionen-weltweit/>.