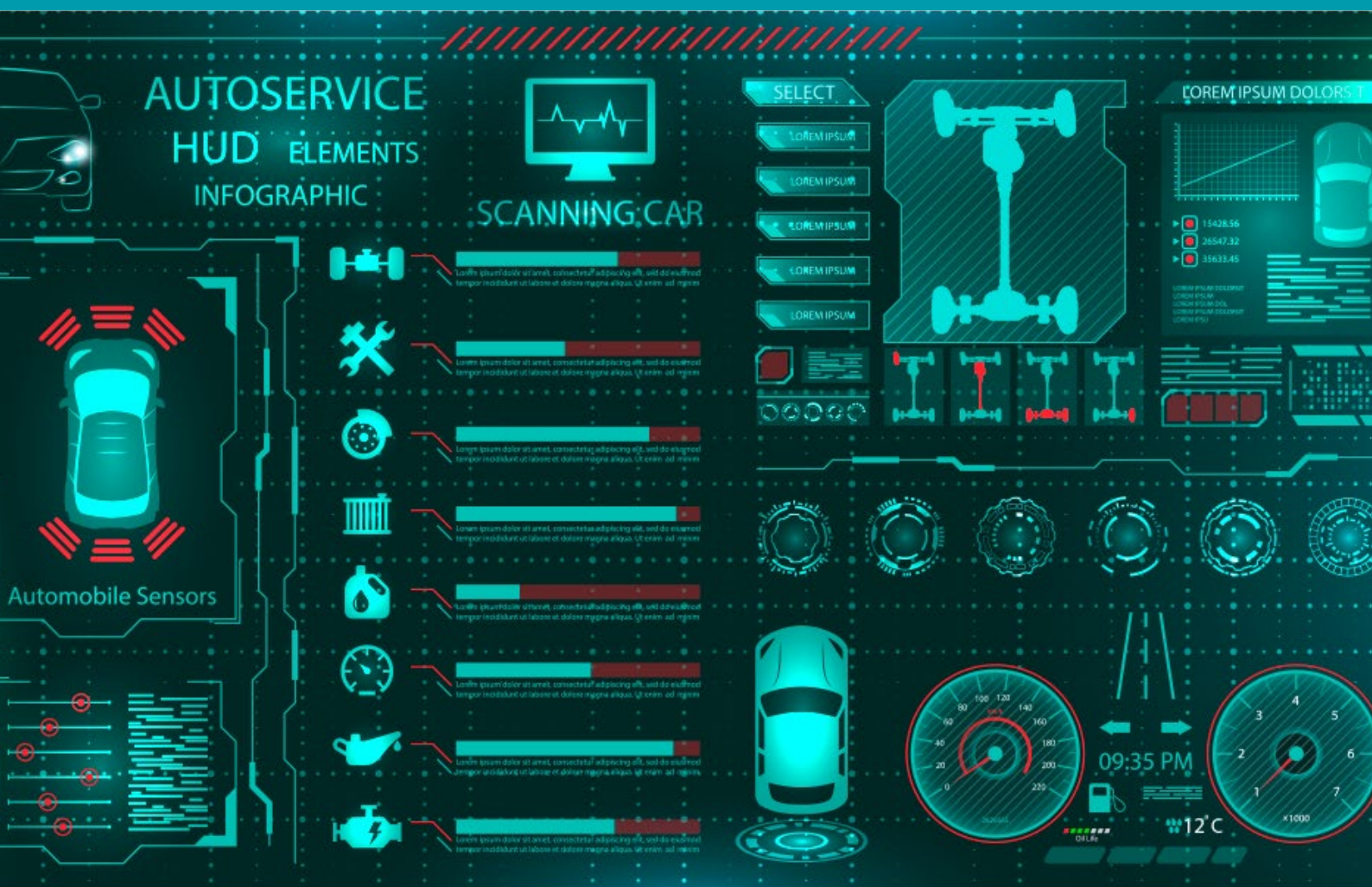


PAS 1880:2020

Guidelines for developing and assessing control systems for automated vehicles



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 04031 9

ICS 43.020

Publication history

First published April 2020

Contents

Foreword	ii
Introduction	iv
1 Scope	1
2 Normative references	2
3 Terms and definitions	3
4 Objectives	6
5 Mission	7
6 Operational design domain (ODD)	8
7 Designing the AV sensor operation (AVSO)	9
8 Designing the AV planning operation (AVPO)	12
9 Designing the AV control operation (AVCO)	14
10 Designing the AV monitoring operation (AVMO)	16
11 Safety, security and effectiveness	18
Annexes	
Annex A (informative) – Sources of evidence	19
Annex B (informative) – Designing an automated vehicle unit (AVU)	21
Annex C (informative) – Artificial intelligence (AI)	24
Annex D (informative) – Autonomous machines	25
Annex E (informative) – Related safety standards	27
Bibliography	29
List of figures	
Figure 1 – A schematic representation of a possible architecture for an AV control system that is compatible with the guidelines presented in this PAS	iv
Figure B.1 – A schematic representation of an automated road vehicle showing a possible AVU configuration	21
Figure B.2 – A schematic representation of an automated pod vehicle showing a possible AVU configuration	22
Figure B.3 – A schematic representation of a Category 3 -designated architecture	23

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 30 April 2020.

Acknowledgements

Acknowledgement is given to Michael J. Pont of SafeTTY Systems Ltd, as the technical author, and the following organizations that were involved in the development of this PAS as members of the steering group:

- Adelard
- Centre for Connected and Autonomous Vehicles (CCAV)
- Centre for the Protection of National Infrastructure (CPNI)
- Connected Places Catapult
- HORIBA MIRA
- Infineon Technologies AG
- J.C. Bamford Excavators Ltd (JCB)
- Nova Modus Limited
- SafeTTY Systems Ltd
- Tata Motors Limited
- Test and Verification Solutions Limited (T&VS)
- University of York
- WMG, University of Warwick

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

Recognition is made to the Automotive Electronics Systems Innovation Network (AESIN) who supported the pre-development phase of this PAS in a series of industry workshop with BSI and members of the CAV community.

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 will be reviewed at intervals not exceeding two years, and any amendments arising from the review will be published as an amended PAS and publicized in *Update Standards*.

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

The PAS process enables a guide 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.

Relationship with other publications

PAS 1880 has been developed as part of a wider programme sponsored by CCAV in conjunction with the Department for Transport (DfT), Innovate UK and Zenic 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 1880 is intended to be read in conjunction with:

- guidance on system safety, including PAS 1881, PAS 1882¹⁾, PAS 1883²⁾; BS ISO 26262, IEC 61508 and BS EN ISO 13849-1;
- existing legislation for UK vehicles and roads.

¹⁾ In preparation.

²⁾ In preparation.

Use of this document

As guidelines, this PAS takes the form of guidance and recommendations. It should not be quoted as if it were a specification or a code of practice and claims of compliance cannot be made to it. It has been assumed in the preparation of this PAS that the execution of its provisions will be entrusted to appropriately qualified and experienced people, for whose use it has been produced.

Presentational conventions

The guidance in this PAS is presented in roman (i.e. upright) type. Any recommendations are expressed in sentences in which the principal auxiliary verb is “should”.

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

Compliance with a PAS cannot confer immunity from legal obligations.

0 Introduction

Work on the document that eventually became this PAS began in 2017 when a lack of accepted common standards and working practices was identified as a significant impediment to UK progress in the area of automated vehicles (AVs) [1].

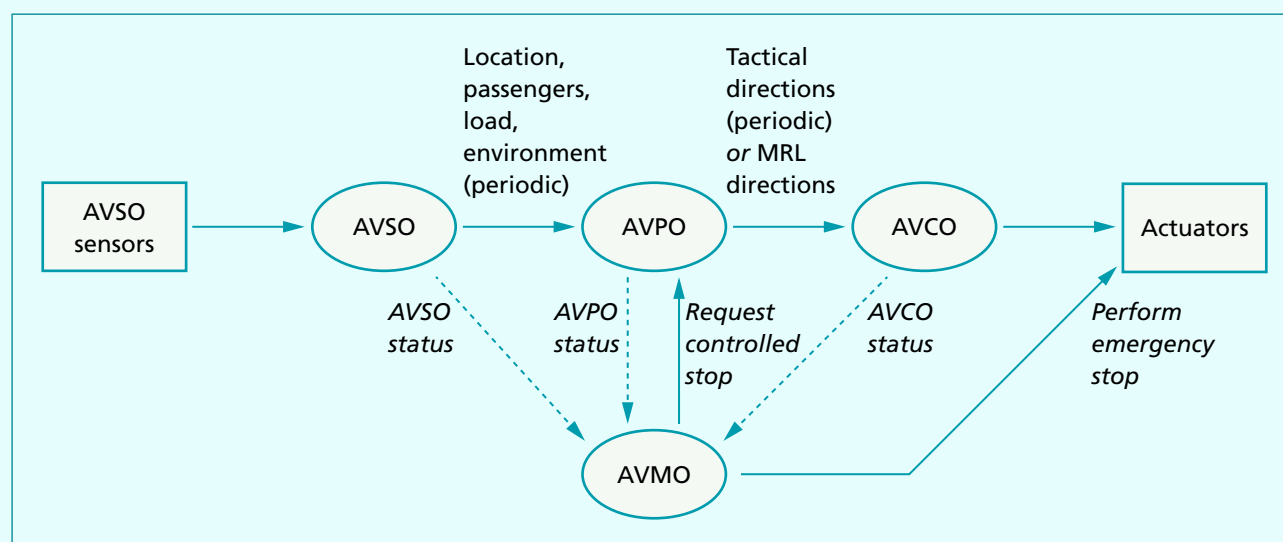
In order to begin to address this challenge, this PAS is intended to provide an initial set of guidelines for developers of control systems for AVs.

One possible architecture for such a control system is given in Figure 1: the different elements in this diagram and their interconnections are explored in the body of this PAS.

This document (along with PAS 1881, PAS 1882³⁾ and PAS 1883⁴⁾) is intended to support developers of AVs during vehicle trials in which there is a human safety operator who is able to take control of the vehicle (when they are required to do so).

This PAS is also intended to be of value to developers of production vehicles (in which no safety operator will be involved).

Figure 1 – A schematic representation of a possible architecture for an AV control system that is compatible with the guidelines presented in this PAS



³⁾ In preparation.

⁴⁾ In preparation.

1 Scope

This PAS provides a set of initial guidelines for developers of control systems for the safe, secure and effective deployment of automated vehicles (AVs).

This PAS covers AVs that are capable of moving passengers and/or goods, without human intervention, within defined operational design domains.

This PAS does not cover general techniques for achieving functional safety in AVs; instead, reference is made to related standards for information about such matters.

***NOTE** For further information on general techniques for achieving functional safety in AVs see BS ISO 26262.*

This PAS does not cover off-road machinery in any detail. However, some of the existing standards in this sector are considered in Annex D.

This PAS is intended for manufacturers and developers of AVs, their sub-assemblies and components.

This PAS is also of interest to organizations involved in trials or other test/validation activities on AVs.

2 Normative references

There are no normative references in this document.

3 Terms, definitions and abbreviations

3.1 Terms and definitions

3.1.1 artificial intelligence

theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception and route planning

NOTE Artificial intelligence is assumed to be an umbrella term that incorporates fields such as machine learning, expert systems, neural networks and deep learning.

3.1.2 automated pod vehicle (APV)

automated vehicle that does not operate primarily on public roads

NOTE An automated pod vehicle is distinguished by the fact that:

- a) it does not operate primarily on public roads (but might have to interact with such roads at times, e.g. by crossing a public road);
- b) it is likely to be used in environments – such as within an airport terminal or shopping mall – in which it might have to interact with (for example) pedestrians, cyclists, scooter users, wheelchair users, animals and other APVs;
- c) it has a maximum operating speed that is low enough to ensure that a controlled stop can be performed at any time (in response to a detected system failure) without significant risk of injury to any vehicle occupants or those in the vicinity of the vehicle; and
- d) during automated vehicle trials, it can be supported by a remote safety driver and/or a safety driver.

3.1.3 automated road vehicle (ARV)

automated vehicle that operates primarily on public roads

NOTE An automated road vehicle is distinguished by the fact that:

- a) it operates primarily on public roads;
- b) it is likely to interact with other road users, including AVs and HDVs, and possibly cyclists and pedestrians;
- c) compared with an APV, an ARV can have complex MRL/MRC requirements (because simply bringing the vehicle to a controlled stop is unlikely to be an appropriate response to a system failure in all circumstances); and

- d) during automated vehicle trials, it can be supported by a safety driver.

3.1.4 automated vehicle (AV)

vehicle fitted with an automated driving system that uses both hardware and software to perform dynamic driving tasks associated with moving the vehicle within one or more defined operational design domains

NOTE An AV can be viewed as a machine. Annex C provides an overview of standards for machines (with a focus on autonomous machines).

3.1.5 automated vehicle control operation (AVCO)

function that controls the movement of an automated vehicle

NOTE 1 Typically (but not necessarily) implemented by means of a computer program running on an automated vehicle unit.

NOTE 2 This can include communicating status and intended movement to other road users (e.g. by means of indicators).

3.1.6 automated vehicle monitoring operation (AVMO)

function that monitors the operation of an automated vehicle

NOTE Typically (but not necessarily) implemented by means of a computer program running on an automated vehicle unit.

3.1.7 automated vehicle planning operation (AVPO)

function that performs route-planning operations for an automated vehicle

NOTE Typically (but not necessarily) implemented by means of a computer program running on an automated vehicle unit.

3.1.8 automated vehicle sensing operation (AVSO)

function that performs sensing (or perception) operations for an automated vehicle

NOTE Typically (but not necessarily) implemented by means of a computer program running on an automated vehicle unit.

3.1.9 automated vehicle trial (AVT)

trial of an AV in which a safety operator has responsibility for the safe operation of the vehicle

3.1.10 automated vehicle unit (AVU)

form of embedded system for use in an automated vehicle that includes one or more microcontrollers plus related software (or “firmware”)

3.1.11 controlled stop

process for bringing an automated vehicle to a halt as quickly as possible while minimizing the risk to the vehicle occupants and other road users

NOTE A controlled stop involves reducing the vehicle speed to zero over an interval (e.g. 5 s) that varies depending on the nature of the vehicle and the situation. During a controlled stop, the risk to (and caused by) any vehicle loads should be considered: for example, possible spillage of hazardous chemicals.

3.1.12 emergency stop

process for bringing an automated vehicle to a halt as quickly as possible

NOTE It is assumed that an emergency stop should be performed when it is not possible to perform a controlled stop (e.g. because of some form of system failure).

3.1.13 human-driven vehicle (HDV)

A vehicle that is operated under the primary control of a human driver

3.1.14 minimal risk condition (MRC)

configuration in which an AV is intended to be placed in circumstances where it cannot complete the journey successfully, after it has (where possible) reached a minimal risk location

NOTE 1 Prior to entering an MRC, the AV is expected to be stationary, where possible. Entering the MRC then involves performing any actions that are needed (and possible), with a focus on reducing the risks to the vehicle passengers, other people in the vicinity of the vehicle, and animals in or in the vicinity of the vehicle. This might be as simple as turning on “hazard lights” and/or sending out some form of warning message and/or opening contactors in an electric vehicle to reduce the risk that passengers come into contact with a high-voltage supply.

NOTE 2 In some AVs, it might be appropriate to contact the relevant authorities (e.g. police) when an MRC has been entered.

3.1.15 minimal risk location (MRL)

location that an automated vehicle attempts to move to from its current position in circumstances where it cannot complete the journey successfully

NOTE 1 The primary goal in moving to the MRL is to reduce the risk of injury or death to passengers in the AV or people or animals in the vicinity of the AV as far as practically possible.

NOTE 2 The choice of appropriate MRL might depend on the location in the ODD and the AV’s current status. For example, the ARV might need (if possible) to move to the side of the road, move away from a road junction or change lanes to enter the MRL. To move from the current vehicle location to the MRL, the AV follows the MRM directions. The vehicle then performs a controlled stop (where possible). Once it reaches the MRL, the vehicle then moves into a minimal risk condition.

3.1.16 minimal risk manoeuvre (MRM) directions

sequence of tactical directions that detail how an AV can move from its current location to the required MRL

3.1.17 operational design domain (ODD)

specific conditions or operating environment under which a given automated vehicle is designed to operate

3.1.18 remote safety driver (RSD)

form of safety operator who performs remote monitoring of an AV

NOTE The RSD performs the following activities during automated vehicle trials of an AV:

- a) monitoring the vehicle behaviour; and
- b) forcing the vehicle to perform a controlled stop (or emergency stop) in situations where it is determined that the vehicle is behaving in a manner which might lead to death or injury to the passengers in the AV, or to others in the vicinity of the vehicle (e.g. other road users, including pedestrians and cyclists), or to animals in the vehicle or in the vicinity of the vehicle, or to the road infrastructure.

The RSD is not located in the AV: instead, they have a remote link to the vehicle (at least a high-speed visual link) and an ability to trigger a controlled stop. If the link between the RSD and the AV is broken, this also triggers an immediate controlled stop.

An RSD can be responsible for the operation of an APV but not for the operation of an ARV.

3.1.19 safety driver (SD)

form of safety operator who is based in an AV

NOTE The safety driver (SD) performs the following activities during automated vehicle trials of an AV:

- a) monitors the vehicle behaviour; and
- b) takes control of the vehicle in situations where it is determined that the vehicle is behaving in a manner which might lead to death or injury to passengers in the vehicle, the SD, to others in the vicinity of the vehicle (e.g. pedestrians, cyclists, other road users), or to animals in the vehicle or in the vicinity of the vehicle

The SD can be located in an ARV or an APV.

3.1.20 safety operator (SO)

person who is trained to supervise an AV during an automated vehicle trial and intervene at any time as required

NOTE The SO can be a safety driver or a remote safety driver.

3.1.21 tactical direction

low-level specification of the required next step in the journey of an automated vehicle

NOTE 1 Examples include:

- “Slow down by 1 mph and turn steering to the right by 1 degree”;
- “Continue at the same speed and direction”;
- In a given design, it might be decided that tactical directions are to be provided every 10 ms, so that at the maximum vehicle speed of 110 km/h, the AV will move approximately 300 mm between such directions.

NOTE 2 Tactical directions are provided to the AVCO by the AVPO. Under normal circumstances, the AV will progress towards the location identified in the strategic directions (e.g. “Drive to Pitlochry, Scotland”), by means of a series of operational directions (e.g. “Take the next left turn into Birstall Avenue”) that will in turn be broken down into a series of tactical directions.

3.2 Abbreviations

AI	artificial intelligence
AOZ	autonomous operating zone
APV	automated pod vehicle
ARV	automated road vehicle
ASAMS	autonomous and semi-autonomous machine system
AV	automated vehicle
AVCO	automated vehicle control operation
AVMO	automated vehicle monitoring operation
AVPO	automated vehicle planning operation
AVSO	automated vehicle sensing operation
AVT	automated vehicle trial
AVU	automated vehicle unit
CAN	controller area network (serial communication bus)
DL	deep learning
FMEA	failure modes and effects analysis
FTA	fault tree analysis
HDV	human-driven vehicle
HIL	hardware in the loop
MCU	microcontroller (unit)
ML	machine learning
MRC	minimal risk condition
MRL	minimal risk location
MRM	minimal risk manoeuvre
ODD	operational design domain
ODS	object detection system
PES	programmable electronic system
PTI	proof test interval
RSD	remote safety driver
SD	safety driver
SIL	software in the loop
SMS	site management system
SO	safety operator
TMR	triple modular redundancy
VA	visibility aid

4 Objectives

COMMENTARY ON CLAUSE 4

This Clause summarizes the set of core objectives that developers of AVs are to meet in order to comply with this PAS.

The remaining Clauses in this document provide further guidance on how to meet these objectives.

Annex A provides examples of techniques that can be used to provide evidence of compliance with the objectives presented in this Clause.

The focus of this PAS is on the high-level design of control systems for AVs. Some suggestions about possible low-level design/implementation techniques are provided in Annex B.

4.1 Mission

The mission of the AV is defined (see Clause 5).

4.2 Operational design domain (ODD)

The AV's ODD (or ODDs) is:

- a) defined; and
- b) encompasses all aspects of the mission (see Clause 6).

4.3 Sensing operations

It is demonstrated that, throughout the mission, the AV:

- a) is able to determine that it is operating in compliance with its ODDs; and
- b) is able to provide the data required by the AV planning operations (see Clause 7).

4.4 Planning operations

It is demonstrated that the AV can perform all planning activities that are necessary in order to complete its mission (see Clause 8).

4.5 Control operations

It is demonstrated that the AV:

- a) is able to control its own movements during normal operation in order to complete its mission; and
- b) is able to take appropriate action if it determines that it is not operating correctly (see Clause 9).

4.6 Monitoring operations

It is demonstrated that, throughout the mission, the AV is able to monitor its own operation (see Clause 10).

4.7 Safe, secure and effective

The AV is demonstrated to be capable of operating safely, securely and effectively at all times (see Clause 11).