Allianz Position Paper on Accident Data from Connected and Automated Vehicles (October 2019)

Introduction

In the event of an accident, modern motor vehicles store a series of event data that are of increasing importance for accident clarification. However, even for experts, the type of data that is recorded in different vehicle models, its quality and readability, is not transparent enough. While, for example, a minimum standard for data recording in vehicles has existed for years in the USA, a similar regulation in the EU will become effective in 2022 and is subject to further specifications in the coming years.
For highly and fully automated driving to be widely accepted in society, it must be possible to determine liability and responsibility in case of accidents involving these vehicles. Concurrently, victim protection and speedy compensation must be guaranteed, for which it must be possible to monitor and evaluate the performance and safety of automated systems. Accident data must therefore be treated independently from "commercial" vehicle data. In light of the recent overhaul of the EU General Safety Regulation 2018/0145 which mandates an event data recorder for all new vehicles by 2022, Allianz developed the following positions with regard to event recording, storage and access to data.

Compliance with the below proposed standards should in future be a prerequisite for the homologation of vehicles with automated systems in the European Union.

Event data recording

Allianz, together with its external partners, has developed a data model for accident investigation in vehicles with highly automated functions ranging from SAE automation level 3 and above.
The proposed standardised data model comprises a catalogue of necessary data elements, trigger thresholds for storage and possibilities for data processing, initially referring 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:

1. **Driving data**

- 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)

- Software/firmware versions of critical components and time of last update

2. **Driver activity**
- Steering, seating position, pedal positions, driver activity

3. **Environment and object recognition**
- Sensor data including video footage and external information, classified objects, object position, object direction, object velocity, calculated motion

4. **Accident/Collision**
- Date, timestamp, location, acceleration, collision speed, seat belt status, airbag, restraint system
- Trigger sensor data

The trigger threshold for data storage must be defined by an advanced algorithm in such a way that even accidents involving low accelerations and low speed changes, e.g. accidents with vulnerable road users, reliably lead to storage.

Overall, storage of recorded data shall be limited to the time period necessary for the accident clarification. Therefore, a continuous storage of general driving data is not needed for accident clarification. Further, data recording must follow highest data privacy and customer protection regulations. The data subject shall make the decision as to whether data beyond the mandatory minimum shall be recorded and/or stored or not.

Event data access and 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 should be:

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

Adherence to these guidelines would ensure the integrity and reliability of the evidence.

Once the data has been stored in the vehicle, access must be guaranteed to authorized parties. The necessary data should rest in the hands of a neutral, independent third party (data trustee), in order to allow all authorized parties to access the data under the same legal conditions. In addition to storing the data in the vehicle itself, wireless transmission to the independent third party is crucial. In the event of a vehicle being sold or being destroyed in an accident, the data trustee should be the only source of clarification for the interest of all parties involved.
If an authorized party needs to receive the data for defined legal purposes, a simple and user-friendly process would be required. Exclusive storage of data in the motor vehicle would lead to complexities and delays for all parties involved. After successful transmission to the data trustee, the data stored in the vehicle should be deleted. Nowadays, since connected vehicles

constantly exchange data with back end infrastructures, the necessity of physically accessing the vehicle to read the data no longer exists.
In general, it is especially important that the transmission of data to authorized parties meets all requirements for the highest data security standards. This applies in particular to ensuring integrity and preventing data misuse. In addition to local storage of data in the vehicle, remote storage by the data trustee ensures that the risk of manipulation of the data is reduced to a minimum.

Overall, data processing via an independent data trustee would enable fair access for all authorized parties. Access would be technically simpler and faster, while respecting privacy. The data trustee could also meet the various requirements for data storage and deletion, manage the data, verify access rights and protect against manipulation.

Document version: 25 October 2019

This document reflects the current view of the autonomous driving expert group mentioned below. Content is subject to change and will be updated on a regular basis as both technology and society are changing rapidly.

Group members:
Amselem, Jacques (Allianz Technology);
Behling, Rolf (Allianz Partners);
Ben Hamida, Alaeddine (Allianz en France);
Boertjes, Erik (Allianz Benelux);
Fiedler, Hannah (Allianz SE);
Kreutner, Melanie Andrea (Allianz Center for Technology);
Kroha, Dr. Nadja (Allianz Deutschland);
Lauterwasser, Dr. Christoph (Allianz Center for Technology);
Sangiorgi, Daniele (Allianz Spa);
Senn, Sebastian (Allianz Deutschland),
Stait, Graham (Allianz UK);
Weichert, Juergen (AGCS SE),
Winter, Wolfgang (Allianz SE).