Investigating Accidents Involving Highly Automated Vehicles: Concept of a Data Trustee and Data Model for Future Homologation

Dipl.-Ing. (FH) Melanie Kreutner, Dr. Christoph Lauterwasser, Dr. Johann Gwehenberger,

AZT Automotive GmbH - Allianz Center for Technology

Germany

Paper Number 19-0035

ABSTRACT

According to statements by the EU Commission, 95% of all traffic accidents involve human error, and in 76% of accidents, humans are solely to blame [1]. A similar picture also emerges in the settlement of damages by Allianz Versicherungs-AG, and in detailed analyses of the accident research by Allianz Center for Technology.

At the same time, human drivers set high standards with regard to road traffic safety. Based on market figures over the past few years, in Germany, a passenger car causes material damage only every 250.000 km, and personal injury every 2.3 million km. Since the 1960s, the number of liability claims per passenger car has decreased to a third of the previous figure, and today the claims frequency is at around 60 claims per 1.000 insured units per year [2].

Above the level of high vehicle automation [3] from which the driver is no longer responsible for continuously monitoring the vehicle and the driving task, however, completely new issues will arise in the road traffic accident statistics. In the case of highly automated driving, extremely high requirements must be placed on vehicle safety and on protecting functions in order to not only keep road traffic safety at the current level, but actually improve it significantly. Unfortunately, accidents in the USA with vehicle prototypes in highly automated driving mode show that some accidents cannot be prevented with the current state of technology. Coupled with this is the question as to how cases can be investigated should an accident or criminal misconduct involving a highly automated vehicle occur after the legal authorization of highly automated driving functions and their introduction into the market in the EU.

As explained elsewhere [4], the German liability and insurance system is well suited to covering the risks that exist in the operation of highly automated vehicles. However, the selective operation of the vehicle by the driver and by a highly automated driving function raises fundamental questions concerning the investigation of cases in the event of accidents or traffic offenses.

Early on, Allianz already supported creating conditions so that accidents involving automated vehicles can be reconstructed in the future in order that victim protection, clarification of liability, and regress and product liability claims can still be ensured in a non-discriminatory manner. This is because, in the course of the motor vehicle insurer investigating a case and settling claims, particular importance is attached principally to the driving mode (highly automated driving/transfer phase/driver in control) in which the vehicle was moving at the time of the accident or the traffic offense. On the one hand, a driving error by the driver could be the cause of damage, on the other hand, errors by sensors, inadequate algorithms, deficient software quality or interoperability of systems cannot be ruled out as the cause of an accident. The driver’s statement that a collision or non-compliance with traffic regulations occurred after handing over control to the vehicle cannot be verified or disproved without a sufficient set of relevant data.

DRIVING MODE RECORDER / DSSAD

Whereas standards for the data logged in vehicle event data memories have been established in the USA for several years (NHTSA DOT rule 49 CFR Part 563 [5]), outside the USA, there are no such standards to date. In the current stock of vehicles in the EU, reading accident data remains primarily a privilege afforded to the vehicle manufacturer. For external parties, for example experts, reading data is possible only – if at all – with high technical expertise, suitable reading devices, and still limited to some vehicle models.

This problem has been recognized by both the EU and the German government. Thus, in the course of amending the regulation UN ECE-R79 Steering systems, the “World Forum for Harmonization of Vehicle Regulations (WP.29)” develops continuous driving mode storage. The “Data Storage System for Automated Driving”, or DSSAD for short, is intended to store data relating to [5]:

- GPS location and time
- Activation of the AD System (Automated Driving Function)
- Transition demands
- Activation of a “minimal risk maneuver”
- Takeover of the driving task by driver
- System error

These data elements are also required in § 63a StVG [7] of the German Road Traffic Act, amended in 2017, in the case a vehicle is equipped with a highly or fully automated function.

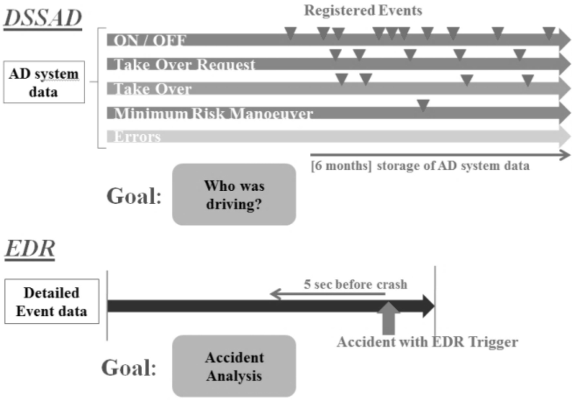


Figure 1: Difference between DSSAD and EDR

Figure 1 shows the difference between DSSAD and EDR. The DSSAD can clarify the question as to whether the vehicle or the driver is in control at a given time. But there is no trigger for data storage in an incident. Besides, it has not yet been determined how authorized persons or parties can access this data and in what location, internally in the vehicle or externally, said data have to be stored. Authorized persons or parties should have easy, tamper-proof, fair and non-discriminatory access to the relevant data elements. These requirements cannot be met when the data is solely stored in the vehicle. A brief example should illustrate this:
A person drives on the freeway in highly automated driving mode and, after this journey, receives a penalty notice as a result of having exceeded the maximum permitted speed by 20 km/h. If the data is stored only in the vehicle, the person in question would have to drive to a workshop or to an expert so that the data can be read in order to prove their innocence.
In the digital age, in which vehicles drive in a highly automated or even autonomous mode, this investment of money and time cannot be considered appropriate. Therefore, the data should be stored externally and should be accessible online, or available on request.

CONCEPT OF THE DATA TRUSTEE

Regulated external data storage and management could be ensured in practice by the concept of an independent data trustee. The data trustee must treat the encrypted raw data transmitted online impartially and check authorized access by interested parties. Figure 2 shows the advantages of double storage, i.e. in the vehicle and with an independent data trustee. Vehicle data that can be attributed to the occurrence of an accident or a criminal offense must not be made available exclusively to the driver, the insurer, the public prosecutors or the vehicle manufacturer. Independent data management by a trustee would ensure that the regulated dataset is accessible to all authorized persons or parties [2].

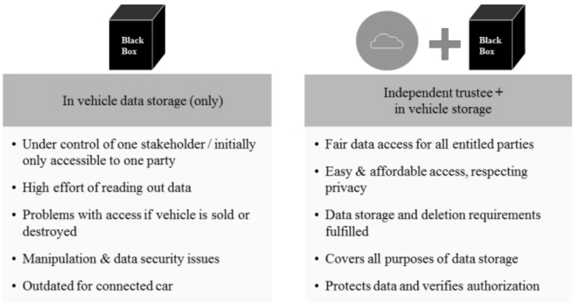

Black Box
In vehicle data storage (only)
Under control of one stakeholder / initially only accessible to one party
High effort of reading out data
Problems with access if vehicle is sold or destroyed
Manipulation & data security issues
Outdated for connected car
Black Box
Independent trustee + in vehicle storage
Fair data access for all entitled parties
Easy & affordable access, respecting privacy
Data storage and deletion requirements fulfilled
Covers all purposes of data storage
Protects data and verifies authorization

Figure 2: in vehicle storage versus data trustee and in vehicle storage

Example I:
In the case of a notification of a claim where responsibilities are to be clarified, the vehicle owner requests a clarification of the cause from the insurance company. On the basis of the owner's request and authorization and a specific loss event, the insurance company requests the data from the data trustee. In turn, the data trustee distributes the re-encrypted data to the insurance company via a secure channel for further analysis and, if necessary, to the OEM e.g. for product improvement (see Figure 3).
Since the request to the data trustee is ideally made only via a vehicle ID that is generated at the beginning of the authorization, it is not possible for the data trustee to establish a connection between the owner and the vehicle data.

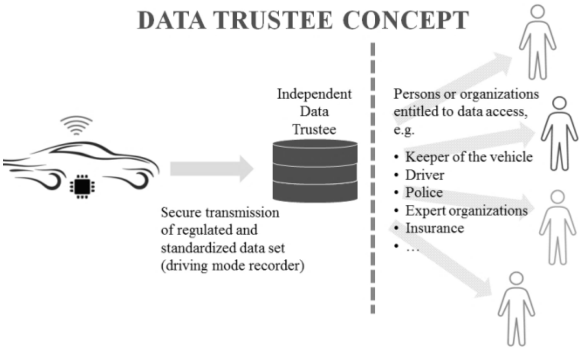

DATA TRUSTEE CONCEPT
Independent Data Trustee
Secure transmission of regulated and standardized data set (driving mode recorder)
Persons or organizations entitled to data access, e.g.
• Keeper of the vehicle
• Driver
• Police
• Expert organizations
• Insurance
• …

Figure 3: Data Trustee Concept

Example II:
If an owner wishes to view their data independently of the insurance company, e.g. to check for possible self-incrimination, they could make their request directly to the data trustee themselves or via the "Central Vehicle Register", via their attorneys or via an expert. As an alternative to personal requests, anonymous requests could also be answered in this way.
When data is transmitted to the data trustee, said trustee does not require any knowledge about the natural person with which a vehicle/driving mode memory is associated. From the perspective of the data trustee, the data is anonymous or under a pseudonym.
The data trustee should not have any direct contractual relationship with the data owner. Likewise, the data trustee should be independent and, in the relationship between the vehicle manufacturer, the vehicle owner, the driver, the other party involved in an accident (if applicable), and the insurance company, should represent a neutral party without own interests.

The data trustee guarantees the authenticity of the data (i.e. its origin and that it is unchanged) to the aforementioned parties and ensures that the (decrypted) data is provided

a) only to authorized parties,
b) only in authorized situations and
c) only in the regulated scope.

The trustee is also responsible for the security of the stored data against tampering, theft, etc.
Since the dataset as well as the access to data is defined by law, there is no need for the vehicle owner to sign a declaration of consent to storage. A data trustee would be able to provide the data to fulfill statutory require-

ments (e.g. a court order) without the permission of the data owner and, in standard circumstances, without access to the vehicle.

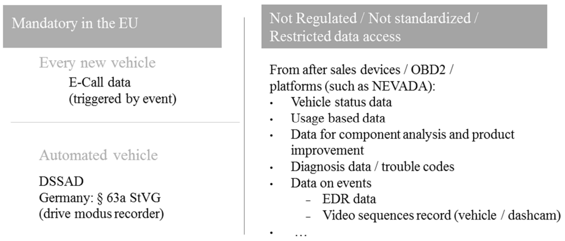
Technically, the requirements on data transmission can be met analogously, that is to say that the data transmission between the vehicle or the driving mode recorder and the trustee is carried out in a tamper-proof and tap-proof manner under any circumstances.

In this case, protecting the transmission via TLS (Transport Layer Security) is obvious, since this is an established protocol which, in addition to the encryption, also ensures that the vehicle's communication partner is also actually the chosen trustee. Additionally, a conventional asymmetric and symmetric encryption method could be used. Handling the data in this manner appears to be modern, convenient and fair.

NEED FOR ADDITIONAL DATA

As shown above some vehicle data have been subject to regulation, however the majority of vehicle data is not regulated in the EU. Figure 4 shows an overview of regulated and unregulated datasets in the EU. From the perspective of accident reconstruction, further standardization of the datasets would be desirable in order to clarify, in addition to the driving mode, the actual cause of the accident and additional questions of liability. An event data recorder is a prerequisite for:

- the ability of the driver and the vehicle owner to exonerate themselves where necessary and to assert product defects or service errors (e.g. in the case of updates and patches)
- protecting vehicle manufacturers and suppliers against unjustified claims
- a fair basis in any product liability cases/regress claims between the vehicle owner or the insurance company and the vehicle manufacturer or supplier



Mandatory in the EU

Every new vehicle

E-Call data
(triggered by event)

Automated vehicle

DSSAD
Germany: § 63a StVG
(drive modus recorder)

Not Regulated / Not standardized /
Restricted data access

From after sales devices / OBD2 /
platforms (such as NEVADA):

- Vehicle status data
- Usage based data
- Data for component analysis and product improvement
- Diagnosis data / trouble codes
- Data on events
  - EDR data
  - Video sequences record (vehicle / dashcam)
- …

Figure 4: Overview of data handling in the EU

With a view to international harmonization of standards, the profile of requirements in NHTSA DOT rule 49 CFR Part 563 could be a starting point for standardized data logging. However, in the EU project VERONICA II [8] from 2007 to 2009, it has already been shown that this regulation also has its weaknesses in the triggering of an event and the correct interpretation of the data that is read. This also corresponds to the experiences in AZT [9]. In AZT crash tests, multiple tested vehicles from several manufacturers demonstrated good correlations with respect to the crash data when comparing external laboratory measuring equipment with the EDR data logged by the vehicle. The tests also show that it has to be provided that the limitations in data generation in the vehicle are recognized and taken into account.

The analysis of EDR protocols from real road traffic accidents shows that in particular the pre-collision speed data cannot always be interpreted unambiguously, and data elements (such as the turn signal) often are not available for inferring liability.

Regarding triggering an event, it should additionally be noted that the US regulation is not specifically adapted for the requirements of automated driving, but is rather focused on restraint systems being triggered by a change in speed of above approximately 8 km/h within 150 ms as a result of an impact. In the variety of collisions and accident types that are settled by vehicle insurers, from a present-day perspective in accordance with evaluations by Allianz Center for Technology, an airbag is triggered only in a very low percentage of less than 3% of the settled claims. Even fatal accidents involving vulnerable road users exceed the described trigger thresholds on urban road only in very few cases. However, based on 2016 data, in Germany, 27.8% of accidents with fatalities, 33.2% of accidents with severe injuries and 27.8% of accidents with minor injuries in road traffic were attributable to accidents involving cyclists and pedestrians [10]. In addition, a research initiative by Allianz, Continental and Munich University of Applied Sciences showed that approximately 40% of all passenger car accidents with material damage are parking and maneuvering accidents [11]. In these collisions as well, the change in speed of the passenger car as a result of an impact is generally below the trigger threshold of the US regulation.
With a view to protecting victims and clarifying questions of liability, in the future, a much higher percentage of accidents should be able to be captured and stored by an event data recorder in highly automated cars.

OUTLOOK FOR AHEAD DATA MODEL

Automated Driving requires a highly sophisticated degree of vehicle, event and accident information well above US-EDR standard for data capturing, period, recording, storage, retrieval and safety. The work group “AHEAD” (Aggregated Homologation-Proposal for Event-Recorder-Data for Automated Driving), established in 2017, a cooperation by Allianz, AXA, CARISSMA/TH Ingolstadt, Continental and DEKRA, has therefore committed to drafting detailed requirements for an event data recorder for vehicles with automated functions of level 3 and above. The aim is to develop a data model that allows transparent, non-discriminatory and tamper-proof accident reconstruction and is compatible with current data protection laws. Storing crucial vehicle data shall be limited to a short timeframe before, during and after a triggering an event with the goal of obtaining accurate, in-depth accident data. The technical level of EDR as defined in the VERONICA II Project (2007-09) and as referred to in the “European Parliament resolution of 27 September 2011 on European road safety 2011-2020 (2010/2235(INI))” is a good starting point. But with regard to Automated Driving it is not sufficient any more. AHEAD has set out to update the requirements. Building on the results from the EU project VERONICA II and taking into consideration the automated driving functions, AHEAD describes data elements and organizes them into four standardized categories. According to the AHEAD White Paper [**Error! Reference source not found.**] the AHEAD Data Model includes but is not limited to the following data:

- Driving Data
  - Vehicle Status, Operation Mode (e.g. manual, autonomous, remotely controlled), Speed, Yaw Angle, Control interventions of the assistance system, Takeover request
  - Diagnostic data of safety relevant systems and components (condition, status, system failures/ technical malfunction)…
- Driver Activity
  - Video feeds from cabin cameras, Steering, Seat Position, Pedal Positions, Driver Alertness…
- Surroundings- and Object Recognition
  - Video feeds from front and rear-facing cameras, Sensor Data, Classified Objects, Object Position, Object Direction, Object Speed, Calculated Movement…
- Crash
  - Date, Timestamp, Location, Acceleration, Collision Speed, Seat Belt Status, Airbag, Restraint System…
  - Sensor technology, e.g. advanced and sensitive trigger which recognizes accidents with low acceleration in order to detect and measure accidents with vulnerable road users involved, or parking/maneuvering accidents

Whereas the required driving data, the data elements relating to driver activity and the crash data can be described by individual signals, the data related to environment and object recognition consist of elements that may have already been merged, calculated and assessed, which make it possible to compare the generated model of the vehicle environment with the reality and to check the plausibility of the control commands of the vehicle. The process of generating a virtual world and moving in a real world provides a high potential for errors. A highly automated vehicle must therefore provide data relating to this process. Since the calculation algorithms of manufacturers’ systems relating to sensor fusion, environmental model calculation and path planning of the highly automated ego-vehicle are strictly confidential, storing the raw sensor data is insufficient in this case.

The vehicle sensors, the vehicle cameras and other networking or communication channels of the highly automated and connected vehicle must be able to keep track of the entire vehicle environment. In practice, this means multiple overlapping and redundant "sensor cocoons" [13]. The detected sensor signals must be checked for plausibility, classified, provided with a time stamp, prioritized and annotated a thousand times per second. Lastly, in the generated environmental model, the location of the ego-vehicle relative to its environment must be determined in a repeatable manner and to within a centimeter. This processing of the signals can no longer take place by means of the bus systems used up to now, but rather must be processed by means of software blocks, which contain corresponding algorithms, on sensor platforms. The situational awareness of the highly automated vehicle which is calculated on said platforms part of the basis for the standardized data storage according to AHEAD.

The raw data supplied by the sensors (camera, laser scanner, radar, ultra sound) is prepared and evaluated by a number of different algorithms. The environment with the objects located in it must be classified and located by different methods. Thus the actual state of the vehicle environment is determined on the basis of a model, taking into consideration weather and visibility conditions. By means of GPS data, HD card data, the inertial sensor, the cameras, the laser scanner, the radar and ultrasound sensors, the ego-vehicle can locate itself in said environment. So that the ego-vehicle can also move in this environmental model, the future must also be calculated. For this purpose, numerous assumptions about the movements of other objects must be made. If the system has decided on path planning at a certain speed, this can ultimately be implemented in the form of control commands to the longitudinal and lateral control.

One of the greatest challenges for AHEAD will be getting this variety of data to a suitable level and an enforceable standard. This must also be done in accordance with the following AHEAD Guiding Principles for access to vehicle data:

- Consent
- Fair and undistorted competition
- Data privacy and data protection
- Tamper proof access and liability
- Data economy
- Standardized interface
- Crash resistance of data storage system in vehicle
- Event Data Storage for limited period of time before and after an incident (~ 30 sec)

Therefore the individual data elements required are continuously validated on the basis of real accidents and crash tests and evaluated and publicly discussed in various discussion groups. The AHEAD members invite stakeholders involved in setting the rules and requirements for Automated Driving (Parliament, Commission, Member States and others) to enter into dialogue.

CONCLUSIONS

An EU wide regulation with respect to a driving mode recorder, access to the data via a data trustee in combination with the introduction of an event data recorder for highly automated driving functions would have considerable advantages for the parties involved:

- The main focus would be on the public interest in integrity and victim protection.
- The ability of the driver and the vehicle owner to exonerate themselves where necessary and to assert product defects.
- Protecting vehicle manufacturers and suppliers against unjustified claims.
- Access to data would be politically endorsed and legitimized.
- Fairness for all parties.

In order for highly and fully automated driving to be widely accepted by society, the driver must only be able to be prosecuted for his own misconduct. It must therefore always be possible to clarify who is responsible (if the system has failed or if the person has failed). This driving mode data must be available for investigation through storage in order to clarify whether the vehicle was controlled by the automated system at the time of the incident or by the driver or was in the handover phase between the human driver and the automated system.

The necessary data must be in the hands of a neutral, independent third party (data trustee) in order to allow all authorized persons access to the data under the same legal conditions. In addition to storing the data in the vehicle itself, transmission to an independent third party is therefore mandatory. In the event of a vehicle being sold or after the vehicle has been destroyed in an accident, the data trustee is the only source of clarification in the interest of all parties involved.

Moreover, for highly automated vehicles (Level 3 and higher), a standardized event data set from the vehicle in the event of an incident is required. Only in this way will it be possible in future to clarify accidents or legally punishable events involving automated vehicles in a proper and transparent manner. The AHEAD working group develops parameters for such a data set. The data model includes elements on the vehicle status, driving environment, driving situation and driver activity which are defined for accident clarification. In addition trigger thresholds are defined with the goal of storing crucial vehicle data limited to a short timeframe before, during and after relevant events.

REFERENCES

1. European Commission. Digital Single Market, Mobility. Available at: https://ec.europa.eu/digital-single-market/en/mobility, accessed Mai 14, 2018

2. Hüttinger M.; Lauterwasser C.; Trinitis J., Standardized data recorders in highly automated vehicles [Standardisierter Datenschreiber bei hochautomatisierten Fahrzeugen] Insurance industry requirements and the data trustee model [Anforderungen der Versicherungswirtschaft und Modell eines Datentreuhänders], Haus der Technik, Developing methods for active safety and automated driving [Methodenentwicklung für aktive Sicherheit und Automatisiertes Fahren], 2nd Expert Dialog on Effectiveness – Controllability – Protection [2. Expertendialog zu Wirksamkeit – Beherrschbarkeit - Absicherung], expert verlag, Renningen 2017

3. Federal Highway Research Institute. Research Compact 11/12. Gasser T. et al. Legal consequences of an increase in vehicle automation. [Rechtsfolgen zunehmender Fahrzeugautomatisierung, Bundesanstalt für Straßenwesen, Forschung kompakt 11/12]. Available at: https://www.bast.de/BASt_2017/DE/Publikationen/Foko/Downloads/2012-11.html, accessed Mai 14, 2018

4. Stadler M. Civil law issues relating to automated driving. Paper presented at: 56th German Traffic Court Conference. Work Group II [56. Deutscher Verkehrsgerichtstag. Arbeitskreis II. Zivilrechtliche Fragen des Automatisierten Fahrens]. Goslar 2018

5. NHTSA National Highway Traffic Safety Administration. Rule 49 CFR Part 563. Event Data Recorders. Available at: https://one.nhtsa.gov/Laws-&-Regulations/Vehicles, accessed Mai 14, 2018

6. World Forum for Harmonization of Vehicle Regulations WP.29. ACSF-06-28 Secretary Consolidated document after 6th session. Available at: https://wiki.unece.org/display/trans/ACSF+6th+session. Accessed Mai 14, 2018

7. Dejure.org. Rechtsinformationssysteme GmbH. § 63a – 63b German Road Traffic Act [StVG]. Available at: https://dejure.org/gesetze/StVG/63a.html, Accessed Mai 14, 2018

8. Schmidt-Cotta R., EU Project VERONICA-II Final Report. Available at: http://www.veronica-project.net/. Accessed Mai 14, 2018

9. Dürnberger S.; Kreutner M. EDR data now and in the future [EDR-Daten heute und in Zukunft]. VKU Road Accidents and Vehicle Technology [Verkehrsunfall und Fahrzeugtechnik] 10/17. 55th Volume. October 2017

10. Federal Statistical Office of Germany. [Statistisches Bundesamt]. Road Accident. Fachserie 8 Reihe 7. Available at: https://www.destatis.de/DE/Publikationen/Thematisch/TransportVerkehr/Verkehrsunfaelle/VerkehrsunfaelleJ2080700167004.pdf?__blob=publicationFile. Accessed Mai 14, 2018

11. AZT Automotive GmbH, Continental, Munich University of Applied Sciences. A sudden bang when parking, Research Initiative on Parking and Maneuvering Accidents 2015. Press release [AZT Automotive GmbH, Continental, Hochschule für angewandte Wissenschaften München, Es kracht beim Ausparken,

Forschungsinitiative zu Park-und Rangierunfällen 2015, Pressemeldung]. Available at: https://www.allianzdeutschland.de/es-kracht-beim-ausparken/id_73896418/index. Accessed Mai 14, 2018

12. Forster, A. AHEAD Positions on EDR. EDR is active legal certainty and data privacy. Paper presented at: EU parliament. October 18, 2018, Brussels
13. Schrepfer J., Mathes J., Picron V., Barth H. Automated Driving and its Sensors under Test, ATZ Automotive Technology Magazine [Automatisiertes Fahren und seine Sensorik im Test, ATZ-Automobiltechnische Zeitschrift], 01/2018 Edition, Springer Professional, Wiesbaden, 2018