ZENZIC

SELF-DRIVING REVOLUTION

United Kingdom

It is essential that trials of Connected and Automated Mobility (CAM) technology are conducted safely to protect the public and those conducting the trials. When dealing with systems that present a risk of harm, everyone involved has a responsibility to ensure safety.

Safety Case Framework: The Guidance Edition Explainer

Our partners:

MIRA

WMG THE UNIVERSITY OF WARWICK

TRL

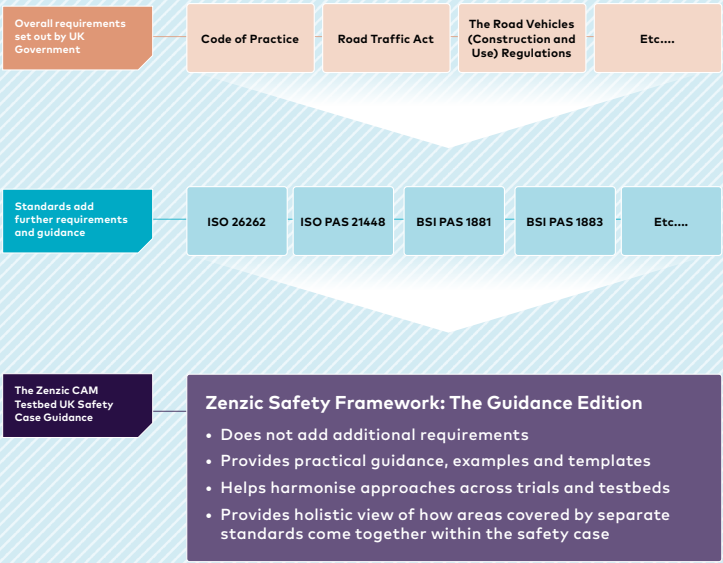
Zenzic
@ZenzicUK
info@zenzic.io
zenzic.io

Why is a safety case Important?

A safety case helps to ensure that all safety evidence is documented, so there is a 'single source of the truth' defining the risks, mitigations and evidence. This provides the basis for the safety of trials to be reviewed and approved, and also provides a key defence should an incident occur.

Zenzic has provided a detailed safety case guidance to help organisations conducting CAM testing and trialling to apply best-practice safety measures. In parallel to this, guidance is available to those reviewing safety cases, to help them understand what safety measures and what level of detail they should expect.

The Zenzic guidance aims to provide support through explanations and examples showing suitable approaches to meet the relevant regulations, codes and standards. It is important to note that there is no 'one true solution' for safety cases, and therefore flexibility should remain to allow alternative methods to be used.



WHAT IS IN A SAFETY CASE?

A safety case would typically include multiple separate documents such as process definitions, risk assessments and test data, with a '**safety argument**' being included to explain how the separate pieces of evidence fit together to demonstrate that the activity is safe.

The goal of the overall trial being **Acceptably safe** would typically be supported by multiple sub-goals relating to the operational safety, system safety and security. These subgoals can be further broken down as required to create a complete **safety argument**.

Risk assessments: Method of estimation of the likelihood and severity of harm.

Safety argument: Explanation of how the safety evidence, when taken together, supports the overall goal of the trial being safe.

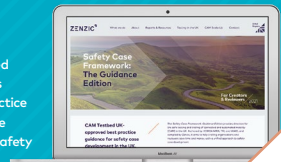
Operational safety: Safety measures put in place to mitigate hazards caused by the vehicle, such as the presence of a safety driver.

System safety: Ensuring that the system behaves in a safe way.

Security case: Assessing and mitigating the risks posed by physical and cyber security threats.

Framework for creating and reviewing safety cases

Zenzic, with CAM Testbed UK partners, have produced a detailed safety case guidance to help organisations conducting CAM testing and trialling to apply best-practice safety measures. A guidance is also available to those reviewing safety cases, to help them understand what safety measures and what level of detail they should expect.



How detailed should the safety case be?

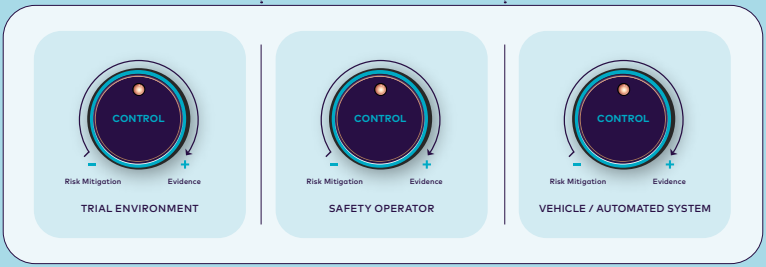
Some trials are inherently harder to make safe than others. For example, a trial on a private track with controlled access and with a '**safety driver**' behind the wheel will be easier to make safe than a trial upon a busy public road with only remote supervision.

The balance between minimising risk and supporting innovation therefore needs to be tailored according to:

Ability to control the test environment

Ability of safety operator to intervene

Maturity of vehicle and automated driving system



DEFINING THE TRIAL CHARACTERISTICS

To support the analysis of safety, the characteristics of the intended operating environment need to be clearly defined. This is referred to as the **Operational Design Domain** (ODD). It is important that the ODD of the vehicle is compatible with the test locations and scenarios that are planned, and that stakeholders understand what is in scope when considering possible hazards.

ODD: Operational Design Domain, the surrounding environment that the system is intended to operate in.

Safety Operator: Person responsible for monitoring system behaviour and intervening where necessary to prevent accidents.

Safety Driver: A safety operator who is in the vehicle and has access to conventional vehicle controls.

Method Statement: A document describing safe systems of work and the key roles and responsibilities, so it is clear to all involved.

THE OPERATIONAL SAFETY CASE

For most trials, the technology will not have completed sufficient testing to be able to be relied upon in all conditions without needing human intervention. The key to most safety cases will be the operational measures such as the use of a safety operator or selection of an appropriate test environment for the still-developing technology.

THE SYSTEM SAFETY CASE

For advanced trials that do not use a conventional safety driver. It is necessary to undertake analysis and testing to ensure that the system is able to operate safely without human intervention. This would typically require a programme of 'scenario-based testing' to cover the range of scenarios the vehicle could encounter – and as every driver knows, the range of situations that can be experienced on the road is vast! However, even for less complex trials with a conventional safety driver, it is still necessary to provide assurance that the system is controllable; for example, any controls used to disengage or override the system must be robust.

THE SECURITY CASE

Security breaches include cybersecurity threats such as hostile actors deliberately interfering with the system and well-meaning individuals inadvertently compromising it, but also include physical breaches such as vandalism and theft. The guidance therefore sets out methods to assess the security risk presented by the trial and to put in place suitable mitigations. Trials conducted in secure locations, on a small scale and with trial personnel always present, for example, would be inherently more secure than trials featuring large numbers of remotely supervised vehicles operating in public places.

PROCESS CONSIDERATIONS

Guidance is provided on:

- Suitable sign-off processes to ensure both the initial safety case version and any future updates are subjected to an appropriate review;
- Incident reporting processes to allow incidents to be recorded and learnt from, and;
- Consultation with stakeholders such as testbed operators, highway authorities and emergency services.

This is important to ensure that due diligence is applied and continues to be applied throughout the life of the trial.

CAM Testbed UK

In order to fully explore the capabilities and limitations of new technology, it is vital to have a testbed that allows a wide range of tests to be carried out. CAM Testbed UK allows connected and autonomous mobility solutions to be trialled in a range of environments, including public and private facilities and a vast range of road configurations. For more information please visit:

https://zenzic.io/testbed-uk/

ZENZIC