

Taxonomy and Definition of Safety Principles for Automated Driving System (ADS)

RATIONALE

For automated driving systems (ADSs) and ADS-equipped vehicles, there are many interpretations of what constitutes a “safety principle.” Some principles focus on design and development, some on behavior, and others on maintenance and support of ADS-equipped vehicles. With the variety of information and attempts at defining ADS safety principles available for industry and public alike, the need for clarification on classification and definitions of safety principles has become urgent.

The clarification on classification and definitions will enable the industry to have a common taxonomy and terminology when discussing safety principles and will serve to facilitate ADS developers in applying and adhering to appropriate principles for safer design, development, and deployment of ADS-equipped vehicles.

In addition to the recognized need for ADS safety principles by the industry itself, the National Highway Traffic Safety Administration (NHTSA) has also called upon SAE to define and develop a set of safety principles for industry use. This document is intended to respond to these needs.

1. SCOPE

This SAE Information Report classifies and defines a harmonized set of safety principles intended to be considered by ADS and ADS-equipped vehicle development stakeholders. The set of safety principles herein is based on the collection and analysis of existing information from multiple entities, reflecting the content and spirit of their efforts, including:

- SAE ITC AVSC Best Practices
- CAMP Automated Vehicle Research for Enhanced Safety - Final Report
- RAND Report - Measuring Automated Vehicle Safety: Forging a Framework
- U.S. DOT: Automated Driving Systems 2.0 - A Vision for Safety
- Safety First for Automated Driving (SaFAD)
- UNECE WP29 amendment proposal
- UNECE/TRANS/WP.29/GRVA/2019/13
- On a Formal Model of Safe and Scalable Self-Driving Cars (Intel RSS model)
- SAE J3018

SAE Executive Standards Committee Rules provide that: “This report is published by SAE to advance the state of technical and engineering sciences. The use of this report is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user.”

SAE reviews each technical report at least every five years at which time it may be revised, reaffirmed, stabilized, or cancelled. SAE invites your written comments and suggestions.

Copyright © 2021 SAE International

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of SAE.

TO PLACE A DOCUMENT ORDER: Tel: 877-606-7323 (inside USA and Canada)
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
http://www.sae.org

SAE WEB ADDRESS:

Full document details: SAE J3206_202107

For more information on this standard, visit
https://www.sae.org/standards/content/J3206_202107

Documents

Document Sharing Hub

This SAE Information Report provides guidance for the consideration and application of the safety principles for the development and deployment of ADS and ADS-equipped vehicles. This SAE Information Report is not intended to encompass all aspects of system-level safety for an ADS-equipped vehicle, including communication with other traffic participants. Addressing all identified safety principles is intended to support, but not fully ensure, comprehensive system-level safety.

As an SAE Information Report, this document is non-normative, imposes no requirements, and does not address:

- Requirements for methodology, metrics, and/or acceptance thresholds.
- Ethics-related safety principles, or any link between the safety principles defined in this document and ethical studies/frameworks.
- Conformance with safety principles for purposes of liability and/or fault assignment.

As ADS technology and deployment are expanded in the future, this document may be reconsidered for future revision including normative requirements.

2. REFERENCES

2.1 Applicable Documents

The following publications form a part of this specification to the extent specified herein. Unless otherwise indicated, the latest issue of SAE publications shall apply.

2.1.1 SAE Publications

Available from SAE International, 400 Commonwealth Drive, Warrendale, PA 15096-0001, Tel: 877-606-7323 (inside USA and Canada) or +1 724-776-4970 (outside USA), www.sae.org.

SAE J1698	Event Data Recorder
SAE J3016	Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles
SAE J3018	Safety-Relevant Guidance for On-Road Testing of Prototype Automated Driving System (ADS)-Operated Vehicles
SAE J3171	Identifying Automated Driving System-Dedicated Vehicles (ADS-DVs) Passenger Issues for Persons with Disabilities
SAE J3197	Automated Driving System Data Logger
SAE J3216	Taxonomy and Definitions for Terms Related to Cooperative Driving Automation for On-Road Motor Vehicles
AVSC00001201911	AVSC Best Practice for In-Vehicle Fallback Test Driver Selection, Training, and Oversight Procedures for Automated Vehicles Under Test
AVSC00002202004	AVSC Best Practice for Describing an Operational Design Domain: Conceptual Framework and Lexicon
AVSC00003202006	AVSC Best Practice for Passenger-Initiated Emergency Trip Interruption
AVSC00004202009	AVSC Best Practice for Data Collection for Automated Driving System-Dedicated Vehicles (ADS-DVs) to Support Event Analysis
AVSC00005202012	Best Practice for First Responder Interactions with Fleet-Managed Automated Driving System-Dedicated Vehicles (ADS-DVs)

2.1.2 ISO Publications

Copies of these documents are available online at <http://webstore.ansi.org/>.

ISO 26262-1:2018 Road Vehicles - Functional Safety - Part 1: Vocabulary

ISO 26262-2:2018 Road Vehicles - Functional Safety - Part 2: Management of Functional Safety

ISO/PAS 21448:2019 Road Vehicles - Safety of the Intended Functionality

ISO/TS 21974-1:2018 Naturalistic Driving Studies - Vocabulary - Part 1: Safety Critical Events

2.1.3 Code of Federal Regulations (CFR) Publications

Available from the United States Government Printing Office, 732 North Capitol Street, NW, Washington, DC 20401, Tel: 202-512-1800, www.gpo.gov.

49 CFR Part 563 Event Data Recorders

2.1.4 UL Publications

Available from UL, 333 Pfingsten Road, Northbrook, IL 60062-2096, Tel: 847-272-8800, www.ul.com.

UL 4600 Ed.1 Standard for Evaluation of Autonomous Products

2.1.5 Other Publications

Aptiv Services U.S., LLC, et al., "Safety First for Automated Driving," 2019.

Blumenthal, M.S., Fraade-Blanan, L., Best, R., and Irwin, J.L., "Safe Enough: Approaches to Assessing Acceptable Safety for Automated Vehicles," Santa Monica, Calif.: RAND Corporation, RR-A569-1, 2020. As of December 18, 2020: https://www.rand.org/pubs/research_reports/RR-A569-1.html.

Crash Avoidance Metrics Partnership on behalf of the Automated Vehicle Research, "Consortium Automated Vehicle Research for Enhanced Safety Final Report," June 2016. DTNH22-050-H-01277, <https://www.regulations.gov/document/NHTSA-2014-0070-0003>.

Fraade-Blanan, L., Blumenthal, M.S., Anderson, J.M., and Kalra, N., "Measuring Automated Vehicle Safety: Forging a Framework," RAND Corporation, RR-2662, 2018, https://www.rand.org/pubs/research_reports/RR2662.html.

Shalev-Schwartz, et al., "On a Formal Model of Safe and Scalable Self-Driving Cars," arXiv.org:1708.06734, 2017.

U.S. DOT: "Automated Driving Systems 2.0 - A Vision for Safety," 2017, https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf.

United Nations ECE Global Forum for Road Traffic Safety (WP.1), "Resolution on the Deployment of Highly and Fully Automated Vehicles in Road Traffic," 2018, <https://unece.org/transport/publications/resolution-deployment-highly-and-fully-automated-vehicles-road-traffic>.

United Nations ECE/TRANS/WP.29/2019/34, "Framework Document on Automated/Autonomous Vehicles (Levels 3 and Higher) - Amendment Proposal," 2019, <https://unece.org/fileadmin/DAM/trans/doc/2019/wp29/WP.29-178-10r2e.pdf>.

United Nations ECE/TRANS/WP.29/GRVA/2019/13, "Proposal for the Future Certification of Automated/Autonomous Driving Systems," 2019, <https://unece.org/DAM/trans/doc/2019/wp29grva/ECE-TRANS-WP29-GRVA-2019-16e.docx>.

3. DEFINITIONS

3.1 AUTOMATED DRIVING SYSTEM (ADS) (SAE J3016)

The hardware and software that are collectively capable of performing the entire DDT on a sustained basis, regardless of whether it is limited to a specific operational design domain (ODD); this term is used specifically to describe a Level 3, 4, or 5 driving automation system.

Further details can be found in SAE J3016.

3.2 ADS-DEDICATED VEHICLE (ADS-DV) (SAE J3016)

An ADS-equipped vehicle designed for driverless operation under routine/normal operating conditions during all trips within its given ODD (if any).

Further details can be found in SAE J3016.

3.3 (ADS SAFETY PRINCIPLE) CLASSIFICATION

Collection of safety principles that are common to a specific aspect in the design and development, behavior, or support and maintenance of an ADS-equipped vehicle.

3.4 CONFLICT (Adapted from ISO 21974)

Situation where the trajectory(ies) of one or more road users (including subject vehicle) or objects (conflict partner) led to one of three results:

1. A crash or road departure,
2. A situation where an evasive manoeuvre(s) was required to avoid a crash or road departure, or
3. A hazardous proximity between the conflict partners.

3.5 DRIVERLESS OPERATION (OF AN ADS-EQUIPPED VEHICLE) (SAE J3016)

On-road operation of an ADS-equipped vehicle that is unoccupied, or in which on-board users are not drivers or in-vehicle fallback-ready users.

Further details can be found in SAE J3016.

3.6 DRIVING AUTOMATION SYSTEM OR TECHNOLOGY (SAE J3016)

The hardware and software that are collectively capable of performing part or all of the DDT on a sustained basis; this term is used generically to describe any system capable of Level 1 to 5 driving automation.

Further details can be found in SAE J3016.

3.7 (ADS-EQUIPPED) DUAL-MODE VEHICLE (SAE J3016)

An ADS-equipped vehicle designed to enable either driverless operation under routine/normal operating conditions within its given ODD (if any), or operation by an in-vehicle driver, for complete trips.

Further details can be found in SAE J3016.

3.8 DYNAMIC DRIVING TASK (DDT) (SAE J3016)

All of the real-time operational and tactical functions required to operate a vehicle in on-road traffic, excluding the strategic functions such as trip scheduling and selection of destinations and waypoints, and including, 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).
- Maneuver planning (tactical).
- Enhancing conspicuity via lighting, signaling and gesturing, etc. (tactical).

Further details can be found in SAE J3016.

3.9 (DDT) FALLBACK (SAE J3016)

The response by the user to either perform the DDT or achieve a minimal risk condition (1) after occurrence of a DDT performance-relevant system failure(s), or (2) upon operational design domain (ODD) exit, or the response by an ADS to achieve minimal risk condition, given the same circumstances.

Further details can be found in SAE J3016.

3.10 FALLBACK TEST DRIVER (SAE J3018)

A person specially trained and skilled in supervising the performance of prototype ADS-operated vehicles in on-road traffic for testing purposes.

Further details can be found in SAE J3018.

3.11 (DDT) FALLBACK-READY USER (SAE J3016)

The user of a vehicle equipped with an engaged Level 3 ADS feature 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 in the vehicle compelling him or her to perform the DDT fallback.

Further details can be found in SAE J3016.

3.11.1 REMOTE FALLBACK READY USER (SAE J3016)

A fallback-ready user of a Level 3 ADS-equipped vehicle in driverless operation who is not in the driver's seat.

Further details can be found in SAE J3016.

3.12 MINIMAL RISK CONDITION (MRC) (SAE J3016)

A stable, stopped condition to which a user or an ADS may bring a vehicle after performing the DDT fallback in order to reduce the risk of a crash when a given trip cannot or should not be continued.

Further details can be found in SAE J3016.