FINAL DRAFT
Technical Specification

ISO/DTS 5083

ISO/TC **22**/SC **32**

Secretariat: **JISC**

Voting begins on:
2024-11-21

Voting terminates on:
2025-01-16

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

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

iTeh Standards
(https://standards.iteh.ai)
Document Preview

ISO/DTS 5083
https://standards.iteh.ai/catalog/standards/iso/b0e17c08-7ba2-4f61-80d5-45fb0aa73f7e/iso-dts-5083

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

Reference number
ISO/DTS 5083:2024(en)

© ISO 2024

iTeh Standards
(https://standards.iteh.ai)
Document Preview

ISO/DTS 5083
https://standards.iteh.ai/catalog/standards/iso/b0e17c08-7ba2-4f61-80d5-45fb0aa73f7e/iso-dts-5083

COPYRIGHT PROTECTED DOCUMENT

© ISO 2024

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ISO/DTS 5083
https://standards.iteh.ai/catalog/standards/iso/b0e17c08-7ba2-4f61-80d5-45fb0aa73f7e/iso-dts-5083

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ISO/DTS 5083
https://standards.iteh.ai/catalog/standards/iso/b0e17c08-7ba2-4f61-80d5-45fb0aa73f7e/iso-dts-5083

iTeh Standards
(https://standards.iteh.ai)
Document Preview

ISO/DTS 5083
https://standards.iteh.ai/catalog/standards/iso/b0e17c08-7ba2-4f61-80d5-45fb0aa73f7e/iso-dts-5083

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.

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ISO/DTS 5083
https://standards.iteh.ai/catalog/standards/iso/b0e17c08-7ba2-4f61-80d5-45fb0aa73f7e/iso-dts-5083

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.

© ISO 2024 – All rights reserved

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 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.

iTeh Standards
(https://standards.iteh.ai)
Document Preview

ISO/DTS 5083
https://standards.iteh.ai/catalog/standards/iso/b0e17c08-7ba2-4f61-80d5-45fb0aa73f7e/iso-dts-5083

© ISO 2024 – All rights reserved

iTeh Standards
(https://standards.iteh.ai)
Document Preview

ISO/DTS 5083
https://standards.iteh.ai/catalog/standards/iso/b0e17c08-7ba2-4f61-80d5-45fb0aa73f7e/iso-dts-5083

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.

iTeh Standards
(https://standards.iteh.ai)
Document Preview

3 Terms and definitions

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

ISO/DTS 5083
https://standards.iteh.ai/catalog/standards/iso/b0c17c08-7be3-4f61-8045-45fb0ca73f7e/iso-dts-5083

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).

© ISO 2024 – All rights reserved

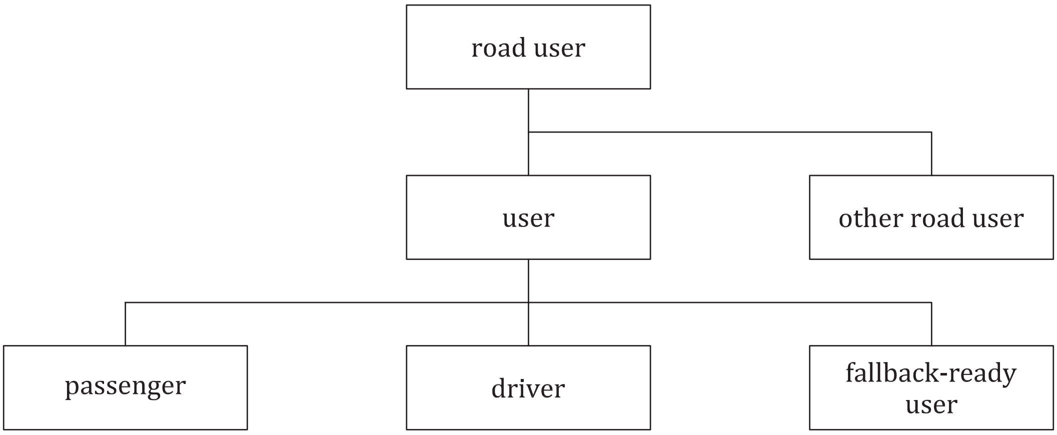

Figure 1 — Structure of human-related terms

[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.

iTeh Standards
(https://standards.iteh.ai)
Document Preview

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.

ISO/DTS 5083
https://standards.iteh.ai/catalog/standards/iso/b0e17c08-7ba2-4f61-80d5-451b0aa7317e/iso-dts-5083

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.]

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ISO/DTS 5083
https://standards.iteh.ai/catalog/standards/iso/b0e17c08-7ba2-4f61-80d5-45fb0aa73f7e/iso-dts-5083

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.]

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ISO/DTS 5083
https://standards.iteh.ai/catalog/standards/iso/b0e17c08-7ba2-4101-80d5-45180aa7317e/iso-dts-5083

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 was 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.

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ISO/DTS 5083
https://standards.iteh.ai/catalog/standards/iso/b0e17c08-7ba2-4f61-80d5-45160aa737c8/iso-dts-5083

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.]

© ISO 2024 – All rights reserved

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.]

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ISO/DTS 5083
https://standards.iteh.ai/catalog/standards/iso/b0e17c08-7ba2-4f61-80d5-45fb0aa73f7e/iso-dts-5083

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]

© ISO 2024 – All rights reserved