TECHNICAL REPORT

ISO/TR 4804

First edition
2020-12

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

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

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).