# MISRA SC

## Safety assurance argument context for automated driving

April 2024

First published March 2024 by The MISRA Consortium Limited
1 St James Court
Whitefriars
Norwich
Norfolk
NR3 1RU
UK

www.misra.org.uk

ISBN 978-1-911700-01-2 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:

| | |
|---|---|
| John Birch | UL Solutions |
| David Blackburn | Rimac Technology |
| Helen Monkhouse | HORIBA MIRA Ltd |
| Norina Ratiu | Oxa |
| 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

Serrie Chapman

## Other acknowledgements

# Contents

# 1 Background

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 [12]).

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. 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 including the physical road network and supporting infrastructure, the agents that use the road network, the weather and agent interactions with the external environment.

The aim of this white paper is to provide an overall context within which a safety assurance argument for a vehicle with high or full driving automation has to be made. To do this two contexts are presented. The first context views personal transport as a service, within 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 considers the complete lifecycle of a vehicle from development, through operation and maintenance, to decommissioning.

For both contexts we provide an ontology of terms, the subject matter, and a claim structure showing 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, as this only becomes necessary when product development standards are used, e.g., ISO 26262, ISO 21448. Although this document focuses on the harm to people, it would be possible to expand the assurance argument to include other losses. For example, financial or reputational loss.

The ontologies simply present what is already known, but the novelty is in showing the relationships between different aspects that up to now have largely been addressed in isolation from each other. The point of showing these larger composite views is to highlight the relationships between the different aspects, as assumptions will have been made, either explicitly or implicitly, when creating a safety argument for a vehicle, or some part thereof[2]. At present, no one organization has responsibility for assuring that all the different aspects work together to avoid harm to people. The need for such a holistic view is increasing due to the introduction of new technologies, such as ADS equipped vehicles, the use of vehicle-to-everything (V2X) communication and the Internet of Things (IoT). MISRA are not aware that the comprehensive views presented in this white paper have been attempted previously.

MISRA has no current plans to progress the ideas expressed in the white paper further, their purpose is to provide the wider context and identify aspects about which assumptions may have to be made when creating safety assurance arguments for vehicles with high and full driving automation. Future white papers will address the creation of a safety assurance argument for an ADS equipped vehicle, with relevant aspects identified in this paper carried forward as assumptions.

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

[2] Ontologies can also support and inform the definition of operational domains, use cases and scenarios, which provide the context for the safety argument

# 2 Personal transport modelled as a service

In this first context, we use a vehicle operating on the public roads as a personal transport service. This approach is taken to identify all the aspects that are relevant to the vehicle being used on the public roads, with the vehicle being a component of this service. The subject vehicle could be a manually driven vehicle, with or without driver assist features, or it could be a vehicle with high or full driving automation.

We first start with a generic model of a public service and then adapt it solely for the service of personal transport on the public road network.

## 2.1 General public service model

An ontology of a generic public service, expressed using SysML notation [6], is shown in Figure 1. It models a *subject service*[3] as being the interaction of three different entities: the *service support delivery mechanism*, the *end user service delivery mechanism* and the *end user*. The interactions may come under the auspices of one or more *governing prescriptions*. The interacting entities, together with the *physical environment* and the *governing prescriptions* are part of the *socio-physical context* within which the *subject service* operates.

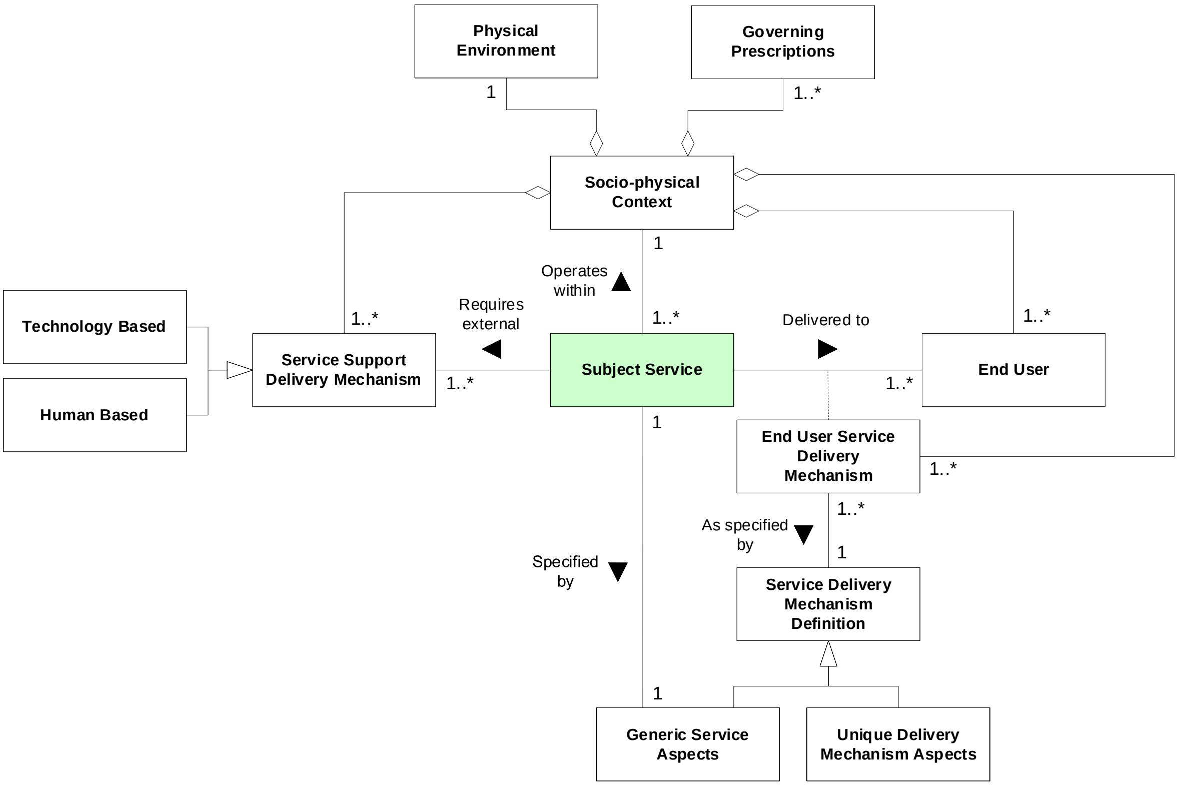

Figure 1: Generic ontology for public services

The *subject service* is the societal service being provided. Example *subject services* include health care and different types of public transport, such as railways, aerospace, or road transport. The *end users* are those who make use of the service. A *service delivery mechanism definition* typically states what is being provided as a service. There is an aspect of the *service delivery mechanism definition* that is generic, namely the overall goal of the service. Then there is an aspect of the *service delivery mechanism definition* that is particular to the *end user service delivery mechanism*, such as the particular train, aeroplane or

[3] Terms in italics reference entities used in an ontology or claim structure

vehicle. The *service support delivery mechanisms* include all the auxiliary services that the *subject service* relies on, but that are not part of the defined *subject service* itself. For example, for a hospital one such *service support delivery mechanism* could be the ambulance service. The *service support delivery mechanisms* may be *technology based*, e.g., equipment, or *human based*. The *governing prescriptions* include related laws, regulations, standards and procedures.

## 2.2 General public service claim structure

Based on the generic service ontology of Figure 1, a possible high-level claim structure, expressed using GSN [7], is shown in Figure 2.

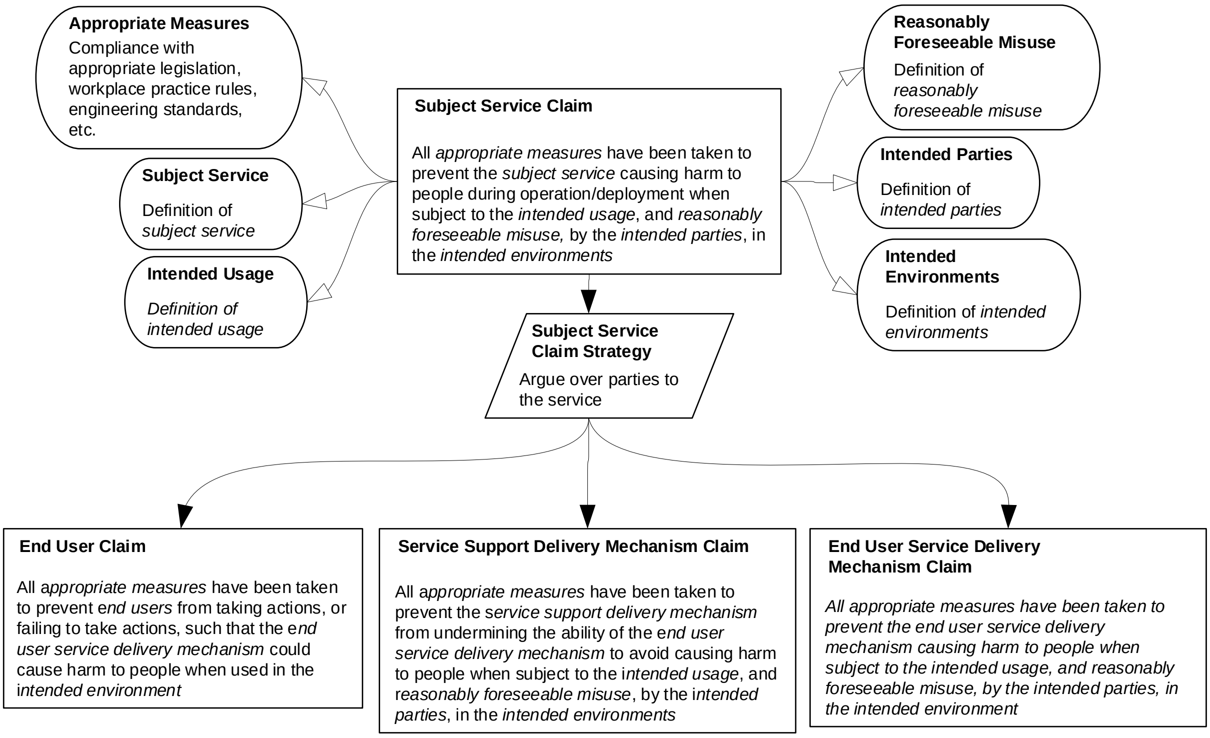
Appropriate Measures
Compliance with appropriate legislation, workplace practice rules, engineering standards, etc.
Subject Service
Definition of subject service
Intended Usage
Definition of intended usage
Subject Service Claim
All appropriate measures have been taken to prevent the subject service causing harm to people during operation/deployment when subject to the intended usage, and reasonably foreseeable misuse, by the intended parties, in the intended environments
Reasonably Foreseeable Misuse
Definition of reasonably foreseeable misuse
Intended Parties
Definition of intended parties
Intended Environments
Definition of intended environments
Subject Service Claim Strategy
Argue over parties to the service
End User Claim
All appropriate measures have been taken to prevent end users from taking actions, or failing to take actions, such that the end user service delivery mechanism could cause harm to people when used in the intended environment
Service Support Delivery Mechanism Claim
All appropriate measures have been taken to prevent the service support delivery mechanism from undermining the ability of the end user service delivery mechanism to avoid causing harm to people when subject to the intended usage, and reasonably foreseeable misuse, by the intended parties, in the intended environments
End User Service Delivery Mechanism Claim
All appropriate measures have been taken to prevent the end user service delivery mechanism causing harm to people when subject to the intended usage, and reasonably foreseeable misuse, by the intended parties, in the intended environment

Figure 2: Generic public service claim structure

The primary claim in Figure 2 concerns the *subject service* not causing harm. In this context harm is prevented by taking the "*appropriate measures*". This phrase is used because, at this level, there is no common approach to avoiding harm that is taken by all the ontological entities that contribute to delivering the service. In practice, the "*appropriate measures*" are often given in the *governing prescriptions*. Depending on the specific ontological entity, *governing prescriptions* may relate to fulfilling safety relevant legal regulations, industry standards and guidelines or to local procedures. The measures may also relate to the provision of training or equipment or to the design of facilities.

The scope of this *subject service claim* is restricted. As the name suggests, *intended usage* states what the service can only be used for, while *reasonably foreseeable misuse* states the extent to which the claim addresses misuse of the service. *Intended parties* states who is allowed to use the service. *Intended environments* states the *physical environment* (e.g. the presence of people, geography, weather) and the social circumstances in which the service can operate. The use of the service outside of these restrictions is not covered by the *subject service claim*. Other *subject service claims* could be defined having wider or narrower scopes.

The ontology shows three ontological entities which interact to deliver the *subject service*. All three of these have the potential to directly affect the *subject service's* ability to cause harm, namely, the *end user*, the *service support delivery mechanism* and the *end user service delivery mechanism*. Therefore, the natural strategy for developing the *subject service claim* is to reframe the *subject service claim* for each ontological entity. It should be noted that meeting these three claims does not necessarily mean the top claim has been met. This may be due to emergent properties or invalid assumptions made by one party about the work of another, which both have the potential to undermine the legitimacy of the top claim.

The people who could potentially be harmed include the *end users* and other people in the *physical environment*.

*End user claim*
The opportunity for people in harms way (e.g., the *end user*) to take action depends on the controls available to them, and these actions could include *reasonably foreseeable misuse*. The less interaction that they can have with the *end user service delivery mechanism*, the less opportunity there is for their actions to cause harm to people.

*Service support delivery mechanism claim*
To substantiate this claim, it is first necessary to identify all the ways in which the performance of each auxiliary service could lead to the *subject service* causing harm. It then has to be demonstrated that each such service has had the *appropriate measures* applied so as to prevent the undesired performance resulting in harm.

*End user service delivery mechanism claim*
To substantiate this claim, it is first necessary to identify all the ways in which the *end user service delivery mechanism* can cause harm. For each of these, it then has to be demonstrated that *appropriate measures* have been applied.

## 2.3 Automotive personal transport service

Figure 3 is an adaption of Figure 1, drawn for the vehicle operating on public roads as a personal transport service.

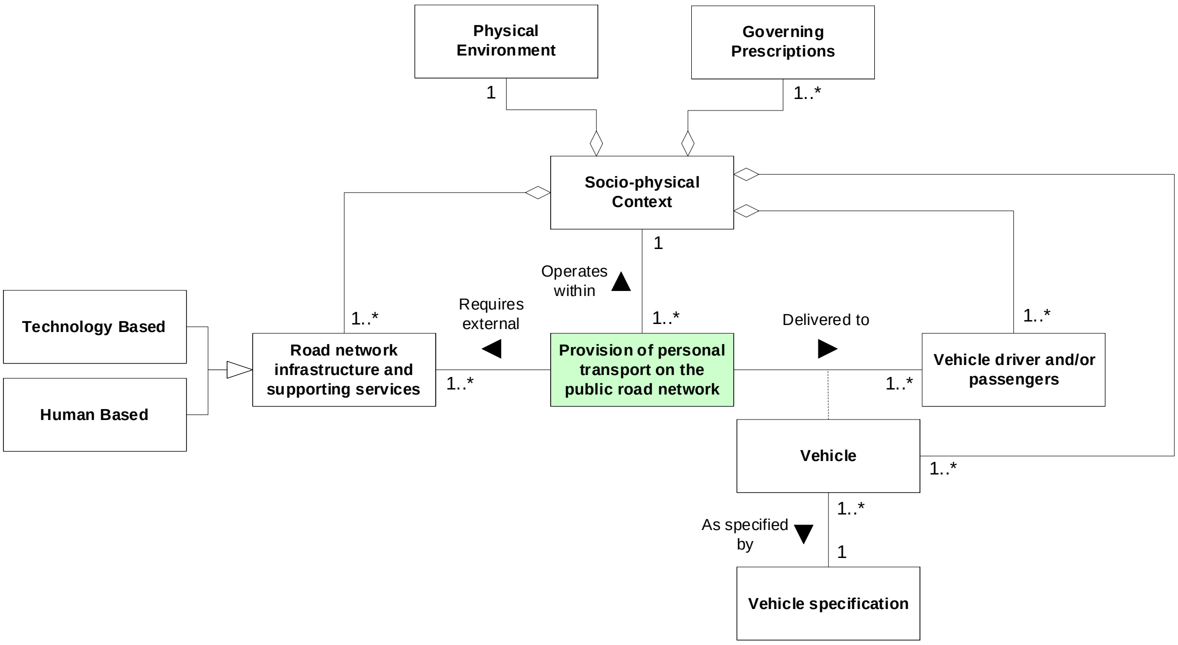

Figure 3: Service view of personal transport on the public road network

Here the generic *subject service* from Figure 1 has been adapted to represent an automotive personal transport system. In this context the *subject service* is the use of a vehicle for personal transport on the public road network. The *end users* are vehicle occupants which could be the *vehicle driver and/or passengers*. Other road users outside the vehicle, e.g. other vehicle occupants, pedestrians, cyclists, are part of the *physical environment* and can be impacted by the service.

The *generic service aspects* block has not been included, as the personal public road transport concept is a well-established notion requiring no further elaboration.

The *vehicle specification* addresses aspects of the vehicle such as the number of people and the amount of goods that can be transported, plus the speed and comfort with which they can be transported and the vehicle's maximum range. It also includes the degree to which the vehicle is self-driven, with or without degrees of assistance, or uses driving automation.

The *service support delivery mechanisms* includes the provision and maintenance of the road network and of control measures, both active and passive. It also includes aspects such as the provision of signage and the provision of weather and traffic information, fuel stations, electric charging points and motorway service stations. The *service support delivery mechanisms* may be *technology based* (e.g., traffic lights), or *human based* (e.g., school crossing patrol warden).

The *governing prescriptions* includes legal regulations and vehicle development and build standards. It also includes laws and guidelines for all users of the road network.

## 2.4 Automotive personal transport service claim structure

Figure 4 shows the generic claim structure from Figure 2 reworked to be applicable to the use of a vehicle for personal transport on the public road network.

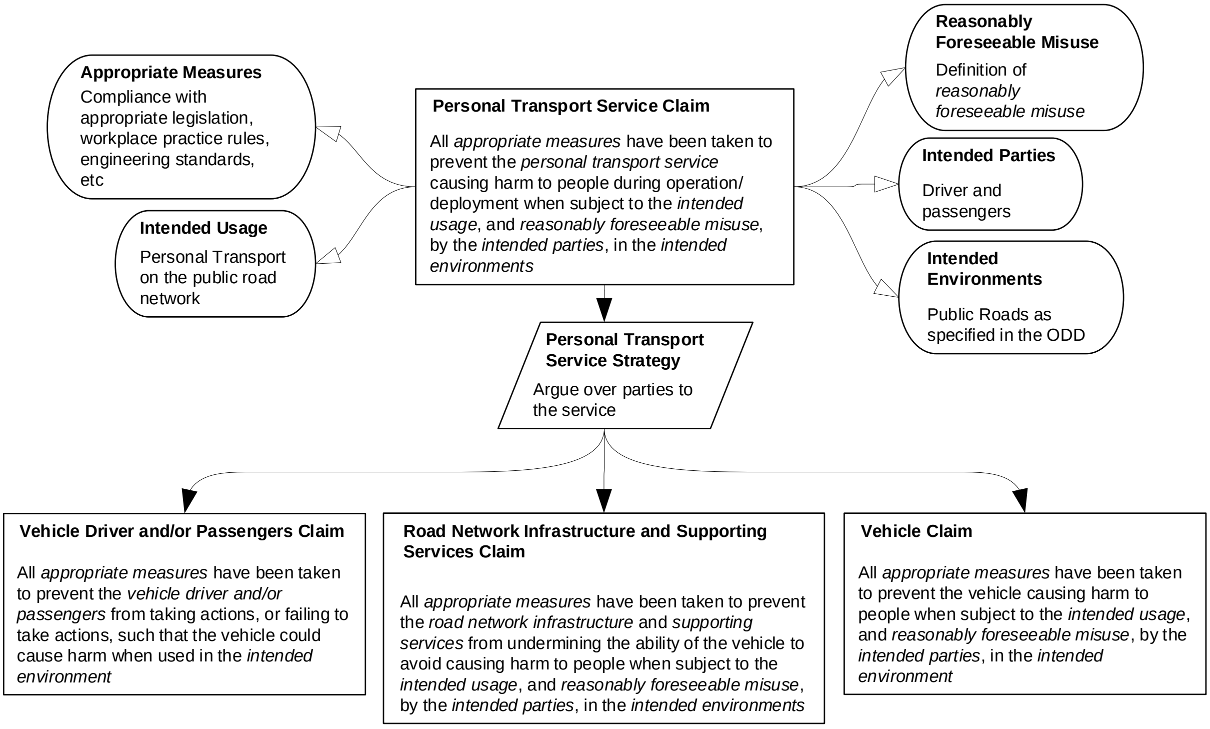
Appropriate Measures
Compliance with appropriate legislation, workplace practice rules, engineering standards, etc
Intended Usage
Personal Transport on the public road network
Personal Transport Service Claim
All appropriate measures have been taken to prevent the personal transport service causing harm to people during operation/ deployment when subject to the intended usage, and reasonably foreseeable misuse, by the intended parties, in the intended environments
Reasonably Foreseeable Misuse
Definition of reasonably foreseeable misuse
Intended Parties
Driver and passengers
Intended Environments
Public Roads as specified in the ODD
Personal Transport Service Strategy
Argue over parties to the service
Vehicle Driver and/or Passengers Claim
All appropriate measures have been taken to prevent the vehicle driver and/or passengers from taking actions, or failing to take actions, such that the vehicle could cause harm when used in the intended environment
Road Network Infrastructure and Supporting Services Claim
All appropriate measures have been taken to prevent the road network infrastructure and supporting services from undermining the ability of the vehicle to avoid causing harm to people when subject to the intended usage, and reasonably foreseeable misuse, by the intended parties, in the intended environments
Vehicle Claim
All appropriate measures have been taken to prevent the vehicle causing harm to people when subject to the intended usage, and reasonably foreseeable misuse, by the intended parties, in the intended environment

Figure 4: Automotive personal transport service claim structure

In this context, the "*appropriate measures*" include fulfilling vehicle legal regulations [8] and the use of automotive standards such as ISO 26262 [2], ISO 21448 [9], and ISO/SAE 21434 [10]. It also includes the use of guidance documents such as MISRA C [11].

The *intended parties* are the vehicle driver and/or passengers and the *intended usage* is the use of a vehicle for personal transport on the public road network.

In this context the *intended environment* is the public road network, possibly constrained by a defined Operational Design Domain (ODD) [12], which includes "environmental, geographical, and time-of-day restrictions, and/or the requisite presence or absence of certain traffic or roadway characteristics." This may include infrequent or exceptional environments, for example accessing a camping pitch in a field.

The people who could potentially be harmed include the *end users* and other people in the *physical environment*.

*Vehicle driver and/or passengers claim*

The opportunity for people in harms way (e.g., the *end user*) to take actions to cause or avoid harm depends on the controls available to them. A vehicle which retains some driver controls related to vehicle movement (e.g., the ability to revert to manual driving), obviously affords the *end user* more scope to cause or avoid harm than a vehicle offering no such manual control provision. Other *end user* actions leading to harm could be related to specifying the destination or operating the doors. The development of this claim may involve making assumptions concerning the expected behaviour of both the driver and the passengers.

*Road network infrastructure and supporting services claim*

The development of this claim requires many different organizations analysing their contributions and applying the measures appropriate to that contribution. There is no reason to presuppose that this activity is not currently undertaken by organizations. However, for the top claim to be met, it is also necessary for the different organizations to know that their rationale does not depend on invalid assumptions concerning other organizations. As there is no one organization that has responsibility for ensuring that this is the case, and it is not known to what extend such assumptions are discharged in practice.

*Vehicle claim*

This claim has been the focus of vehicle manufacturers and their suppliers for many years and is a topic of standards such as ISO 26262 [2], ISO 21448 [9], and ISO/SAE 21434 [10]. The move to fully automated vehicles requires further work in this area. Such work is ongoing, with the development of new guidance material (e.g., ISO/TS 5083 [13]), and the MISRA Safety Case working group also working on this topic.

Figure 4 does raise the question of whether it would be beneficial to have an overall safety argument. This is not the case at present for road transport, or for any comparable service. This situation is unlikely to change, as the responsibilities for the different elements of the service reside with different organizations and there is no central coordination.

It may be seen as being beneficial to have a service level contract between organizations, but this is probably not a practical proposition as it is unlikely that the additional effort involved would be seen as yielding sufficient value. In practice the different organizations only address their own concerns and make assumptions about the work of the other organizations. It would be beneficial if each organization were to operate transparently and document the significant assumptions made concerning the other elements of the overall service. For example, the assumptions about the vehicle capability made by the organizations responsible for the design of the public road infrastructure. However, closely guarded intellectual property and the competitive nature of the automotive industry make this an improbable aspiration.

# 3 Vehicle parts and lifecycle

We now present the second context which considers the potential impact of any vehicle on people during its complete lifecycle from development, through operation and maintenance, to decommissioning. It is acknowledged that the development of a vehicle is a distributed endeavour, with parts being designed by different organizations before being assembled into vehicles. Consequently, claims encompass both the parts and the complete vehicle. In this paper we present a generic approach which applies to both the parts and the whole vehicle.

## 3.1 Ontology

Figure 5 is an ontological model which acknowledges that people can be impacted during any of the different lifecycle phases that a *vehicle*, and its *constituent parts*, typically go through.

Underlying this model is the understanding that the mechanism for causing harm to people is the interaction of physical engineering artefacts with people. By physical engineering artefacts we are referring to the *vehicle* and its *constituent parts* which undergo their own separate development. Processes, protocols, standards, guidelines, human actions, etc. may be in the causal chain, but they are not the mechanism for harm.

The focus on physical engineering artefacts is because it is only these that can cause harm. The mechanisms are typically the transformation of chemical, electrical and potential energy into movement, heat, light or the release of hazardous substances.

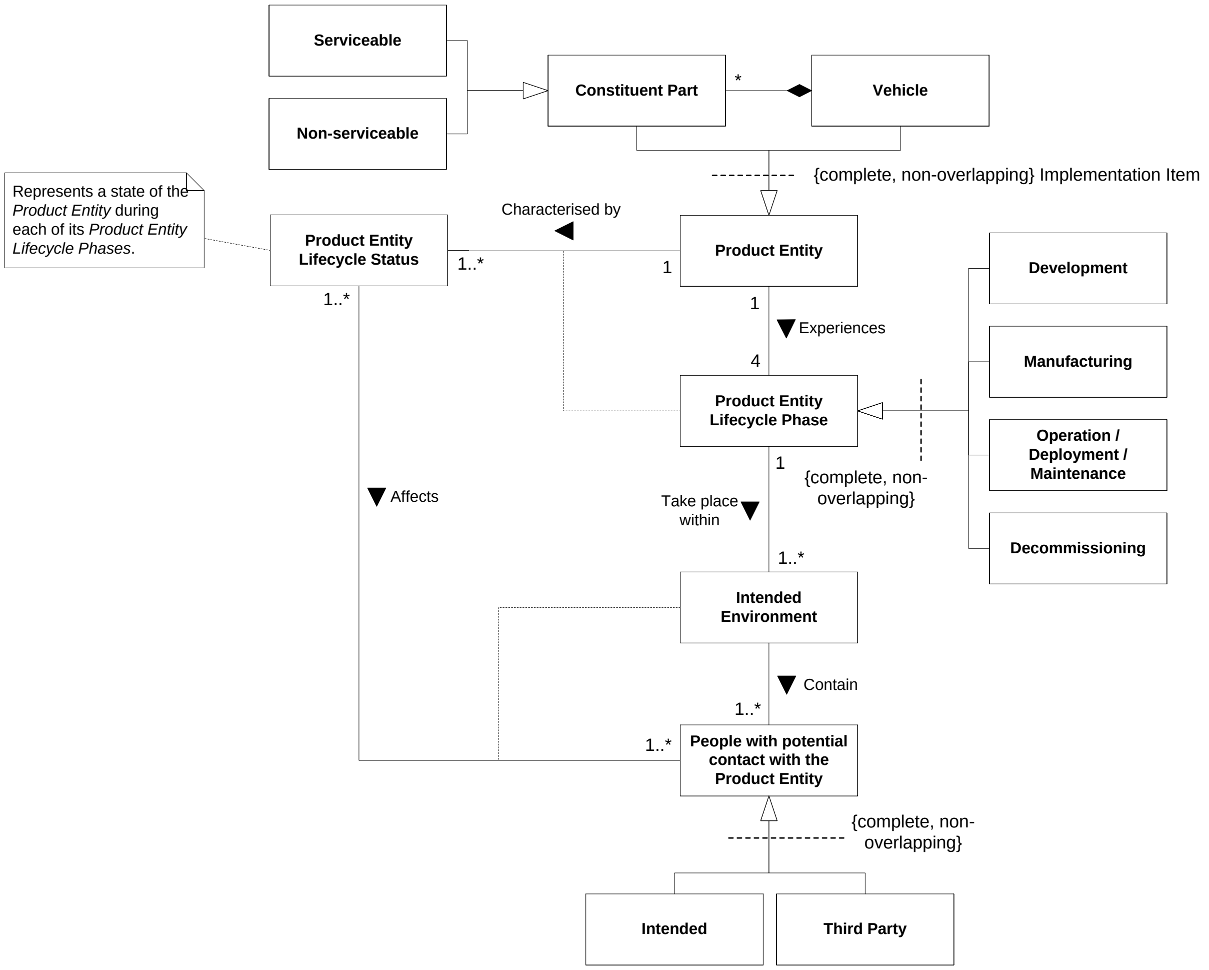
Serviceable
Non-serviceable
Constituent Part
*
Vehicle
{complete, non-overlapping} Implementation Item
Represents a state of the *Product Entity* during each of its *Product Entity Lifecycle Phases*.
Characterised by
Product Entity Lifecycle Status
1..*
1
Product Entity
1..*
1
Experiences
4
Development
Manufacturing
Product Entity Lifecycle Phase
Operation / Deployment / Maintenance
Affects
1
{complete, non-overlapping}
Take place within
Decommissioning
1..*
Intended Environment
Contain
1..*
1..*
People with potential contact with the Product Entity
{complete, non-overlapping}
Intended
Third Party

Figure 5: Product entity ontology

## 3.2 Examples for each lifecycle phase

The subsections below describe the ontological elements for each *product entity lifecycle phase*, depicted in Figure 5.

### 3.2.1 Development

*Product entity lifecycle status*: The *constituent parts* are often tested on rigs, as parts fitted onto donor vehicles (i.e. an existing vehicle with some similarity to the new vehicle being developed) or as parts fitted onto prototype vehicles. During the development lifecycle phase the *vehicle* will evolve through a number of prototypes.

*Intended environment*: The *constituent parts*, and the *vehicle* itself, are typically developed in different physical facilities. These include labs, workshops, rolling roads, test tracks and publicly accessible roads.

*People with potential contact with the product entity*: Those who come into contact with the physical *constituent parts* and the *vehicle* itself may be involved in accidents which could occur in any of the *intended environments*. The *product entity lifecycle status* influences the possible impact that the *product entity* can have on people.

*Intended*: These are the people who are intended to come into contact with the physical *constituent parts*, and the *vehicle* itself. People with intended contact will typically be the development staff and other authorized personnel, such as the company's managers.

*Third parties*: Visitors to the development areas may also come into contact with the physical *constituent parts* and the *vehicle* itself. When donor or prototype vehicles are used on publicly accessible roads, then the general public may also come into contact with the *vehicle*.

### 3.2.2 Manufacturing

*Product entity lifecycle status*: The *constituent parts* and the *vehicle* are produced on a production line and therefore exist in a number of incomplete incarnations before evolving into the finish item. The *constituent parts* and the *vehicle* may also exist in an incomplete state off the production line due to lack of components or because they are in need of rectification.

*Intended environment*: The manufacture of both the *constituent parts* and the *vehicle* takes place in a manufacturing plant. Typically, the *constituent parts* will be manufactured in a supply chain, with manufacturing responsibility being shared between several organisations.

*People with potential contact with the product entity*: Those who come into contact with the physical *constituent parts* and the *vehicle* itself may be involved in accidents which could occur in the manufacturing plant. The *product entity lifecycle status* influences the possible impact that the *product entity* can have on people.

*Intended*: These are the people who are intended to come into contact with the physical *constituent parts*, and the *vehicle* itself. People with intended contact will typically be the assembly staff, development staff and the company managers.

*Third parties*: Visitors to the manufacturing plant may also come into contact with the physical *constituent parts* and the *vehicle* itself. For example, visitors might include logistics and supply chain staff.

### 3.2.3 Operation, deployment and maintenance

The whole *vehicle* and its *serviceable constituent parts* are in scope within this phase.

*Product entity lifecycle status*: The *vehicle* may be fault free or experiencing a fault or a failure. It may be moving, or it may be stationary.

*Intended environment*: There are a number of different environments that a vehicle may encounter during this phase. While driving on the roads, the *vehicle*, or one of its systems, may be considered to be inside, or outside, the ODD (Operational Design Domain) that it was designed for. When not driving on the roads, the *vehicle* may be in a car park or layby/pullout or may be being fuelled or charged. During maintenance or repair the *vehicle* may be in a workshop. If it is involved in a crash, then the crash site itself is another environment.

*People with potential contact with the product entity*: Those who come into contact with the physical *serviceable constituent parts* and the *vehicle* itself may be involved in accidents which could occur in any of the intended environments. The *product entity lifecycle status* influences the possible impact that the *product entity* can have on people.

*Intended*: These are the people who are intended to come into contact with the *vehicle* or its *serviceable constituent parts*. People with intended contact will typically be the vehicle driver and passengers as well as maintenance and repair staff.

*Third parties*: Those who may come into contact with the *vehicle* include other road users, emergency service personnel (police, fire, ambulance, breakdown, etc.) and malicious actors e.g. thieves.

### 3.2.4 Decommissioning

*Product entity lifecycle status*: The *constituent parts* and the *vehicle* may exist in a number of incomplete incarnations before being completely disassembled or destroyed.

*Intended environment*: Due to the use of hazardous materials, for example pyrotechnics (as used for airbags) and lithium-ion batteries, the decommissioning of the *vehicle* should take place in a specialized facility. *Constituent parts* may also need to be decommissioned in specialized facilities.

*People with potential contact with the product entity*: Those who come into contact with the physical *constituent parts* and the *vehicle* itself may be involved in accidents which could occur in the decommissioning plant.

*Intended*: These are the people who are intended to come into contact with the *constituent parts*, and the *vehicle* itself. Intended people contacts will typically be the decommissioning staff, the company managers and anyone associated with the handling and distribution of used *constituent parts*, e.g. a breaker's yard.

*Third parties*: Visitors to the decommissioning plant may also come into contact with the physical *constituent parts* and the *vehicle* itself.

## 3.3 Product entity claim

The ontology (**Figure 5**) covers both the *vehicle* and its *constituent parts*. A single claim structure cannot cover both aspects adequately. At the *vehicle* level the goal is to phrase a claim in terms of preventing harm to people. This is possible because the *vehicle* behaviour can be directly related to the ways in which people can be harmed. However, for a *constituent part* without the context of the whole vehicle design, it is not always possible to determine the relationship between the behaviour of the *constituent part* and the behaviour of the *Vehicle.*

For the lower levels of *constituent parts* the issues that need to be understood, foreseen and addressed are phrased in terms of failure modes or deviations from specification. Responses to these issues take the form of prevention, detection, mitigation and communication. These terms would be used in the claim structure for the *constituent parts*, in contrast to those illustrated in the *vehicle* claim structure of Figure 6. In this paper we only address the *vehicle* level claim.

It should be noted that having a valid safety assurance argument for each of the vehicle's *constituent parts* does not obviate the need for a valid safety assurance argument for the *vehicle*; it is still possible to construct an "unsafe vehicle" from "safe parts".

The *vehicle claim* structure follows the same style as the *generic public service claim structure*. As our interest is in preventing harm to people, the claim is phrased in these terms and carries over the same type of contextual information as previously used:

> All *appropriate measures* have been taken to prevent the *vehicle* causing harm to people during any of its lifecycle phases when subject to the *intended usage*, and *reasonable foreseeable misuse*, by the *intended parties*, in the *intended environment*.

The ontology is defined in terms of the *product entity lifecycle phases*, therefore the natural strategy for developing the claim is to reframe the *product entity claim* for each lifecycle phase. This is shown in Figure 6.

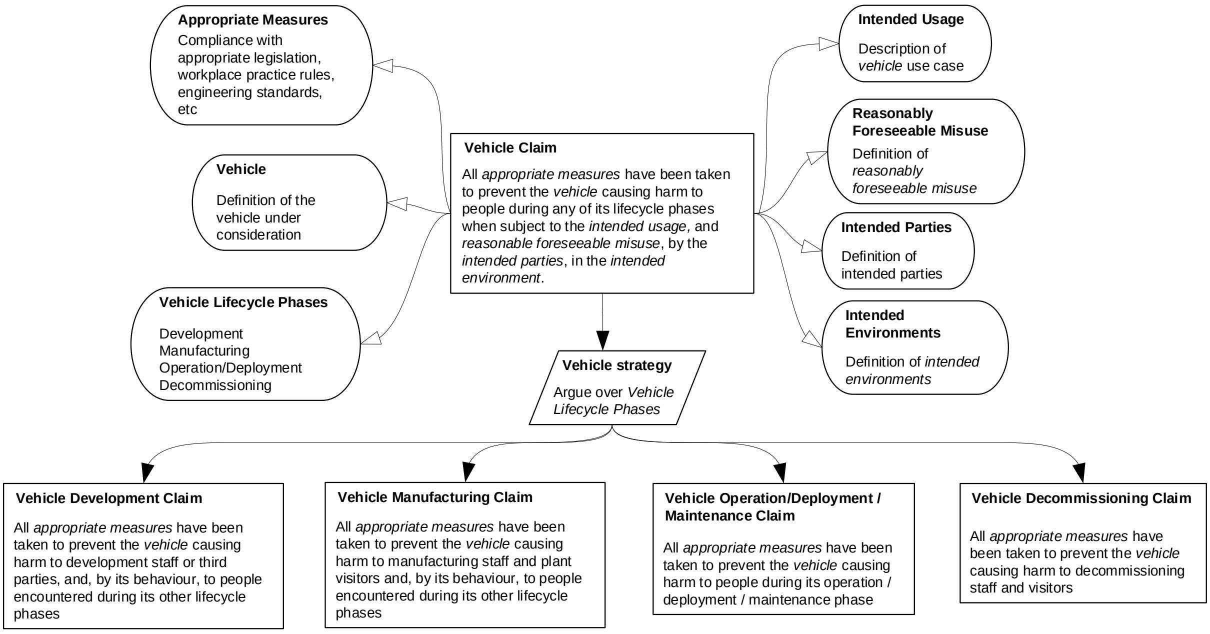
Appropriate Measures
Compliance with appropriate legislation, workplace practice rules, engineering standards, etc
Vehicle
Definition of the vehicle under consideration
Vehicle Lifecycle Phases
Development
Manufacturing
Operation/Deployment
Decommissioning
Vehicle Claim
All appropriate measures have been taken to prevent the vehicle causing harm to people during any of its lifecycle phases when subject to the intended usage, and reasonable foreseeable misuse, by the intended parties, in the intended environment.
Intended Usage
Description of vehicle use case
Reasonably Foreseeable Misuse
Definition of reasonably foreseeable misuse
Intended Parties
Definition of intended parties
Intended Environments
Definition of intended environments
Vehicle strategy
Argue over Vehicle Lifecycle Phases
Vehicle Development Claim
All appropriate measures have been taken to prevent the vehicle causing harm to development staff or third parties, and, by its behaviour, to people encountered during its other lifecycle phases
Vehicle Manufacturing Claim
All appropriate measures have been taken to prevent the vehicle causing harm to manufacturing staff and plant visitors and, by its behaviour, to people encountered during its other lifecycle phases
Vehicle Operation/Deployment / Maintenance Claim
All appropriate measures have been taken to prevent the vehicle causing harm to people during its operation / deployment / maintenance phase
Vehicle Decommissioning Claim
All appropriate measures have been taken to prevent the vehicle causing harm to decommissioning staff and visitors

Figure 6: Vehicle lifecycle claim structure

The phrase "*all appropriate measures*" is used because at this level of abstraction there is still no common approach to avoiding harm in all the different *product entity lifecycle phases*. Depending on the particular circumstances, the "*appropriate measures*" may relate to fulfilling safety relevant legal regulations, industry standards and guidelines or local procedures. It may also relate to the provision of training or equipment or the design of facilities.

By still continuing to use the phrases "*the intended usage, and reasonably foreseeable misuse, by the intended parties, in the intended environments*" the claim acknowledges that there may be circumstances that are not covered by the overall claim.

*Vehicle claim*

There are two categories of people who could be harmed as a results of activities in the development phase, the development staff themselves and those who encounter the *vehicle* in this and other phases.

The prevention of harm to the development staff is usually addressed by health and safety at work procedures. The *appropriate measures* to avoid harm during the *operation, deployment and maintenance* phase currently include the activities covered by ISO 26262 [2], ISO 21448 [9] and ISO/SAE 21434 [10]. The *manufacturing* phase may rely on *constituent part* functionality to avoid harm during assembly. This is similar for repair during *operation, deployment and maintenance* phases and for the *decommissioning* phase during disassembly.

*Vehicle manufacturing claim*

Again, there are two categories of people who could be harmed as a result of activities in the manufacturing phase, the manufacturing staff themselves and those who encounter the *vehicle* during the manufacturing phase.

The prevention of harm to the manufacturing staff is usually addressed by health and safety at work procedures.

*Vehicle operation, deployment and maintenance claim*

This claim is usually based on the collection of data showing the actual performance achieved by the *vehicle* in the field, and the actions taken to maintain that desired performance and to address any incidents that occur.

The prevention of harm to people in this phase typically relies on ensuring that the *vehicle* performance achieved when new is maintained throughout its operating life, using techniques such as regular maintenance schedules, product recalls, etc.

*Vehicle decommissioning claim*

The prevention of harm to the decommissioning staff is usually addressed by health and safety at work procedures.

It is recognized that many measures are already in place to mitigate against the potential for the *vehicle* to cause harm to people during each of the *vehicle lifecycle* phases, even though they are not presented as part of the claim structure. Our concern is in how these measures may be affected by the rapid development of ADS equipped vehicles and the challenges this may present to the creation of safety assurance arguments.

# 4 Summary

In this white paper we have presented two contexts relevant to the development of automated driving system equipped vehicles when considering the prevention of harm to people: personal transport as a service and the complete lifecycle.

These contexts represent different overlapping layers of a complex picture, which we have teased apart to provide clarity. There is no intent for a direct connection between the two sets of ontologies and claim structures produced. The claim structures illustrate the full scope of the claims that can be associated with producing, using and disposing of an ADS equipped vehicle. However, in each case no single argument is currently produced.

Future work will incorporate the insights from these two contexts into developing ontologies and claim structures for the design, deployment and operation of a high or full automated driving vehicle. In particular, the following are expected to be significant:

- The *product entity*
- *Appropriate measures* context
- *Intended usage* context
- *Reasonably foreseeable misuse* context
- *Intended parties* context
- *Intended environments* context
- Assumptions regarding the *vehicle driver and/or passengers*
- Assumptions regarding the *road network infrastructure and supporting services*.
- Assumptions about manufacturing
- Assumptions about decommissioning

## 4.1 Terminology

The majority of terminology used is defined within the document. The following table defines additional key terms.

| Type | Description |
|---|---|
| Harm | Physical injury or damage to the health of persons. |
| Safety case | Argument that functional safety is achieved for items, or elements, and satisfied by evidence compiled from work products of activities during development. |
| System | Set of components or sub-components that relates at least a sensor, a controller and an actuator with one another. |

# 5 References

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

[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 04/02/2024)

[5] A. Ziebinski, R. Cupek, D. Grzechca, and L. Chruszczyk, "*Review of Advanced Driver Assistance Systems (ADAS)*", presented at the AIP Conference, 2017. https://pubs.aip.org/aip/acp/article-abstract/1906/1/120002/681133/Review-of-advanced-driver-assistance-systems-ADAS?redirectedFrom=fulltext (accessed 04/02/2024)

[6] SysML Open Source Specification Project. Available: http://www.sysml.org/ (accessed 04/02/2024)

[7] SCSC-141C:2021, "*Goal Structuring Notation Community Standard Version 3*", editor: Safety-Critical Systems Club C.I.C., 2021. https://scsc.uk/r141C:1?t=1 (accessed 04/02/2024)

[8] UK Parliament (07/09/23). *The Road Vehicles (Approval) Regulations 2020*. Available: https://www.legislation.gov.uk/uksi/2020/818/made (accessed 04/02/2024)

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

[10] ISO/SAE 21434 *Road vehicles — Cybersecurity engineering*

[11] MISRA C:2023 *Guidelines for the Use of the C Language in Critical Systems*, ISBN 978-1-911700-08-1 (paperback), ISBN 978-1-911700-09-8 (PDF), The MISRA Consortium Limited, 2023.

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

[13] ISO/TS 5083 *Road vehicles — Safety for automated driving systems — Design, verification and validation*. Under development

# 6 Revision history

| Revision | Description of changes | Release date |
|---|---|---|
| Version 1.0 | First version release | April 2024 |