TECHNICAL REPORT

ISO/TR 4804

First edition

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

Véhicules routiers - Sécurité et cybersécurité pour les systèmes de conduite automatisée - Conception, vérification et validation

PROOF/ÉPREUVE

Reference number
ISO/TR 4804:2020(E)

COPYRIGHT PROTECTED DOCUMENT

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 v
Introduction vi
1 Scope 1
2 Normative references 1
3 Terms and definitions 1
4 General approach and overview 11
4.1 Introduction and motivation 11
4.2 Overview of this document 11
4.3 Structure and development examples used in this document 12
4.4 Safety vision 13
4.4.1 Background 13
4.4.2 Positive risk balance and avoidance of unreasonable risk 14
4.4.3 Principles of safety and cybersecurity for automated driving 14
5 Systematically developing dependability to support safety by design 17
5.1 General 17
5.2 Deriving capabilities of automated driving from dependability domains 18
5.2.1 Applying the related safety standards 18
5.2.2 ISO/PAS 21448 - Safety of the intended functionality 19
5.2.3 ISO 26262 series - Functional safety 19
5.2.4 ISO/SAE 21434 - Automotive cybersecurity 20
5.2.5 Capabilities of automated driving 21
5.2.6 Minimal risk conditions and minimal risk manoeuvres 25
5.3 Elements for implementing the capabilities 27
5.3.1 Implementing the capabilities 27
5.3.2 Elements 33
5.3.3 Generic logical architecture 45
6 Verification and validation 48
6.1 General 48
6.2 The scope and main steps of verification and validation for automated driving systems 49
6.3 Key challenges for verification and validation of SAE L3 and SAE L4 automated driving systems 50
6.3.1 Challenge 1: Statistical demonstration of avoidance of unreasonable risk and a positive risk balance without driver interaction 51
6.3.2 Challenge 2: System safety with driver interaction (especially in takeover manoeuvres) 51
6.3.3 Challenge 3: Consideration of scenarios currently not known 51
6.3.4 Challenge 4: Validation of various system configurations and variants 51
6.3.5 Challenge 5: Validation of (sub)systems that are based on machine learning 51
6.4 Verification and validation approach for automated driving systems 51
6.4.1 Defining test goals and objectives (why and how well) 52
6.4.2 Test design techniques (how) 52
6.4.3 Test platforms (where) 53
6.4.4 Test strategies in response to the key challenges 53
6.5 Quantity and quality of testing 57
6.5.1 Equivalence classes and scenario-based testing 58
6.6 Simulation 58
6.6.1 Types of simulation 60
6.6.2 Simulation scenario generation 61
6.6.3 Validating simulation 61
6.6.4 Further applications of simulation 62
6.7 Verification and validation of elements 62
6.7.1 A-priori information and perception (map) 63

6.7.2 Localization (including GNSS) 63
6.7.3 Environment perception sensors, V2X and sensor fusion 64
6.7.4 Interpretation and prediction, drive planning and traffic rules 64
6.7.5 Motion control 65
6.7.6 Monitor, ADS mode manager (including the vehicle state) 65
6.7.7 Human machine interaction and user state monitor 65
6.8 Field operation (monitoring, configuration, updates) 65
6.8.1 Testing traceability 65
6.8.2 Robust configuration and change management process 66
6.8.3 Regression prevention 67
6.8.4 Cybersecurity monitoring and updates 67
6.8.5 Continuous monitoring and corrective enforcement 67

Annex A (informative) **Development examples** **69**

Annex B (informative) **Using deep neural networks to implement safety-related elements for automated driving systems** **80**

Annex C (informative) **Principles of safety and cybersecurity for automated driving** **92**

Annex D (informative) **List of proposed standards** **95**

Bibliography **106**

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 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 to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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*.

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 modern technologies. In addition to offering broader access to mobility, it may also help to reduce the number of road traffic related accidents and crashes. When doing so, the safe operation of automated driving vehicles is one of the most important factors. Designed to supplement existing standards and publications on various aspects of safety, this document presents a more technical overview of the recommendations, guidance and methods to achieve a positive risk balance and to avoid unreasonable risk and cybersecurity related threats, emphasizing the importance of safety by design. This document closes the loop to provide a discussion with recommendations and methods on the verification and validation of automated driving systems.

Set forth are a proposed framework and guidelines focused on the safety and cybersecurity during the development, verification, validation, production and operation of automated driving systems for all stakeholders in the automotive and mobility world – from technology start-ups through to established OEMs and the tiered suppliers of key technologies.

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

1 Scope

This document describes steps for developing and validating automated driving systems based on basic safety principles derived from worldwide applicable publications. It considers safety- and cybersecurity-by-design, as well as verification and validation methods for automated driving systems focused on vehicles with level 3 and level 4 features according to SAE J3016:2018. In addition, it outlines cybersecurity considerations intersecting with objectives for safety of automated driving systems.

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 terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
automated driving system
ADS
set of *elements* (3.14) that offer a specific conditional or higher automated driving *use case* (3.63) in or for a specific *ODD* (3.37)

3.2
automated vehicle
AV
vehicle equipped with at least one conditional (SAE level 3) or higher (SAE level 4/level 5) *automated driving system* (3.1)

3.3
availability
capability (3.4) of a product to provide a stated function if demanded, under given conditions over its defined lifetime

Note 1 to entry: In the context of this document the product is the *automated driving system* (3.1).

Note 2 to entry: In the context of this document "availability" is defined solely referring to the automated driving system aspects and does not include human factor aspects.

[SOURCE: ISO 26262-1:2018, 3.7]

3.4
capability
ability of a product to deliver a function, feature or service

Note 1 to entry: In the context of this document the product is the *automated driving system* (3.1).

3.5
conventional driver
driver (3.11) who manually exercises in-vehicle braking, accelerating, steering and transmission gear selection input devices in order to operate the vehicle

[SOURCE: SAE J3016:2018, 3.29.1.1]

3.6
corner case
scenario (3.53) in which two or more parameter values are each within the *capabilities* (3.4) of the system, but together constitute a rare condition that challenges its capabilities

Note 1 to entry: In the context of this document the system is the *automated driving system* (3.1).

[SOURCE: ISO/PAS 21448:2019, Table 11]

3.7
crash
undesirable, unplanned event that leads to an unrecoverable loss due to unfavourable external conditions (e.g. human error), typically involving material damage, financial loss or human injuries and/or fatalities

3.8
cybersecurity
condition in which assets are sufficiently protected against threat *scenarios* (3.53) to electrical or electronic components of road vehicles and their functions

[SOURCE: ISO/SAE 21434]

3.9
degradation
state or transition to a state of the *item* (3.26) or *element* (3.14) with reduced functionality, performance, or both

Note 1 to entry: In the context of this document the item is the *automated driving system* (3.1).

[SOURCE: ISO 26262-1:2018, 3.28, modified — Note 1 to entry added.]

3.10
dependability
ability of a system to provide a service or function regarding the attributes of *reliability* (3.44), *availability* (3.3), maintainability, *safety* (3.51) and security (RAMSS)

Note 1 to entry: In the context of this document the system is the *automated driving system* (3.1).

3.11
driver
user (3.64) who performs in real-time part or all of the *DDT* (3.13) and/or DDT fallback for a particular vehicle

[SOURCE: SAE J3016:2018, 3.29.1, modified — The word "human" was removed from the term and the note was deleted.]

3.12
driver in the loop
DiL
execution of the target software on prototype or target hardware in the target vehicle or a mock-up, in which the environment is modified with virtual stimuli, and the driver's reaction influences the vehicle's behaviour

EXAMPLE Driving simulator or vehicle in the loop (ViL) (augmented reality for safety-related manoeuvres in real vehicles).

3.13
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: SAE J3016:2018, 3.13, modified — Note 1 to entry was previously part of the definition, the notes, figure and additional information were removed.]

3.14
element
at least first-level decomposition of *capabilities* (3.4) to a logical system architecture

Note 1 to entry: One or more elements realize one or more capabilities.

3.15
equivalence class
class being identified based on the division of inputs and outputs, such that a representative test value can be selected for each class

Note 1 to entry: See ISO 26262-6:2018, Table 8.

3.16
fail-degraded
property of the *item* (3.26) to operate with reduced functionality in the presence of a *fault* (3.20)

Note 1 to entry: This property can be realized as fail-degraded *capability* (3.4) of fail-degraded mode.

Note 2 to entry: In the context of this document the item is the *automated driving system* (3.1).

Note 3 to entry: This means that the item is fault-tolerant for a subset of its intended functionality.

Note 4 to entry: The absence of *unreasonable risk* (3.62) can require the duration of the presence of the fault to be time limited and/or system maintenance in a limited time frame.

Note 5 to entry: The absence of unreasonable risk in the presence of the fault can require limitations of the item behaviour.

3.17
fail-operational
property of the *item* (3.26) to maintain its full intended functionality in the presence of a *fault* (3.20)

Note 1 to entry: In the context of this document the item is the *automated driving system* (see 3.1).

Note 2 to entry: This means that the item is fault-tolerant for its intended functionality.

Note 3 to entry: The absence of *unreasonable risk* (3.62) can require the duration of the presence of the fault to be time limited and/or system maintenance in a limited time frame.

3.18
fail-safe
property of an *automated driving system* (3.1) to achieve a *minimal risk condition* (3.29) and to achieve a *safe state* (3.50) in the event of a *failure* (3.19)

Note 1 to entry: A fail-safe condition is to be reached for example, by means of: demanding the vehicle control to driver/vehicle *operator* (3.39) and/or switching off the automated driving function.

3.19
failure
termination of an intended behaviour of an *element* (3.14) or the *automated driving systems* (3.1) due to a *fault* (3.20) manifestation

[SOURCE: ISO 26262-1:2018, 3.50, modified – The term "automated driving system" replaces "item" and Note 1 to entry is not included here.]

3.20
fault
abnormal condition that can cause an *element* (3.14) or the *automated driving system* (3.1) to fail

[SOURCE: ISO 26262-1:2018, 3.54, modified – The term "automated driving system" replaces "item" and Notes to entry are not included here.]

3.21
field operational testing
FOT
use of large-scale testing programs aimed at generating a comprehensive assessment of the efficiency, quality, robustness and acceptance of transport solutions

3.22
high definition map
HD map
maps with high level precision mostly used in the context of *automated driving system* (3.1) to give the vehicle precise information about the road environment

3.23
hardware in the closed loop
HiL
execution of target software on target hardware, whereby the hardware outputs influence the hardware inputs

Note 1 to entry: HiL executes the target software in real time.

EXAMPLE AUTOSAR stack on radar with no frontend.

3.24
hardware open loop
HoL
execution of target software on target hardware, whereby the hardware outputs do not influence the hardware inputs

EXAMPLE Monitor hardware testbench.

3.25
human-machine interaction
interdisciplinary interaction between a human and an *automated vehicle* (3.2), considering the human-machine interface (HMI) with the aim to develop a user interface that satisfies requirements regarding mental, cognitive and manual abilities of the *user* (3.64)

3.26
item
system or combination of systems, that implements a function or part of a function at the vehicle level

[SOURCE: ISO 26262-1:2018, 3.84, modified — The phrase “to which ISO 26262 is applied” and the Note 1 to entry are deleted.]

3.27
lagging measure
metrics that are assessed after deployment of an *automated driving system* (3.1) and provide confirmation that the *positive risk balance* (3.42) as well as the conformance with the safety-by-design techniques have been achieved

EXAMPLE Statistics for *crashes* (3.7) or other *safety* (3.51) events.

Note 1 to entry: See Reference [1].

3.28
leading measure
metrics that are derived from data that is assessed prior to deployment of an *automated driving system* (3.1) indicating that the automated driving system conforms with safety-by-design techniques to achieve a *positive risk balance* (3.42) and avoidance of *unreasonable risk* (3.62)

EXAMPLE A design *verification* (3.67) that the HMI guidelines were incorporated into the vehicle’s design.

Note 1 to entry: See Reference [1].

3.29
minimal risk condition
MRC
condition to which a *user* (3.64) or an *automated driving system* (3.1) may bring a vehicle after performing the *minimal risk manoeuvre* (3.30) in order to reduce the risk of a *crash* (3.7) when a given trip cannot be completed

Note 1 to entry: The minimal risk condition integrates the meaning of avoidance of *unreasonable risk* (3.62), according to the ISO 26262:2018 series. They can be combined but they never exclude one each other.

[SOURCE: SAE J3016:2018, 3.17, modified — The term “minimal risk manoeuvre” replaces “DDT fallback”, the notes and examples were deleted and the Note 1 to entry was added.]

3.30
minimal risk manoeuvre
MRM
automated driving system’s (3.1) *capability* (3.4) of transitioning the vehicle between nominal and *minimal risk conditions* (3.29)

3.31
operating mode awareness
driver’s (3.11) *capability* (3.4) to identify the current automation mode and his/her driving responsibility

3.32
naturalistic driving study
NDS
driving study where research subjects are recruited to drive on public roads (not in a simulator or on a test track), where there is no in-vehicle experimenter or confederate vehicles, and where driving conditions are not experimentally controlled or manipulated

Note 1 to entry: Subjects are not instructed to drive differently than they normally would and the data collection instrumentation is unobtrusive.

Note 2 to entry: Typically, these studies last a minimum of several weeks for each subject and can go much longer.

Note 3 to entry: An approach during which the driver becomes unaware of observation as data is collected as discreetly as possible. This data is then used to examine the relationship between the driver, vehicle and/or environment.

3.33
nominal performance
performance of the system free from *fault* (3.20) and that meets its defined performance criteria

3.34
non-vulnerable road user
protected *road users* (3.46) such as *users* (3.64) in other vehicles, trucks, construction and agricultural machines

3.35
object under test
OuT
item (3.26) or *element* (3.14) to be tested as planned and specified

Note 1 to entry: Similar usage as ISO 16750 for device under test.

3.36
open road testing
execution of target software on target hardware in the target vehicle with a *driver* (3.11), whereby the driving environment is real, road infrastructures are public and can be only partially controlled

EXAMPLE *Field operational testing* (3.21) or *naturalistic driving studies* (3.32), testing in the development vehicles.

3.37
operational design domain
ODD
operating conditions under which a given *automated driving system* (3.1) 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

Note 1 to entry: These limitations, as from constraints as specified in operating conditions, reflect the technological *capability* (3.4) of the automated driving system.

[SOURCE: SAE J3016:2018, 3.22, modified — Note 1 to entry is added, and the note and examples are not included here.]

3.38
ODD functional adaptation
operational design domain functional adaptation
property of a system to operate safely with reduced performance in the case of detected functional insufficiencies inside the *ODD* (3.37)

EXAMPLE Speed adaptation because of low fuel level, or dense fog, or sensor performance insufficiencies.

3.39
operator
designated person, appropriately trained and authorized, to operate the vehicle

3.40
other road user
vulnerable road users (3.68) and *non-vulnerable road users* (3.34) with no role in the ego *automated vehicle* (3.2)

3.41
passenger
user (3.64) in a vehicle who has no role in the operation of that vehicle

3.42
positive risk balance
benefit of sufficiently mitigating residual risk of traffic participation due to *automated vehicles* (3.2)

Note 1 to entry: This includes the expectation that automated vehicles cause less *crashes* (3.7) on average compared to those made by drivers.

Note 2 to entry: Positive risk balance is one of the concepts that can be considered when defining the acceptance criteria of ISO/PAS 21448:2019.

3.43
proving ground testing
execution of target software on target hardware in the target vehicle in a realistic but controlled and private driving environment

Note 1 to entry: The driver can be real or a robot.

EXAMPLE Emergency braking assistant tests on soft crash target.

3.44
reliability
ability of a system to continuously provide correct service

3.45
reprocessing
replay of time stamped, recorded data to provide input for the *object under test* (3.35)

Note 1 to entry: The time stamp needs a sufficient time accuracy.

3.46
road user
anyone who uses a road including sidewalk and other adjacent spaces

Note 1 to entry: Relationship between the human related terms are shown in Figure 1.