Release 11 September 2019

Homologation-proposal for **E**ventRecorderData for **A**utomated **D**riving

Accident data storage is real privacy

In the event of an accident, modern motor vehicles store a series of event data that are of great and increasing importance for accident clarification. However, even for experts it is not transparent in which vehicle models which data is recorded in which quality and how or whether it can be read. While, for example, a minimum standard for data recording in vehicles has existed for years in the USA, there is still no corresponding regulation in the EU.
In Germany, the amendment of the Road Traffic Act (§ 63a StVG) for the first time regulated data processing including data recording in the sense of a driving mode storage device (DSSAD[1]) for highly and fully automated vehicles. However, the data elements defined therein are not sufficient to clarify the causes of accidents and the corresponding liability issues. The regulation does not specify accident recognition by the system, data security and access options. In order for highly and fully automated driving to be widely accepted by the society, it must be possible to clarify accidents involving these vehicles with regard to liability and responsibility. At the same time, victim protection must be guaranteed and it must be possible to monitor and evaluate the safety of automated systems. Accident data must therefore be treated separately from commercially usable vehicle data.
Against this background, a multidisciplinary working group has developed a data model for accident investigation in vehicles with highly automated functions with SAE automation level 3 and above. The data recording shall be limited to the time period necessary for the clarification. A continuous storage of general driving data is not planned. Data privacy and customer protection are the top priorities when defining the data model. The customer shall have the decision whether data beyond the mandatory minimum will be recorded.
The proposed standardisation comprises a catalogue of necessary data elements, trigger thresholds for storage and possibilities for data processing and initially refers to motor vehicles of EC classes M1, M1G, M2, N1, N2 and N3. The data elements to be stored are divided into 4 standardised categories. The data model includes but is not limited to the following data:

<u>Driving data</u>
- Vehicle status, operating mode (e.g. manual, automated, remote-controlled), speed, yaw angle, control interventions of the assistance system, takeover request
- Diagnostic data of safety-relevant systems and components (status, system failures/technical malfunctions)...

<u>Driver activity</u>
- Steering, seating position, pedal positions, driver activity...

<u>Environment and object recognition</u>
- sensor data, classified objects, object position, object direction, object velocity, calculated motion...

<u>Crash</u>
- Date, timestamp, location, acceleration, collision speed, seat belt status, airbag, restraint system...
- Trigger sensor data

[1] DSSAD: Data Storage System for Automated Driving, UNECE

The trigger threshold for data storage must be defined by an advanced algorithm in such a way that even accidents with low accelerations and low speed changes, e.g. accidents with vulnerable road users, reliably lead to storage.
In addition to standardising data elements and trigger thresholds for storage, access to vehicle data must also be regulated. The guidelines for non-discriminatory access to vehicle data are:

- Legitimate interest
- Fair and undistorted competition
- Data privacy and data security
- Tamper-proof access and liability
- Data economics
- Standardized interface
- Crash resistance of the data storage system in the vehicle
- Event data storage for a limited period before and after an event (~ 30 sec)

Once the data has been stored in the vehicle, access to it must be guaranteed for authorised persons. The data processing via an independent data trustee would mean fair data access for all authorised persons. Access would be technically simpler and more affordable while respecting privacy. The data trustee can also meet the various requirements for data storage and deletion, manage the data, verify access rights and protect against manipulation.
Compliance with the standards outlined should in future be a prerequisite for the homologation of vehicles with highly automated systems in the European Union.