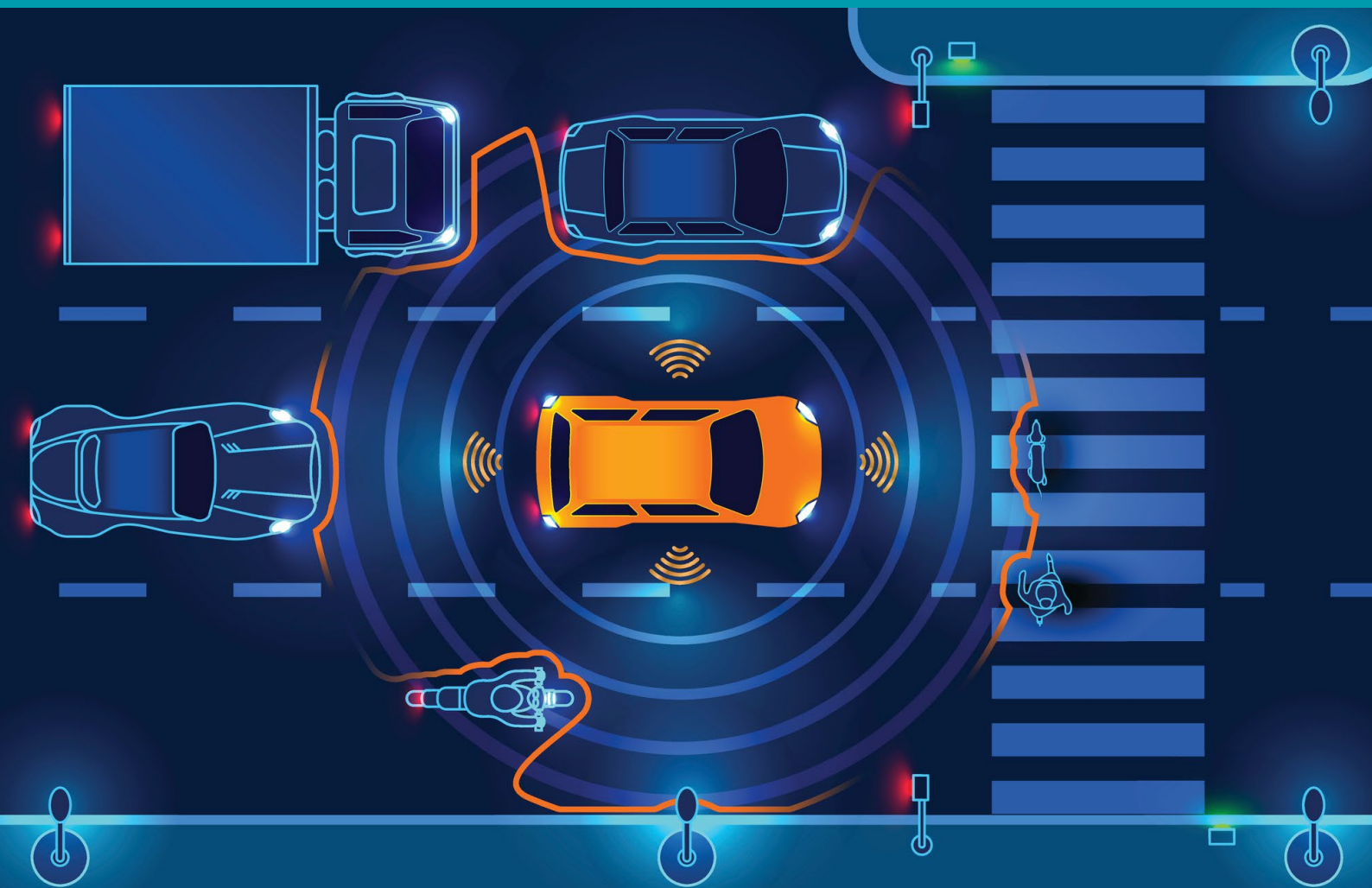


PAS 1881:2020

Assuring the safety of automated vehicle trials and testing – Specification



Centre for Connected
& Autonomous Vehicles



bsi
Documents
Document Sharing Hub

Publishing and copyright information

The BSI copyright notice displayed in this document indicates when the document was last issued.

© The British Standards Institution 2020.

Published by BSI Standards Limited 2020.

ISBN 978 0 539 04058 6

ICS 43.020

No copying without BSI permission except as permitted by copyright law.

Publication history

First published February 2020

Contents

Foreword	ii
Introduction	iv
1 Scope	1
2 Normative references	2
3 Terms and definitions	2
4 Safety case requirements and ownership	5
5 Contents of the safety case	6
Annexes	
Annex A (informative) Safety case development and case studies	15
Annex B (informative) Operational guidance	22
Bibliography	24
List of figures	
Figure A.1 – Overview of safety case development	15
Figure A.2 – Continuous improvement process	19

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.

The British Standards Institution retains ownership and copyright of this PAS. BSI Standards Limited as the publisher of the PAS reserves the right to withdraw or amend this PAS on receipt of authoritative advice that it is appropriate to do so. This PAS shall be reviewed at intervals not exceeding two years, and any amendments arising from the review shall be published as an amended PAS and publicized in Update Standards.

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 1880¹⁾, PAS 1882²⁾, PAS 1883³⁾ 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.

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].

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.

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.