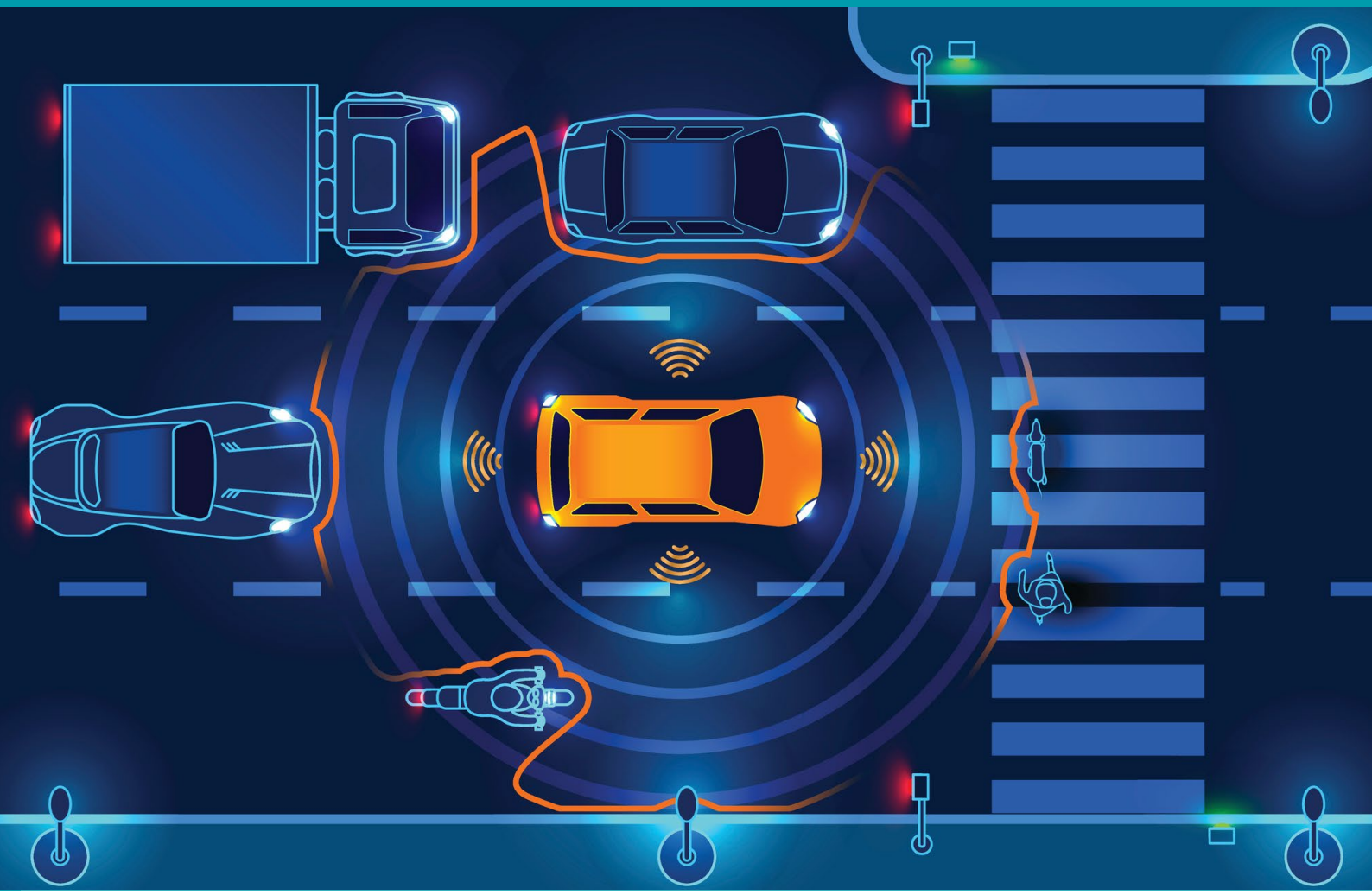
PAS 1881:2020

Assuring the safety of automated vehicle trials and testing – Specification



Centre for Connected & Autonomous Vehicles

bsi.

Publishing and copyright information

Published by BSI Standards Limited 2020.

ISBN 978 0 539 04058 6

ICS 43.020

Publication history

First published February 2020

Contents

Foreword

This PAS was sponsored by the UK's Centre for Connected and Autonomous Vehicles (CCAV). Its development was facilitated by BSI Standards Limited and it was published under licence from The British Standards Institution. It came into effect on 29 February 2020.

Acknowledgement is given to Camilla Fowler of TRL, as the technical author, and the following organizations that were involved in the development of this PAS as members of the steering group:

- Adelard LLP
- Centre for the Protection of National Infrastructure (CPNI)
- Connected Places Catapult
- Consumer and Public Interest Network (CPIN)
- FiveAI
- Highways England
- HORIBA MIRA
- Loughborough University
- Millbrook Proving Ground
- Oxbotica
- Oxfordshire County Council
- Potenza Technology Ltd
- Remote Applications in Challenging Environments (RACE)
- Royal Borough of Greenwich
- Transport for London (TfL)
- Warwick Manufacturing Group (WMG)

Acknowledgement is also given to the members of a wider review panel who were consulted in the development of this PAS.

This PAS is not to be regarded as a British Standard. It shall be withdrawn upon publication of its content in, or as, a British Standard.

The PAS process enables a specification to be rapidly developed in order to fulfil an immediate need in industry. A PAS can be considered for further development as a British Standard, or constitute part of the UK input into the development of a European or International Standard.

Use of this document

It has been assumed in the preparation of this PAS that the execution of its provisions shall be entrusted to appropriately qualified and experienced people, for whose use it has been produced.

Relationship with other publications

PAS 1881 has been developed as part of a wider programme sponsored by CCAV in conjunction with the Department for Transport (DfT), Innovate UK and Zenzic to develop a suite of standardization products to promote the safe testing and deployment of automated vehicles in the UK and inform wider international standardization activity.

PAS 1881 specifies requirements for operational safety cases for automated vehicle trials and development testing in the UK to demonstrate that trialling and testing activities can be undertaken safely and securely. It is intended to be read in conjunction with:

- guidance on system safety, including PAS 1880[1)], PAS 1882[2)], PAS 1883[3)] and PAS 11281;
- where applicable to the trial, safety and stakeholder requirements, including the DfT's *Code of practice: Automated vehicle trialling* [1], Transport for London's (TfL) *Connected and autonomous vehicles: Guidance for London trials* [2], and Highways England's *GG104: Requirements for safety risk assessment* [3]; and
- existing legislation for UK vehicles and roads.

Presentational conventions

The provisions of this PAS are presented in roman (i.e. upright) type. Its requirements are expressed in sentences in which the auxiliary verb is "shall".

Commentary, explanation and general informative material is presented in smaller italic type, and does not constitute a normative element.

Where words have alternative spellings, the preferred spelling of the Shorter Oxford English Dictionary is used (e.g. "organization" rather than "organisation").

Contractual and legal considerations

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard cannot confer immunity from legal obligations.

Particular attention is drawn to the following specific legislation:

- The Road Traffic Regulation Act 1984 [4];
- The Road Vehicles (Construction and Use) Regulations 1986 [5];
- The Road Traffic Act 1988 [6];
- The General Data Protection Regulation (GDPR) [7];
- The Road Vehicles (Approval) Regulations 2009 [8];
- The Data Protection Act 2018 [9]; and
- The Automated and Electric Vehicles Act 2018 [10].

[1)] In preparation.
[2)] In preparation.
[3)] In preparation.

Introduction

As automated vehicle technologies are developed, there is an increasing demand to test and trial driving automation technologies and mobility services on the UK road network. There has been significant government and industry investment in the development of automated vehicle technology, and the UK government is committed to ensuring that automated vehicle trials and ongoing technology testing are conducted safely and securely. The UK government is also committed to building public and consumer trust and acceptance of the technology. This PAS supports the government's commitment by creating a standardized and consistent approach to safety case development for trialling organizations to adopt, and encourages safety to be prioritized during technology development and testing. This PAS also provides the guidance to enable robust and transparent safety cases.

Safety assurance for automated vehicles can be categorized into two interdependent areas: system safety and operational safety. System safety is achieved through ensuring adequate functional safety, safety of the intended functionality (SOTIF) and cybersecurity. This forms an integral part of the vehicle development and includes the vehicle specification, design, implementation, and verification and validation of the automated vehicle's functions. System safety assessments can also be risk-based assessments that identify the vehicle's minimum safety and security requirements for achieving an acceptable level of risk and ensure that this level of risk has been achieved. Operational safety assurance considers the interaction of an automated vehicle with the operating environment, including the route, safety driver or operator, passengers and other road users and road workers. System safety and operational safety are intrinsically linked, but this PAS focuses on the operational safety and references the required outputs from system safety assessments. Further guidance on automated vehicle safety is also available in PAS 1880, which provides a guide for developing and assessing automated control systems, PAS 1883, which focuses on the operational design domain (ODD) and PAS 11281, which focuses on the impact of security on safety.

A safety case is a structured argument supported by a body of evidence that demonstrates that the safety risks have been identified, managed and reduced as low as reasonably practicable (ALARP). The safety case includes (but is not limited to) risks associated with the vehicle, operating platform, vehicle control and the operating environment, and considers risks to all affected parties, including other vehicles, vulnerable road users, the safety driver or operator, passengers, road workers and third parties. The safety case provides assurance to stakeholders, including highway authorities, road operators, landowners, leaseholders, insurers and members of the public. The safety case is a live document that, when updated to reflect changes and learning throughout a trial, promotes continuous improvement and safety assurance.

The safety case framework detailed in this PAS has been developed for automated vehicle trials but is based on existing safety standards and safety governance good practice; the DfT's *Code of practice* [1] recommends that trialling organizations develop a detailed safety case before conducting trials in public domains. This safety case framework has been applied to a number of automated vehicle trials and has been continually refined and updated to reflect learning from those trials and input from stakeholders.

1 Scope

This PAS specifies requirements for safety cases for automated vehicle trials and development testing in the UK to demonstrate that trialling and testing activities can be undertaken safely and securely.

It covers the development of an operational safety case to demonstrate that the risks to all affected parties throughout automated vehicle trials and testing are reduced as low as reasonably practicable (ALARP). This includes operational risk assessments, safety testing, training, safety monitoring, compliance and permissions granted. It is applicable to all real-world testing environments, including test tracks and public domains and to all levels of driving automation systems. However, a safety case developed for test tracks might not need to include all elements detailed in this PAS.

This PAS does not cover the system safety of the vehicle (e.g. functional safety, safety of the intended functionality (SOTIF) and cybersecurity assessments) but does rely on their outputs. This PAS does not include the safety case requirements for the testing of a connected vehicle that is not also automated.

This PAS is intended for use by trialling organizations, including private developers and original equipment manufacturers (OEMs), developing safety cases for automated vehicle trials and testing. Compliance with this PAS does not guarantee acceptance of the safety case by relevant organizations.

This PAS might be of interest to organizations requiring assurance that a safety case has been developed in line with good practice, for example, highway authorities, road operators, landowners, leaseholders and insurers.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purpose of this PAS the following terms and definitions apply.

3.1 as low as reasonably practicable (ALARP)

statement which outlines that all reasonably practicable mitigations and measures to manage the risks of an activity have been implemented

NOTE *Reasonably practicable measures are those that can control the risk and that are not grossly disproportionate to the sacrifice, time and money needed to implement them.*

3.2 automated driving system (ADS)

vehicle system that uses both hardware and software to perform all, or some, of the dynamic driving tasks to undertake a journey

3.3 automated vehicle

vehicle fitted with an automated driving system (ADS) that uses both hardware and software to perform dynamic driving tasks associated with moving the vehicle within a defined operational design domain (ODD)

3.4 controlled environment

area where certain parameters are directly manipulated by the trialling organization or test bed and risk factors outside of the intended test environment are unlikely to occur

3.5 dynamic driving task

tactical functions and operational functions which form part of driving the vehicle, excluding trip scheduling, route planning or other strategical functions

NOTE *Tactical functions are object and event detection and response, and operational functions are longitudinal and lateral motion control.*

3.6 ethics committee

group of qualified individuals formed to protect the interests of participants or persons affected by the trial and to ensure moral issues are addressed

***NOTE** Depending on the potential ethical impact, an ethics committee might require members who are independent from the trialling organization or consortium partners.*

3.7 functional safety

part of the overall safety of a system that concerns the ability of an automatic safety system to operate correctly according to its inputs and to respond to faults and failures in a safe manner

***NOTE** A functionally safe system takes into account likely human errors, hardware failures and operational or environmental stress.*

3.8 hazard

action that has the potential to cause harm and/or illness or damage/loss of property or possessions

3.9 human-machine interface (HMI)

hardware and software that allow users to interact with machines, translating their inputs into signals and providing feedback

3.10 incident

event which results in injury, ill health, damage or loss

3.11 localization

determining the position of an element in a predefined environment

***NOTE** For automated vehicles, determining the vehicle's precise position with respect to the vehicle's surroundings is called "localization".*

3.12 method statement

description in logical sequence of how a task is carried out in a safe manner

***NOTE** A method statement includes all the risks identified and measures to control those risks.*

3.13 minimal risk condition

stable, safe condition to which a user, safety operator or an ADS may bring a vehicle after performing the dynamic driving task fallback

***NOTE 1** A minimal risk condition may vary according to the type and extent of the failure, the ODD, and the presence of a safety driver in the vehicle.*

***NOTE 2** A minimal risk condition is carried out in order to reduce the risk of a crash when a given trip cannot be continued.*

3.14 near miss

event that did not result in injury, illness, loss or damage, but had the potential to do so

3.15 operational design domain (ODD)

operating conditions under which a given driving automation system or feature thereof is specifically designed to function

***NOTE** This includes, but is not limited to, environmental, geographical, and time-of-day restrictions, and/or the requisite presence or absence of certain traffic or roadway characteristics.*

3.16 operational safety

identification and management of all risks associated with completing any activities within the defined operating environment

***NOTE** The measures put in place to ensure appropriate operational safety and security are influenced by the capabilities and safety of the system, as given in PAS 1880, in addition to, for example, consideration of human factors or hazards in proximity to the vehicle.*

3.17 risk

combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: BS ISO 26262-1:2018, **3.128**]

3.18 safety case

structured argument, supported by evidence, intended to justify that a system and activity is acceptably safe for a specific application in a specific operating environment

3.19 safety of the intended functionality (SOTIF)

absence of unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality or from reasonably foreseeable misuse by persons

[SOURCE: PD ISO/PAS 21448:2019, **3.10**]

3.20 safety operator

person who is trained and able to supervise the function of an automated vehicle and intervene at any time it is required

***NOTE** The safety operator is used to describe a safety driver or remote operator. A safety driver is a safety operator who is situated within the vehicle itself to oversee its operation. A remote operator is a safety operator who oversees the operation of the vehicle from a remote location.*

3.21 scenario

series of events that are linked to create a test or hazardous situation

3.22 system safety

assurance that the system as a whole, including the vehicle, ADS and communications, is safe

***NOTE** System safety includes functional safety, SOTIF and cybersecurity.*

3.23 test bed

facility within which the testing of an automated vehicle can take place

***NOTE** Test beds can either be "off-road" or "on-road".*

3.24 track testing

testing conducted in test facilities with a controlled environment used to develop and demonstrate acceptable performance before deployment in less controlled environments

3.25 trialling organization

organization responsible for the automated vehicle testing, trial or service being provided

***NOTE 1** In a consortium, the lead partner might assume the role of "trialling organization".*

***NOTE 2** Trialling organizations could be autonomous vehicle manufacturers, software development companies or sensor manufacturers.*

3.26 validation

extended mileage/duration testing of the product in real-world settings to provide assurance that it meets the needs of the customer or other stakeholders

***NOTE** This often involves acceptance and suitability with external customers.*

3.27 vehicle hardware

physical components of the automated vehicle system or physical components of the base vehicle

***NOTE 1** These components include computer hardware and sensors that enable the vehicle to perform functions such as perceiving its surroundings (through sensors), communicating (through V2X technology) and moving (through actuators).*

***NOTE 2** There are many other sensors used within the vehicle software such as motor torque and accelerometers.*

3.28 vehicle livery

branding or pattern applied to a vehicle

***NOTE** Vehicle livery may be used to ensure a vehicle is easily identifiable or to promote organizations or projects.*

3.29 vehicle software

system/s that process information from the hardware or other pure data inputs about the environment (from sensors and V2X technology) to determine what action the vehicle takes, which is then communicated to the vehicle's actuators

3.30 verification

evaluation of whether or not a product, service, or system conforms to a requirement, specification or imposed condition

***NOTE** This is often an internal process.*

3.31 V2X

wireless communication between a vehicle and any entity including other vehicles and infrastructure

3.32 vulnerable road user

road user who is more vulnerable to injury than a typical driver or passenger of a car, lorry, bus or coach

***NOTE** Vulnerable road users can include pedestrians, cyclists, horse riders, motorcyclists and persons using mobility scooters.*

4 Safety case requirements and ownership

The trialling organization shall develop, document and maintain a safety case for automated vehicle trials and testing to ensure and demonstrate that risks to all affected parties, including vulnerable road users, are assessed and reduced ALARP to an acceptable level throughout the lifecycle of the testing and trials.

NOTE 1 *Attention is drawn to the DfT's Code of practice [1] that recommends trialling organizations develop a detailed safety case before conducting trials in public domains.*

The safety case shall include all relevant requirements in accordance with Clause **5**. The safety case shall be proportionate to the level of risk posed; as such, not all requirements are necessary for some testing scenarios and environments.

The safety case shall be developed for all environments where testing or trials are conducted, including test tracks and public domains.

The safety case shall complement the safety processes and procedures implemented by test beds where such documents exist.

NOTE 2 *One safety case can be developed and expanded as trialling organizations transition from one testing environment to another.*

The safety case shall be prepared by (or prepared under the supervision of) a competent and experienced person. They shall be provided with accurate and timely information regarding ADS functionality, capabilities and limitations.

NOTE 3 *Additional input to the safety case may be sought from other appropriately qualified professionals, e.g. security engineers, software experts, machine learning (ML) experts, or artificial intelligence (AI) experts.*

The safety case shall be owned by the trialling organization.

NOTE 4 *Where the lead consortium partner assumes the role of trialling organization, the safety case content should be agreed with the relevant consortium partners.*

NOTE 5 *The safety case may be shared as appropriate with stakeholders, including highway authorities, road operators, landowners, leaseholders and insurers.*

5 Contents of the safety case

COMMENTARY ON CLAUSE 5

Attention is drawn to the legislative and good practice framework underpinning the safety case, specifically the following.

a) For trial and testing attention is drawn to:

1) the Road Traffic Regulation Act 1984 [4];

2) the Road Vehicles (Construction and Use) Regulations 1986 [5];

3) the Road Traffic Act 1988 [6];

4) the DfT's safety requirements for automated vehicle trials and testing, including its latest Code of practice [1];

5) the Highway Code [11];

6) the Law Commission's review of the legal framework of automated vehicles[4] [12]; and

7) any code of practice or guidance note published by the relevant local authority responsible for the area in which testing is undertaken, such as Transport for London's Guidance for London trials [2].

b) For trial vehicles attention is drawn to:

1) PAS 1880;

2) UK regulations relevant to the vehicle, including the Road Vehicles (Construction and Use) Regulations 1986 [5], the Road Vehicles (Approval) Regulations 2009 [8]; and

3) the appropriate regulatory body governing the assessment being performed, e.g. the Driver and Vehicle Standards Agency or the Vehicle Certification Agency.

c) For the testing location attention is drawn to the DfT's safety requirements for automated vehicle trials and testing, including its Code of practice [1].

d) For data, security and connectivity attention is drawn to:

1) the General Data Protection Regulation (GDPR) [7];

2) the Data Protection Act 2018 [9];

3) the DfT's safety requirements for automated vehicle trials and testing, including its Code of practice [1];

4) the DfT's Principles of cybersecurity [13]; and

5) PAS 11281 and PAS 1885.

[4] In preparation.

Reference should be made to safety cases developed for related systems, subsystems and equipment.

See also Annex A for a high-level overview of safety case development, including a flowchart and relevant case studies.

5.1 Purpose and scope of the safety case

The safety case shall demonstrate that at any given point in time the testing or trial being proposed is safe.

The safety case shall:

a) identify the name(s) of the organization that has developed the safety case; and

b) identify the trialling organization that owns the safety case.

The scope of the safety case shall be included and shall provide an overview of the testing or service being conducted, including the objectives, high-level methodology and testing or service phases, where appropriate.

The overview shall include (if appropriate) the project name and details of consortium partners and their role.

The scope shall state what information the safety case excludes, e.g. functional safety.

The scope shall contain information regarding the testing phase the safety case version refers to and how the safety case is managed and updated.

NOTE *The scope should detail when the safety case should be updated and under what circumstances, e.g. periodic review, additional complexity, hardware or software update, or in response to an incident or near miss (and the associated required timescales).*

The safety case documents shall state the version number, how versions are controlled and detail the edits made and dates of document release.

5.2 The safety case introduction

The safety case introduction shall include an overview of the methodology for the trial, testing or service.

NOTE 1 *The methodology overview should include:*

a) what vehicles are being used and the maximum number of vehicles the safety case covers;

b) where the testing is being conducted (test track or public domain) and the location(s);

c) how technology trials or service models are progressed or advanced over time; and

d) details of the service, if appropriate, including the purpose, maximum number of passengers in each vehicle and duration.

The roles and responsibilities of parties involved in the trials, testing or service shall be included in the safety case introduction.

The safety case introduction shall include a high-level description of vehicles, services or fleet management system being tested.

NOTE 2 *The high-level description should include:*

a) the vehicle type;

b) the vehicle use case, e.g. development testing, research trial, or service;

c) the maximum number of passengers;

d) a summary of the types of hardware used for sensing, processing and actuation, and the software and V2X communication used for the ADS;

e) the types of objects and features that the sensors and ADS are capable of detecting, including angles and ranges;

f) a summary of the AI or ML used and what it is used for;

g) the control of the vehicle, e.g. safety driver/remote operation;

h) the ODD;

i) the details of the fleet management system; and

j) the capabilities and limitations of the vehicles and the driving automation system.

A description of public involvement in the trial shall be included.

NOTE 3 *This section should detail how the public can be involved in the trial or testing and for what purpose, e.g. passengers, monitoring other road user interactions, and feedback.*

5.3 Vehicle and automated driving system

The safety case shall include high-level information regarding the vehicle(s) and ADS to provide context to the safety case and risk assessment, including:

a) the vehicle build and/or vehicle modifications, including a safety justification of any modifications made and alignment with existing specifications;

NOTE 1 *Attention is drawn to the DfT's Prototype road vehicles – Construction requirements [14].*

b) vehicle livery and conspicuity, including:

1) details of any specific markings or livery that are to be used and the justification for use;

2) assurance that additional livery meets required standards for vehicles types; and

3) the decision regarding livery;

c) assurance of compliance with appropriate vehicle and design standards;

d) sensors and camera locations and how they are secured to the vehicle;

NOTE 2 *Attention is drawn to the Road Vehicles (Construction and Use) Regulations 1986 [5] regarding sensor mounting.*

e) sensor location zones;

f) ADS modes and functionality. Details regarding the following shall include:

1) who developed the system and how it connects with the vehicle platform;

2) software versions in use;

3) how safety related applications specified for systems and subsystems have been implemented;

4) the vehicle elements that are controlled by the automated system; and

5) limitations of the ADS to inform the ODD, risk assessment and required mitigations, e.g the vehicle cannot reverse or the ADS can detect obstacles in front of the vehicle but not entering from the side;

g) a high-level overview of the navigation and localization for automated operation, including navigational dependencies of the system (e.g. high-definition maps, satellite localization, inertia sensors). Requirements such as pre-mapping the route, satellite systems, system calibrations and fleet management systems shall also be included;

h) an overview of the human-machine interface (HMI) including safety operator alerts and safety controls;

i) where AI or ML is used, the safety case shall demonstrate that decisions made are reliable and safe and that training data are representative of the ODD;
j) data storage and accessibility; and
k) security of the system (including cyber and physical).

NOTE 3 *Where the same information is required in multiple sections of the safety case, cross references should be used.*

NOTE 4 *Documents or additional safety cases that supplement the information in the safety case can be referenced for more information.*

5.4 Operational design domain and test objectives

The ODD shall be outlined in the safety case.

The safety case shall include the following information regarding the ODD:

a) the high-level boundaries, e.g. high-speed network including dual carriageways and motorways but not junctions;
b) how the ADS verifies that it is operating within the defined ODD;
c) specific road-environment limitations of the system, if applicable, e.g. identified road features, vulnerable road users, environmental conditions (including weather and lighting), visibility, and traffic flows;
d) specific vehicle limitations, if applicable, e.g. speed, manoeuvres;
e) the process (or minimal risk manoeuvre) for defaulting to a minimal risk condition given a hazardous situation or abort condition;
f) the process for monitoring ADS behaviour within the ODD and safety operator interventions; and
g) evidence that the system is capable of safely operating within the ODD.

Test objectives shall be documented in the safety case, including what the test scenario consists of, the elements or boundaries of the ODD being challenged or verified, software being tested, details of specific tests and how the tests are conducted, monitored and evaluated.

NOTE 1 *The description might include information on the vehicle movements, travel speed and disengagement zones. A diagram might aid in the description.*

The safety case shall include the following information:

1) scenarios outside the ODD which the system might be unable to negotiate or manage safely, including security or malicious threats;
2) safety operator responsibilities including takeover scenarios;
3) safety related roles assigned to other personnel;
4) how the minimal risk condition is achieved;
5) the checks and dynamic assessments that shall be conducted prior to and during testing;
6) required support functions including emergency services and vehicle recovery; and
7) safety monitoring, analysis and feedback.

NOTE 2 *Restrictions might include not testing when there are identified environmental conditions, e.g. narrow road sections, schools, poor lane markings, visibility restricted by street furniture or road layout.*

NOTE 3 *Dynamic assessments might include traffic flow rates, weather conditions, or other road user behaviour (including vulnerable road users).*

NOTE 4 *Safety operator requirements might include specific training, passing safety operator tests (pertinent to their organization or recognized body) and familiarity with the route.*

NOTE 5 *Other personnel performing safety related roles might be, for example, a second person present in the vehicle to monitor and manage systems (to avoid safety driver distraction), marshals or support vehicle drivers.*

5.5 Operational risk assessment

The trialling organization shall conduct a suitable and sufficient operational risk assessment and include this within the safety case.

NOTE 1 *A suitable and sufficient risk assessment is one that identifies and assesses all potentially hazardous scenarios, so far as is reasonably practicable, for the automated vehicle trial or tests.*

NOTE 2 *The trialling organization may contract another organization to conduct the risk assessment.*

The safety case shall provide an overview of the methodology used to identify hazards and assess and evaluate all operational risks that are foreseeable for each test scenario.

The risk assessment shall assess the risks posed to all affected parties, including the safety operator, passengers, other road users, road workers and third parties.

The risk assessment shall assess the risks associated with the vehicle hardware and software (including physical security, cybersecurity and inputs from analysis of the system), vehicle monitoring and control, external dependencies, including communications, the test procedures and the route (including infrastructure).

Interactions with road users and the impact on third parties shall be a key risk evaluated within the assessment, and include assumptions made about other road user behaviour.

***NOTE 3** Risk assessments can be conducted qualitatively using a risk matrix but should have sufficient risk levels as an outcome to allow risks to be prioritized.*

***NOTE 4** Road operators might hold an existing assessment of the most hazardous activities on their roads. Testing organizations should assess the potential impact on these hazardous activities and ensure the level of risk remains tolerable.*

All risks shall be reduced ALARP through the identification and implementation of effective controls for the identified risks. All controls implemented to manage the level of risk (including operational controls implemented to manage system safety) and decisions regarding the tolerability of the risk shall be documented within the safety case.

5.6 Operational guidance

Operational guidance shall be required to document safe working practices to be followed to assure safety and security throughout the lifecycle of the trial.

***NOTE 1** Operational guidance documents outline the safe working practices identified as mitigations in the risk assessment. The purpose of operational guidance is to ensure all people involved in the trial or testing know how to, and are able to, conduct tasks safely and securely and ensure a consistent approach is adopted.*

An emergency response plan shall be developed in consultation with emergency services and key stakeholders for all trials and testing.

***NOTE 2** The emergency response plan should contain all the information required to respond rapidly and effectively to an emergency situation and may include:*

a) information about the trial or test location, recovery and testing programme;

b) vehicles (including vehicle registration) and vehicle-specific hazards that could impact emergency services intervention or safety (for example, lidar safety requirements, battery isolation points, safe extraction points and the location of cables);

c) how to ensure vehicle motion is disabled;

d) an overview of the vehicles and trial;

e) definitions of the incident levels and the appropriate emergency response;

f) key roles and responsibilities of those involved in the emergency plan;

g) key contact details;

h) route information;

i) places of relative safety;

j) escalation;

k) incident reporting; and

l) details of emergency plan rehearsal and outcome reporting.

***NOTE 3** Key stakeholders might include highway authorities, road operators, landowners, leaseholders, insurers and emergency service professional bodies, e.g. National Fire Chiefs Council.*

***NOTE 4** See Annex B for other elements that may be included in operational guidance documents.*

5.7 Route selection and assessment

The safety case shall identify the route(s) where the vehicle(s) shall operate. Landowners or the appropriate authority shall be consulted prior to route selection.

***NOTE 1** Consultation with appropriate highway and transport authorities ensures local knowledge and future works, e.g. construction projects or road works, can be fed into the route selection and assessment.*

***NOTE 2** Consultation with stakeholders representing higher risk populations can inform the route assessment.*

For testing within a public domain, a safety assessment shall be conducted on the route(s), and the methodology and results included within the safety case to demonstrate that the route is suitable for the vehicle type and the testing being conducted.

For track testing the safety case shall conform to existing safety processes and requirements for the test track.

The safety case shall also detail any changes to infrastructure or street furniture and control measures implemented to minimize the level of risk posed from the vehicle trial, e.g. traffic management.

***NOTE 3** The purpose of a route assessment is to identify any hazards that could increase the level of risk posed during testing to an intolerable level, for example, a route feature, other route users (density and type), a high-risk area (e.g. hospital or school) or traffic characteristics that:*

a) could increase the probability of a hazardous event being realized;

b) increase consequence severity; or

c) are not within the boundaries of the ODD and require additional control.

***NOTE 4** Control measures might include safety operator awareness of hazards, marked vehicle routes, safe passing areas, warning signs and barriers.*

***NOTE 5** Route information recorded in the safety case might include the following:*

a) route length;

b) carriageway type;

c) speed limit;

d) traffic flows and composition;

e) pedestrian and vulnerable road user density;

f) review of available historical collision data;

g) hazards and potentially hazardous scenarios;

h) barriers to performing the trial that may lead to disengagement;

i) agreed planned disengagement zones;

j) details of any licences acquired for use of road or specific road types or lane use; and

k) storage facilities and security access measures.

***NOTE 6** The safety case should provide evidence that the safety operator is able to make corrections to the vehicle trajectory within the route boundaries and without increasing the risk of collision.*

***NOTE 7** The route selected should be appropriate for the vehicle, ADS and safety operator capabilities, i.e. the route should be wide enough to ensure foreseeable safety operator corrective action can be safely achieved in the available space.*

5.8 Safe operation and control

The safety case shall identify:

a) how the automated vehicle is monitored;

b) the minimal risk condition for the automated vehicle;

c) how control of the automated vehicle is maintained; and

d) how the safety operator is alerted that action is required.

The safety case shall provide evidence to demonstrate that the safety driver or remote operator has an appropriate level of control to ensure the minimal risk condition can always be achieved within appropriate timescales to avoid an incident.

Safety operator training and competency testing shall be detailed within the safety case.

If a safety driver is used, the safety case shall include:

1) how the effectiveness of a safety driver is maintained, e.g. managing complacency, distraction, or fatigue;

2) evidence to demonstrate that the safety driver has sufficient time to effectively diagnose and safely respond to anomalies; and

3) methods of monitoring safety driver performance during operation.

If the automated vehicle is monitored remotely, the safety case shall demonstrate that the system is able to deliver at least the same level of safety, situational awareness, control and response times as an alert and competent safety driver manually driving the same vehicle within the same ODD.

***NOTE** The same level of safety could mean that the vehicle can reliably navigate within the boundaries of the defined ODD and revert to the minimal risk condition without intervention, or that the remote operator can resume control of the vehicle in line with a safety driver's expected performance from the driver's seat.*

The safety case shall specify:

i) how the automated vehicle is monitored by the remote safety operator;

ii) how effectiveness of the remote operator is maintained;

iii) the ODD of the remote operation;

iv) the monitoring and maintenance requirements;

v) what the system is dependent on to operate safely (e.g. fully operating network communications);

vi) how safety is maintained if a fault or failure occurs (e.g. network communications or safety operator);

vii) how the system dynamically identifies and achieves a minimal risk condition within appropriate timescales to achieve an acceptable level of risk; and

viii) what control measures are employed to ensure reliable, safe and secure remote operation, including the integrity, latency and availability of communications.

5.9 Security

A security assessment shall be conducted to assess the security of the vehicle throughout the lifecycle of the trial or testing.

The assessment shall include cyber, physical and personnel security and shall include the systems (including the host company internal systems), vehicle, communications, control, monitoring and remote systems.

The assessment shall demonstrate that the risks posed to all affected parties, as a result of a threat to the safety of the system, are reduced ALARP through the implementation of demonstrably effective controls.

NOTE 1 *The hierarchy of options in the Health and Safety Executive's (HSE) Reducing risks, protecting people: HSE's decision-making process [15] should be taken into account when selecting risk control measures.*

NOTE 2 *For prototype vehicles, some cybersecurity risks can be effectively managed through the implementation of operational controls, e.g. a safety operator with emergency override.*

The safety case shall include an overview of how security has been tested with regards to safety functionality. The safety case shall demonstrate that the integrity of data and communication is preserved for the entire duration of the trial or testing period, even in the case of an incident.

NOTE 3 *Attention is drawn to the following guidance and standards that might be useful when undertaking the assessment: ISA/IEC 62443 (all parts), PAS 1885, and PAS 11281.*

5.10 Assurance of system safety

An overview of system safety assessments conducted shall be included in the safety case to provide assurance that the system is safe for the defined operating environment.

The system safety assessments shall be proportionate to the level of risk posed and shall include functional safety, SOTIF and security assessments. The overview shall include:

a) assessment details, including who performed the assessments, who had overall responsibility, their competency and their independence from any trial participants;

b) high-level objectives, including the identification of potential hazards resulting from system failure and safety goals to be used as targets for ensuring safety; and

c) assurance that the system being tested can always be overridden and returned to the minimal risk condition in the event of incidents or failures;

NOTE 1 *This could include a Design Failure Mode and Effect Analysis (DFMEA) to show adequate engineering effort has gone into ensuring the vehicle can always be made safe in the event of various system failures*

d) a safety assessment process, including an overview of how the safety assessment was conducted and what relevant standard(s) the safety assessments follow; and

e) details of the functional safety goals that result from the hazard analysis.

NOTE 2 *Depending on the complexity of the trial, it might be appropriate to incorporate functional safety requirements and technical safety requirements into the design of the system to ensure safety.*

If vehicle functionality relies on data provided by other vehicles or infrastructure (V2X), a mechanism to verify and validate the input and output data shall be identified and included in the safety case with reliable supporting evidence.

NOTE 3 *Attention is drawn to the following guidance and standards that might be useful when undertaking the assessment: PAS 1880, PD ISO/PAS 21448, and BS ISO 26262 (all parts).*

5.11 Safety testing and acceptance process

When testing in a public domain, the safety case shall include an overview of the previous system safety testing conducted and acceptance processes. The safety case shall include or make reference to specific tests conducted, test objectives and acceptance criteria.

NOTE 1 *Details of safety tests are not necessarily expected for controlled environments as prior test data might not be available, or it might be justified that presenting prior data is not essential to demonstrate safety.*

The safety case shall include the following information about pre-trial safety tests:

a) where the testing was performed and the features of the facility;

NOTE 2 *This might include whether testing was on a controlled test track or within the public domain, as well as the geographical location.*

b) the type of testing conducted, e.g. modelling and simulation;
c) what was tested (for example sensors, software, hardware, safety operator operation and reaction) and what the criteria were for each test (i.e. acceptance testing, planned lane change);
d) the results of the safety tests; and
e) the trial release procedure or criteria.

Where software includes any aspect of ML or AI, additional detail shall be required as to how the software has been assured, especially looking at aspects of model assurance, traceability of decision and validation/confidence of training data. The safety case shall include an overview of tests conducted to demonstrate the reliability of decisions through ML or AI.

The safety case shall include information regarding the testing being conducted during the trial or testing period, including:

1) what is to be tested (i.e. sensors, software, hardware, safety operator operation and reaction, new routes or system functionality etc.) and what the criteria are for each test (i.e. acceptance testing, planned lane change etc.);
2) the test scenario for each test, including a numbered or bullet point list of the test procedure followed by the associated pass or fail criteria; and

   NOTE 3 *The design of the test scenario should include operational conditions (traffic flow, vehicle compositions, weather conditions etc.) and a full set of variables.*
3) how test results are fed back into the safety case and safety requirements/design implementation.

The safety case shall identify all technology that is critical to the safe, secure and effective completion of each test, and conduct a security risk assessment for each test, including the potential impact of security compromises on the test. The safety case shall outline how security risks identified during testing have been effectively managed.

5.12 Modelling and simulation

The safety case shall include information about modelling or simulation conducted prior to the trial to support the overall testing programme, including:

a) the type of model or simulation used;
b) the scope and ODD of the simulation;
c) details of any limitations of the simulator, including any constraints, assumptions or imperfections of the simulation environment;
d) evidence demonstrating validity and reliability of the test results;
e) the technology or scenario tested in the model or simulation, the test objective and test results;
f) details regarding how the results were used, including the reliance on the tests for safety assurance;
g) the design of each scenario, including operational conditions (for example, traffic flow, vehicle compositions, weather conditions) and the full set of variables within each scenario; and
h) a comparison of the simulation environment with the ODD, and the intended trial environment with the ODD, in order to identify any potential differences and determine whether the differences are acceptable in terms of risk posed.

5.13 Change control

The safety case shall remain a live document throughout the trial or testing period. Systems or operational changes that could impact safety shall be classified, managed and included in the safety case to ensure it remains up to date, and assesses and manages new or changed risks. An audit trail detailing changes and the classification of the change (based on the safety impact) shall be maintained and referenced in the safety case.

NOTE 1 *Changes might include, but are not limited to, vehicle systems, vehicle hardware, software updates, the ODD, HMI, high definition (HD) mapping, communications, trial design, test scenarios, number of vehicles, and route. Particular attention (assessment and validation) should be given to changes that could impact the safety operator hand over process.*

The safety case shall include:

a) the process for monitoring and capturing changes made;
b) the process of assessing the level of risk posed by the change to safety and security;
c) the process for documenting, classifying, and testing, as appropriate;
d) the process for validating system performance before continuing trials or testing in the public domain;

   NOTE 2 *It might be appropriate to get changes authorized by relevant stakeholders prior to continuing the trial or testing.*
e) how changes to the safety case are communicated and implemented; and
f) the method for monitoring the subsequent effects of any changes made.

5.14 Stakeholder consultation and engagement

The safety case shall include a comprehensive list of stakeholders and detail relevant communication and consultation with the identified organizations.

NOTE 1 *Stakeholder consultation might not be required for testing on test tracks.*

NOTE 2 *Key stakeholders might be required to review and accept the safety case prior to the trial or testing. Stakeholders might include insurers, highway authorities, road operators, landowners, leaseholders or members of the community.*

NOTE 3 *Information in the safety case might include the:*

a) specific groups or areas within an organization that have been consulted;

b) type of consultation and reason for consultation;

c) main area(s) of engagement and the outcomes, including any requests or permissions granted; and

d) dates of meetings and specific agenda items discussed.

The safety case shall include details of any public education and awareness campaign that might have been launched regarding the trial that could foreseeably influence, or has been launched to influence, the safety of the trial, including the reason for education and awareness, an overview of the methodology used and any relevant safety feedback received.

NOTE 4 *The safety case should cross reference any advisory board and panel or safety review group(s) that have been established and consulted as part of a trial. Optionally, details may be reproduced such as:*

a) the purpose of the panel, its areas of input and key objectives that the board or panel were set up to achieve;

b) the organizations, groups or person(s) who were consulted as part of the panel; and

c) dates of meetings and specific agenda items discussed.

Contact details for the trialling organization and stakeholders consulted shall be included in the safety case.

Approvals and permissions shall be detailed in the safety case, including permissions from landowners, local authorities or licensing agencies to use a route, change the route use or infrastructure, operate the vehicle, or operate a service. Evidence of permissions and agreements shall be included in the safety case.

The trialling organization shall be responsible for conducting an ethics impact assessment prior to trials or testing in the public domain. Public trials shall obtain approval from an ethics committee (arranged by the trialling organization) prior to any testing that could impact on a member of the public or participant, whether these people are directly or indirectly affected. The ethics approval process shall be proportionate to the potential impact. Process outcomes shall be included in the safety case and shall detail how approval was attained.

If trials or testing is intended for public domains, trialling organizations shall develop and publish a publicly available and accessible version of the safety case.

NOTE 5 *Public references to the trial should state how the publicly available safety case can be accessed.*

NOTE 6 *There is no expectation that sensitive information should be included in this, and it is therefore permissible to restrict it to a high-level summary, provided that readers are able to follow the overall methodology used to ensure operational safety.*

5.15 Insurance

The safety case shall include details of who is insuring the trial, vehicles and safety operators and any specific equipment being tested. Insurance certification shall be included in the safety case.

5.16 Monitoring, reporting and continuous improvement

The monitoring being conducted during the trial shall be included in the safety case. The safety case shall include:

a) the person(s)/role responsible for data capture processes;

b) what safety data is being collected, how (for example, via dashcams, sensors, cameras or surveys) and the frequency of collection;

c) how sensors, redundancy and failure modes are monitored;

d) how safety case assumptions are monitored;

e) how dynamic hazards are monitored, e.g. weather/environment;

f) how the data is being downloaded, stored and analysed (during and after the trial or testing);

g) the security of data collection, transfer and storage;

h) who has access to the data during the project and how security is managed;

i) any parameters (i.e. start, end, sources) of any logging/monitoring to be stored/saved. This shall also include assurance that data has not been tampered with;

j) the procedure for analysis and reporting of issues that affect trial safety and continuation; and

k) the name of a nominated person who is responsible for ensuring compliance with the safety case and to act as a single point of contact for any concerns or questions related to the safety case.

NOTE 1 *The data gathered should reflect safety case requirements, required evidence to support risk decisions, assumptions made and current good practice. Attention is drawn to the General Data Protection Regulation (GDPR) [7], including data anonymity, and the DfT's safety requirements for automated vehicle trials and testing, including its latest Code of practice [1].*

The process for incident and near miss reporting and analysis shall be included in the safety case. Information shall include:

1) how incidents are identified and reported;

2) how incidents and near misses are categorized, for example, emergency, non-emergency, near miss, breakdown, or undesired event;

3) how automatic disengagement for respective automated systems is captured and analysed;

4) the person(s) responsible for escalating incidents (part of the emergency response plan);

5) the data being captured for the purpose of investigation;

   NOTE 2 *Data should be preserved and made available to emergency services in an intelligible format following an incident, if requested.*

   NOTE 3 *The data being captured should be sufficient to determine the root causes of an incident and should reflect current good practice.*

6) the person(s) responsible for reviewing recorded incidents or near misses; and

7) the abort criteria, including what level or type of incident would result in an abort scenario and stop further trials until a safety review has been completed.

The safety case shall include the process for learning lessons throughout the trial and ensuring the safety case is reviewed, updated and communicated to reflect learning. The lessons learnt shall be documented and used to validate and review risk decisions and the safety case shall include an audit trail of this process.

NOTE 4 *Lessons learnt might include evidence from simulator studies, track testing, data analysis or incident reports.*

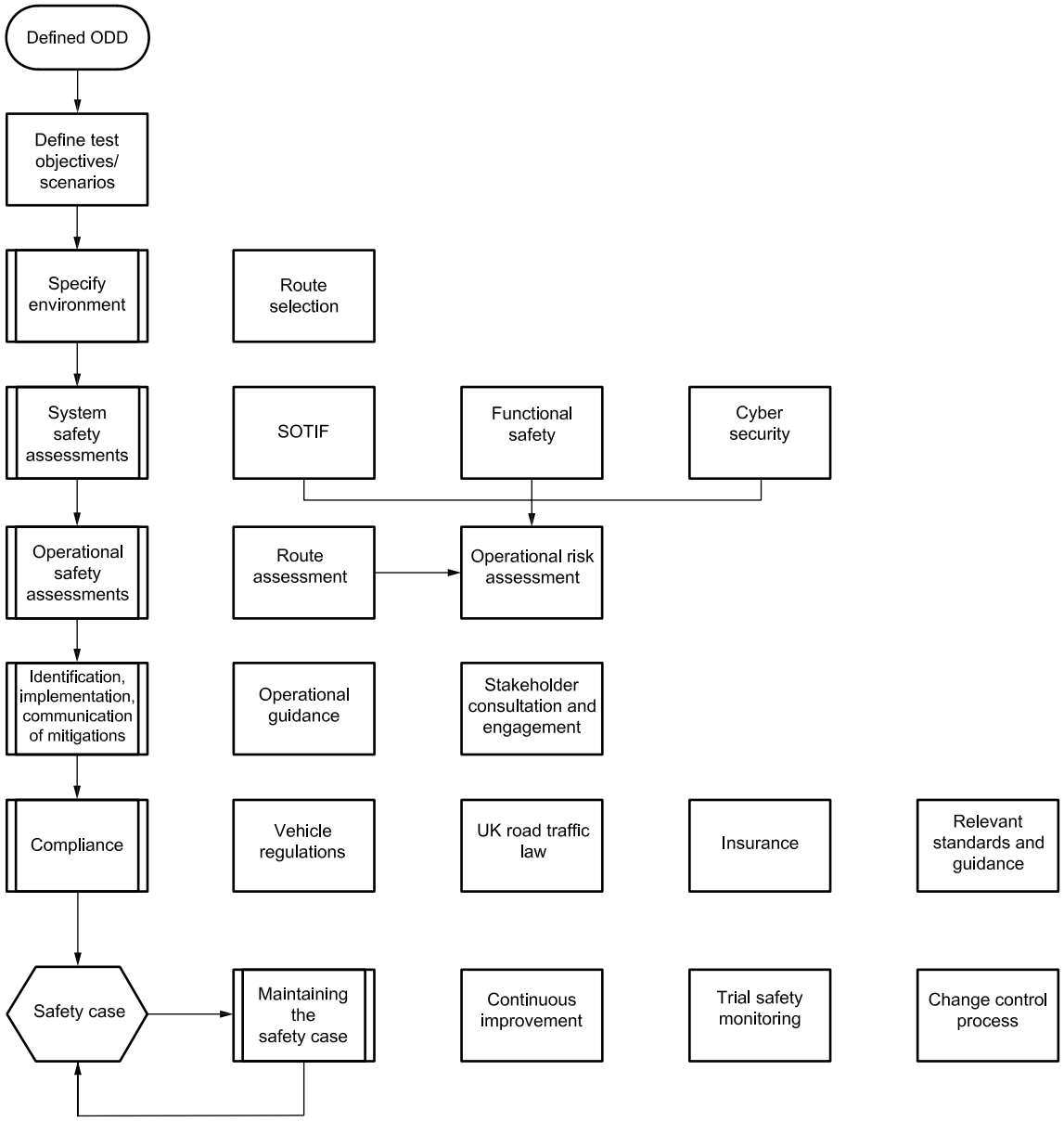
NOTE 5 *Non-compliance with the safety case should be monitored, recorded and included in lessons learnt and the continuous improvement process.*

The safety case shall remain a live, version-controlled document throughout the trial and shall be updated as lessons are learnt and evidence gathered. An edits log shall be included in the safety case to ensure an audit trail of changes is maintained.

Annex A (informative)
Safety case development and case studies

The flow chart below (see Figure A.1) provides a high-level overview of safety case development. Case studies are also provided as examples of how different elements of the safety case framework have been applied to automated vehicle trials and testing. These case studies highlight lessons learnt that should be taken into account when implementing the safety case framework.

Figure A.1 – Overview of safety case development



***NOTE** The left-hand column shows the high-level tasks in safety case development. Subsequent columns on the right are subsets of those tasks, for example, the route assessment and operational risk assessment are part of the operational safety assessments task.*

Case study 1: Route assessments

This project was initiated to develop and demonstrate the technology, safety validation methods, insurance and service models for delivering an automated personal mobility solution, targeted at replacing the urban commuter car. The project delivery team consisted of a consortium of companies including specialist technology suppliers, innovators in the transport sector and an insurance provider.

To meet the necessary legal requirements to conduct testing on UK public roads and secure insurance for the trial, a robust safety case was created and through this, a process for assessing and classifying routes was developed. To be able to comprehensively identify the key hazards and potential hazardous scenarios, the safety team initially established the boundaries of the ODD and test scenario. The following route analysis tasks were identified:

a) walk-through analysis of the route;
b) accident data analysis;
c) use of geographical information system tools; and
d) consultation with stakeholders and experts.

This led on to the identification of mitigations and the development of implementation plans and training materials, as well as the creation of the route safety assessment document which supported the project safety case.

Case study 2: Operational risk assessment and operational guidance

General

This project was initiated to evaluate the benefits and issues of an innovative transportation concept using a real-world trial on the strategic road network.

Operational risk assessment

The operational risk assessment was conducted in accordance with *GG104: Requirements for safety risk assessment* [3] and in consultation with Highways England. The purpose of this risk assessment was to identify the potential impact of the trial on other road users, road workers and third parties. The following safety risk assessment steps were followed to systematically identify and assess the resulting risks:

a) hazard identification;
b) hazard analysis;
c) analysis of safety risk;
d) evaluation of safety risk; and
e) safety risk mitigations.

Hazards were identified by a variety of methods for the trial, including through a review of relevant literature and available evidence, assessment of the existing hazard logs, strategic road network analysis, risk workshops and hazards identified by stakeholders.

Hazard analysis was conducted using a top down approach, which started from a list of top-level events that the trial should aim to avoid. A systematic method was used to consider and assess all reasonably practicable causes and possible consequences.

The safety risk was then analysed and evaluated using a 5×5 matrix in accordance with BS ISO 31000. This assigned a colour-coded risk rating to each undesired event with an associated action plan. Where the initial findings identified high risk situations, additional analysis was conducted to more accurately assess these risks and propose additional mitigations.

Case study 2: Operational risk assessment and operational guidance *continued*

Mitigations were identified and implemented based on the findings of the risk assessment and included operational decisions, safe working practices and procedures, driver training and vehicle design and selection. Through the application of these mitigations, the risks posed by the trial were considered to be both ALARP and Globally At Least Equivalent (GALE) to the existing risk posed on the strategic road network.

Operational guidance and training

During the operational risk assessments for the trial, key operational risks were identified relating to aspects such as incidents and near misses, worker safety and welfare, and legal compliance. To help mitigate these risks, a suite of operational documents was developed for both drivers and trial managers participating in the trial. This guidance defined roles and responsibilities and provided clear instructions on how the trials would operate, what tasks were required to be completed and key rules to be followed. The operational guidance was also fully incorporated into the driver and trial manager training packages to ensure that everyone was familiar with the procedures prior to the trials commencing.

Operational guidance was developed for the following areas:

1) security, vehicle checks and maintenance;
2) safe loading of vehicles;
3) monitoring and reporting, e.g. workload monitoring, fatigue and distraction monitoring, incidents and undesired events, driver briefs and debriefs;
4) trial policies, e.g. conduct, legal compliance, mobile phone policy;
5) health and wellbeing, e.g. fatigue, distraction, drivers' hours and breaks, drugs and alcohol policy;
6) training and selection of safety drivers, managers and support team members;
7) data handling;
8) eligibility and abort criteria; and
9) emergency response plan.

The incident and undesired event reporting process created for the trials formed one of the key feedback methods to ensure continuous improvement throughout the trial. An incident and undesired event operational procedure was developed, outlining the key incident categories and the actions to be taken by drivers and trial managers.

An incident and investigation team was established to review details of incidents and undesired events using the event forms, driver debrief notes, event marker information and video footage to establish root cause and necessary remedial actions. The findings, including communication of any changes required and decisions made regarding subsequent trials, were then shared with the trial team and relevant stakeholders.

Case study 3: Emergency response plan

This project was a multi-million-pound research and development project designed to understand and overcome the technical, legal and societal challenges of implementing connected and automated vehicles in an urban environment. The programme consisted of three automated vehicle trials: a passenger vehicle service using low speed automated driving systems; a vehicle parking service; and a local delivery service, which were carried out in urban locations.

The route comprised a shared-use public footpath which consisted of both cyclist and pedestrian lanes. Pod vehicles were used for the trial which were developed and adapted to enable automation of the vehicle in public spaces without dependence on a dedicated trackway. These two elements, an off-road route and the use of non-typical vehicles, meant that the development of the emergency response plan required a unique, measured approach together with detailed initial, and on-going, engagement with the landowner and emergency services.

Key areas of particular scrutiny included, but were not limited to:

a) consideration of a range of potential incident/emergency scenarios given the route, likely route users, and vehicle type used;
b) emergency service access to/from the route;
c) passenger extrication in the event of an emergency;
d) disabling vehicle systems or features, particularly during automated mode; and
e) appropriate response to address vehicle-based issues or emergencies, e.g. battery fire.

Each of the trials had specific emergency response plans to ensure that a clear and effective response was implemented to manage any incident, and to ensure the safety of all affected parties. All emergency response plans were developed in consultation with local emergency services, stakeholders and members of the consortium, in order to confirm that they were suitable for a range of potential types of emergency and that they aligned with local emergency responders' existing response procedures. In particular, the plan for the passenger vehicle service trial incorporated evacuation and welfare plans to assist with scene management and to provide support to any affected parties. All members of the trials team were trained to implement the plan if required.

A crisis communications plan was developed in parallel with the emergency response plans to facilitate effective communications during an incident, and to ensure the safety of the project team, members of the public and the successful operation of the project. This involved applying measures to enable an integrated and coordinated approach between the project partners, to ensure that clear and consistent messaging was conveyed to the right people at the right time and to provide reassurance to the project stakeholders. A steering committee was created so that in the event of an incident, relevant parties could be brought together and any reputational threats minimized.

Case study 4: Stakeholder engagement, continuous improvement and change control

General

This was a long-term project that centred around a test bed for connected and automated vehicles, using public and private roads. The project team consisted of parties from across the industry including local authorities, technology innovators and research establishments.

Stakeholder engagement

Given the proximity of the test beds to a densely populated area, local citizens, businesses and interest groups were engaged on the project to establish that they were comfortable with the tests. The project team developed a stakeholder engagement plan which focused on how to communicate and engage with these groups to gain an insight into how they would be affected by the testing and to address any concerns and associated infrastructure.

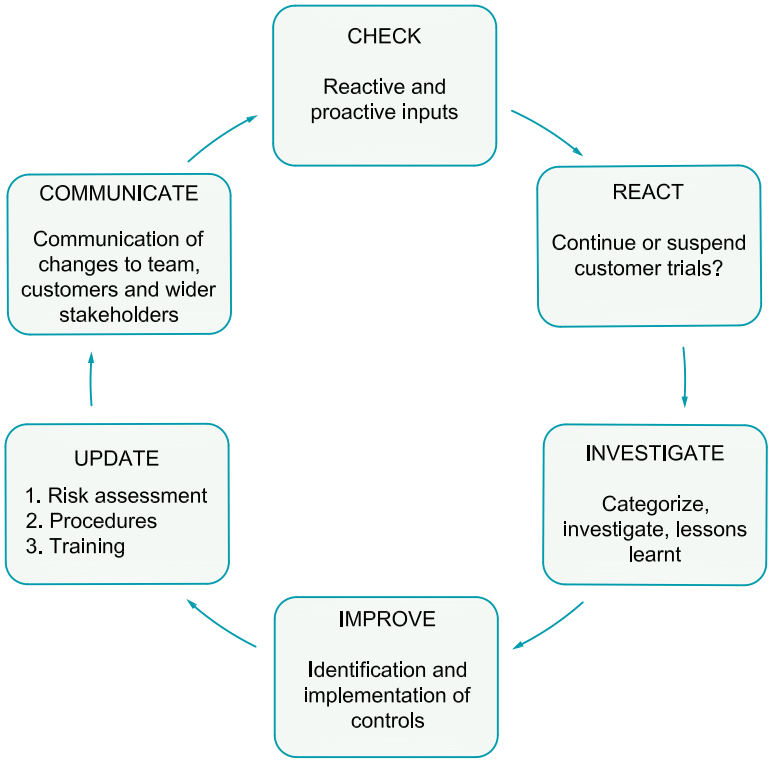
In addition, a customer stakeholder engagement checklist was developed to provide customers with detailed guidance on which stakeholders they should engage with and the key stakeholder engagement activities they were advised to undertake before, during and after their trials at the test bed. This checklist ensured all customers met the minimum engagement recommendations outlined in the DfT's *Code of practice* [1]. It also encouraged customers to share key information regarding the trials with the wider public.

Continuous improvement

Due to the long-term nature of this project, a robust and continuous improvement process was in place to ensure that the test bed facility remained at the leading edge of innovation and continued to be fit for purpose in the future.

The high-level continuous improvement process consisted of the stages outlined in Figure A.2.

Figure A.2 – Continuous improvement process



This project actively sought input into the continuous review process by undertaking routine benchmarking activities with other test beds and by carrying out periodic reviews of the test bed facilities, e.g. monitoring equipment, route assessments and facility checks. The project also made reactive changes in response to events such as updates to guidance or legislation, new customer requirements, incidents and undesired events, feedback from stakeholders or customers and route changes, e.g. road works, diversions, collision, debris or vegetation.

Case study 4: Stakeholder engagement, continuous improvement and change control *continued*

Change control

Rigorous change control management was used in this project for managing changes to both hardware and software throughout the test period to ensure the safety of the trials. A process was developed to minimize any potential risk that might arise as a result of changes being made to a system without first giving careful consideration to all the possible consequences of those changes. This process aimed to ensure:

a) the potential consequence of any change was carefully analysed and evaluated prior to implementing a change;

b) changes were evaluated against the stakeholder objectives;

c) the observed behaviour of the system was as expected based on the build state of the system; and

d) compliance with necessary standards, such as the DfT's *Code of practic*e [1].

NOTE *Attention is also drawn to data protection laws.*

To ensure the customer understood the process requirements, a guidance document was generated outlining the change control process and requirements for running the trial.

Case study 5: Integrating system safety and operational safety

This is based on a real project and summarizes an approach to a safety case for trialling an AV operating on public roads with a safety driver present and able to take manual control at any time. The ODD was defined early in the project, which was important due to the influence it had upon subsequent documents that made up the safety case, yet was adapted as the project progressed, e.g. due to becoming aware of unforeseen route hazards or to compensate for limitations identified in the ADS.

System safety and operational safety were intrinsically linked. System safety analyses (in line with functional safety standards) resulted in operational safety requirements to mitigate against identified system limitations (e.g. for the safety driver to take over in a particular hazardous location or scenario type), and operational safety analyses led to system requirements (e.g. for the robustness of the emergency cut-out switch, the clarity of feedback to the driver, or ensuring hardware had not been attached in hazardous locations where it could, for example, cause injury or obstruct the inflation of an airbag).

Operational and system safety requirements were captured, maintained and tracked, with operational safety requirements incorporated into a "method statement" describing roles, responsibilities and safe systems of work for each trial. This proved an effective communication channel to ensure that the operational safety requirements were visible to all personnel to whom they were applicable.

Testing was carried out to ensure that the safety driver was able to successfully intervene to prevent an incident in all foreseeable scenarios. The safety driver, however, cannot be held responsible if there are permutations where it is uncertain that they would be able to intervene sufficiently quickly to prevent an incident. The ability of the safety driver to intervene was gauged through fault injection testing within a controlled environment, with the safety driver responses informing decisions as to what scenarios are acceptable. For example, if the AV is to operate on narrow roads where the available gap on each side is less than the maximum lateral deviation seen in the fault injection testing, it would be necessary for the safety driver to take manual control pre-emptively if there are any hazards present immediately beside the lane.

Fault injection testing also ensures that all safety drivers have practical experience. They should be highly qualified in general test driving and competent to control the specific AV in the specific scenarios they could be exposed to, necessitating extensive knowledge of the ODD and the AV characteristics. Throughout the AV trials, a safety driver was able to take control of the vehicle at any time and was accompanied by an engineer in the passenger seat.

Case study 6: Route assessment, testing and continuous improvement

The purpose of this project was to build passenger, regulatory and market confidence in autonomous pods as a practical, safe and affordable way to travel. The proposed ODD for the trials provided the initial scope to base the data collection and investigation phase around but was primarily focused around a short loop of segregated pathways with mixed, non-motorized traffic.

The data collection and exploratory phase initially consisted of a review of the immediate facilities and pathways around the route to gain an understanding of the basic interactions that could be expected when the Vehicle Under Test (VUT) started using the site.

The initial stage involved desk-based examinations of the site and proposed routes, which were supported by site walk throughs and static site surveys. These physical investigations aided the understanding of the range, frequency and complexity of expected interactions. Data was recorded from these surveys in video form alongside physical measurements, where needed, and plots of park user movements. The investigations were strengthened by external inputs such as specific insurance or park operator requirements. The outcome of this process led to the first draft of the hazard identification and test plan documentation, which were to be included in the safety case.

The vehicle was tested based on the hazard and interaction parameters identified through surveys and stakeholder engagement. All planned pre-trial testing fitted into four general groups:

a) VUT running straight with a static hazard;
b) VUT running straight with a moving hazard;
c) VUT turning with a static hazard; and
d) VUT turning with a moving hazard.

These simplified groups covered all types of scenario that the VUT could be expected to encounter using its capabilities. The VUT as presented for testing was identical to the vehicle destined for public trials.

The results of the testing initiated a process of evaluation to identify whether the sensing and decision making of the VUT were enough to address all the expected risks within the test plan documentation and ultimately to be ready for full public use. Where issues were identified (typically only a small subset of the testing plan), software and sensor revisions were made to the VUT to enable it to meet the requirements. Once revisions were made, the retesting of previously successful tests was carried out alongside previously unsuccessful tests to ensure that any changes did not adversely affect previously good performance.

The safety performance of the VUT during pre-trial testing was carefully balanced against the usability of the VUT at the specific ODD. An acceptable level of safety performance was balanced with an acceptable level of service performance.

During public testing the vehicle was continually evaluated to determine whether the performance in the real world reflected that seen during testing, and also to verify whether the interactions and hazards identified during the initial stage were valid.

Annex B (informative) Operational guidance

Operational guidance documents outline safe working practices that should be followed to assure safety and security throughout the lifecycle of the trial. They outline the safe working practices identified as mitigations in the risk assessment and ensure all people involved in the trial or testing know how to, and are able to, conduct tasks safely and securely and ensure a consistent approach is adopted.

Operational guidance documents should reflect findings from the risk assessment and might include:

a) method statements detailing the testing methods being used, roles and responsibilities of the trials team, key risks and mitigations and reference to appropriate operational guidance documents;

b) a process for halting testing by any stakeholder in the event of a safety concern;

c) operation of the vehicle and ADS, visual indicators, engaging and disengaging ADS, how the automated function can be overridden, failure warnings, advanced warnings and corrective actions;

d) route safety requirements and necessary restrictions to ensure safety, including disengagement zones, where required, and known or foreseeable hazards on the route;

e) safety operator policies;

NOTE 1 *Safety operator policies might cover conduct, mobile phone use and work hours.*

f) vehicle storage and security;

g) vehicle maintenance, inspection and cleaning, including fault logging and required actions;

h) vehicle charging and fuelling;

i) vehicle recovery;

j) data storage, security and access;

k) safety operator selection, training and on-going development;

NOTE 2 *Safety operator selection and training might cover a number of elements including:*

a) a defined operator role profile to ensure the suitability of those recruited to participate and the criteria on which selection is based;

b) an operator training programme, which might include the objectives of the training, how the training is delivered (classroom, simulator or test track), logging and auditing of training and final sign-off/certification of competency. Training includes safety drivers gaining experience of performing overrides upon the specific vehicle(s) used in the trial within a controlled environment, before being responsible for the vehicle in less controlled environments, which could be achieved through fault injection testing if suitable experience is not gained through system errors in the course of normal testing; and

c) the monitoring plan for operators and training updates to be provided in response to any incidents, hazards or lessons learnt during the trials.

l) safety operator fatigue and workload. This guidance should detail how safety operator workload is managed and what procedures or tools are in place. The guidance should also detail:

1) trial-specific risks and mitigations, for example, scenarios which could place greater strain on the operator or potential disengagement from safety tasks, or tasks that expect unreasonable safety operator performance;

2) duration of safety operator monitoring;

3) safety operator behaviour and alertness monitoring; and

4) undesired safety operator behaviour, warnings provided by monitoring systems and corrective actions;

m) eligibility and abort criteria, which should cover:

1) specific routes or areas eligible for testing;

2) places of relative safety, if no additional risk is incurred from moving the vehicle;

3) route and environmental considerations, e.g. road works, parked vehicles, vegetation, standing water;

4) abort procedures and responsibilities; and

5) circumstances that might require testing to be aborted, e.g. weather conditions, environment, road incident and safety operator fatigue;

n) incident and near miss reporting process and escalation, safety and security monitoring and feedback of lessons learnt;

o) data set recording plan following an incident, intervention or test abort;

p) a log of training provided to relevant persons;

q) a crisis communications plan providing details of the communication plan in case of a crisis event. The crisis communication plan should include:

   1) main point of contact and person(s) responsible for media statements;

   2) instructions that no other person(s) other than designated person(s) should make public statements; and

   3) details and contact details of those responsible for media statements;

r) a log of stakeholder engagement; and

s) a vehicle recovery plan for the recovery of vehicles in case of breakdown or aborted trials. This should detail any variation to typical breakdown procedures by the company responsible for recovery.

Bibliography

Standards publications

For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS ISO 26262 (all parts), *Road vehicles – Functional safety*[5)]

BS ISO 31000, *Risk management – Guidelines*

ISA/IEC 62443 (all parts), *Security for industrial automation and control systems*

ISO/PAS 21448, *Road vehicles – Safety of the intended functionality*

PAS 1880, *Guidelines for developing and assessing control systems for automated vehicles*[6)]

PAS 1882, *Data collection and management for automated vehicle trials – Specification*[7)]

PAS 1883, *Operational design domain (ODD) taxonomy for an automated driving system (ADS) – Specification*[8)]

PAS 1885, *The fundamental principles of automotive cybersecurity – Specification*

PAS 11281, *Connected automotive ecosystems. Impact of security on safety – Code of practice*

PD ISO/PAS 21448, *Road vehicles – Safety of the intended functionality*

Other publications

[1] DEPARTMENT FOR TRANSPORT. *Code of practice: Automated vehicle trialling.* London: DfT, 2019.

[2] TRANSPORT FOR LONDON. *Connected and autonomous vehicles: Guidance for London trials*. London: TfL, 2019.

[3] HIGHWAYS ENGLAND. *GG104: Requirements for safety risk assessment.* London: Highways England, 2018.

[4] GREAT BRITAIN. The Road Traffic Regulation Act 1984. London: The Stationery Office.

[5] GREAT BRITAIN. The Road Vehicles (Construction and Use) Regulations 1986. London: The Stationery Office.

[6] GREAT BRITAIN. The Road Traffic Act 1988. London: The Stationery Office.

[7] EUROPEAN COMMUNITIES. Regulation (EU) 2016/679. Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (Data Protection Directive). Luxembourg: Office for Official Publications of the European Communities, 2018.

[8] GREAT BRITAIN. The Road Vehicles (Approval) Regulations 2009. London: The Stationery Office.

[9] GREAT BRITAIN. The Data Protection Act 2018. London: The Stationery Office.

[10] GREAT BRITAIN. The Automated and Electric Vehicles Act 2018. London: The Stationery Office.

[11] DEPARTMENT FOR TRANSPORT. *Highway Code. London: DfT, 2015.*

[12] LAW COMMISSION. *Automated vehicles.* [Due for publication in 2021, information on current status of project available at: https://www.lawcom.gov.uk/project/automated-vehicles/]

[13] DEPARTMENT FOR TRANSPORT. *The key principles of vehicle cybersecurity for connected and automated vehicles.* London: DfT, 2017.

[14] DEPARTMENT FOR TRANSPORT. *Prototype road vehicles – Construction requirements.* London: DfT, 2015.

[15] HEALTH AND SAFETY EXECUTIVE. *Reducing risks, protecting people: HSE's decision-making process.* London: HSE, 2001.

Further reading

HIGHWAYS ENGLAND. *Design manual for roads and bridges.* London: Highways England, 2019.

[5)] This PAS also gives a reference to BS ISO 26262-1:2018, *Road vehicles – Functional safety – Part 1: Vocabulary.*
[6)] In preparation.
[7)] In preparation.
[8)] In preparation.

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards-based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email cservices@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Relations
Tel: +44 345 086 9001
Email: cservices@bsigroup.com

Subscription Support
Tel: +44 345 086 9001
Email: subscription.support@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI, 389 Chiswick High Road
London W4 4AL
United Kingdom
www.bsigroup.com

9 780539 040586