MISRA SC

Uncovering the historical road safety argument

March 2025

First published March 2025 by The MISRA Consortium Limited
1 St James Court
Whitefriars
Norwich
Norfolk
NR3 1RU
UK

www.misra.org.uk

ISBN 978-1-911700-25-8 PDF

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library.

MISRA Mission Statement

We provide world-leading best practice guidelines for the safe and secure application of both embedded control systems and standalone software.

MISRA is a collaboration between manufacturers, component suppliers, engineering consultancies and academics which seeks to research and promote best practice in developing safety- and security-related electronic systems and other software-intensive applications.

To this end MISRA conducts research projects and publishes documents that provide accessible information for engineers and management.

MISRA also facilitates the dissemination and exchange of information between practitioners through supporting and holding technical events.

Disclaimer

Compliance with the requirements of this document, or any other standard, does not of itself confer immunity from legal obligations.

Acknowledgements

The MISRA SC Working Group

The MISRA Consortium would like to thank the following individuals for their significant contribution to the writing of this document:

David Blackburn	Rimac Technology
Helen Monkhouse	HORIBA MIRA Ltd
Roger Rivett	Independent Functional Safety Specialist

The MISRA Consortium also wishes to acknowledge contributions from the following individuals to the development and review process:

David Ward	John Botham	John Birch

Other acknowledgements

Contents

1 Introduction

The MISRA Safety Case working group published the *Guidelines for Automotive Safety Arguments* (GASA) [1] in September 2019. This document restricted its scope to the safety case argument required by ISO 26262 *Road vehicles — Functional safety* [2]. Since 2019, the working group has been responding to the automotive industry's work to produce vehicles with high and full driving automation. Our focus is safety which means the scope of this document is the prevention of harm to people. The aspiration of the group is to understand what will be necessary to produce a safety assurance argument for vehicles with high and full driving automation (i.e. SAE Levels 4 and 5 [5]).

In 2020 the working group published *A Structured Argument for Assuring Safety of the Intended Functionality (SOTIF)* [3], which introduced the concept of the 4-state model. This model is intended to help reason about completeness when defining behaviour in the context of SOTIF [7]. In 2022, Roger Rivett published *Public Road Transport and Vehicle Models* [4], which presents an ontology[1] of the whole public road transport system. This includes the physical road network and supporting infrastructure, the weather, users of the road network and their interactions with the external environment.

In April 2024, MISRA SC published the white paper *Safety assurance argument context for automated driving* [6]. This white paper provided an overall context within which a safety assurance argument for a vehicle with high or full driving automation has to be made. The white paper consisted of two potential contexts for driving automation. The first was personal transport viewed as a service, in which an Automated Driving System (ADS) equipped vehicle [5] would participate. This view includes all the aspects that contribute to the overall service. The second context addressed the complete vehicle lifecycle from development, through operation and maintenance, to decommissioning.

For both contexts, an ontology of the terms used in the subject matter was presented, and also a claim structure to show how a safety assurance argument could be made. The ontologies provide a definition of the terms used and the relationships between them. The claim structures suggest a possible top-level claim related to the avoidance of harm to people and shows how the claim could be supported. The concept of risk is not used at this stage. This only becomes necessary when product development standards are used, e.g. ISO 26262 [2], ISO 21448 [7].

The overall concern of this paper is the avoidance of vehicle accidents e.g. collisions; these are an obvious source of harm to people. It explores the historical implicit argument for road safety, the roles of the parties involved and the differences between manually driven and AD-equipped vehicles. This paper does not address measures to mitigate the severity of an accident after it has occurred; these will be common to both manually driven and automated vehicles. Other ways that a vehicle can cause harm to people, e.g. pollution, are not addressed in this document. While examples from the UK may be quoted, it is believed that these are indicative of the situation in most other countries.

[1] 'Ontology' — a set of concepts and categories in a subject area or domain that shows their properties and the relations between them

2 Pre-autonomy vehicle safe operation

This section considers the implicit safety argument for the case when the role of vehicle control authority is performed by a human driver and how the argument applies to the case where the role is performed by an ADS.

During the first 150 years or so of the use of vehicles on the public road, measures have been progressively developed to minimize the likelihood of a vehicle driven by a person being involved in an accident, and the severity of subsequent accidents should they still occur. The measures introduced are common in most developed countries and effectively define the baseline with which automated vehicles have to conform. These measures are the responsibility of a number of different parties, e.g. manufacturers, governments. While many of the measures adopted will be equally applicable to the case where the ADS performs the role of the vehicle control authority, the change from a person to a machine inevitably requires some changes to be made. The identification of the necessary and sufficient changes is a topic of ongoing work in the industry.

This document presents a simple model intended to include the majority of the measures, and the associated parties, that make up the overall approach that was established prior to the development of automated vehicles.

2.1 Model of road transport as a service

A previous MISRA white paper [6] introduced a model of personal transport on the public roads. This model has been enhanced in Figure 1, to support the discussion below. This is an application of the generic Public Road Transport System ontology presented in [4].

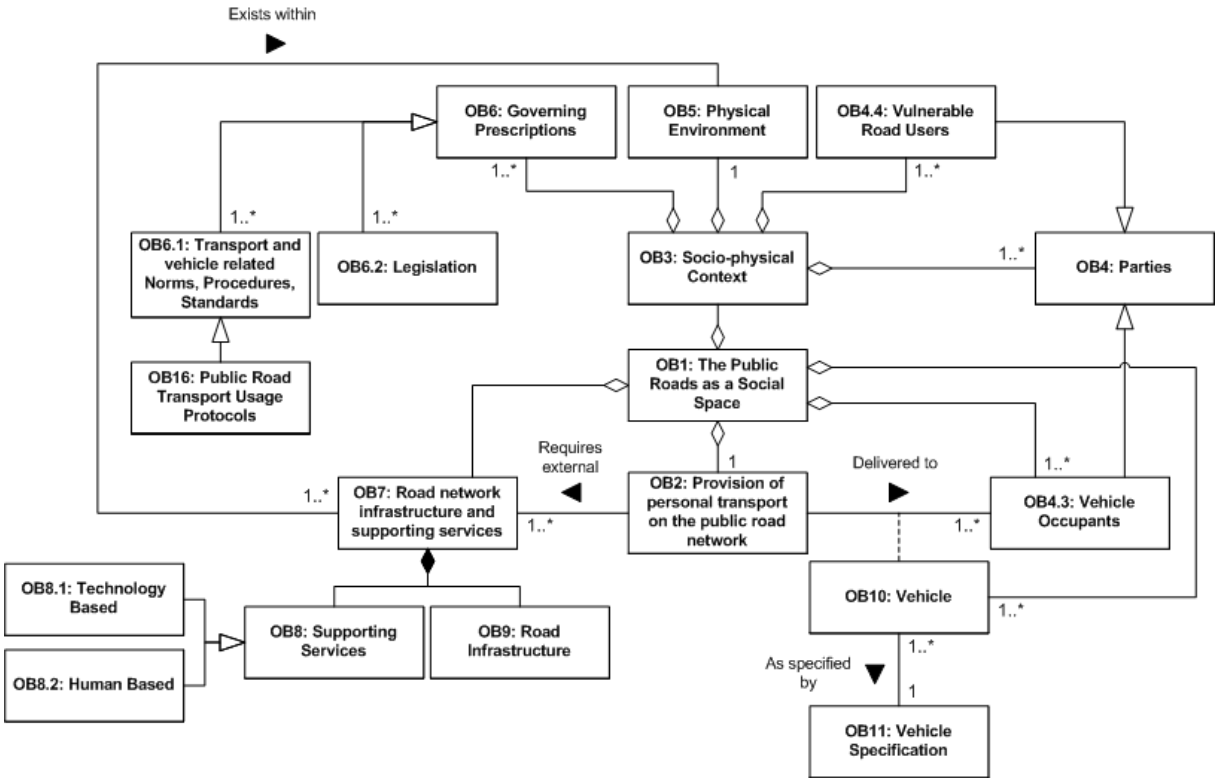

Figure 1: Enhanced model of personal transport on the public roads

The *parties* (OB4) block is further developed in Figure 2. This taxonomy is not claimed to be complete, but it is sufficient to allow an insight into the many different participants, both direct and indirect, who play a role in the provision of personal transport on the public road network.

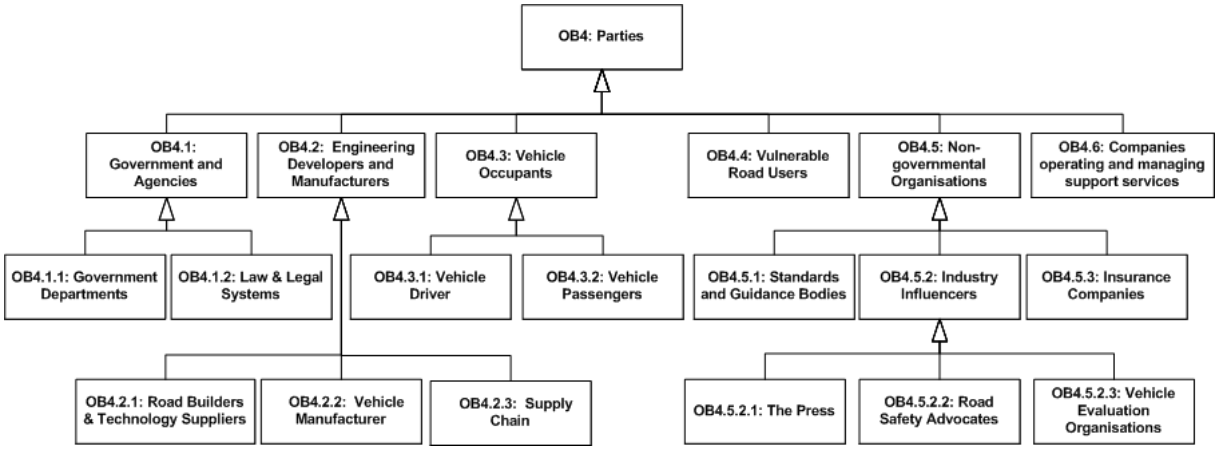

Figure 2: Parties involved in the provision of personal transport on the public road network

2.2 Roles and responsibilities of the parties

Each of the *parties* (OB4) has a role and/or a responsibility in the provision of personal transport on the public road network. Indicative examples of these are now given.

2.2.1 *Government and agencies* (OB4.1)

This describes the UK situation, including local government. Through its departments, the government plays a key part in facilitating road transport, e.g. it commissions new roads and road upgrades for the *road infrastructure* (OB9). It also commissions and permits or licenses the deployment of *supporting services*, e.g. highway control centres (OB8). It also runs road safety campaigns. The government is also responsible for the legal system which includes the provision of a driving licensing scheme, the enforcement of laws and the punishment of offenders (OB4.1.1 and OB4.1.2). It also passes legislation concerning vehicles, roads and supporting services.

2.2.2 *Engineering developers and manufacturers* (OB4.2)

The *vehicle manufacturer* (OB4.2.2) and *supply chain* (OB4.2.3) parties are responsible for the development of the *vehicle specification* (OB11) and production of the *vehicle* (OB10) and its components. The *vehicle manufacturer* provides the end product, which includes organizations that fit an ADS to a base vehicle. The *supply chain* provides the vehicle components which may also include manufacturers of the base vehicle.

The *road builders & technology suppliers* (OB4.2.1) are those that build and maintain the *road infrastructure* (OB9) and development and manufacture the *supporting services* (OB8), e.g. traffic-light control systems, street lighting.

2.2.3 *Vehicle occupants* (OB4.3)

The *vehicle occupants* (OB4.3) are the individuals who directly benefit from the service. In a manually driven vehicle, the *vehicle driver* (OB4.3.1) is responsible for taking actions that result in the behaviour of the *vehicle* (OB10) and they are also responsible for ensuring that the *vehicle* (OB10) is roadworthy before embarking on a journey. The correctness of the driver's actions are judged in UK law as being what would reasonably be expected of a driver. This applies to the behaviour of the car and the appropriateness of strict compliance with the laws of the road or the Highway Code [9] guidance.

2.2.4 *Vulnerable road users* (OB4.4)

Vulnerable road users (OB4.4) exist within the *socio-physical context* (OB3), and interact with the road infrastructure, but lack the physical protection of a vehicle. *Vulnerable road users* include pedestrians, cyclists and motorcyclists. See York PRTS model for a fuller model of some of the *socio-physical context* content, [4].

2.2.5 *Non-governmental organizations* (OB4.5)

Standards and guidance bodies (OB4.5.1) provide guidance as part of the *governing prescriptions* (OB6). These include guidance covering *road network infrastructure and supporting services* (OB7). *Industry influencers* (OB4.5.2) run campaigns, lobby governments, disseminate information and opinions via various media outlets. *Vehicle evaluation organizations* (OB4.5.2.3) perform their own independent assessments of the vehicle, e.g. Euro NCAP (The European New Car Assessment Programme). *Insurance companies* (OB4.5.3) set insurance premiums, which may affect the *vehicle specification* (OB11), e.g. the desire for a vehicle to achieve a Euro NCAP 5-star assessment.

2.2.6 *Companies operating and managing support services* (OB4.6)

Companies operating and managing support services (OB4.6) are responsible for the recruitment, training and deployment and management of staff that facilitate *supporting services* (OB8). Supporting services include:

- the repair, maintenance and servicing of vehicles
- the decommissioning of vehicles
- the operation of vehicle fleets to provide the transport service
- the provision and maintenance of the road network
- the provision of road signage
- the provision of weather and traffic information
- the provision of fuel stations, electric charging points and highway service stations
- the shipping companies transporting vehicles.

2.3 Vehicle movement harm model

The approach taken by the PRTS (3.5.2 Kinetic Energy) [4] is adopted in this paper. The primary reason that the movement of a v*ehicle* (OB10) can cause harm is due to the kinetic energy associated with its movement and mass. Uncontrolled dissipation of kinetic energy may result from a collision with other *vehicles* (OB10), *vulnerable road users* (OB4.4), the *road infrastructure* (OB9) or the *physical environment* (OB5). Kinetic energy dissipated by a collision may be transferred through mechanical forces to humans whose bodies cannot withstand such mechanical forces without sustaining harm. This model is illustrated in Figure 3.

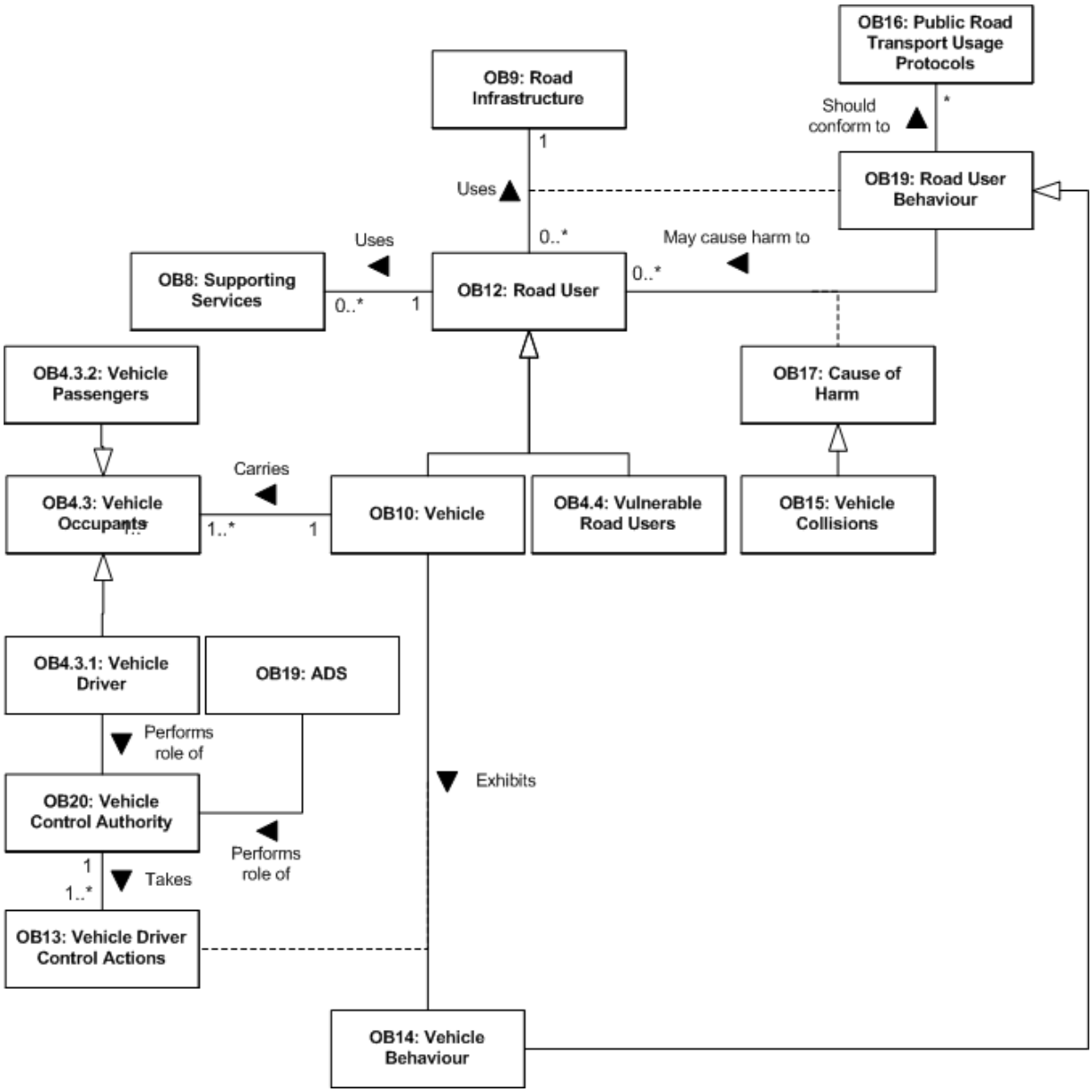

Figure 3: Vehicle movement and harm causation model

From the perspective of the vehicle movement and harm causation model, Figure 3, to avoid harm it is necessary to avoid collisions. From the perspective of a single vehicle, collisions arise as a result of *vehicle behaviour*[2] (OB14). The attributes of the blocks in the model affect the ability of the *vehicle driver* (OB4.3.1) to produce the v*ehicle behaviour* (OB14) which does not lead to, or which avoids, collisions. These attributes are now considered.

The *road infrastructure* (OB9) used by vehicles needs to be designed and maintained such that it is appropriate for the vehicles that use it. The v*ehicle* (OB10) has to be fit-for-purpose when it is operating on the *road infrastructure* (OB9). There are several aspects to this. The vehicles original design must be such that it is not inherently prone to producing inappropriate v*ehicle behaviour* (OB14) despite the v*ehicle driver control actions* (OB13). Before the vehicle starts a new journey on the *road infrastructure*

[2] In the case where a collision arises from the behaviour of other r*oad users* (OB12), it is the subject vehicle's inability to modify its own v*ehicle behaviour* (OB14) to avoid the collision; which may well be impossible in some circumstances

(OB9) it must be in a fit-for-use state as required by its manufacturer or prescribed in law. This includes pre-journey checks as well the vehicle being maintained according to the manufacturer's schedule.

Although not related to vehicle movement, it is noted that the maintenance of the v*ehicle* (OB10) must be performed such that the maintenance staff are not harmed. The human *vehicle driver* (OB4.3.1) responsible for performing the v*ehicle driver control actions* (OB13) must be competent and in fit state to drive. It is also noted that in general, correct storage of a v*ehicle* (OB10) when not is use is also necessary to avoid harm.

In addition to the behaviour of all vehicles using the *road infrastructure* (OB9), the *vulnerable road users* (OB4.4) have a responsibility to behave appropriately in order for collisions to be avoided.

These considerations are captured more succinctly in the following seven aims, discussed in more detail in section 3:

- Aim 1: That the *road infrastructure* (OB9) to be used by vehicles is suitable and fit for purpose
- Aim 2: That the *vehicle* (OB10) placed into the public domain is not inherently prone to causing accidents
- Aim 3: That the *vehicle* (OB10) used is adequate to fulfil the journey
- Aim 4: That the agent with *vehicle control authority* (OB20) is able to drive in a manner likely to avoid accidents
- Aim 5: That *vulnerable road users* (OB4.4) have the knowledge, attitude and ability to use the road infrastructure in a manner likely to avoid accidents

There are also situations when the vehicle is not undertaking a journey, where provision has to be made to ensure that the vehicle does not cause harm to people:

- Aim 6: That the *vehicle* (OB10) used is the subject of routine maintenance, undertaken by qualified maintenance staff in the protected environment of *companies operating and managing support services* (OB4.6)
- Aim 7: That the *vehicle* (OB10) is correctly stored and transported by *companies operating and managing support services* (OB4.6), and while not operational on the *road infrastructure* (OB9), is under the responsibility of either the owner or fleet operator

Although the measures intended to achieve the above aims will not always be complete or fully effective, the historic position has been to assume that human common-sense and a sense of self-preservation on behalf of the road users will fill the gap and avoid an accident, or at least reduce the severity of the accident.

Operational tasks such as access, egress, refuelling or loading need to be considered from an overall safety point of view but are not core to the themes discussed within this paper.

3 Accident mitigating measures

The phrase "accident mitigating measures" refers to the actions taken by the *parties* (OB4) to reduce the likelihood of accidents and consequently collision and harm to people. From what has been described above, it can be seen that the different *parties* all have a role, and corresponding responsibilities, in contributing to the achievement of the seven aims. The discussion of Aim 1 to Aim 5 covers the ontological blocks in Figure 1.

The sections that follow consider each of the seven aims, firstly in the context of manual driving (e.g. the status quo that exists today) and then in the context of automated driving. We also discuss the responsible parties' roles to achieve each aim (from Figure 2), in the context of the personal transport

model (Figure 1). Focus is placed on highlighting where responsibilities might have changed or where responsibilities are now placed on other *parties* with the introduction of automated driving.

3.1 Aim 1 — road infrastructure is fit for purpose

3.1.1 Aim 1 in a manual driving context

The first accident mitigation measure relates to the road infrastructure, the aim of which being to ensure that the *road infrastructure* (OB9) to be used by vehicles is suitable and fit for purpose.

Historically, the *vehicle manufacturers* (OB4.2.2) and the *supplier chain* (OB4.2.3) have had no involvement in, or responsibility for, any part of the road infrastructure design, construction or maintenance. Nor have *vehicle manufacturers* and the *supplier chain* had any reliance on the road infrastructure to ensure vehicle safety; other than being able to demonstrate the robustness of their vehicle to the demands of the infrastructure over the vehicle's lifetime. For example, ensuring that a luxury passenger car can achieve its ride and handling characteristics for 15 years, whether it is being driven on a European highway or in Downtown New York. There is an understanding that the human *vehicle driver* (OB4.3.1) will deal with situations outside of the normal. For example, one would not expect a human driver to knowingly control their vehicle into a large hole that has appeared in the road.

Standards bodies (OB4.5.1) develop road infrastructure regulations that specify the requirements for safe road networks. These include road network design requirements and guidelines for the geometry, position of roadside furniture. Versions of these standards exist at Federal, European and UK levels[3].

Road builders and technology suppliers (OB4.2.1) of new road infrastructure networks will design the road layout to be sympathetic to the requirements of the relevant national and international standards (OB4.5.1) discussed above. However, different revisions of the regulations exist, and compliance is not mandatory in each case. For example, the geography and topography of a particular location might mean that the road geometry deviates from the maximum permissible radius requirement specified. However, such instances are typically accompanied by additional signage to provide sufficient forewarning to drivers.

Currently, Government and Agencies (OB4.1) (e.g. local authorities) have a responsibility to maintain the *road infrastructure* (OB9) in their area. This includes carrying out routine maintenance and responding to individual incident reports from road users. When a road needs to be closed (e.g. for repair) the local authority is responsible for scheduling the road closure and publishing when the closure will happen. The *companies operating and managing support services* (OB4.6) responsible for carrying out the works use specified signage to make road users visually aware of the closure. Developers should also take into account the needs of the pedestrian, especially for road crossings, and the way in which the design of the infrastructure may affect the behaviour. Poor design may provoke poor behaviour.

As the name suggests, *vulnerable road users* (OB4.4) denotes those who lack the physical protection of a vehicle, e.g. pedestrians, cyclists and motorcyclists. Pedestrians typically walk within the road infrastructure and use the pedestrian provisions (e.g. pavements, pedestrian crossings) provided by the road infrastructure, but otherwise their interaction with the road infrastructure will likely be minimal. For example, other than reporting holes in the pavement to the local authority, or "dressing" potholes[4] in

[3] An example from the UK would be a publication by the Highways Agency, "Design Manual for Roads and Bridges Volume 6 Road Geometry Section 1 Links Part2 2 TD 27/05 Cross-Sections and Headrooms", ed 2005.

[4] Dressing of potholes is where citizens place cones or decorate holes in the road to draw attention to them.

the local vicinity, the pedestrian will typically have no interactions with the road infrastructure. Cyclists and motorcyclists, on the other hand, will have direct interactions with the road infrastructure.

There is a voluntary obligation on the human *vehicle driver* (OB4.3.1) to report incidents encountered on the road. For example, a vehicle sustaining wheel and suspension damage having hit a pothole in the road at speed. However, in practice an individual will typically only report an incident when significant damage has happened to the vehicle and the individual wishes to make a claim for damages (e.g. an insurance claim). This obligation can also be applied to all road users, e.g. motorbikes, cyclists.

Non-governmental organisations (OB4.5) can provide additional information upon which drivers come to rely. This information could be in the form of warning broadcasts associated with severe weather or accidents and road closures. In the UK, the Met Office publishes severe weather warnings as an advisory to motorists. Additionally, other non-governmental organizations may highlight deficiencies in the road infrastructure and campaign for improvements. Although this type of information may not be readily assessable, the human driver's ability to adapt to unforeseen circumstances means the lack of such information is unlikely to have a detrimental impact on safety.

3.1.2 Aim 1 impact of automated driving

Whereas human drivers can quickly assimilate new information (e.g. through public information messages) and are expected to adapt quickly when first encountering a change, the training required for automated vehicles will necessarily take longer and so the change will need to be communicated some time prior to its introduction. Consequently, to mitigate the potential impact of road infrastructure changes on the ADS, some form of mechanism or contract will be needed between the road infrastructure suppliers and the *vehicle manufacturers* (OB4.2.2). Such agreements will be needed to formalize infrastructure requirements and the implementation dates for changes being introduced, e.g. changes to existing or the addition of new road furniture. Any proposed changes to the road infrastructure would need to be provided to all ADS developers (OB4.2.2, OB4.2.3) ahead of their introduction. As these changes can impact the Operational Design Domain (ODD), provision would need to be made for both existing AD equipped vehicle fleets and new ADS developments.

With continued correct and safe AD equipped vehicle behaviour being dependent on the road infrastructure meeting its specification, there will be a requirement for the *vehicle manufacturers* (OB4.2.2) to report to the responsible road infrastructure parties any anomalies with the road infrastructure, e.g. a road sign being partially covered by vegetation or road markings being incoherent. This will typically involve each AD-equipped vehicle identifying and recording any road infrastructure anomalies detected and regularly transmitting the in-field data recorded to a central location. Any ADS behavioural anomalies identified during vehicle operation could be the result of either a road infrastructure deficiency or a deficiency in the ADS behaviour itself. Therefore, it would be incumbent on the *vehicle manufacturers* (OB4.2.2) to determine the root cause of the reported anomaly and then inform the appropriate responsible parties. If the anomaly identified was found to be due to an infrastructure failing, then other AD equipped vehicles will potentially need to be made aware, as well as the responsible government agencies. Due to the potential impact on other AD-equipped vehicles, there will be a need to report such infrastructure failings in a timely manner. Once notified, then it becomes the responsibility of the *government and agencies* (OB4.1) to rectify the infrastructure deficiency identified. There may also be a responsibility for the *government agencies* to report deficiencies to the wider *vehicle fleet operators* (OB4.6) and users of the AD-equipped vehicle.

Non-governmental organizations (OB4.5) typically publish safety advice to drivers through public broadcast channels, e.g. severe weather warnings or information about road traffic accidents or road closures. Like the human driver, the ADS may be designed to modify its behaviour based on the safety advisory information received. Consequently, the quality, accuracy, and integrity of this type of information may need to be assured. As an ADS is likely to be less able than a human driver to adapt to unusual situations, the ADS may need detailed and timely information about the changing environment.

3.2 Aim 2 — the vehicle placed in the public domain is not inherently prone to causing accidents

3.2.1 Aim 2 in a manual driving context

Vehicle manufacturers (OB4.2.2) and the *supply chain* (OB4.2.3) are required to meet regulations and observe best practice in the design of vehicles and vehicle components to ensure safety, as well as ensuring that other performance characteristics are met.

The vehicle manufacturer has a responsibility to ensure that the vehicle gives consistent handling feel and response to the human *vehicle driver* (OB4.3.1) for the life of the vehicle. Typically, several methods are used to achieve this. The vehicle specification will be such that many of the vehicle's components will be designed and manufactured to last the expected life of the vehicle. Other vehicle components will have maintenance intervals, where components are replaced within a certain time interval. Where there is the potential for components to fail and adversely affect correct vehicle operation, then component diagnostics and safety mechanisms are typically deployed to put the vehicle into a known safe state on detection of a faulty component. For example, fixing the vehicle's roll stiffness or ride height when a chassis actuator has failed, to avoid the vehicle handling becoming inconsistent.

Facilitating the vehicle driver to operate the vehicle safely will typically require the vehicle manufacturer to provide the user with specific instructions for safe operation and maintenance of the vehicle. This could include, how to top-up the screen wash, checking the correct tyre pressures, and the required service interval. To ensure that this pertinent information passes from user to user, as vehicle ownership changes, this information is typically contained within a Driver's Manual (and stored in the glove box!) or as a digital manual (accessed through the vehicle's infotainment system).

National and international *standards and guidance bodies* (OB4.5.1) have a role to document best practice for vehicle development. In a manual driving context, there is a critical requirement for *standards and guidance bodies* to define requirements for the visual representation of warnings and messages to the human *vehicle driver* (OB4.3.1). It is important that critical messages are represented uniformly across all vehicle types to ensure consistent human interpretation and therefore safe vehicle operation.

It is the role of the human *vehicle driver* to read and understand the published information provided to them by the *vehicle manufacturer* (OB4.2.2) for safe use and control of the vehicle. It is assumed that the human driver can interpret the safe use of the vehicle controls in most contexts without the need to explicitly define all use cases.

Government and agencies (OB4.1) define the laws and regulations that *vehicle manufacturers* need to demonstrate compliance with. This sets a compliance framework that can be enforced through mechanisms such as Type Approval (OB4.1.2) [8].

To demonstrate the achievement of functional safety, independent safety assessments can be used to demonstrate conformity with the applicable standards. The need for this type of non-governmental independent assessment, by *vehicle evaluation organizations* (OB4.5.2.3), is likely to grow as regulatory bodies move to a goal-based performance Type Approval model. In such a context, an independent assessment might be used as a way of demonstrating adherence to the regulations, rather than the vehicle being required to pass a limited set of performance tests.

Vehicle evaluation organizations (OB4.5.2.3), such as Euro NCAP, influence the adoption and use of vehicle safety features. This is particularly true for ADAS, where achieving a Euro NCAP 5-star rating requires the vehicle to be fitted with various ADAS features.

3.2.2 Aim 2 impact of automated driving

The responsibility placed on the *vehicle manufacturers* (OB4.2.2) and *supply chain* (OB4.2.3) to deliver a safe vehicle design (to meet regulations and to observe best practice design principles) does not change with AD-equipped vehicles.

This is also true of vehicle handling, performance and response, where again the vehicle manufacturer has a responsibility to design a vehicle that is consistent throughout the vehicle's operational life.

The ADS performing the role of *vehicle control authority* (OB20) is required to correctly interface with the vehicle platform to maintain control of the vehicle. The ADS may be provided to the *vehicle manufacturer* (OB4.2.2) by a third-party organization, so it is useful to treat the ADS as a separate entity with an interface to the vehicle platform controls. Operating outside of the defined interface specification can have safety implications, therefore it could be anticipated that this will be formally controlled.

Standards and guidance bodies (OB4.5.1) have a role to document best practice for vehicle systems and component development. This applies equally to vehicles, and vehicle components used in manual and automated driving context. However, with automated driving being a complex emerging field, best practice is still evolving so can be difficult to define.

For AD-equipped vehicles, warnings about any degradation to vehicle platform performance still needs to be communicated to the ADS performing the role of *vehicle control authority* (OB20). This suggests potential benefits associated with standardizing the interface between the vehicle platform and the ADS. However, the exact implementation may be dependent upon the specifics of the vehicle architecture and the boundaries of responsibility between the vehicle platform manufacturer and the ADS developer, making it difficult to currently envisage how a standard interface might be achieved.

As with manual driving, for an AD-equipped vehicle the vehicle manufacturer is responsible for providing a vehicle that delivers consistent performance over its lifetime. However, there is the potential for vehicle platform components to fail and not be readily identifiable[5] as such, by either the vehicle platform systems or the *vehicle control authority* (OB20). In situations such as these, there will be a responsibility on the *vehicle manufacturer* to detect and communicate vehicle performance reductions to the *vehicle control authority*, to avoid the *vehicle control authority* making vehicle control requests that cannot be honoured by the vehicle platform due to the faults being present.

The organization (e.g. the *vehicle manufacturer* (OB4.2.2)) responsible for developing the *ADS* (OB19) could be the same organization responsible for developing the platform vehicle. Equally, they could be separate independent entities. Irrespective of the commercial agreements involved, it is important that a complete and correct definition of the interface between the *ADS* and the platform vehicle exists. As operating outside of the defined interface specification can have safety implications, it is recommended that this is formally controlled. When the vehicle and *ADS* are being produced by different parties (OB4.2.2) there is a responsibility on both the vehicle platform manufacturer and the *ADS* developer to provide a safety manual with their product.

As with manual driving, to facilitate safe vehicle use, the *vehicle manufacturer* (OB4.2.2) will need to provide AD-equipped vehicle users with information about the vehicle. Although the use case for an AD-equipped vehicle might be different, the types of information that users require is likely to be similar to those needed when driving the vehicle manually, e.g. the AD-equipped vehicle may be being operated as part of a ride hailing service fleet (OB4.6). In such a case, the information about the vehicle that the end user might need will be limited. However, the information that the fleet operator organisation will need about the vehicle will be more detailed, particularly regarding daily AD system checks, vehicle

[5] These are failures typically identifiable by a human driver (OB4.3). For example, identifying that the vehicle has worn brake pads, because audible squeaks and squeals are heard during each brake application.

servicing and maintenance. Given the relative cost of AD-equipped vehicles, it is likely that vehicles will be sold on from one fleet operator to another. An analogous example can be found in the aviation industry where expensive passenger aircraft are refurbished and operated by successive fleet operators. If AD-equipped vehicle fleets follow the aviation industry model, then when AD-equipped vehicles are sold on to the next fleet operator, operational and service history information will also need to be passed on with the vehicle.

Demonstrating conformity to standards, and hence the achievement of functional safety, through independent safety assessment, is likely to become the dominant approach used when type approving AD-equipped vehicles. The recently published ADAS regulations suggest that regulatory bodies (OB4.1.2) are moving from a reliance on witnessed performance testing towards a goal-based engineering assessment. This shift towards a greater reliance on long-term goal-based Type Approval assessments is expected[6], as ADS and ADS operating environment complexity grows, and the insight gained from observing an AD-equipped vehicle undertaking a few prescribed tests on a test track becomes more and more limited.

It could be expected that to retain its licence to operate, fleet operators will be required to demonstrate continuous fleet monitoring, and the swift identification and resolution of any anomalies occurring during operation. Capturing data like this helps to validate the AD-equipped vehicle behaviour achieved in the real world and will either support or challenge the safety rationale. This could require the ADS to publish near-miss and accident data, as well as reporting any other anomalies that occur during operation. For example, an incident could be adjudged a near-miss by either the real-time or background analysis of proximity parameters, or an anomaly could be identified if the in-service classification confidence level, for the perception system, drops below a predefined target.

Vehicle evaluation organizations (OB4.5.2.3), such as Euro NCAP, influence the adoption and use of vehicle safety features. This relationship does not change between a manually driven vehicle and an AD-equipped vehicle, but consideration will need to be applied to new aspects prevalent in AD-equipped vehicles. For example, in future Euro NCAP might specify the safety criteria for rear-facing seats used in AD-equipped vehicles. Additionally, one could imagine that in future, the abovementioned in-service performance data, could be used as justification for a particular vehicle to either retain or lose its 5-star rating.

3.3 Aim 3 — the vehicle used is adequate to fulfil the journey

3.3.1 Aim 3 in a manual driving context

Ideally, the *vehicle manufacturer* (OB4.2.2) would have no responsibility for the vehicle beyond the start of production. However, issues arise post-production which means that *companies providing support services* (OB4.6) are required to take actions to rectify vehicles in service. For example, service actions could be required in order that the *vehicle manufacturer* meets their warranty obligations, or it could be that a *government and agencies* (OB4.1.1) organization has enforced a vehicle recall.

Type Approval assumes that a vehicle is adequate at the time of introduction and will offer consistent operation for the lifetime of the vehicle. Consequently, vehicle faults that lead to potentially inconsistent vehicle behaviour either need to be detected by in-service diagnostics and repaired or replaced by a regular maintenance schedule recommended by the *vehicle manufacturer*. Where faults occur that

[6] An example of a shift towards long-term goal-based Type Approval can be found in the following document: Regulation (EU) 2022/1426, regarding laying down rules for the application of Regulation (EU) 2019/2144 of the European Parliament and of the Council as regards uniform procedures and technical specifications for the type-approval of the automated driving system (ADS) of fully automated vehicles.

require the human *vehicle driver* (OB4.3.1) to change their behaviour to maintain vehicle safety, the *vehicle manufacturer* needs to ensure that these faults are reported to the *vehicle driver* through consistent driver warnings. The expectation is that the *vehicle driver* will understand the warning received and make the necessary changes to maintain safety e.g. pulling over to the side of the road. In addition, the human *vehicle driver* must be sensitive to changes in the vehicle's performance and behaviour, e.g. listening for unusual noises, or vibrations that indicate a compromised vehicle state.

Government and agencies (OB4.1) support the adequacy of vehicles in service by imposing regular inspections, e.g. the annual MOT inspection in the UK. This sets a minimum level of vehicle condition (predominantly mechanical and emissions based) deemed suitably safe to operate on the public highway. If, during a spot-check, a vehicle fails to meet the necessary minimum requirements then the *vehicle driver* may face legal action. The legal action typically takes the form of a fine. *Government and agencies* also enforce recalls, based on field data. Product recalls can require the *vehicle manufacturer* (OB4.2.2) to make updates to all types of technology to improve or ensure safety, as well as other key aspects. *Vehicle manufacturers* can be punished for not meeting their obligations during a recall campaign.

Standards and guidance bodies (OB4.5.1) do not have a direct role in ensuring that the vehicle in service is adequate. There is an assumption that the original design incorporates the best practice for when the vehicle is first made available to the public and that this will remain appropriate for the life of the vehicle.

Prior to the start of any journey, there is a requirement on the human *vehicle driver* (OB4.3.1) to ensure that the vehicle is safe and fit to be used, e.g. do the lights work, are the windows clean, are the tyres worn and do they have sufficient pressure? In reality, the frequency and number of checks performed by the human *vehicle driver* prior to starting a journey are often less than required. Given that the *vehicle driver* will normally deal with the situation should a failure occur, the consequences of not performing these checks are perhaps considered less serious, typically resulting in an inconvenience rather than a direct hazard.

In terms of the adequacy of vehicles in service, the *vulnerable road users* (OB4.4) do not have any influence here.

Non-governmental organizations, such as the *press and media* (OB4.5.2), may independently assess vehicles in service, reporting on their perceived suitability, performance and behaviour. This may add pressure on *vehicle manufacturers*, *governments and agencies* to address weaknesses observed in service, prompting recalls and changes in design.

3.3.2 Aim 3 impact of automated driving

Where base vehicle faults that require the ADS to change its behaviour occur in service, to maintain vehicle safety, the same obligation on the *vehicle manufacturer* (OB4.2.2) exists to inform the *ADS* (OB19). Consequently, the medium of the warnings will be different, i.e. the warning will likely take the form of a serial communications message rather than a visual or audible warning.

From a *vehicle manufacturer's* (OB4.2.2) perspective, the in-service responsibilities remain largely similar for automated driving. However, what does change is the need to monitor and understand the performance of the ADS component. Depending on the business model, this could be the responsibility of the *vehicle manufacturer* (OB4.2.2) or it could be the responsibility of the ADS supplier. Irrespective of organizational responsibility, there is a need to monitor the performance of the vehicle operating in the field to identify operational anomalies when they occur, to determine the root cause of those anomalies, to design and implement a fix, and to test and ensure all vehicles in the fleet have been updated accordingly. Depending on the responsibility split, this will likely require a formal agreement between the *vehicle manufacturer* (OB4.2.2) and *supply chain* (OB4.2.3). This potentially necessitates the need for some approval by the fleet operator before new software is downloaded.

The ADS would be required to complete some or all of the pre-journey checks, which in reality will mean the checks being completed more often than would occur for a manually driven vehicle. However, the criticality of pre-journey test outcomes will likely become greater, since the ADS may be less able to adapt to in-journey changes arising from incorrect or incomplete pre-journey checks. During the journey, there is an expectation that the ADS is responsible for responding to the warnings issued by the base vehicle and for monitoring any changes in the base vehicle. Changes to the base vehicle could include, changes in performance, noise or vibration, all of which are indicators of potential problems with the vehicle.

The regular inspections imposed by *government and agencies* (OB4.1) may need to be more frequent given the higher usage expected by automated vehicles, similar to that of taxis.

The responsibility to ensure that the vehicle meets a minimum level of safety before each journey moves to the service provider (for non-private fleet operated vehicles). The responsibility for enforcing the safety requirements placed on fleet operators may fall to *government and agencies* (OB4.1) or other local authorities. For example, if a vehicle's tyre tread fell below the minimum allowed threshold, then the *companies operating and managing support services* (OB4.6) (e.g. the service provider) could be penalized by *government and agencies*, rather than the vehicle's occupants being held responsible or accountable. Typically, the human *vehicle driver* performs additional safety checks before starting each journey, e.g. checking that passengers have their seatbelts fastened and their door closed. This responsibility would also move the service provider.

3.4 Aim 4 — that the agent with vehicle control authority is able to drive in a manner likely to avoid accidents

3.4.1 Aim 4 in a manual driving context

The *government and agencies* (OB4.1) uphold minimum skill levels by requiring prospective *vehicle drivers* to hold a licence to drive. The type of driving licence required depends on the vehicle type and can only be obtained by passing a driving test, the content of which the government controls. Governments also impose driving restrictions on individuals considering their physical and mental capabilities, e.g. governments impose limits on the concentration of drugs and alcohol permissible in the blood and require individuals to declare any health changes which could impact that individual's physical or cognitive capability e.g. changes to medication or recent surgical procedures. Through the legal system, the government also punishes those individuals who do not adhere to the rules of the road or who drive in a manner deemed to be dangerous, careless, or inconsiderate. Punishments range from additional training e.g. speed awareness courses, to fines, to loss of license and imprisonment. G*overnment and agencies* publish standards for the design of the road network and for the associated traffic signalling. Additionally, *government and agencies* approve changes to the road network and commissions contractors to implement the changes.

International regulation prescribes the design properties of the vehicle controls used by a human *vehicle driver* to control the vehicle. These design properties are chosen to account for the possible range of physical attributes that individual *vehicle drivers* might have, and to make vehicle controls consistent and intuitive irrespective of the vehicle type. The *vehicle manufacturer* (OB4.2.2) then has a responsibility to develop vehicles fulfilling these design properties. Vehicle system warnings also have to be easy for the human *vehicle driver* to understand, both how to interpret a given warning, and also how to respond. While a level of driver control and warning commonality exists across vehicle types, for well-established controls and warnings, the same is not true for new vehicle features. *Vehicle manufacturers* typically support driver understanding by publishing printed material, regarding controls and warnings e.g. a handbook, or as information online. The vehicles may also include systems that provide the *vehicle driver* with warnings related to the current road situation e.g. collision warning, or to prompt the *vehicle driver*

when a control action is needed (e.g. Lane Keeping Assist). These types of systems are collectively known as ADAS. Other vehicle systems can monitor the human *vehicle driver's* fitness to drive, e.g. alcohol interlocks that prevent a *vehicle driver* using the vehicle if the level of alcohol in the blood exceeds the legal limit [10]; these are not normally a factory-fit item.

Many different parties contribute to the human *vehicle driver* (OB4.3.1) having the knowledge, ability and attitude to drive in a manner likely to avoid accidents. Driving instructors (part of the *companies operating and managing support services* (OB4.6) group) provide instruction for the practical control of the vehicle, the correct way to use the road network as well as the *public road transport usage protocols* (OB16) for using the road in the presence of other road users. *Insurance companies* (OB4.5.3) may offer lower premiums on the proviso that the vehicle is fitted with a data recorder to encourage cautious driving. Good practice for driving is published, or otherwise disseminated, by groups including *standards and guidance bodies* (OB4.5.1) and road safety advocates (OB4.5.2.2). Pharmaceutical companies provide guidance on the use of vehicles for those who have taken medication. Doctors do likewise after surgical procedures.

Where the human *vehicle driver* (OB4.3) performs the role of vehicle control authority, they should have the knowledge, ability, and attitude to drive in a manner likely to avoid accidents; this entails driving carefully and competently. The driver is legally required to practice what they have been taught and be cognisant of changes to the law and associated guidance. *Vehicle drivers*, particularly those newly qualified, should drive within what they understand their current skill level and experience to be. The *vehicle driver* should act appropriately to new information that they receive during journey (OB4.6), e.g. weather warning and traffic information. While driving the *vehicle driver* should maintain self-discipline and not allow any heightened emotional states to affect their driving style. They should also show courtesy to other road users and drive with sympathy for both the *vehicle occupants* (OB4.3), e.g. avoid excessive accelerations, and for the vehicle itself, e.g. avoid potholes if possible. Driving involves predicting the behaviour of other road users. Traditionally this has been based on all human *vehicle drivers* having been taught to drive in a common manner. Consequently, if other road users are observed not driving in the prescribed way, a response could be to drive more cautiously, e.g. allow a greater distance and or time from the misbehaving vehicle, or to monitor the other vehicles more closely.

The human *vehicle driver* is expected to communicate their intentions to other road users, which can be achieved in several ways. These include: the use of the indicators, lights and horn; the speed and acceleration of the vehicle; visual contact with other road users and the use of facial expressions and hand gestures. However, *road users* (OB12) should not inflame the emotions of other road users by what they say, what they gesticulate or by their actions on the road.

Those responsible for providing information, or instructions (from the *companies operating and managing support services* (OB4.6) group), during a journey have a responsibility to ensure that the information is up to date and accurate.

3.4.2 Aim 4 impact of automated driving

The expectation is that *government and agencies* (OB4.1) will set driving performance criteria and license the right to operate an AD-equipped vehicle. This licence will be contingent on the AD-equipped vehicle meeting the prescribed driving performance criteria. The *government and agencies* may set expectations on how quickly in-field anomalies are corrected and potentially remove a licence to operate if this expectation is not met. In relation to the driving performance criteria, *standards and guidance bodies* (OB4.5.1) may publish good practice guidance regarding driving policies and risk acceptance criteria.

It may be beneficial for *road builders and technology suppliers* (OB4.2.1) to adapt designs, making it easier for AD-equipped vehicles to avoid accidents as they traverse the *road infrastructure* (OB9).

Changes to the environment that are relevant to the safe operation of the ADS need to be retrospectively applied to the vehicles in service. These could be the introduction of new road infrastructure types

and signage, changes in the rules of the road (as part of the *law & legal systems* (OB4.1.2)), or the introduction of new vehicle and/or road user types. As discussed in Section 3.4.1 above, in a manual driving context, the human *vehicle driver* (OB4.3.1) is expected to keep abreast of all changes related to driving a vehicle on the public highway, so they can adapt to these changes. For automated driving, this needs to be handled in a similar way to any other issue arising during operation. Suitable updates to the deployed vehicles need to be made, ideally with 100% coverage. Depending on the particular implementation, this responsibility could lie with the *vehicle manufacturer* or the ADS component supplier. Given that safety is an inherent property of the deployed vehicle, then the responsibility for vehicle safety remains for the entire time that the vehicle is in operation. If support ceases and safety updates cannot be made, or the capability of the ADS cannot be updated due to other limitations, e.g. hardware, then the vehicle would need to be removed from service.

The *vehicle manufacturer* (OB4.2.2), together with its *supply chain* (OB4.2.3), has to maintain a state-of-the-art safety policy that takes account of changes to the law and guidance as they occur. If an AD-equipped vehicle relies on predicting the behaviour of other road users, it may also have to detect non-standard behaviour and respond appropriately. In such a case, the *vehicle manufacturer* would have to monitor in-field performance and re-train the ADS in response to all detected in-field anomalies. The *vehicle manufacturer* would also have to have a system in place capable of deploying updates onto the entire vehicle fleet.

Like the human driver, the AD-equipped vehicle will need to act upon new information received from *companies operating and managing support services* (OB4.6) during the journey, e.g. current weather and traffic information. Additionally, *vehicle occupants* (OB4.3) will be expected to adhere to the instructions for using the AD-equipped vehicle correctly. Conversely, the *companies operating and managing support services* (OB4.6) will have to keep abreast of automated vehicle developments and make the necessary changes to provide the best operating and support services.

Where AD-equipped vehicles are likely to share the r*oad infrastructure* (OB9) with manually driven vehicles, it may be beneficial for the *government and agencies* (OB4.1) to specify behaviour expectations for the interaction between an AD-equipped vehicle and other road users. This would potentially help other road users to correctly anticipate the actions of the AD-equipped vehicle. This topic will be the subject of future white papers in this MISRA series.

3.5 Aim 5 — vulnerable road users have the knowledge, attitude and ability to use the road infrastructure in a manner likely to avoid accidents

Pedestrian crash protection aside, for a manually driven vehicle, the *vehicle manufacturer* (OB4.2.2) and *supply chain* (OB4.2.3) have limited responsibilities regarding *vulnerable road users* (OB4.4). It is assumed that these road users will usually act responsibly and be able to anticipate the actions of the human *vehicle driver*. Likewise, it is assumed that the human *vehicle driver* (OB4.3.1) will be able anticipate the actions of the other road users.

This characteristic of mutual anticipation cannot be assumed in the case of an AD-equipped vehicle. It is therefore important that provision is made for the AD-equipped vehicle to provide the means to clearly communicate the vehicle's intentions to other road users.

The *government and agencies* (OB4.1) provide the *road infrastructure* (OB9) that is used by both *vehicles* (OB10) and *vulnerable road users* (OB4.4). It is then incumbent on the *government and agencies* to design the *road infrastructure* to allow *vulnerable road users* to use that network safely. The *government and agencies* (OB4.1) also provide guidance to both *vehicle drivers* and *vulnerable road users* through published material, e.g. the Highway Code, and through public information campaigns.

In addition to the *government and agencies*, other bodies may provide guidance for *vulnerable road users*. These are mostly likely to be *non-governmental organisations* (OB4.5) e.g. cycling organizations, may provide guidance on using the *road infrastructure*. Such guidance should encourage responsible behaviour and may need to be adapted to take into account the presence of AD vehicles.

It is the responsibility of *vulnerable road users* to abide by the guidance produced by *government and agencies*, some of which may be a legal requirement (part of the *law & legal systems* (OB4.1.2)), and to not act irresponsibly.

The behaviour of an AD-equipped vehicle should be consistent when compared to manually driven vehicles, which can exhibit inconsistent and potentially misleading behaviour. There is also a need for the AD-equipped vehicle to provide the means to be able to actively communicate its behaviour or intent.

3.6 Aim 6 — provision for correct vehicle maintenance — protection of maintenance staff

The *vehicle manufacturer* (OB4.2.2) produces workshop manuals, processes and procedures to safely maintain vehicles in use. This expectation is the same for manual and AD-equipped vehicles. For AD-equipped vehicles, the ADS would need to be "aware" that vehicle maintenance is being performed and to not perform any unwanted actuations until maintenance is completed, otherwise, maintenance staff (working for *companies operating and managing support services* (OB4.6)) could be injured during the maintenance process. Therefore, there is a need for the provision of dedicated maintenance modes for the ADS and AD-equipped vehicle. Such maintenance modes could prevent the ADS from being able to command vehicle actuation, while at the same time the AD-equipped vehicle could be programmed to ignore vehicle actuation requests. Potentially, provision also needs to be made to extend the operating procedures beyond the approved dealer network to enable independent repairers to safely repair AD-equipped vehicles. All modes that the AD-equipped vehicle can be placed into will need to be documented and communicated to those parties operating and maintaining the AD-equipped vehicle fleets.

Standards and guidance bodies (4.5.1) as well as *vulnerable road users* (OB4.4) do not have a role in the protection of maintenance staff during vehicle maintenance.

For a manually driven vehicle, once the vehicle control authority (i.e. the human *vehicle driver*) has secured and stepped away from the vehicle, the focus of any dedicated procedures is then to make the vehicle safe before beginning any maintenance activity, e.g. disconnecting the low-voltage battery before beginning any maintenance work. Contrast that with the AD use case, where the vehicle control authority cannot be removed from the AD-equipped vehicle, so potentially remains active while maintenance work is undertaken on the vehicle. To ensure the safety of those working on and around the AD-equipped vehicle while maintenance is undertaken, the maintenance modes provided by the *vehicle manufacturer* (OB4.2.2) would need to be entered by the AD-equipped vehicle systems, i.e., the ADS and the platform vehicle, prior to the maintenance activity beginning, to remove the potential for the ADS to cause injury to maintenance staff.

Companies operating and managing support services (OB4.6) that undertake maintenance and service actions will need to observe *vehicle manufacturer* (OB4.2.2) provided guidance and processes for safe maintenance of all vehicle types. The criticality of not adhering to documentation giving guidance to maintenance staff to ensure their safety will be significantly increased for AD-equipped vehicles. This is due to the possible range of ADS requests.

3.7 Aim 7 — provision for correct vehicle storage and transport while not operational — owner or fleet operator

Transport and storage modes need to be provisioned for by the *vehicle manufacturer* (OB4.2.2). For manually driven vehicles, these modes typically cover energy use and comfort systems, with little direct impact on safety. For AD-equipped vehicles which can request vehicle movement, storage and transport modes are more critical and of higher interest to those *companies operating and managing support services* (OB4.6) which involve shipping AD-equipped vehicles and their *insurance companies* (OB4.5.3). Transport mode also could be used to move an AD-equipped vehicle manually using external means, e.g. to manually move the AD-equipped vehicle onto a trailer for transport, or from outside to inside a designated operational area.

Standards and guidance bodies (OB4.5.1) already have a role defining requirements for the movement of hazardous goods, which are then enforced by *government and agencies*. Additional enforced standards and guidance for the transport of AD-equipped vehicles may be required to ensure controlled and intended vehicle movement, whilst maintaining safety.

To align with the *vehicle manufacturer* defined operating modes for transport and storage, the ADS needs to be aware that one of these restrictive operating modes has been activated and abide by the restrictions imposed by that mode.

Vulnerable road users (OB4.4) do not have a direct role or responsibility in relation to vehicle storage and transport. However, one could perhaps imagine a situation where incorrect vehicle transport or storage could place a *vulnerable road user* in harm's way.

To facilitate the storage and transport of AD-equipped vehicles, shipping services and *insurance companies* (OB4.5.3) will require assurances from the *companies operating and managing support services* (OB4.6), that safety is achieved during storage and transportation. This will also include the provision of training for fleet operators and transport staff to correctly configure and handle AD-equipped vehicles in passive or manually driven states used for storage and transport. This training should also include redeployment of the vehicle after storage or transport, to ensure all functionality has been correctly re-enabled.

4 Summary of accident mitigation measures

Within this document we have considered the roles and responsibilities of the parties involved in the provision of personal transport, with a view to avoiding harm. Comparing manually driven vehicles to AD-equipped vehicles for these roles and responsibilities highlights several key dependencies. These dependencies for AD-equipped vehicles include:

- In-service legal requirements — the responsibility for a vehicle's in-service legal obligations move from the human *vehicle driver* (OB4.3.1) to the fleet operator or *vehicle manufacturer (OB4.2.2)*.
- Lifetime fit-for-purpose requirements — there is a need for compliance to the latest applicable regulatory requirements throughout a vehicle's lifetime, and not just at the point of product homologation or of the vehicle's first introduction into the market.
- Implementation of critical updates — vehicle fleet monitoring will be required to identify issues occurring in the field. Once identified, deployment and acceptance guarantees will be needed for those critical updates.
- Road infrastructure incident reporting — there is a requirement for the AD-equipped vehicle to report incidents that would normally have been reported by the human *vehicle driver (OB4.3.1)*. For example, potholes or other critical road conditions.
- Road infrastructure topology changes — an AD-equipped vehicle will be sensitive to any unpublished changes to the *road infrastructure* (OB9) topology. This creates a critical link between the *vehicle manufacturer* (OB4.2.2) and the *government and agencies* (OB4.1) defining or modifying the road layouts and infrastructure.

- Transparent in-field reporting—— the provision of a shared database of all in-field reports. The quality and timely availability of this information would be critical to enable all parties to identify deficiencies in system aspects for which they are responsible.
- Unpublished changes within the vehicle's deployment domain — safe AD-equipped vehicle operation may be sensitive to unpublished changes occurring within the vehicle's deployment domain. For example, the introduction of a new vehicle or road user type. This possibly places a requirement onto *government and agencies* (OB4.1) to catalogue, manage and publish all actor types.
- Vehicle performance early indicators — there is a requirement for AD-equipped vehicles to sense and deal with early indicators of vehicle performance issues. This could require the ADS being sensitive to the presence of, or changes in, noise, vibration, smell, smoke and to identify vehicle performance issues.
- Data integrity — the quality and robustness of the information that the AD-equipped vehicle bases its actions on becomes critical. As without the human *vehicle driver* (OB4.3.1), the human oversight ensuring correct vehicle movement no longer exists.

These dependencies arise from the implicit, undocumented requirements placed on the human *vehicle driver* being transferred to the ADS and the processes required around them. Ideally, a safety argument for the safe operation of AD-equipped vehicles would include claims that provide confidence that all parties involved have performed their roles as required. However, there is a clear lack of overall accountability for the provision of personal transport, as no one entity oversees the coordination and performance of all parties. A partial safety argument is likely to be made by the *vehicle manufacturer* (OB4.2.2) and the *supply chain* (OB4.2.3), centred around the vehicle development itself. Therefore, evidence, claims and assumptions made at the interface to other parties requires special attention. This safety argument will be the focus of the next white paper in this MISRA series.

5 Terminology

Most terminology used within the document is defined at the point of first use. The following table defines additional key terms.

Term	Description
Agent	A person or thing (e.g. ADS) that takes an active role, produces, or takes responsibility for a specified effect. For example, the human driver or ADS with vehicle control responsibility.
AD	Automated Driving
ADAS	Advanced Driver Assistance Systems
AD-equipped Vehicle	A vehicle fitted with an ADS capable of being driven without a human driver for part or all of the mission.
ADS	Automated Driving System: electronics and software that replaces the human driver as the VCA in an AD driving context.
Harm	Physical injury or damage to the health of persons.
ODD	Operational Design Domain
Party	A group of people who undertake activities together. For example, a group of people writing standards on behalf of a standards organisation.
Safety case	Argument that functional safety is achieved for items, or elements, and satisfied by evidence compiled from work products of activities during development, as required by ISO 26262 [2].
System	Set of components or sub-components that relates at least a sensor, a controller and an actuator with one another.

VCA	Vehicle Control Authority — responsible for controlling the vehicle. This can be the human driver or the ADS.
Vulnerable road user	Road users that interact with the road infrastructure, but lack the physical protection of a vehicle, for example pedestrians, cyclists, motorcyclists.

6 Ontology block references

ID	Title	Figure
OB1	The Public Roads as a Social Space	1
OB2	Provision of personal transport on the public road network	1
OB3	Socio-physical Context	1
OB4	Parties	1,2
OB4.1	Government and Agencies	2
OB4.1.1	Government Departments	2
OB4.1.2	Law & Legal Systems	2
OB4.2	Engineering Developers and Manufacturers	2
OB4.2.1	Road Builders & Technology Suppliers	2
OB4.2.2	Vehicle Manufacturer	2
OB4.2.3	Supply Chain	2
OB4.3	Vehicle Occupants	1,2,3
OB4.3.1	Vehicle Driver	2,3
OB4.3.2	Vehicle Passengers	2,3
OB4.4	Vulnerable Road Users	1,2,3
OB4.5	Non-governmental Organizations	2
OB4.5.1	Standards and Guidance Bodies	2
OB4.5.2	Industry Influencers	2
OB4.5.2.1	The Press	2
OB4.5.2.2	Road Safety Advocates	2
OB4.5.2.3	Vehicle Evaluation Organizations	2
OB4.5.3	Insurance Companies	2
OB4.6	Companies operating and managing support services	2
OB5	Physical Environment	1
OB6	Governing Prescriptions	1
OB6.1	Transport and vehicle related Norms, Procedures, Standards	1
OB6.2	Legislation	1
OB7	Road network infrastructure and supporting services	1
OB8	Supporting Services	1,3
OB8.1	Technology Based	1
OB8.2	Human Based	1
OB9	Road Infrastructure	1,3
OB10	Vehicle	1,3
OB11	Vehicle Specification	1
OB12	Road Users	3
OB13	Vehicle Driver Control Actions	3
OB14	Vehicle Behaviour	3
OB15	Vehicle Collisions	3
OB16	Public Road Transport Usage Protocols	1,3
OB19	ADS	3
OB20	Vehicle Control Authority	3

7 References

[1] MISRA, *Guidelines for Automotive Safety Arguments*: HORIBA MIRA Limited, 2019. ISBN

[2] ISO 26262:2018, *Road vehicles — Functional safety*

[3] J. Birch, D. Blackburn, J. Botham, I. Habli, D. Higham, H. Monkhouse, et al., *"A Structured Argument for Assuring Safety of the Intended Functionality (SOTIF)"* presented at the SafeComp, 2020. http://safecomp2020.di.fc.ul.pt/ (accessed 04/02/2024)

[4] R. S. Rivett, *"Public Road Transport System and Vehicle Models"*, University of York 2022. https://www.york.ac.uk/assuring-autonomy/research/publications/public-road-transport-system-vehicle-models/ (accessed 17/03/2025)

[5] SAE J3016:2021 "*Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*"

[6] MISRA, *Safety assurance argument context for automated driving*: 2024

[7] ISO 21448:2022 *Road vehicles — Safety of the intended functionality*

[8] UK government, *Vehicle Approval*. https://www.gov.uk/vehicle-approval (accessed 17/3/2025)

[9] UK government, *The Highway Code*. https://www.gov.uk/guidance/the-highway-code (accessed 17/3/2025)

[10] European Commission General Safety Regulation (GSR2), *"Regulation (EU) 2019/2144 of the European Parliament and of the council"* 07/07/2024

8 Revision history

Revision	Description of changes	Release date
Version 1.0	First version release	March 2025