ZENZIC

SELF-DRIVING REVOLUTION

Safety Case Framework Report 2.0

A report by Zenzic
Authored by TRL

March 2020

Disclaimer

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

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 cannot accept any liability for any error or omission, or reliance on part or all of the content in another context.

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

For further information on this report please contact the Zenzic team

Email: info@zenzic.io
Web: zenzic.io

Foreword

This Safety Case Framework Report 2.0 is the culmination of a programme of work which has distilled best practice in the creation and sharing of connected and automated mobility (CAM) safety cases for the testing and development of connected and self-driving technologies. It brings together the best practice and learnings from many organisations to develop a consistent approach to both the creation and understanding of safety cases.

A safety case is a body of evidence of the steps taken to ensure the safe operation of self-driving vehicles. It is crucial that it can be shared and understood. The processes developed within this report set expectations of how safety cases can be ported between test facilities to allow each safety case to be evolved, as well as provide those who may need to review or receive safety cases some clarity on what a good safety case looks like.

This work, and the previous Safety Case Framework report, has been instrumental in informing the recently released *PAS 1881 Assuring safety of automated vehicle trials and testing,* by providing a considered and expert input into the consensus approach to bring these findings to a national and international audience.

This framework is implemented within CAM Testbed UK and has been used in building safety cases for existing on-road trials. It is the hope that this publication opens up the framework to all those seeking to trial CAM in the UK and allows Cities and Regions to understand, transparently, how safety cases are built and provides a base from which safety cases can be understood.

With this safety framework and process, CAM Testbed UK can provide a seamless transition between controlled, semi-controlled and public testing to allow testing organisations to build robust safety cases and accelerate their journey towards deployment.

Richard Porter
Technology and Innovation Director, Zenzic

About CAM Testbed UK

CAM Testbed UK, coordinated by Zenzic, is a collection of world-class testing and development facilities for connected and self-driving technologies. Supported by the UK government's Centre for Connected and Autonomous Vehicles (CCAV), it is the hub for excellence in testing and assurance for CAM and is built on a long history of testing and assurance of vehicles in both private and public scenarios.

Contents

Disclaimer ii

Foreword iii

About CAM Testbed UK iv

1 | **Introduction** 6

2 | **The Safety Case Framework** 7
2.1 Overview 7

3 | **Safety Case Development and Supporting Processes** 8
3.1 Ownership 8
3.2 Safety Case Development and Requirements 8
3.3 Acceptance 16
3.4 Transition Process 17
3.5 Independent Review Process 19
3.6 Publication 19
3.7 Safety Case Framework Updates 19

4 | **Next steps** 21

5 | **References** 22

6 | **Appendix A Safety Case Framework Guidance** 23

1 | Introduction

Zenzic is committed to promoting the United Kingdom as a global centre for CAM innovation and seek to ensure that a consistent and robust approach to safety is adopted in the UK's world-leading connected and self-driving vehicle testing facilities.

CAM Testbed UK is an ecosystem of connected and self-driving vehicle testbeds comprising world-class vehicle testing facilities that aids connected and self-driving vehicle testing across the entire development lifecycle in a wide range of environments. The focus of Zenzic and CAM Testbed UK is to deliver a seamless transition process between testing facilities to provide full support to their customers including connected and self-driving vehicle developers and trialling organisations.

The Centre for Connected and Autonomous Vehicles' (CCAV) Code of Practice: *Automated Vehicle Trialling* (DfT, 2019) states that a safety case is expected to be developed for testing in the public domain that demonstrates that a trial activity can be conducted safely. The Code of Practice imposes a number of high-level requirements for safety case development but also expects duty holders to develop and build on those requirements and produce a suitable safety case proportionate to the activity and the level of risk posed.

British Standards Institute (BSI) PAS 1881: *Assuring safety for automated vehicle trials and testing* (technically authored by TRL) builds on the Code of Practice and specifies requirements for safety case development that reflect good practice for automated vehicle trialling. BSI PAS 1881 reflects the Safety Case Framework initially developed by TRL in 2015 and matured in partnership with Zenzic and CAM Testbed UK published in the *Zenzic Safety Case Framework report* (2019).

This report updates the Safety Case Framework in line with good practice and BSI PAS 1881 and includes high level guidance and supporting processes to ensure a consistent approach is adopted across the ecosystem that is proportionate to the level of risk posed from the defined testing.

The guidance and processes, developed by TRL in collaboration with Zenzic and CAM Testbed UK, provide the baseline for the future development of safety case requirements and supporting processes.

2 | The Safety Case Framework

2.1 Overview

The overarching headings in the Safety Case Framework are listed below. These headings are in line with BSI PAS 1881. It should be noted that not all sections will be relevant for track testing or manually driven vehicles within the public domain. This is discussed further in Section 3 |.

- Purpose and scope of the safety case
- Introduction to the safety case
- Vehicle and automated driving system
- Operational Design Domain (ODD) and test scenarios
- Operational risk assessment
- Operational guidance
- Route selection and assessment
- Safe operation and control
- Security
- Assurance of system safety
- Safety testing and acceptance process
- Modelling and simulator studies
- Change control
- Compliance
- Stakeholder consultation and engagement
- Monitoring, reporting and continuous improvement
- Supporting documents referred to in this safety case

The Safety Case Framework Guidance is provided in Appendix A. The aim of the guidance is to provide CAM Testbed UK with initial high-level requirements for each of the Safety Case Framework headings to ensure a consistent and common approach is adopted that reflects good practice and is aligned with CAM Testbed UK requirements, the draft BSI PAS 1881 and the Code of Practice (2019). The guidance has been written by TRL with input from CAM Testbed UK but will need further development in line with the evolving testbed requirements and the safety case levels defined in Section 7.

3 | Safety Case Development and Supporting Processes

CAM Testbed UK is committed to ensuring that automated vehicle trials and testing are conducted safely but also want to ensure safety requirements do not become a barrier to testing in dedicated test facilities. It is important that technology developers and trialling organisations are able to move seamlessly between testbeds and that a common approach to safety is adopted. The processes detailed in this section have been developed by TRL but with significant input from the CAM Testbed UK ecosystem including Millbrook, HORIBA MIRA, Midlands Future Mobility, Smart Mobility Living Lab, CAVWAY, Highways England and CCAV.

The aims of the safety case development and supporting processes are to ensure that:

- Customers can move between testbeds seamlessly and that safety requirements do not present a barrier to testing.
- There is one common approach to safety case development that encourages testbeds to work collaboratively to assist the customer and assure safety.
- The safety case requirements are proportionate to testing being conducted and the level of risk posed.
- Existing, effective processes are built on rather than redesigned.
- Testbeds have a common understanding of safety case requirements for different testing levels.
- Safety cases are evaluated in a consistent manner.
- Requirements are suitable for all testing environments.

3.1 Ownership

The trialling organisation has the most control of the trial and is also likely to have the best understanding of the technology under test. The trialling organisation should develop the safety case and hold overall responsibility for risks presented by the trial.

3.2 Safety Case Development and Requirements

Factors influencing the level of risk posed

It may not be appropriate to categorise testbeds into controlled, semi-controlled and uncontrolled environments as the level of control within a defined environment may vary. Safety case requirements cannot solely be determined according to the type of testing environment being used. This is because the level of risk posed depends on variables such as vehicle capabilities and level of control over the system, as well as the level of control over the environment.

It was found that the level of risk posed by testing depends on three broad, but interdependent factors;

- Safety operator

- Vehicle
- Environment

Safety case requirement levels

There are three levels of safety case that are linked to the potential level of risk posed during testing. Each level of safety case should have its own requirements that are proportionate to the level of risk posed, reflect the type of testing being conducted and are appropriate for the testing environment.

Table 3.1 below identifies the proposed levels of safety case, the applicable testing environments, parameters and considerations for the development of future safety case requirements.

Table 3.1 Description of the three safety case level categories

	Definition	Applications	Considerations for development of detailed requirements
Safety Case Level 1	Requirements for proving ground testing and testing using manually driven vehicles	Proving grounds potential use cases: • Connected vehicle testing (V2X) • Connected infrastructure testing • Pre-trial preparation using manually driven vehicles	Level 1 safety case requirements will be developed to align with existing proving ground requirements and requirements for identified use cases.
Safety Case Level 2	Minimum requirements for testing in a public domain (i.e. not a proving ground)	Applicable to all testing in the public domain including private land and off-road public spaces	Level 2 requirements will be developed in line with current good practice, BSI PAS 1881 and the Code of Practice (2019) requirements. Minimum safety case requirements on testing in a public domain. Level 2 is likely to be the standard safety case requirement for more mature technologies or less complex on-road testing.
Safety Case Level 3	Additional safety case requirements to provide further safety assurance for testing in the public domain	Applicable for testing in a public domain where there is potentially a higher level of risk or less mature technology Level 3 requirements will apply to all passenger trials	Level 3 requirements will include all Level 2 requirements but with additional supporting evidence for higher risk activities or additional controls for activities where insufficient evidence exists.

Evaluating the level of risk posed

The level of safety case required depends on the potential level of risk posed by the vehicle testing. It would not be practicable to assess the actual level of risk posed by vehicle testing prior to developing the safety case, so it is proposed that an initial, high-level assessment of risk is conducted considering the factors identified in *Section 3.2.* The level of risk posed depends on the maturity and reliability of the **vehicle** and automated driving system (ADS), the ability for a **safety operator** to control the vehicle and revert to a minimum risk state should a failure occur, and the level of control or predictability of the testing **environment**. The potential risk posed depends on the assessed level of confidence in the evidence that exists to support the system claims.

It is important that the process for determining the level of safety case required is simple and transparent, whilst allowing for expert judgement to be applied. To ensure this, levels of confidence for the three identified factors (vehicle, safety operator, environment) have been categorised into high, medium and low as shown in *Table 3.2.* The following sections provide more detailed considerations for each of the three factors and combine them in a matrix to allow assessors to determine the level of safety case required.

Table 3.2 Generic Confidence Descriptors

Confidence	Definition
High	The evidence to support system claims is proven and robust. Through the implementation of systematic and standardised processes, risks are predictable, and identified controls are reliable. At this level, current good practice is adopted across all aspects of trial design and implementation.
Medium	Some evidence exists to support system claims but further evidence is required to increase levels of confidence. Risks and the reliability of controls may be unpredictable.
Low	The evidence to support system claims is limited. Reliability of control is unknown, and the risks posed are unpredictable.

Confidence levels for identified risk factors

It is suggested that the safety case level required for testing is conducted as part of the entry process for testbeds. The safety case confidence levels have been designed to promote discussion between the testbed and trialling organisation around the identified risk factors so a safety case requirement level can be mutually agreed that is proportionate to the level of risk posed.

Safety operator

This factor considers the capability of the safety driver or remote operator to take full control of the vehicle and for operations to revert to the minimum risk state. Confidence in the safety operator control should consider a combination of the following factors:

- System design
- System latency
- Safety operator competency
- Safety operator alertness

Table 3.3 Safety Operator Confidence Levels and Considerations Assessing Confidence

Confidence	Definition
High	The system has been designed to ensure that full control of the vehicle can be resumed by the safety operator (system or operator initiated) within a time period that minimises the risk of an incident and in line with expected operator alertness. The safety operator is fully trained and competent to fulfil identified roles and responsibilities. System reliability and is supported with robust evidence.
Medium	Less confidence due lack of evidence around system design, reliability and latency and/ or safety operator competency or alignment with system design.
Low	System reliability is unsupported by sufficient evidence.
Additional considerations	
• Whether operator selection is aligned to the responsibilities of the operator and consistently applied to all safety operators for the trial. • How clearly safety operator roles and responsibilities are defined and communicated through procedures and training. • How effectively operator alertness (i.e. fatigue, distraction, workload) and competency is monitored throughout the trial. • How effectively the operator can monitor the system (e.g. visibility, latency, distraction). • The extent of the operator's experience with the system including the amount and appropriateness of the training supplied. • The degree of assurance provided through certification of competency of the safety operator by the trialling organisation. • The ergonomics of the system design to either alert the safety operator of the requirement to resume vehicle control or to enable the safety operator to effectively intervene.	

Vehicle (Automated Driving System)

This factor considers the level of confidence in the effectiveness, reliability and predictability of the ADS to safely and predictably operate within the defined ODD. The confidence level is dependent on the robustness and sufficiency of evidence to support identified vehicle capabilities and the alignment of capabilities with the test scenarios.

Table 3.4 Vehicle Confidence Levels and Considerations Assessing Confidence

Confidence	Definition
High	The behaviour of the ADS is predictable, the vehicle functions have been verified and the boundaries of the ODD are supported with robust evidence. Test scenarios are within the boundaries of the defined ODD.
Medium	Some verification of the ADS has been conducted rigorously but insufficient evidence for some ADS requirements within the defined ODD.
Low	The behaviour of the ADS is not supported by sufficient evidence and reliability to operate within the defined ODD without intervention is uncertain.
Additional considerations	
• The extent and sufficiency of previous safety testing to verify and validate the ADS and define the boundaries of the ODD. The application of design safety standards both for vehicle design and systems safety. • The identification and management of system failure modes and appropriate controls.	

Control of the environment

This factor considers the level of control over the testing environment, in particular; potential interactions between the vehicle, infrastructure and other road users and the impact on the risk of collision. An additional 'very high' confidence level has been included for proving grounds where interactions with other road users can be reliably controlled or eliminated.

Table 3.5 Environmental Control Confidence Levels and Considerations Assessing Confidence

Confidence	Definition
Very High	This level of confidence is only applicable to trials conducted on proving grounds with sufficiently robust risk management processes to control interactions with other road users.

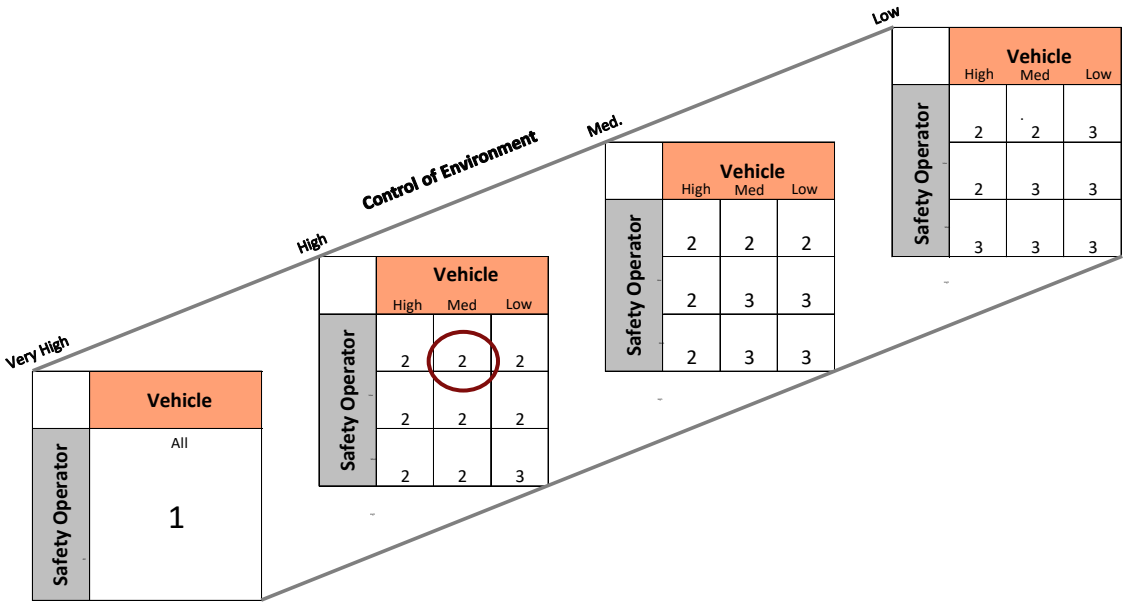
High	Risks associated with the testing environment have been identified and effective controls are in place (e.g. restrictions on road user access) to ensure foreseeable interactions (with all road user types) beyond the boundaries of the defined ODD have been minimised.
Medium	Risks associated with the testing environment have been identified and controls are in place that minimise the probability of interactions (with all road user types) beyond the scope of the ODD.
Low	Limited control over interactions beyond the scope of the ODD within the testing environment.
Additional considerations	
• The probability of a hazardous event being realised as a result of identified road users or route feature and potential consequence severity. • The level of confidence that all environment related risks have been identified and effectively managed. • The likely effectiveness of the controls implemented. • The reliability or authority of the parties responsible for implementing the identified controls.	

Safety case level matrix

Combining the confidence levels for the three factors will provide assessors with the level of safety case required. The safety case level matrix *Figure 3.1* shows the overall safety case level required for all combinations of confidence level. The matrix is a qualitative tool that can guide testbeds and trialling organisations but should allow for the flexibility to exercise professional judgement.

The safety case level matrix also shows the overall safety case level required for all combinations of confidence level. For example, if confidence levels are control of environment – high, vehicle – medium and safety operator – low, the level of safety case would be 2 (circled in the matrix). The matrix is a qualitative tool that can guide testbeds and trialling organisations but should allow for the flexibility to exercise professional judgement.

Figure 3.1: Safety Case Level Matrix



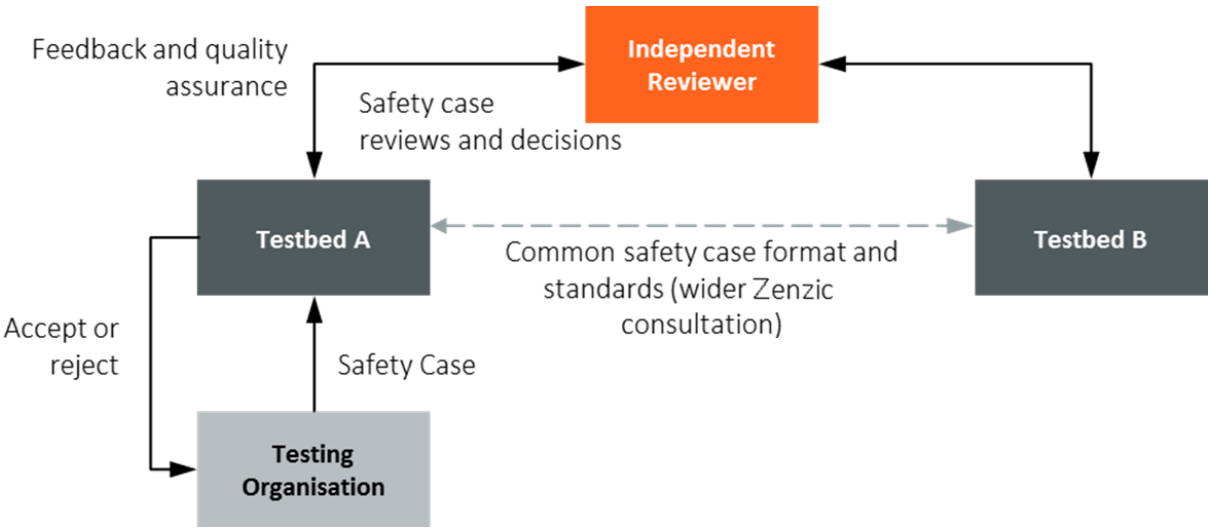
3.3 Acceptance

While the trialling organisation retains overall responsibility for the safety case, a verification process is required to make sure that the processes defined in this report are followed and the application is consistent across all testbeds. The following desirable features are a key part of this process:

- Testbeds should have the final say about whether a trial goes ahead once they have reviewed the safety case. They may have legal responsibilities regarding trials that take place at their facility and should not be expected to accept a safety case on the basis of another organisation's review.
- The safety case requirements should be consistent between testbeds of the same type.

Figure 3.2 shows a possible structure which has the potential to deliver the features above.

Figure 3.2 Potential Process Structure for Safety Case Acceptance



There is an emerging consensus amongst testbeds that they should accept, rather than approve, safety cases. Approval would require a more rigorous process: the testbeds may not be competent to assess everything required and unnecessary complexity could encourage trialling organisations to trial outside the testbed system.

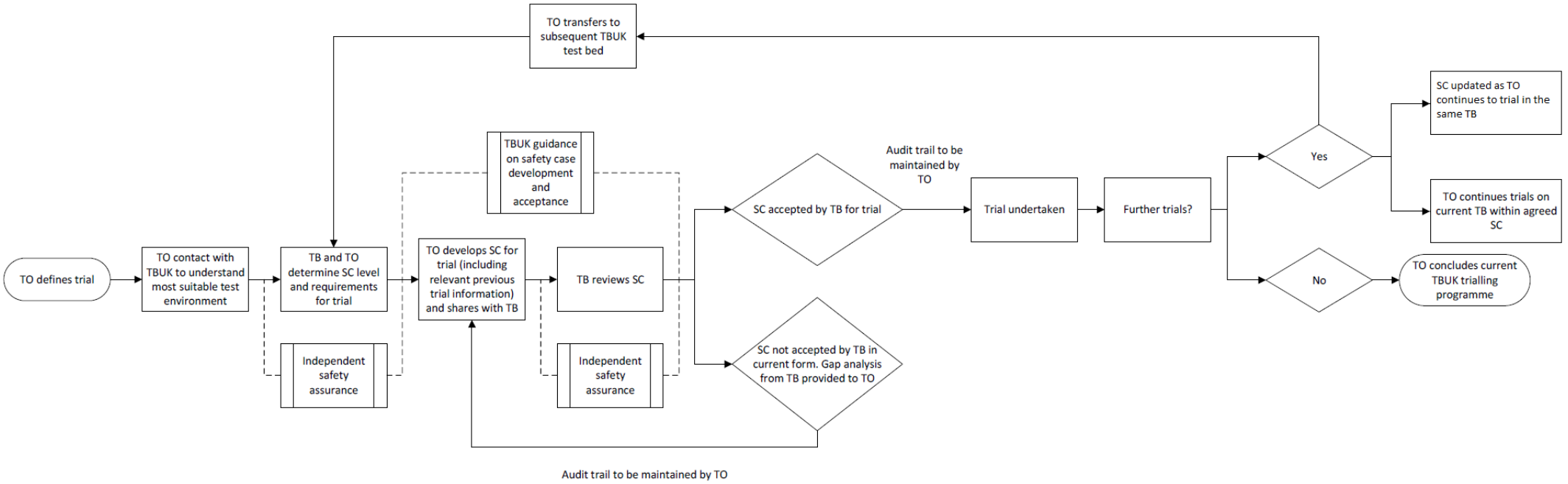
Consistent acceptance criteria for the safety case will need to be defined.

3.4 Transition Process

BSI PAS 1881 and the Safety Case Framework promote a consistent approach to risk management across testbeds where one safety case is developed, and evidence added at each stage of testing. Testbeds provide a wide range of testing environments for trialling organisations and it is important that customers can seamlessly transfer from one environment to another. To enable this ambition, it is important that:

1. Testbed guidance is written, in consultation with end users (trialling organisations), detailing a consistent approach and specific requirements for the development, evaluation and acceptance of safety cases.
2. Trialling organisations consult with testbeds to understand the most appropriate test facility or environment to meet test objectives safely.
3. Trialling organisations determine the level of safety case requirement in line with the Safety Case Level Matrix and agree with the testbed.
4. Trialling organisations consult with testbeds to ensure entry requirements are understood and that the safety case is developed in line with guidance and good practice (BSI PAS 1881 and CAM Testbed UK supporting guidance).
5. Trialling organisations share the safety case and supporting documentation with testbeds.
6. Testbeds review safety cases using a standardised approach and document acceptance decisions and recommendations.
7. Testbeds have access to technical support, if required, when evaluating safety cases.
8. Trialling organisations maintain an audit trail detailing acceptance decisions, recommendations and any changes implemented that can be provided to testbeds with the safety case.
9. Acceptance decisions are independently and periodically reviewed to ensure consistency between testbeds.
10. Testbeds feedback lessons learned to Zenzic regarding the implementation of the guidance to ensure continuous improvement and guidance that reflects the requirements of the end user.

Figure 3.3 Transfer Process



Definitions:

TO: Trialling organisation
TB: Testbed
TBUK: CAM Testbed UK
SC: Safety Case

3.5 Independent Review Process

Taking a consistent approach to risk management would considerably simplify the transition from one testbed to another. An independent review process could help to achieve this consistency. The role of the independent reviewer could include:

- Review of safety cases against predefined evaluation criteria (either all safety cases or a sample to ensure consistency between testbeds)
- Assistance in the safety case review process and gap analysis
- Review of testbeds entry requirements
- Involvement in assigning a safety case level

An audit process could also be applied to ensure that the controls suggested in safety cases are applied in reality. Audits could be internal by a trialling organisation, or external by the testbed or another party, each approach has advantages and disadvantages. Further consideration is required on an audit process.

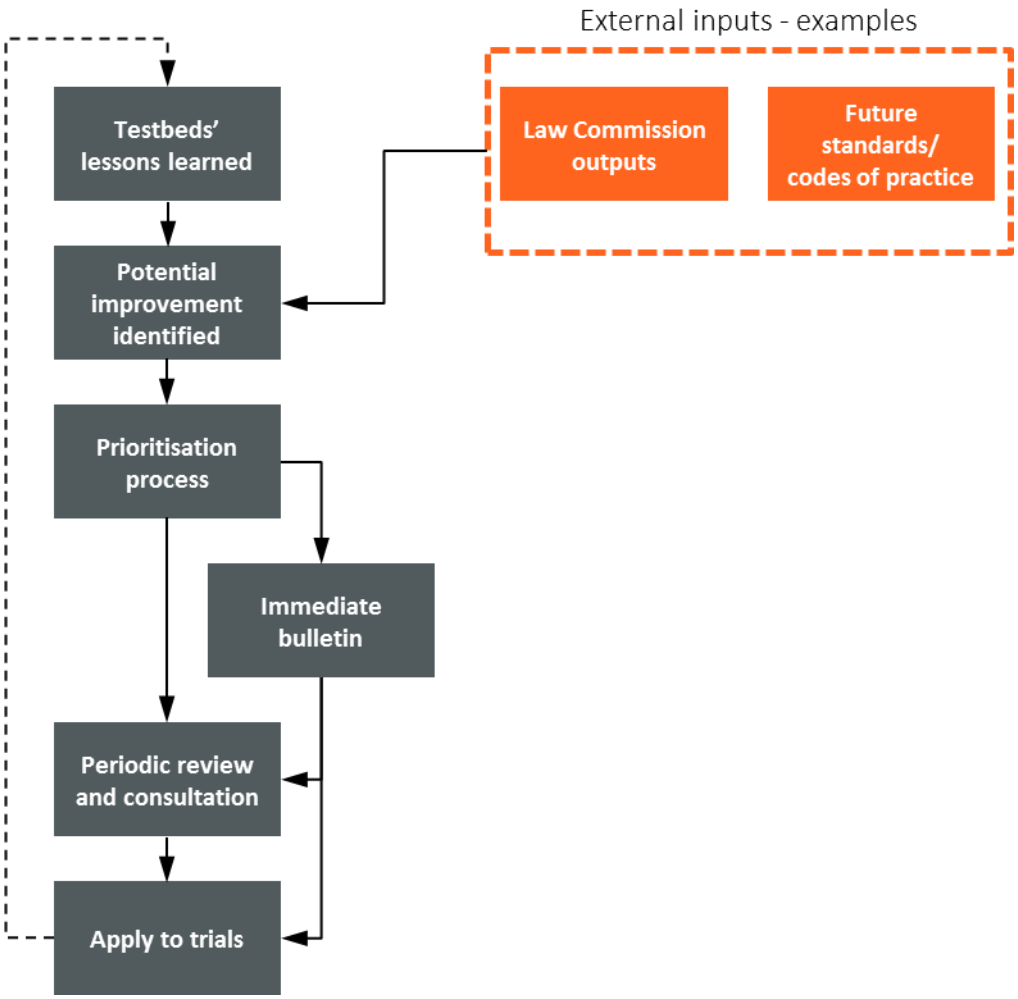
3.6 Publication

The 2010 Code of Practice recommends that an abridged, public version of the safety case should be made freely available. Testbeds should be aligned regarding the information required in published safety cases.

3.7 Safety Case Framework Updates

Inevitably, safety case requirements will evolve as connected and self-driving vehicle trials take place and technology is developed. *Figure 3.4* suggests a continuous review and improvement process to manage the updating of the Zenzic safety standard guidance with further updates. This process starts with knowledge gained from an internal input (such as a connected and self-driving vehicle trials taking place) or externally (such as a report from the Law Commission). This information must be reviewed to identify possible improvements to the guidance. Depending on the urgency of the change, it could then be passed on to be implemented immediately through an urgent bulletin or left until the next periodic review.

Figure 3.4 Continuous review and improvement process



4 | Next steps

This report represents the second phase of work in creating a safety case framework for connected and self-driving vehicle testing – a topic that is continuously evolving. This Safety Case Framework has already been adopted by CAM Testbed UK and the next steps for development are outlined in *Table 4.1* below.

Table 4.1 Next steps for safety case development

Feedback	Feedback from testbeds and trialling organisations on: • Risk factors • Safety Case Levels • Transition process
Implement	Implement the Safety Case Framework in testbeds
Develop	• Detailed guidance for different levels of safety case for connected and self-driving vehicle trials (including pre-trial activities within testbeds) • Acceptance/evaluation criteria for testbeds • Requirements for publicly available safety cases • Supporting processes: - Independent safety assurance - Safety case updates process

5 | References

DfT. (2019). *Code of Practice: Automated Vehicle Trialling.* London: DfT.

Transport Research Laboratory. (2019). *Safety Case Framework - A Report by Zenzic.* Zenzic.

6 | Appendix A Safety Case Framework Guidance

A.1 Purpose and scope of the safety case

This section should provide the purpose of the safety case, background information regarding the trialling organisation and consortium partners (if applicable) and an overview of the testing or service being conducted. The scope of the safety case should include the phases of testing or test scenarios the document covers and information regarding how safety case versions are managed and updated as well as notable exclusions (i.e. outside the scope of the safety case). In this section, the author should state to what codes of practices, standards and guidance the safety case has been developed to comply with.

A.2 Introduction to the safety case

An overview of the vehicle, ADS, safety driver and test environment should be included. A detailed list of objectives should be provided which covers the intended outcomes for the trial. This may include validation criteria, testing research hypotheses, and aims of service testing.

It may benefit testbeds to provide details of the test environment intended for use. Useful details may include a route map, restrictions (i.e. which areas of a testbed which are going to be used) and ownership of the roads e.g. Highways England/Transport for West Midlands.

This section should also detail what stages of testing and vehicle development the safety case refers to and may detail the planned development pathway (through other testing facilities). Where applicable, the safety case author should give a brief description of the intent and level of public involvement.

The introduction should also clarify who was involved in the development of the safety case and outline the roles and responsibilities of the parties involved. The Code of Practice (DfT 2019) expects trialling or trialling organisations to develop a detailed safety case before conducting trials in public domains. Safety case development is the responsibility of the trialling organisation, but it is recognised that all parties involved in the trial (including testbed staff) have a responsibility for safety.

A.4 Vehicle and automated driving system

In order to test automated vehicles on UK roads, the vehicle must be roadworthy and in accordance with UK Law. In this section, a description of the vehicle should be provided which details the vehicles build, design and approval status of the vehicle.

In order to demonstrate vehicle roadworthiness, evidence should be provided of its compliance with UK regulations. This includes certification under pre-registration approval schemes (either Type Approval, Individual Vehicle Approval, or National Small Series Type Approval) and roadworthiness certification via a MOT (where applicable). For any modifications after vehicle registration, especially for safety related equipment/components be declared and addressed. Any modifications must also be demonstrated as compliant with applicable regulations (including Construction & Use Regulations 1986) and any required legal dispensation should be sought and

acquired. Applicable regulations will depend on the testing environment, so it is beneficial to declare which regulations specifically apply and are being followed as well as any dispensations granted.

Detail should be provided of the automated control modes and function of the ADS. This is to explain the expected capabilities and limitations of the vehicle (ODD) and the safety driver's monitoring responsibilities. Safety driver intervention criteria should also be supplied. Appropriate and reliable handover between driver and AV is a key factor in ensuring safety so supporting evidence should be provided to demonstrate that the driver is able to retake full control in normal operation and under all foreseeable fault conditions/hazardous situations and revert the vehicle to a minimal risk condition. This should include physical testing to validate the ability of the safety operator to override or resume control within appropriate timescales.

In this section practical considerations should be identified including suitably secure storage, appropriate maintenance and refuelling/charging procedures to demonstrate that the vehicle can safely operate as intended for the duration of the trial.

A.5 Operational Design Domain and test scenarios

The ODD of the vehicle specifies the operating conditions in which the vehicle is designed to safely operate. This section is intended to demonstrate that the ADS has been designed to operate within the environment and scenarios it is being tested in and within the defined boundaries of the ODD. In this section of the safety case, details of the ODD and expected vehicle behaviour should be provided. Details include (but not limited to): the high-level boundaries, identified road features, environmental conditions, visibility, traffic flows, specific vehicle limitations. Evidence on the reliability of operation according to the ODD should be provided along with the process for monitoring ADS behaviour and departures from the ODD.

The ODD should align with the testing environment or appropriate controls identified that mitigate the risks associated with testing outside the defined ODD.

A.6 Operational risk assessment

The purpose of the risk assessment is to assess the tolerability of risk and demonstrate that, through the inclusion of suitable risk decisions and effective mitigations, the level of risk posed by the testing or trial is reduced as low as reasonably practicable (ALARP).

The operational risk assessment is the core of the safety case and should include the entire scope of tests planned at the testbed, all aspects of the system (vehicle, ADS, safety operator, route, infrastructure, V2X, fleet management) and the potential impact on all affected parties. This is an essential requirement for all safety cases regardless of the trial complexity, level of automation or test environment. It is essential for all testing including connected vehicle testing and manually driven trial preparations.

The risk assessment methodology (either qualitative or quantitative), scope and tolerability criteria should be defined. The methodology should also outline a suitable process for identifying all hazards in scope of the assessment and analysing their causes. Parties affected by each hazardous scenario should also be identified and considered when assessing risk. The risk assessment should detail appropriate mitigations to reduce the risks to a tolerable level.

Additional technical assessments may be conducted to assess the risks associated with specific aspects of the trial (e.g. cybersecurity, functional safety, SOTIF and route assessments). While these may be detailed elsewhere in the safety case or in additional documentation, the findings of these assessments should be appropriately incorporated into the operational risk assessment in order to suitably evaluate all risks associated with the trial.

Risk mitigations, including control measures and safe working practices, should be identified in the operational risk assessment and incorporated into operational guidance, trial management requirements, emergency response plans and training.

A.7 Operational guidance

Operational guidance consists of the policies, procedures and guidance documents provided to educate and train all trial members how to conduct trial activities in a safe manner. Operational guidance should be produced incorporating the findings of the risk assessment so that key risks, their controls, and responsibilities for enforcing them are clearly communicated to trials team members. As part of this section, a clear outline should be provided of each trial role and their responsibilities for implementing and complying with operational guidance and ensuring safety through the trial.

The documentation should cover safe working practices and safety policies as well as procedures for safety monitoring and incident reporting.Safety driver training, selection and safety including the management of fatigue, workload and distraction should be documented. The testing environment, route sections and operational restrictions should be clearly identified including the required dynamic checks, eligibility and abort criteria.

Demonstration of appropriate contingency planning should be provided. It is important to recognise, that even though the risks have been controlled to a tolerable level, residual risk remains and a timely, appropriate response to an incident is key to mitigating the consequences. It is also important to have an appropriate emergency response plan that details the appropriate response to key risk being realised and should detail the necessary line of communication to ensure timely response and escalation to the relevant parties. The emergency response crisis communications plans should be shared with the relevant stakeholders (e.g. landowners, emergency services and escalation points within the trialling organisations).

This section of the safety case should also identify how trial staff will be trained on the contents of operational guidance. The intended involvement, if any, of testbed staff should also be defined and their requirements for training and guidance included.

This section of the safety case should also identify how trial staff will be trained on the contents of operational guidance. The intended involvement, if any, of testbed staff should also be defined and their requirements for training and guidance included.

The safety driver training objectives should be established in line with the ODD, responsibilities, risks assessed, and the safe working practices the safety driver is required to implement. Details of the training delivery should also be provided including a final sign-off/certification of competency by the trialling organisation. An ongoing development plan should be outlined including plans for additional training/retraining in response to lessons learnt and technology developments.

A.8 Route selection and assessment

Evidence is required to show that the route selected for trial is suitable, the vehicle is designed to operate in it (it is within the boundaries of the defined ODD), and the associated risks are assessed and controlled effectively. An assessment methodology and key findings should be provided to demonstrate that the identified route(s) for automated driving/ identified test scenarios is appropriate and can be safely navigated and appropriate controls have been identified and implemented to manage the risks associated with static and dynamic hazards.

A.9 Safe operation and control

This section is concerned with demonstrating that control of the vehicle can always be maintained during trialling. This is a key requirement for ensuring that positive control of the vehicle can be maintained under all circumstances.

Details of the systems, training and procedures that demonstrates that a safety driver/ remote operator is always able to retake control of the vehicle should be provided. The purpose is to demonstrate that the driver/ operator and/ or control systems can reliably revert the vehicle to a minimum risk state at any time.

If remotely operated, it is necessary to demonstrate that the same level of monitoring and control can be exerted by a remote operator and deliver the same level of safety as a safety driver sat in the vehicle's driving seat.

A.10 Security

As a connected and/or automated vehicle, it is potentially easier to gain unauthorised access to take control or sabotage compared to a normal vehicle. As such, a greater level of assurance is required to demonstrate that the vehicle and connected infrastructure is protected from physical and cyber security threats.

This section should consider all physical and virtual access points to the vehicle and trial equipment and assess the associated risks with unauthorised access. The evidence should demonstrate that all appropriate controls have been put in place to ensure that the risks of unauthorised access and control of the vehicle or equipment has been reduced ALARP.

There are several relevant guidance documents and standards that should be referred to:

- CCAV Code of Practice: Automated Vehicle Trialling (DfT, 2019);
- The Key Principles of Vehicle Cyber Security for Connected and Automated Vehicles (DfT, 2017);
- BSI c PAS 1885:2018 The fundamental principles of cyber security (BSI, 2018);
- BSi PAS 11281:2018 Connected automotive ecosystems – impact of security in safety (BSI, 2018);
- The General Data Protection Regulation (GDPR) 2018 (EU, 2016/679), and;
- The Data Protection Act 2018.

Compliance with these standards indicates that good practice security management has been achieved.

A.11 Assurance of system safety

This safety case is primarily concerned with operational safety. However, it is important to provide high level assurance that a safe systems development process for the ADS has been followed and the necessary tests conducted to demonstrate the level of functionality required for the identified test scenarios. System Safety assurance should consider appropriate standards and guidance e.g. ISO26262, ISO/PAS 21448 – Safety of the Intended Function, BSI PAS 1880 – Guidelines for developing and assessing control systems for automated vehicles.

Findings from system safety assessment(s) should be used to inform the operational risk assessment to identify hazardous scenarios and assess risks relating to the failure modes and reliability of the systems functions and their consequences in an operational setting. These assessment findings should also be considered when evaluating the effectiveness of vehicle fail-safes and mitigations

A.12 Safety testing and acceptance process

The extent of assurance required from safety testing will be dependent on the stage of vehicle development, the test environment and the test scenarios identified. Vehicle capabilities required to undertake the identified test scenarios in the public domain should be supported with sufficient evidence of testing in a controlled environment e.g. proving ground. Simulated testing should be validated through real world testing prior to testing in the public domain.

An overview of the relevant safety testing conducted to date should be provided including the test objectives, test acceptance criteria and the location of the testing. The purpose of this testing is to ensure and demonstrate that the essential vehicle functionality has been achieved to safely conduct the identified test scenarios. The results from the safety testing and acceptance should be incorporated into the systems road release procedure and inform the decision for final sign-off/ certification of competency prior to on road testing.

An overview of the relevant safety testing conducted to date should be provided including the test objectives, test acceptance criteria and the location of the testing. The purpose of this testing is to ensure and demonstrate that the essential vehicle functionality has been achieved to safely conduct the identified test scenarios.

A.13 Modelling and simulator studies

The purpose of this section is to identify what modelling or simulator testing has been conducted prior to the trial or testing to support the overall test program. This may include information about the type of modelling or simulation used, the scope of the ODD, limitations of the testing and how the results have been used to provide safety assurance.

A.14 Change Control

An overview of the change control process should be provided. The process should define what events trigger a review of the safety case (and those that do not) and a process for documenting and communicating changes. Changes may include hardware or software changes as well as operational changes such as increasing the number of vehicles, a new route or different test scenarios.

A.15 Compliance

The safety case must demonstrate the trial is being conducted in a safe manner and in accordance with UK law. For test facilities in the public domain, there is a requirement to comply with UK road traffic laws as well as the requirements of the land owners and good practice. Evidence of required compliance should be provided in the form of assessment and declaration/statement of compliance with the relevant standards and regulations. For testing in the public domain, compliance with at least the following should be evidenced:

- UK Vehicle Regulations and in-service requirements;
- DfT Code of Practice: Automated Vehicle Trialling;
- The Highway Code and Road Traffic Law;
- General Data Protection Regulation (GDPR); and
- Relevant Cybersecurity Standards

Any areas of non-compliance with the above should be stated and reasonably justified. Evidence that all necessary legal dispensation has been achieved to conduct the trial should be provided.

A.16 Stakeholder consultation and engagement

Stakeholder consultation and engagement in advance of the trials is conducted to:

- Educate, raise awareness and get feedback from stakeholders and members of the public about the risks and potential benefits of the trial, and
- Acquire the relevant approvals and permissions to conduct the trial safely, ethically and legally.

Stakeholder consultation may be achieved by different means, for example: advisory groups, marketing campaigns and published materials. By any means, a PR and communications strategy to inform stakeholders about the trial should be developed. The list of consulted parties and the method through which they were engaged with should be detailed in the safety case. Safety feedback and recommendations should be detailed in the safety case as well as measures implemented to address these concerns (where reasonably practicable) to ensure trial safety.

As part of this section, evidence of insurance providing adequate cover for the trial and details of any pre-arranged vehicle recovery services should be provided. In order to ensure all relevant approvals and permissions have been granted, a list of all authorities contacted should be detailed as well as the permissions granted. This may include approval/permission to use or change the desired route.

Connected and self-driving vehicle trials involving human participants should ensure that ethics assessment procedures for ensuring the safety of research participants is followed. The mechanism for assessing the ethical implications of the trial (independent from the project) should be defined and details of internal/external ethics approval panels held, and their outcomes should be provided.

A.17 Monitoring, reporting and continuous improvement

The confidence in the risk decisions made will increase as technology matures and more evidence is gathered as a result of trials and testing. It is important that lessons are learned through monitoring and fed back into the safety case.

A suitable monitoring and analysis plan should be in place that demonstrates that key risks are being monitored throughout the trial. The sensors, instrumentation and the data captured specifically for monitoring safety throughout the trial should be defined and a process for recording, identifying and analysing undesired events should be established and implemented.

Incident reporting and investigation is a key feedback mechanism. Failure to review the risks in response to an incident is a clear indication that the safety case is not being used and robustly maintained. The procedure should define a mechanism for reporting, escalation and investigation for all involved parties.

This section should also detail plans for cooperation for police investigators and relevant organisations to allow these organisations to readily and immediately access data in the event of an incident. This is recommended to be facilitated by an event data recorder to capture that information surrounding the time of the incident. Similar plans are recommended to be adopted to share data with the testbeds as well.

In order to demonstrate continuous improvement of the safety case, the findings from safety monitoring should be fed back into the risk assessment in order to capture the new risks or validate risk decisions. A change control process should be identified to ensure that the changes to the risk assessment trigger an appropriate review of the risk decisions and mitigations and any changes are effectively implemented. An appropriate method to ensure this continuous improvement feedback loop should be detailed within the safety case.