



BSI Standards Publication

Road vehicles — Safety for automated driving systems — Design, verification and validation

National foreword

This Published Document is the UK implementation of ISO/TS 5083:2025. It supersedes PD ISO/TR 4804:2020, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee AUE/32/1.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

This publication is not to be regarded as a British Standard.

© The British Standards Institution 2025
Published by BSI Standards Limited 2025

ISBN 978 0 539 16506 7

ICS 43.020

Compliance with a Published Document cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 May 2025.

Amendments/corrigenda issued since publication

Date	Text affected



Technical Specification

ISO/TS 5083

Road vehicles — Safety for automated driving systems — Design, verification and validation

*Véhicules routiers — Sécurité des systèmes de conduite
automatisée — Conception, vérification et validation*

**First edition
2025-04**

Reference number
ISO/TS 5083:2025(en)

Full document details: PD ISO/TS 5083:2025

© ISO 2025  **Documents**
Document Sharing Hub



COPYRIGHT PROTECTED DOCUMENT

© ISO 2025
All rights reserved.

ISO publications, in their entirety or in fragments, are owned by ISO. They are licensed, not sold, and are subject to the terms and conditions set forth in the ISO End Customer License Agreement, the License Agreement of the relevant ISO member body, or those of authorized third-party distributors.

Unless otherwise specified or required for its implementation, no part of this ISO publication may be reproduced, distributed, modified, or used in any form or by any means, electronic or mechanical, including photocopying, scanning, recording, or posting on any intranet, internet, or other digital platforms, without the prior written permission of ISO, the relevant ISO member body or an authorized third-party distributor.

This publication shall not be disclosed to third parties, and its use is strictly limited to the license type and purpose specified in the applicable license grant. Unauthorized reproduction, distribution, or use beyond the granted license is prohibited and may result in legal action.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword	vi
Introduction	ix
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	7
5 Document overview and motivation	7
5.1 Purpose	7
5.2 Overall goals of this document	7
5.3 Application of this document	7
5.4 Safety life cycle	8
5.4.1 Purpose	8
5.4.2 General	8
5.5 Description of ADS safety case	8
5.5.1 Purpose	8
5.5.2 General	8
5.5.3 How this document supports a layered structure of an ADS safety case	9
5.5.4 Perspective from the ADS-equipped vehicle	11
5.6 Role of the ADS within safe vehicle operation	12
5.6.1 Purpose	12
5.6.2 General	12
5.6.3 Task dependency of ADS safety	12
5.6.4 Time dependency of ADS safety	13
5.6.5 Examples	14
5.7 Application of other standards	15
5.7.1 Purpose	15
5.7.2 Classification of standards	15
5.7.3 Applying the related (safety) standards	16
5.8 Safety principles of ADS	17
5.8.1 Purpose	17
5.8.2 ADS safety principles	17
6 Safety strategy	18
6.1 Defining the ADS feature	18
6.1.1 Objectives	18
6.1.2 Requirements and recommendations	18
6.1.3 Example solution: ADS feature description with capabilities	19
6.2 Defining the risk acceptance criteria	20
6.2.1 Objectives	20
6.2.2 Requirements and recommendations	20
6.2.3 Example solution: Absence of unreasonable risk and risk acceptance criteria	21
6.2.4 Example solution: Selection and use of risk acceptance criteria	21
6.2.5 Example solution: Defining a risk acceptance criterion	21
6.2.6 Example solution: Quantitative risk balance	21
6.2.7 Example solution: A quantitative risk acceptance criterion	21
6.3 Defining safety requirements	21
6.3.1 Objectives	21
6.3.2 Requirements and recommendations	21
6.3.3 Example solution: Quantitative risk acceptance criterion and incident classification approach	22
6.3.4 Example solution: Safety capabilities	22
6.3.5 Example solution: ADS external assumptions with respect to injury risk	22
7 Safety by design	22

7.1	ADS design.....	22
7.1.1	Objectives.....	22
7.1.2	Requirements and recommendations.....	22
7.1.3	Example solution: A design for adapting tactical decisions to variations in the operational capabilities.....	23
7.1.4	Example solution: Elements defining the design.....	23
7.2	ADS external design, prerequisites and assumptions.....	23
7.2.1	Objectives.....	23
7.2.2	General.....	23
7.2.3	Requirements and recommendations.....	30
7.2.4	Example solution: Training for users.....	30
7.2.5	Example solution: Instructions to first responders.....	31
7.2.6	Example solution: Organizational aspects of a robo taxi service.....	31
7.2.7	Example solution: Organizational aspects of an L4 hub-to-hub transport service.....	31
7.3	ADS verification.....	31
7.3.1	Objectives.....	31
7.3.2	General.....	31
7.3.3	Requirements and recommendations.....	31
7.3.4	Example solution: Verification of elements.....	32
7.3.5	Example solution: The layered approach facilitating verification of safety arguments.....	32
7.4	Verification and confirmation of aspects external to the ADS.....	32
7.4.1	Objectives.....	32
7.4.2	General.....	32
7.4.3	Requirements and recommendations.....	32
8	Validation.....	33
8.1	Objectives.....	33
8.2	General.....	33
8.3	Requirements and recommendations.....	33
8.4	Example solution: Metrics.....	33
8.5	Example solution: Validation through computation of collision rates.....	34
8.6	Example solution: Generating evidence for injury risk assumptions external to the ADS.....	34
9	Operation of the ADS-equipped vehicle.....	34
9.1	Objectives.....	34
9.2	General.....	34
9.2.1	Overview.....	34
9.2.2	Field monitoring including data collection.....	35
9.2.3	Cybersecurity monitoring related to safety of ADSs.....	35
9.2.4	Change management during the operational phase.....	35
9.2.5	Inspection, maintenance and repair.....	37
9.2.6	Management of crashes and incidents.....	37
9.3	Requirements and recommendations.....	37
10	Verification and validation requirement considerations.....	38
10.1	General.....	38
10.2	Example solution: Verification and validation.....	38
	Annex A (informative) Example application of the concepts of this document.....	39
	Annex B (informative) Safety for artificial intelligence (AI) – Application to automated driving systems.....	48
	Annex C (informative) List of related standards.....	65
	Annex D (informative) Safety principles for ADS.....	69
	Annex E (informative) Safety strategy example solutions.....	73
	Annex F (informative) Safety by design and verification example solutions.....	98
	Annex G (informative) Validation example solutions.....	129

Annex H (informative) Verification and validation example solutions	136
Bibliography	152

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 22, *Road vehicles*, Subcommittee SC 32, *Electrical and electronic components and general system aspects*.

This first edition cancels and replaces the first edition (ISO/TR 4804:2020), which has been technically revised.

The main changes are as follows:

- a fully revised scope;
- the inclusion of objectives and requirements for normative clauses of the document;
- a revised presentation of the overarching safety strategy applicable to ADS development (including the addition of clarifications on assumptions and requirements that are to be allocated externally to the ADS);
- connections to cybersecurity concerns; and
- a revision of annexes with example applications and further considerations of artificial intelligence safety.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Licensing and use terms

The ISO publications, as well as any updates and/or corrections, and any intellectual property or other rights pertaining thereto, are owned by ISO. ISO publications are licensed, not sold. Nothing in this document shall operate to assign or transfer any intellectual property rights from ISO to the user. The ISO publications are protected by copyright law, database law, trademark law, unfair competition law, trade secrecy law, or any other applicable law, as the case may be. Users acknowledge and agree to respect ISO's intellectual property rights in the ISO publications.

The use of ISO publications is subject to the terms and conditions of the applicable licensing agreement.

ISO publications are provided under different licensing agreement types (“License Type”) allowing a non-exclusive, non-transferable, limited, revocable right to use/access the ISO publications for one or more of the following purposes described below (“Purpose”), which may be internal or external in scope. The applicable Purpose(s) must be captured in the licensing agreement.

a) License Type:

- i. a single registered end-user license (watermarked in the user’s name) for the specified Purpose. Under this license the user cannot share the ISO Publication with anyone, including on a network;
- ii. a network license for the specified Purpose. The network license may be assigned to either unnamed concurrent end-users or named concurrent end-users within the same organization.

b) Purpose:

- i. Internal Purpose: internal use only within user’s organization, including but not limited to own implementation (“Internal Purpose”).

The scope of permitted internal use is specified at the time of purchase or through subsequent agreement with ISO, the ISO member body in the user’s country, any other ISO member body or an authorized third-party distributor, including any applicable internal reproduction rights (such as internal meetings, internal training programs, preparation of certification services, integration or illustration in internal manuals, internal training materials, and internal guidance documents). Each internal use must be explicitly specified in the purchase order, and specific fees and requirements will apply to each permitted use.

- ii. External Purpose: external use, including but not limited to:

- testing services
- inspection services
- certification services
- auditing services
- consulting services
- training services
- software development and other digital platform or software-enabled digital services; and

any other services or activities conducted by the user or users’ organization to third parties, whether for commercial or non-commercial purposes (“External Purpose”).

The scope of permitted external use is specified at the time of purchase or through subsequent agreement with ISO, the ISO member body in user’s country, any other ISO member body or an authorized third-party distributor, including any applicable external reproduction rights (e.g. in publications, products, or services marketed and sold by user/user’s organization). Each external use must be explicitly specified in the purchase order, and specific fees and requirements will apply to each permitted use.

Unless users have been granted reproduction rights according to the above provisions, they are not granted the right to share or sub-license the ISO publications in- or outside their organization for either Purpose. If users wish to obtain additional reproduction rights for ISO publications or their content, users may contact ISO or the ISO member body in their country to explore their options.

In case the user or the user’s organization is granted a license for the External Purpose of providing any of the following services to third parties:

- testing services
- inspection services
- certification services

- auditing services
- consulting services

the user or user's organization agrees to verify that the third party receiving such services has obtained a license for its own implementation of the ISO Standard being used from the ISO member body in their country, any other ISO member body, ISO or an authorized third-party distributor. This verification obligation shall be included in the applicable license agreement obtained by the user or user's organization.

The ISO publications shall not be disclosed to third parties, and Users shall use them solely for the purpose specified in the purchase order and/or applicable licensing agreement. Unauthorized disclosure or use of ISO publications beyond the licensed purpose is prohibited and may result in legal action.

Use restrictions

Except as provided for in the applicable License Agreement and subject to a separate license by ISO, the ISO member body in user's country, any other ISO member body or an authorized third-party distributor, users are not granted the right to:

- use the ISO Publications for any purpose other than the Purpose;
- grant use or access rights to the ISO Publications beyond the License Type;
- disclose the ISO Publications beyond the intended Purpose and/or License Type;
- sell, lend, lease, reproduce, distribute, import/export or otherwise commercially exploit ISO Publication(s). In the case of joint standards (such as ISO/IEC standards), this clause shall apply to the respective joint copyright ownership;
- assign or otherwise transfer ownership of the ISO Publications, in whole or in fragments, to any third party.

Regardless of the License Type or Purpose for which users are granted access and use rights for ISO publications, users are not permitted to access or use any ISO publications, in whole or in fragments, for any machine learning and/or artificial intelligence and/or similar purposes, including but not limited to accessing or using them (i) as training data for large language or similar models, or (ii) for prompting or otherwise enabling artificial intelligence or similar tools to generate responses. Such use is only permitted if expressly authorized through a specific license agreement by the ISO member body in the requester's country, another ISO member body, or ISO. Requests for such authorization may be considered on a case-by-case basis to ensure compliance with intellectual property rights. For the avoidance of doubt, you cannot claim the benefit of copyright exception of Article 4 of the Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market, for the purpose of text and data mining on ISO Publications, as ISO hereby opts out of this exception.

If ISO, or the ISO member body in the user's country, has reasonable doubt that users are not compliant with these terms, it may request in writing to perform an audit, or have an audit performed by a third-party auditor, during business hours at user's premises or via remote access.

Introduction

Automated driving is one of the key emerging technologies for road vehicles, where major goals in deploying automated driving systems (ADS) include the societal benefits due to broader access to mobility and the reduction of human driver related crashes. Successful deployment is contingent upon ensuring safety of the ADS. This document presents guidance and requirements for achieving safety through the ADS development, including design, verification and validation, as well as operation post deployment.

The successful design and deployment of the ADS can involve a variety of stakeholders, from technology, component, and subsystem suppliers to system integrators and vehicle OEMs, as well as transportation service providers and regulatory bodies; this document is intended to be used by all those involved.

Road vehicles — Safety for automated driving systems — Design, verification and validation

1 Scope

This document provides guidance for achieving and demonstrating safety of an automated driving system (ADS) integrated in a road vehicle. The approach is based on safety principles derived from worldwide applicable publications and top-level safety objectives. It considers safety by design, verification and validation, and post deployment activities for level 3 and level 4 ADS features defined according to ISO/SAE PAS 22736^[2]. In addition, it outlines cybersecurity considerations.

The application of this document is intended for road vehicles, including trucks and buses and excluding motorcycles and mopeds.

Any ADS or related elements that are in operation, or under development, prior to the publication of this document are exempted from the application of this document.

NOTE While not covered in this document, safety during development activities is a key consideration. Development includes activities of design, verification and validation.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

3.1 Human-related terms

3.1.1

road user

traffic participant on, or adjacent to, an active roadway

Note 1 to entry: Persons operating an *automated driving system (ADS)* (3.2) remotely are considered as persons adjacent to the road.

Note 2 to entry: [Figure 1](#) provides an overview how terms are hierarchically defined, e.g. a *driver* (3.1.3) is a specific *user* (3.1.2).

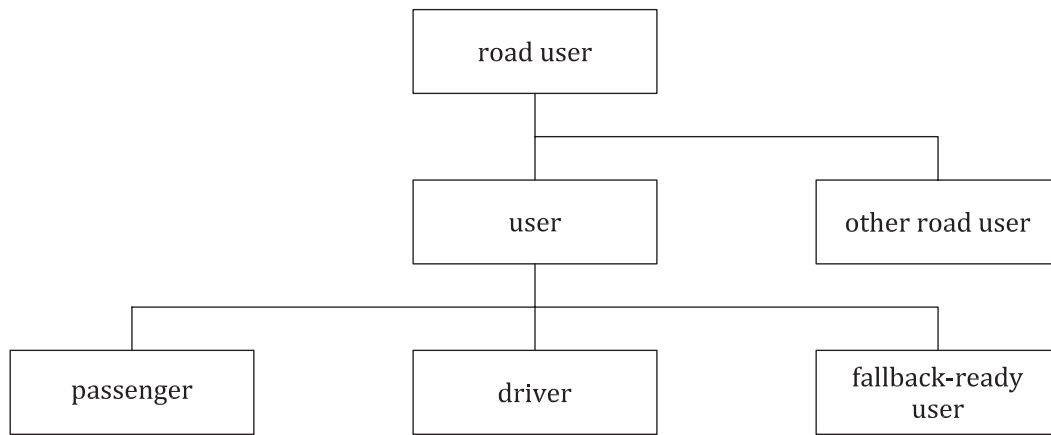


Figure 1 — Structure of human-related terms

[SOURCE: SAE J3216:2021, 4.13.1, modified — "for the purpose of travelling" has been deleted and the notes to entry and Figure 1 were added.]

3.1.2

user

ADS user

road user (3.1.1) who has a role with regard to the subject *automated driving system (ADS)*- (3.2) equipped vehicle

Note 1 to entry: A user can either be a *driver* (3.1.3), or a *passenger* (3.1.4), or a *fallback-ready user* (3.1.5). These roles do not overlap and may be performed in varying sequences during a given trip. An example can be found in A.6.

3.1.3

driver

user (3.1.2) who performs in real-time part or all of the DDT or the *DDT fallback* (3.11) to operate a particular vehicle

EXAMPLE Person with a driving licence who operates the vehicle.

Note 1 to entry: Consistent with Reference [4] the term "operator" can be used instead of driver if the vehicle's operation requires special training and authorization.

[SOURCE: ISO/SAE PAS 22736:2021, 3.31.1, modified — "To operate" has been added, Note was replaced by Note1 to entry and the example was added.]

3.1.4

passenger

user (3.1.2) in a vehicle who has no role in the operation of that vehicle

EXAMPLE 1 The person seated in the driver's seat of a vehicle equipped with a level 4 *ADS feature* (3.3) designed to automate high-speed vehicle operation on access-controlled freeways is a passenger while this level 4 ADS feature is engaged. This same person, however, is a *driver* (3.1.3) before engaging this level 4 ADS feature and again after disengaging the feature in order to exit the controlled access freeway.

EXAMPLE 2 The users of an L4 *automated driving system (ADS)*- (3.2) equipped vehicle are passengers whenever the L4 ADS feature is engaged.

[SOURCE: ISO/SAE PAS 22736:2021, 3.31.2, modified — Examples 2 and 3 have been removed, a new example 2 has been added.]

3.1.5

fallback-ready user

user (3.1.2) of an engaged level 3 *ADS feature* (3.3) who is properly qualified and able to operate the vehicle and is receptive to ADS-issued requests to intervene and to evident DDT performance-relevant system *failures* (3.12) in the vehicle compelling him or her to perform the *DDT fallback* (3.11)

[SOURCE: ISO/SAE PAS 22736:2021, 3.31.3, modified — 'of a vehicle equipped' has been deleted after "user" and the notes have also been removed.]

3.1.6

other road user

road user (3.1.1) who has no role with regard to the subject *automated driving system (ADS)*- (3.2) equipped vehicle

Note 1 to entry: The other road user can also be a *user* (3.1.2) of another ADS-equipped vehicle.

Note 2 to entry: Other road users can affect what the subject ADS-equipped vehicle will do, but the subject automated driving system decides what to do.

3.2

automated driving system

ADS

hardware and software that are collectively capable of performing the entire *dynamic driving task(DDT)* (3.10) on a sustained basis, regardless of whether or not it is limited to a specific *operational design domain (ODD)* (3.20)

Note 1 to entry: An ADS can consist of on-board and/or off-board elements.

Note 2 to entry: This term is used specifically to describe an L3 or L4 driving automation system.

[SOURCE: ISO/SAE PAS 22736:2021, 3.2, modified — Note has been deleted and replaced by Note 1 to entry, Note 2 to entry was previously a modified portion of the definition.]

3.3

ADS feature

ADS (3.2)'s design-specific functionality at a given level of driving automation within a particular *operational design domain (ODD)* (3.20), if applicable

EXAMPLE Highway pilot, automated valet parking.

Note 1 to entry: A given ADS can have multiple ADS features, each associated with a particular level of driving automation and *dynamic driving task(DDT)* (3.10) specification.

3.4

ADS safety case

structured argument, supported by evidence, that provides a compelling, comprehensible and valid claim that the *automated driving system (ADS)*- (3.2) equipped vehicle has been developed to achieve *safety* (3.24) for a given *ADS feature* (3.3) in a given environment

Note 1 to entry: Including intentional and unintentional *reasonably foreseeable* (3.21) engagement or disengagement sequences.

Note 2 to entry: Adapted from Reference [5], 13.2.1.

3.5

availability

capability to continue to provide a stated function under given conditions once the function is active

Note 1 to entry: In the context of this document, availability is defined solely referring to the *automated driving system (ADS)* (3.2) aspects and does not include human factor aspects.

Note 2 to entry: Adapted from ISO 26262-1:2018, 3.7.

3.6

conflict

situation where the trajectory of one or more *road users* (3.1.1), *other road user* (3.1.6) or objects lead to an *incident* (3.16)

3.7

crash

situation in which the subject *automated driving system (ADS)*- (3.2) equipped vehicle has any contact with at least one other conflict partner either on or off the trafficway, either moving or stationary (fixed or non-fixed), that is observable or in which kinetic energy is measurably transferred or dissipated

[SOURCE: ISO/TR 21974-1:2018, 3.4, modified — Added "ADS-equipped" and deleted notes to entry.]

3.8

cybersecurity

condition in which assets are sufficiently protected against threat scenarios to the *automated driving system (ADS)* (3.2) of road vehicles, their functions and their electrical or electronic components

Note 1 to entry: This can include considerations of malicious modifications to the driving environment.

[SOURCE: ISO/SAE 21434:2021, 3.1.9, modified — "item" was replaced by "ADS" and the Note 1 to entry was replaced.]

3.9

dual-mode vehicle

automated driving system (ADS)- (3.2) equipped vehicle designed to enable either driverless operation or operation by an *in-vehicle driver*

[SOURCE: ISO/SAE PAS 22736:2021, 3.32.2, modified — "under routine/normal operating conditions within its given ODD", "for complete trips" and Notes were deleted.]

3.10

dynamic driving task

DDT

all of the real-time operational and tactical functions required to operate a vehicle in on-road traffic

Note 1 to entry: This excludes the strategic functions such as trip scheduling and selecting destinations and waypoints, and includes without limitation:

- lateral vehicle motion control via steering (operational);
- longitudinal vehicle motion control via acceleration and deceleration (operational);
- monitoring the driving environment via object and event detection, recognition, classification, and response preparation (operational and tactical);
- object and event response execution (operational and tactical);
- manoeuvre planning (tactical); and
- enhancing conspicuity via lighting, signalling or gesturing, etc. (tactical).

[SOURCE: ISO/SAE PAS 22736:2021, 3.10, modified — Note 1 to entry was previously part of the definition and notes and figures were deleted.]

3.11

DDT fallback

response by the *user* (3.1.2) to either perform the *dynamic driving task (DDT)* (3.10) or achieve a *minimal risk condition (MRC)* (1) (3.17) after occurrence of DDT performance-relevant system *failures* (3.12), or (2) upon *operational design domain (ODD)* (3.20) exit, or the response by an *automated driving system (ADS)* (3.2) to achieve an MRC, given the same circumstances

[SOURCE: ISO/SAE PAS 22736:2021, 3.12, modified — Notes, examples and figures were deleted.]

3.12
failure

deviation from an intended behaviour of the *automated driving system (ADS)* (3.2) due to a *fault* (3.13) manifestation

[SOURCE: ISO 26262-1:2018, 3.50, modified — "item and element" was replaced by "ADS", "termination of" was replaced by "deviation from" and Note 1 to entry was deleted.]

3.13
fault

abnormal condition that can cause the *automated driving system (ADS)* (3.2) to fail

[SOURCE: ISO 26262-1:2018, 3.54, modified — "item and element" was replaced by "ADS" and Notes to entry were deleted.]

3.14
harm

physical injury or damage to the health of persons

[SOURCE: ISO 26262-1:2018, 3.74]

3.15
HD map

map with high level precision and/or high level of detail mostly used in the context of the *automated driving system (ADS)* (3.2) to give the ADS precise information about the road environment

3.16
incident

event that could have caused or actually caused *harm* (3.14) or property damage, or an anomaly that has the potential to cause harm or property damage in the future

Note 1 to entry: Incident includes near-miss.

3.17
minimal risk condition

MRC

stable, stopped condition to which a *user* (3.1.2) or an *automated driving system (ADS)* (3.2) may bring a vehicle after performing the *DDT fallback* (3.11) in order to reduce the risk of an *incident* (3.16) when a given trip cannot or should not be continued

Note 1 to entry: The minimal risk condition integrates the meaning of avoidance of *unreasonable risk* (3.26), according to the ISO 26262 series.

[SOURCE: ISO/SAE PAS 22736:2021, 3.16, modified — "crash" replaced by "incident", notes and were deleted.]

3.18
minimal risk manoeuvre

MRM

vehicle movement directed by the *automated driving system (ADS)* (3.2) or by the *fallback-ready user* (3.1.5) during *DDT fallback* (3.11) to achieve a *minimal risk condition (MRC)* (3.17)

3.19
object and event detection and response

OEDR

subtasks of the *dynamic driving task(DDT)* (3.10) that include monitoring the driving environment and executing an appropriate response to such objects and events

[SOURCE: ISO/SAE PAS 22736:2021, 3.19, modified — "(detecting, recognizing, and classifying objects and events and preparing to respond as needed)" and "(i.e., as needed to complete the DDT and/or DDT fallback)". were deleted.]

3.20

operational design domain

ODD

operating conditions under which an *automated driving system (ADS)* (3.2) or feature thereof is specifically designed to function, including, but not limited to, environmental, geographical, and time-of-day restrictions, and/or the requisite presence or absence of certain traffic or roadway characteristics

[SOURCE: ISO/SAE PAS 22736:2021, 3.21, modified — "a given driving automation system" was replaced by "ADS" and all notes and examples were deleted.]

3.21

reasonably foreseeable

technically possible and with a credible or measurable rate of occurrence

Note 1 to entry: Expected misuse can be understood as a subclass of reasonably foreseeable events.

[SOURCE: ISO 26262-1:2018, 3.120]

3.22

risk acceptance criterion

criterion representing the absence of an unreasonable level of risk

EXAMPLE The comparison with an equivalent vehicle-level effect that is proven in use to be controllable by the driver (3.1.3) can support the definition of risk acceptance criteria. For instance, the trajectory perturbation due to an unwanted lane keeping assist function intervention might be compared to a lateral wind gust to define an acceptable level of authority for the function.

Note 1 to entry: The risk acceptance criteria can be of qualitative as well as quantitative nature, e.g. physical parameters that define when a specific behaviour is considered as hazardous behaviour, maximum number of *incidents* (3.16) per hour, as low as reasonably practicable (ALARP).

[SOURCE: ISO 21448:2022, 3.1, modified — The term was originally acceptance criterion and example 1 was removed.]

3.23

safe

free from *unreasonable risk* (3.26)

3.24

safety

absence of *unreasonable risk* (3.26)

[SOURCE: ISO 26262-1:2018, 3.132]

3.25

safety capability

property of an *automated driving system (ADS)* (3.2) needed for *safe* (3.23) operation

Note 1 to entry: Several safety capabilities are needed to ensure safe operation for an ADS.

Note 2 to entry: Safety capabilities are not only defined for the *dynamic driving task(DDT)* (3.10), but also for the *DDT fallback* (3.11) and *post-incident* (3.16) behaviour.

Note 3 to entry: Safety capabilities can be systematical (e.g. behavioural), but also of other types like operational, or organizational.

3.26

unreasonable risk

risk judged to be unacceptable in a certain context according to valid societal moral concepts

[SOURCE: ISO 26262-1:2018, 3.176]

3.27

validation

activities to determine that the operation of the ADS-equipped vehicle achieves *safety* (3.24) for an *ADS feature* (3.3) in the intended environment

Note 1 to entry: The intended environment does not have to be equal to the *operational design domain (ODD)* (3.20).

Note 2 to entry: The term validation in this document is limited to safety; development can include other types of validation.

3.28

verification

activities to determine that an examined object meets its specified safety requirements

[SOURCE: ISO 26262-1:2018, 3.180, modified — "activities to" was added, "whether or not" was deleted and the example was deleted.]

4 Abbreviated terms

L3 level 3

L4 level 4

HMI human machine interface

ITS intelligent transportation system

V&V verification (3.28) and validation (3.27)

VRU vulnerable road user (3.1.1)

5 Document overview and motivation

5.1 Purpose

This clause is intended to provide an overview of, and informative guidance on, the application of this document.

5.2 Overall goals of this document

This document is intended to provide guidance and requirements for developing and operating an ADS that demonstrates achievement of safety through safety by design, verification and validation, and field operation. While it does not define solutions, as these can be unique to the respective developer and application, it provides informative examples of how this can be done in practice.

As part of the overall concept of ADS safe operation, this document incorporates the usage of existing industry standards and best practices, where applicable, to ensure utilization of common industry-wide methods and requirements.

To help guide users of this document in its usage, the (sub-)clause structure is presented in a consistent manner according to the following flow: objectives of the clause, related general information (where applicable), requirements or recommendations, and a summary to linked example solutions or applications.

5.3 Application of this document

The user of this document is assumed to have a relation to safety of an ADS. This document provides guidelines and requirements for the generation of the arguments and evidence needed for developing a safety case fulfilling the requirements of this document. While not described in this document, it can also be applicable for development of ADS or ADS elements, where design, verification and validation are performed

partly before making agreements for a specific delivery, as well as contexts of continuous integration and continuous deployment, (CI/CD).

5.4 Safety life cycle

5.4.1 Purpose

This subclause describes the safety life cycle to provide guidance on the development flow followed in achieving safety, as well as the relationship between relevant clauses in this document.

5.4.2 General

The development and deployment of an ADS and its constituent components will typically follow a regular process flow for product design and deployment. For the purposes of this document this process flow is represented as a V-model safety life cycle, where the left-side leg encompasses the product design development, and the right-side leg encompasses evaluation and deployment. In practice, different components and models are deployed using multiple life cycles and more iterative processes.

[Figure 2](#) shows the V-model safety life cycle with the associated clauses in this document. The safety life cycle V-model in [Figure 2](#) allows stakeholders to visualize the ADS safety development flow, including the relation between clauses, as well as between clauses and phases of development.

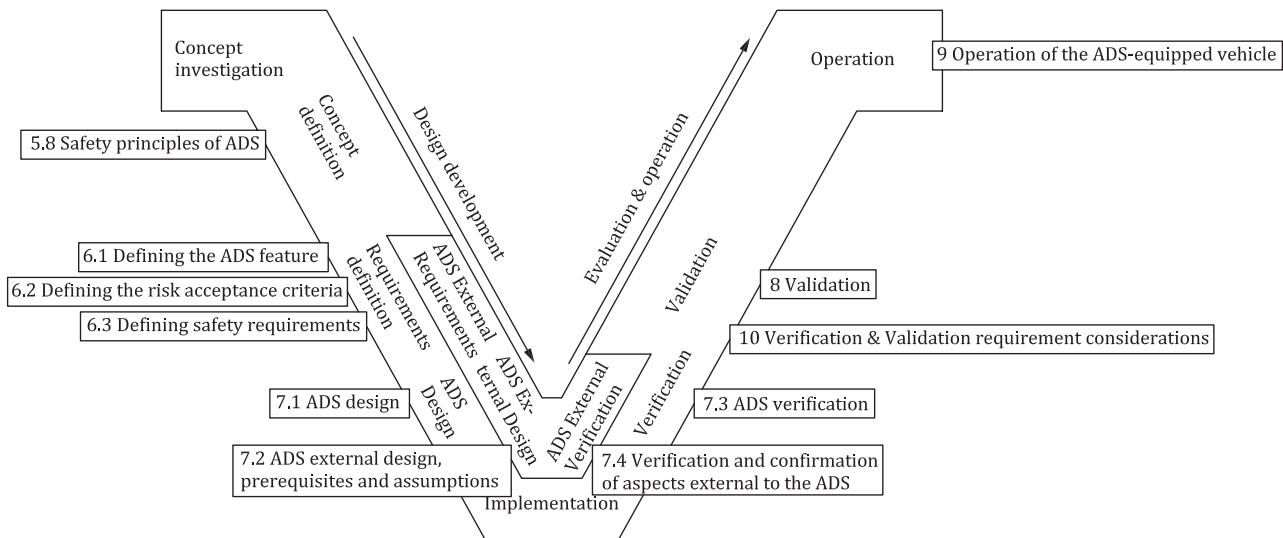


Figure 2 — ADS safety life cycle V-model

5.5 Description of ADS safety case

5.5.1 Purpose

This subclause provides a description of how an ADS safety case can be developed, and how this document can contribute to that. This subclause also highlights how this document can guide the structure of the ADS safety case, through argumentation and evidence, in support of the claims made to demonstrate safe operation of the ADS-equipped vehicle.

5.5.2 General

This document provides guidance for structuring an ADS safety case. The ADS safety case can be made by fulfilling the normative requirements of [Clauses 6](#) through [9](#) and incorporating argumentation and evidence according to other documents. The normative contents of this document constrain its contribution to the ADS safety case in two dimensions. The first dimension can be illustrated by a layered model, whereas this document only contributes to the inner layers as shown in [Figure 4](#). This is elaborated below together with

a description of how the normative content of this document corresponds to the layered model. The second dimension can be understood by considering the ADS feature from the perspective of the ADS-equipped vehicle as explained in 5.5.4.

5.5.3 How this document supports a layered structure of an ADS safety case

The evidence generated by considering of the subclauses of this document, together with those from other standards, allow different types of assurance claims to be made regarding the ADS feature. The evidence supporting these types of assurance claim can be conceptualised using a layered model as shown in Figure 3 and are described in more detail below.

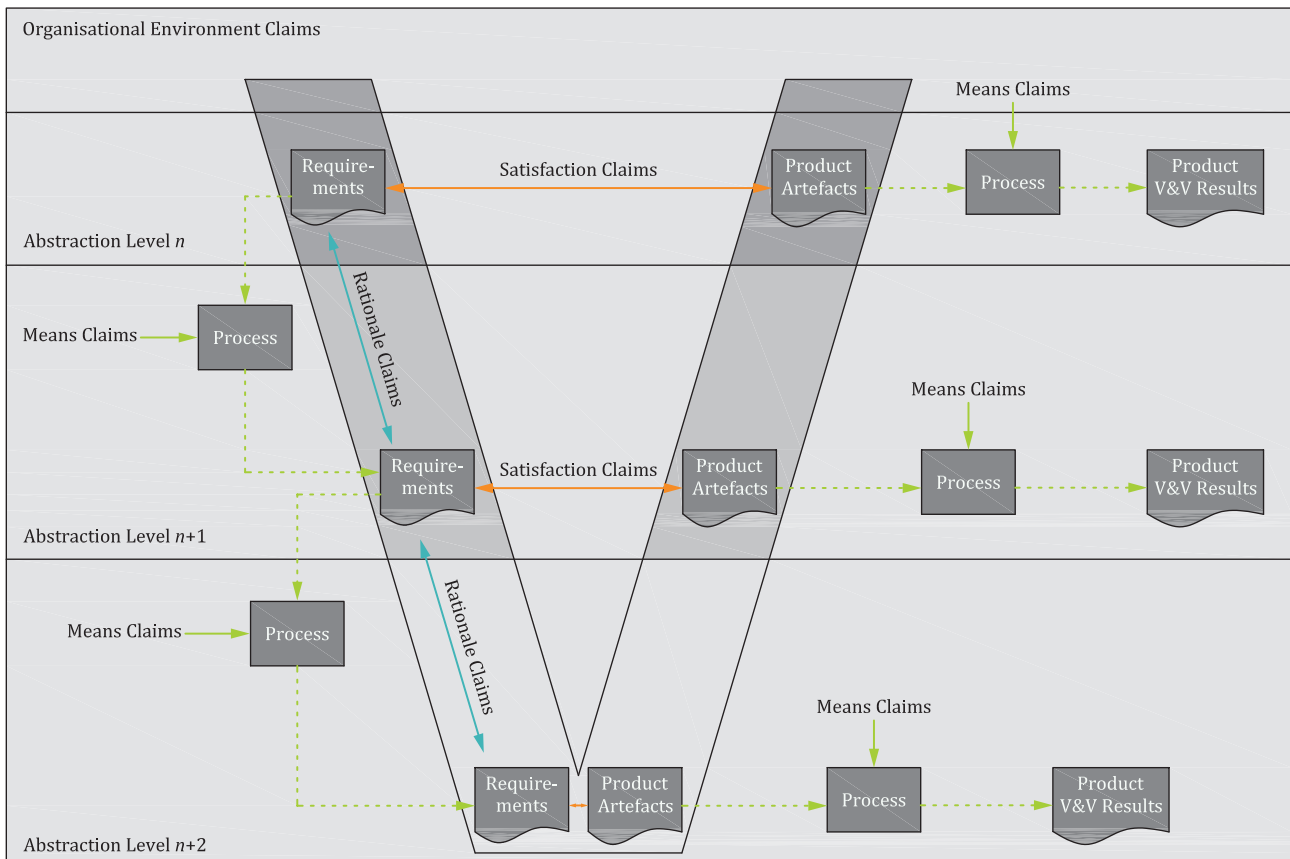


Figure 3 — Safety argumentation pattern^[12]

The layered model provides a useful example of how an ADS safety case could be constructed, through the use of four types of claims described as follows:

— Rationale claims

These are claims related to the technical adequacy of the safety requirements and the basis for these requirements being appropriate.

EXAMPLE 1 “The safety requirements allocated to sensor X call for behaviour that sufficiently and correctly fulfils the requirements of the role that the sensor plays in the overall ADS safety concept.”

— Satisfaction claims

These are claims related to the relationship between the safety requirements and the corresponding product artefacts, such as systems, hardware or software. These are the claims resulting from establishing traceability between left side of the V life cycle model and right side of the V life cycle model as shown in

[Figure 3](#). Note that the satisfaction claims are to cover all assumptions, prerequisites, or requirements external to the ADS.

EXAMPLE 2 “Sensor X fully satisfies the behaviour called for by the safety requirements allocated to it.”

— Means claims

These are claims related to the methods (such as the people, process or tools) used to perform a specific safety-related activity during development.

EXAMPLE 3 “An independent review has successfully been undertaken of the test cases developed to demonstrate that sensor X satisfies the safety requirements allocated to it.”

— Organisational environment claims

These are claims related to the organisational context in which the safety-related activities have been carried out.

EXAMPLE 4 “The department in which the test cases for sensor X were developed has been successfully audited against the requirements of standard Y.”

These four types of claims are depicted in the layered safety argument model shown in [Figure 4](#).

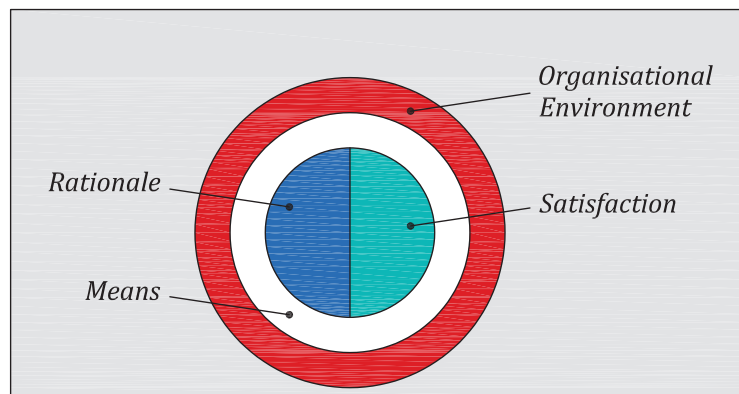


Figure 4 — Layered safety argument model^[12]

The general pattern of [Figure 3](#) can be used to depict the clauses of this document as seen below in [Figure 5](#).

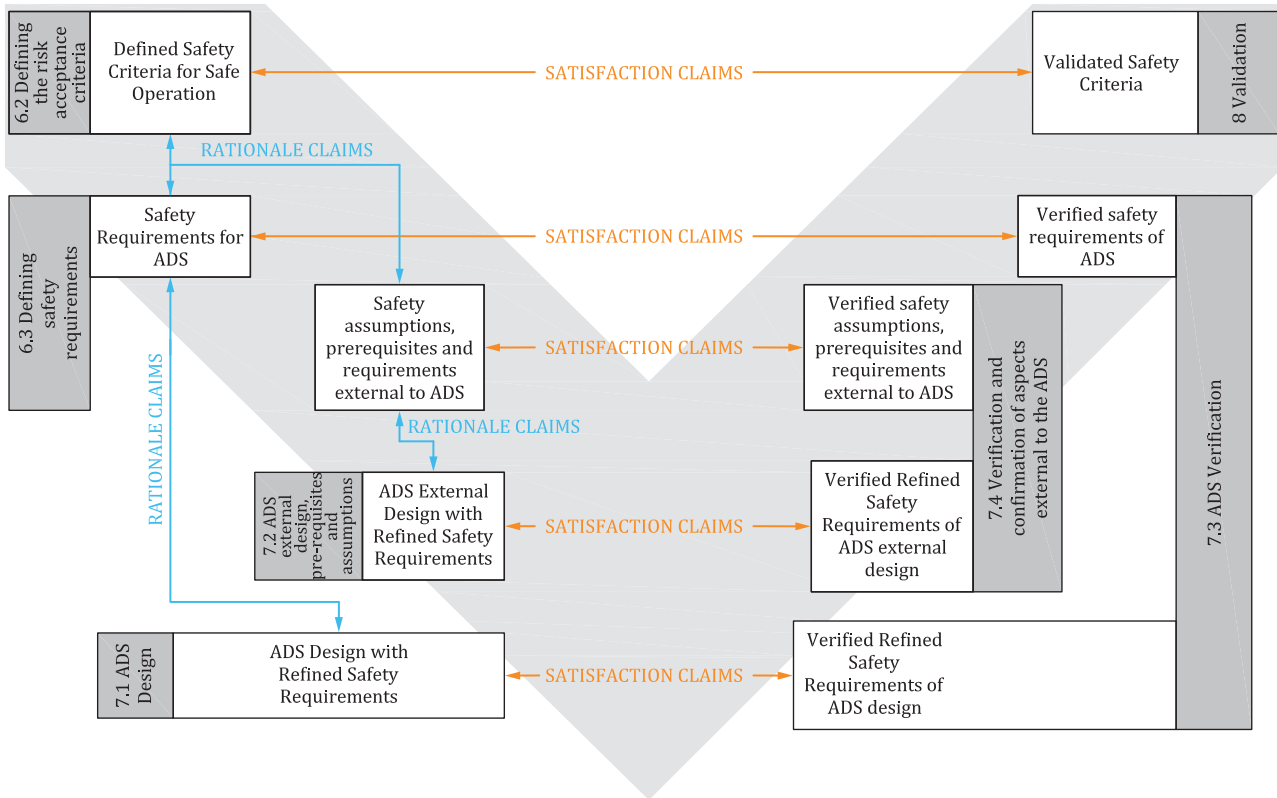


Figure 5 — Layered safety argument structure of this document

The rationale and satisfaction claim types occupy the core of the argument model. These are the claim types to which the content of this document relates. The means claim type is depicted as providing a surrounding layer of confidence to the core of the argument, which is then further supported by the organisational environment layer. The latter two claim types are related to the process used and followed in developing the product, and typically these will relate to the content of other standards (e.g. the ISO 26262 series), further described in [5.7](#).

All four claim types provide an important and unique contribution to the development of a compelling, consistent and holistic safety argumentation. Note, however, that the means and organisational environment claim types are intrinsically linked to, and dependent on, the core of the argument that they support. This, then yields a corresponding dependency between safety claims related to the content of this and other standards in the development of an ADS safety argumentation.

The normative requirements in the subclauses of this document provide a structure that can be used to support the development of a sufficient set of rationale claims together with satisfaction claims. Fulfilling the normative requirements of this document achieves an appropriate rationale safety claim structure. Furthermore, the normative part of this document, requires the user of this document to formulate all the refinement steps such that they all are verifiable, which means to be possible to create a corresponding satisfaction argument. The rationale and satisfaction structures are covered by the subclause structures in [Clauses 6](#) through [9](#), and the corresponding normative requirements.

The informative subclauses in this document, following normative subclauses, provide examples of how to generate rationale and satisfaction argument strands, as well as suggested references to other standards that could be considered in developing those related to means and organizational environment.

5.5.4 Perspective from the ADS-equipped vehicle

When considering the structure of an ADS safety case, the different operating situations experienced by the ADS-equipped vehicle can be taken into account, including:

- a) ADS-operated vehicle;

- b) human-operated ADS-equipped vehicle;
- c) ADS-equipped vehicle not being operated.

NOTE The transition between ADS-operated vehicle and human-operated ADS-equipped vehicle, and the ADS feature achieving MRC, are intended to be part of an ADS-operated vehicle.

This document mainly focuses on the first aspect, a). The main difference of ADS compared to ADAS and other vehicle technologies is the fact that the entire DDT (and DDT fallback for L4 ADS feature) are performed by the ADS, therefore the user is assumed not to be involved in the DDT. This difference mainly appears in the risk acceptance criteria and the associated measures to reduce the risk to an acceptable level without human involvement to a certain extent. [5.6](#) provides further information.

Considerations for b) human operated ADS-equipped vehicles can be considered as an extension of existing ADAS and not specific to ADS. For example, hazards such as unintended activation of vehicle control actuators can be considered to be common between ADS and ADAS while the driver is operating the vehicle. Therefore, this factor is not the focus of this document and ISO 21448, ISO/SAE 21434 and the ISO 26262 series can be referenced depending on the cause of the hazard.

Considerations for c) ADS-equipped vehicle not being operated could be valid in case the ADS feature consists of functions or interfaces to activate the powertrain of the ADS-equipped vehicle. However, since this is a design specific factor, it is not directly addressed in this document, ISO 21448, ISO/SAE 21434 and the ISO 26262 series can be referenced depending on the cause of the hazard.

5.6 Role of the ADS within safe vehicle operation

5.6.1 Purpose

This subclause identifies the role of the ADS within safe vehicle operation according to the following dependencies:

- a) task dependency ([5.6.3](#)); and
- b) time dependency ([5.6.4](#)).

5.6.2 General

ADS safety is demonstrated by safe operation of the ADS-equipped vehicle. Safe operation includes safety of the users of the ADS-operated vehicle and other road users.

However, safe operation of the ADS-equipped vehicle cannot be realized without the contribution of tasks or aspects external to the ADS (for examples, see [Figure 6](#)). [5.6.3](#) describes the aspects that contribute to safe operation of the ADS-equipped vehicle in order to identify the task dependencies for which the ADS has its role in safe vehicle operation.

ADS sub-trip feature equipped vehicles and dual-mode vehicles can be operated by the ADS or human drivers. [5.6.4](#) outlines the time dependency aspects for which the ADS has its role in safe vehicle operation.

5.6.3 Task dependency of ADS safety

The ADS, by definition, is comprised of hardware and software collectively capable of performing the entire DDT on a sustained basis. Therefore, the role of the ADS within safe vehicle operation, from a task perspective, will apply to the DDT as well as the DDT fallback for L4 ADS features.

Tasks or aspects other than the DDT (such as those examples shown in [Figure 6](#) and the respective clauses), which contribute to safe vehicle operation, can be considered external to the ADS.

NOTE This document does not employ the terminology “vehicle-level”. This is because ADS features can include off board elements that are physically located outside of the vehicle.

EXAMPLE Automated valet parking systems (see ISO 23374-1) as a level 4 ADS feature, distributes its DDT relevant elements between the subject vehicle and parking facility equipment. Such parking facility equipment is typically installed onto the walls and ceilings of the parking facility and can perform part or all of the OEDR, depending on the design choice.

Depending on the task dependencies for a given ADS feature, absence of these ADS external tasks/aspects can result in unsafe vehicle operation. Therefore, the ADS is expected to determine if safe operation is possible by actively monitoring these ADS external tasks or aspects, and to actively monitor the driving environment relative to its ODD.

This document focuses on the development of the ADS. This document also provides guidance on allocation of safety-related tasks/aspects external to the ADS, but does not provide detail on how to realize those ADS external elements.

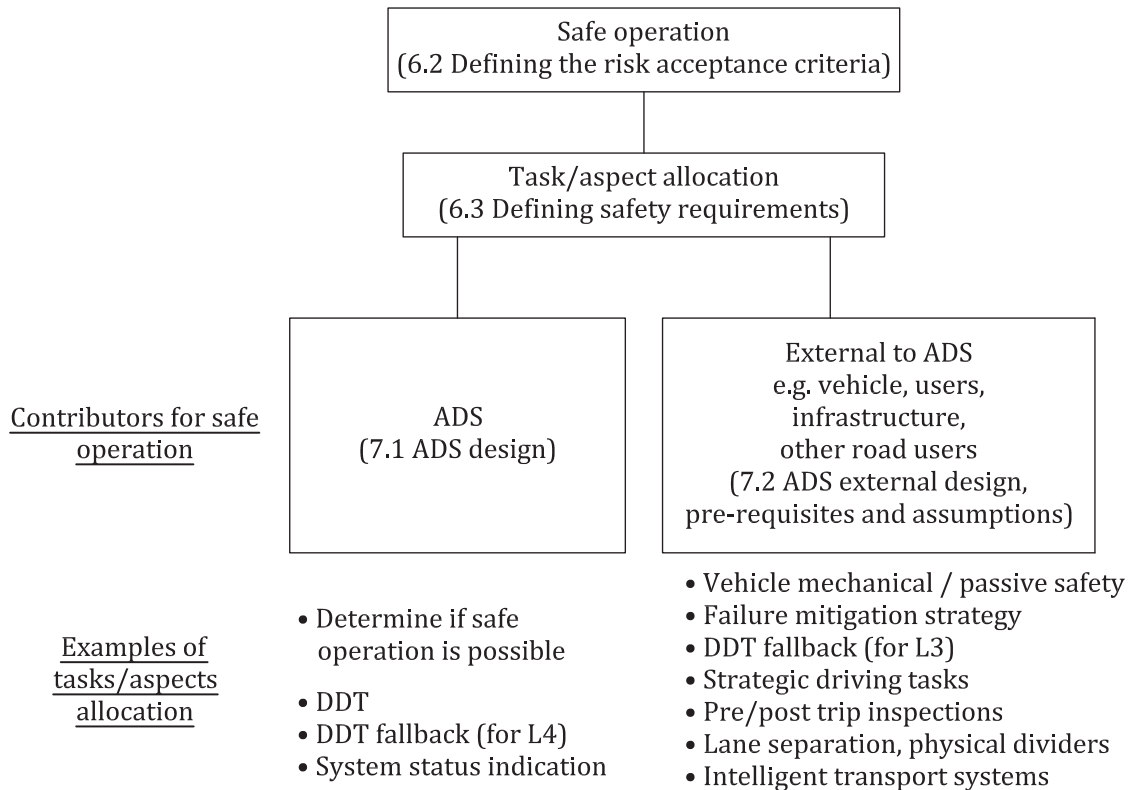


Figure 6 — Contributors and examples of tasks/aspects allocation for safe operation of an ADS-equipped vehicle

5.6.4 Time dependency of ADS safety

ADS sub-trip feature equipped vehicles and dual-mode vehicles can be operated by the ADS or manually by a human driver. Regardless of the different types of configurations of ADS-equipped vehicles (e.g. either dedicated for ADS operation or not), the ADS will perform the entire DDT when an ADS feature is engaged. Therefore, the role of the ADS within safe vehicle operation applies to the time between engagement and disengagement of the ADS feature as illustrated in [Figure 7](#). The risk acceptance criteria defined in [6.2](#), then, applies during this time frame. The ADS does not have a role within safe vehicle operation under conditions where no ADS feature is engaged, and therefore not operating the ADS-equipped vehicle.

From a time-dependency perspective, the following considerations are necessary to argue ADS safety.

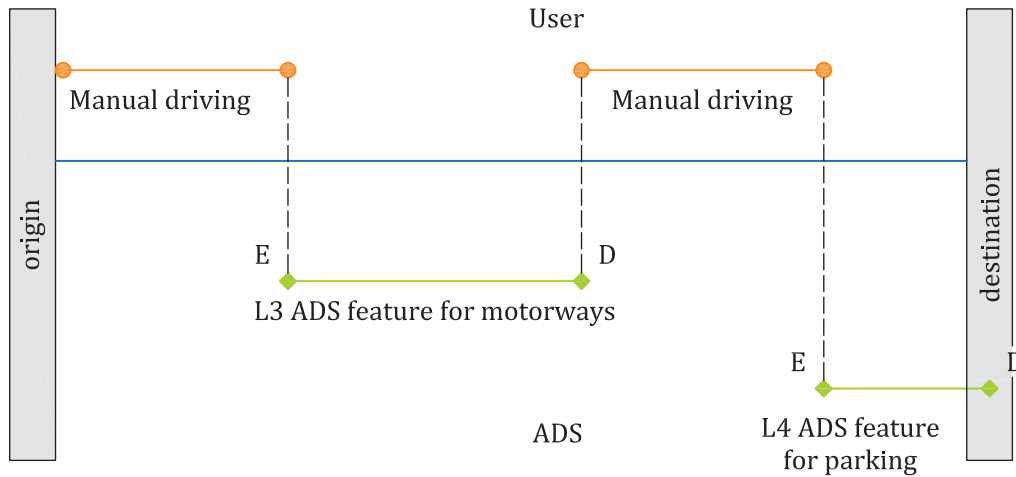
- When an ADS feature is requested to be engaged, the ADS feature determines if safe operation of the ADS-equipped vehicle can be initiated before starting to perform the DDT.
- While the ADS feature is engaged, the ADS determines if safe operation can be continued, staying inside its ODD.

— The ADS feature disengages in an appropriate way and stops performing the DDT.

NOTE 1 The ADS-equipped vehicle reaches the intended destination and the ADS is deactivated¹⁾ (e.g. upon the successful completion of a trip).

NOTE 2 For L3 ADS features, the feature disengages upon: 1) confirming the fallback ready user is performing or ready to perform the DDT; or 2) issuing a request to intervene to the fallback ready user while continuing to perform the DDT for a reasonable amount of time (see also 5.6.5.1).

NOTE 3 For L4 ADS features, the feature disengages upon: 1) achieving a minimal risk condition; or 2) confirming that a driver is beginning to perform the DDT.



Key

E engagement
D disengagement

Figure 7 — Time dependency for safe operation of an ADS-equipped vehicle

5.6.5 Examples

5.6.5.1 Role of the ADS within safe vehicle operation by an L3 ADS feature

The ADS, by definition, performs the entire DDT while an L3 ADS feature is engaged, but in general, is not required to perform the DDT fallback. From a task dependency viewpoint, the role of the ADS within safe vehicle operation is applied to the DDT, and the fallback ready user has the task to perform the DDT fallback. Having issued a request to intervene the ADS can stop performing the DDT under certain conditions. For these reasons, the role of the ADS can end regardless of the fallback ready user's response. So from a time perspective, both the task and the time dependencies for a L3 ADS feature can change.

To address such a situation where neither the ADS nor human is operating the vehicle, the vehicle is expected to have a task to mitigate the risk of crashes to support the fallback ready user in the event they do not respond adequately to the request to intervene. Such a situation can be considered as part of safe operation of the L3 ADS-equipped vehicle, but not subject to the role of the ADS itself for L3 ADS features.

NOTE An L3 ADS feature can be designed to reach an MRC under certain conditions.

5.6.5.2 Role of the ADS within safe vehicle operation for an L4 ADS feature

The ADS, by definition, performs both the DDT and DDT fallback while an L4 ADS feature is engaged. The ADS will achieve an MRC in the event that normal operation cannot be continued. Once an MRC is achieved, the L4 ADS feature disengages from both the task and time dependencies.

1) Within this explanation, it is assumed that an ADS feature can be engaged/disengaged when the ADS is activated. If the ADS is deactivated, the ADS feature will be disengaged accordingly.

Tasks to maintain safety of the L4 ADS feature disengaged vehicle can be performed external to the ADS. Tasks to maintain the ADS-equipped vehicle at its stopped location can be allocated to the vehicle. Tasks in response to changes in the environment after reaching an MRC (e.g. moving the ADS-equipped vehicle to a different location due to change in traffic conditions) might be allocated to the users of the ADS or other supporting personnel or entities.

5.7 Application of other standards

5.7.1 Purpose

This subclause describes the general use of other standards in this document. The aim of this subclause is, therefore, to identify the relationship between different types of standards and how these standards could be applied to facilitate the achievement and demonstration of safety of the ADS.

5.7.2 Classification of standards

5.7.2.1 General

The clustering of documents into classes with similar scope of application is intended to facilitate the understanding and the general use of standards in this document.

For the purpose of this document, related standards have been organized under the classifications of: base documents, generic ADS documents and specific ADS documents. This clause provides guidance on the application of standardization documents in terms of their contribution to achieving safety for ADS.

A detailed overview of the standards and specifications related to safety of automated driving systems can be found in [Annex C](#).

5.7.2.2 Base documents

This document class contains standards that were not developed specifically for ADS, but which are intended to be applied to any hardware (HW) and software (SW) based functionality in the automotive industry to reduce the risks as described in their corresponding scopes. This document class consists of standards such as engineering, test equipment, HMI and simulation related requirements not only applicable to ADS.

EXAMPLE The ISO 26262 series on functional safety, ISO 21448 on safety of the intended functionality, and ISO/SAE 21434 on cybersecurity engineering.

The ISO 26262 series is intended to be applied to safety-related systems that include electrical and/or electronic (E/E) systems installed in road vehicles. The ISO 26262 series addresses possible hazards caused by malfunctioning behaviour of safety-related E/E systems, including interaction of these systems. The integration of functional safety activities into a company-specific development framework is intended to support the development of safety-related E/E systems and contributes to the overall goal of ensuring that the risk is low enough to achieve safety of an ADS.

This automotive-specific risk-based approach determines and communicates and/or maps risks through the use of automotive safety integrity levels (ASIL). These ASILs indicate which of the requirements of the ISO 26262 series are applicable to avoid unreasonable residual risk. The approach proposed by this document will not attempt to directly trace and decompose ASIL values in a traditional application of functional safety.

The basic concept of ISO 21448 is to provide a general argumentation framework and guidance on measures to ensure the safety of the intended functionality that includes analyses, verification and validation. This approach leads to an intended functionality that contributes to the demonstration of safety. Application of this standard results in several activities, that together contributes with evidence and arguments towards the development of a safe automated driving system. This approach classifies scenarios in four different areas. These four areas are differentiated between known and unknown scenarios and whether hazardous behaviour can occur in these scenarios or not. The objective of ISO 21448 is to reduce the impact of known potentially harmful scenarios as well as to reduce the amount of unknown hazardous scenarios to a minimum meeting the defined risk acceptance criteria.

ISO/SAE 21434 focuses on the risks represented by unauthorized actions, including those by active adversaries. This requires the use of additional engineering activities and technical mechanisms that can nevertheless also affect safety. ISO/SAE 21434 describes the cybersecurity activities, including those for a secure development process, with a special focus on risk management. For automated driving systems, ISO/SAE 21434 is, therefore, fully applicable. However, while using a certain risk approach, it is important to think about specifics of automated driving.

One dimension of a cybersecurity risk is the impact of a damage scenario that could be realized by an attack. Here, there are also differences between human controlled driver assistance functions and system controlled automated driving functions. ISO/SAE 21434 requires monitoring of cybersecurity threat information, events, vulnerabilities and incidents to address potential cybersecurity attacks. Such cybersecurity threats have the potential to impact both human controlled driver assistance and system controlled automated driving functions. Approaches to use the safety analysis results as input for cybersecurity analysis, can be found in ISO/SAE 21434:2021, Clause 15.

In short, we have advanced to a level where vehicles cannot maintain an MRC unless they also operate securely. Most importantly, the cybersecurity activities of ISO/SAE 21434 are applied as a starting point to ensure that, for example, attackers cannot gain control of a vehicle's movement, and that attacks are difficult to scale to the level of simultaneously exploiting multiple vehicles.

5.7.2.3 Generic ADS documents

The content of this document class is limited to automated driving systems, with the requirements therein being applicable to all types of automated driving systems. This document class consists of standards such as taxonomies, testing, and ADS safety related requirements applicable to all types of ADS.

EXAMPLE 1 ISO/SAE PAS 22736.

EXAMPLE 2 ISO 23793-1.

EXAMPLE 3 ISO/TR 21934-1.

5.7.2.4 Specific ADS documents

The content of this document class is limited to a specific topics/features of automated driving systems. In contrast to generic ADS documents, the requirements contained therein are not applicable to all automated driving systems to the same extent, as they are intended for specific sub-areas such as: defined ADS use cases, environment perception, or the hardware being used (e.g. sensors, ECUs, etc.).

EXAMPLE 1 ISO 23374-1.

EXAMPLE 2 ISO 23792-1.

5.7.3 Applying the related (safety) standards

The goal of this subclause is to act as a guideline on how related standard documents are used in this document and how they contribute to achieving and demonstrating safe operation of an ADS.

This document is an application standard, that provides the starting point and the framework to argue safety for an ADS. As explained in [5.5](#), the core of an ADS safety is given by the structure of this document, where other (safety) standards can then be used for guidance on what are considered valid arguments and evidence for means and organizational environment-based claims (see [Figure 4](#)). Due to their relevance for safety of an ADS, the ISO 26262 series on functional safety, ISO 21448 on safety of the intended functionality and ISO/SAE 21434, in particular, form the basis for this document and its content.

The normative requirements in this document constitute a structure for what is needed as content in the rationale claims and satisfaction claims of an ADS safety case. Other standards are expected to give guidance contributing to how this is fulfilled, i.e. what are valid arguments and evidence related to claims about rationale, satisfaction, means and organizational environment.

In some cases, explicit links to existing standards are given in this document, however their relations to this document is largely implicit and assumed to be understood by the user of this document. The informative parts of this document provide different possible solutions on how to fulfil the normative requirements. As there are different possible solutions, there are also different ways how to reference the other standards. It remains the expectation of the user of this document to ensure that the rationale claims and satisfaction claims are, in fact, met by the methods used.

5.8 Safety principles of ADS

5.8.1 Purpose

This subclause provides a set of safety principles as verifiable guidelines that, when followed, can facilitate the achievement of safety of an ADS or ADS-equipped vehicle throughout development, and operation.

The safety principles described in this subclause were developed based on an analysis of ADS safety information, guidelines and requirements from a collection of expert entities, including industry organizations, government agencies, academia and advocacy groups, and are intended to provide a comprehensive set of considerations for ADS safety. These principles represent the current state of industry knowledge. However, they are not exhaustive, and dependent on the ADS feature not necessary all applicable. In addition, extensions, enhancements and adjustments are likely as development and operational experience and knowledge grows.

The safety principles can be applied throughout the subsequent clauses of this document, for which further detail of the principles is provided in [Annex D](#), and examples of their usage in [E.2](#) and [A.2.2](#).

5.8.2 ADS safety principles

- a) Safe operation – The ADS operation is free from unreasonable risks to users and other road users.
- b) Safety assessment – A safety assessment of the ADS is conducted to determine that the design and operation achieve the safety requirements and that the safety requirements are sufficient.
- c) Passive safety – The addition of an ADS does not negatively impact crashworthiness and passive safety achievement of the vehicle or safety of other road users, regardless of operating mode.
- d) Cybersecurity – The ADS employs appropriate strategies to protect against cybersecurity threats and safeguard information stored by the ADS.
- e) Operational design domain – The ADS has a clearly defined ODD.
- f) Behaviour in traffic – The ADS is designed with the ability to comply with road traffic regulations as well as common traffic behaviour applicable for performing the DDT or DDT fallback within its ODD, with selected exceptions permitted, commensurate with those for human drivers.
- g) Conflict avoidance – The ADS behaviour accounts for conflict avoidance competencies, such that the ADS behaviour does not initiate new conflicts and promptly reacts to, and mitigates consequences of, conflicts initiated by other road user(s).
- h) DDT fallback – The ADS is designed to detect DDT performance-relevant system failure(s), or the exiting of the ODD, and subsequently initiates DDT fallback or issues a request to intervene.
- i) DDT handover – The ADS evaluates the safety of the DDT handover, whether user- or ADS-initiated, before doing so.
- j) Human user requests – The ADS responds appropriately to user requests based on their role in safe operation, while considering foreseeable misuse.
- k) Mode awareness – The ADS displays the ADS active operating mode and transitions between modes, as well as respective DDT and/or DDT fallback roles of the driver (when present), and any other safety-relevant information to the user(s) of an ADS-equipped vehicle.

- l) Reaction to incident(s) – The ADS is designed to take appropriate action(s) when an incident occurs, including communication of emergency information to relevant parties.
- m) Data recording – The ADS records and secures relevant data sufficient for incident analysis.
- n) Maintenance and repair – Published procedures are available for maintenance, update and repair of the ADS to achieve safety over its operational lifetime.
- o) Operational monitoring – Monitoring of the ADS is conducted to assess safety in operation, with potential corrective actions applied to ensure safety.
- p) Intended usage – The ADS developer provides information regarding the intended proper usage and limitations of the ADS for all stakeholders involved.

NOTE For an ADS-equipped vehicle where none of the DDT or DDT fallback is allocated to a human user, some or all of the principles with regards to human user involvement would not be applicable.

6 Safety strategy

6.1 Defining the ADS feature

6.1.1 Objectives

The objectives of this subclause are:

- a) to define the ADS feature, its intended usage and the intended ODD; and
- b) to describe the DDT fallback strategy, the applicable MRCs and argumentation as to why the risk of harm in each MRC is acceptably low.

6.1.2 Requirements and recommendations

6.1.2.1 Interactions between the ADS and its users and environment shall be defined for the ADS feature.

NOTE 1 The user of the ADS can be inside or outside the ADS-equipped road vehicle.

NOTE 2 While the ADS can receive strategic task requests from a number of sources (e.g. users or other entities carrying out operation assistance functions), it is always the role of the ADS to accept such requests only if it can execute the request safely under the actual conditions.

EXAMPLE Engagement/disengagement procedures are interactions between the ADS feature and its users.

6.1.2.2 The functionality shall be specified for the ADS feature.

EXAMPLE An ADS feature for motorways including lane changes and in-lane driving.

6.1.2.3 An ODD shall be defined for the ADS feature.

NOTE 1 Refer also to ISO 34503 for defining an ODD.

NOTE 2 While an ADS feature has a single uniquely defined ODD, different use cases and/or locations considered for deployment can lead to only including portions of such ODD (i.e. certain ODD attributes but not others).

NOTE 3 Specific operating conditions for the ADS features can be defined as a part of ODD definition. When such operating conditions are essential to understand the proposed use case for the ADS feature, they are included in the safety argumentation.

6.1.2.4 The ODD (in accordance with [6.1.2.3](#)) shall be defined such that the sustained execution of the DDT starts and remains inside the ODD.

NOTE 1 While the V&V activities are assessed considering the entire ODD (including the ODD boundary), the safety argumentation for deployment can only embed specified sustained behaviours of the DDT, and the DDT fallback (for L4 ADS features), inside of the ODD (including the ODD boundary).

NOTE 2 While L3 and L4 ADS features are designed to operate exclusively within their respective ODDs, some ODD conditions are subject to rapid change during on-road operation (e.g. inclement weather, obscured lane lines). Such transient changes in the operating environment do not necessarily represent an “ODD exit,” as the ADS feature determines when such a change in conditions requires fallback performance (whether by the fallback-ready user or ADS feature).

NOTE 3 While V&V activities with respect to the sustained execution of the DDT, and the DDT fallback (for L4 ADS features) are assessed considering the entire ODD, there cannot be any specified sustained behaviour of the DDT, and the DDT fallback (for L4 ADS features) outside the ODD (detecting and reacting on being outside the ODD for example). All safety-related behaviour of the DDT, and the DDT fallback (for L4 ADS features) are specified as being inside the ODD in order to determine semantics for the completion of the V&V activities regarding DDT, and DDT fallback (for L4 ADS features).

NOTE 4 The sustained execution of the DDT fallback for L4 ADS feature is triggered once the ADS is about to exit the ODD or is suddenly outside the ODD. This is specified in [Clause 7](#) and [Clause 8](#). While performing DDT fallback, an ADS feature can operate temporarily outside of its ODD. Nevertheless, verification and validation of the DDT fallback can still be confined to a certain domain other than the ODD; However, it does not imply that operation of the ADS feature outside of the ODD is an indefinite task.

6.1.2.5 The ODD (in accordance with [6.1.2.3](#)) shall be defined such that the sustained execution of the DDT fallback (for L4 ADS features) starts inside the ODD.

See notes in [6.1.2.4](#).

6.1.2.6 The DDT fallback strategy shall be described.

NOTE The response by an ADS when performing the DDT fallback is to achieve an MRC. The ADS does so by performing MRMs. Additionally, non-manoevre behaviours, such as appropriate signalling, can be conducted.

6.1.2.7 A number of MRCs shall be defined for the ADS feature.

NOTE 1 If a DDT performance-related system failure in a L3 ADS feature occurs, the DDT fallback-ready user is expected to achieve an MRC when it is deemed necessary or perform the DDT if the vehicle is operable. In this case, the L3 ADS feature could not have a defined MRC but an implemented failure mitigation strategy at vehicle level can reduce harm, in case of non-available DDT fallback-ready user.

NOTE 2 L4 ADS features can have one or several MRCs defined.

6.1.2.8 The definition of an MRC shall be complemented by a rationale as to why its risk of harm is acceptably low.

NOTE The argumentation can include:

- expectations for a user to operate the vehicle after reaching the MRC;
- expected conditions and limits on frequency for reaching the MRC;
- expected limits on duration for reaching and staying in the MRC;
- conditions for exiting the MRC; and
- expected amount of time to stay in the MRC.

6.1.3 Example solution: ADS feature description with capabilities

This example solution applies the concept of capabilities to the automotive industry. Capabilities are known to be used for efficient management of complex ventures. Mastering the complexity of defining the ADS feature is supported by defining a necessary set of capabilities. Details of this solution and an overview of suggested safety capabilities are presented in [E.2](#).

6.2 Defining the risk acceptance criteria

6.2.1 Objectives

The objectives of this subclause are:

- a) to define risk acceptance criteria;
- b) to rationalize the chosen risk acceptance criteria; and
- c) to describe how the argumentation for absence of unreasonable risk relies on the specification of risk acceptance criteria.

6.2.2 Requirements and recommendations

6.2.2.1 Risk acceptance criteria shall be defined for the ADS with respect to the context of the proposed use cases and ODD.

NOTE 1 Risk acceptance criteria are either qualitative or quantitative (see ISO 21448).

EXAMPLE Risk acceptance criteria can consist of a combination of consequences of harm, $H = [h_1, h_2, \dots, h_n]$, and their respective frequency limits, $N = [v_1, v_2, \dots, v_n]$.

NOTE 2 Appropriate definition of risk acceptance criteria might consider both the event-level (individual scenarios or scenarios with equivalent risk acceptability) as well as the aggregated level as these complement each other. See more in [E.4](#).

NOTE 3 While this document requires risk acceptance criteria to be defined, it does not constrain the use of any specific validation target.

NOTE 4 Results from cybersecurity risk assessments are included in the definition of risk acceptance criteria.

6.2.2.2 Risk acceptance criteria shall account for all identified hazards.

NOTE 1 Hazards are potential sources of harm. However, some of these sources can be unknown.

NOTE 2 Sources of harm include but are not limited to failures (e.g. incorrect assumptions made in safety argumentation, and failures due to random hardware faults or systematic design faults), functional insufficiencies within the intended functionality, cybersecurity threats, aggressive behaviour of other road users, environmental conditions, and foreseeable misuse by the users.

6.2.2.3 Rationalization shall be provided for the chosen risk acceptance criteria.

NOTE Sources that can impact the selection of risk acceptance criteria include:

- comparison data or information with existing risks for given use cases (PoRiBa, GAME, MEM, ALARP, etc.);
- applicable legislation; or
- benefits to customers and society.

6.2.2.4 The argumentation for safety shall be described.

NOTE 1 Safety can be argued for by identifying hazards, defining sufficient mitigations and relying on the specified risk acceptance criteria to evaluate and accept the residual risk.

NOTE 2 The argumentation for safety can include more than one risk acceptance criterion.

6.2.3 Example solution: Absence of unreasonable risk and risk acceptance criteria

This example introduces a few risk acceptance criteria. The justification of these risk acceptance criteria and how they are used to argue for safety are discussed. Further information on the rationale for these risk acceptance criteria and how the argumentation for safety relies on their specification are discussed in [E.3](#).

6.2.4 Example solution: Selection and use of risk acceptance criteria

This example presents qualification attributes for risk acceptance criteria and their associated validation targets. The content exemplifies how different qualitative or quantitative benchmarks potentially impact the stringency and sufficiency of the risk acceptance criteria, and thus the importance of risk acceptance criteria selection and usage. Further information on this topic can be found in [E.4](#).

6.2.5 Example solution: Defining a risk acceptance criterion

This example presents a manoeuvre-based risk acceptance criterion in a potentially hazardous scenario. A methodology to derive a reasonable time gap between ADS and other road users in an intersection is given, which precludes safe driving of the ADS when compared to an experienced and attentive driver. Further information can be found in [E.5](#).

6.2.6 Example solution: Quantitative risk balance

This example for quantitative risk balance presents an approach in which risk criteria based on accident data are derived for different injury severities. It illustrates how these risk criteria, which describe the human driving performance, provide, under the consideration of additional safety factors, the baseline for comparison with the automated driving system. Further information on quantitative risk balance can be found in [E.6](#).

6.2.7 Example solution: A quantitative risk acceptance criterion

This example presents the quantitative risk acceptance criterion (QRAC) and its general parametrization. A quantitative risk acceptance criterion is useful to express a relative-performance criterion, such as “better than a human”, explicitly, and provides justification that meeting the quantitative risk acceptance criterion implies that the relative-performance criterion is also met. Further information on the quantitative risk acceptance criterion can be found in [E.7](#).

6.3 Defining safety requirements

6.3.1 Objectives

To achieve the risk acceptance criteria, the objectives of this subclause are to define:

- a) safety requirements for the ADS; and
- b) assumptions, prerequisites or requirements external to the ADS.

NOTE Safety requirements regarding the DDT are allocated to the ADS.

6.3.2 Requirements and recommendations

6.3.2.1 Safety requirements shall be defined for the ADS feature.

NOTE The definition of safety requirements follows best practices that include a requirement being explicit and verifiable.

6.3.2.2 The safety requirements shall be allocated to the ADS and/or external to the ADS.

NOTE 1 The safety requirements defined for the ADS feature can be refined for the purpose of allocation to ADS and/or external to ADS.

NOTE 2 Allocation to either ADS or external to ADS is partly a design choice, but all safety requirements regarding the DDT and the DDT fallback (when applicable) are allocated to the ADS (per the DDT and DDT fallback definitions in [Clause 3](#)).

NOTE 3 An ADS can consist of on-board and off-board elements (see Note 1 to entry in *ADS safety case* ([3.4](#))). For example, portions of the infrastructure could be part of off-board elements of the ADS, depending on the chosen design.

NOTE 4 Safety requirements allocated external to the ADS can include safety requirements on the vehicle, infrastructure, users, other road users and intelligent transportation systems (ITS).

6.3.2.3 Assumptions and prerequisites external to the ADS, for the ADS feature to operate safely, shall be defined.

6.3.2.4 The safety requirements, together with corresponding assumptions and prerequisites, shall fulfil the risk acceptance criteria.

NOTE These safety requirements are at a high level for the ADS as explained in [Clause 5](#). Further refinement is specified in [Clause 7](#).

6.3.3 Example solution: Quantitative risk acceptance criterion and incident classification approach

This example presents one method for meeting the objectives of [6.3](#) when a quantitative risk acceptance criterion (QRAC) is chosen as a risk acceptance criterion in [6.2](#). The method makes use of injury risk assumptions allocated external to the ADS and an exhaustive incident analysis to define safety requirements allocated to the ADS, that limits how often incidents can occur and lead to a certain consequence. Further information on this methodology and its usage with quantitative risk acceptance criteria can be found in [E.8](#).

6.3.4 Example solution: Safety capabilities

This example solution is based on an ADS feature with defined capabilities (see [6.1.3](#)). From this, requirements for a proper ADS design ([7.1](#)) and prerequisites external to the ADS ([7.2](#)) can be derived. Further information can be found in [E.9](#).

6.3.5 Example solution: ADS external assumptions with respect to injury risk

This example presents a formulation of assumptions with respect to injury risk that can be allocated external to the ADS. Injury risk assumptions are often used together with ADS requirements to provide the rationale for why consequences are sufficiently mitigated. Further information can be found in [E.10](#).

7 Safety by design

7.1 ADS design

7.1.1 Objectives

The objective of this subclause is to:

- a) refine the safety requirements allocated to the ADS and develop an ADS design in accordance with them.

7.1.2 Requirements and recommendations

7.1.2.1 The safety requirements allocated to the ADS shall be refined.

NOTE This requirement ([7.1.2.1](#)) can be applied several times as a chain of refinements.

7.1.2.2 The refined safety requirements shall satisfy the safety requirements allocated to the ADS.

7.1.2.3 The design shall be developed for the ADS in accordance with the refined safety requirements.

NOTE Multiple levels of hierarchy of the design are possible. This requirement might be applied several times as a chain of refinements.

7.1.3 Example solution: A design for adapting tactical decisions to variations in the operational capabilities

This example shows how the objectives for [7.1](#) can be achieved in two steps of requirement refinement when the ADS requirements take the form as frequency limits to the occurrence and consequence of incidents. The design adapts tactical decisions to run-time variations in operational capabilities, allowing the ADS to continuously maintain its capability and respond accordingly to future situations. Further information on the design and its characteristic properties can be found in [F.2](#).

7.1.4 Example solution: Elements defining the design

This example solution provides example elements and combinations thereof to achieve the suggested safety capabilities. It continues the method of using capabilities presented in [6.1.3](#) and adapting it to the respective ADS feature to be developed. Details on the implementation of safety capabilities and elements can be found in [F.3](#).

7.2 ADS external design, prerequisites and assumptions

7.2.1 Objectives

To satisfy the requirements, prerequisites and assumptions allocated to ADS external elements, the objectives of this subclause are to:

- a) define the ADS external elements;
- b) allocate requirements, prerequisites, and assumptions to the ADS external elements; and

NOTE These requirements, prerequisites and assumptions are defined in [7.2](#).

EXAMPLE 1 Dedicating a traffic lane for a local automated shuttle bus service as a requirement.

EXAMPLE 2 Median barriers between traffic lanes in opposite direction as a prerequisite.

EXAMPLE 3 The fallback-ready user immediately responding to a request to intervene as an assumption.

- c) specify the ADS external design satisfying the requirements, prerequisites and assumptions allocated to the ADS external.

7.2.2 General

7.2.2.1 Overview

The safety of an ADS-equipped vehicle depends on the safety measures of the ADS, the base vehicle and the ADS environment. Safety measures in the ADS environment include those provided by the physical infrastructure, activities performed by humans and intelligent transportation systems (ITS), with related services. Where these types of safety measures are part of the safety argumentation of the ADS, the following sections provide guidance and requirements for fulfilment.

7.2.2.2 Base vehicle

For the purposes of this document, a distinction is made between the ADS and the vehicle in which the ADS is installed (hereafter the “base vehicle”).

The ADS utilizes some of the systems in the base vehicle (e.g. brakes and steering) that are also used for manual operation. This document does not specify which parts of the ADS-equipped vehicle are to be considered as part of the ADS or as part of the base vehicle, as this will be a design choice. This approach

supports the development of ADS-equipped dual mode vehicles, where the DDT can be executed by the ADS or human driver.

The following are examples of base vehicle aspects that can contribute to safety of the ADS-equipped vehicle:

- passive safety; and

EXAMPLE 1 Crashworthiness.

EXAMPLE 2 Seatbelts.

EXAMPLE 3 Airbags.

- vehicle dynamics.

EXAMPLE 4 Actuators for braking and steering.

7.2.2.3 The infrastructure in which the ADS-equipped vehicle operates

The infrastructure in which the ADS-equipped vehicle operates can contribute to the safety of ADS-equipped vehicles in some types of operation. This can include safety measures in the physical infrastructure and intelligent transportation systems. The infrastructure in which the ADS-equipped vehicle operates, can be outside the span of control or within the span of control of the ADS developer.

EXAMPLE 1 An ADS developer for an automated transportation system on a public road has very limited control of the infrastructure in which the ADS-equipped vehicle operates.

EXAMPLE 2 An ADS developer for an automated transportation system in a greenfield mine can to a large degree control the infrastructure in which the ADS-equipped vehicle operates.

Some types of safety measures in the infrastructure in which the ADS-equipped vehicle operates with their contributions are the following.

- Barriers

- Barriers can ensure that ADS-equipped vehicles are operated only in areas designated for automated driving, which can be static or dynamic in their application;

NOTE 1 Dynamic barriers can be actuated using ITS.

EXAMPLE 3 Automatic bollards preventing access to a parking lot without required credentials.

- Barriers can ensure that traffic is separated to avoid head-on-collisions, reducing the impact speed and thus lowering severity in the event of a crash;

- Barriers can effectively ensure that automated and manually driven vehicles are separated.

- Fences

- Fences can ensure that persons are kept outside the driving areas of ADS-equipped vehicles.

- Traffic control gates

- Traffic control gates include control of moveable infrastructure that only permits entry by authorized vehicles, or when cross traffic (such as a commuter train) has cleared the intersection. Lights that change colour to regulate the entry of vehicles into a congested traffic lane or service area are also considered a form of traffic control gate.

EXAMPLE 4 A weigh station, with traffic control gate as a service area for weighing vehicles.

- Electronic safety gates

- Electronic safety gates can be used to ensure ADS-equipped vehicles only operate in a particular controlled area when safe to do so.

EXAMPLE 5 A loading dock that will prevent ADS-equipped vehicles to enter when there are humans present on the dock.

— Emergency stop systems

- Emergency stop systems for ADS-equipped vehicles within the infrastructure, can efficiently prevent crashes when an emergency stop is requested by a system or a person. These systems can be for individual vehicles and for fleets of vehicles.

EXAMPLE 6 An emergency stop system that stops ADS-equipped vehicles from entering prohibited areas.

EXAMPLE 7 An emergency stop system which stops a fleet of ADS-equipped vehicles when a person enters a prohibited area, even if not allowed to enter.

— Remote assistance

- Remote assistance by ADS fleet operator can ensure that ADS-equipped vehicles that stopped operating are moved to safe areas to avoid additional incidents and crashes.

— Centralized vehicle and transportation management

- Vehicle and transportation management can coordinate ADS-equipped vehicles, individually or as part of a fleet, in operation to drive in different areas to increase safety.

EXAMPLE 8 ADS-equipped vehicles are routed around roads undergoing construction work.

EXAMPLE 9 A fleet of ADS-equipped vehicles is routed around an area with icy road conditions.

EXAMPLE 10 Notification of vehicle breakdowns to ADS fleet operator, allowing towing to recover the vehicle.

EXAMPLE 11 A fleet operations centre directs the ADS-equipped vehicles to defined parking areas to receive over-the-air updates of ADS software.

— Digital maps

- Digital maps can be used with localization systems by an ADS-equipped vehicle for path planning. The sensor array compares the planned path to lane markings to establish ground truth.

NOTE 2 Digital maps can also be part of the ADS.

— Weather and road condition updates

- Unexpected changes in weather and road conditions can change the behaviour of the ADS, e.g. re-routing and stopping ADS operation.

EXAMPLE 12 A rock slide scatters debris across the roadway triggers re-routing a fleet of ADS equipped vehicles.

NOTE 3 Sensor systems located external to the ADS-equipped vehicle are part of the ADS if performing part of the DDT (ISO 23374-1) provides one example of this.

NOTE 4 In addition to barriers, fences, traffic control gates, and electronic safety gates in the infrastructure, there can be signs, markings and signals to inform users and ADS fleet operators. These are described in [7.2.2.4](#).

7.2.2.4 Human activities and interfaces to relevant humans

7.2.2.4.1 Overview

Safety measures based on activities performed by humans can contribute to the safety of ADS-equipped vehicles in operation. If safe operation of an ADS-equipped vehicle of an ADS relies on humans, it is important to argue that these humans are able to perform their tasks. However, when defining the safety requirements, activities to be performed by humans are likely to be considered as assumptions, especially when they are not under the jurisdiction of ADS developers (e.g. other road users).

This section includes how different humans can contribute to safety, how requirements can be handled to strengthen the argumentation for the assumptions regarding these human activities, and also includes supporting information for some key areas.

Human activity can contribute to the safe operation of ADS-equipped vehicles, depending on a number of factors, including:

- the level of the automated feature engaged;
- the type of feature engaged;
- the use case; and
- the area of operation.

7.2.2.4.2 Other road users

Assumptions can be made that road users follow traffic rules. Requirements can be set to monitor the behaviour of other road users and changes the driving behaviour of the ADS-equipped vehicle accordingly.

7.2.2.4.3 Passengers

Passengers can interact with the ADS-equipped vehicles. Their contribution to safety can be assumed primarily as adhering to described behaviour for riding in an ADS-operated vehicle. Requirements can be set to instruct passengers to put on their seatbelts in the ADS-equipped vehicle.

7.2.2.4.4 Fallback-ready users

Fallback-ready users of an L3 ADS feature engaged vehicle can be assumed to be receptive to requests to intervene, and is capable of performing the fallback manoeuvre. There can be requirements for visual and audible warnings in the ADS-equipped vehicle that instruct the fallback-ready user to take over control of the vehicle.

NOTE Fallback-ready users are assumed to have the appropriate driving license for the vehicle under operation.

7.2.2.4.5 ADS fleet operators

ADS fleet operators can dispatch ADS-equipped vehicles into driverless operation, perform fleet operating functions and provide ADS assistance in accordance with ISO 21448. Their tasks can also include vehicle inspections and repairs, refuelling, charging, mission management and mode management. ADS fleet operators can work in close proximity to the vehicles or more remotely. In both cases, they can contribute to safety.

ADS fleet operators might be needed for different purposes, to ensure the safety of the ADS-equipped vehicles and to ensure the safe operation of the ADS-equipped vehicles. It can be assumed that ADS fleet operators are trained. Safety of the ADS fleet operators is also important.

NOTE 1 An ADS fleet operator is a user who has a role in the operation of an ADS-equipped vehicle.

NOTE 2 The safety of the ADS fleet operators can be ensured in similar ways as safety is ensured for road users.

NOTE 3 The decision to rely on ADS fleet operators for safe operation depends on the automation level, type of feature, types and area of operation, and other factors.

EXAMPLE 1 An ADS fleet operator who regularly inspects the ADS-equipped vehicle prior to dispatching it into driverless operation.

EXAMPLE 2 An ADS fleet operator who repairs an ADS-equipped vehicle with faults.

EXAMPLE 3 An ADS fleet operator who assigns driving destinations to ADS-equipped vehicles.

EXAMPLE 4 An ADS fleet operator who fuels an ADS-equipped vehicle during operation.

EXAMPLE 5 An ADS fleet operator who operates a stopped ADS-equipped vehicle to a safe state on the side of the road using remote driving functionalities.

EXAMPLE 6 An ADS fleet operator who is responsible for cybersecurity, monitors the operation of the ADS-equipped vehicles to ensure safe operation in the presence of cybersecurity threats.

7.2.2.4.6 Service provider

The role of service providers in the operation of ADS-equipped vehicles includes personnel that are not directly involved in the operation, but are needed for other reasons. Their roles include tasks in weigh stations, valet parking lots, loading and unloading of goods, and requesting transportation assignments. These roles can work in close proximity to the vehicles or more remotely. In both cases, these service providers can contribute to safety and can also be put at risk, that will be mitigated.

Service providers might be needed for the operation of ADS-equipped vehicles in common and in specific driving situations. To ensure safety during operation, service providers need all relevant information for interacting with ADS-equipped vehicles.

NOTE 1 A service provider is a user who interacts with ADS-equipped vehicles during their operation.

NOTE 2 Service providers include personnel working at road-tolls, weigh stations and transfer hubs.

7.2.2.4.7 First responders

First responders might be needed in the event of incidents. To ensure correct and efficient rescue, first responders need access to all relevant information for interacting with ADS-equipped vehicles.

NOTE 1 A first responder is a human who provides emergency support in the event of incidents.

NOTE 2 First responders include emergency response personnel, law enforcement personnel, fire and rescue personnel, and emergency medical service personnel.

7.2.2.4.8 Police and traffic control personnel

Police and traffic control personnel might need to interact with ADS-equipped vehicles. To ensure correct and safe interaction, police and traffic control personnel need access to all relevant information when interacting with ADS-equipped vehicles.

NOTE 1 The instruction on how to interact with ADS-equipped vehicles depends on the location and ODD.

NOTE 2 The types of relevant users depend on the operation of how the ADS-equipped vehicle is operated.

7.2.2.4.9 Information for users and other road users

Information for users and other road users can contain the tasks expected of humans. Humans have the need for all the relevant information. This information is kept up to date at all times, and can be communicated via different means, such as:

- user interfaces;

EXAMPLE 1 A display in the ADS-equipped vehicle showing the current operating mode as well as any need to intervene.

- training with associated material:

- theoretical;

- practical;

NOTE There can be a need for refresher training sessions.

EXAMPLE 2 Training for ADS fleet operators with ADS operated vehicles on public roads.

— instructions;

EXAMPLE 3 A repair instruction for ADS fleet operators that describes how to replace a faulty sensor.

— contracts and agreements;

EXAMPLE 4 A service agreement between a vehicle manufacturer and an ADS fleet operator.

— signs and markings:

— signs and markings can inform persons on how to behave around ADS-equipped vehicles;

EXAMPLE 5 Signs warning that ADS operated vehicles are in a road segment.

— signals:

— signals on vehicles can alert persons to the active operating mode of the ADS-equipped vehicles;

— signals around the operation area can alert other road users about the status of the ADS-equipped vehicles.

EXAMPLE 6 ADS operated vehicles with lighting beacons to notify other road users about its current mode of operation.

7.2.2.4.10 User training and education

This subclause applies to training and education for users of commercially available ADS-equipped vehicles. Safety and trust can be improved when users and the ADS share an understanding of system capabilities and the scenarios that can be encountered by the ADS-equipped vehicle.^[20] Training and education can improve this understanding and can lead to improved safety and acceptance outcomes.

Training and education for users are made available throughout the life cycle of an ADS and accommodate relevant updates or changes to the system design. Completion of training and education is acknowledged and verified through testing or other methods. Changes that can trigger a need for updated training and education material includes changes in the ODD and type of operation.

7.2.2.4.11 Passenger initiated emergency trip interruption (PITI) and passenger initiated emergency call (PEC)

It is assumed that any fallback-ready user has the requisite training to operate the vehicle following a transition of the DDT from the ADS to the fallback-ready user. Users with no role in conducting the DDT or DDT fallback can be passengers.

Passengers can still benefit from education initiatives, especially with regard to the use of passenger-initiated emergency trip interruptions (PITI) or passenger-initiated call (PEC). Passenger education for the proper use of these functions can be implemented through various means, including visual and verbal instructions.

The PITI is distinctly different from ADS-initiated emergency trip interruption (i.e. when the ADS manages a DDT-related emergency) and passenger-initiated non-emergency trip interruption (e.g. changing trip destinations). The presence of one or both of PITI and passenger-initiated emergency call (PEC) features can improve passenger trust, reduce anxiety and therefore, improve safety of passengers as well as overall social acceptance of ADS-equipped vehicles (see Reference ^[21]). During field monitoring, tracking the number and type of events leading to passenger initiation of PES or PEC can also help improve safety through refinement of the ODD, type of operation, or other operational aspects that can be associated with risk management.

The PITI is comprised of an onboard vehicle system that allows a passenger to send a command to bring the ADS-operated vehicle to a controlled stop as a result of a perceived emergency. Fleet operations can restart the vehicle once the stop manoeuvre has been completed.

The PEC allows passengers to contact fleet operations for support when needed during a perceived emergency. Fleet operations can then take action (e.g. reroute or stop the vehicle).

The user controls for PITI and PEC features should be easily recognizable, accessible and the feature should be always available. To minimize potential misuse and abuse of PITI/ PEC features by passengers, clear instructions should be available and easily viewable by passengers.

EXAMPLE 1 A label on a PITI button marked “emergency stop”.

When passengers initiate an emergency stop or emergency call feature, an acknowledgement that the request has been received follows.

NOTE Interior cabin lighting can be activated, and in-cabin sound can be reduced to help with remote assessment of the emergency.

For passenger safety, and to reduce the risk of other road users crashing into a vehicle performing an emergency stop, other road users are alerted that an emergency stop is taking place.

EXAMPLE 2 Hazard lamps are activated when an ADS-equipped vehicle performs an emergency manoeuvre.

Passengers and fleet operations are alerted once an emergency stop is complete. Following a PITI, the ADS-equipped vehicle resumes operation only after receiving authorization by an appropriate user. If the vehicle is stopped, passengers can be reminded to observe their surroundings and be aware of potential hazards in the environment before exiting the vehicle (see Reference [22]).

7.2.2.4.12 First responder instructions and education

It is likely that ADS-equipped vehicles will interact with emergency first responders at some point during their operation on public roadways. First responders include emergency response personnel associated with the public safety domain. Their roles include law enforcement (police), fire and rescue, and emergency medical services. Others, who could potentially provide emergency support include roadway response services, towing and recovery services, and other road users. ADS-equipped vehicles typically have controls that differ from manually driven vehicles (e.g. without steering wheel, pedals).

Common approaches for the interactions between first responders and ADS-operated vehicles can improve safety and reduce the amount of information provided by ADS developers to ADS fleet operators and first responders. This will become increasingly important as more ADS-equipped vehicles from more developers are commercially deployed.

The below list includes common situations describing interaction between ADS-equipped vehicles and first responders:

- responding to an incident – arriving at an emergency or unplanned traffic scenario to render assistance or take control of the situation;
- securing a scene – blocking or diverting traffic to assess a scene and the humans present, collecting information and protecting against potential harm;
- traffic direction and control – signalling or directing a specific action or path that differs from normal traffic flow;
- traffic stop and checkpoint – recognizing and responding to gestures from first responders;
- investigating a stationary unoccupied ADS-equipped vehicle in an unexpected location;

NOTE 1 An unoccupied ADS-equipped vehicle parked in an unexpected location can appear to be inactive and start driving at any time.

- stabilization and extrication – stabilization prevents vehicle movement. Extrication involves removing users and typically involves bending, cutting or removing vehicle pieces and parts;
- motorist assist – includes vehicle repairs, towing or waiting with a vehicle for another responder to provide aid.

ADS and first responder interaction types are:

- direct – involves physical contact between a first responder and an ADS-equipped vehicle, including touching the vehicle directly or with a piece of equipment;
- indirect – involves the first responder influencing an ADS without coming into physical contact;
- informational – when information must be obtained from or about an ADS-equipped vehicle by the first responder. Depending on the circumstances, the first responder can potentially come into physical contact with the ADS-equipped vehicle.

NOTE 2 Examples of educational content for first responders can be found in [7.2.5](#).

7.2.3 Requirements and recommendations

7.2.3.1 The ADS external elements needed for safe operation of the ADS shall be defined.

7.2.3.2 Requirements, prerequisites and assumptions external to the ADS shall be allocated to the defined ADS external elements if feasible.

NOTE 1 Requirements, prerequisites and assumptions external to the ADS are defined in [6.3](#).

NOTE 2 It is a design choice in which requirements, prerequisites, and assumptions are feasible to allocate to ADS external elements. Regardless of the allocation, the requirements, prerequisites and assumptions, external to the ADS, are verified or confirmed in [7.4](#).

7.2.3.3 If the safe operation of an ADS-equipped vehicle relies on safety measures in the base vehicle, the design specification of these safety measures shall define the prerequisites and satisfy the requirements allocated to the base vehicle.

7.2.3.4 If the safe operation of an ADS relies on users and other road users, the instruction and training material for users and other road users shall describe the prerequisites and satisfy the requirements allocated to ADS external elements related to users and other road users.

7.2.3.5 There shall be up to date instructions and information for users involved in the operation of ADS-equipped vehicles to inform how users are intended to interact with the ADS-equipped vehicles to ensure safe operation.

7.2.3.6 If the safe operation of an ADS relies on users, ADS fleet operators, or service providers, it shall be ensured that they are competent and informed of their roles.

7.2.3.7 There shall be up to date instructions and information on how first responders are intended to safely interact with ADS-equipped vehicles to mitigate the effects of potential incidents.

NOTE The information material can include description of the ODD, the operation of the ADS-equipped vehicles including approaching, disabling and towing the vehicle, contact information, extricating humans and firefighting.

7.2.3.8 If the safe operation of an ADS-equipped vehicle relies on safety measures in the infrastructure in which the ADS-equipped vehicle operates, the design specification of these safety measures shall describe the prerequisites and satisfy the requirements allocated to the infrastructure in which the ADS-equipped vehicle operates.

7.2.4 Example solution: Training for users

This example discusses instructions on how to train the users using an ADS. Mechanisms on how to train as well as what topics to be included in the training are part of the ADS design. Further information on the mechanisms and topics to educate the ADS users is presented in [F.4](#).

7.2.5 Example solution: Instructions to first responders

This example discusses the information needed by the first responders when interacting with the ADS. Different types of interactions (direct, indirect, or informational) and information share or request are needed depending on the use case. Further information on the use cases and the information exchanged between the ADS and first responders are presented in [F.5](#).

7.2.6 Example solution: Organizational aspects of a robo taxi service

This example solution describes the organizational aspects of a robo taxi service, operating in an urban ODD. The roles of the base vehicle provider, the ADS provider, the providers of the digital and physical infrastructure, and the ADS fleet operators and users each contribute towards this L4 ADS feature.

7.2.7 Example solution: Organizational aspects of an L4 hub-to-hub transport service

This example solution describes the organizational aspects of an L4 hub-to-hub cargo transport service, operating primarily on limited access free-ways. The roles of the base vehicle provider, the ADS provider, the providers of the digital and physical infrastructure, and the ADS fleet operators and users each contribute towards this L4 ADS feature.

7.3 ADS verification

7.3.1 Objectives

The objectives of this clause are to:

- a) provide evidence that the refined requirements implemented into the ADS (all together) satisfies the requirements of the ADS design; and
- b) provide evidence that the safety requirements for the ADS are achieved by the ADS in with its intended usage and ODD.

NOTE The provided evidence can be used for validation.

7.3.2 General

This subclause has its focus on verification, and in [Clause 8](#) the focus is on validation. The verification as of this subclause, is to cover both to the satisfaction claims and the rationale claims related to the requirements from the previous subclauses on "ADS Design" and on "Defining the Safety Requirements" in [6.3](#).

Satisfaction claim verification means verifying that the safety requirements are met, and verification of the rationale claims is the activity of ensuring sufficient completeness and consistency of the safety requirements refinement.

Note that this document is not providing normative process requirements. This means that for a verification activity part of an ADS safety case, process requirements regarding planning, specification, execution and evaluation, etc. are to be found in another document, e.g. the ISO 26262 series.

Because many of the possible solution strategies can be general for verification and validation, informative examples of such common content have been included in [Clause 10](#), and [Annex H](#).

7.3.3 Requirements and recommendations

7.3.3.1 All refined safety requirements for the ADS design shall be verified.

NOTE If refinement as of [7.1](#) is applied several times with a chain of refinements, this implies that every refinement instance of safety requirements will be verified.

7.3.3.2 All safety requirements allocated to the ADS shall be verified.

7.3.3.3 Verification of safety requirements allocated to the ADS, and of refined safety requirements for the ADS design, shall consider the entire ODD as defined in accordance with the definition of the ADS feature.

NOTE 1 Further connection of the ODD definition and the coverage of the scenario space is detailed in ISO 34503.

NOTE 2 Some related verification activities can go beyond the ODD, such as verifying that engagement of the ADS feature is not possible outside the ODD.

7.3.4 Example solution: Verification of elements

Static (e.g. reviews) and dynamic (e.g. HiL tests) testing activities on element level are called verification in contrast to validation activities on ADS feature level. This example gives details of how the elements are verified to achieve the requirements stated in [7.3.3](#).

Details for the example elements are stated in [7.1.4](#) and [F.3](#) whereas examples on the verification of such elements are stated in [F.6](#).

7.3.5 Example solution: The layered approach facilitating verification of safety arguments

This example presents the activities related to verifying the rationale claims and the satisfaction claims, respectively. The verification of the rationale claims becomes a theoretical task while the verification of the satisfaction claims typically involves real-world physical parts. Further information can be found in [F.7](#).

7.4 Verification and confirmation of aspects external to the ADS

7.4.1 Objectives

The objectives of this subclause are to:

- a) provide evidence that the implementation of the ADS external elements satisfies their requirements;
- b) confirm evidence that ADS external prerequisites are satisfied; and
- c) confirm that ADS external assumptions have argumentation.

NOTE 1 The evidence and arguments provided can be used for validation.

NOTE 2 Some assumptions and prerequisites are not allocated to ADS external elements but are confirmed in [7.4](#).

7.4.2 General

This subclause describes the activities for the verification and confirmation of assumptions, prerequisites and requirements that are external to the ADS. The content of this subclause applies to the base vehicle, the infrastructure in which the ADS-equipped vehicle operates, and the activities performed by users.

Requirements are fulfilled by ADS external elements and evidence can be provided that these requirements are satisfied. On the other hand, prerequisites can be confirmed for ADS external elements and ADS external in general. The confirmation can be documented as evidence. For assumptions, these can also be confirmed for ADS external elements and ADS external in general. However, it is not possible to provide evidence for these assumptions, due to their nature, and it is only possible to provide arguments for these.

There are several different possibilities to provide the evidence and arguments for these requirements, prerequisites and assumptions related to what is external to the ADS. This document describes what has to be done, but not how to do it, as the design and implementation of these are out of the scope of this document. There are other standards and established ways of working to rely upon instead.

7.4.3 Requirements and recommendations

7.4.3.1 Evidence shall be provided that the requirements allocated to ADS external elements are satisfied by the implementation of the ADS external elements.

NOTE 1 Evidence can be part of a verification report or a safety case.

NOTE 2 The requirements for ADS external are specified in [7.2](#).

7.4.3.2 Evidence shall confirm that the prerequisites are satisfied for ADS external, including those allocated to ADS external elements.

NOTE 1 Evidence can be part of a verification report or a safety case.

NOTE 2 The prerequisites for ADS external are specified in [7.2](#).

7.4.3.3 Arguments shall justify that the assumptions are satisfied for ADS external, including those allocated to ADS external elements.

NOTE 1 Arguments can be part of a verification report or a safety case.

NOTE 2 The assumptions for ADS external are specified in [7.2](#).

8 Validation

8.1 Objectives

The objective of this clause is to provide evidence that the risk acceptance criteria (in accordance with [6.2](#)) are achieved prior to the operation of the ADS in accordance with its intended usage and ODD.

NOTE The intended usage of an ADS operated vehicle includes operating where the safety requirements allocated external to the ADS are met.

8.2 General

This subclause is focused on validation, and in [7.3](#) the focus is on verification. How these two activities are related in this document, is explained in [Clause 5](#), and in particular in [5.4](#). Because many of the possible solution strategies are general for verification and validation, [Clause 10](#) and [Annex H](#) provide additional verification and validation content.

Validation discussed in this subclause is related to the assumptions connecting risk acceptance criteria to the safety requirements of the ADS feature.

8.3 Requirements and recommendations

8.3.1

The ADS feature together with the ADS external measures integrated in an ADS-equipped vehicle shall be validated using the risk acceptance criteria (in accordance with [6.2](#)) considering the entire ODD (in accordance with [6.1](#)).

NOTE 1 Validation of risk acceptance criteria can be based on metrics.

NOTE 2 The ADS feature together with the ADS external measures integrated in an ADS-equipped vehicle can be validated against the defined metrics utilising the respective industry standards (e.g. the ISO 26262 series and ISO/SAE 21434).

NOTE 3 Some validation activities can go beyond the ODD.

8.4 Example solution: Metrics

This subclause presents examples of ADS safety metrics that can support safety activities and contribute to system-level safety assessments and provide a common understanding of the performance of ADS operated vehicles. A set of these metrics, referred to as a common foundational set of metrics by the Automated Vehicle Safety Consortium (AVSC)^[23] include: crash severity and frequency, severity and frequency of

citable offences, safety envelope maintenance / longitudinal and lateral distance, longitudinal and lateral acceleration and jerk (leading), and OEDR reaction time (leading).

These foundational metrics are described in [H.7](#).

8.5 Example solution: Validation through computation of collision rates

This example presents a possible process for the computation of an ADS performance in terms of collision rates. A methodological pipeline is described together with highlighting of associated challenges and limitations connected to the estimation of injury risk in the presence of uncertainty. Further information on this particular metric of performance and its usage within quantitative risk acceptance criteria can be found in [G.2](#).

8.6 Example solution: Generating evidence for injury risk assumptions external to the ADS

This example shows how to provide evidence for injury-risk assumptions allocated external to the ADS. Assumptions regarding the relationship between incidents and their consequences are useful for defining ADS requirements that limit consequences, such as in [E.8](#) and [E.10](#). Further information can be found in [G.3](#).

9 Operation of the ADS-equipped vehicle

9.1 Objectives

The objectives of this subclause are to:

- a) establish and document measures for field monitoring of the performance of ADS-equipped vehicles before the start of operation;
- NOTE Field monitoring includes monitoring of safety relevant cybersecurity threats.
- b) establish and document measures for change management of ADS-equipped vehicles during the operational phase;
 - c) establish and document procedures for inspection, maintenance and repair of ADS-equipped vehicles during the operational phase; and
 - d) establish and document measures for crash and incident management, including reporting of information, for ADS-equipped vehicles before start of operation.

9.2 General

9.2.1 Overview

At the time of a successful ADS safety assessment, the safety related risks of an ADS feature have been reduced to an acceptable level, and the vehicle design has potentially been released for operation. Continuous field monitoring and corrective action using change management procedures are necessary during the operational phase to address previously unforeseen safety and cybersecurity concerns. It is also fundamental to manage other change requests needed. In case of crashes and incidents, these are also to be managed and potentially reported to stakeholders. The operation phase also includes vehicle inspections, preventive maintenance and repairs in case of failures. [Figure 8](#) clarifies the relationships between these different areas.

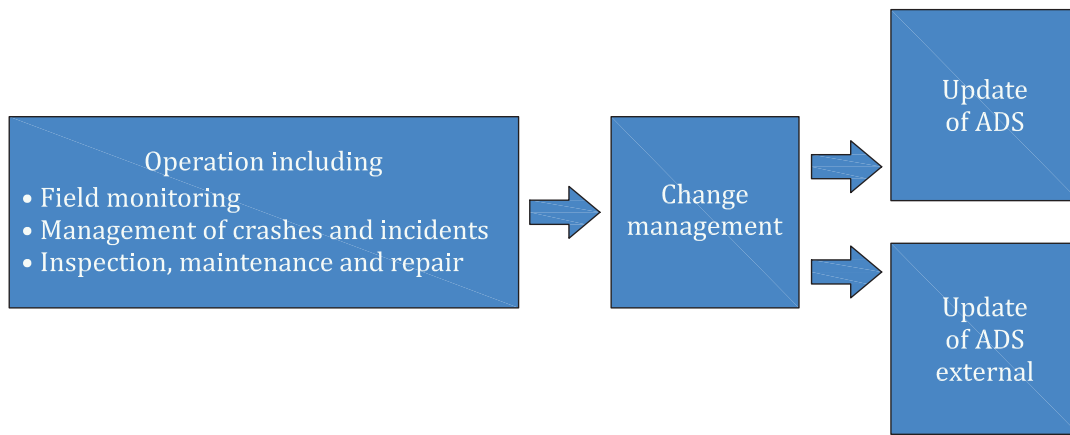


Figure 8 — Overview of ADS operation

9.2.2 Field monitoring including data collection

During the deployment and operation of the ADS, field monitoring is essential. The safety metrics identified in [Clause 8](#) can be monitored throughout field operation. In addition, there can be other metrics related to, e.g. near crashes that can be monitored. These metrics are relevant for evaluating safety of the ADS during intended driving in operation.

It is assumed that the companies involved with the development and field operation will follow the appropriate data management requirements to account for privacy.

EXAMPLE The European Union's General Data Protection Regulation (GDPR).

The collected data, including the data aggregated into the metrics, can be used for several different purposes. In the case where the data indicates higher risks than expected, corrective actions are needed. Such corrective actions are undertaken in accordance with a change management process (see [9.2.4](#)). Additionally, the data collected can be used for the validation of future ADS versions.

9.2.3 Cybersecurity monitoring related to safety of ADSs

Cybersecurity monitoring is important during the operation phase of ADS-equipped vehicles. To increase effectiveness, processes for field monitoring can be coordinated with the processes for cybersecurity monitoring. Cybersecurity monitoring is considered a continuous activity as it occurs throughout the life cycle of an ADS-equipped vehicle.

NOTE 1 ISO/SAE 21434 includes requirements for continuous cybersecurity activities including cybersecurity monitoring.

As well as cybersecurity monitoring, continual cybersecurity activities also include cybersecurity event evaluation, vulnerability analysis and vulnerability management. These activities evaluate cybersecurity events to determine if they are exploitable vulnerabilities that could compromise the cybersecurity of the vehicle systems. Cybersecurity incident response activities can be required during operation.

NOTE 2 Organizations that adopt ISO/SAE 21434 have processes established to identify potential threats to ADS and to respond to incidents if needed.

9.2.4 Change management during the operational phase

There are different causes that can trigger a change to the ADS or the environment of the ADS as shown in [Figure 9](#). These include:

- changes needed in the ADS;
- changes in the ADS environment;

NOTE 1 Changes in the ADS environment can be outside the span of control or within the span of control of the ADS developer.

- field monitoring of safety metrics indicating higher risks than expected;
- field monitoring of safety-relevant cybersecurity threats where subsequent vulnerability management results in scenarios indicating higher risks than expected; and
- crashes or incidents.

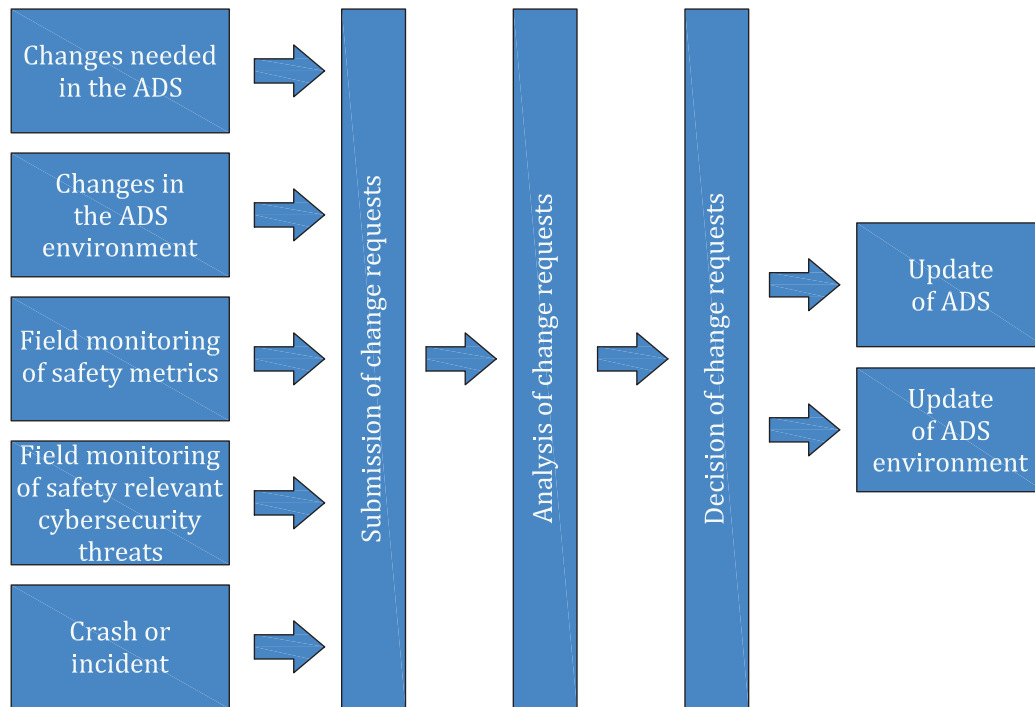


Figure 9 — Change management

Whenever an unreasonable risk is identified, a decision regarding mitigation strategies is needed, potentially changing the ADS, limiting the ODD or changing the ADS environment.

For managing unreasonable risks and improving the ADS, a robust change management process is needed. Changes to the affected vehicle population are typically made over-the-air, or in a workshop visit. Performance monitoring during the operational phase requires a careful balance between privacy and safety considerations.

Changes follow an appropriate way of working including:

- documentation of change requested;
- analysis of change requested;
- decision and rationale regarding the change request;
- implementation, verification and validation of the accepted changes; and
- update of documentation as needed.

NOTE 2 A change management process according to the ISO 26262 series is sufficient and appropriate.

Where there are ADS changes impacting the user interaction, there are some additional considerations, including notification and training.

9.2.5 Inspection, maintenance and repair

To ensure continuous safe operation of ADS-equipped vehicles, it is important to detect, prevent and repair defects and damage, including preventing potential defects due to wear-and-tear.

To detect defects and damage, procedures for inspection of the vehicles can be used. Inspection can be performed at different intervals, e.g. at each start-up or yearly. Such inspections can be made by a technician next to the vehicle, remotely or by diagnostic systems. In addition to inspections, preventive maintenance can be used to prevent defects from occurring. In particular, this can address faults with higher degrees of wear and tear or ageing.

If defects are detected, these are to be repaired using approved components and procedures to ensure fulfilment of requirements. Depending on the type of components that are defective, calibration and testing can be required according to approved processes.

For both preventive maintenance and repair, it is important that procedures are provided to ensure a level of functionality comparable to the original functionality.

9.2.6 Management of crashes and incidents

Ideally incidents are avoided, but in case of incidents during operation, it is important to be prepared. This includes ensuring that correct actions are taken before, during and after incidents. Actions that are prepared before incidents include instructions and processes as described in [7.2.2.4](#). In particular these include providing information for first responders.

In the case of crashes, actions are primarily taken by first responders. For near misses involving L3 ADS features, actions can also include requesting fallback-ready drivers to take over the DDT.

Actions to be taken after the incident can be grouped into two categories, those taken directly at the scene and those taken afterwards for follow-up and improvements.

The actions to be taken directly after the incident can include collecting data at the scene. Relevant data are collected from the site of the incident, and also from the vehicles and ADS external elements involved in the incident.

The actions following data collection at the scene are less time critical in general. These can include:

- key stakeholders, including authorities, are informed as appropriate and required;
- collected data are fed back to the field monitoring process (see [9.2.2](#));
- corrective actions are taken following a change management process (see [9.2.4](#)); and
- decision is made whether to resume automated operation.

9.3 Requirements and recommendations

9.3.1

Processes for field monitoring shall be established for the operation of ADS-equipped vehicles, including detection of crashes, incidents and changes in the ADS environment.

NOTE The processes for field monitoring includes monitoring to identify abnormal operation that can indicate cybersecurity threats.

9.3.2

Processes for change management shall be established for managing changes to the ADS or the ADS environment, including management of change requests, analysis of change requests, decisions regarding the change requests, implementation and verification of change requests and documentation of the changes.

NOTE 1 The ISO 26262 series describes how change management can be established.

NOTE 2 Change requests can be triggered by requested changes to the ADS and identification of crashes, incidents and changes in the ADS environment.

NOTE 3 Implementation of change requests can be done in the ADS or ADS environment.

NOTE 4 ISO 24089 covers update requirements for road vehicles.

9.3.3

Processes for inspection shall be established for the ADS-equipped vehicles to ensure detection of defects in these vehicles during operation.

9.3.4

Processes for preventive maintenance and repair shall be established for the operation of ADS-equipped vehicles to ensure continuous safe operation of the ADS-equipped vehicles.

9.3.5

Processes for incident management shall be established for managing crashes and incidents detected in the operation of ADS-equipped vehicles, including reporting of these to appropriate stakeholders.

NOTE Crashes and incidents are reported to stakeholders, which can be internal or external.

10 Verification and validation requirement considerations

10.1 General

Although [7.3](#) (verification) and [Clause 8](#) (validation) have different objectives, they have mutual dependencies and commonalities. [Clause 10](#) and [Annex H](#) are intended to elaborate these.

Refer to [Table C.1](#) for specific ISO/IEC standards addressing detailed V&V topics.

10.2 Example solution: Verification and validation

This example presents information on verification and validation to show how the requirements of [7.3.3](#) and [8.3](#) can be fulfilled. First of all, an overview of the V&V activities are given; followed by the description of a structured approach, see [H.1](#) and [H.2](#). Key V&V challenges and how they can be solved are elaborated in [H.3](#). [H.4](#) describes methods to maximize the quantity and quality of testing. [Annex H](#) closes with details concerning simulation as, for most ADS applications, this plays a significant part in V&V.