TSB Reference No.	102584
Project Title	MOVE_UK - Accelerating automated driving by connected validation and big data analysis
Deliverable No.	D10.9 Final proposal for EDR standards for autonomous vehicles
Principal Authors	Tony Ollieuz, DLG. &. Sam Chapman, The Floow
Date	18/07/2019
Issue/Revision No.	1.2

Work Package 10: Insurance Research

Content:

10.9: Overview

The purpose of this paper is to consider proposals for Event Data Recorders (EDRs)to be used in Autonomous Vehicles (AVs), based on widely available technology, which will meet the needs of insurers while also being acceptable to typical OEMs. This document provides recommendations for a minimum standard whilst identifying the potential for added value additions that can be provided from within vehicle systems and data.

Key Essential Recommendations are detailed in the following format throughout the document.

Added value additions are detailed in the following format throughout the document.

1 What is an Event Data Recorder (EDR)?

An Event Data Recorder (EDR) is a vehicle mounted device, or an agreed incorporated device within the vehicle architecture. These devices persist vehicle data temporarily such that in the event of a potential collision recorded evidential data can be used for later investigations. Evidential data from EDR's may be used by the Police, insurers, collision investigators, manufacturers and researchers to grow understandings for the cause of collisions. Investigations supported by EDR data target:

1) Fault and liability finding (to determine claim outcomes)
2) Building needed evidence for how to better mitigate future accidents.

EDR data persistence operates in two key manners:

1) Only when triggered upon detection of pre-set conditions that are understood to be indicative of a potential collision. For example: an airbag deployment, seatbelt restraint trigger or a large accelerometer impact to the vehicle frame (or other key indicator) each could trigger a persisted EDR record to be maintained. A limited number of EDR records will be maintained until written over with future trigger events.
2) Continuously throughout operation such that a buffer of recent behaviour is maintained. This is to support the above capability of key potential event recording but this capability also enables potential data consultation in some cases where the most recent data recorded is of interest following an incident. This only works if buffered recording stops following an incident of interest. Most typically this data is not as valuable as the triggered captured data which is the prime data EDR's can make available.

As EDRs collate a 'rolling window' of evidential data it will include data both before and after a triggered potential collision event to capture needed data before and after. Typically recording consists of high frequency records for key operational parameters (e.g. vehicle speed and other higher impacting fields). These fields cover many seconds before and also for a period of time after a potential incident trigger. Typically (from US market deployments and legislation) devices include 5 seconds of data from before the point of trigger as well as a similar (sometimes longer) period after the trigger event. This time window provides a snapshot of key data providing vital evidence surrounding potential incidents for later analysis and reuse.

An EDR is most typically a separated system to the host of sensors and embedded software that permanently monitor modern vehicle systems (via the "CAN bus' communication channels within modern vehicles). EDR's are also typically separate to any continual monitoring systems (e.g. telematics) as used commercially by The Floow, DLG and wider insurers to monitor driver performance and risk prediction. In practice, EDR deployments constantly capture and temporarily retain key data related to the vehicle operation surrounding potential incidents however it should be recalled that data is constantly over-written, with the EDR only designed to retain a set amount of data for the most recent activity and triggered events.

Figure 1 - A typical US market standard EDR device

2 What is the current position regarding EDR fitment within the EU

Under current European legislation there is no guideline or requirement for EDR's to be installed into production vehicles. Despite this, there is a large and increasing number of vehicles in the UK and Europe that already have EDR capabilities. Current adoption is in place strictly when related to vehicle standardisation and design to enable sale into the US market where EDR has been mandated since 1st September 2010. These US specific technical requirements and legislation detail technically the data a device must persist and how it can be accessed.

So far Europe and other global markets have undertaken numerous studies regarding the benefits of mandatory/voluntary fitment of EDR devices at the point of manufacture however these as yet have not resulted in system wide legislative changes. The most recent comprehensive study for the European Commission undertaken in 2014 makes firm recommendations that EDR's should be fitted across all new EU vehicles.

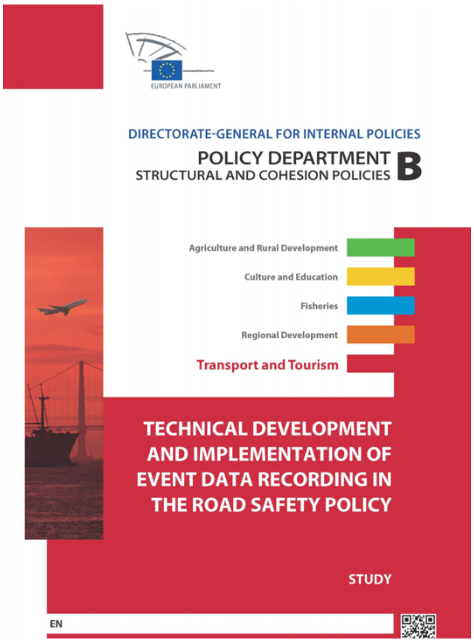

Figure 2 - The most recent comprehensive review of EDR technology undertaken by the European Union

It should be noted that related legislation does exist in the EU for regulation of incident alerting technology. This 'eCall' technology is ratified in parts of the EU region with a technical specification aiming to trigger automated location calls for emergency response given trigger identification of a potential serious accident. It should be highlighted however for eCall that although recognising severe accidents in key scenarios they do not cover all incidents. This means the technology available focuses upon detection of severe incidents only nor do they persist data to help understand incidents or fit the needs of investigation of incidents.

It is also worthy to note recent legislation in Germany regarding the testing of vehicles with SAE Level 3 or above autonomous technologies[1]. In these specific cases the German regulation indicates the need for a third party EDR device is specifically. These German legislations aim to gain evidence from any autonomous technology deployment adding within its technical specification the need to maintain records of autonomous and human control handover events, the means to enable this is not declared.

3 Automated Vehicles (AVs) and EDRs

Following the introduction of UK's Automated and Electric Vehicles Act 2018, liability for accidents caused by AVs has been placed on the motor insurer of the vehicle. In these instances, the person who is sat in the driving seat should be treated as a passenger and therefore entitled to compensation for any injuries they may have sustained. As an absolute minimum therefore, it is critical for insurers to have access to post collision data sufficient to be able to determine at the time of the accident whether the vehicle was driving itself.

Although data could be gathered in a variety of technical means it is highly likely to be delivered via extensions of existing EDR technology for ease of widespread deployment across

[1] I.e. ranging from ability for drivers to disengage from aspects of the driving task to full coverage autonomous driving .

all of the automotive sector. It is anticipated that the first wave of AVs, capable of 'out-of-the-loop' motorway driving, will be mandated to have an EDR fitted. These are expected to be regulated on an international basis like most vehicle technologies.

Some of the key questions for how these devices should be regulated however remains in debate with open questions specifically built around the following areas:

1) the triggering configuration,
2) the level and types of data an EDR should record,
3) how data is persisted,
4) how data is transmitted or accessed,
5) how data will be analysed (and other processing).

Each of these areas is detailed more fully with insight from the MOVE_UK project in the following sections.

The Association of British Insurers (ABI) and Thatcham in their report 'Regulating Automated Driving, the UK insurer view' July 2017 noted that:

> *It is unarguable that the market entry of Automated Driving systems requires development of an international standard for the transparent storage of an agreed minimum level of vehicle-related information. This is critical to ensure that, in the event of a collision, it can easily be established whether the driver, or the vehicle, was in control of the vehicle at the time. Global Regulators already use the term Data Storage System for Automated driving (DSSA) to identify the necessary process.*

As many modern vehicles already have capability to store crash data in their internal Network and where manufacturers voluntarily fit EDRs, the US Government has mandated that they must contain a certain minimum dataset, standardising the format of available data to ensure it can be downloaded using a standardised tool. The European Union propose mandating a similar capability from 2022. MOVE_UK investigations have studied the range of potential data available to support both risk estimation and incident understanding. The methodology for this process is discussed and reported in D10.3 and D10.7 The findings of these and key data to be persisted by an EDR for autonomous vehicles is detailed in the following section.

4 MOVE_UK insight and recommendations for EDR configuration for installations into AV's

Throughout MOVE_UK analysis has been undertaken such that insight into regulation and specification of optimal EDR configuration can be explored. This includes reviews of five key areas related to the open questions for a UK/EU deployment of EDR's. These areas match the open questions related to EDR's in light of application for autonomous vehicles. These areas are:

1) the triggering configuration,
2) the level and types of data an EDR should record,
3) how data is persisted,
4) how data is transmitted or accessed,
5) how data will be analysed (and other processing).

Each of these areas is each now discussed in more detail.

4.1 Triggering configuration

EDR triggers aiming to capture vehicle incidents have long been studied in the likes of the EU e.g. Veronica and Veronica2 projects (plus other incident trigger investigation projects). These prior investigations have informed automotive safety systems plus helping to specify key 'eCall' legislation and technical standards which include means for severe automated incident detection. Despite these prior investigations and legislations triggering configuration has thus far been developed and tested on track and crash test scenarios. This focus has required dedicated crash testing to help ensure triggers respond to pre-set incident scenarios in a suitable manner so to maximise effectiveness whilst minimising false data triggers. What is required for incident understanding in autonomous vehicles however is clear identification of incident fault for **all** incidents not just extreme events. This important distinction provides a clear need for improved coverage of real-world incidents – this area of investigation was considered in MOVE_UK investigations.

Within MOVE_UK vehicle data capture and the focus of investigations was based on real world deployments with a variety of drivers capturing wide naturalistic driving data. As such this focus provided means to test trigger events against real world gathered data. This is especially helpful to ensure that some triggers do not fire when not required. It should be noted however that MOVE_UK vehicle tests lacked any significant volume of real crash events preventing all aspects of trigger refinement. For such an investigation it would be beyond the scope of MOVE_UK and would require follow up studies or future work.
The MOVE_UK investigations of triggers focused specifically upon key use cases surrounding known risk scenarios with real world data capture. These key project trigger scenarios are:

1. **Driver Harsh Breaking** – upon extreme braking events and the circumstances for them
2. **Automatic Radar Braking** – upon radar triggered extreme events and the circumstances for them
3. **Automatic Video Braking** – upon video triggered extreme events and the circumstances for them
4. **Cut in Notification** – upon vehicle 'cut in' in front of the target vehicle and the circumstances for the more extreme 'cut in's.

Each of these investigations helped to focus exploration regarding triggers in each area upon 'sub-critical' triggers to capture wider evidential data rather than simply focusing upon clear extreme incidents. This would have had lower data capture across the project given the limited number of monitored vehicles if only selecting 'critical' incidents.

What these investigations showed is detailed more fully in D10.7 however the clear recommendations for future EDR technology to apply to autonomous vehicles can be summarised as follows.

Record and store data in all incidents, including minor crashes, insufficient to trigger the Supplementary Restraint System (SRS) e.g. Seat Belt Pre-tensioners and Airbags.

4.2 Levels and types of data an EDR should record

MOVE_UK has investigated data fields suitable to support EDR for autonomous vehicles. This work is already detailed in D10.3 and later in D10.7. This work reviewed a wide range of potential data suitable to give insight into incident understanding. This approach evaluated static and volatile fields in a process developed and described in D10.3.

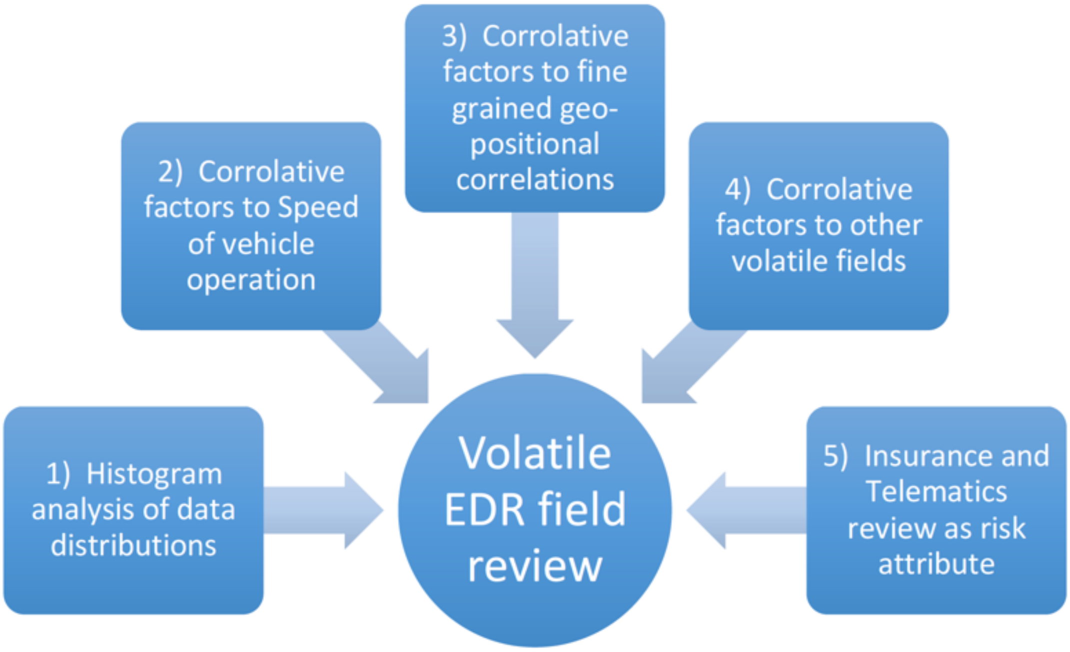

Figure 3 - High Level view of D10.3 approach for data field valuation in EDR settings for autonomous and future vehicle technology incident understanding. (This image is taken from D10.3)

Within this process data fields from within the vehicle and available to the MOVE_UK project analysis across all stages of the project where considered. This process aimed to quantify the value of key data fields for EDR incident understanding. This approach generated a scored approach on the valuation of available data to the task of EDR. Across this analysis value is given to each data field with:

- some fields being regarded of extreme high value
- some fields being of added but lesser value
- some fields being of low or negligible value to EDR

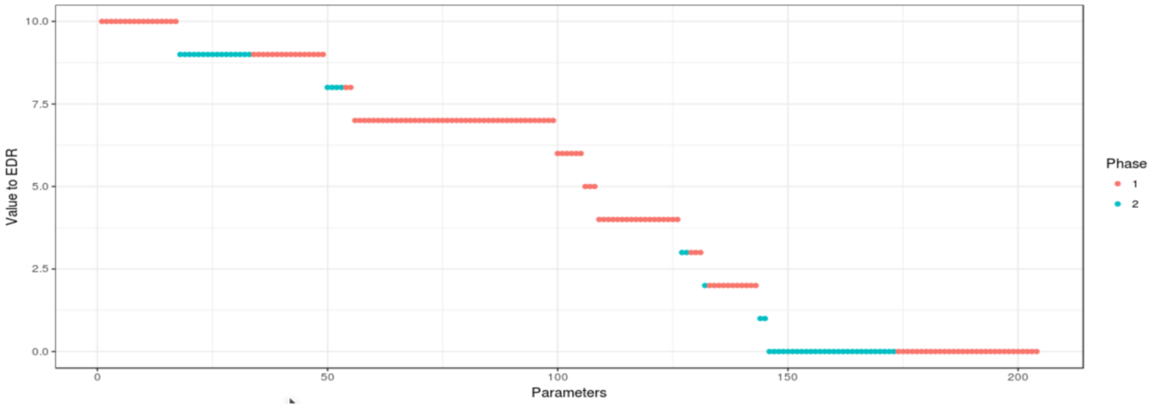

Figure 4 - Data Value analysis outcomes from D10.7 summarising the volatile field value to EDR incident understanding.

Despite this analysis of data available within the project analysis this does not represent the full value of all potential data beyond the project visibility. As such analysis for recommendations was extended beyond this project data focus to also consider wider evidence of potential data beyond that available in the project. For instance, the project did not have nor make available information on triggering of autonomous functionality (as not deployed in these data gathering vehicles) yet this would have clear and high value in incident understanding. As such wider recommendations must considered taking into account this wider data potential and not just those informed from the project directly.

One important aspect to consider beyond the project is the current discussions in the regulatory framework regarding regulation ECE R79 which is under review in Geneva (WP29). This regulation from the UNECE considers "Uniform provisions concerning the approval of vehicles with regard to steering equipment." This raises the mandated need for a Data Storage System for Automated driving (DSSA) as an EU deployment of EDR style data recording technology. Discussion of this provision is very much needed and welcomed. Although this approach is fully supported the Association of British Insurers and Thatcham as well as insight from the MOVE_UK project highlight limitations that will not allow an efficient and fair insurance claims process. This proposes amendments to help meet these gaps in order to fully support implementation needs of the Autonomous and Electric Vehicle Act 2018.

These recommendations are:

A clear understanding of the vehicle fit and functionality for autonomous operations needs to be available to enable correct incident understanding.

Include the identification, classification, fit and functionality of the system

Although data is not available in the MOVE_UK vehicles to indicate human driving vs machine driving it can however be clearly stated that this data is vital to understand incidents and the liability of them.

Identify the status of the automation system(s) (automated mode, transition of control, manual driver mode).

As incidents can occur at any time during driving operation across wide geography and operating modes it is important that incident triggers and data is available at all times across vehicle operation.

Ensure the system is capable of recording and storing data at all times, including when stationary, in any geographic location and in all automation modes and collects and stores data when appropriately triggered.

Throughout any incident observed key data is essential to understand liability. From D10.3 analysis and the findings of D10.7 it is clear that key data should ideally be available in order to understand incidents. This includes GPS telemetry, Vehicle speed data, Accelerometer data in high fidelity. Other data fields related to vehicle operation could add additional value to understanding potential incidents however the aim of recommendations aims to provide the minimum data possible so are not included in recommendations at this time and these values are value add recommendations.

Provide GPS location in high fidelity within the time period of the incident record

Provide Vehicle Speed in high fidelity within the time period of the incident record

Provide Accelerometer in high fidelity within the time period of the incident record

To enable event mapping to incident data a clear GPS position must be made available if high fidelity GPS data is not available to enable incident handling.

Provide GPS location at the point of event trigger

The scope of application for incident data capture must apply to autonomous control to a vehicle as set in UNECE regulation. This must cover all aspects of such control as declared in legislation.

Apply to all systems capable of continuously controlling the steering for a time, including remote parking or distance control systems and whether or not in combination with any automated lane change or speed control functions (ACSF-A and ACSF-B2 up to E) as defined in proposed amendments to UNECE Regulation 79.

EDR data should cover the full entirety of any incident to enable its review. Given insight from the sub-critical triggers in the use cases at times full capture of incidents could not be determined. To get a clear understanding a period of 30 seconds before an incident and 15 seconds after is required to understand all possible incidents.

Record and store data 30 seconds before and 15 secs after an incident.

It is important to clearly specify data formats for key fields to standardise data formats and expectations of data to be captured and made available. These are as follows.

Key recommendations for Data Fields to be recorded and stored are:

Field	Description	Format	Example
Event time stamp	Time stamp when triggered	UTC Format (corrected for GPS offset)	YYYYMMDD:HH:MM:SS
Automated Mode	Aligned to UNECE modes that are		“A”,”AA”

	currently under development A-Highway B- Inter Urban C-Urban D-Parking E--Traffic Jam Pilot Z- Not Active	Text field aligned to GRVA codes	
Driver Acceptance between Automated / Manual mode Time Stamp	Change in Automated Mode from not active (Z) and other Modes, or from other Modes to (Z) Not Active Modes - Time stamp when triggered	UTC format (corrected for GPS offset)	YYYYMMDD:HH:MM:SS
Record of Driver Intervention of steering or braking, acceleration or gear shift	Time stamp of the last intervention activity that occurred	UTC Format (corrected for GPS offset)	YYYYMMDD:HH:MM:SS
Driver Seat Occupancy	Indicator of Occupancy for each seat at the time of a triggered event	Binary	Y / N
Had a Minimum Trigger manoeuvre been triggered		UTC Format (corrected for GPS offset)	YYYYMMDD:HH:MM:SS
System Status (linked to fault codes)		Text field	Fault Codes
GPS at point of Trigger	Please note this field is not required only if full GPS records are provided	WGS 84 GPS format	Doubles of (Lattitude, Longitude)
GPS records		WGS 84 GPS format + UTC Format (corrected for GPS offset)	Triples of (latitude, longitude, UTC timestamp)
Vehicle speed records		Integer (rounded to nearest kph) + UTC Format (corrected for GPS offset)	Doubles (int_speed_kph, UTC timestamp)
Accelerometer records		Floating point normalised values (x,y and z)) + UTC Format	Quads floating point normalised values (x,y,y, UTC timestamp)

		(corrected for GPS offset)	

4.6 How EDR data should be persisted

It is clear that incidents captured must be persisted for a period of time supporting legal needs to determine liability and review incidents. Meeting this time period would prevent data being lost to help fulfil a legal process. This period is 6 months to enable all claims to be reasonably considered.

Store data for at least six months for all incidents.

It should be noted that devices may have a fundamental limit of data storage available such that data cannot be persisted on the device itself for this length of time. Therefore it is recommended that devices buffer a number of incidents (each capable of extraction should transmission fail. It is clear that data should be transmitted immediately from the device when possible to persist data centrally for review in the event of an incident.

Devices should enable standardised access to make available data not possible to transmit

Devices should buffer a number of incidents (10) to ensure available data for recent incidents can be available if needed

4.7 How EDR data can be transmitted or accessed

Given device limitations for storage and a need to build evidence for how to better mitigate future accidents. It is essential that data be centralised for analysis. It is also essential that this data is protected and handled according to exacting standards. This gives rise to clear recommendations for how data should be treated.

Allow insurers neutral, unbiased access to decoded data either by direct access or via over the air telematics links through a neutral third-party data handler.

Resist attempts to manipulate or delete recorded and stored data. To be held according to ISO 27037 standards to ensure data can be used in potential court proceedings for evidential purposes.

Provide means for standardised non-discriminating access to these data sets for all parties with a legitimate interest in an individual case (owner of the vehicle, driver, insurer, vehicle manufacturer, supplier, authorities).

It is suggested that an independent trustee for the management of DSSA data (for example the Motor Insurers Bureau for UK located incidents) would guarantee impartial access, while providing for data security and data protection.

4.8 How EDR data will be analysed (and other processing).

MOVE_UK determined in D10.1 a process for how EDR data could be processed the following high level process map remains unchanged from this period. This shows the steps an AV insurer must take when they receive notification from their policyholder (or another channel) that their vehicle has been involved in an accident.

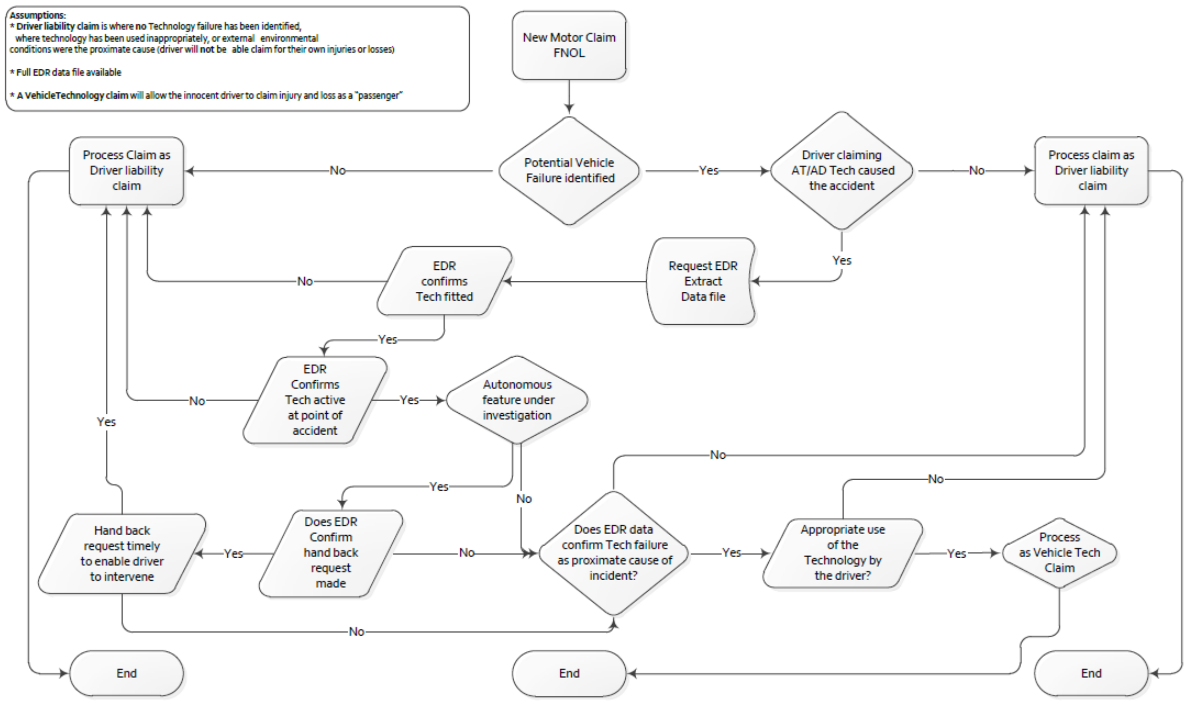

Figure 5 - Process for undertaking an Insurance claim involving an autonomous vehicle. This is taken from D10.1

5 Summary and key recommendations

MOVE_UK supports the recommendations outlined by The ABI and Thatcham in their report 'Regulating Automated Driving, the UK insurer view' July 2017 in relation to data information. It also builds further on these.

In particular it is agreed that the technical requirements for DSSA (for both AV and non-AV vehicles) should be harmonised internationally through the UNECE and implemented in Europe through EU Whole Vehicle Type approval in a timeframe to keep pace with that of the automation systems themselves.

It is also noted that a framework is needed for how this data will be made available following an incident, so that standardised access is guaranteed for all parties with a legitimate interest, and that the appointment of an independent trustee for the management of DSSA data would be the best way of achieving this while also providing data security and protection.

Following is a collated view of all recommendations made in the deliverable.

(1) Include the identification, classification, fit and functionality of the system

(2) Identify the status of the automation system(s) (automated mode, transition of control, manual driver mode).

(3) Ensure the system is capable of recording and storing data at all times, including when stationary, in any geographic location and in all automation modes and collects and stores data when appropriately triggered.

(4) Provide GPS location at the point of event trigger

(5) RECOMMENDED BUT OPTIONAL - Provide GPS location in high fidelity within the time period of the incident record.

(6) RECOMMENDED BUT OPTIONAL - Provide vehicle speed in high fidelity within the time period of the incident record.

(7) RECOMMENDED BUT OPTIONAL - Provide accelerometer data in high fidelity within the time period of the incident record.

(8) Apply to all systems capable of continuously controlling the steering for a time, including remote parking or distance control systems and whether or not in combination with any automated lane change or speed control functions (ACSF-A and ACSF-B2 up to E) as defined in proposed amendments to UNECE Regulation 79.

(9) Record and store data 30 seconds before and 15 secs after an incident

(10) Store data for at least six months for all incidents.

(11) Devices should enable standardised access to make available data not possible to transmit

(12) Devices should buffer a number of incidents (10) to ensure available data for recent incidents can be available if needed

(13) Record and store data in all incidents, including minor crashes, insufficient to trigger the Supplementary Restraint System (SRS) e.g. Seat Belt Pre-tensioners and Airbags.

(14) Allow insurers neutral, unbiased access to decoded data either by direct access or via over the air telematics links through a neutral third-party data handler.

(15) Resist attempts to manipulate or delete recorded and stored data. To be held according to ISO 27037 standards.

(16) Provide means for standardised non-discriminating access to these data sets for all parties with a legitimate interest in an individual case (owner of the vehicle, driver, insurer, vehicle manufacturer, supplier, authorities).

(17) It is suggested that an independent trustee for the management of DSSA data (for example the Motor Insurers Bureau for UK located incidents) would guarantee impartial access, while providing for data security and data protection.

(18) Key recommendations for Data Fields to be recorded and stored are:

Field	Description	Format	Example
Event time stamp	Time stamp when triggered	UTC Format (corrected for GPS offset)	YYYYMMDD:HH:MM:SS
Automated Mode	Aligned to UNECE modes that are currently under development A-Highway B- Inter Urban C-Urban D-Parking E--Traffic Jam Pilot Z- Not Active	Text field aligned to GRVA codes	"A","AA"
Driver Acceptance between Automated / Manual mode Time Stamp	Change in Automated Mode from not active (Z) and other Modes, or from other Modes to (Z) Not Active Modes - Time stamp when triggered	UTC format (corrected for GPS offset)	YYYYMMDD:HH:MM:SS
Record of Driver Intervention of steering or braking, acceleration or gear shift	Time stamp of the last intervention activity that occurred	UTC Format (corrected for GPS offset)	YYYYMMDD:HH:MM:SS

Driver Seat Occupancy	Indicator of Occupancy for each seat at the time of a triggered event	Binary	Y / N
Had a Minimum Trigger manoeuvre been triggered		UTC Format (corrected for GPS offset)	YYYYMMDD:HH:MM:SS
System Status (linked to fault codes)		Text field	Fault Codes
GPS at point of Trigger	Please note this field is not required only if full GPS records are provided	WGS 84 GPS format	Doubles of (Lattitude, Longitude)
GPS records		WGS 84 GPS format + UTC Format (corrected for GPS offset)	Triples of (latitude, longitude, UTC timestamp)
Vehicle speed records		Integer (rounded to nearest kph) + UTC Format (corrected for GPS offset)	Doubles (int_speed_kph, UTC timestamp)
Accelerometer records		Floating point normalised values (x,y and z)) + UTC Format (corrected for GPS offset)	Quads floating point normalised values (x,y,y, UTC timestamp)

Abbreviations used in this report:

eCall – Automated Emergency Call – a specification of automated emergency response triggering in the event of detected serious incidents.
EDR – Event Data Recorder – device to record incident related data within a vehicle.
DSSA – Data Storage System for Automated driving – a term given to an enhanced EDR capable of capturing data required to understand incidents in Automated driving.
FNOL – First Notification of loss, this is the initial call when the Insured advises their Insurance company of the claim.
SRS – Supplemental Restraint Systems – passenger passive safety system designed to trigger in the event of a potential accident, e.g. seat belt tensioners or airbag restraint systems.
UNECE – United Nations Economic Commission for Europe – a body that supports ratification of DSSA technology to be fitted into the EU type approval process for vehicle regulation.