ISO/DTS 5083

ISO/TC 22/SC 32

~~ISO/CD TS 5083(en)~~

Secretariat: JISC

Date: 2024-11-05

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

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

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

Published in Switzerland

Contents

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Terms and definitions 1
3.1 Human-related terms 1

4 Abbreviated terms 8

5 Document overview and motivation 9
5.1 Purpose 9
5.2 Overall goals of this document 9
5.3 Application of this document 9
5.4 Safety life cycle 9
5.5 Description of ADS safety case 10
5.6 Role of the ADS within safe vehicle operation 17
5.7 Application of other standards 21
5.8 Safety principles of ADS 23

6 Safety strategy 25
6.1 Defining the ADS feature 25
6.2 Defining the risk acceptance criteria 27
6.3 Defining safety requirements 29

7 Safety by design 30
7.1 ADS design 30
7.2 ADS external design, pre-requisites and assumptions 31
7.3 ADS Verification 41
7.4 Verification and confirmation of aspects external to the ADS 42

8 Validation 43
8.1 Objectives 43
8.2 General 44
8.3 Requirements and recommendations 44
8.4 Example solution: Metrics 44
8.5 Example solution: Validation through computation of collision rates 44
8.6 Example solution: Generating evidence for injury risk assumptions external to the ADS 44

9 Operation of the ADS-equipped vehicle 45
9.1 Objectives 45
9.2 General 45
9.3 Requirements and recommendations 50

10 Verification and validation requirement considerations 51
10.1 General 51
10.2 Example solution: Verification and validation 51

Annex A (informative) Example application of the concepts of this document 52

Annex B (informative) Safety for artificial intelligence (AI) – Application to automated driving systems 63

Annex C (informative) List of related standards 83

Annex D (informative) Safety principles for ADS 88

Annex E (informative) Safety strategy example solutions 93
Annex F (informative) Safety by design and verification example solutions 130
Annex G (informative) Validation example solutions 170
Annex H (informative) Verification and validation example solutions 179
Bibliography 197

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 ~~documents~~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).

~~Attention is drawn~~ISO draws attention to the possibility that ~~some of~~ the ~~elements~~implementation of this document may ~~be~~involve the ~~subject~~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. ~~Details of any patent rights identified during the development of this document will be in the Introduction and/or on the ISO list of patent declarations received (see).~~

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

For an explanation ~~on~~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~~ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT~~)~~), see www.iso.org/iso/foreword.html~~the following URL:~~ .

This document was prepared by Technical Committee ISO/TC 22, *Road* ~~Vehicles~~*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 ~~compared to the previous edition~~ are as follows:

- a fully revised scope;
- the inclusion of objectives and requirements for normative clauses of the ~~TS~~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 ~~informative Annexes~~annexes with example applications and further considerations of ~~Artificial Intelligence~~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.

Introduction

Automated driving is one of the key emerging technologies for road vehicles, where major goals in deploying automated driving systems 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 ~~sub-system~~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

~~3.1 General~~

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

ISO and IEC maintain ~~terminological~~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/

~~3.2~~3.1 Human-related terms

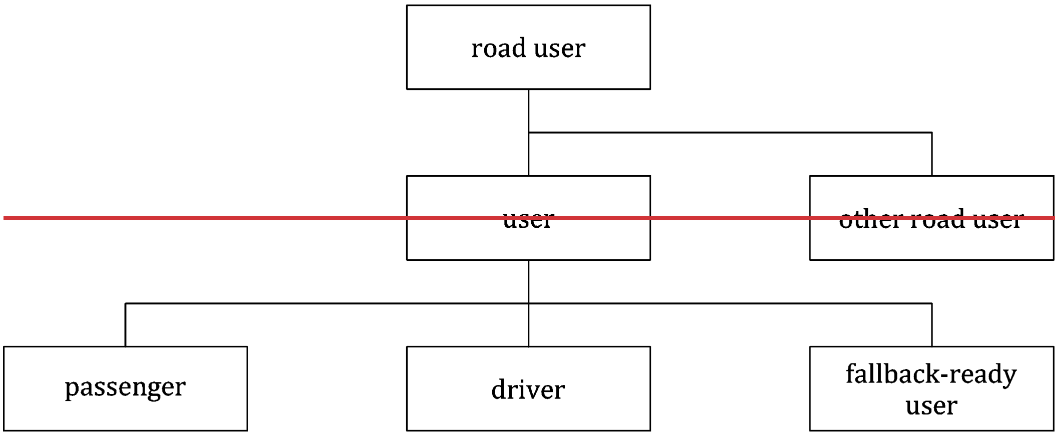
~~3.2.1~~3.1.1 **~~3.2.1~~**

road user

traffic participant on, or adjacent to, an active roadway

Note 1 to entry: ~~persons~~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.~~2~~1.2).



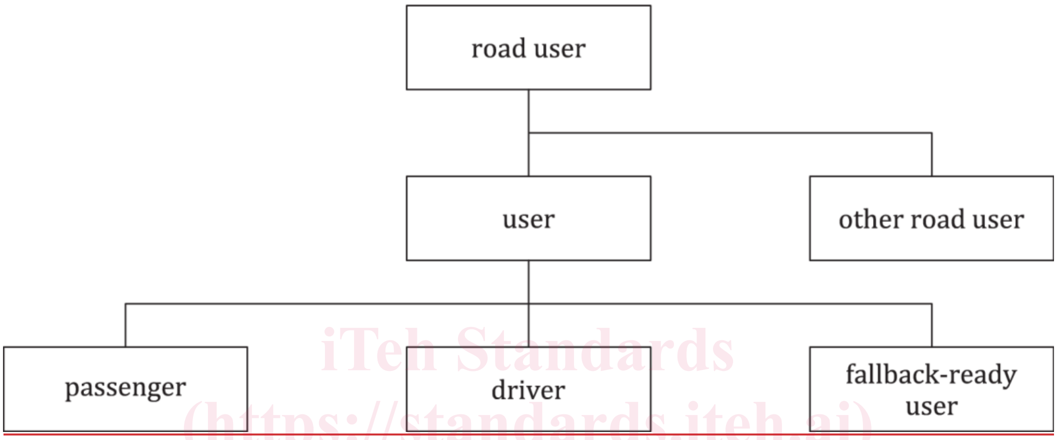


Figure 1 — Structure of human-related terms

[SOURCE: ~~with modification: removed~~ SAE J3216:2021, 4.13.1, modified — "for the purpose of travelling~~,~~ ~~added note 1~~" has been deleted and ~~note 2 with~~ the ~~overview figure of the term hierarchy~~notes to entry and Figure 1 were added.]

~~3.2.2~~3.1.2 ~~3.2.2~~

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 ~~Annex~~ A.6.

~~[SOURCE: , with modification: inserted "who has a" to comply with ISO insertion rule; removed "a general term referencing the", and note 1 regarding consistency with terms in this subclause, and not exhaustive.]~~

~~3.2.3~~3.1.3 ~~3.2.3~~

driver

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

EXAMPLE ~~person~~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: , with modification: grammatically rearranged the definition to match the substitution rule.]~~

~~3.2.4~~
[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 ~~free-ways~~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 ~~free-way~~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~~ with modification, to fit the substitution rule, on~~, modified — Examples 2 and 3 have been removed, a new example 2 ~~clarified "ADS-equipped vehicle" and singular usage, removed one note, and modified another~~has been added.]

~~3.2.4~~3.1.5 ~~3.2.5~~

fallback-ready user

user (3.1.2) of an engaged ~~Level~~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: ~~with modification: removed 'the',~~ISO/SAE PAS 22736:2021, 3.31.3, modified — 'of a vehicle equipped'~~,~~ has been deleted after "user" and ~~replaced 'with' by 'of', and removed~~ the notes ~~to focus on the definition~~have also been removed.]

~~3.2.5~~3.1.6 ~~3.2.6~~

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.

~~3.3~~3.2 ~~3.3~~

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~~ with modification, added note 1, added note 2~~, modified~~ some~~ — Note has been deleted and replaced by Note 1 to entry, Note 2 to entry was previously a modified portion of the definition~~ and made it note 3~~.]

~~3.4~~3.3 ~~3.4~~

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~~*ODD*~~) specification.

~~[SOURCE: with major modifications to fit to the scope of this document: focus on L3 and L4, removed notes and examples to focus on the application of the term in this document.]~~

~~3.5~~3.4 ~~3.5~~

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.~~4~~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~~[SOURCE: with modification: replaced "body of evidence" by "evidence", and "system" by "ADS".]~~

~~3.6~~], 13.2.1.

~~3.6~~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.

~~[SOURCE: , 3.7 with modification: removed "of a product" for consistency with the insertion rule.]~~

~~3.7~~

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 ~~3.8~~

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 ~~traffic-way~~trafficway, either moving or stationary (fixed or non-fixed), that is observable or in which kinetic energy is measurably transferred or dissipated

[SOURCE: ~~with modification: added 'ADS-equipped'; removed internal references~~ISO/TR 21974-1:2018, 3.4, modified — Added "ADS-equipped" and deleted notes to entry.]

3.8 ~~3.9~~

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: In this document, for the sake of brevity, the term cybersecurity is used instead of road vehicle cybersecurity.~~

~~Note 2 to~~ Note 1 to entry: This can include considerations of malicious modifications to the driving environment.

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

3.9 ~~3.10~~

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~~ with modification, removed~~, modified — "under routine/normal operating conditions within its given ODD", ~~removed 'for~~ "for complete ~~trips']~~trips" and Notes were deleted.]

3.10 ~~3.11~~

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

[SOURCE: ~~,~~ISO/SAE PAS 22736:2021, 3.10~~ with modification, fit~~, modified — Note 1 to ~~substitution rule by moving major text~~entry was previously part of the definition ~~to note 1,~~ and ~~deleted all~~ notes and figures ~~to focus on the definition~~were deleted.]

3.11 ~~3.12~~

DDT fallback

response by the *user* (3.1.2) to either perform the *dynamic driving task*(*DDT*) (3.10) or achieve ~~an~~ 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: ~~, 3.12 with modification, did not take over~~ISO/SAE PAS 22736:2021, 3.12, modified — Notes, examples and figures~~, as their meaning needs to be adapted for this document,~~ were deleted~~ all notes to focus on the definition~~.]

3.12 ~~3.13~~

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~~ with modification: Replaced ~~, modified — "item ~~by ADS~~ and ~~removed~~ element~~,~~" was replaced ~~'termination of'~~by "ADS", "termination of" was replaced by "deviation from" and Note 1 to ~~'deviation from'~~entry was deleted.]

3.13 ~~3.14~~

fault

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

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

3.14 ~~3.15~~

harm

physical injury or damage to the health of persons

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

3.15 ~~3.16~~

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 ~~3.17~~

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.

~~[SOURCE: , 2.9 with modification: split the definition to account differently for "event" and "anomaly" and added "in the future".]~~

3.17 ~~3.18~~

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~~ with modification, ~~, modified — "crash" replaced ~~"crash"~~ by "incident", ~~deleted all~~ notes and ~~examples to focus on the definition~~were deleted.]

3.18 ~~3.19~~

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 ~~an~~ a *minimal risk condition (MRC)* (3.~~18~~17)

3.19 ~~3.20~~
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:]~~

~~3.21~~
[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~~ with modification, replaced "~~, modified — "a given driving automation system" was replaced by "ADS~~",~~" and ~~deleted~~ all notes ~~to focus on the definition~~and examples were deleted.]

~~3.20~~3.21 ~~3.22~~
reasonably foreseeable
technically possible and with a credible or measurable rate of occurrence

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

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

~~3.21~~3.22 ~~3.23~~
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~~ with modification: Term is named as risk~~, modified — The term was originally acceptance criterion ~~instead of only acceptance criterion, emphasizing the risk aspect in the context of ADS safety~~and example 1 was removed.]

~~3.22~~3.23 ~~3.24~~
safe
free from *unreasonable risk* (3.26)

~~3.23~~3.24 ~~3.25~~
safety
absence of *unreasonable risk* (3.26)

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

~~3.24~~3.25 ~~3.26~~

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.

~~3.25~~3.26 ~~3.27~~

unreasonable risk

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

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

~~3.26~~3.27 ~~3.28~~

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~~ODD.~~).

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

~~3.27~~3.28 ~~3.29~~

verification

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

[SOURCE: ~~,~~ISO 26262-1:2018, 3.180~~ with modification: simplified definition, removed~~, modified —"activities to" was added, "whether or not" was deleted and ~~inserted "activities to".]~~the example was deleted.]

~~4 Abbreviations~~

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)