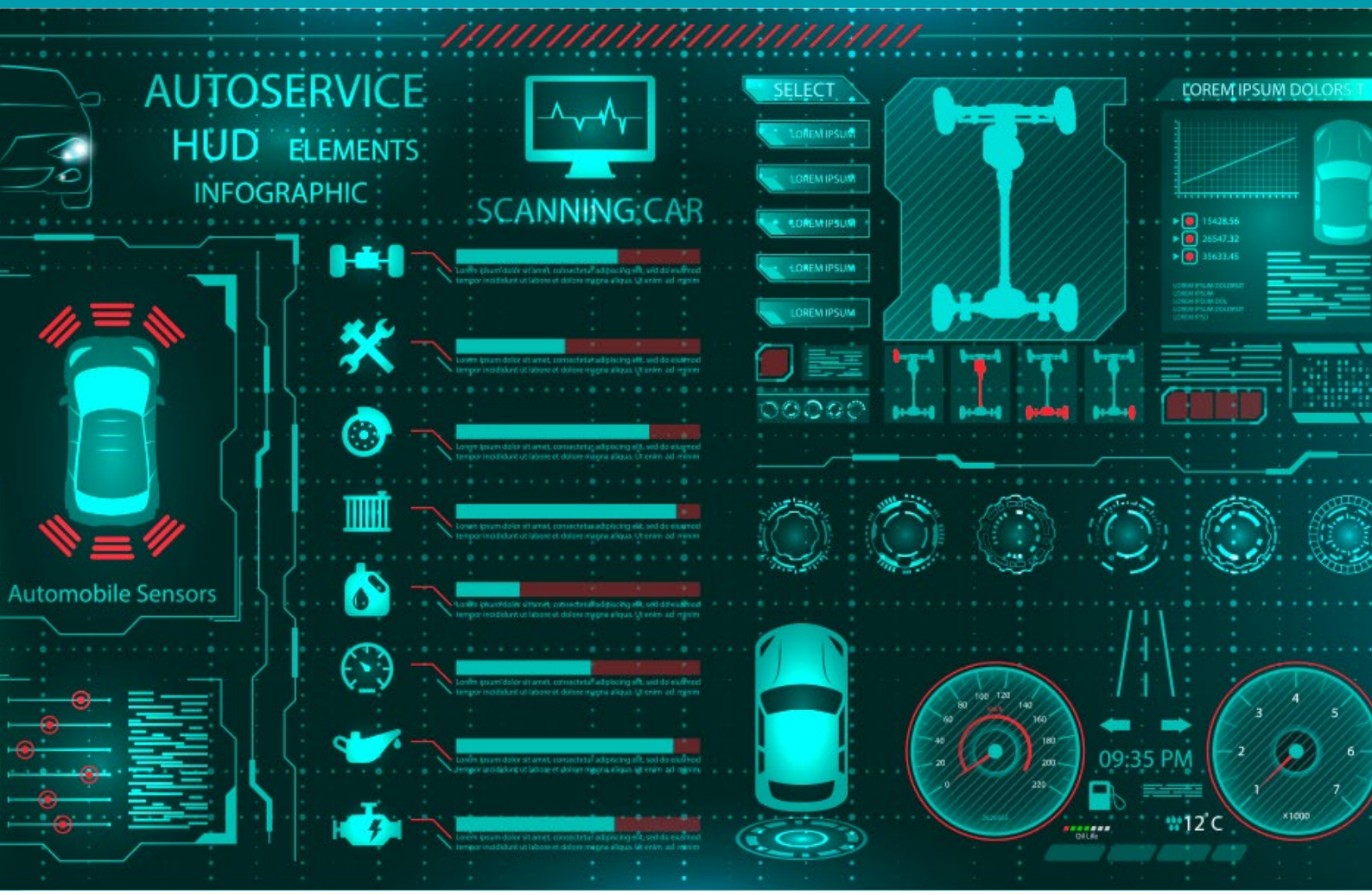
PAS 1880:2020

Guidelines for developing and assessing control systems for automated vehicles



Centre for Connected & Autonomous Vehicles

bsi.

Publishing and copyright information

Published by BSI Standards Limited 2020.

ISBN 978 0 539 04031 9

ICS 43.020

Publication history

First published April 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 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 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 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 1880 is intended to be read in conjunction with:

- guidance on system safety, including PAS 1881, PAS 1882[1)], PAS 1883[2)]; 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].

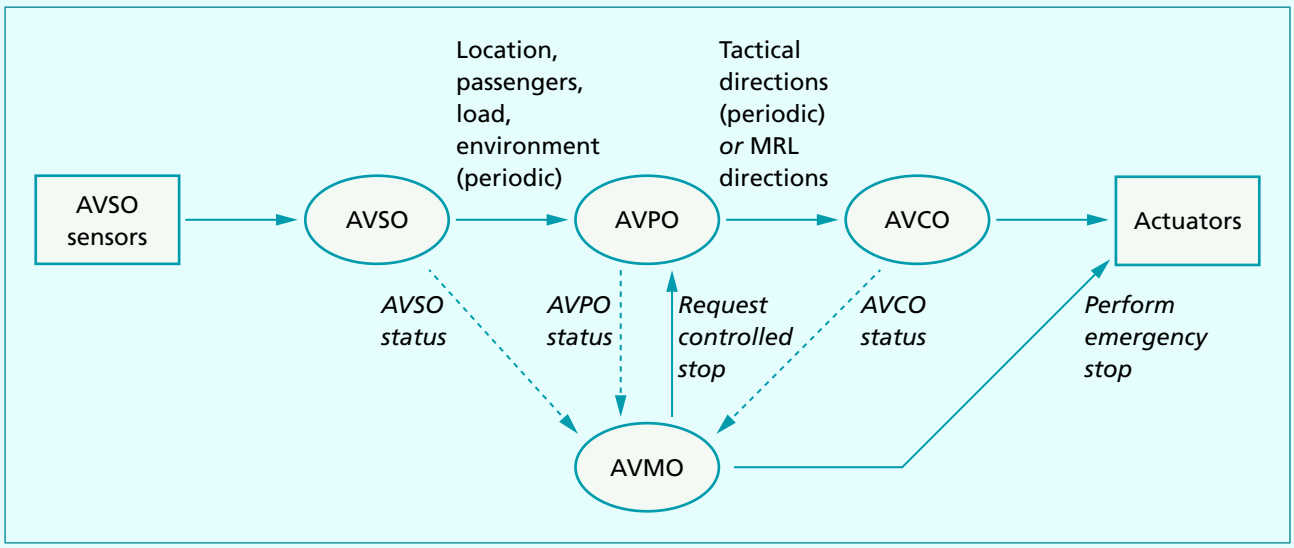
In order to begin to address this challenge, this PAS is intended to provide an initial set of guidelines for developers of control systems for AVs.

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 1882[3)] and PAS 1883[4)]) 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**).

5 Mission

5.1 Objective

The mission of the AV should be defined (**4.1**).

5.2 Defining the mission

The following are some example questions a development team should consider when drawing up a specification for the mission:

a) Will the AV carry people?

b) If people are to be carried, what will be the maximum number of passengers?

c) Will the AV carry goods?

d) If goods are to be carried, what are the characteristics of these goods be (e.g. weight, volume, hazardous materials, liquid, solid)?

e) Will the route followed by the AV be essentially pre-defined (for example, something like a bus) or dynamic (for example, something like a taxi)?

f) What are the configuration limits of the AV? For example, can the AV tow a trailer or caravan?

5.3 Evidence that objectives have been met

The development team should provide evidence that they meet the objective that is laid out in **5.1**.

NOTE *Annex A provides examples of techniques that can be used to provide this evidence.*

6 Operational design domain (ODD)

6.1 Objective

The AV's operational design domain (ODD) (or ODDs) should:

a) be defined; and

b) encompass all aspects of the mission (**4.2**).

6.2 Defining the ODDs

NOTE *PAS 1883*[5] *is intended to cover ODD specification.*

The following are some example questions a development team should consider when drawing up a specification for the ODD:

a) What are the geographical limits to the ODD? For example, can the AV operate:
   1) within 10 miles of location A?
   2) within the area marked on Map B on the indicated roads only?
   3) within Terminal C of Airport D?

b) What are the interaction limits of the ODD? For example, can the AV interact with cyclists/pedestrians/other AVs/HDVs? Are there limits to the density of traffic or pedestrians (for example) that the AV can handle?

c) What kind of road features are included in the ODD? For example, what type of road junction? What about road works? What about localized speed restrictions?

d) What are the incline limits to the ODD? For example, can the vehicle:
   1) climb very steep hills? How steep?
   2) descend steep hills? How steep?

e) What are the ambient temperature limits to the ODD?

f) What are the humidity limits to the ODD?

g) What are the weather limits to the ODD? Can the AV handle rain/hail/ice/snow? At what level (e.g. heavy driving rain)? What about light levels? What about fog? What about low sun levels? What about thunderstorms?

h) What are the terrain limits to the ODD? For example, can the AV handle only smooth road surfaces?

i) Many existing road-based HDVs are essentially identical whether they are sold for use on desert roads or on snow. The driver is expected to adapt to the conditions (and perhaps, where necessary, make appropriate modifications to the vehicle, such as fitting winter tyres for a drive from England to Scotland in January). Does the ODD need to cover such scenarios? How many ODDs are there?

6.3 Transitioning into/out of/between ODDs

The focus in this PAS is on AVs (in which a human driver/safety operator will be involved only during trials).

If this PAS is employed in the development of a vehicle control system for which transitions into/out of/between ODDs have to be supported, then evidence that such manoeuvres can be carried out safely, securely and effectively should be provided.

In circumstances where such a transition is attempted and fails, then the AV should enter an MRC.

NOTE *For example:*

a) entering an ODD is likely to involve a complete handover from a safety operator or driver to the AVCO;

b) exiting an ODD is likely to involve a complete handover from the AVCO to a safety operator or driver; and

c) transitioning between ODDs is likely to involve both an ODD exit and an ODD entry [as given in items a) and b)], with supervision from a driver or safety operator.

6.4 Evidence that objectives have been met

The development team should provide evidence that they meet the objective that is laid out in **6.1**.

NOTE *Annex A provides examples of techniques that can be used to provide this evidence.*

[5] In preparation.

7 Designing the AV sensor operation (AVSO)

7.1 Objective

It should be 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 (**4.3**).

7.2 The AVSO

Meeting the objective provided in **7.1** should be (primarily) the responsibility of the AVSO.

NOTE *One possible architecture for an AV control system (showing the AVSO in context) is given in Figure 1.*

The AVSO should:

a) supply all sensor information required to support the planning operation of the AV to the AVPO (see Clause **8**); and

b) supply information about its own status to the AVMO.

7.3 Location

The sensor suite and related processing required to determine the location of the AV should be specified.

In some cases, a map reference might be appropriate, but the location information should be in a form (and with an accuracy) that is appropriate for the particular vehicle and given ODD.

7.4 Passengers

Where an AV is capable of transporting passengers, the sensor suite, and related processing, required to determine whether any passengers are currently in the vehicle should be specified.

NOTE 1 *This is necessary because the required behaviour in the event of a system failure is likely to be different in a vehicle that is carrying passengers to a vehicle that is empty.*

NOTE 2 *Variations in the number of passengers alters the weight of the vehicle and might therefore have an impact on control strategy that is followed; it might therefore be necessary to determine how many passengers are present in some AVs.*

NOTE 3 *In many AVs, the location of any passengers in the vehicle (e.g. are they in a seat) and the status of the passengers (e.g. are they wearing a seatbelt) might need to be determined.*

7.5 Loads

The sensor suite and related processing required to determine the nature and state of any load that is being carried by the vehicle should be specified.

NOTE *This is necessary because, for example:*

a) some loads might alter the height, width, length and/or weight of the vehicle: this could, in turn, have an impact (for example) on possible route options;

b) some loads might be potentially hazardous (e.g. flammable or corrosive liquids). This could have an impact on the required vehicle behaviour in the event of a crash;

c) it might be necessary for an AV to monitor the state of its load (such as the position of a stack of logs) in case material falls from the vehicle.

7.6 Environment – General

The sensor suite, and related processing required to identify the environment of the AV, should be specified.

As with the vehicle location, information about the environment should be in a form (and with an accuracy and timeliness) that is appropriate for the particular vehicle, the ODDs and the mission as it has been defined.

NOTE *For example:*

a) An ARV on a motorway might need to identify its location, the lane in which it is travelling, other vehicles in the vicinity, pedestrians and other animals on the road.

b) It might be necessary for an AV to recognize parts of the road infrastructure (such as traffic lights) and determine their state appropriately (for example, the traffic light is on red).

c) The temperature outside a terminal or airport might be much higher or lower than an APV was designed for. What happens if the vehicle is moved into this area? Is there a risk of dangerous failure? Even if the AV is intended to operate over a limited temperature range it might need to be able to identify temperatures over a much wider range.

7.7 Environment – People

The sensor suite, and related processing required to predict the possible actions of people in the vicinity of the AV, should be specified.

NOTE *For example:*

a) *An ARV might need to predict the possible actions of other road users correctly by "reading the road";*

b) *An ARV or APV might need to be able to determine that a pedestrian ahead is looking away or visually impaired and might, therefore, be unaware that the AV is approaching. It might be considered appropriate to slow down and/or sound a warning in these circumstances.*

c) *An ARV that is designed for use on motorways might not be expected to encounter bicycles. Suppose such a vehicle is activated in a city environment (perhaps outside a school). Is it clear that the vehicle can detect that it is outside its ODD? Does the AV need to have sensors that detect bicycles or people or other animals even if it is never expected to encounter them (so that it can determine that it is outside its ODD)? Are such "bicycle sensors", "people sensors" or "horse sensors" – for example – required in all designs?*

7.8 External communication

Where it is possible to obtain relevant information from outside the AV (for example, from the road infrastructure or from other vehicles) then this should be considered.

Particular consideration should be given to the security of the AV system in these circumstances.

NOTE *See PAS 11281 for information on security of the AV system.*

7.9 Other aspects of the ODD

In addition to issues considered explicitly in this clause, any other sensors and related processing required to determine whether the AV is operating in compliance with its ODD specification should be specified.

In determining whether the AV is operating in compliance with its ODD specification, the development team should consider (for example) the following questions:

a) What sensors are required to detect that the vehicle is operating in compliance with its ODD specification?

b) How reliable are the data upon which this assessment is based (can the sensor outputs be relied upon)?

c) What is the lifetime of the sensors (and is this compatible with the mission and other AV requirements)?

7.10 Other planning requirements

In addition to issues considered explicitly in this clause, any other sensors and related processing required to support the planning operations (Clause **8**) of the AV should be specified.

In doing so, the development team should consider the following questions:

a) What sensors are required to support the planning operations?

b) How reliable are the sensor outputs (can the sensor outputs be relied upon)?

c) Have issues of sensor drift, sensor degradation and intermittent sensor fault been considered and adequately addressed?

7.11 Covering the full ODD specifications

The development team should demonstrate that the operation of the sensor suites addressed in this clause remains valid across all of the ODD specifications.

NOTE *This means when the ARV is going through tunnels, operating in the dark, operating at high temperatures, operating in rain, operating in snow, etc.*

7.12 Detecting sensor failure

Safe operation of the AV (see the objective provided in **4.7**) relies upon rapid detection of sensor failure.

If the development team cannot be confident that sensor failure will be detected before erroneous data are sent from the AVSO to the AVPO, then use of sensor duplication and redundancy should be considered, with the goal (in this case) of increasing the likelihood that sensor failure is detected sufficiently quickly.

This might involve the use of homogeneous or heterogeneous sensor redundancy (and the choice between these two options should be supported by evidence).

7.13 Sensor fault tolerance

To ensure that the AV operates effectively (see **4.7**), additional sensor coverage should be considered, in order to reduce the possibility that degradation or loss of a single sensor would make it necessary to bring the vehicle to a stop.

NOTE 1 *Some form of sensor-fusion algorithm might be appropriate to support this goal, for example:*

a) Dempster-Shafer techniques might be considered [2].

b) Use of a form of machine-learning algorithm might be considered [3].

NOTE 2 *See Annex C for guidance on the use of artificial intelligence (AI) in AVs.*

7.14 Monitoring the AVSO

The AVSO should not provide sensor data to the AVPO in situations in which it cannot be confident that correct data will be provided.

To achieve this, the AVSO should perform self-monitoring activities, to determine whether it is operating correctly. The results of this monitoring activity should be reported to the AVMO.

If, as a result of such monitoring, it is determined that the AV cannot continue to operate safely or securely and it cannot recover from this situation in an appropriate time, then the vehicle should perform a controlled stop or emergency stop.

NOTE 1 *Annex D provides examples of monitoring techniques that have been used in autonomous machines.*

NOTE 2 *In some designs, it might be possible for the AVSO to generate both data and a confidence rating for these data. In the event that specific faults are identified in the AVSO, it might then still be possible to generate data but at a lower confidence level. Such "lower confidence" data might make it possible for the vehicle to come to a controlled stop (rather than having to force an immediate emergency stop).*

NOTE 3 *During trials (and in some cases with production vehicles), it might be appropriate to store data that are generated by the AVSO monitoring process for later analysis.*

7.15 Use of artificial intelligence (AI) in the AVSO

If AI is employed in the AVSO then evidence should be provided that this design decision is compliant with the objective presented in **4.7**.

NOTE *See Annex C for guidance on the use of AI in AVs.*

7.16 Evidence that objectives have been met

The development team should provide evidence that their AVSO design meets the objectives that are laid out in **7.1** and the related sub-objectives that are identified in **7.2** to **7.15**.

NOTE *Annex A provides examples of techniques that can be used to provide this evidence.*

8 Designing the AV planning operation (AVPO)

8.1 Objective

It should be demonstrated that the AV can perform all planning activities that are necessary in order to complete its mission (**4.4**).

8.2 The AVPO

Meeting the objective provided in **8.1** should be the responsibility of the AVPO.

NOTE *One possible architecture for an AV control system (showing the AVPO in context) is given in Figure 1.*

The AVPO should:

a) receive all sensor information required to support the planning operation of the AV from the AVSO (see Clause **7**);

b) supply information about the next required vehicle movement (in the form of tactical directions or MRM directions) to the AVCO (see Clause **9**);

c) comply with requests from the AVMO to perform a controlled stop (see Clause **10**); and

d) supply information about its own status to the AVMO.

8.3 Maps and related information

When the AV is operating normally, the AVPO is likely to be responsible for interpreting the readings from one or more vehicle "surrounding sensors" (e.g. Lidar units) and combining this with additional information such as "location sensors" (e.g. GPS units) to conduct plausibility checks and generate the tactical directions to be provided to the AVCO.

A suitable form of map (or maps) should be incorporated in the AVPO to assist with this process, if required.

Evidence should be provided to show that any maps used are compatible with the mission and the ODD specification, are current, and of the required accuracy.

Evidence should also be provided that appropriate processes are in place to deal with updates to any maps, and handle situations where the AV determines that the current map is (apparently) incorrect.

8.4 Providing pre-determined route-planning information

The AVPO might be required to provide a pre-determined sequence of tactical directions to the AVCO in situations where a pre-determined route is required.

For example, there might be some form of database that records the movements needed, in terms of tactical directions, to move from Terminal 1 to Terminal 5 in an airport. Limited deviations from this pre-defined route are to be expected: for example, if luggage is left on the pre-defined route, the APV might need to navigate around this obstacle.

NOTE *To assist in this process, the following example questions an organization might consider are:*

a) How are the required route data stored (what form does the database take)?

b) How are the route data to be updated?

c) How much deviation from the pre-defined route is allowed (and how will this be handled)?

The development team should provide evidence that the AVPO will be able to meet such requirements.

8.5 Providing dynamic route-planning information

The AVPO might be required to provide a highly-dynamic sequence of tactical directions to the AVCO in situations where the operating environment changes quickly.

For example, the AVPO might be required to operate rather like a "satellite navigation" unit in an HDV.

The development team should provide evidence that the AVPO will be able to meet any dynamic route-planning requirements.

8.6 Providing MRM directions

The AVPO should provide MRM directions to the AVCO (in place of tactical directions) when notified by the AVMO that it is to do so.

***NOTE** For ARVs, one possible way of achieving this might be to store MRL data alongside mapping information for as much of the ODD as possible. For example, on motorways the maps could store information about "hard shoulder" availability from which MRM directions can be calculated. In areas of the ODD where such MRM directions cannot be provided, it might be considered appropriate to have the vehicle operate at low-speed (so that a controlled stop can be carried out safely in the event of a system failure).*

For an APV (by definition), a controlled stop can be performed at any time a fault is detected. The MRM directions can, therefore, be summarized as "perform a controlled stop in the current location" (at all times) for such vehicles, if a better alternative cannot be identified for a given AV in a particular situation.

8.7 Monitoring the AVPO

The AVPO should not provide either tactical directions or MRM directions to the AVCO in situations in which it cannot be confident that correct data will be provided.

To achieve this, the AVPO should perform self-monitoring activities, to determine whether it is operating correctly. The results of this monitoring activity should be reported to the AVMO.

If, as a result of such monitoring, it is determined that the AV cannot continue to operate safely or securely and it cannot recover from this situation in an appropriate time, then the vehicle should perform a controlled stop or emergency stop.

***NOTE 1** Annex D provides examples of monitoring techniques that have been used in autonomous machines.*

***NOTE 2** In some designs, it might be possible for the AVPO to generate both data and a confidence rating for these data. In the event that specific faults are identified in the AVPO, it might then still be possible to generate data but at a lower confidence level. Such "lower confidence" data might make it possible for the vehicle to come to a controlled stop (rather than having to force an immediate emergency stop).*

***NOTE 3** During trials (and in some cases with production vehicles), it might be appropriate to store data that are generated by the AVPO monitoring process for later analysis.*

8.8 Use of AI in the AVPO

If AI is employed in the AVPO then evidence should be provided that this design decision is compliant with the objective presented in **4.7**.

***NOTE** See Annex C for guidance on the use of AI in AVs.*

8.9 Evidence that objectives have been met

The development team should provide evidence that their AVPO design meets the objectives that are provided in **8.1** and the related sub-objectives that are provided in **8.2** to **8.8**.

***NOTE** Annex A provides examples of techniques that can be used to provide this evidence.*

9 Designing the AV control operation (AVCO)

9.1 Objective

It should be 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 (**4.5**).

9.2 The AVCO

Meeting the objective provided in **9.1** should be primarily the responsibility of the AVCO, supported by the AVPO and AVMO.

NOTE *One possible architecture for an AV control system (showing the AVCO in context) is given in Figure 1.*

The AVCO should:

a) receive information about the next required vehicle movement (in the form of tactical directions or MRM directions) from the AVPO (see Clause **8**); and

b) supply information about its own status to the AVMO.

9.3 Movement control

The AVCO should control the vehicle actuators (e.g. electric drive motor, brake unit, steering unit) in order to implement the tactical directions or MRM directions it receives and/or to perform a controlled stop.

In order to demonstrate that the AV can operate safely, securely and effectively (**4.7**) the development team should be confident that the AV will be able to move to an MRL even in the presence of identified faults in the vehicle (including faults in the actuator system itself).

The development team should document how the AVCO meets these recommendations.

9.4 Interactions and feedback

The development team should provide evidence that the need for the AV to interact with/provide feedback to other people in the vicinity of the vehicle has been considered during the design process, and that the AVCO is capable of meeting the identified requirements.

In any environment in which it shares with people, the AV should provide appropriate signals to indicate its intentions. In some cases, this is expected to be comparatively straightforward (for example, through use of indicator lights when changing direction or brake lights when slowing down).

NOTE *APVs might have to share their operating environment with pedestrians, cyclists, other animals, other APVs and possibly HDVs or ARVs (e.g. if the APV needs to cross a public road).*

ARVs might have to share their operating environment with HDVs, other ARVs, pedestrians, cyclists, other animals and possibly APVs (for the reason noted above).

Other interactions between drivers of current HDVs (road vehicles or pods) might involve human-to-human interaction. For example, a driver of a road vehicle might make eye contact with someone waiting at a pedestrian crossing; having made such contact, the pedestrian will know that they have been seen and will start to cross the road.

9.5 Use of AI in the AVCO

If AI is employed in the AVCO then evidence should be provided that this design decision is compliant with the objective presented in **4.7**.

NOTE *See Annex C for guidance on the use of AI in AVs.*

9.6 Monitoring the AVCO

The AVCO should not provide tactical directions to the actuators in situations where it cannot be confident that correct data will be provided.

To achieve this, the AVCO should perform self-monitoring activities, to determine whether it is operating correctly. The results of this monitoring activity should be reported to the AVMO.

If, as a result of such monitoring, it is determined that the AV cannot continue to operate safely or securely and it cannot recover from this situation in an appropriate time, then the vehicle should perform a controlled stop or emergency stop.

NOTE 1 *Annex D provides examples of monitoring techniques that have been used in autonomous machines.*

NOTE 2 *During trials (and in some cases with production vehicles), it might be appropriate to store data that are generated by the AVCO monitoring process for later analysis.*

9.7 Evidence that objectives have been met

The development team should provide evidence that their AVCO design meets the objectives that are laid out in **9.1** and the related sub-objectives that are identified in **9.2** to **9.6**.

NOTE *Annex A provides examples of techniques that can be used to provide this evidence.*

10 Designing the AV monitoring operation (AVMO)

10.1 Objective

It should be demonstrated that, throughout the mission, the AV is able to monitor its own operation (**4.6**).

10.2 The AVMO

Meeting the objective provided in **10.1** should be (primarily) the responsibility of the AVMO.

NOTE *One possible architecture for an AV control system (showing the AVMO in context) is given in Figure 1.*

If the AVMO determines that:

a) the AV is not operating in compliance with the ODD specification; or

b) the vehicle is not otherwise operating correctly; or

c) the AVMO is not itself operating correctly,

then the AVMO should issue a command to the AVPO requiring that the vehicle perform a controlled stop. If the AV does not respond to this command within an appropriate time, then the AVMO should trigger a controlled stop directly (e.g. see Figure 1).

NOTE *Other "recovery" behaviour might also be considered here. For example, suppose that the vehicle is intended to carry passengers but currently has no passengers. If a fault occurs to (say) the seat-belt system, this will have no impact on other road users but does mean that the AV cannot safely carry passengers. In these circumstances, performing a controlled stop or emergency stop might not be the most appropriate course of action. Instead, it might be more appropriate to have the vehicle travel (without passengers) to the nearest repair centre.*

10.3 Self-monitoring (high level)

The team developing the AVMO should demonstrate that:

a) safety-related faults in the vehicle that it might reasonably be expected that a driver of an equivalent HDV could detect, can be detected by the AVMO and handled appropriately;

b) safety-related faults in the AVMO can be detected by the AVMO and handled appropriately; and

c) all other safety-related faults in the vehicle can be detected by the AVMO and handled appropriately.

Data provided by the AVSO, AVPO and AVCO (as a result of their self-monitoring processes) should be used to support the monitoring requirements that are identified in this clause.

NOTE 1 *Detection of safety-related faults in the vehicle that it might reasonably be expected that a driver of an equivalent HDV could detect might be carried out directly by the AVMO. Alternatively, detection of such faults might be carried out by the AVSO, AVPO or AVCO and reported to the AVMO for handling.*

NOTE 2 *To assist in this process, the following examples of situations involving a human driver might help to illustrate some of the high-level fault monitoring that is envisaged here:*

a) *"On returning to my vehicle in the car park, I noticed that someone had run into it: I called my garage to check that it was still safe to drive."*

b) *"There was an unusual noise coming from the front right wheel/wheel bearing so I pulled over to the side of the road."*

c) *"The vehicle had started to stall when I slowed down to approach a junction; I was concerned that this was becoming dangerous and I stopped using it."*

10.4 Self-monitoring (low level)

The AVMO should not provide "controlled stop" requests (or any other requests) to the AVPO in situations in which it cannot be confident that correct requests will be made.

To achieve this, the AVCO should perform self-monitoring activities, to determine whether it is operating correctly.

If, as a result of such monitoring, it is determined that the AV cannot continue to operate safely or securely and it cannot recover from this situation in an appropriate time, then the vehicle should perform an emergency stop.

NOTE 1 *Annex D provides examples of monitoring techniques that have been used in autonomous machines.*

NOTE 2 *During trials (and in some cases with production vehicles), it might be appropriate to store data that are generated by the AVMO monitoring process for later analysis.*

10.5 Use of AI in the AVMO

If AI is employed in the AVMO then evidence should be provided that this design decision is compliant with the objective presented in **4.7**.

NOTE *See Annex C for guidance on the use of AI in AVs.*

10.6 Evidence that objectives have been met

The development team should provide evidence that their AVMO design meets the objectives that are laid out in **10.1** and the related sub-objectives that are identified in **10.2** to **10.5**.

NOTE *Annex A provides examples of techniques that can be used to provide this evidence.*

11 Safety, security and effectiveness

11.1 Objective

The AV should be demonstrated to be capable of operating safely, securely and effectively at all times (**4.7**).

11.2 General safety requirements

Four general hazards that can be identified for control systems in an HDV:

a) the vehicle performs "unintended acceleration" (with the possible consequence – for example – that it runs into another vehicle or pedestrian) or "unintended deceleration" (with the possible consequence – for example – that another vehicle runs into it from behind);

b) the vehicle does not accelerate or decelerate when it is required to do so (with similar potential for collisions);

c) the vehicle performs an unplanned lateral movement (potentially – for example – pulling into the path of another vehicle); or

d) the vehicle does not perform a lateral movement when it is required to do so (potentially – for example – running off the edge of a road).

In order to comply with the objective in **4.7**, the development team should provide evidence that the AV they are developing is able to address these hazards effectively.

NOTE *To assist in this process, the development team might wish to consider that such hazards are addressed in a road-based HDV by the driver, who provides capabilities similar to the following (from an engineering perspective):*

a) a "monitoring system" that is independent from vehicle control systems;

b) independent "actuator units" (to move the steering wheel, for example);

c) a "power supply" for the above "units" that is independent of the vehicle power supplies; and

d) diversity in all of the above "designs" (when compared with the vehicle systems).

11.3 General security requirements

The ability to address the general hazards given in **11.2** might be compromised by a cybersecurity attack on the AV. The development team should provide evidence that the AV has mechanisms in place that allow it to withstand such an attack.

NOTE *Annex C provides information on some standards that might be useful.*

11.4 Effective operation

Evidence should be provided by the development team that the AV will operate effectively.

NOTE *To be effective requires that the AV can meet the mission requirements (see **4.1** and Clause **5**). It is (theoretically) possible to meet both the safety and security concerns in the objective given in **4.7** by creating an AV that is therefore very unlikely to cause injuries or death. Such an AV will, however, not meet the requirement given in **4.7** that the vehicle be effective.*

11.5 The role of the safety operator

If, during trials, a safety operator is utilised then this should be in accordance with PAS 1881.

11.6 Evidence that objectives have been met

The development team should provide evidence that their AV design meets the objectives that are laid out in **11.1** and the related sub-objectives that are identified in **11.2** to **11.5**.

NOTE *Annex A provides examples of techniques that can be used to provide this evidence.*

Annex A (informative) Sources of evidence

A.1 Overview

Annex A provides examples of techniques that can be used to provide evidence of compliance with the objectives presented in Clause **4** to Clause **11**.

A.2 Processes

Documented development processes can help to provide evidence that (for example) a given design is compatible with a particular set of system requirements.

For users of this PAS, the processes described in the BSI ISO 26262 series might be an appropriate starting point.

A.3 Generic safety case

Safety cases are widely used across a range of domains.

For example, in the nuclear industry:

"A safety case is a logical and hierarchical set of documents that describes risk in terms of the hazards presented by the facility, site and the modes of operation, including potential faults and accidents, and those reasonably practicable measures that need to be implemented to prevent or minimize harm. It takes account of experience from the past, is written in the present, and sets expectations and guidance for the processes that should operate in the future if the hazards are to be controlled successfully. The safety case clearly sets out the trail from safety claims through arguments to evidence."

NOTE *See Office For Nuclear Regulation (ONR). Safety Assessment Principles For Nuclear Facilities, 2014 Edition Revision 1 (January 2020) [4].*

For users of this PAS, the "MISRA Guidelines for Automotive Safety Arguments" [5] might be an appropriate starting point.

A.4 Hazard analysis and risk assessment

A hazard analysis and risk assessment (HARA) process is employed as part of various safety standards and guidelines.

For users of this PAS, the HARA process described in the BSI ISO 26262 series might be an appropriate starting point.

NOTE *When a HARA is performed in compliance with BS ISO 26262, controllability "by persons involved" is to be determined. As there is no driver in an AV (outside of a trial situation), controllability involves actions by people in the vicinity of the vehicle only: such actions can be expected to be of very limited benefit in the majority of scenarios.*

A.5 Safety of the intended function (SOTIF)

In addition to the hazards that can be identified through what might be seen as a traditional HARA process (see **A.4**), the use of complex components in an AV (e.g. complex sensors) means that additional hazards can be presented, due to limitations of the system/system components when operating as intended (with no faults present). Such issues are described by the phrase "safety of the intended functionality" (SOTIF).

For users of this PAS, PD ISO/PAS 21448 might be an appropriate starting point when considering SOTIF issues.

NOTE *The AVMO might provide a means of mitigating some SOTIF issues in AVs that are developed in compliance with this PAS.*

A.6 Fault-based analysis

Analysis techniques such as failure modes and effects analysis (FMEA) and fault-tree analysis (FTA) are useful in conducting a structured and comprehensive analysis of a system design to consider both causes of unwanted conditions and the effects of faults.

A.7 STPA/STAMP

System theoretic process analysis (STPA) and system theoretic accident model and processes (STAMP) provide an alternative approach to hazard analysis.

At the heart of these processes is an assumption that sometimes the cause of systems failure is not that (for example) a component has failed to operate correctly but – instead – that the system design was simply inadequate. Note that there is some overlap here (at least in terms of concept) with SOTIF (**A.5**).

Further information about STPA and STAMP can be found in *Engineering a Safer World: Systems Thinking Applied to Safety* [6].

A.8 Hazard and operability (HAZOP) studies

A hazard and operability (HAZOP) study is a structured examination of a complex system or process that is carried out in identify and evaluate problems that can represent risks to people or equipment.

HAZOPs originated in the chemical industry. They are now employed more widely.

A guide by Tyler, Crawley & Preston provides further information [7]. See also Medoff and Faller "Functional Safety – An IEC 61508 SIL 3 Compliant Development Process" [8] and Redmill, Chudleigh & Catmur *System Safety: HAZOP and Software HAZOP* [9].

A.9 Simulators

If simulators or similar test facilities are used to demonstrate compliance with any of the objectives detailed in this PAS, then confidence in the results obtained can be increased if such facilities are appropriately qualified. For example, a simulator can be developed in compliance with one or more international safety standards (such as BS ISO 26262).

***NOTE** Simulation can include "hardware in the loop" (HIL) testing, "software in the loop" (SIL) testing and other bench tests. PAS 1881 provides further information.*

A.10 Trials

Confidence in the safe, secure and effective operation of an AV can be increased by recording the results from trials that involve a safety driver or remote safety driver.

A.11 Independent assessment

An independent assessment (by a suitably-qualified individual) of the evidence assembled by a development team to demonstrate compliance with the objectives presented in Clause **4** to Clause **11** can help to increase confidence in the conclusions reached.

Annex B (informative)
Designing an automated vehicle unit (AVU)

B.1 Overview

Throughout this PAS, the focus has been on the design of the AVSO, AVCO, AVPO and AVMO functions.

In this Annex, possible ways of implementing these functions by means of AVUs are explored.

By default, it is assumed in this PAS that each of the operations (AVSO, AVCO, AVPO and AVMO) are implemented using a separate AVU: this is sometimes called a "federated architecture" (see Figure B.1 which provides schematic representation of an automated road vehicle showing a possible AVU configuration).

Using a more integrated architecture (where two or more of these operations are implemented by means of a single AVU) can also be considered, provided that evidence can be provided that the different operations do not interfere with one another. Use of an integrated architecture might be easier to justify in an APU (see Figure B.2 which provides a schematic representation of an automated pod vehicle showing a possible AVU configuration).

NOTE *Use of an integrated architecture might increase the risk of common-cause failures in a design. Provided that such failures can be detected by the AVMU (which can then trigger an emergency stop) then it is possible to be confident that the system based on an integrated architecture will operate safely – if (and only if) performing an emergency stop is an appropriate response to a system failure. In the control-system designs considered in this PAS, performing an emergency stop at any time is more likely to be an appropriate response for an APV than it is for an ARV.*

Figure B.1 – A schematic representation of an automated road vehicle showing a possible AVU configuration

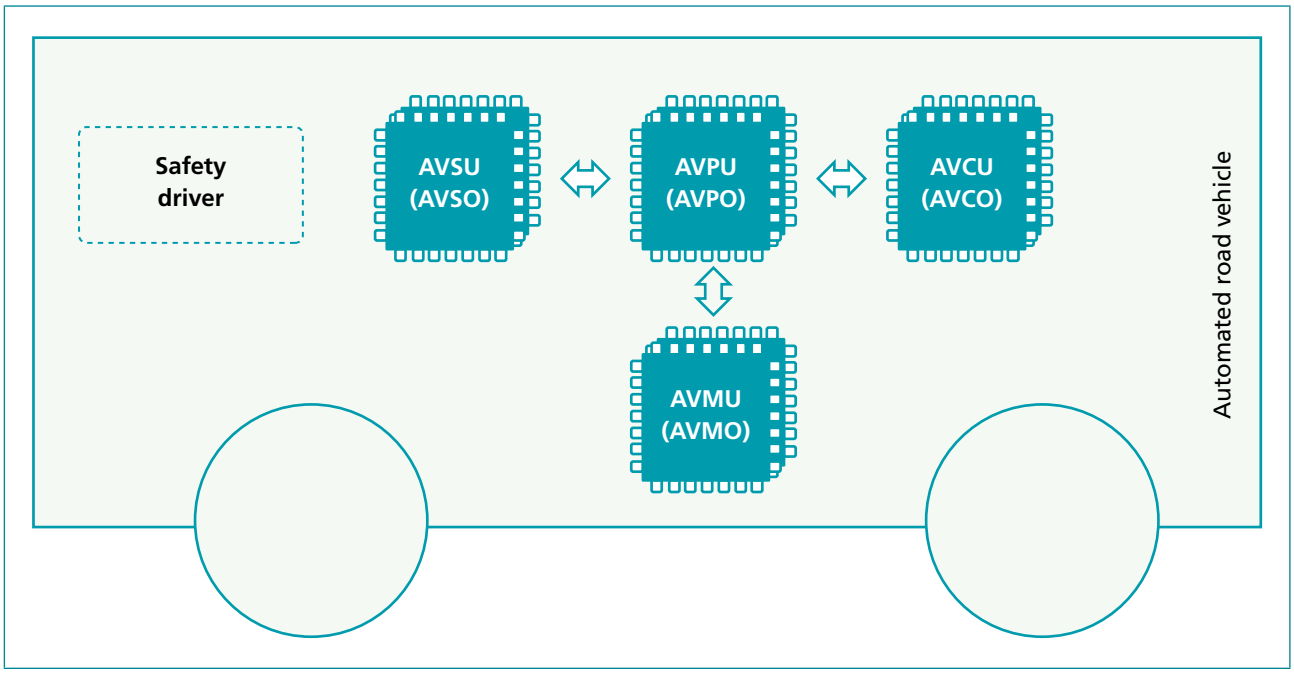
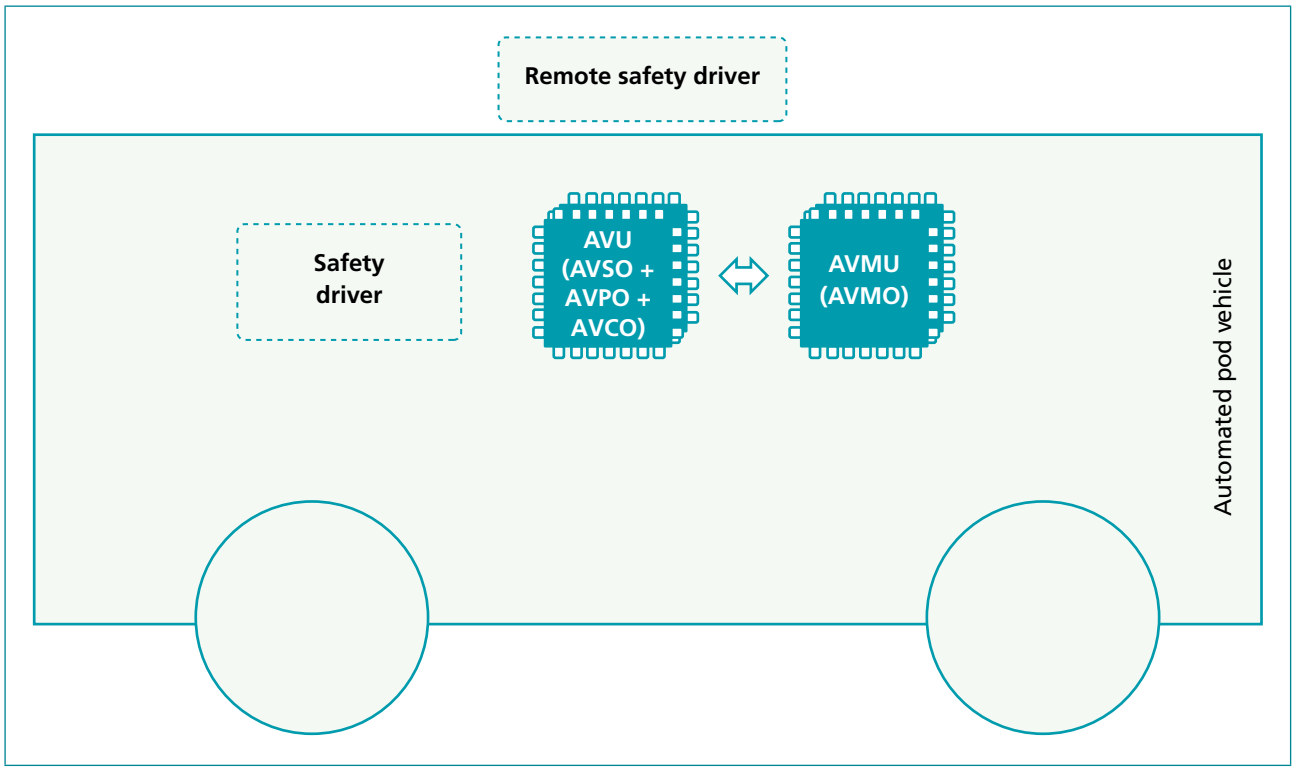


Figure B.2 – A schematic representation of an automated pod vehicle showing a possible AVU configuration



B.2 Self-monitoring

Each AVU is assumed to be responsible for self-monitoring, to ensure that the AVU is itself operating correctly.

BS ISO 26262-6, IEC 61508 and BS EN ISO 13849-1 provide useful guidance on the development of monitoring software for complex embedded systems like the AVU.

B.3 Designing the AVU architecture

Developers of AVUs can consider a technical safety concept in accordance with BS ISO 26262-4 to detect and react to faults and failures. During such a process, consideration of the hardware architectural metrics (BS ISO 26262) or hardware fault tolerance and safe failure fraction (IEC 61508) might suggest use of a dual-processor architecture.

Dual-processor designs are commonly employed in systems that are developed in compliance with IEC 61508 and BS EN ISO 13849. These standards have a focus on "machines" that might be required to operate without human intervention for long periods. For example, it is not uncommon for designs developed in compliance with IEC 61508 and/or BS EN ISO 13849-1 to have a proof test interval (PTI) of 10 years or more.

The PTI represents the time after which the unit is either:

a) subject to a complete test and verification process to ensure that it is in an "as new" condition; or

b) replaced.

There might be little (or nothing) by way of maintenance performed during the PTI. In these circumstances the unit will monitor its own condition throughout this period and determine whether it is able to operate safely. If it cannot do so, it will enter an appropriate safe state.

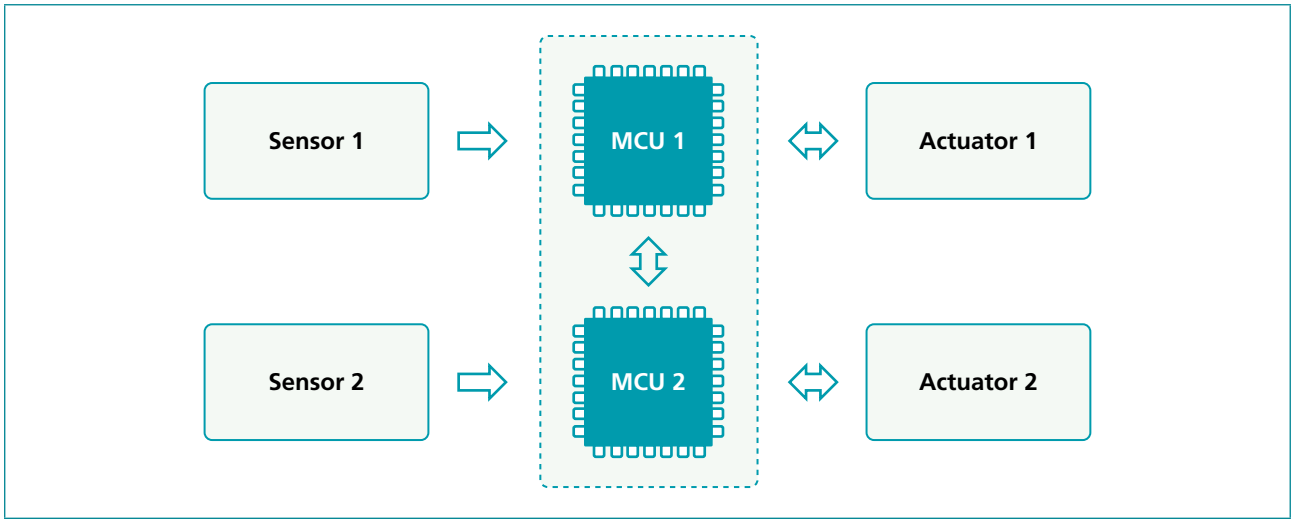
In order to support comprehensive monitoring over long periods (potentially measured in years), and to provide confidence that the system is able to enter what is referred to in this PAS as an MRC if problems are detected during this monitoring process, many machinery designs have a hardware fault tolerance (HFT) of 1. HFT = 1 means that there are two processing paths available. In practice, this typically means that the hardware design is based on two microcontrollers that:

a) can perform cross checks; and

b) might be able to operate independently – at least for a limited period – if one microcontroller fails.

Such dual-processor designs are represented explicitly in the form of the "designated architectures" for safety-critical systems in BS EN ISO 13849-1 (see Figure B.3 which provides a schematic representation of a Category 3 -designated architecture that involves dual microcontrollers).

Figure B.3 – A schematic representation of a Category 3 -designated architecture



NOTE *SOURCE BS EN ISO 13849-1: 2015.*

B.4 Multi-processor options

In some designs (particularly in ARVs) it might be necessary to consider triple-modular redundancy in the AVU in order to meet the requirements for effectiveness (**4.7**).

In other designs, use of multiple processors (e.g. four or more) might be considered, in order to meet such requirements.

B.5 Linking AVUs together

When linking multiple AVUs in a given AV design, consideration is to be given to mechanisms for detecting and reacting to communication failures: see for example BS ISO 26262-6:2018 Annex D.

Many proprietary protocols (such as CAN), while designed with an inherent degree of resilience, often need to be supplemented with additional error checking capabilities, e.g. periodic message transmission, "alive counter", additional checksum, when used in such designs.

In some designs, following an industry-standard protocol (e.g. SAE J1939) might be appropriate.

Annex C (informative) Artificial intelligence (AI)

C.1 Overview

Use of AI being explored in trials of AV systems (e.g. see Salay, R. et al. "An Analysis of ISO 26262: Using Machine Learning Safely in Automotive Software" [10]).

Use of AI techniques in AVs is considered in this Annex.

C.2 Should AI be avoided in AVs?

The core challenge with any form of AI application (as far as current safety standards are concerned) lies in the learning element. As the system learns, the traceability (between requirements, design and implementation) that lies at the heart of such standards is difficult (or impossible) to demonstrate with the level of confidence that would be expected in current safety-critical design processes.

As a consequence, it is perhaps not surprising that international safety standard IEC 61508 suggests that use of AI is not recommended in systems of "SIL 2", "SIL 3" or "SIL 4" (see IEC 61508-3:2010, Annex A, Table A.2)].

Similarly, according to Aravantinos, V. and Diehl [11], p.1:

"The success of deep learning (DL), in particular in computer vision, makes its usage more and more tempting in many applications, including safety-critical ones. However, the development of such applications must follow standards … which typically do not envision the usage of machine learning. At the moment, practitioners therefore cannot use machine learning for safety-critical functions (e.g., ASIL-D for ISO 26262, or DAL-A for DO178)."

C.3 If AI is to be used in AVs, how can the risks be reduced?

If AI is to be used in AVs, the risks of doing so can only be reduced by understanding why traditional standards express concerns about the use of such technology and exploring ways of addressing these concerns.

PD ISO/PAS 21448:2019 (particularly Annex G) discusses the use of AI in the context of AVs.

The following papers also provide further information on the use of AI in the context of AVs: Salay, R. et al [10], Aravantinos, V. and Diehl, F. (2019) "Traceability of Deep Neural Networks" [11], Salay, R. and Czarnecki, K. "Using Machine Learning Safely in Automotive Software: An Assessment and Adaption of Software Process Requirements in ISO 26262" [12] and Ashmore, Calinescu and Paterson (2019) "Assuring the Machine Learning Lifecycle: Desiderata, Methods, and Challenges" [13].

Annex D (informative) Autonomous machines

D.1 Overview

This Annex provides an illustrative relationship of the use of AVs in an earthmoving/mining context and some of the related standards that apply or are under development.

D.2 The ODD description

A construction, earthmoving or mining site typically has restricted public access and defined "operational zone" (which are similar to the concept of ODDs that is presented in this PAS). As the site evolves the operational zones might change significantly.

Automated machine operation can additionally have physically defined or geo-fenced operational zone (a defined ODD) under site management systems (SMS) coordination. SMS are typically manned control rooms and so can be equated to the "remote safety driver" (RSD) concept within this PAS.

In addition to the SMS monitoring capability and machine telemetry, drones can also be utilized for over the horizon and real-time data collection/feedback to the SMS. The SMS task schedulers can define the machines mission and highly automated machines can provide pre-determined route planning, with dynamic route-planning based upon the localized conditions and machine detection and operational capabilities and SMS updates.

Conditions within the operational zones might be environmentally arduous when compared with those experienced by typical on-highway vehicles.

The machines operating on such sites might be considerably larger than on-highway vehicles. Some might have multi-axis movement. Typically a machine is designed for a specific task, but – through the addition of attachments – can perform different tasks.

Machine telemetry can provide current health and productivity data which is typically used to improve operational efficiency. If a machine experiences health issues it might be stood down to a minimal risk condition, operate in a reduced capacity, or move to a defined service area/location away from its original intended task (the equivalent of an MRL in this PAS).

Some machines have automated features such as adaptive cruise control and collision avoidance warnings. The machines are used to extract/move material with automation supplementing base machine functionality with systems such as auto dig, auto compaction and auto grade. For some features the machine operational kinematics are augmented by the desired topological design data, uploaded to the machines either over the air or manually.

Where automated functions are used, these might be operator selected and monitored. The operator might also initially "teach" and/or monitor the expected operation of the machine during its defined task. If such trials proved successful, repeatable tasks might then become fully automated.

In this context, the AVCO, AVMO, AVPO and AVSO functionality presented in this PAS become elements of an autonomous or semi-autonomous machine system (ASAMS). The ASAMS can then collectively determine the most effective way of performing the desired task (mission) in an applicable machine mode.

If multiple machines are assigned the same mission then either the on board, or remote SMS might collaboratively decide the order of operations to complete the desired task.

D.3 BS ISO 17757:2017, *Autonomous and semi-autonomous machine system safety*

BS ISO 17757:2017 provides safety requirements for autonomous machines and semi-autonomous machines used in earth-moving and mining operations, and their autonomous or semi-autonomous machine systems (ASAMS). It specifies safety criteria both for the machines and their associated systems and infrastructure, including hardware and software, and provides guidance on safe use in their defined functional environments during the machine and system life cycle. It also defines terms and definitions related to ASAMS. Many of its provisions can be applied to other types of autonomous or semi-autonomous machines.

D.4 ISO 15998:2008, *Machine control system using electronic components – Functional safety requirements*

Microprocessor-based systems, generically referred to as programmable electronic systems (PES), are at present being used in machines to perform non-safety-related and, increasingly, safety-related functions. Safety is typically achieved by a number of protective systems which might rely on various technologies (e.g. mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic). The safety strategy considers not only all the elements within an individual system, such as sensors, controlling devices and actuators, but also all of the safety-related system parts. The second part of ISO 15998:2008 defines the envisaged functional safety requirements for the applicable machine type and typical operation.

D.5 BS EN ISO 16001:2017, *Earthmoving machinery – Object detection systems and visibility aids – Performance requirements and tests*

BS EN ISO 16001:2017 provides guidance for visual aids test procedures and sets criteria for the development of object detection systems (ODSs) and visibility aids (VAs) which indicate to the operator the presence of objects which are within the detection zone of such systems as fitted to the machines that might be found in similar environments.

D.6 ISO/CD TS 21815, *Collision warning and avoidance*[6)]

Earthmoving machinery has seen increasing use of detection system and avoidance technology to support the operators to safely operate machines. ISO/CD TS 21815 is intended to be a multi-part standard under development resulting from application demands to set standards for machines and systems capable of detecting, alerting and intervening machinery operation, hopefully mitigating the risks presented. It describes hazard awareness, risk areas detection and envisaged behaviours in relation to a typical human response that are expected to be performed by the machine control systems in a multi-axis domain.

D.7 PD ISO/TS 15143, *Worksite data exchange*

Information and measuring technology are being used to develop worksite information systems to support the control of the finished form of work performed by machinery used within a job site. PD ISO 15143 is a multi-part standard provides a mechanism for data to be easily and reliably exchanged between the site's machinery, measuring equipment and site information systems. Automated functions are increasing being rationalized with common terms to permit interoperability between different vendors.

[6)] In preparation.

Annex E (informative) Related safety standards

E.1 Overview

Annex E provides a list of standards that might be of interest to readers of this PAS.

E.2 BS ISO 26262:2018

BS ISO 26262:2018 does not cover general techniques for achieving functional safety in AVs; instead, reference is made to related standards for information about such matters.

Now in its second edition, BS ISO 26262:2018 was adapted from the IEC 61508 series of standards to address the sector-specific needs of electrical and/or electronic systems within road vehicles. BS ISO 26262:2018 applies to all activities during the safety lifecycle of safety-related systems comprised of electrical, electronic and software components.

E.3 IEC 61508:2010 and BS EN ISO 13849-1:2015

IEC 61508:2010 and BS EN ISO 13849-1:2015 also provide guidance on achieving functional safety that might be relevant to developers of AVs (see also Annex B).

Unlike BS ISO 26262 (which has a focus on vehicles in which there is a driver present at all times), IEC 61508 and BS EN ISO 13849 have a focus on "machines" that might be required to operate without human intervention for long periods.

E.4 BS ISO 17757:2017

BS ISO 17757:2017 provides safety requirements for autonomous machines and semi-autonomous machines used in earth-moving and mining operations, and their autonomous or semi-autonomous machine systems (ASAMS). It specifies safety criteria both for the machines and their associated systems and infrastructure, including hardware and software, and provides guidance on safe use in their defined functional environments during the machine and system life cycle. It also defines terms and definitions related to ASAMS.

It is applicable to autonomous and semi-autonomous versions of the earth-moving machinery (EMM) defined in BS ISO 6165 and of mobile mining machines used in either surface or underground applications. Its principles and many of its provisions can be applied to other types of autonomous or semi-autonomous machines used on the worksites.

E.5 ISO 19014: 2018

ISO 19014:2018 provides a methodology for the determination of performance levels required for earth moving machinery, as defined in BS ISO 6165.

E.6 PD ISO/PAS 21448:2019

PD ISO/PAS 21448:2019 is intended to be applied to systems in which proper situational awareness is critical to safety, and where that situational awareness is derived from complex sensors and processing algorithms; especially emergency intervention systems (e.g. emergency braking systems) and advanced driver assistance systems (ADAS) with levels 1 and 2 on the SAE standard J3016 automation scales. PD ISO/PAS 21448:2019 can be considered for higher levels of automation, however additional measures might be necessary.

E.7 PAS 1881:2020

This PAS covers assuring safety in AV trials and testing.

E.8 PAS 1882[7)]

This PAS is intended to cover data collection, storage and accessibility of data AV trials and testing.

E.7 PAS 1883[8)]

This PAS is intended to cover ODD specification.

E.8 SAE J3016_201806

SAE J3016_201806 contains potentially useful definitions; although note that "levels" defined in SAE J3016 are not used in this PAS.

[7)] In preparation.
[8)] In preparation.

E.9 PAS 11281:2018

PAS 11281:2018 gives recommendations for managing security risks that might lead to a compromise of safety in a connected automotive ecosystem.

E.10 PAS 1885:2018

PAS 1885:2018 covers fundamental principles of automotive cyber security.

E.11 J3061_201601

J3061_201601 provides guidance on vehicle cybersecurity and was created based on existing practices which are being implemented or reported in industry, government and conference papers.

E.12 ISO/SAE CD 21434[9)]

This standard is intended to have a focus on cybersecurity for road vehicles.

[9)] In preparation.

Bibliography

Standards publications

PAS 1881:2020, *Assuring the safety of automated vehicle trials and testing – Specification*

PAS 1882, *Automated vehicle trials – Data collection, storage and accessibility – Specification*[10)]

PAS 1883, *Operational design domain (ODD) taxonomy for an automated driving system (ADS) – Specification*[11)]

PAS 1885: 2018, *The fundamental principles of automotive cyber security – Specification*

PAS 11281:2018, *Connected automotive ecosystems – Impact of security on safety – Code of practice*

IEC 61508:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 61508-7:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems: Overview of techniques and measures*

PD ISO/PAS 21448:2019, *Road vehicles — Safety of the intended functionality*

PD ISO/TS 15143, *Worksite data exchange*

ISO/CD TS 21815, *Collision warning and avoidance*[12)]

ISO/SAE CD 21434, *Road Vehicles – Cybersecurity engineering*[13)]

ISO/WD 23724, *Remote stop function for autonomous machines*

ISO 15998:2008, *Machine control system using electronic components – functional safety requirements*

BS ISO 17757:2017 *Autonomous and semi-autonomous machine system safety*

BS ISO 26262:2018, *Road vehicles – Functional safety*

BS ISO 26262-4:2018, *Road vehicles – Functional safety – Product development at the system level*

BS ISO 26262-6:2018, *Road vehicles – Functional safety – Product development at the software level*

BS EN ISO 6165: 2012, *Earth-moving machinery – Basic types – Identification and terms and definitions*

BS EN ISO 13849-1: 2015, *Safety of machinery – Safety-related parts of control systems – General principles for design*

BS EN ISO 16001:2017, *Earth moving machinery – Object detection systems and visibility aids – Performance requirements and tests*

DO-178C, *Software considerations in airborne systems and equipment certification*

SAE J1939_201808, *Serial control and communications heavy duty vehicle network*

SAE J3016_201806, *Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles*

SAE J3061_201601, *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems.*

[10)] In preparation.
[11)] In preparation.
[12)] In preparation.
[13)] In preparation.

Other publications

[1] BRITISH STANDARDS INSTITUTION/TRANSPORT SYSTEMS CATAPULT. "Connected and autonomous vehicles: A UK standards strategy". Published: London, 2017.

[2] SHAFER, G. *A Mathematical Theory of Evidence*, Princeton University Press. Published: 1976.

[3] RUMELHART, D. and MCCLELLAND, J.L. *"Parallel Distributed Processing"*, Volume 1. M.I.T. Press. Published: 1986.

[4] OFFICE FOR NUCLEAR REGULATION (ONR). *Safety Assessment Principles For Nuclear Facilities. 2014 Edition Revision 1*. Published: 2020. http://www.onr.org.uk/saps/saps2014.pdf [Accessed March 2020].

[5] MISRA. *Guidelines for Automotive Safety Arguments*. Published: 2019.

[6] LEVESON, N.G. *Engineering a Safer World: Systems Thinking Applied to Safety*. MIT Press. Published: 2017.

[7] TYLER, B., CRAWLEY, F. and PRESTON, M. *HAZOP: Guide to Best Practice* (3rd edition) Institution of Chemical Engineers/Elsevier. Published: 2015.

[8] MEDOFF, M.D. and FALLER, R.I. *Functional Safety – An IEC 61508 SIL 3 Compliant Development Process* (3rd edition). Exida. Published: 2014.

[9] REDMILL, F. CHUDLEIGH, M. and CATMUR, J. *System Safety: HAZOP and Software HAZOP*. Wiley. Published: 1999.

[10] SALAY, R. QUIEROZ, R. and CZARNECKI, K. (2017) "An Analysis of ISO 26262: Using Machine Learning Safely in Automotive Software", arXiv:1709.02435v1 [cs.AI]. Published: 2017. Available at: https://arxiv.org/pdf/1709.02435.pdf [Accessed March 2020].

[11] ARAVANTINOS, V. and DIEHL, F. (2019) "Traceability of Deep Neural Networks", arXiv:1812.06744v2 [cs.LG]. Published: 2019. Available at: https://arxiv.org/pdf/1812.06744.pdf [Accessed March 2020].

[12] SALAY, R. and CZARNECKI, K. "Using Machine Learning Safely in Automotive Software: An Assessment and Adaption of Software Process Requirements in ISO 26262" arXiv:1808.01614v1 [cs.LG]. Published: 2018. Available at: https://arxiv.org/ftp/arxiv/papers/1808/1808.01614.pdf [Accessed March 2020].

[13] ASHMORE, R. CALINESCU, R. and PATERSON, C. (2019) "Assuring the Machine Learning Lifecycle: Desiderata, Methods, and Challenges. arXiv:1905.04223 [cs.LG). Published: 2019. Available at: https://arxiv.org/abs/1905.04223 [Accessed March 2020].

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

This page is deliberately left blank.

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