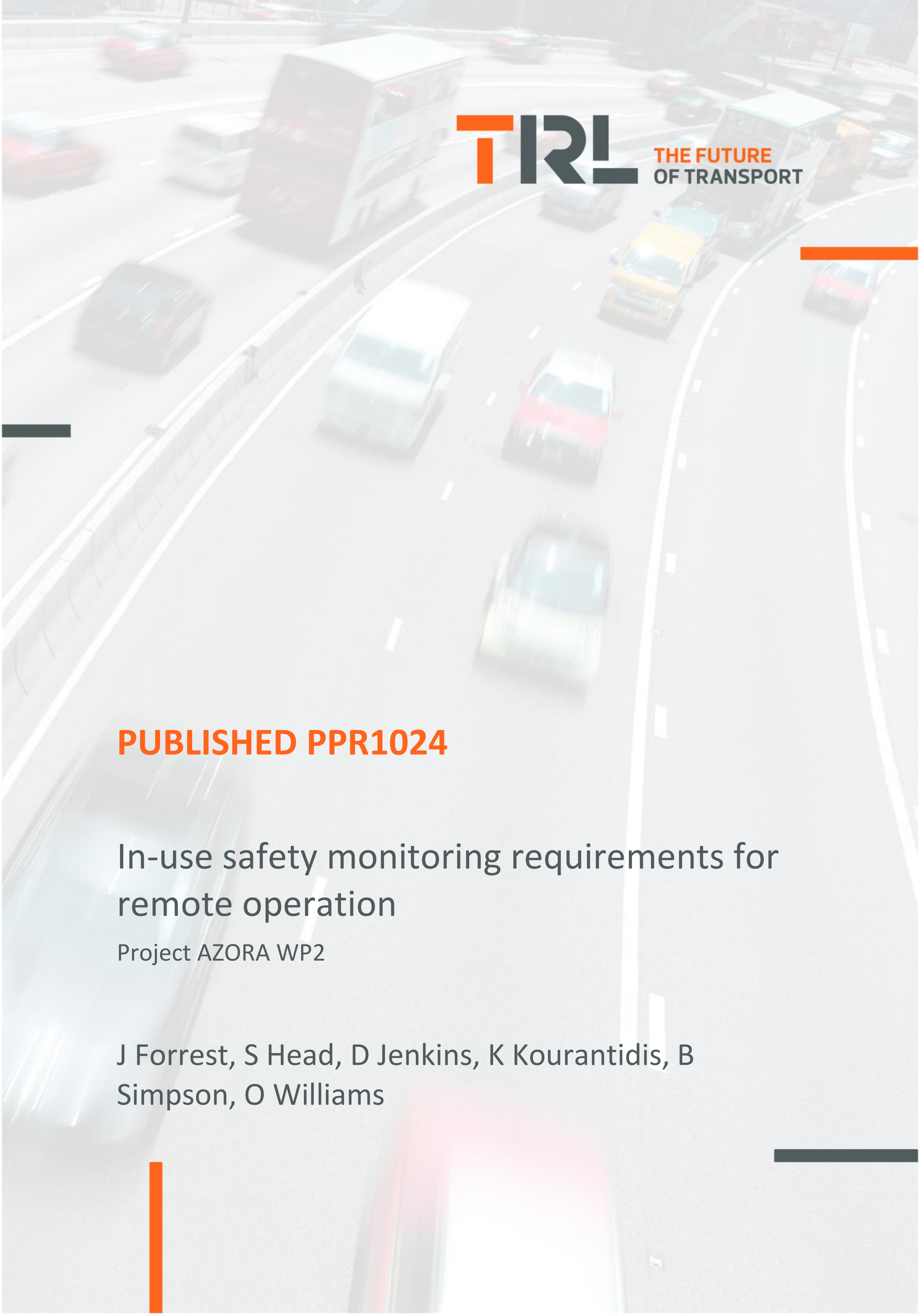


PUBLISHED PPR1024

In-use safety monitoring requirements for remote operation

Project AZORA WP2

J Forrest, S Head, D Jenkins, K Kourantidis, B Simpson, O Williams

Report details

Report prepared for:	Innovate UK		
Project/customer reference:	11226168		
Copyright:	© TRL Limited		
Report date:	March 2022		
Report status/version:	V0.1		
Quality approval:			
Richard Oliver (Project Manager)		Will Perren (Technical Reviewer)	

Disclaimer

This report has been produced by TRL Limited (TRL) under a contract with Innovate UK. Any views expressed in this report are not necessarily those of Innovate UK

The information contained herein is the property of TRL Limited and does not necessarily reflect the views or policies of the customer for whom this report was prepared. Whilst every effort has been made to ensure that the matter presented in this report is relevant, accurate and up to date, TRL Limited cannot accept any liability for any error or omission, or reliance on part or all of the content in another context.

When purchased in hard copy, this publication is printed on paper that is FSC (Forest Stewardship Council) and TCF (Totally Chlorine Free) registered.

Contents amendment record

This report has been amended and issued as follows:

Version	Date	Description	Editor	Technical Reviewer
V0.1	09/03/2022	First draft for submission to AZORA consortium	SH, DJ, BS, OW	WP

Document last saved on:	11/04/2022 12:02
Document last saved by:	David Jenkins

Table of Contents

1 Introduction

TRL have been commissioned to work on the Autonomous Zero Occupancy with Remote Authority (AZORA) project, which brings together experts from Oxbotica, TRL, Ocado, BSI and UKAEA-RACE to understand the requirements for the safe remote operation of automated vehicles within visual line of sight.

This report covers part of the project's second work package (WP2), focusing on how the safety of automated vehicles (AVs) can be monitored while being driven by a Remote Operator, and how data collected during this process can be shared and used to improve safety across remote operation trials.

This report details the hazard analysis approach undertaken to identify the hazards and associated causes related to remote operation. This report also explores how data collected through in-use monitoring could be used to understand and improve the standard of safety for all trials involving remote operation.

The report builds on the first WP2 deliverable, *Safety Case Requirements for Visual Line of Sight Remote Operation*, by identifying the in-use monitoring requirements for remote operation of an automated vehicle. In-use monitoring is necessary to ensure the remotely operated vehicle is performing safely by identifying measurable information that can be used as metrics to assess the safety performance of both the vehicle and the Remote Operator. To do this, the report identifies different levels of hazardous events that may happen during remote operation of a vehicle, identifying failure modes and their causes to create in-use monitoring metrics to ensure a high level of safety when using remote operated vehicles.

2 Definitions

2.1 Remote operation[1]

Remote operation is an umbrella term that encompasses the functions needed to support the operation of an AV or a fleet of AVs by a Remote Operator. Remote operation includes both driving and non-driving related tasks. During remote operation, the Operator may have full authority for the AV's actions, the AV may retain final authority, or it may be split depending on the system design, maturity and safety assessments of the Automated Driving System (ADS) developer and trialling organisation.

[1] Definition taken from https://trl.co.uk/publications/remote-operation-of-connected-and-automated-vehicles--summary-report-

2.2 Remote Operator

A Remote Operator is a generic term for a human who supervises the operation of an AV from a remote location. Supervision can comprise monitoring the AV, intervening in the AVs' operation, assisting passengers, or managing part of the AV service. The supervision of operations may need to be real-time, such as for remote driving, and the Remote Operator may or may not have final authority for control of the AV[2].

A Remote Operator can be based either within Visual Line of Sight (VLOS), when the Remote Operator can see the vehicle, or Beyond Visual Line of Sight (BVLOS), for example, when the Remote Operator is at a remote workstation.

2.3 In-use monitoring

In-use monitoring is the real-time of assessment of a vehicle's safety performance during its operation. In-use monitoring principally involves the collection of data to generate a series of metrics. These metrics are indicators that a hazardous event has, or is likely to, occur. Therefore, monitoring and reducing the frequency of these metrics can lead to a reduction in unsafe events and ensure the operation of the vehicle is safe. It also provides the data necessary to evaluate causal and contributory factors relating to unsafe events and high risk scenarios so that safety learnings can be generated. The scope of this in-use monitoring task includes any metrics that relate to the remote operation of AVs, including metrics relating to the Remote Operator, the ADS and the connection between the vehicle and operator.

3 Methodology

To understand the requirements for in-use monitoring of remotely operated vehicles it is necessary to look at what the possible hazards associated with remote operation and what the causes of those hazards are. Taking this approach, a list of hazardous events can be generated. These events are then classified as either Level 1, Level 2 or Level 3 causes. Metrics were then developed that would detect when these events occurred.

4 Hazardous events – levels of causes

4.1 Level 1 causes

The top-level hazardous event is the physical event or trigger that directly leads to an incident – the Level 1 hazardous event. Therefore, identifying such events is the first step towards assessing what could go wrong during the course of a remote operation trial.

[2] Definition taken from https://trl.co.uk/publications/remote-operation-of-connected-and-automated-vehicles--summary-report-

There are several things that can go wrong when an entity is driving a vehicle, and thus be classified as a Level 1 hazardous event. These events relate to interactions between the vehicle and other actors or objects within the environment and are inherently hazardous. They are independent of how the vehicle is controlled, whether this is an in-vehicle driver, an external (remote) operator, or an ADS. Metrics for such hazards are generally related to physical aspects of vehicle behaviour, and may be objectively measured. To identify events, the capture of data related to a metric is triggered when they exceed a pre-established threshold. Table 1 presents some example Level 1 causes, and metrics that could be used to identify when they occur.

Table 1: Example Level 1 hazardous events and related metrics

Level 1 hazardous event	Possible identifying metric
The vehicle is driven erratically	Vehicle acceleration
Traffic infractions (i.e., violations) committed by the remotely operated vehicle	Counts of infractions
Vehicle left unattended in an unsafe location	Time (e.g., how long the vehicle is left unattended)
Proximity conflicts with other actors or objects.	TTC

Level 1 events are hazardous, irrelevant of why they happened. For example, driving through a red traffic signal is an unacceptable and unsafe action regardless of whether it happened because:

i) The driver was tired and didn't notice;

ii) The Remote Operator controlling the vehicle lost connection with the vehicle and was unable to stop;

iii) The Remote Operator monitoring the vehicle thought the ADS would stop and therefore took no action; and

iv) The ADS failed to recognise the traffic signals so didn't stop.

These events can be compared by the number of times the event (e.g., infraction) happened, or amount of time the threshold (e.g., acceleration, TTC) was exceeded. Events are likely to be comparable across all types of operation, while thresholds are likely to vary across conventional operation, remote operation, and automated operation. For example, it is not well understood whether a Remote Operator needs the same size safety envelope as an in-vehicle driver. These events are not necessarily specific to remote operation; nonetheless, they may occur during remote operation, and remote operation may be the cause of such events or increase the severity if these events do occur, and they should therefore be monitored. Figure 1(below) presents all the Level 1 causes identified, followed by the metrics that can detect if each specific event has occurred.

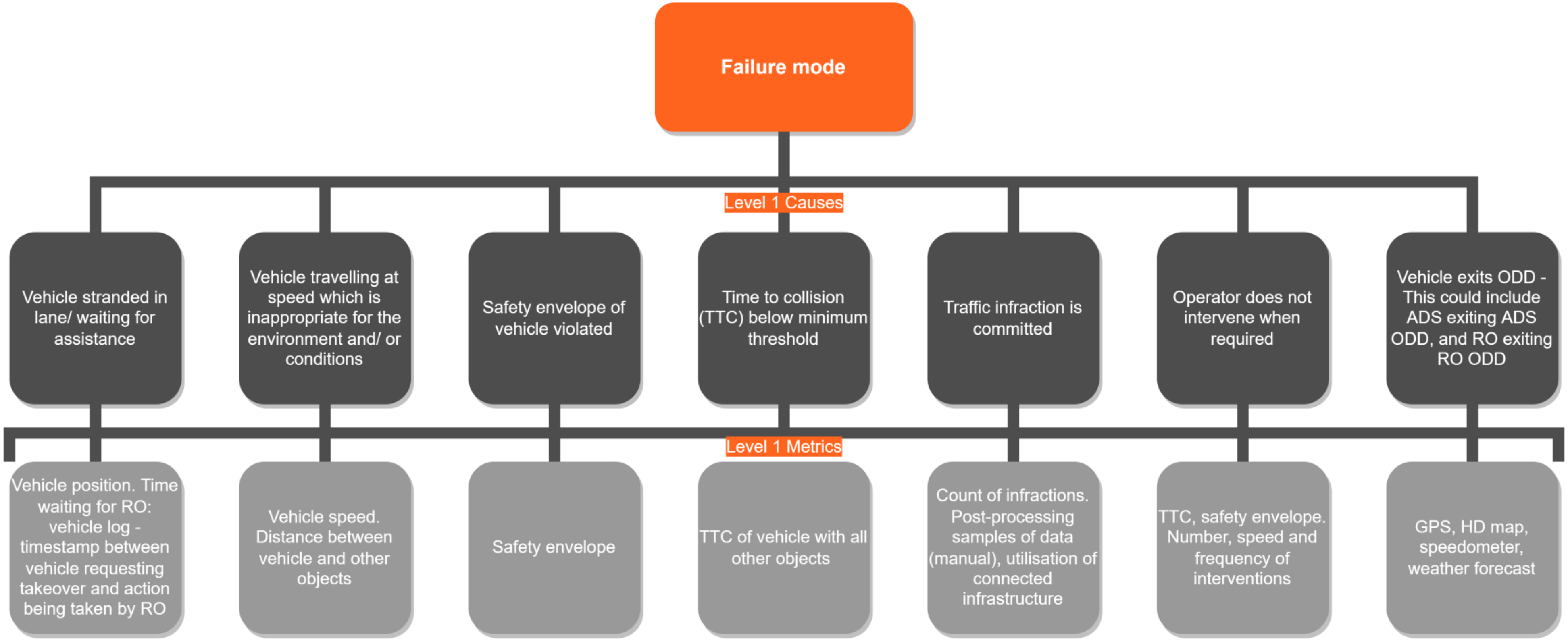
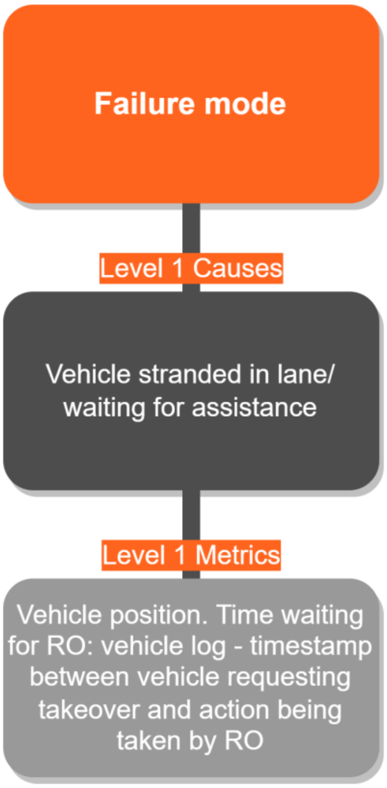

Failure mode
Level 1 Causes
Vehicle stranded in lane/ waiting for assistance
Vehicle travelling at speed which is inappropriate for the environment and/ or conditions
Safety envelope of vehicle violated
Time to collision (TTC) below minimum threshold
Traffic infraction is committed
Operator does not intervene when required
Vehicle exits ODD - This could include ADS exiting ADS ODD, and RO exiting RO ODD
Level 1 Metrics
Vehicle position. Time waiting for RO: vehicle log - timestamp between vehicle requesting takeover and action being taken by RO
Vehicle speed. Distance between vehicle and other objects
Safety envelope
TTC of vehicle with all other objects
Count of infractions. Post-processing samples of data (manual), utilisation of connected infrastructure
TTC, safety envelope. Number, speed and frequency of interventions
GPS, HD map, speedometer, weather forecast

Figure 1: Level 1 causes and metrics.

To provide a more detailed example, Figure 2 below, draws out one of the hazardous events associated with remote operation and related metrics that should be put in place to identify its occurrence during operation.

The Level 1 event shown in Figure 2 is that the vehicle is stranded in a lane waiting for assistance - this is specific to remote operated vehicles. If a remote operated vehicle becomes stranded, it will contact the Remote Operator for assistance. The time it takes for the Remote Operator to assist the remote operated vehicle is crucial to ensure no further problems occur. To identify, and then ultimately address, the issue, the Level 1 metrics in the subsequent box should be monitored. For example, the time waiting for the Remote Operator (RO) should be monitored to ensure that this is within acceptable limits. This could be done by looking at the timestamp between the vehicle requesting the takeover and action being taken by the RO. As previously highlighted, the threshold for acceptability will vary across types of operation and is yet to be determined.


Failure mode

Level 1 Causes

Vehicle stranded in lane/ waiting for assistance

Level 1 Metrics

Vehicle position. Time waiting for RO: vehicle log - timestamp between vehicle requesting takeover and action being taken by RO

Figure 2 A section of figure 1 highlighting the Level 1 event and Level 1 metric to monitor.

4.2 Level 2 and Level 3 causes

Hazardous events can occur for a variety of reasons. To understand the root cause of the event, the question must be asked ‘why did something go wrong?’. This helps further identify what should be measured and monitored during remote operation.

As discussed in Section 4.1, there are lots of reasons why an entity could fail to stop at a red traffic signal. However, these reasons are likely to be different for remote operation when compared with conventional or automated driving. Therefore, it is important to understand what can go wrong with remote operation systems which can cause hazardous events and how to monitor those risks. As a result, there are many metrics (e.g., Remote Operator welfare) that would need to be monitored for remote operation that would not need to be monitored for other forms of operation.

Therefore, metrics which relate to why an event occurred tend to be:

i) Specific to remote operation;

ii) Indicators of whether certain aspects of the remote operation system are functioning as intended; and

iii) Where most of the in-use monitoring for remote operation focuses

Examples of these include:

i) Operator welfare and distraction;

ii) Operator’s ability to have situational awareness and control of the vehicle from an external location;

iii) System latency; and

iv) Connection between vehicle and Remote Operator

4.2.1 The difference between Level 1 and Level 2 and 3

Level 2 causes are essentially categories of why the event occurred, with Level 3 causes being the specific area of fault. Level 1 hazardous events can be the result of one or more Level 2 causes, which in turn can be the result of one or more Level 3 causes. Conversely Level 2 or 3 causes can occur but may not lead to a level 1 hazardous event – however they indicate poor system (including Remote Operator) performance which may lead to a hazardous event in the future. As such, these lower level causes need to be captured.

Figure 3 (below) illustrates the Level 2 cause of ‘information not being transmitted between operator and vehicle due to a breakdown in communication’. This in turn can be the result of one or more of the Level 3 causes which fall underneath. The Level 3 metrics apply to a Level 3 Cause and the metric specifies what should be monitored.

The metrics would identify why something went wrong by monitoring the Level 2 and 3 causes. These further levels recognise that the reasons behind a hazardous event occurring are often multi-layered, and that each of these layers can be observed by different means.

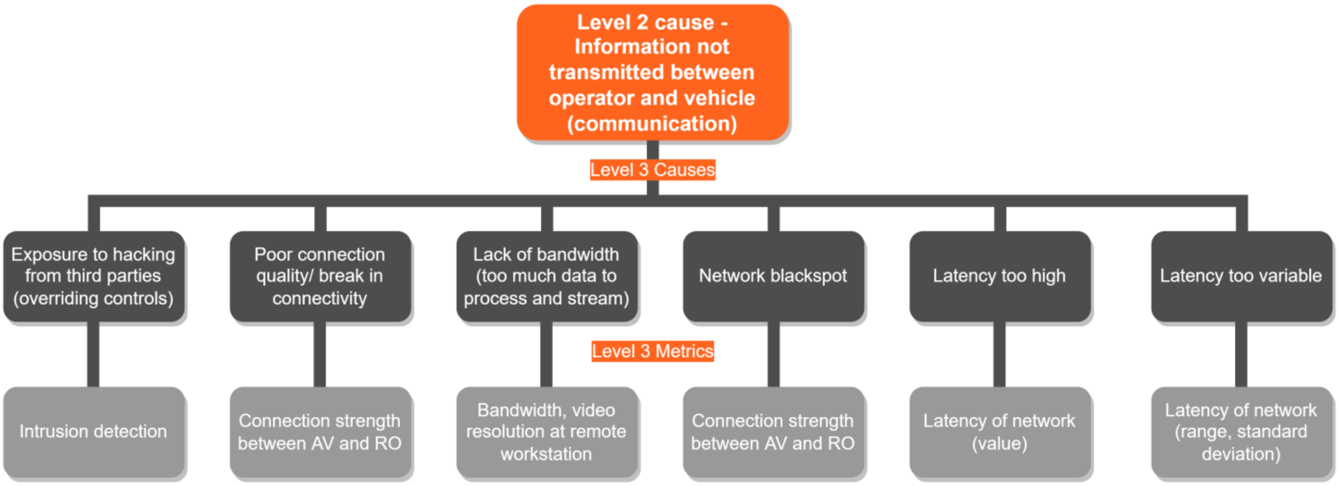

Level 2 cause - Information not transmitted between operator and vehicle (communication)
Level 3 Causes
Exposure to hacking from third parties (overriding controls)
Poor connection quality/ break in connectivity
Lack of bandwidth (too much data to process and stream)
Network blackspot
Latency too high
Latency too variable
Level 3 Metrics
Intrusion detection
Connection strength between AV and RO
Bandwidth, video resolution at remote workstation
Connection strength between AV and RO
Latency of network (value)
Latency of network (range, standard deviation)

Figure 3- Example Level 2 cause and Level 3 causes and metrics.

The other Level 2 causes consist of:

i) Problems with transition;

ii) RO inattention;

iii) Operator welfare;

iv) Interaction with general public;

v) Vision;

vi) Inadequate operator facilities and controls;

vii) Environmental conditions; and

viii) Perception and awareness.

These causes are all related to why something may go wrong during a remote operation trial. They will all have different Level 3 causes underneath them followed by metrics for the in-use monitoring. A full set of flow charts for all Level 2 causes and metrics can be found in 7Appendix B

Finally, while many of the causes of a hazardous event can be directly observed, there are some for which data cannot be collected while in-use. Typically, these are events which require understanding of the reasoning behind the Remote Operator's actions. In the example of a vehicle running a red light because the Remote Operator did not intervene when the ADS took a wrong action, this may have occurred because the operator placed too much trust in the ADS while monitoring, and therefore thought it would take action. However, this level of detail cannot be obtained through metric based in-use monitoring and would require further investigation after the event.

5 Use cases

Remote operation is an umbrella term which encompasses a range of modes of operation in a range of environments, using a range of vehicle types. The hazardous events, and by extension the metrics which should be monitored while in use in order to identify those events, are likely to be different across these implementations of remote operation. As such, in order to help understand how different metrics might be applied in trials, it is useful to look at some potential use cases for remote operation which highlight these differences. To provide further detail, an estimated frequency and severity is identified for each cause for each use case, to give an indication of how important the measurement of each metric is. Some hazardous events and associated causes may be present in multiple use cases; however, the risk they pose may differ in both frequency and severity.

Examples of the difference in risk are as follows:

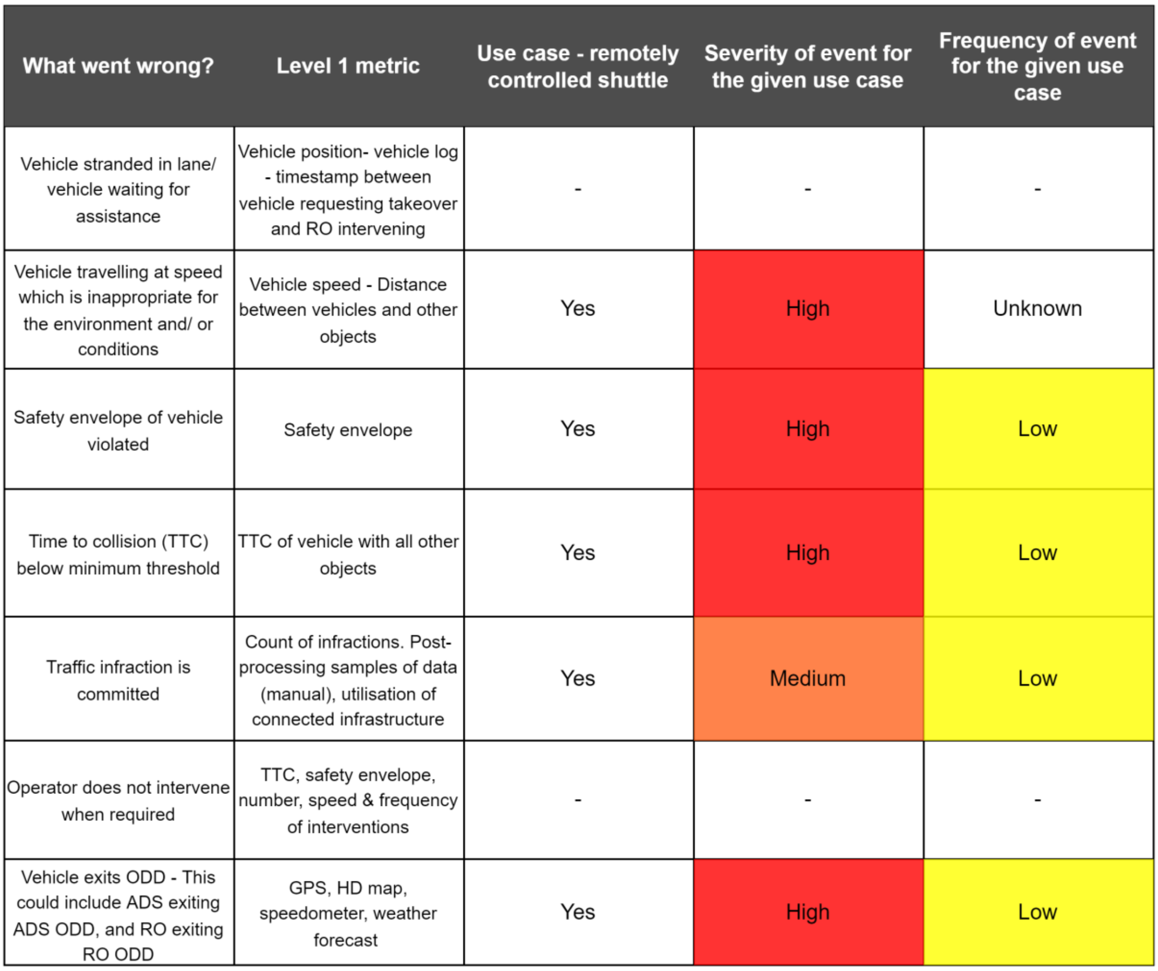
i) a passenger-carrying vehicle which is stranded on a busy road presents a much greater risk than a stranded machine in a controlled environment such as a warehouse; and

ii) a temporary drop in communications connection between the vehicle and the Remote Operator is more likely to occur for a vehicle operating in a mine than in a state-of-the-art warehouse.

Therefore, TRL has completed a hazard analysis exercise to indicate the likelihood and severity of certain events that may occur for different remote operation applications.

As an example, Table 2 below examines the use-case of a remotely controlled shuttle. The remotely controlled shuttle is an example of on-road remote driving that experiences a constant level of monitoring by an operator who would control one vehicle. The shuttle would be within a low-speed environment while operating at a low speed; however, the environment it is in would be uncontrolled.

Table 2: Frequency and severity of risk factors for remotely controlled shuttles.



What went wrong?	Level 1 metric	Use case - remotely controlled shuttle	Severity of event for the given use case	Frequency of event for the given use case
Vehicle stranded in lane/ vehicle waiting for assistance	Vehicle position- vehicle log - timestamp between vehicle requesting takeover and RO intervening	-	-	-
Vehicle travelling at speed which is inappropriate for the environment and/ or conditions	Vehicle speed - Distance between vehicles and other objects	Yes	High	Unknown
Safety envelope of vehicle violated	Safety envelope	Yes	High	Low
Time to collision (TTC) below minimum threshold	TTC of vehicle with all other objects	Yes	High	Low
Traffic infraction is committed	Count of infractions. Post-processing samples of data (manual), utilisation of connected infrastructure	Yes	Medium	Low
Operator does not intervene when required	TTC, safety envelope, number, speed & frequency of interventions	-	-	-
Vehicle exits ODD - This could include ADS exiting ADS ODD, and RO exiting RO ODD	GPS, HD map, speedometer, weather forecast	Yes	High	Low

5.1 Example use case: AZORA

As part of AZORA, witness tests are taking place whereby an AV drives in a controlled environment while being remotely monitored by an operator within VLOS of the vehicle. This provides a suitable initial use case to identify in-use monitoring requirements. Key information about the attributes and characteristics of AZORA witness tests are displayed in Table 3 below.

Table 3: AZORA witness test properties

Category	AZORA – attributes and characteristics
Location	Controlled off-road environment (test facility)
Level of Remote Operator assistance	Remote assistance – constant monitoring
Remote Operator observation of vehicle	Visual Line of Sight
Vehicles for Remote Operator to monitor	One
Type of vehicle	Conventional (Car)
Speed of environment	Low
AV Speed of operation	Low
Number of passengers	None

The trial properties for AZORA indicate the different in-use monitoring metrics required to ensure safety. The Level 1 hazardous events events that apply to AZORA are listed below, followed by the metrics that should be while in-use to understand the reason for those Level 1 events occurring.

Table 4: Level 1 hazardous events and related metrics for the AZORA use-case

1	**Hazardous event**	Vehicle stranded in lane/ vehicle waiting for assistance
	Metric	Vehicle position. Time waiting for RO: vehicle log – timestamp between vehicle requestion takeover and action being taken by RO
2	Hazardous event	Vehicle travelling at speed which is inappropriate for the environment and/or conditions
	Metric	Vehicle speed. Distance between vehicle and other objects
3	Hazardous event	Operator does not intervene when required TTC, safety envelope. Number, speed and frequency of interventions Vehicle exits ODD. This could include ADS exiting ADS ODD, and RO exiting RO ODD
	Metric	GPS, HD map, speedometer, weather forecast, etc.

To identify the Level 2 and Level 3 causes the same procedure was adopted, with a list of causes followed by in-use monitoring metrics to identify why a hazardous event occurred. Examples include:

- Connection strength between AV and RO
- Latency of network (value, range, standard deviation)
- Bandwidth, video resolution at remote workstation
- Connection strength between AV and RO

6 Data Sharing

In-use monitoring has immediate safety benefits for the trialling organisation undertaking the trial to which it directly relates. However, as organisations start to collect this data, there will likely be lessons learnt, for example some metrics are likely to be identified as having a strong correlation to safety, or there may be some challenges with obtaining certain data sets or validating them. However trialling organisations are likely to be collecting this data independently of one another, which limits the industry-wide safety benefits in-use monitoring has the potential to bring. In addition, due to the relative infancy of automated vehicle trialling, there is limited standardisation for validating safety. This has the knock on effect of severely limiting TOs in terms of what trials they can safely undertake, and what support they may receive from insurers, landowners, or even governing bodies. By sharing data amongst a variety of involved parties, including other TOs or vehicle operators, they can combine resources to gain more insight in risks relating to autonomous vehicle trials, and in use operation.

6.1 Stakeholders for in-use monitoring

The relevance of which bodies receive what information, and to what extent is important since specific parties will be interested in different aspects, formats, and quantities of vehicle data. Therefore, ensuring that the appropriate bodies and parties receive exactly what they need is paramount not only for the progression of trials but also to generate a relationship of data sharing between them, this relationship is key as developing a level of trust and rapport between parties will mean that they feel more inclined to share data, and can draw in more parties and bodies into the data sharing circle.

6.1.1 Testing organisations

Testing organisations will likely largely be interested in the results and data from the trial, this would involve:

- Sensor data;
- Incident/near miss reports;
- Driver feedback.

Testing organisations main focus falls on safety performance, as this is directly related to the commercial viability of automated vehicles and is something that can be easily obtained through in-use monitoring, which in turn allows for continuous improvement and development of their systems.

Alongside this they will likely be interested in the factors that influences risk, looking at causations, the probability of said risk, and how it can be appropriately mitigated, with the final aim being a trial with all risks mitigated as low as reasonably possible (ALARP). By utilising prior trial risk data from either their own, or other companies it extends their ability to mitigate risks by understanding the factors where their main focus lays.

6.1.2 Insurers

Insurers' are likely to be interested in:

- The chance of risks;
- The potential costs of the risks;
- How the risk chance changes with different parameters.

Insurers interest in cost will likely extend to costing up repairs, replacements, and injuries to persons that the trial could entail. With this data helping them to make informed decision relevant to the actual trial, and with more data available through sharing mediums, it would allow them to more accurately assess the potential of risks and also the magnitude and after-effects of the risk.

6.1.3 Regulatory bodies

Regulatory bodies would most likely look for trial results and use them as a method to inform potential regulatory or legislation changes, with excessive risks generating more stringent changes to existing regulations and legislations.

Access to trial data and then in-use monitoring data would allow them to evaluate and validate their response to regulatory changes, with regulations mostly interested in the safe operation and trialling of Connected Autonomous Vehicles (CAVs). Over time trends will appear, for example displaying a reduction, or no change in risks related to regulatory or legislation change. This allows continuous improvement of the regulatory position in as close to real time as possible.

Due to the close links within the data sharing platform all parties will likely have access to these changes in legislation as they happen, meaning that there is a constant loop of communication in terms of what can and can't be done, with this increasing TOs awareness of regulatory limitations, or what direction the sector automated vehicles is taking.

6.1.4 Public

The public will likely be uninterested in the intricacies of the trial and results, and will more be interested in larger, more generalised questions such as "are they safe?", "how do they work?", and "when can I use one?". They will also want to know how it will affect their day-to-day life in terms of dealing them as a road user (including vulnerable road users e.g., cyclists) or pedestrians, as there may be multiple misconceptions.

In-use monitoring can also be utilised as an assurance to the general public that adequate data is being captured to investigate safety related incidents, forming the level of assurance required to prove to road users that automated vehicles are being implemented in a safe manner.

6.1.5 Research Bodies

Research bodies' main interests may lie in the outcome of trials and vehicle operation, with a view to advising parties such as TOs on the development of standardisation such as the PAS series of regulations related to automated driving systems.

The prerogative for TOs to share with research bodies especially is the potential for them helping to accelerate research, with a reduced workload meaning shorter lead times for reports or data processing. These shorter lead times mean that when utilising processes such as the continuous improvement cycle there is reduced gaps between recognising incidents or risks and implementing solutions.

6.1.6 Landowners

Landowners represent the facilities where tests will be undertaken. The progression of automated vehicle safety through shared trial data will allow automated vehicle TOs to assure landowners that seemingly higher risk manoeuvres can be undertaken with very little to no risk, this makes undertaking trials more accessible to all TOs as there is a larger assurance that there is less risk of undertaking trials, or for automated vehicles operating in a borough or council area.

6.2 How do people currently share trial data

Across automotive, aviation, and rail industries there are currently data-sharing platforms and systems used, they provide a variety of benefits to both small- and large-scale manufacturers and operators, with the aim being to reduce risks, increase service quality, and share this data as openly as possibly with involved parties.

6.2.1 What do existing data sharing processes look like?

Aviation

Aviation use a shared database with deidentified data, data can be information on their operational risks, which can be as simple as typing up observations following an incident. Which can often be made simpler, and quicker by the introduction of a hazard report system.

An example of this is the ASIAS (Aviation Safety Information Analysis and Sharing). Which utilises internal FAA datasets, safety data, publicly available data, and manufacturer data in order to asses safety enhancements, monitor known risks, and discover vulnerabilities with aviation systems and processes in order to enhance aviation safety. It serves as a central conduit for exchanging data among its participants, which comprises of at least 50 domestic and international airlines (ASIAS, 2020).

Each participant within the ASIAS signs a memorandum of understanding that allows the exchange of deidentified data, limits disclose of proprietary information, and allows them access to other unique ASIAS products (Federal Aviation Administration, 2019). The point behind deidentifying data is the removal of all identifying factors which can allow identification of the owner or creator of the data, meaning that .

Rail – Data action plan

Current rail data sharing processes highlight issues with lack of conformity, with different systems they use having different software, and accuracies, also highlighting the lack of conformity within data publishing standards (Department for Transport, 2018).

The data rail action plan aims to generate a more transparent data sharing platform by following a series of themes:

- Data transparency;
- Data use and access;
- Data standards and quality;
- Data value and principles;
- Rail culture and information/data skills

Spain – DGT 3.0

The DGT V-16 is a system being considered for utilisation in Spain which allows vehicles to communicate and log locations and speeds of vehicles in real time, in line with the European Commission's 2011-2020 road safety policy guideline and also to contribute to the target of a 50% reduction in the number of deaths and serious injuries related to road traffic accidents (Direccion General de trafico, 2022).

6.2.2 What format is shared data presented in?

The requirement for data to be specifically formatted is a credible consideration for issues within data sharing, with different parties having requirements for different levels of processed data, with some needing entire trials of raw data, and others potentially only being interested in finished reports. Alongside the format, the quality of the data will have to be considered, with a minimum level of accuracy necessary to appropriately portray the incident or happening, which will likely be standardised.

There is the possibility that the data can be laid out and transferred in a report, this would mean that insurers, regulatory bodies, and even landowners can input their own information, which can still aid TOs and vehicle operators in keeping them up to date on costings, regulations, and considerations for their trials and operations. The other benefit is that all information would be clearly conveyed and an abstract or conclusion would allow the information of the report to be conveyed for ease and speed.

The data can be presented and stored in its rawest form, so if the data involves velocity, and lateral and longitudinal acceleration the data would be presented in this format, although in this way the data is its 'purest' form there is still the issue that for each entry a full description of the trial would still be necessary to explain where and when the data came from. For both rail and aviation applications safety system triggers and general functions are logged, with trains not utilising positional data, but aircraft doing so.

6.2.3 How is data processed in terms of time frame (short, long, mid-term) and how does this data impacts trialling

Due to the infancy of CAV trialling there is very little validation and corroborating data that is openly available, thus spotting causations of risks is difficult at this stage, the data processing will likely be a long term project largely due to the fact that it will take a large amount of trials to be undertaken before any real correlations begins to show.

6.3 How could the sharing process managed?

6.3.1 Who should be responsible for owning and managing the data

Other bodies such as the ASIAS use a central body to distribute and manage shared data, in their case it is MITRE corp., a central body which creates the high-level architecture for databases necessary to store, organise, and collate data from various sources.

A potential issue of a central body managing all the data is that initially TOs will be very unlikely to share data due to the fact that the information being shared could be seen and utilised by competition. De-identification or anonymisation of data is already utilised to mitigate this problem, with it involving the removal of all identifying factors, the knock on effect of this being that by removing any identifying points from the data, it could potentially scrub relevant trial information.

There will be some existing data sharing between bodies such as TOs and insurers, which presents the issue of them potentially circumnavigating the central body, this would have to be highlighted in agreements or regulations whether this was allowed, as it may mean they can work outside of the limitations highlighted to them. Also, it directly goes against the ethos of fostering a culture of sharing which is beneficial to everyone, this can be developed to consider whether this sharing of data was mandated, meaning that all involved parties have to share data, or all parties involved full stop with CAV have to.

at some point as a form of assurance data will have to be related to the general public, what data is shared and who that data originally belonged to may present issues as there is an agreement for open trial and in-use data sharing within the specified groups, but not exterior to that, with some form of regulation or agreement necessary to share data exterior to the group.

6.3.2 Cyber security

Ensuring the data is stored, managed, and shared in a safe manner is of the utmost importance, with breaches and leaks being potential areas for concern. The process requires that all data is deidentified in order to be shared, so that direct competitors can’t identify each other’s information. The ethical issues of sharing data can be largely circumnavigated by the deidentification of the data, but a limit has to be proposed so that relevant incident or operation data isn’t scrubbed. Factors such as location, occupant age, etc. could be relevant for generating risk trends.

The final point of contact for most of the shared data is likely to be to the general public, with vehicle operators and other bodies releasing media to increase uptake and confidence in the technology. The issue with this lies in the fact there needs to be some checkpoint to ensure that only relevant data is being shared, and that in the event of it being shared the parties involved have consented for it to be shared, as it is no longer being shared within the given sphere.

6.4 Example structure

The initial parties would hand their identified and appropriately formatted data to the main management body, the main body then puts it through deidentification and security steps, with it then being placed into an evaluation stage, in the event of the data not being formatted correctly, high enough quality, or any other issues it will be sent back to the source. From this the data is transferred to the relevant party for use, with their being a feedback loop between each party and the management body.

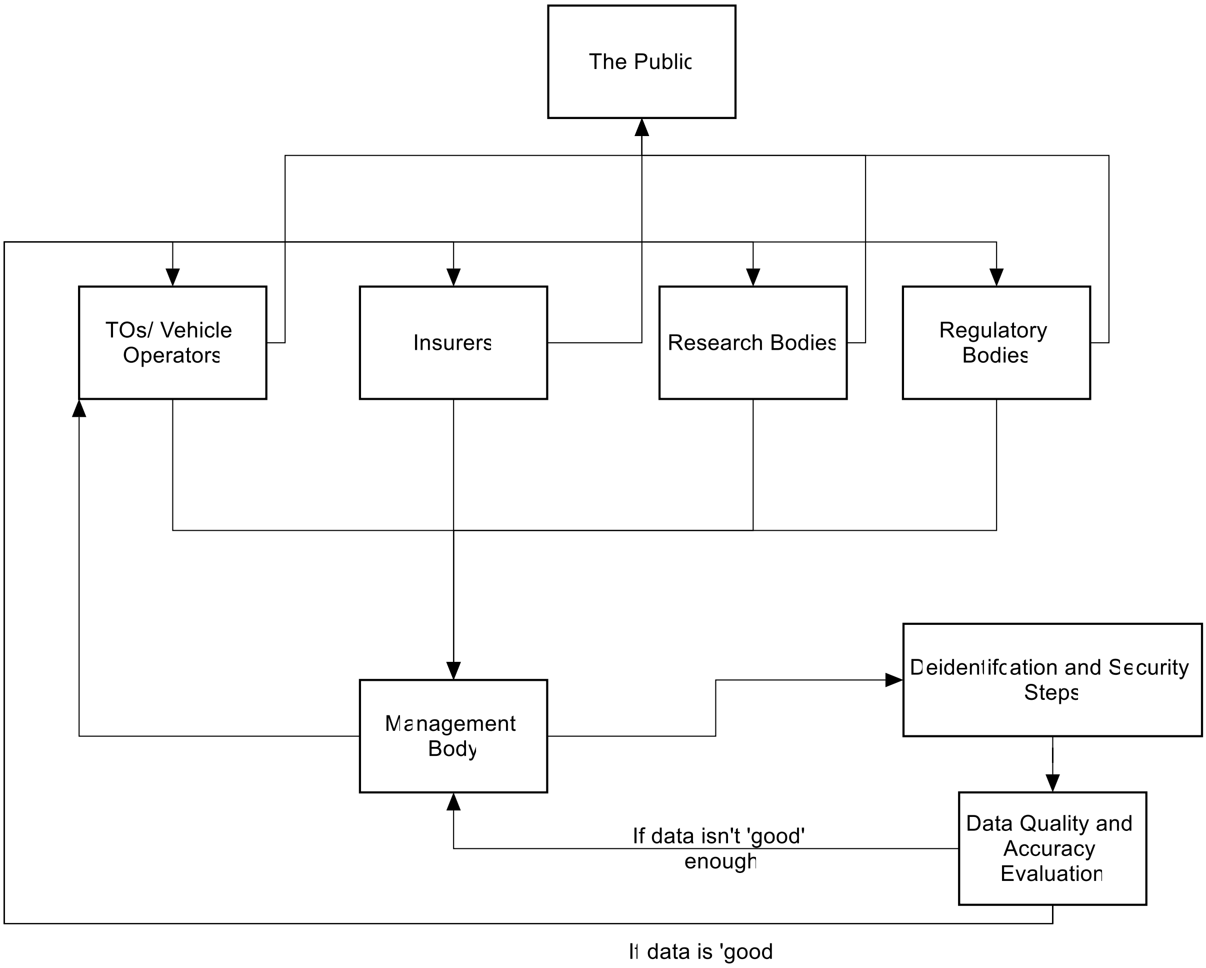


Figure 4: Example of data sharing flow structure

The limitation of data 'not being good enough' is a factor which will have to be defined by the management body, data quality and standards is an overcharging theme presented by the rail action plan, this would be of interest as regardless of what level of detail a party may need for the shared data, there will still need to be an underlying level of quality and accuracy to ensure that it is useable and representative but also that it is a manageable size for storage.

7 Conclusion

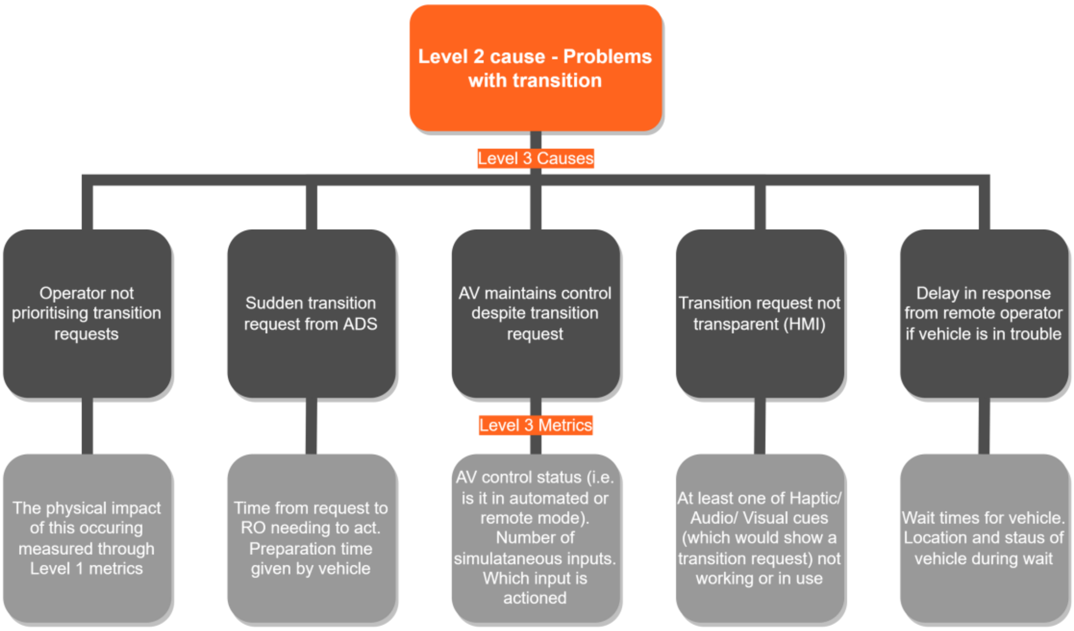
To assess the in-use monitoring requirements of any given remotely operated autonomous vehicle trial, the use case of the trial should first be considered. By assessing the potential risks that could occur for each use-case (based on the characteristics), and the associated metrics that can be measured, the in-use monitoring requirements can then be examined. When a remote operated vehicle is used, this process can be used identify what in-use monitoring is needed to identify hazardous events. However, it is important to note that not all metrics are going to be applicable or relevant for all use cases, and appropriate metrics should be identified before commencing a trial

Once in-use monitoring is in place, consideration should be given to data collected by individual trialling organisations, but that may be relevant to the industry as a whole. It is important that structures are put in place for the sharing of such information, to improve the overall safety of AV trials by giving a better understanding of what could go wrong, and improving the safety of remotely operated AVs as a whole over time.

Appendix A Hazard Analysis

[Excel file shared separately]

Appendix B Level 2 causes and metrics



Level 2 cause - Problems with transition

Level 3 Causes

Operator not prioritising transition requests

Sudden transition request from ADS

AV maintains control despite transition request

Transition request not transparent (HMI)

Delay in response from remote operator if vehicle is in trouble

Level 3 Metrics

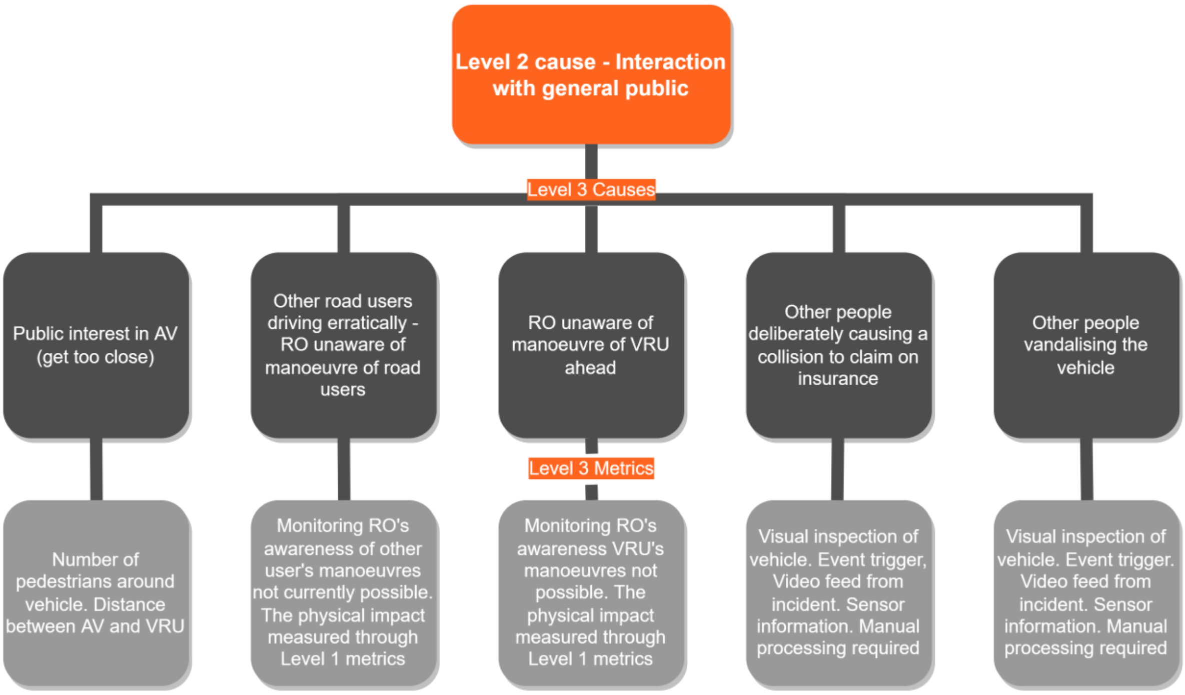
The physical impact of this occuring measured through Level 1 metrics

Time from request to RO needing to act. Preparation time given by vehicle

AV control status (i.e. is it in automated or remote mode). Number of simulataneous inputs. Which input is actioned

At least one of Haptic/ Audio/ Visual cues (which would show a transition request) not working or in use

Wait times for vehicle. Location and staus of vehicle during wait



Level 2 cause - Interaction with general public

Level 3 Causes

Public interest in AV (get too close)

Other road users driving erratically - RO unaware of manoeuvre of road users

RO unaware of manoeuvre of VRU ahead

Other people deliberately causing a collision to claim on insurance

Other people vandalising the vehicle

Level 3 Metrics

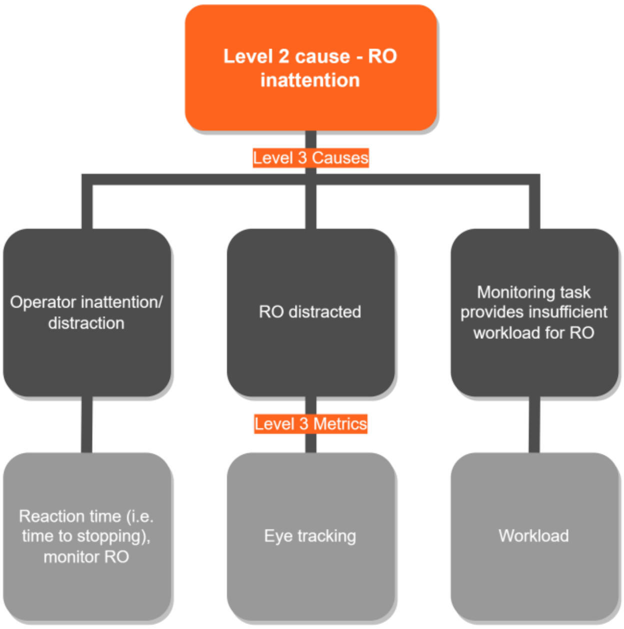
Number of pedestrians around vehicle. Distance between AV and VRU

Monitoring RO's awareness of other user's manoeuvres not currently possible. The physical impact measured through Level 1 metrics

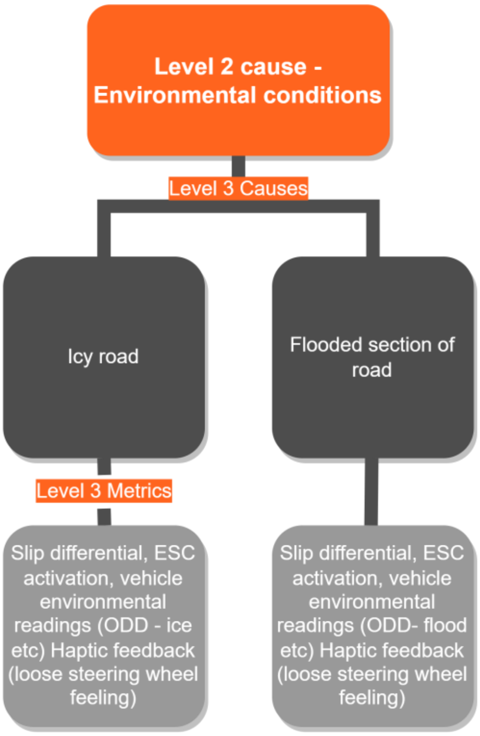
Monitoring RO's awareness VRU's manoeuvres not possible. The physical impact measured through Level 1 metrics

Visual inspection of vehicle. Event trigger, Video feed from incident. Sensor information. Manual processing required

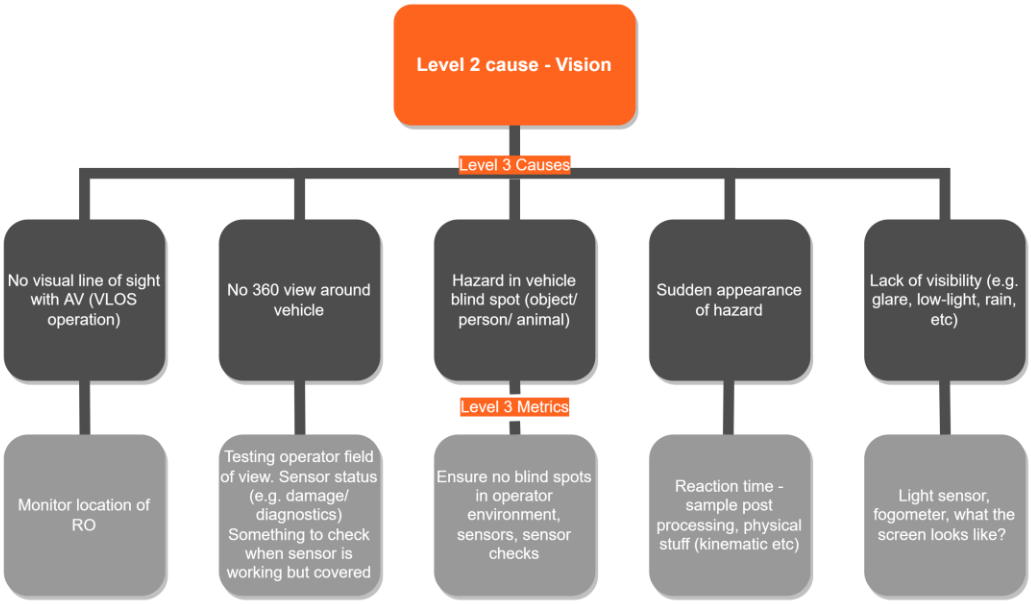
Visual inspection of vehicle. Event trigger. Video feed from incident. Sensor information. Manual processing required

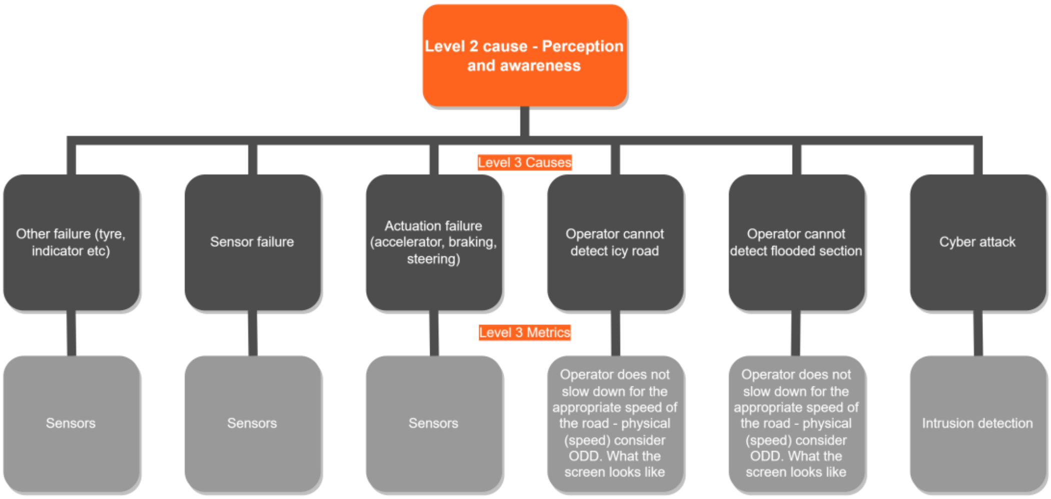


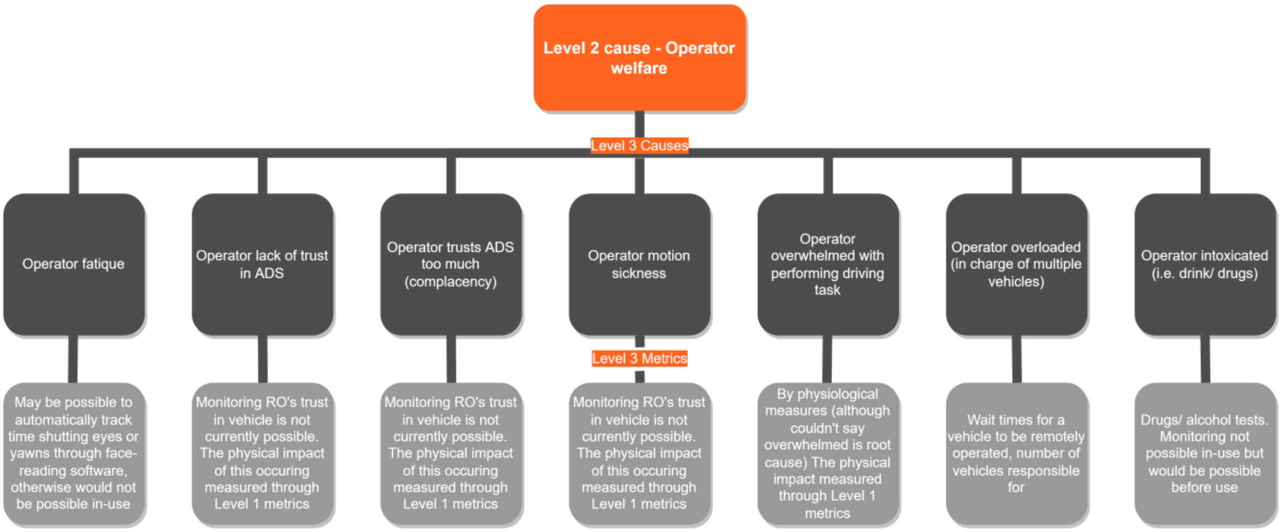
Level 2 cause - RO inattention
Level 3 Causes
Operator inattention/ distraction
RO distracted
Monitoring task provides insufficient workload for RO
Level 3 Metrics
Reaction time (i.e. time to stopping), monitor RO
Eye tracking
Workload



Level 2 cause - Environmental conditions
Level 3 Causes
Icy road
Flooded section of road
Level 3 Metrics
Slip differential, ESC activation, vehicle environmental readings (ODD - ice etc) Haptic feedback (loose steering wheel feeling)
Slip differential, ESC activation, vehicle environmental readings (ODD- flood etc) Haptic feedback (loose steering wheel feeling)


Level 2 cause - Vision
Level 3 Causes
No visual line of sight with AV (VLOS operation)
No 360 view around vehicle
Hazard in vehicle blind spot (object/ person/ animal)
Sudden appearance of hazard
Lack of visibility (e.g. glare, low-light, rain, etc)
Level 3 Metrics
Monitor location of RO
Testing operator field of view. Sensor status (e.g. damage/ diagnostics) Something to check when sensor is working but covered
Ensure no blind spots in operator environment, sensors, sensor checks
Reaction time - sample post processing, physical stuff (kinematic etc)
Light sensor, fogometer, what the screen looks like?


Level 2 cause - Perception and awareness
Level 3 Causes
Other failure (tyre, indicator etc)
Sensor failure
Actuation failure (accelerator, braking, steering)
Operator cannot detect icy road
Operator cannot detect flooded section
Cyber attack
Level 3 Metrics
Sensors
Sensors
Sensors
Operator does not slow down for the appropriate speed of the road - physical (speed) consider ODD. What the screen looks like
Operator does not slow down for the appropriate speed of the road - physical (speed) consider ODD. What the screen looks like
Intrusion detection



Level 2 cause - Operator welfare

Level 3 Causes

Operator fatigue

Operator lack of trust in ADS

Operator trusts ADS too much (complacency)

Operator motion sickness

Operator overwhelmed with performing driving task

Operator overloaded (in charge of multiple vehicles)

Operator intoxicated (i.e. drink/ drugs)

Level 3 Metrics

May be possible to automatically track time shutting eyes or yawns through face-reading software, otherwise would not be possible in-use

Monitoring RO's trust in vehicle is not currently possible. The physical impact of this occuring measured through Level 1 metrics

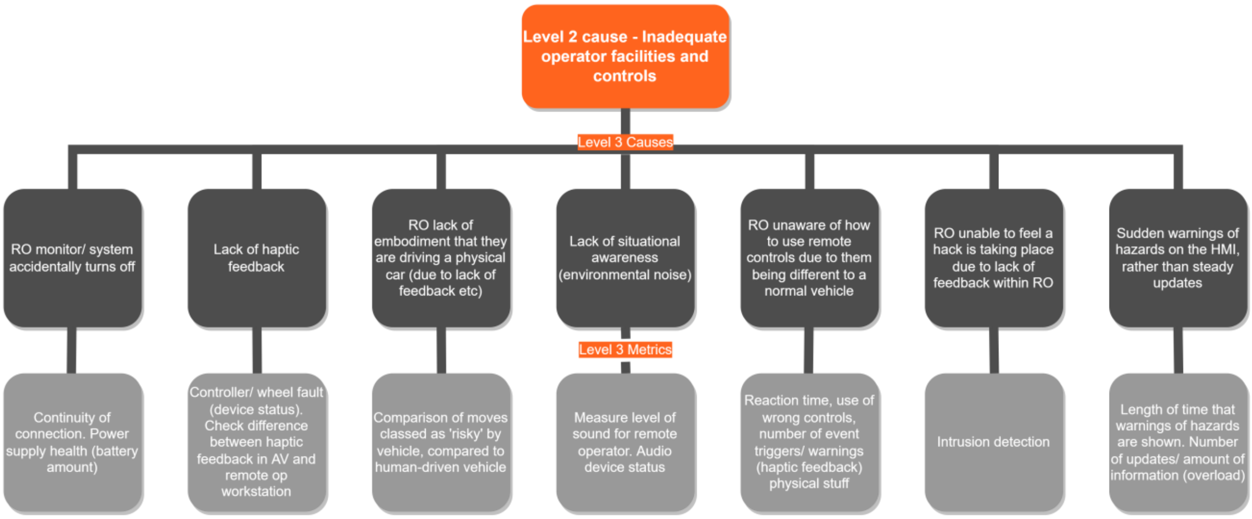
Monitoring RO's trust in vehicle is not currently possible. The physical impact of this occuring measured through Level 1 metrics

Monitoring RO's trust in vehicle is not currently possible. The physical impact of this occuring measured through Level 1 metrics

By physiological measures (although couldn't say overwhelmed is root cause) The physical impact measured through Level 1 metrics

Wait times for a vehicle to be remotely operated, number of vehicles responsible for

Drugs/ alcohol tests. Monitoring not possible in-use but would be possible before use



Level 2 cause - Inadequate operator facilities and controls

Level 3 Causes

RO monitor/ system accidentally turns off

Lack of haptic feedback

RO lack of embodiment that they are driving a physical car (due to lack of feedback etc)

Lack of situational awareness (environmental noise)

RO unaware of how to use remote controls due to them being different to a normal vehicle

RO unable to feel a hack is taking place due to lack of feedback within RO

Sudden warnings of hazards on the HMI, rather than steady updates

Level 3 Metrics

Continuity of connection. Power supply health (battery amount)

Controller/ wheel fault (device status). Check difference between haptic feedback in AV and remote op workstation

Comparison of moves classed as 'risky' by vehicle, compared to human-driven vehicle

Measure level of sound for remote operator. Audio device status

Reaction time, use of wrong controls, number of event triggers/ warnings (haptic feedback) physical stuff

Intrusion detection

Length of time that warnings of hazards are shown. Number of updates/ amount of information (overload)

This report examines how the safety of automated vehicles (AVs) can be monitored while they are being driven by a Remote Operator, and how data collected during this process can be shared and used to improve safety across remote operation trials. It identifies different levels of hazardous events that may happen during remote operation of a vehicle, identifying failure modes and their causes to create in-use monitoring metrics to ensure a high level of safety when using remote operated vehicles. The report was developed as part of the Innovate UK project AZORA (Autonomous Zero Occupancy with Remote Authority).

This report examines how the safety of automated vehicles (AVs) can be monitored while they are being driven by a Remote Operator, and how data collected during this process can be shared and used to improve safety across remote operation trials. It identifies different levels of hazardous events that may happen during remote operation of a vehicle, identifying failure modes and their causes to create in-use monitoring metrics to ensure a high level of safety when using remote operated vehicles. The report was developed as part of the Innovate UK project AZORA (Autonomous Zero Occupancy with Remote Authority).

TRL
Crowthorne House, Nine Mile Ride,
Wokingham, Berkshire, RG40 3GA,
United Kingdom
T: +44 (0) 1344 773131
F: +44 (0) 1344 770356
E: enquiries@trl.co.uk
W: www.trl.co.uk

PPR1024