PROPOSAL FOR AN IN-USE SAFETY AND SECURITY MONITORING FRAMEWORK FOR AUTOMATED VEHICLES (AV)

William Perren, Craig Arnold, Dr Kostas Kourantidis, Ben Simpson
Transport Research Laboratory (TRL Limited)
United Kingdom

Bryn Balcombe
ADA Innovation Lab Ltd.
United Kingdom

Nick Reed
Reed Mobility Ltd.
United Kingdom

Sam Chapman
The Floow Ltd.
United Kingdom

Paper Number 23-0280

ABSTRACT

The UK government are committed to bringing forward legislation to allow the safe and secure deployment of self-driving vehicles, as set out in the recent policy paper, "Connected and automated mobility 2025: realising the benefits of self-driving vehicles". As part of the Connected and Automated Vehicle Process for Assuring Safety and Security (CAVPASS) programme, TRL was commissioned to propose a concept for assuring the safety of Automated Vehicles (AVs) throughout their operational life.

The work involved developing technical, procedural and administrative approaches for safety incident identification, investigation and reporting based on an evidence review of current and proposed in-vehicle datasets, safety metrics and collision investigation methodologies and supported by expert judgment. A Hazard Analysis and Risk Assessment (HARA) and an analysis of domestic traffic rules was conducted to assess the monitoring coverage of relevant risk events. Based on these activities, an overall framework for in-use safety and security monitoring has been proposed.

The study identified the need to monitor compliance against the behavioural competencies and safety arguments stated prior to deployment in order to continually assess the performance of the AV and the validity of the safety case during operation. A taxonomy for event classification has been developed to specify events to monitor safety and rules compliance. The study proposes that event-based data capture is the most feasible method of capturing data required to understand event context and causation to enable investigation. A minimum dataset specification has been developed which specifies a set of data metrics and thresholds for event detection as well as the data to be recalled supporting incident investigation. The HARA found that the proposed measures could not cover all safety relevant events and data sources external to data processed by the AV are required. Therefore, a set of operational processes for monitoring have been proposed.

A concept for monitoring traffic rules compliance has been introduced whereby AV perception data is processed independently. Analysis of domestic traffic rules identified requirements to record relevant dynamic objects, static objects and AV behaviours to enable monitoring of rules compliance. Processes for in-depth investigation and data analysis have been developed to enable the identification of compliance issues, produce learnings to be shared across the industry, and continuously improve the safety scheme. In-use monitoring data was found to be vital in ensuring accountability of AV safety performance by the manufacturer and contributes to an open and transparent safety culture by enabling just and proportionate regulatory sanctions to be applied.

Due to their paucity, data from AV collisions could not be used to base monitoring approaches on. The approach taken in this work was to identify safety monitoring protocols based on known approaches from conventional driving and other transport domains. A principle of continuous improvement was proposed such that the accuracy, quality and relevance of the monitoring framework can be assessed through AV deployment. This independent study proposes a framework for the safety performance assessment of AVs during operation to provide regulatory oversight, accountability and improve public trust in the technology.

INTRODUCTION

The United Kingdom government are committed to bringing forward legislation to allow the safe and secure deployment of self-driving vehicles. As part of the CAVPASS (Connected and Automated Vehicles Process for Assuring Safety and Security) programme, a partnership led by TRL was commissioned to develop a concept for a framework for monitoring the safety and security of automated vehicles during their use (i.e. post-deployment). The study initially focussed on Low-Speed Automated Vehicles (LSAVs), i.e. fully electric vehicles with a maximum speed not greater than 20 miles per hour (approx. 32 kilometres per hour) to be used in mixed traffic on roads with a speed limit not higher than 30 miles per hour (approx. 48 kilometres per hour). Table 1 provides additional details of the use cases and vehicle designs in scope. Further, it was envisaged that these vehicles would be owned and operated as part of a fleet providing goods or passenger services, rather than privately owned.

Table 1.
Scope of use cases and vehicle designs considered

Characteristic	Scope
Body shape	To include novel vehicle designs which do not conform with legacy design conventions such as windscreens, long bonnets, driver controls, etc.
Purpose	Carriage of goods or passengers (seated, standing or mixed)
Powertrain	Fully electric
Maximum speed	20 mph
Maximum mass (gross vehicle weight)	5,000 kg for passenger-carrying vehicles 3,500 kg for goods vehicles
Operating environment	Roads with a speed limit up to 30 mph with mixed traffic (including VRUs), or Dedicated roadways (which may or may not have segregation barriers) Areas which may include high density of pedestrians Operating on a fixed route or within a fixed geographical area

The initial focus on LSAVs was because they are expected to be an early use case for Connected and Automated Mobility (CAM) technology, and because there are no conventionally (i.e. human) driven vehicles in widespread use today that are comparable. While LSAVs were the primary focus, the work considered how a framework could be scaled and adapted to other CAM technology and use cases in line with the UK government's CAM policy [1]. This work considered an in-use monitoring framework to support a safety assurance process. As such, the purpose of the work was to develop a framework that provides continued validation of the safety and security of the automated vehicle during its deployment lifetime which allows for oversight and accountability for manufacturers and operators. This paper presents the work performed to develop an in-use monitoring framework.

METHODS

Evidence Review

The scope of this work set the basic requirements which an in-use monitoring framework must meet. These requirements were:

- The framework must specify requirements for manufacturers and operators to capture data to support evaluation of safety performance throughout deployment. Safety performance should be assessed and validated against the safety performance claimed or expected prior to deployment.

- Data requirements should be set out which support Automated Vehicle (AV) collision investigations as well as enable monitoring of any trends in safety performance during normal operation. The data requirements and monitoring processes should allow for the identification of causal and contributory factors associated with an event which can support safety learning and continuous improvement within the nascent AV industry.

- The framework should be aligned to and interoperable with AV assurance approaches in development by other nations and at the international level.

- The framework should enable non-compliance with, for example, regulations, standards or best-practice to be identified and reported and allow for intervention if necessary.

Based on these requirements, an evidence review was conducted which reviewed current and proposed monitoring approaches for road vehicles including proposals made for AV regulatory schemes such as the United Nations Economic Commission for Europe (UNECE) in-service monitoring and reporting [2] as well as current conventional vehicle data recording methods such as Event Data Recorders (EDR) [3], telematics for usage-based insurance, and fleet monitoring. Monitoring approaches from other transport industries such as rail, aerospace and marine transport were also reviewed. It was noted that safety assurance and governance approaches for these industries have a greater focus on safety learning and continuous improvement, which would provide a good basis for a safety assurance scheme for AVs. Approaches for investigating road collisions were also reviewed to identify the data necessary to support investigation. This primarily focused on approaches from national road safety investigation branches which are focused on independent blame-free investigations for safety learning and continuous improvement. Based on the review, in-vehicle data elements and safety performance metrics relevant to in-use safety monitoring were collated. This was evaluated against the objectives of this scheme to identify a rationalised set of data elements which forms the basis of an in-use monitoring framework using data collected from the automated vehicle.

Hazard Analysis and Risk Assessment (HARA)

It was necessary for the monitoring approach to be able to adequately identify realised risk events such as collisions and near miss events as well as capture data to support investigation and analysis. In order to understand whether proposed monitoring approaches adequately cover all likely risk scenarios encountered by an LSAV, a hazard analysis and risk assessment was conducted. Hazards were identified and structured using a deductive logic approach starting with a top-level hazard and then broken down into the sequential causes. An example is shown in Figure 1.

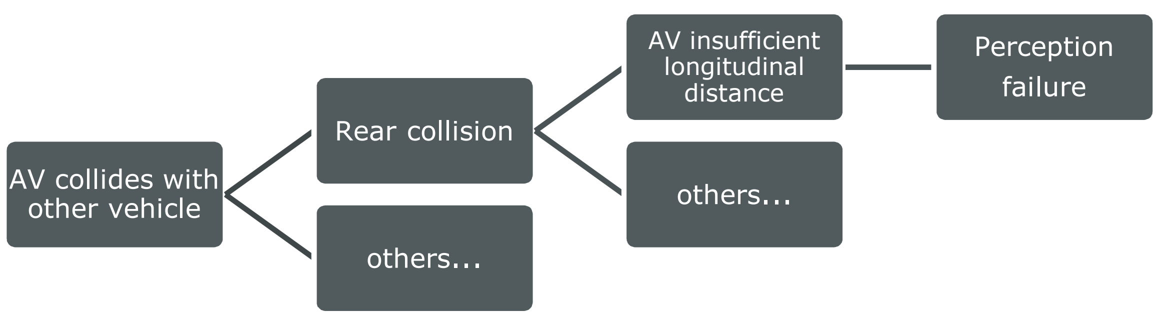

Figure 1: Hazard analysis structure

Each identified hazard or hazardous scenario was mapped to the data elements identified during the evidence review where there was a credible scenario where said data element could identify either the hazard or its causes. This allowed for evaluation of the coverage of the proposed data metrics and identified where in-use monitoring using vehicle data could not detect them.

Analysis of Domestic Traffic Rules

Compliance with road traffic rules (both mandatory and good practice) was found to be an important measure of safety performance and a key requirement to assure consistent, predictable and safe behaviour of AVs when operating alongside other road users. As such, proposals for an in-use monitoring framework include methods for identification of noncompliance with traffic rules by AVs. Other work in the CAVPASS programme set out a refined list of traffic rules relevant to the scope of operation which were collated from the Great Britain (GB) Highway Code [4]. For each of the GB domestic traffic rules relevant to LSAV operation, monitoring requirements were specified in this work, which identified:

- Elements of the rule that define relevant Operational Design Domain (ODD) attributes
- Elements of the rule that define Object Event Definition and Response (OEDR) requirements and driving behaviour considered part of the Dynamic Driving Task (DDT)
- If the rule specifies or requires the use of metrics and thresholds to determine compliance
- The type of measures, metrics, thresholds that are specified or required by the rule, where relevant
- Whether data regarding the vehicle’s environment is required to determine rule compliance/violation

The findings from this analysis were used to develop a proposal for rule compliance monitoring using in-vehicle data.

Framework Development

Based on the above work, a concept for a holistic in-use monitoring framework has been proposed the enables oversight of LSAV deployments in the UK which is intended to be scalable to further CAM deployments. For context, it is assumed that the monitoring framework is a part of a wider framework which includes pre-deployment assessment, which would involve the development of a safety case. Monitoring would be in support of validation of the requirements of the safety case. Additionally, the framework was required to define the requirments of 4 types of entities that would be involved in conducting in-use monitoring. Their roles are summarized below:

Manufacturers Responsible for producing the LSAV and putting it forward for pre-deployment assessment. They will have responsibilities to collect data around safety performance and share that data with the regulator to provide evidence of ongoing safety performance and to support investigation.

Service operators Responsible for the safe operation of the vehicle while the Automated Driving System (ADS) is engaged. Their responsibilities include oversight of the vehicle (including remote supervision or operation) and will have an operator Safety Management System that will reference operational monitoring.

In-use regulator The agency (or agencies) with the responsibility to ensure the continuing safety and legal compliance of self-driving vehicles while they are in-use by learning from mistakes and preventing their re-occurrence. They will monitor AV safety performance, investigate safety events and road traffic infractions, and intervene to maintain safety.

Independent investigator This independent body will select safety events involving AVs to investigate for the purposes continual learning, but not attributing blame or liability. This role in the UK may, for example, be carried out by the newly proposed Road Safety Investigation Branch [5].

In this work, we use these terms without prejudice to terms identified elsewhere (for example in the policy paper Connected & Automated Mobility 2025: Realising the benefits of self-driving vehicles in the UK [1]). A ‘manufacturer’ may assume the role of an Authorised Self-Driving Entity (ASDE) and an ‘operator’ may be assume the role of a No User-in-Charge Operator (NUiCO).

RESULTS

Monitoring Using Vehicle Data

In order to fulfil the requirements of in-use monitoring and reporting, data needs to be collected that identifies potential occurrences where the AV was not safe (i.e. collisions and unsafe occurrences), not compliant with traffic rules or, acted in a way not in line with the safety claims made by manufacturer. Data then needs to be collected around these occurrences to provide an explanation of the event. The starting point for this work was to consider how best to utilise the wealth of data collected and computed by AVs during normal operation to develop an effective method for collecting the data needed for in-use monitoring.

Event based data capture Event-based data capture involves monitoring for road scenarios and occurrences that act as trigger events for more comprehensive data capture. Trigger events are specified such that they are indicative of a risk event, or potential risk event. In this way, comprehensive data can be collected around events that are likely to be of interest for in-use monitoring, thus minimising the amount of data collected in nominal situations.

In this work, measures for triggering events have been expressed as having 3 components; the data, the metric, and the threshold. Data is collected on the vehicle to calculate a metric in real-time. That metric correlates to increased safety risk. When the measured data exceeds some threshold value, a safety event is identified, and further data is then recorded by the vehicle which supports investigation and analysis. Real-time evaluation of these measures mitigates the need for continuous data capture which is likely to be resource intensive and infeasible. Instead, event-based data capture allows for comprehensive data to only be collected where relevant to specific safety events. This framework is required to detect collisions as well as detect potential safety issues prior to harm arising. This gives rise to leading and lagging measures.

- Lagging measures strongly correlate to a realised risk outcome. They are highly precise in that they are very likely to identify an event of interest, such as a collision. However, they are likely to only cover events where a risk outcome has already occurred.

- Leading measures on the other hand are proxies, they indicate a potential increase in risk of a collision occurring but does not necessarily mean a risk event has occurred. Because of this they are considered less precise, meaning they have a higher propensity to capture events that are not relevant (i.e., false positives). However, they also cover a wider range of possible risk events and thus provide a wider data set for analysis and the ability to predict safety performance in the absence of real risk events.

It is proposed that LSAV manufacturers should be required to collect a set of both leading and lagging measures. Based on this, a minimum set of lagging and leading measures have been proposed, summarized below in Table 2 and Table 3 respectively.

Table 2.
List of proposed lagging measures and the benefits and usefulness of the measures to identify collisions and other risk events.

Trigger considered	Description
Vulnerable Road Users (VRU) impact detection system activation triggers	The operating environment for the most common LSAV use cases is likely to include a high proportion of VRUs such as pedestrians. Many collision scenarios involving VRUs do not typically include high delta velocity changes. The activation of any of the following technologies should act as a trigger for data collection: • body panel VRU impact detection • continuously running pedestrian protection control algorithms • non-reversible deployable pedestrian protection device
"wake up" of occupant roll over protection systems	Crash scenarios in lower speed urban environments do not commonly include roll-over events. However, "wake up" of occupant roll over protection systems, if equipped, should also trigger data collection.
Minimum Risk Manoeuvre (MRM) activation	Execution of an MRM may not result in risk realisation but remains a risk scenario of high importance given that exit from an approved operating design domain is likely to correlate to a risk event.
System triggers of "wake-up" occupant protection systems	Activation of the Airbag control unit/module (ACU/ACM) or other "wake-up" occupant protection systems likely correlate to a high-risk scenario.
Battery / under vehicle impact protection	Presents insight to risk realisation from vehicle grounding or object non avoidance.
Vehicle door release when in motion	Representative of a realised passenger risk if it occurs.

Safety Envelope close proximity detected	Extremely close proximity to objects while in motion is indicative of a collision scenario. Proximity may be measured in different methods and may be an absolute measurement of distance or may be a time-based algorithm for collision risk such as Time To Collision (TTC). Many different proximity measures exist. A summary of those reviewed and considered is provided in Appendix A. Rather than specify which one to be used, it was found that manufacturers could define one that best suited their technology and use case which would need to be justified prior to deployment (i.e. within a safety case).
Passenger emergency or operator control override mechanism	Indicator of emergency disengagement event or passenger emergency requiring data capture.
Vehicle dynamics beyond expected ranges (e.g. over max speed, or harsh events beyond design range)	Extremely harsh events such as harsh braking or acceleration which are outside of operational parameters could be indicative of a realised risk scenario or a collision avoidance manoeuvre. In either instance, data collection should be triggered.
Unavailable or disabled automated system sensor or control, fault triggers	Considers degraded functionality of automated systems (e.g loss of perception system) which constitutes an unintended deviation from the operational design safety parameters.

Table 3.
List of proposed leading measures and the benefits and usefulness of the measures to identify near miss events and assess safety performance.

Trigger considered	Description
Infraction Measurement – excess speed (Limit)	A measure of compliance with enforceable speed limits. Not strictly relevant to safety performance but a necessary measure of compliance with road traffic laws.
Infraction Measurement – excess speed (Safe)	Relative to context dependent safe speed such as reducing speed in roads with reduced visibility or in icy conditions. Manufacturers are expected to define their strategy for selecting a safe speed for the driving context and monitor for compliance.
Safety Envelope – proximity	Proximity may be measured in the same way as in Table 2 but with a larger threshold representing a breach of safe operating parameters and potential operation at increased risk.
Driving style – longitudinal and lateral jerk	Jerk is often used as an indicator of risky driving as it correlates to an increased rate of collision involvement. Longitudinal jerk measures the rate of change of acceleration/deceleration in the axis of forward motion of the vehicle and indicates instances of harsh braking or rapid acceleration. Lateral jerk is measured perpendicular to the direction of motion and is indicative of unsafe turning. Both measure undesired and unsafe driving performance.
Operational Design Domain (ODD) exit	Outside of operational design safety parameters that may represent operation at risk.
Hazard Identification, reaction, and risk perception	It is anticipated that some automated vehicle control systems may implement a model for dynamic risk assessment of current and foreseen situations for motion planning. If utilised, outputs of such a system which predict imminent high-risk scenarios should trigger data capture. Manufacturers would be expected to define how their control system is utilised to monitor for risk scenarios and identify the thresholds which would trigger data capture.
Safety pre trigger events – e.g., Anti-lock Braking System (ABS) pre-charge, Forward Collision warning	Pre-activation of safety systems are indicative of higher risk scenarios which may develop into realised risk events or represent narrowly avoided “near-miss” scenarios.

The proposed set of measures listed above represent a minimum set of measures thought to be necessary for safety event detection and assessment of safety performance. It is noted that some LSAV manufacturers may wish to use a broader set of measures for event-based data capture if required for adequate safety oversight of their system. If so, those additional measures would be expected to be defined and shared within a safety case prior to deployment.

It is noted that some measures are dependent on whether safety systems are equipped to the vehicle (e.g. ABS). It was outside of the scope of this work to determine whether such systems are to be mandated on LSAVs, however it was recommended that if they are equipped, they should be considered as inputs for data collection for in-use monitoring. It was found that many of the proposed measures are expected to be defined relative to the operating parameters of the system, such that data capture would be triggered should the defined operating parameters be violated. This implicitly requires the operating parameters that are monitored against to be clearly defined prior to deployment.

The HARA found that the context behind the event is crucial in determining whether a proposed measure could credibly detect the event. The activation of data triggers may be dependent on the severity of the hazardous event. For example, a high-speed differential collision may trigger the wake-up of occupant protection systems, whereas a lower speed differential collision may not. Detection of other events, based upon proximity or acceleration, may be dependent on the value of the detection threshold. The HARA also found that safety envelope proximity triggers were found to be key for both leading and lagging measures due to its high coverage of safety relevant events. By selecting different thresholds, it could also serve as a measure for near miss scenarios and realised risk events, serving as both a leading and a lagging measure. However, proximity triggers are reliant on correct object event detection by the Automated Driving System (ADS). The HARA found that the following causes of a hazardous event would not be possible to identify by relying on vehicle data alone:

- Detection of object too late
- Failure to detect object
- Incorrect classification of object
- Failure to identify ODD exit
- Failure to predict object trajectory
- Detection of object which does not exist

As such, operational monitoring approaches that are not reliant on vehicle data have been proposed as redundancies and are discussed later in this paper. It is inevitable that there will be instances where that collision avoidance fails and other situations where a collision is truly unavoidable. In these instances, the HARA found that the residual risk for not detecting a collision is high. If the AV fails to detect a collision it will not initiate the appropriate response (MRM, or E-stop, etc.) which could result in increased consequence severity and potential for secondary collisions before intervention. As a result of this finding, it is recommended that collision detection should itself become a safety goal which must be argued prior to deployment.

Threshold selection For most of the above measures, the threshold for data capture may be discrete, i.e. it can take a fixed number of values. This corresponds to a state change in the system, such as safety system activation, deactivation, or fault code. In these cases, thresholds should correspond to a discrete value where a system change indicates a risk event has occurred. For proximity based and driving style metrics, data may be continuous and so the threshold may be set at any value. This work found that for these measures, the threshold selected will delineate between what is considered safe and unsafe driving performance.

Thresholds for acceptable performance may relate to current standards and rules for driving in the nation/region. For example, the GB Highway Code recommends that drivers maintain a 1.5 metre clearance when overtaking cyclists at 30 mph or less. This sets a clear threshold for safe performance. However, this threshold is only applicable during an overtaking manoeuvre for a cyclist at 30 mph. For overtaking horse riders, the recommended passing distance is 2 metres. As such, this study found that thresholds must be dependent on the ODD elements (in this case speed and the type of road user) as well as the driving context (in this case overtaking) in order to adequately monitor for contextually safe behaviour. It is not appropriate to develop universal thresholds and they need to be context dependent. For other measures, such as longitudinal jerk, the GB Highway Code does not provide clear threshold values. In this case it is proposed that manufacturers develop their own thresholds that define acceptably safe limits of performance for their vehicle in its defined ODD. Manufacturers may wish to use simulation to define these thresholds prior to deployment, however it is expected that manufacturers will evaluate their thresholds and refine them throughout operation. Manufacturer-defined thresholds should be shared with the regulator prior to deployment (potentially as part of a safety case). The regulators would be expected to assess the manufacturer's processes for defining thresholds and determine their suitability for the proposed deployment. They would also assess whether any manufacturer defined thresholds conflict with the relevant driving rules and whether that conflict is acceptable or not.

Monitoring compliance with traffic rules There is a clear need to be able to establish when road rules have been breached and gather evidence on these incidents in order to apply the appropriate level of corrective action. The analysis of 165 LSAV relevant Highway Code rules identified that a majority of them are context specific and refer to both elements of the driving situation and the environment. Therefore, for an LSAV to be able to comply with a traffic rule, it must have awareness of both the ODD and DDT (OEDR) elements that are specified in that rule. In order to monitor for compliance with the rule, a metric must also be defined which assesses the relevant OEDR performance. An example of the results is shown in Table 4 for rule 212 of the GB Highway Code.

Table 4.
Summary of the traffic rules analysis for rule 212 of the GB Highway Code.

Rule 212 excerpt: Give motorcyclists, cyclists, horse riders, horse drawn vehicles and pedestrians walking in the road (for example, where there is no pavement), at least as much room as you would when overtaking a car. Drivers should take extra care and give more space when overtaking motorcyclists, cyclists, horse riders, horse drawn vehicles and pedestrians in bad weather (including high winds) and at night.	
ODD attributes relevant to rule	• Weather (ice/snow/rain/high winds) • Time of day • Presence of motorcyclist, cyclist, horse rider, horse drawn vehicles and pedestrians in lane
DDT (OEDR) performance relevant to rule	• Passing distance - "giving more space" in bad weather • "taking extra care"
Performance metric and threshold requirements	• Proximity to object during passing manoeuvre • Different thresholds for operation during bad weather

Table 5 summarises the results of the analysis for the 165 identified LSAV relevant rules within the GB Highway Code. It shows that compliance with 97% of the rules requires the AV to have knowledge about either the DDT performance or the ODD attributes (or both). It also shows that compliance for 90.3 % of the rules can be monitored with a performance metric calculable by an AV.

Table 5.
Summary results of traffic rules analysis for 165 LSAV relevant UK Highway Code rules identifying which rules require DDT elements, ODD attributes and performance metrics to assess rule compliance.

Rule attributes	No of rules	Percentage %
Total LSAV relevant rules	165	100 %
Specifies DDT elements only	41	24.8 %
Specifies DDT and ODD attributes	119	72.2 %
Does not specify any DDT or ODD elements	5	3 %
Monitored via OEDR performance metric and threshold	149	90.3 %

OEDR requirements and ODD attributes are both datasets collected by an AVs perception module as part of normal operation and used as an input into the planning module. Since this data must be collected for functional operation of the AV, it is proposed that this data also be made available for monitoring compliance with traffic rules. As this data is extracted from the AV prior to OEDR planning, it provides an output of how the AV perceives the world, and is the information used by the AV for its decision making and planning OEDR execution. By processing this data independently from the ADS, it is possible to establish the desired OEDR performance which can be compared to the actual performance. By doing this it is possible to determine potential non-compliance as a result of improper OEDR performance. This processing can feasibly be conducted onboard the vehicle in real-time so that safety critical rule infractions can be detected as they occur and used as trigger events for more comprehensive data recording. It is recommended that the manufacturer's safety case should outline what data is collected and how it is used for assessing OEDR performance.

An ADS does not need to explicitly classify rule relevant ODD and DDT elements in order to drive safely and comply with traffic rules and it is known that some ADS solutions do not have this capability. For example, an AV may overtake all other road users with a clearance of 2.5 metres. Rather than classifying the object and selecting a more specific clearance, broad compliance with this element of the Highway Code rules has still been achieved.

Manufacturer Defined Monitoring Processes

It is common good practice with safety case development to ensure a process by which the arguments and assumptions made in the safety case are monitored. In line with this practice, it is proposed that manufacturers develop a monitoring plan that is evidenced within the safety case. The monitoring plan should evidence that there are processes in place to collect and investigate data in line with the minimum dataset specification as well as any additional processes required to monitor continued compliance with the safety case. A key part of monitoring for safety arguments will be to test the assumptions made in the safety case around the presence of hazards, and the effectiveness of the proposed mitigations. To this end, manufacturer defined monitoring processes should seek to understand:

- The occurrence of unmitigated hazards and partially mitigated hazards.
- The occurrence of hazards that have been accepted without mitigation.
- Violations of assumptions, design goals, and conclusions made based on an evaluation of evidence made in the safety case.
- Manufacturers should be encouraged to identify further measures and other monitoring approaches to ensure tolerable coverage and evidence this as part of their safety case.

Operational Monitoring Approaches

The HARA showed that both leading and lagging measures and monitoring of traffic/safety rules accounted for a considerable amount of safety relevant events but identified certain hazards which could not be monitored. Notably risks caused by a failure to detect objects were identified as being impossible to monitor using the monitoring methods proposed, as they all rely on data collected by the vehicle. In order to account for this, it is proposed that operational monitoring mechanisms should be integrated into in-use monitoring and reporting processes in order to widen the coverage of possible risk events. Three mechanisms are proposed below and would fall under the responsibility of the LSAV operator.

Maintenance and inspection Operators of current fleets have a responsibility to develop and operate processes for walkaround checks, maintenance and inspection of their vehicles. The purpose of these processes is to identify and remedy any vehicle faults prior to operation to minimise risk. It was found that reports made through these processes could be incorporated into a monitoring system. These processes could provide context on issues with the vehicle that may not have been internally detected, such as sensor that appears to function but is not calibrated accurately to detect objects and so provide context to events that could have previously happened but weren't detected, or reasons as to why an event happened that were not considered in internal monitoring. It could also uncover previously unseen damage that triggers a review of data to investigate the time during operation when the damage occurred.

Public feedback It is proposed that service operators maintain a mechanism for public feedback and outline their processes. Oversight for this could be achieved through a mechanism of deployment licensing and the regulator would be expected to sample public reports made to operators to ensure they are handled appropriately. This work specifies that a public feedback mechanism should be in place that allows eyewitnesses and passengers to report unsafe events to the operator. Since the scope of this work considers vehicles that have no driver who is usually legally responsible for reporting a collision, witness or passenger reporting is thought to be an effective redundancy for detecting events that supports vehicle data led approaches. Limitations are foreseen with this system, however. Members of the public may report significant amounts of irrelevant events since they do not know what constitutes a safety relevant event. This could lead to unnecessary burdens on the operator. It is recommended that public reports be used to trigger a review of operational data that then may trigger further investigation and reporting. It would be expected that the processes for handling public reports, disregarding false reports, and investigating genuine events be defined and evidenced by the operator.

Police and enforcement reports In the immediate term, traffic events are expected to be reported to the police as with conventional vehicles, including through witness testimony and collision reports. Furthermore, speed cameras and other enforcement infrastructure may also identify an issue. It is recommended that once the police identify that an AV was involved, then the responsible party for the AV would be notified who would have a duty to report to the regulator. We expect operators would use the reports as a trigger to conduct their own investigation in collaboration with the AV manufacturer as required.

Recall Data

The purpose of data recall is to provide data that supports investigation of an event to determine its causes as well as any corrective action required to prevent future occurrences. This work proposes primarily event-based data capture whereby a comprehensive set of data is collected by the vehicle when an event is detected. This method means that only data relevant to the event in question is captured. However, it was found that some degree of continuous data collection is required.

Continuously transmitted data This data is not associated with any event identified by the vehicle. As a result, it can provide data for a basic risk evaluation if a risk event is reported where an ADS may not be aware of it. However, because data needs to be continuously transmitted, there are limits on the amount of data that can collected before its capture and storage becomes economically and practically unfeasible. As a result, it cannot support detailed investigation of safety events to understand their causes. It is proposed that a minimal dataset be collected continuously. This may be stored on the vehicle or transmitted elsewhere. The primary purpose of this dataset will be to provide basic risk analysis and liability determination in situations where no other data is recorded. A continuously transmitted dataset is proposed in Table 6, which is based on commercial telematics systems.

Table 6.
List of data elements proposed for continuous collection during LSAV operation to enable basic risk and liability determination.

Data elements	Values
Continuous transmission	
Vehicle telemetry	GPS, speed, gyroscopes, accelerometers, telemetry accuracy and quality measurement
Values transmitted upon state change	
Autonomous systems	Operating status change and override events
Door, boot, window and hood status	Open/closed/locked/position/status
Horn and light operations	On/off/low beam/high beam/flash/fog/hazard, accuracy and quality measurement
Vehicle dynamics and safety systems	ABS pre-charge, forward collision warning, stability and traction control, etc.
Crash restraint and seat sensors	Status, occupancy, accuracy and quality measurements
Wipers	Speed/state/front/rear/accuracy and quality measurement
Trailer / wheelchair ramp / assistive systems	Trailer/wheelchair ramp/assistive systems - status/ detection
Ignition control	Interaction and operation of ignition and auto/start-stop technologies or in the case of EVs engine on and off.

Event data recall The purpose of comprehensive data recall is to provide data that supports investigation of the event to determine its cause as well as any corrective action required to prevent future occurrences. Broadly, it is proposed that a requirement is placed on the manufacturer to store and share all data necessary to the regulator to enable investigation upon a trigger event. This work found that it is not possible to specify this data completely as the data required would be manufacturer-specific and dependent upon the configuration of sensors, compute and software used. Rather than specifying the exact sensors, data rates and formats for this, the manufacturer should define what data is recalled as part of a monitoring plan that is submitted prior to deployment. A minimum dataset has also been defined that is to be recalled following a trigger of leading and lagging measure triggers. This minimum dataset is defined in Appendix B. This is to create a basic standardised data set for collection within the framework that is technology agnostic and enables fundamental event investigation. This also ensures similar data is being captured across manufacturers to enable identification of safety themes. Manufacturers would be expected to assure regulators that the minimum dataset is being captured in addition to any further data defined by the manufacturer as necessary.

Reporting to Regulator

It is proposed that the scope of reportable occurrences should align with best practice from aviation. In addition, this framework aims to support continued validation of the safety performance declared pre-deployment and monitor ongoing compliance. As such, manufacturers and operators should be required to report:

- Any occurrence which endangers or which, if not corrected, would endanger the AV, its occupants or any other person.
- Any occurrences or set of occurrences that indicates an actual or potential violation of the safety case or safety performance declared at prior to deployment
- Any occurrence which violates road traffic or other laws (such as data privacy)

Sub definitions for events in scope of this scheme have been developed under this project and are summarized in Table 7. These event classifications are intended to allow compliance monitoring of the AV as well as code events to generate data for comparative assessment of safety performance across an AV fleet.

Table 7.
Definitions for proposed event classifications used for trend analysis.

Event	Definition
Collision	An incident in which the LSAV makes contact with an object, either moving or fixed, at any speed, in which kinetic energy is measurably transferred or dissipated. Includes other vehicles, roadside barriers, objects on or off the roadway, pedestrians, cyclists, or animals.
Near-collision	Any circumstance that requires a rapid, evasive manoeuvre by the LSAV (or any other vehicle, pedestrian, cyclist, or animal) to avoid a collision. A rapid, evasive manoeuvre is defined as steering, braking, accelerating, or any combination of control that is significantly greater than that expected in normal operation.
Safety critical event	Any circumstance that requires a collision avoidance response on the part of the LSAV or any other vehicle, pedestrian, cyclist, or animal that is less severe than a rapid evasive manoeuvre but greater in severity than a normal operation to avoid a crash. A collision avoidance response can include braking, steering, accelerating, or any combination of control inputs.
Proximity conflict	Any circumstance resulting in extraordinarily close proximity of the LSAV to any other vehicle, pedestrian, cyclist, animal, or fixed object when, due to apparent unawareness on the part of the vehicle, driver, pedestrians, cyclists or animals, there is no avoidance manoeuvre or response. Extraordinarily close proximity is defined as a clear case in which the absence of an avoidance manoeuvre or response is inappropriate for the driving circumstances (e.g. speed, sight, distance, etc.).
Non-conflict critical incident	Any event that increases the level of risk associated with driving but does not result in any of the events as defined above.
Safety-relevant infraction	Road rule violations that have direct safety implications even if another event type (e.g. collision, near collision etc.) does not occur.
Traffic infraction	Road rule violations not directly related to safety but that negatively impact the flow of traffic or safe movement of other road users.

Individual event reporting The reporting of safety critical incidents such as collisions is required in regulatory schemes in other transport modes and is common practice in the aviation industry. The purpose in aviation is to ensure relevant information on safety is reported, collected, stored, protected and disseminated with the prevention of accidents and incidents as the sole priority. It is recommended that a similar approach be adopted for reporting be adopted for an in-use monitoring framework. It is proposed that individual reports be made for:

- Lagging measures (see Table 2) – their low frequency would inhibit statistical evaluation, but their high data availability allows in depth analysis.
- Police reported events such as traffic infractions – where the regulator would require the manufacturer to investigate the event.
- Events not recorded by the event data capture system but detected through other processes – indicating there is a potential failure
- Any other event requested by the regulator – For instance, where the regulator receives significant public complaints.

Individual event reports should be underpinned by case study analysis with the approach for investigating and analysing events detailed within a manufacturer's Safety Management System. The broad requirement set is that the event reports should display sufficient information required for the regulator to understand the nature and cause of the event. It is also recommended that collisions be reported to the regulator immediately after identification in order to enable the regulator to manage crisis communications and media reporting as this was found to be required to maintain public confidence in the regulator.

Aggregated data reports The purpose of collecting aggregated datasets is to enable statistical evaluation in order to evaluate safety performance over time. This is to identify trends in safety performance that may be inconsistent with the safety performance expected prior to deployment. It is proposed that aggregated data sets of the rate of occurrence of leading and lagging measures be reported to the regulator. This includes the measures defined by the data set as well as any others required by the manufacturer for safety case compliance monitoring.

Aggregated data should detail:

- The event partner and the category of event
- The number of false positives and confirmed events to determine the suitability of selected thresholds
- The number of confirmed events investigated to root cause and their conformance with the safety arguments stated within the safety case
- The relevant crash characteristics that could inform blame determination. For example: The ego vehicle is hit from behind at a stop sign would by default be blamed on the trailing vehicle. An elevated rate of not-blamed loss events could still be indicative of safety issues, such as the AV behaving in a manner that provokes mistakes by human drivers.
- The demographic of involved parties. This is intended to identify patterns is safety performance for different user groups. For example, this may identify biases in machine learning training sets or defects in ODD construction so that they can be corrected.

Reporting frequency It is proposed that reporting occur in two ways; periodically, and immediately following certain events. Periodic reporting would be at a fixed interval (e.g., every six months) and its purpose would be to report the aggregated data. Reactive reporting would take place as soon as collected data (either aggregated data or case studies) provides evidence of an inconsistent ADS behaviour compared to the safety performance claims made prior to market introduction, or when collected data provides evidence of degradation of safety performance). It is also recommended that collisions be reported to the regulator immediately in order to enable the regulator to manage crisis communications and media reporting to ensure public confidence in the regulator.

Regulator Assessment and Sanctions

Once in-use monitoring detects a safety issue, it will be necessary for the regulator to determine the most appropriate corrective action. It is proposed that rather than punitive criminal action, the regulator should have access to a gradated system of enforcement actions, similar to aviation authorities. It was found in this work that the proposed in-use monitoring data is a desirable data source for regulators to be able to understand the extent and nature of the failure and the potential risk of recurrence which would enable them to take an evidence-based decision on the fairest and most proportionate level of corrective action to apply. It is proposed that any regulatory system for enforcement be based on evidence gathered through in-use monitoring. Fair and appropriate sanctions, rather than cautious and severe ones, are expected to reinforce an open and transparent safety culture that promotes proactive reporting to the regulator. Manufacturers and operators both have responsibilities for ensuring safety. As such, it is proposed that sanctions can be applied to both parties if necessary for the interest of public safety.

DISCUSSION AND LIMITATIONS

This study proposes a framework for in-use monitoring to assess the safety performance of automated vehicles. This novel framework proposal is intended to be used to support ongoing safety assurance on behalf of a regulator responsible for ensuring the safety of AVs throughout their deployment lifetime. However the overall approach is consistent with best practice safety management and is applicable to AV manufacturers and operators outside of a regulatory scheme. The proposals made in this framework are novel in that there is no currently comparable mechanism of in-use monitoring for conventionally driven road vehicles. However, this study found that other transport sectors, notably aviation, had mature safety assurance processes that promotes a culture of shared learning and prioritising safety above all else. The principles of knowledge sharing, open and transparent data collection, reporting practices and evidence based regulatory enforcement are all good practice approaches used in aviation have been adapted for this framework. While based in good practice of other sectors, there is limited practical evidence to determine whether it remains feasible for automated vehicles.

The scope of this framework was primarily (although not solely) focused on LSAV use cases as these were likely to be some of the earliest use cases adopted. As a result, it remains to be seen as to whether the proposed approaches are scalable and adaptable to other use cases. It is noted however that the proposed framework is largely independent on specific ODD attributes, use cases, and operating contexts that would limit its applicability to other use cases. One limitation noted is that the proposed framework is reliant on the existence of a fleet service operator who has responsibilities to cooperate with manufacturers, and to collect and report data. There is no equivalent entity for privately owned Automated Vehicles, instead having to pass some or all of this responsibility to the driver. Nevertheless, much of the data elements needed for assurance are likely to be transferable.

This study proposes that the wealth of data collected by automated vehicles during operation can and should be utilised for the purposes of ongoing assurance. It is anticipated that event-based data capture be the primary method of collecting data as continuous capture of all the data required to support event investigation would be inefficient and largely unfeasible. Much of the data required by the proposed scheme is already being collected and utilised for existing processes such as current event data recorders, telematics-based insurance models and fleet monitoring. However, due the paucity of automated vehicle collision data, it is not possible to determine the value and usefulness of collecting the proposed datasets. A principle of continuous improvement is proposed such that the accuracy, quality and relevance of the monitoring framework is assessed through AV deployment.

This work has shown that monitoring for compliance with traffic rules requires data to be collected on ODD attributes, DDT (OEDR) requirements and performance metrics relevant to the rule. As such a method of continuous rule compliance assessment is recommended by independently processing the data and comparing against real-time AV performance. As this relies solely on datasets only available to automated vehicles, there is limited evidence to suggest the ease and practicality of collecting and processing such data. However, the data required for this is the same dataset required for safe AV operation.

CONCLUSION

This independent study proposes a framework for the safety performance assessment of AVs during operation to provide oversight, accountability and improve public trust in the technology. The proposed framework is based on the principle of leveraging the data collected by automated vehicles during normal operation to assess and validate the safety performance of the AV against the performance expected prior to deployment. The study outlines the data elements necessary to support ongoing assurance and investigation of incidents as well as the administrative and technical processes and procedures necessary for sharing and reporting safety learnings to drive improvements in the nascent automated vehicle industry.

ACKNOWLEDGMENTS

The authors wish to acknowledge the United Kingdom's Department for Transport for funding this study. The findings and recommendations do not necessarily reflect the views of the UK Department for Transport and will not necessarily be implemented in future AV safety assurance requirements.

REFERENCES

[1] HM Government, *Connected and automated mobility 2025: Realising the benefits of self-driving vehicles in the UK* (2022). London. Retrieved December 11, 2022, from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1099173/cam-2025-realising-benefits-self-driving-vehicles.pdf.

[2] Informal Working Group (IWG) on Validation Methods for Automated Driving (VMAD) 2022, *New Assessment/Test Method for Automated Driving (NATM) Guidelines for Validating Automated Driving System (ADS) – amendments to ECE/TRANS/WP.29/2022/58.* Available at: https://unece.org/sites/default/files/2022-05/GRVA-13-35e.pdf

[3] United Nations, *E/ECE/TRANS/505/Rev.3/Add.159, UN Regulation No.160 Uniform provisions concerning the approval of motor vehicles with regard to the Event Data Recorder* (n.d.). Retrieved December 11, 2022, from https://unece.org/sites/default/files/2021-10/R160e%20_0.pdf.

[4] HM Government. (2022). *The Highway Code*. Retrieved December 11, 2022, from https://www.highwaycodeuk.co.uk/

[5] HM Government Department for Transport. (2022, June 28). Government launches country's first ever investigation branch focused on Road Safety. GOV.UK. Retrieved December 11, 2022, from https://www.gov.uk/government/news/government-launches-countrys-first-ever-investigation-branch-focused-on-road-safety

APPENDIX A

A summary of the reviewed proximity and safety-envelope calculation metrics is given below:

- **Time to Collision (TTC).** A calculated time to collision between objects if each object continued on current trajectory and speed.
- **Time Exposed Time-to-Collison (TET**). A summation of TTC values (above) over a windowed time period – used to smooth uncertainty in TTC distance and speed estimations.
- **Time Integrated Time-to Collision (TIT).** An integral of TTC values when below a threshold – used in microscopic level traffic simulations.
- **Modified Time-to-Collision (MTTC).** This approach considers possible acceleration changes in objects to present a worst case scenario TTC where speed can increase.
- **Crash Index (CI).** This is a severity index measured by pairs of moving objects kinetic energy differences – used to understand potential crash severity but can be used to minimise strong differential speed risk scenarios.
- **Headway (H).** The elapsed time between following vehicles passing reference locations – used in lane following to associate risk from unsafe stopping distances in following traffic.
- **Time to Accident (TA).** The time until a vehicle would have had an accident had either it or another vehicle not taken evasive speed or direction change already occurred – a what if scenario for risk proximity if no action had been taken to calculate proximity to a realised accident.
- **Post Encroachment Time (PET).** The time between when one road users leaves a potential collision risk area and another enters it – used typically in junction safety understanding.
- **Potential Index for Collision with Urgent Deceleration (PICUD**). The distance between two vehicles if both undergo urgent deceleration – used in some lane changing and merge safety algorithms.
- **Margin to Collision (MTC).** A ratio of the ego and following vehicles stopping distances when following a lead vehicle - used in close following deceleration understanding not just forward but also rear collision potential.
- **Difference of Space Distance and Stopping Distance (DSS).** A difference between stopping distance and actual distance – used to understand degrees of safe operation in following traffic.
- **Time Integrated DSS (TIDSS).** A time integrated DSS (above) approach that factors in duration of risk exposure into its formulae.
- **Deceleration Rate to Avoid the Crash (DRAC).** A declaration indicator looking at differential speeds and closing distance ratios to look for unsafe deceleration when more is required – used in some ADS safety systems.
- **Crash Potential Index (CPI).** An extension of DRAC (above) that considers future time events and potential to exceed a vehicle maximum deceleration rate – used in some ADS safety systems.
- **Criticality Index Function (CIF).** A potential risk severity measure combining vehicle speed with required deceleration – used to indicate a potential severity for a speed and needed deceleration for any impact at a point in time, used in some ADS safety systems.

APPENDIX B

Table 8.
Recommended data elements for recall following trigger of lagging measures including reasoning for inclusion in the minimum dataset

Data element	Recording interval/time (relative to time zero)	Data sample rate (per second)	Minimum range	Accuracy	Resolution	Event (s) recorded for
Delta-V, longitudinal	0 to 250 ms or 0 to End of Event Time plus 30 ms, whichever is shorter.	500	-100 km/h to + 100 km/h.	±10%	1 km/h.	Planar VRU Rollover
				REASONING: This data field provides fine grained velocity change data allowing reconstruction of kinetic energy exchange in a longitudinal direction. Not required if longitudinal acceleration recorded at ≥500 Hz with sufficient range and resolution to calculate delta-v with required accuracy		
Maximum delta-V, longitudinal	0–300 ms or 0 to End of Event Time plus 30 ms, whichever is shorter.	NA	-100 km/h to + 100 km/h.	±10%	1 km/h.	Planar VRU Rollover
				REASONING: This data field provides a single peak value (helping to inform any incident severity) from fine grained velocity change data allowing severity estimation in a longitudinal direction. Not required if longitudinal acceleration recorded at ≥500 Hz.		
Time, maximum delta-V, longitudinal	0–300 ms or 0 to End of Event Time plus 30 ms, whichever is shorter.	NA	0–300 ms, or 0-End of Event Time plus 30 ms, whichever is shorter.	±3 ms	2.5 ms.	Planar VRU Rollover
				REASONING: This data field provides a single timestamp value helping to indicate when in the sample the maximum severity impact occurred in reference to time zero trigger. Not required if longitudinal acceleration recorded at ≥500 Hz.		
Speed, vehicle	-5.0 to 0 sec	2	0 km/h to 250 km/h	±1 km/h	1 km/h.	Planar VRU Rollover
				REASONING: Providing operating speed to enable understanding of overall kinetic energy in precursor to time zero trigger events.		
Motor Transition Demand	-5.0 to 0 sec	2 (or more frequent as possible to record)	0 to 100%	±5%	1%	Planar VRU Rollover
				REASONING: To determine precursor motor transition changes and vehicle motion intention prior to the event.		
Service brake Demand	-5.0 to 0 sec	2 (or more frequent as	0 to 100%	±5%	1%	Planar VRU Rollover
				REASONING: To determine precursor braking		

		possible to record)		operation of the vehicle prior to the trigger event.		
Ignition/start cycle, crash	-1.0 sec	N/A	0 to 60,000	±1 cycle	1 cycle.	Planar VRU Rollover
				REASONING: To determine recorded trigger events by journey cycles to understand power/ignition on/off cycles.		
Ignition/start cycle, download	At time of download	N/A	0 to 60,000	±1 cycle	1 cycle.	Planar VRU Rollover
				REASONING: To determine additional vehicle usage following a trigger event.		
Occupant protection system deployment, time to deploy, in the case of a single stage air bag, or time to first stage deployment, in the case of a multi-stage air bag(s)	Event	N/A	0 to 250 ms	±2ms	1 ms.	Planar VRU Rollover
				REASONING: To detail deployment times for safety systems fitted. Needed to determine effectiveness of mitigations vs. injury in the event of a trigger		
Multi-event crash, number of events	Event	N/A	1 or more	N/A	1 or more.	Planar VRU Rollover
				REASONING: To detail the potential of multiple trigger events in temporal proximity, each adding insight about incidents with multiple impacts or triggers occurring.		
Time from event 1 to 2	As needed	N/A	0 to 5.0 sec	±0.1 sec	0.1 sec.	Planar VRU Rollover
				REASONING: To detail the potential of multiple trigger events in temporal proximity, each adding insight about incidents with multiple impacts or triggers occurring.		
Complete file recorded	Following other data	N/A	Yes or No	N/A	Yes or No.	Planar VRU Rollover
				REASONING: To detail the potential of incomplete recording due to device or sensor damage making expected data unavailable. Indicates mechanical failure of incident recording means in an incident.		
Lateral acceleration (post-crash)	0–250 ms or 0 to End of Event Time plus 30 ms, whichever is	500	-50 to +50g	± 10%	1 g	Planar VRU Rollover
				REASONING: To allow forensic reconstruction post trigger of any side impact.		

	shorter.					
Longitudinal acceleration (post-crash)	0–250 ms or 0 to End of Event Time plus 30 ms, whichever is shorter.	500	-50 to +50g	± 10%	1 g	Planar VRU Rollover
				REASONING: To allow forensic reconstruction post trigger of any front/rear impact.		
Normal acceleration (post-crash)	0–300 ms or 0 to End of Event Time plus 30 ms, whichever is shorter. (This is still under debate and subject to change)	10 Hz	-5 g to +5 g	± 10%	0.5 g	Planar VRU Rollover
				REASONING: Details the downward acceleration (typically gravity) of a vehicle. Is used to determine in any trigger any up-down acceleration of a vehicle which helps forensic reconstruction.		
Delta-V, lateral	0–250 ms or 0 to End of Event Time plus 30 ms, whichever is shorter.	100	-100 km/h to + 100 km/h.	±10%	1 km/h.	Planar VRU Rollover
				REASONING: The cumulative change in velocity in lateral direction that helps to understand kinetic energy transfer in any side impact. Not required if lateral acceleration recorded at ≥500 Hz and with sufficient range and resolution to calculate delta-v with required accuracy.		
Maximum delta-V, lateral	0–300 ms or 0 to End of Event Time plus 30 ms, whichever is shorter.	N/A	-100 km/h to + 100 km/h.	±10%	1 km/h.	Planar VRU Rollover
				REASONING: The highest change value in side velocity during the trigger data capture period. Allows to understand peak severity of side impacts. Not required if lateral acceleration recorded at ≥500 Hz.		
Time maximum delta-V, lateral	0–300 ms or 0 to End of Event Time plus 30 ms, whichever is shorter.	N/A	0–300 ms, or 0-End of Event Time plus 30 ms, whichever is shorter.	±3 ms	2.5 ms.	Planar VRU Rollover
				REASONING: The time point of the highest side velocity change in the monitoring trigger window. Not required if lateral acceleration recorded at ≥500 Hz.		
Time for maximum delta-V, resultant.	0–300 ms or 0 to End of Event Time plus 30 ms, whichever is shorter.	N/A	0–300 ms, or 0-End of Event Time plus 30 ms, whichever is shorter.	±3 ms	2.5 ms.	Planar VRU Rollover
				REASONING: The time from the trigger point (time zero) to the maximum velocity change recorded. Used to understand the point of highest severity in relation to the trigger point aiding forensic reconstruction. Not required if relevant acceleration recorded at ≥500 Hz		
Engine/Motor rpm	-5.0 to 0 sec	2	0 to 10,000 rpm (or high maximum rpm	±100 rpm10	100 rpm.	Planar VRU Rollover

			as needed for the vehicle type)	REASONING: details the number of revolutions per minute of the engine/motor output (in fuel driven vehicles via the crankshaft, in electric vehicles the output rotations of the device applying motive power). This details the engine/motor operating speed in the approach to the trigger event.		
Vehicle roll angle	-5.0 to 5.0 sec	10	-1080 deg to + 1080 deg.	±10%	10 deg.	Rollover
				REASONING: vehicle rollover events being considered this indicates the degree of roll observed in the trigger window. These values can be used in crash reconstruction.		
Anti-lock braking system ABS activity	-5.0 to 0 sec	2	Faulted, Non-Engaged, Engaged Active, Intervening	N/A	Faulted, Non-Engaged, Engaged Active, Intervening	Planar VRU Rollover
				REASONING: If fitted, the status of anti-lock braking pre trigger can help to understand anti-lock braking behaviour in any rapid velocity change before the trigger event.		
Stability control	-5.0 to 0 sec	2	Faulted, On, Off, Engaged Intervening	N/A	Faulted, On, Off, Engaged Intervening	Planar VRU Rollover
				REASONING: If fitted, the status of stability control pre trigger can help to understand stability control status in any rapid velocity change before a trigger event.		
Digital requested Steering input	-5.0 to 0 sec	2	-250 deg CW to + 250 deg CCW.	±5%	±1%.	Planar VRU Rollover
				REASONING: Requested steering input prior to the trigger helps to determine any potential collision avoidance activity or swerving behaviour.		
Safety belt status	-1.0 sec	N/A	Fastened, not fastened	N/A	Fastened, not fastened	Planar VRU Rollover
				REASONING: If fitted, the status of any passenger restraint system has impacts in any trigger events resulting in physical injury.		
Occupant protection systems deployment, time to nth stage,	Event	N/A	0 to 250 ms	±2 ms	1 ms.	Planar VRU Rollover
				REASONING: If fitted the deployment time of multi-stage occupant protection system deployments required to understand the relationship to the ability to mitigate injury in a realised risk incident.		
Occupant size classification , any passenger	-1.0 sec	N/A	6yr old HIII US ATD or Q6 ATD or smaller	N/A	Yes or No.	Planar Rollover
				REASONING: If monitored, seat weight sensors help to understand impact injuries and effectiveness of any fitted restraint systems.		
Automated Driving System Status	[-30.0] to +30.0 second relative to time zero	2	N/A	N/A	On, Off - Manually Deactivated, Off-Automatically	Planar VRU Rollover

					Deactivated Faulted	
				REASONING: To detail the operating status of any automated driving system (one for each possible in the vehicle) to understand the status in connection to an incident as automated vs non automated will require differing handling and statistical aggregation of events.		
Automated Driving System - Minimal Risk Manoeuvre	[-30.0] to +30.0 second relative to time zero	2	N/A	N/A	Yes or No	Planar VRU Rollover
				REASONING: To detail any activation of MRMs in relation throughout a trigger window.		
Automated Driving System - Override	[-30.0] to +30.0 second relative to time zero	2	N/A	N/A	List of possible overrides	Planar VRU Rollover
				REASONING: To detail any listed override events halting automated driving each record gives the reason behind any unplanned disengagement activity that can have safety impacts.		
Latitude	[-30.0] to +30.0 seconds relative to timezero	1 or higher	World Geodetic System 1984 (WGS84)	WGS84 standard error ranges	WGS84 standard ranges	Planar VRU Rollover
				REASONING: Geopositioning may present GDPR challenges for allowable processing however it is vital to understand locational risk and relation to external factors. The course and trajectory understood also have high value in understanding risk scenarios. This collation is recommended within law commission consultations as well as the Insurance Industry to enable liability determination		
Longitude	[-30.0] to +30.0 seconds relative to timezero	1 or higher	WGS84	WGS84 standard error ranges	WGS84 standard ranges	Planar VRU Rollover
				REASONING: Geopositioning may present GDPR challenges for allowable processing however it is vital to understand locational risk and relation to external factors. The course and trajectory understood also have high value in understanding risk scenarios. This collation is recommended within law commission consultations as well as the Insurance Industry to enable liability determination		
All trigger status	[-30.0] to +30.0 seconds relative to timezero	2	N/A	N/A	List of possible trigger types	Planar VRU Rollover
				REASONING: To capture trigger events timing and type throughout the trigger capture period.		
Operating environment static and mobile objects, relative position,	[-10.0] to +10.0 seconds relative to timezero	10	[-50.0m] – [+50.0m] relative position to centre of LSAV (nearest objects)	Relative position	Position used in LSAV decision making	Planar VRU Rollover
				REASONING: To record observed relative object positions that the vehicle detects in near environment to enable reconstruction of third party object relative movements and positions		

longitudinal						
Operating environment static and mobile objects, relative position, lateral	[-10.0] to +10.0 seconds relative to timezero	10	[-50.0m] – [+50.0m] relative position to centre of LSAV (nearest objects)	Sensor estimate position	Position used in LSAV decision making	Planar VRU Rollover
				REASONING: To record observed object positions that the vehicle detects in near environment to enable reconstruction of third party object relative movements and positions		
Operating environment static and mobile objects, speeds, (nearest ‘x’ objects)	[-10.0] to +10.0 seconds relative to timezero	2	0 km/h to 250 km/h	As per accuracy of observed speeds	As per accuracy of observed speeds	Planar VRU Rollover
				REASONING: To record observed object relative speeds that the vehicle detects in near environment to enable reconstruction of third party object relative movements and positions		
Operating environment static and mobile objects, trajectory	[-10.0] to +10.0 seconds relative to timezero	2	[-180.0] to +180.	As per accuracy of observed trajectory	As per accuracy of observed trajectory	Planar VRU Rollover
				REASONING: To record observed object relative bearing that the vehicle detects in near environment to enable reconstruction of third party object relative movements and positions		
Operating environment static and mobile objects, classification	[-10.0] to +10.0 seconds relative to timezero	2	[static, vehicle, VRU, Moving unknown]	As per accuracy of observed object classification	As per accuracy of observed object classification	Planar VRU Rollover
				REASONING: To record observed object types that the vehicle detects in near environment to enable reconstruction of third party object relative movements and positions.		

Table 9.
Recommended data elements for recall following trigger of leading measures

Data element	**Condition for requirement**	**Recording interval/time (relative to time zero)**	**Data sample rate (per second)**	**Minimum range**	**Accuracy**	**Resolution**
Delta-V, longitudinal	Mandatory	-100 to 200 ms	50	-100 km/h to + 100 km/h.	±10%	1 km/h.
Speed	Mandatory	-10.0 to 10.0 sec	50	0 km/h to 250 km/h	±1 km/h	1 km/h.
Delta-V, lateral	Mandatory	-100 to 200 ms	50	-100 km/h to + 100 km/h.	±10%	1 km/h.
Automated Driving System Status	Mandatory	-10.0 to +10.0 second relative to time zero	2 (or event based upon change)	N/A	N/A	On, Off - Manually Deactivated, Off- Automatically

						Deactivated Faulted
Automated Driving System - Minimal Risk Maneuver	Mandatory	-10.0 to +10.0 second relative to time zero	2 (or event based upon change)	N/A	N/A	Yes or No
Automated Driving System - Override	Mandatory	-10.0 to +10.0 second relative to time zero	2 (or event based upon change)	N/A	N/A	List of possible overrides
Latitude	Mandatory	-10.0 to +10.0 second relative to time zero	1 or higher as supported by LSAV and GPS update frequency	WGS84	WGS84 standard error ranges	WGS84 standard ranges
Longitude	Mandatory	-10.0 to +10.0 second relative to time zero	1 or higher as supported by LSAV and GPS update frequency	WGS84	WGS84 standard error ranges	WGS84 standard ranges
Satellite UTC time	Mandatory	Unsigned long – milliseconds since 1970	1	N/A	N/A	N/A
Operating environment static and mobile objects, relative position, longitudinal	If using proximity leading measures	[-10.0] to +10.0 seconds relative to timezero	10	[-50.0m] – [+50.0m] relative position to centre of LSAV (nearest objects)	Sensor estimate position	Position used in LSAV decision making
Bearing (gyroscope)	Mandatory	-10.0 to +10.0 second relative to time zero	1	[0.0 – 360.0]	+- 10 degrees	N/A
Operating environment static and mobile objects, relative position, lateral	If using proximity leading measures	[-10.0] to +10.0 seconds relative to timezero	10	[-50.0m] – [+50.0m] relative position to centre of LSAV (nearest objects)	Sensor estimate position	Position used in LSAV decision making
Operating environment static and mobile objects, speeds,	If using proximity leading measures	[-10.0] to +10.0 seconds relative to timezero	2	0 km/h to 250 km/h	As per accuracy of observed object speeds	As per accuracy of observed object speeds
Operating environment static and	If using proximity leading	[-10.0] to +10.0 seconds relative to	2	[-180.0] to +180.	As per accuracy of observed	As per accuracy of observed object

mobile objects, trajectory,	measures	timezero			object trajectories	trajectories
Operating environment static and mobile objects, classification,	If using proximity leading measures	[-10.0] to +10.0 seconds relative to timezero	2	[static, vehicle, VRU, Moving unknown]	As per accuracy of observed object classification	As per accuracy of observed object classification