AVSC-D-02-2024

Issued 2024-05

Automated Vehicle Safety Consortium™ Best Practice

Automated Vehicle Safety Consortium™
A Program of SAE ITC

AVSC Best Practice for Core Automated Vehicle Safety Information

Citation: Automated Vehicle Safety Consortium. 2024. AVSC Best Practice for Core Automated Vehicle Safety Information. SAE Industry Technologies Consortia.

Rationale

Numerous efforts have been made to establish common practices to communicate automated vehicle (AV) safety. These include white papers, best practices, technical specifications, standards, and more. Further guidance may be helpful to automated driving system (ADS) manufacturers, developers, and fleet operators so they can consistently share clear information on their safety approach to relevant stakeholders. Explainability to diverse audiences helps build trust in statements from these organizations towards the shared value of safety. A defined list of core safety topics helps set expectations when communicating AV safety information. This document serves as a complementary resource to existing materials, such as Voluntary Safety Self-Assessments (VSSAs)[1] and an organization's safety case. The topics listed in this document highlight focus areas for communicating safety information while remaining implementation-agnostic and broadly applicable. The information communicated should be deployment- and use-case-specific.

[1] For additional information, refer to: https://www.nhtsa.gov/automated-driving-systems/voluntary-safety-self-assessment.

Preface

The Automated Vehicle Safety Consortium™ (AVSC) is an industry program of SAE Industry Technologies Consortia® (SAE ITC). The AVSC shares information to inform and accelerate industry-wide standards and advance the safe development, deployment, and fleet operations of automated driving systems (ADSs). The members of this consortium have decades of accumulated experience, including millions of cumulative miles of physical and simulated ADS testing focused on safer, reliable, high-quality transportation. They are committed to applying their experience and combined knowledge to earn public confidence in the safe operation of SAE level 4 and level 5 fleet-managed automated vehicles.

The wide range of technologies, use cases, and operating domains create unique challenges with public perception of ADSs. The consortium recognizes the beneficial role best practices and information reports can have for the industry and for the safe operation of SAE level 4 and level 5 automated driving system-dedicated vehicles (ADS-DVs). These technology-neutral documents provide key considerations for safely deploying ADS-DVs on public roads. AVSC documents are based on current state-of-the-art technology and the experiences of the AVSC members. AVSC members currently support, or intend to support, the best practices or equivalent measures to set a bar for other industry participants to meet.

Technology advances rapidly, and new information is becoming available at an increasing rate. The AVSC's best practices and information reports are living documents. As knowledge and experience grow, our publications will be revisited and updated, as needed, to continue to support the safer on-road use of ADS-DVs. Comments and open discussion on the topics are welcome in appropriate industry forums.

Introduction

Communicating safety is key to public trust and acceptance. The structure, content, and level of detail included in existing information provided by ADS manufacturers, developers, and fleet operators are often informed by the particular use case and intended audience of such publications. Tailored safety guidelines have been developed by both industry and industry standards organizations. Examples include:

- *Aurora's Safety Case Framework* (2023) [1].
- British Standards Institute PAS 1881 *Assuring the Operational Safety of Automated Vehicles* (2022) [2].
- *Edge Case Research's Open Autonomy Safety Framework* (2023) [3].
- UL 4600 *Standard for Safety for Evaluation of Autonomous Products* (2023) [4].
- Uber's *Safety Guidelines for Autonomous Mobility and Delivery Providers on the Uber Platform* (2022) [5].
- Waymo's *Building a Credible Case for Safety* (2023) [6].

In addition to the safety guidelines above, some organizations have published additional safety-related information and benchmarking to clarify requirements and build on existing frameworks. These include:

- *Aurora Safety Report* (2022) [7].
- *The Cruise Safety Report* (2022) [8].
- *Waymo's Safety Methodologies and Safety Readiness Determinations* (2020) [9] and additional safety publications [10].
- Zoox's *Safety Report Volume 2.0* (2021) [11].

Each of the documents above are supported by efforts that address the systems engineering methodologies used, hazards identified and addressed, validation and verification tests performed, organizational safety activities, and deployment of specific analyses.

In addition, some regulatory bodies, government agencies, and research institutions have provided varying levels of guidance to help analyze, identify, and resolve safety issues prior to deployment in documents such as:

- NHTSA's *Automated Driving Systems 2.0: A Vision for Safety* (2017) [12].
- UK government's *Code of Practice: Automated Vehicle Trialling* [13].
- Transport Canada's *Guidelines for Testing Automated Driving Systems in Canada* [14].

Safety is a shared value, and trust in manufacturers, developers, and fleet operators' statements requires explainability to diverse audiences. Sharing a full safety case would be challenging for a number of reasons, including:

- Supporting documentation and terminology may be specific to the ADS developer, manufacturer, or operator and require specialized knowledge to understand.
- Supporting documentation may be extensive, including a large volume of technical output, possibly including test results and process documentation which may require the use of proprietary tools to access or interpret.
- The proprietary nature of certain information, along with sensitivities associated with the potential for inaccurate extrapolations of shared or reported data.

The development of a common language and framing to summarize core ADS safety topics and information—provided at a reasonable level of technical depth—can be beneficial as a stepping stone for industry stakeholders. This document is not intended to suggest any specific communication structure, formatting, precise composition, or modality. It is intended only to provide a set of topics or elements that speak broadly to core ADS-DV safety.

Not all recipients of AV safety information may require or be in a position to evaluate the same amount of information. The objective of this best practice is to identify and describe safety topics that may be considered core to an ADS manufacturer's, developer's, and operator's safety approach.

Table of Contents

1. Scope

This best practice outlines broadly applicable safety information for ADS-DVs. It provides a list of recommended topics, examples where applicable, suggestions of content that could be included for said topics, and relevant references and industry standards. Communicating safety information with the general public is outside the scope of this document. For this, readers are directed to company VSSAs [15] and other publicly available safety information. This information is intended for proactive safety discussions and does not address specific crash documentation or incident reconstruction connected to existing reporting obligations. These are available through other means, such as NHTSA's Standing General Order [16].

1.1 Purpose

This best practice is intended for use by the development and deployment communities (developers, operations, testers, etc.) to aid in consolidating core safety information for ADS-DVs. It supports public and private organizations in preparing for and deploying ADS-DV systems. The intention is to facilitate the communication of AV safety information between relevant parties as complementary to the information included in an organization's VSSA. The information should be tailored to the specific circumstances of the relevant parties, and its breadth and depth may vary accordingly.

This document may be used to illustrate an initial set of core safety topics that have been addressed by the provider. These topics may be adapted or modified as providers address specific considerations related to the technology or application for an ADS. This best practice is intended to garner discussion, foster understanding, and promote acceptance of ADS-DVs.

Note that some information on provided topics may be confidential, proprietary, or competitively sensitive. In some contexts, the manufacturer, developer, or operator may reasonably deem certain proprietary information inappropriate for sharing. When information is shared externally, the recipient should take all appropriate measures, including those agreed upon with the provider, to control access and how it is used. This document is not intended to create any expectation that an ADS manufacturer, developer, or operator shares confidential, proprietary, or competitively sensitive information.

2. References

2.1 Applicable Documents

The following publications were referenced during the development of this document. Where appropriate, documents are cited.

2.1.1 SAE Publications

Unless otherwise indicated, the latest issues of SAE publications apply. 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.

AVSC-I-01-2024	AVSC Best Practice for First Responder Interactions with Fleet-Managed Automated Driving System-Dedicated Vehicles (ADS-DVs)
AVSC-I-04-2023	AVSC Best Practice for ADS Remote Assistance Use Case
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
AVSC00006202103	AVSC Best Practice for Metrics and Methods for Assessing Safety Performance of Automated Driving Systems (ADS)
AVSC00007202107	AVSC Information Report for Adapting a Safety Management System (SMS) for Automated Driving System (ADS) SAE Level 4 and 5 Testing and Evaluation
AVSC00008202111	AVSC Best Practice for Evaluation of Behavioral Competencies for Automated Driving System Dedicated Vehicles (ADS-DVs)
AVSC00009202208	AVSC Best Practice for Interactions Between ADS-DVs and Vulnerable Road Users (VRUs)
AVSC00010202304	AVSC Information Report for Change Risk Management
AVSC00011202307	AVSC Best Practice for Continuous Monitoring and Improvement after Deployment
AVSC00012202308	AVSC Best Practice for Developing ADS Safety Performance Thresholds Based on Human Driving Behavior
ISO/SAE21434	Road Vehicles - Cybersecurity Engineering
SAE J1698_202303	Event Data Recorder
SAE J2728-1_202006	Heavy Vehicle Event Data Recorder (HVEDR) - Data and Triggers
SAE J2980_202310	Considerations for ISO 26262 ASIL Hazard Classification
SAE J3016_202104	Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles
SAE J3018_202012	Safety-Relevant Guidance for On-Road Testing of Prototype Automated Driving System (ADS)-Operated Vehicles
SAE J3061_201601	Cybersecurity Guidebook for Cyber-Physical Vehicle Systems
SAE J3114_201612	Human Factors Definitions for Automated Driving and Related Research Topics
SAE J3131_202203	Definitions for Terms Related to Automated Driving Systems Reference Architecture
SAE J3187_202305	System Theoretic Process Analysis (STPA) Recommended Practices for Evaluations of Safety-Critical Systems in Any Industry
SAE J3197_202107	Automated Driving System Data Logger
SAE J3206_202107	Taxonomy and Definition of Safety Principles for Automated Driving System (ADS)

2.1.2 Other Documents

[1] Aurora. (2023, January). *Aurora's safety case framework*. https://safetycaseframework.aurora.tech/gsn

[2] The British Standards Institution. (2022). *Assuring the operational safety of automated vehicles* (BSI Standard No. PAS 1881:2022). https://knowledge.bsigroup.com/products/assuring-the-operational-safety-of-automated-vehicles-specification?version=standard

[3] Edge Case Research. (2023). *Edge Case Research's open autonomy safety framework*. www.ecr.ai/s/Edge-Case-Safety-Framework-Announcement.pdf

[4] UL. (2023). *Standard for safety for evaluation of autonomous products* (UL Standard No. UL 4600). https://www.shopulstandards.com/ProductDetail.aspx?productid=UL4600

[5] Uber. (2022, September 7). *Safety guidelines for autonomous mobility and delivery providers on the Uber platform*. www.uber.com

[6] Favarò, F., Fraade-Blanar, L., Schnelle, S., Victor, T., Peña, M., Engstrom, J., Scanlon, J., Kusano, K., & Smith, D. (2023). *Building a credible case for safety: Waymo's approach for the determination of absence of unreasonable risk*. Waymo. www.waymo.com/safety

[7] Aurora. (2022). *Aurora safety report.* https://blog.aurora.tech/safety/auroras-2022-safety-report

[8] Zhang, L. (2022, November 21). *The Cruise Safety Report: Advancing our safety mission through a transparent and holistic approach*. Cruise. https://www.getcruise.com/news/blog/2022/the-cruise-safety-report-advancing-our-safety-mission-through-a-transparent-and-holistic-approach/

[9] Webb, N., Smith, D., Ludwick, C., Victor, T., Hommes, Q., Favaro, F., Ivanov, G., & Daniel, T. (2020). *Waymo's safety methodologies and safety readiness determinations*. Waymo. https://arxiv.org/abs/2011.00054

[10] Waymo. (2023). *Safety publications.* https://waymo.com/safety/#:~:text=human%2Ddriven%20vehicles.-,Safety%20Publications,-Year

[11] Zoox. (2021). *Purpose-built for safety: Introducing Zoox safety innovations. Setting the bar for safety in autonomous mobility: Safety report volume 2.0.* https://www.datocms-assets.com/106048/1696536139-zoox_safety_report_volume2_2021_v2.pdf

[12] National Highway Traffic Safety Administration (NHTSA). (2017). *Automated driving systems 2.0: A vision for safety*. U.S. Department of Transportation. https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf

[13] Department of Transport (UK). (2023). *Code of practice: Automated vehicle trialling*. https://www.gov.uk/government/publications/trialling-automated-vehicle-technologies-in-public/code-of-practice-automated-vehicle-trialling

[14] Transport Canada. (2021). *Guidelines for testing automated driving systems in Canada: Version 2.0*. https://tc.canada.ca/sites/default/files/2021-09/automated_driving_system_report_en.pdf

[15] National Highway Traffic Safety Administration (NHTSA). (2021, March). *Voluntary safety self-assessment*. U.S. Department of Transportation. https://www.nhtsa.gov/automated-driving-systems/voluntary-safety-self-assessment

[16] National Highway Traffic Safety Administration (NHTSA). (n.d.). *Standing general order on crash reporting for incidents involving ADS and level 2 ADAS*. U.S. Department of Transportation. https://www.nhtsa.gov/laws-regulations/standing-general-order-crash-reporting

[17] International Organization for Standardization (ISO). (2022). *Road vehicles—Safety of the intended functionality* (ISO Standard No. ISO 21448:2022). https://www.iso.org/standard/77490.html

[18] U.S. Department of Defense. (2012). *Department of Defense standard practice: System safety* (Standard No. MIL-STD-882E). https://quicksearch.dla.mil

[19] International Organization for Standardization (ISO). (2018). *Road vehicles—Functional safety* (ISO Standard No. ISO 26262-1:2018). https://www.iso.org/standard/68383.html

[20] UK Ministry of Defence. (2017). *Safety management requirements for defence systems* (Defence Standard 00-56 Part 1, Issue 7). Defence Equipment and Sport; UK Defence Standardization. https://s3-eu-west-1.amazonaws.com/s3.spanglefish.com/s/22631/documents/safety-specifications/def-stan-00-056-pt1-iss7-28feb17.pdf

[21] Wishart, J., Como, S., Elli, M., Russo, B. Weast, J., Altekar, N., James, E., & Chan, Y. (2020). Driving safety performance assessment metrics for ADS-equipped vehicles. *SAE International Journal of Advances and Current Practices in Mobility*, *2*(5), 2881–2899. https://doi.org/10.4271/2020-01-1206

[22] International Organization for Standardization (ISO). (2023). *Road vehicles—Test scenarios for automated driving systems* (ISO Standard No. ISO 34503:2023). https://www.iso.org/standard/78952.html

[23] The British Standards Institution. (2020). *Operational design domain (ODD) taxonomy for an automated driving system (ADS) – Specification* (BSI Standard No. PAS 1883:2020). https://www.bsigroup.com/globalassets/localfiles/en-gb/cav/pas1883.pdf

[24] Thorn, E., Kimmel, S., & Chaka, M. (2018). *A framework for automated driving system testable cases and scenarios* (Report No. DOT HS 812 623). National Highway Traffic Safety Administration (NHTSA). https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/13882-automateddrivingsystems_092618_v1a_tag.pdf

[25] VDA Working Group 13 of the Quality Management Center. (2023). *Automotive SPICE process assessment / reference model: Version 4.0.* German Association of the Automotive Industry Quality Management Center. https://vda-qmc.de/wp-content/uploads/2023/12/Automotive-SPICE-PAM-v40.pdf

[26] National Highway Traffic Safety Administration (NHTSA). (2023). *Federal motor vehicle safety standards and regulations*. U.S. Department of Transportation. https://www.nhtsa.gov/laws-regulations

[27] International Organization for Standardization (ISO). (2012). *Road traffic safety (RTS) management systems - Requirements with guidance for use* (ISO Standard No. ISO 39001:2012). https://www.iso.org/standard/44958.html

[28] The British Standards Institution. (2023). *System aspects for remote operation of vehicles* (BSI Standard No. BSI Flex 1886 v1.0:2023-08). https://www.bsigroup.com/en-GB/CAV/bsi-flex-1886/

[29] International Organization for Standardization (ISO). (2022). *Information security, cybersecurity and privacy protection—Information security management systems* (ISO Standard No. ISO 27001:2022). https://www.iso.org/standard/27001

[30] National Institute of Standards and Technology (NIST). (2024). *The NIST cybersecurity framework (CSF) 2.0*. [White Paper NIST.CSWP.29]. U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

[31] National Highway Traffic Safety Administration (NHTSA). (2022). *Cybersecurity best practices for the safety of modern vehicles*. U.S. Department of Transportation. https://www.nhtsa.gov/press-releases/nhtsa-updates-cybersecurity-best-practices-new-vehicles

3. Definitions

3.1 Core [AV] Safety Information

Collection of safety topics relevant across ADS applications, consolidated to provide a standardized set for communicating safety across stakeholders.

3.2 Hazard

Potential source of harm caused by the hazardous behavior at the vehicle level [17].

3.3 Lifecycle Process

All phases of the system's life, including design, research, development, test and evaluation, production, deployment (inventory), operations and support, and disposal [18].

3.4 Mitigation

Reduce to an acceptable level of risk [4].

3.5 Operational Design Domain (ODD) (SAE J3016)

Operating conditions under which a given driving automation system, or feature thereof, is specifically designed to function, including, but not limited to, environmental, geographical, and time-of-day restrictions, or the requisite presence or absence of certain traffic or roadway characteristics.

3.6 Residual Risk

Risk remaining after the deployment of safety measures [19].

3.7 Risk

The combination of the probability of occurrence of harm and the potential severity of that harm [19].

3.8 Safety

Absence of unreasonable risk [19].

3.9 Safety Case

A structured argument, supported by a body of evidence, that provides a compelling, comprehensible, and valid case that a system is safe for a given application in a given environment [20].

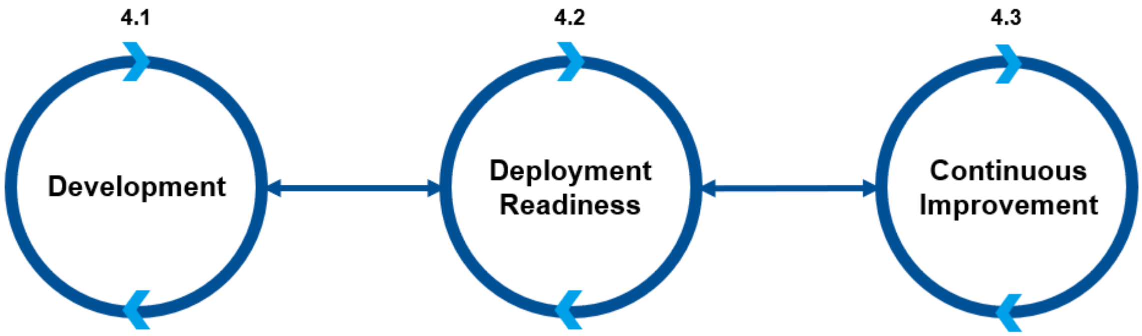
3.10 Safety Performance Indicator (SPI)

A metric used to quantify safety performance [4].

4. Safety-Relevant Lifecycle Processes

To provide context for the various information elements in this best practice, this section describes the safety-relevant lifecycle processes, visualized in Figure 1. Table 2 in Appendix B shows the relationship of AVSC best practices to safety-relevant lifecycle processes. The safety-relevant lifecycle illustrates that safety is continuous and connected throughout the stages of the lifecycle. ADS manufacturers, developers, and operators may choose to include relevant aspects of these processes, as appropriate, when sharing core safety information.

FIGURE 1 Safety-relevant lifecycle



4.1 Development

Safety-relevant development processes should encompass safety-by-design[2] practices as part of a manufacturer's, developer's, or operator's safety approach and should be grounded in rigorous engineering development practices. These processes should encompass all layers of product and operational service design. Development practices are based on a clear understanding and definition of the applicable context (for example, see 6.2 Operational Design Domain or 6.3 High-Level Aspects of System Design). For further guidance on the evaluation of behavioral competencies as part of development processes, documents such as *AVSC Best Practice for Evaluation of Behavioral Competencies for Automated Driving System Dedicated Vehicles (ADS-DVs)* (AVSC00008202111) may be referenced.

4.2 Deployment Readiness

At various points in the development lifecycle, an ADS manufacturer, developer, or operator will make discrete determinations regarding the readiness of specific configurations of its ADS-DV for operational deployment. These determinations will draw from a broad set of inputs collected during the development cycle of the current release. A wide array of methodologies may be used [9], providing distinct but complementary information. Broad data input and multiple methodologies help establish confidence in the ability to safely deploy. ADS manufacturers, developers, and operators **should utilize expert engineering judgment and analysis from experienced safety professionals during the information synthesis process.** Documents such as *AVSC Information Report for Adapting a Safety Management System (SMS) for Automated Driving System (ADS) SAE Level 4 and 5 Testing and Evaluation* (AVSC00007202107) may be referenced for further information.

---

[2] For an overview of safety-by-design principles, refer to https://sma.nasa.gov/sma-disciplines/system-safety.

Determinations of deployment readiness should be based on a range of informative factors. These may include:

- Institutional readiness in terms of areas such as: field operations, established internal safety reporting procedures, software version management procedures, etc.

- In-use monitoring capabilities.

- Ability to respond to events in real time to contain and mitigate residual and latent risk of rare events. For example, in situations which support of ADS operations may rely on remote assistance functions, the *AVSC Best Practice for ADS Remote Assistance Use Case* (AVSC-I-04-2023) may be referenced for further information.

4.3 Continuous Improvement

ADS manufacturers, developers, and operators should ensure that appropriate feedback loops exist across all layers of the safety lifecycle processes. Processes which are supported by the in-use monitoring capabilities allow developers to identify and act appropriately to address any safety issue that may arise post-deployment. Continuous monitoring (as described in *AVSC Best Practice for Continuous Monitoring and Improvement after Deployment* [AVSC00011202307]) and field safety reviews should be utilized to assess whether the ADS's performance continues to align with the targets on which the deployment readiness decisions were made.

5. Safety Metrics

ADS manufacturers, developers, and operators may choose to include safety metrics, as appropriate, when sharing core safety information.

5.1 Developing Safety Metrics

Organizations should measure safety performance status throughout the product lifecycle using safety metrics. Safety metrics provide measurable indicators specific to a safety topic. *AVSC Best Practice for Metrics and Methods for Assessing Safety Performance of Automated Driving Systems (ADS)* (AVSC00006202103) defines safety metrics as "a measurement used to evaluate and track safety performance." In a 2023 update to UL 4600 [4], the standard defined safety performance indicator (SPI) as "metric supported by evidence that uses a threshold comparison to condition a claim in the Safety Case," and notes that "safety metrics may be used to support key performance indicators (KPI) or safety performance indicators (SPI)."

Safety metrics communicated to stakeholders illustrate performance in a specific safety area. Safety metrics should be context-relevant and provide stakeholders with useful information. Safety metrics can measure portions of the intended application. For example, safety metrics can be used to measure the safety of a design (input and process) or performance (outputs) but can have different goals and uses.

Safety metrics should be clear, credible, appropriately contextualized, unambiguous, valid, and available through a practical, repeatable, explainable, and consistently implemented process. Safety metric limitations should be clearly noted.

5.2 Communicating Safety Metrics

Shared safety metrics information should be evaluated in the context and use case for which it is intended. The provider of the information has full discretion of what is shared based on mutually aligned parameters with the receiver.

Guidance on interpretation and notations against misinterpretation may be included. The provider may also provide additional information to support interpretations, such as definitions, context from which the data was gathered, etc. The provider may find it beneficial to use metrics whose definitions are established by standards, best practices, regulations, or are in common use. As an ADS progresses through the safety-relevant lifecycle (see Section 4 Safety-Relevant Lifecycle Processes), it is possible that the metrics, thresholds, and values reported for the metrics may change.

For further guidance and specific safety metrics, documents such as *Driving Safety Performance Assessment Metrics for ADS-Equipped Vehicles* [21], *AVSC Best Practice for Metrics and Methods for Assessing Safety Performance of Automated Driving Systems (ADS)* (AVSC00006202103), and UL 4600 [4] may be referenced.

6. Core Safety Information Elements

AVSC emphasizes the importance of fostering awareness on advancements in ADS technology, which in turn requires a carefully considered approach when sharing safety information. **Core safety information should, at minimum, include the topics specified in this guidance. Content may be tailored based on the specific use case and audience. Excluded or modified topics should feature an explanation of the extent of the changes.** This best practice does not recommend a specific order or underlying framing for these topics, but rather underscores the important role each topic can play in communicating the safety and reliability of ADS-DVs. Additional topics may be necessary or helpful to communicate safety between parties, depending on the ADS-DV use case and relationship of the relevant parties. The information contained should speak to the ADS-DV's ability to operate safely and effectively in diverse real-world scenarios and indicate that unreasonable safety risks are avoided or mitigated. Figure 2 lists topics that should be included as part of core safety information.

FIGURE 2 Topics to be included in core safety information

	Safety Information Element	Description	Relevant AVSC BPs/SAE and ISO Documents
6.1	Use-Case Description	First step in defining the scope of an ADS manufacturer, developer, or operator's safety approach.	AVSC00002202004, UL4600, ISO 21448, ISO 26262
6.2	Operational Design Domain (ODD)	ODD forms the foundation for the development of relevant tests that manufacturers and developers can apply consistently.	AVSC00002202004, AVSC00011202307, ISO 34503
6.3	Non-Proprietary Aspects of System Design	Includes System of Systems Design, Functional Design, Hardware, Software, Supporting System Design.	SAE J3208, AVSC00008202111, ISO 26262, ISO 21448
6.4	Vehicle Integration	Certification of base vehicle and assessment of impact following the introduction of ADS components.	ISO 26262
6.5	Validation and Verification Testing	Activities to analyze how ADS capabilities meet appropriate safety, reliability, and compliance requirements.	ISO 21448, ISO 26262
6.6	Safety-Relevant Human Machine Interactions	Includes HMI for vehicle occupants, remote operators and other road users for safety-related functions.	AVSC00003202006, SAE J3114
6.7	Safety Management System	Includes Safety Policy and Objectives (SPOs), Safety Promotion (SP), Safety Risk Management (SRM), and Safety Assurance (SA).	ISO 26262, AVSC00007202107
6.8	Fleet Operations and Maintenance	Regular and scheduled maintenance checks, software updates, and thorough diagnostics.	AVSC00005202012, AVSC00004202009, ISO 39001, UL4600
6.9	Remote Operations including Remote Assistance	Support and monitoring activities to aid vehicle operations.	AVSC-I-04-2023, SAE J3016
6.10	Incident Response and Post-Incident Analysis	Vehicle platform and ADS response during and after an incident, as well as process implemented.	AVSC00005202012, AVSC00004202009, AVSC00007202107, AVSC00011202307
6.11	Post-Collision Vehicle Response, Data Collection and Analysis	Vehicle platform and ADS response during and after a vehicle collision, loss, or hazardous event.	AVSC00004202009, AVSC00005202012, SAE J1698, SAE J2728-1, SAE J3197
6.12	First Responder Safety Interactions	Collaboration between ADS-DVs and first responders during emergency situations.	AVSC00005202012, AVSC00003202006
6.13	Safety-Relevant Cybersecurity	Should include rigorous testing, regular software updates, intrusion detection, encryption protocols.	ISO 27001, ISO/SAE 21434, SAE J3061
6.14	Misuse Mitigation	Addressing and mitigating potential harm from reasonably foreseeable public and in-vehicle passenger misuse.	ISO 21448

Core Safety Information

For each topic, this document provides the following information:

- **Rationale:** How the topic is relevant in terms of safety and why it is important to include when discussing ADS safety.
- **Example:** A specific applied example that is illustrative but not prescriptive.
- **Description of information that can be included in this example:** Suggested information that could be relevant when addressing the topic in question in the context of the illustrative example.
- **References and industry examples:** Annotated references that may provide additional information.

Although this best practice proposes 14 distinct topics, there may be considerable intersection and interconnection between them.

6.1 Use-Case Description

Rationale for Inclusion of This Topic as Part of Core Safety Information

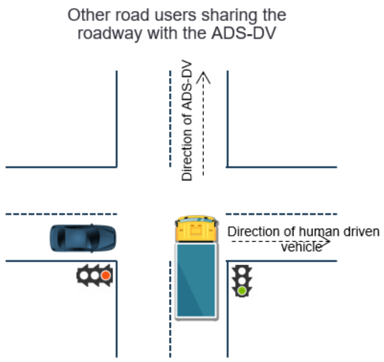
ADS-DVs have a wide and varied range of possible use cases. **Use-case descriptions should be clear, appropriately defined, and describe how an ADS-DV will be utilized in public-facing operations.** This can serve as the first step in defining the scope of an ADS manufacturer's, developer's, or operator's safety approach. Though safety approaches for different services may share commonalities, each sharing of core safety information should be tailored for its respective use case, deployment, and relationship with the recipient of such information. The use-case description of a last-mile delivery vehicle intended to operate within hubs may share many similarities with an in-city passenger transport, yet will differ distinctly in areas such as interaction with the public.

The use-case description explains what is being deployed and operated, including the service provided by the ADS-DV. The use-case description may include high-level limitations associated with ADS-DV operations. Design constraints relevant to the ADS-DV deployment and the recipient may be included in the ODD section, if applicable. For example, a low-speed shuttle may be designed to operate only within a limited geographical area, and on roads within a set range of speed.

Example

This use case includes automated commercial cargo delivery on public roads and includes the following types of interactions with other road users: pickup/drop-off of materials, loading/unloading interactions, and other road users sharing the roadway with the ADS-DV. The expected fleet size is ten vehicles.

FIGURE 3 Sample use case



Description of Information That Can Be Included in This Example

Information included in the use-case description will be specific to the provider and the deployment context. The following are example topics providers may include as part of core safety information:

- **High-level description of the ADS-DV's intended use case:** For example, long-haul freight, local goods delivery, and in-terminal port shuttling.
- **Types of interactions with consumers and other road users:** For example, operating in a freight terminal with human loading/unloading, consumers retrieving goods from within a vehicle compartment, handling interactions with other road users, and on-road inspections.
- **Types of interactions with infrastructure:** For example, weigh stations, border crossings, and fixed inspection sites.
- **Expected fleet size for deployment:** For example, order of magnitude of ADS-DVs in 10s, 100s, 1000s, etc.
- **As appropriate, a list of the likely hazards associated with the use case**. For example, interacting with other road users traveling above posted speed limits.

References and Industry Examples

The following best practices and standards can be utilized to prepare content for this topic:

- AVSC00002202004: Provides guidance and insights into the ODD and use cases, helping stakeholders understand the critical factors that shape the boundaries of where and how the ADS-DV functions. This reference may complement shared core safety information by enhancing its comprehensiveness and aligning it with industry best practices.
- UL 4600 [4]: This standard provides a mature list of areas to consider when building a use case.
- ISO 26262 [19] and ISO 21448 [17]: Standards that address developing production from conceptual stages and considerations that should be evaluated.

6.2 Operational Design Domain (ODD)

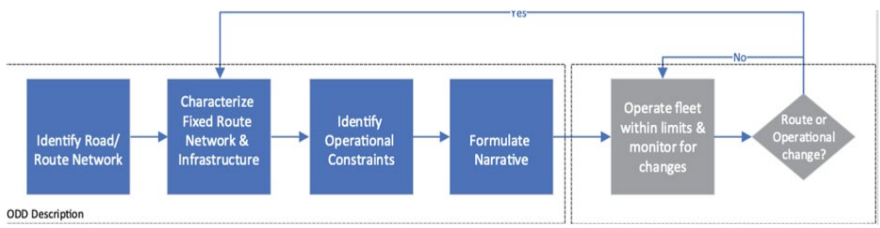
Rationale for Inclusion of This Topic as Part of Core Safety Information

A description of the operational design domain (ODD) should demonstrate a comprehensive understanding of the operational conditions for which the ADS-DV was designed and careful consideration of related safety aspects. An ADS-DV's ODD is defined based on factors such as intended use case, business model, and technological capabilities. An ADS-DV ODD can also be influenced by system complexity and associated risk management. The ODD underpins much of the material included in core safety information by forming the foundation for manufacturer and developer tests.

Example

An ADS shuttle service operating within a retirement community. The ODD for this service includes specific routes within the community, which are free from public road access. The ODD would include detailed parameters, such as roadway speed limits, expected weather conditions, and complexity of the surrounding environment.

FIGURE 4 AVSC ODD description



Description of Information That Can Be Included in This Example

Information included in the operational design domain will be specific to the provider and the deployment context. The following are example topics providers may include as part of core safety information:

- **ODD attributes, specifying covered roadway types:** For example, parking lots within the retirement community.
- **Description of expected road users:** For example, wheelchair users and scooter riders.
- **Description of off-nominal road situations:** For example, constructions, flooded roads, etc., that would restrict service operations.
- **Information on roadway operational speed range within the ODD:** For example, maximum speeds on the covered roadways.
- **Weather conditions that are included or excluded from the ODD:** For example, moderate to heavy snow, moderate to heavy road ice, expected precipitation, including hail or all forms of dust storms.
- **Operational time constraints within the ODD:** For example, operational start and end times and days per week. Time constraints that contribute to the safety and predictability of the service, aligning with the retirement community's schedules and requirements.
- **Geographic maps**: Identifying the roadways where the AV can operate.

References and Industry Examples

The following best practices can be utilized to prepare content for this topic:

- AVSC00002202004: Provides guidance and insights into the operational design domain, helping stakeholders understand the critical factors that shape the boundaries of where and how the ADS-DV functions. This reference may complement shared core safety information by enhancing its comprehensiveness and aligning it with industry best practices.
- AVSC00011202307: Provides guidance into the continued assessment of ODD related assumptions post deployment.
- ISO 34503 [22].
- BSI PAS 1883 [23].
- NHTSA's *A Framework for Automated Driving System Testable Cases and Scenarios* [24].

6.3 Nonproprietary Aspects of System Design

Rationale for Inclusion of This Topic as Part of Core Safety Information

The inclusion of the nonproprietary design processes as part of core safety information may be helpful in the context of safe development and deployment of ADS-DVs. Design elements can form an important link in the safety chain, connecting the ADS-DV to the ODD. This topic provides insights into how certain aspects of the design process for the ADS, its supporting subsystems, integration with the vehicle platform, and operational considerations have been structured to meet safety objectives.

By referencing this content, the safety information will highlight the systematic approach taken in designing the ADS-DV. **It should outline the interaction between key elements within the system of systems and clarify certain aspects of the functional design.** The nonproprietary aspects of the hardware and software design process will highlight the integration of functional requirements and standards.

TABLE 1 Description of information that could be included under design

Design Elements	Information	References and Industry Examples
System of Systems Design	Developers of autonomous vehicles, such as for ride hail or freight delivery services, should discuss how a system of systems-focused design strategy was used in the creation and maintenance of their service.	SAE J3206: This standard offers a harmonized set of safety principles for ADS development and deployment. UL 4600 [4].
Functional Design	Within a development process, conceptualization of system design naturally evolves into the specification of anticipated functionality for the system. Understanding and scoping of such functionality depends on the concept envisioned for ADS operations within the specified ODD. Functional design considerations span multiple topics, including ADS behavioral competencies, an understanding of operational scenarios, and investigation of ADS failures and associated effects, including design of fallback strategies and mitigations.	ISO 26262 [19], ISO 21448 [17].
Hardware Design Methodology and Compliance	Developers should show how functional requirements have been used as guidance in accordance with standards or industry best practices. The material included on this topic should complement existing and appropriate legislation or regulatory requirements (e.g., Federal Motor Vehicle Safety Standards). *Key hardware systems to be considered when providing this information*: sensors, computers and networks, telemetry module, vehicle actuators, data loggers, and event data recorder (EDR).	AVSC00008202111: Offers insights into safety thresholds that can be applied to certain hardware like sensors, computers and networks, telemetry modules, and vehicle actuators. ISO 26262 [19].
Software Design Methodology	When conveying core safety information with regards to software design, guidance can be taken from published standards. *Key software systems that may be considered:* embedded software, platform and health monitor, perception, localization, prediction, planning, and controls.	ISO 26262 [19], ISO 21448 [17], ASPICE [25].
Supporting System Design	Developers should describe the process used to develop and implement the supporting systems that augment AV functionality but exist externally to the AV. This may include tool systems used by operators supporting the AV, as well as automated backend systems. *Key tool systems to be considered when providing this information:* fleet management portal, remote assistance system, and customer service tool.	AVSC-I-04-2023: Offers a set of guidelines to help identify and develop functionalities for RA in SAE level 4 and level 5 ADS-DVs, as applicable. UL 4600 [4].

6.4 Vehicle Integration

Rationale for Inclusion of This Topic as Part of Core Safety Information

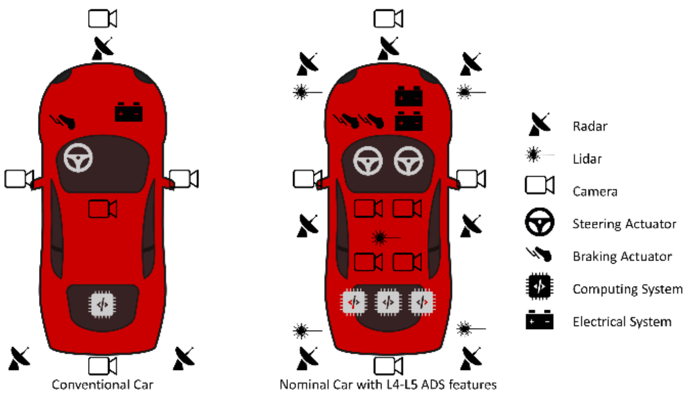
Vehicle platforms comply with a range of regional laws and regulatory safety requirements. This element of core safety information should describe care taken to ensure the ADS integrated into existing vehicle platforms (upfitted) did not compromise existing safety certification. Purpose-built platforms (ground-up design) should describe safety compliance, as appropriate.

The information may include safety validation of the ADS integration into a base vehicle. Content may include the make and model of the base vehicle, system redundancy, efforts to ensure hardware modifications did not reduce the crashworthiness of the base vehicle, and the review process employed when new hardware versions are introduced.

Example

A developer is in the process of upfitting an existing legally compliant vehicle with an ADS. This vehicle, originally designed for manual operation, is being modified to facilitate the developer's efforts to create self-driving capabilities for ride-hailing missions.

FIGURE 5 Vehicle integration example



Description of Information That Can Be Included in This Example

Information included in the vehicle integration will be specific to the provider and the deployment context. The following are example topics providers may include as part of core safety information:

- **Information about the existing vehicle platform:** For example, make, model, trim level, and model year. Key safety features, such as automatic emergency braking (AEB), should also be included.
- **High-level description of the relevant changes made to the vehicle and their impact, if any, to the base vehicle safety features:** For example, installation of sensors, control systems, and additional hardware. Note that changes include the addition, removal, or substitution of components.
- **Acknowledgement that the vehicle is compliant with applicable laws and regulations:** For example, the base vehicle manufacturer has certified that the vehicle complies with Federal Motor Vehicle Safety Standards (FMVSS) and the ADS developer has maintained compliance or been granted an exemption or exception from the appropriate regulatory agency.
- **Description of the integration testing conditions for new hardware or software:** For example, in simulation, on test courses, on public roads, etc.

References and Industry Examples

The following examples can be utilized to prepare content for this topic:

- FMVSS [26]: Set of U.S. federal regulations that establish performance and safety requirements for motor vehicles and certain vehicle equipment. While FMVSS is not specific to the integration of ADS, it does play a significant role in shaping the broader automotive industry's safety standards.
- ISO 26262 [19].

6.5 Verification and Validation (V&V) Testing

Rationale for Inclusion of This Topic as Part of Core Safety Information

Verification serves as a checkpoint within the ADS-DV development lifecycle where all systems must meet safety requirements or be appropriately accounted for to ensure operations are executed according to their specification and as appropriate for the designed use case. Validation addresses how well the ADS-DV meets the desired goals in the actual operational environment and can provide feedback to the verification processes. Feedback from validation activities can provide confidence or improvement in both the original set of verification requirements and the process used to generate them. Overall, V&V activities encompass testing methods such as simulation, closed-course testing, on-road testing, and real-world driving.

By referencing this content, this element of core safety information highlights the provider's commitment to verifying and validating the system's operation—including changes and updates to software, hardware, and vehicle—offboard functions and operations. It may also provide transparency on the use of testing methodologies, ensuring that the ADS-DV is tested appropriately to mitigate or monitor potential safety risks. **Core safety information should include processes for testing and analysis, ensuring completion of testing and analysis, and addressing test failures.**

Example

An ADS-DV is undergoing a software update to improve its existing handling of complex traffic scenarios. To evaluate the safety of this update, the ADS developer conducts simulation testing. Various scenarios are simulated to assess how the system responds with respect to predefined safety requirements. The process demonstrates that the ADS-DV consistently meets the requirements for the relevant scenarios and that the change does not cause significant regressions in other areas of performance.

Description of Information That Can Be Included in This Example

Information included in verification and validation testing will be specific to the provider and the deployment context. The following are example topics providers may include as part of core safety information:

- **Describe how the V&V requirement generation process and testing approach cover known unsafe and unknown unsafe scenarios, as per ISO 21448 [17].**
- **Outline safety assurance processes, explaining the measures in place to assess the effectiveness and safety of all components of the system:** For example, the testing methodology and validation processes used to evaluate potential software updates (including simulation, closed-course, and on-road testing), and their appropriateness.

References and Industry Examples

The following examples can be utilized to prepare content for this topic:

- Waymo [9]: Showcases a layered approach to safety readiness determinations utilizing various V&V methodologies.
- *Cruise Safety Report* [8]: Provides a real-world example of a range of V&V processes to help ensure the safety of ADS-DVs.
- ISO 21448 [17]: Provides guidance on V&V testing for exploring AV safe performance in known and unknown scenarios.
- ISO 26262 [19].

6.6 Safety-Relevant Human-Machine Interactions (HMI)

Rationale for Inclusion of This Topic as Part of Core Safety Information

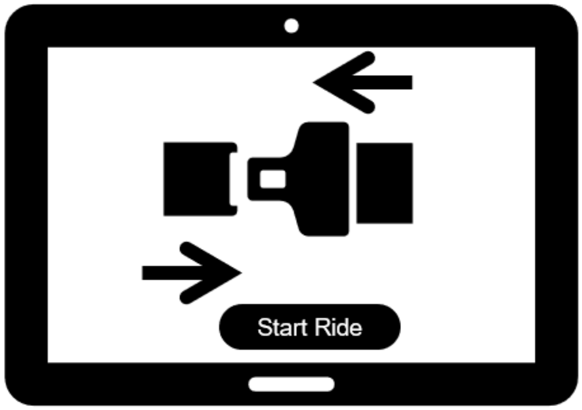
The human machine interface (HMI) facilitates the interactions, communications, and information exchange primarily between the ADS-DV and its users(s), but also between the ADS-DV, remote operators, and other road users. A subset of HMI functions involves safety-related human-machine interactions. For example, HMI designs can be used to convey the intent of the vehicle (maneuvers/behaviors) to other road users. HMI designs should be tested extensively, including with users, as part of development to ensure that design requirements are satisfied, the technology is robust, not error-prone, and enables easy and accessible user interaction.

Incorporating this information as part of core safety information can improve safety outcomes and demonstrates the provider's commitment to transparent and effective communication mechanisms for all actors who interface with the ADS-DV.

Example

A passenger has entered an ADS ridesharing vehicle. A tablet interface inside of the vehicle requests the passenger to close the door and fasten their seatbelt to start the ride. As the passenger closes the door and fastens the seatbelt, the tablet interface acknowledges completion of the tasks. Once all tasks are complete, the tablet allows the passenger to start the ride. This enforces that passenger safety practices are followed prior to starting the ride.

FIGURE 6 Example HMI



Description of Information That Can Be Included in This Example

Information included in safety-relevant human-machine interactions will be specific to the provider and the deployment context. The following are example topics providers may include as part of core safety information:

- **Describe the safety-relevant HMI communication design and functionality of the HMI elements, inside and outside the vehicle.**
- **Explain how the HMI inside the vehicle facilitates effective and accessible communication to passengers.**
- **Describe the functionality of the HMI communication system.**
- **Describe checks and validations conducted during safety assessments, highlighting the safety assurance practices.**

References and Industry Examples

The following best practices and examples can be utilized to prepare content for this topic:

- AVSC00003202006: This best practice is relevant to the HMI topic as it outlines guidelines for HMI interactions in emergency scenarios initiated by passengers, ensuring that HMI design supports safe and effective communication during such critical situations.
- SAE J3114: SAE J3114 is applicable to the HMI topic by offering standards for HMI design, serving as a reference for creating effective and safe HMI elements to facilitate seamless communication in ADS-DVs.

6.7 Safety Management System (SMS)

Rationale for Inclusion of This Topic as Part of Core Safety Information

ADS manufacturers, developers, and operators should demonstrate established, formal, comprehensive, and effective methodology to manage and avoid unreasonable safety risks to establish confidence with stakeholders. Companies may develop their own techniques for managing safety. It is important that a company present its approach in an understandable format.

An ADS company's safety management system (SMS) should address all relevant functions of development, manufacture, testing, monitoring, and operations. SMS frameworks should be deliberate about functions included to cover the full scope of the product's lifecycle. Figure 7 outlines the four components of an SMS as identified in AVSC00007202107: safety policy and objectives (SPOs), safety promotion (SP), safety risk management (SRM), and safety assurance (SA).

FIGURE 7 Safety management system components

Description of Information That Can Be Included in This Example

Information included in the safety management system will be specific to the provider and the deployment context. The following are example topics providers may include as part of core safety information:

- **Describe the company's SPOs, outlining its commitment to safety at the policy level.**
- **Description of how the SMS addresses all relevant functions within the lifecycle:** Including, development, manufacturing, testing, and operations.
- **Describe the company's established methodology for managing safety risks. Identify examples of detected safety incidents and how they were addressed through the SMS.**
- **Information on how the SMS incorporates feedback loops across all areas, as well as the effectiveness of the SMS itself.**

References and Industry Examples

The following best practices and examples can be utilized to prepare content for this topic:

- AVSC00007202107: This best practice outlines four key components of an SMS for ADS companies. It provides a structured framework that providers can reference when compiling information related to the safety management process as part of core safety information.
- ISO 26262 [19].

6.8 Fleet Operations and Maintenance

Rationale for Inclusion of This Topic as Part of Core Safety Information

Compliance with applicable local, state, and federal regulations and requirements relating to operations and maintenance is essential and highlights proactive measures necessary to maintain safe operation of a fleet of ADS-DVs.

Fleet operations: Encompasses monitoring the vehicle fleet, service area, and timely logistical responses to evolving operating conditions and unforeseen situations.

Maintenance: Vehicle maintenance, ADS maintenance, software update processes, and diagnostics serve as preventive measures to preemptively address potential issues that can affect safety.

Inclusion of fleet operations and maintenance processes as part of core safety information highlights the commitment to sustained safety throughout the lifespan of the autonomous fleet. Content may also include actions taken in response to specific scenarios or events that ADS-DVs may encounter while in operation.

Example

An unforeseen thunderstorm severely reduces visibility, creating challenging driving conditions for an ADS-DV. The fleet operations center (FOC) is alerted to this environmental change through real-time weather data. The FOC activates the reduced visibility protocols.

The vehicles which traversed the most severe thunderstorm area are suspected to have sustained hail damage. FOC alerts the maintenance team, takes the affected vehicles out of service, and routes them to maintenance for inspection.

This timely and coordinated response ensures the continued safety of the delivery fleet in the face of changing environmental conditions.

Description of Information That Can Be Included in This Example

Information included in fleet operations and maintenance will be specific to the provider and the deployment context. The following are example topics providers may include as part of core safety information:

- **Description of processes to track damage, required maintenance inspections, maintenance completion, and return to service.**
- **Description of decision processes:** Such as how fleet operations may evaluate available data when choosing to dispatch, recall, or ground an ADS-DV.
- **Processes for tracking scheduled maintenance activities, demonstrating compliance with maintenance schedules:** Such as sensor calibrations, software updates, and hardware checks.

References and Industry Examples

The following best practices and examples can be utilized to prepare content for this topic:

- AVSC-I-01-2024: This best practice provides insights into how first responders should interact with ADS-DVs in various scenarios.
- AVSC00004202009: This best practice offers guidance on data collection for event analysis, aligning with the incident response and data collection aspects of fleet operations. It can be referenced to ensure data collection procedures adhere to best practices, and collected data can be used to analyze incidents or anomalies.
- ISO 39001 [27].
- UL 4600 [4].

6.9 Remote Operations (RO) Including Remote Assistance (RA)

Rationale for Inclusion of This Topic as Part of Core Safety Information

Remote operations (RO), which includes remote monitoring, remote assistance (RA), and customer support functions, supports the safe, efficient, and reliable operations of an ADS. For example, they can provide aid to the ADS in unforeseen situations, or coordinate care for passengers and freight throughout a mission. RO functions play an important role in complex or ambiguous situations where human judgement may provide an additional measure of assurance.

RA specifically provides for real-time communication between the ADS and human operators, allowing for additional guidance in challenging driving or service scenarios.

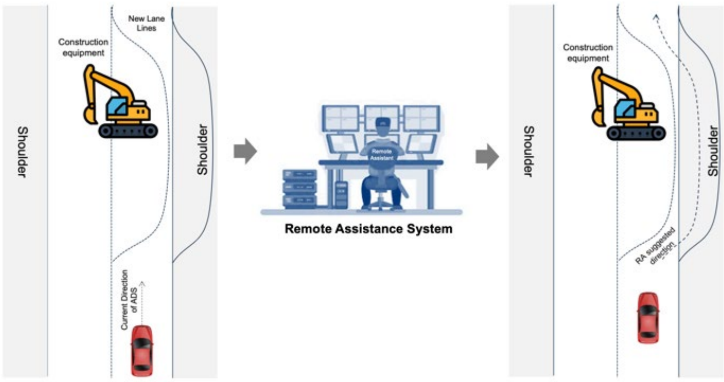
The implementation of RO, including RA, also involves procedures for the selection, training, and oversight of RO staff.

Example

The ADS is navigating on the road when it detects an unexpected lane blockage caused by construction equipment. Temporary lane lines have been painted on the road, extending onto the shoulder. Upon detecting this unexpected scene, the ADS recognizes that further information is needed to navigate through the construction zone safely (e.g., confirmation that it is allowed to drive and maintain speed on a shoulder), and it temporarily stops to request for assistance.

The remote assistant assesses the situation through real time sensor feeds and confirms that it is legal to drive onto the shoulder to pass the obstacle in this specific scenario. The ADS then safely proceeds to the shoulder after receiving confirmation from the remote assistant.

FIGURE 8 Remote assistance function in action



Description of Information That Can Be Included in This Example

Information included in remote operations and remote assistance will be specific to the provider and the deployment context. The following are example topics providers may include as part of core safety information:

- **Broad summary of RA system activation processes:** Such as highlighting the trigger conditions, criteria for initiating remote assistance, and response times.
- **Description of types of data shared with the remote assistant:** Such as camera feeds, vehicle speed, and telematics data. Also describe how this data exchange promotes situational awareness.
- **Description of training processes for remote operators.**

References and Industry Examples

The following best practices and examples can be utilized to prepare content for this topic:

- AVSC-I-04-2023: Offers a set of guidelines to help in identifying and developing functionalities for RA in SAE level 4 and level 5 ADS-DVs, as applicable. The scope of the document includes defining the event types that could trigger RA, such as maneuvering through complex driving scenarios or encountering unexpected obstacles.
- SAE J3016: Offers standardized terminology and concepts that are essential for clear communication regarding remote operator and remote assistance systems.
- BSI Flex 1886 [28]: Provides guidelines for the safe operation and management of autonomous systems, including the interaction between remote operators and automated vehicles.

6.10 Incident Response and Post-Incident Analysis[3]

Rationale for Inclusion of This Topic as Part of Core Safety Information

Incident response is part of a comprehensive safety management system for ADS-DVs. Timely incident response can affect the safety of all involved actors and other road users. Post-incident analysis contributes to continuous improvement by informing incident response strategies in potential areas, such as detection, alerts, recovery, monitoring, and incident on-site interaction. There are a range of incident types, which can include system failures, minimal risk conditions (MRCs), collisions, cybersecurity events, misuse events, and more.

Example

While an ADS cargo delivery vehicle is in transit to a pickup, it is impacted by flying road debris and sustains damage that degrades its perception and vehicle controllability. Based on available data, the vehicle makes use of an empty shoulder to perform a minimal risk maneuver (MRM) by decelerating and moving over to the empty shoulder. It then utilizes indicators to signal that it is in a stationary state.

The status of the cargo is escalated from the ADS to the operations center. The operations center uses available information to evaluate the incident severity and follows the established incident response plan. A maintenance crew is dispatched for further investigation and the appropriate parties, including the customer, are notified of the event. After investigation, it is determined that the vehicle should be driven back to the depot for repairs. Data from the incident is captured for later analysis, contributing to system improvement.

Description of Information That Can Be Included in This Example

Information included in incident response will be specific to the provider and the deployment context. The following are example topics providers may include as part of core safety information:

- **Explanation of incident response processes:** Such as methods for evaluation and severity determination, procedures to facilitate timely and appropriate responses, etc.
- **Describe processes for how information will be shared with third parties as appropriate:** Such as first responders or regulators, etc.
- **Describe processes for testing incident response plans:** Such as simulations, dry runs, tabletop exercises, etc. Explain how lessons learned from past events have been incorporated and have resulted in refinements and improvements to the incident response plan and its effectiveness.
- **Describe procedures for post-incident investigations, in-depth root cause analysis, potential corrective measures, prevention strategies, and information sharing.**

References and Industry Examples

The following best practices can be utilized to prepare content for this topic:

- AVSC-I-01-2024: This best practice provides insights into establishing protocols for first responder interactions with ADS-DVs during incidents which aligns with the importance of data collection and incident response in ensuring safety and providing insights for continuous improvement.
- AVSC00004202009: This best practice emphasizes the significance of collecting data for event analysis, highlighting the role of data collection in post-incident investigations, root cause analysis, and the refinement of ADS functionality to enhance safety and performance.
- AVSC00007202107: This best practice emphasizes organizational safety processes which include incident response.
- AVSC00011202307: This best practice provides an approach to continuous monitoring and potential improvement of safety performance.

[3] There are a wide range of incident types, including vehicle collisions, some interactions with first responders, weather-related incidents, cybersecurity, and more. Subsequent sections have been devoted to various incident types. This is not meant to be an exhaustive coverage of all possible incident types.

6.11 Post-Collision Vehicle Response, Data Collection, and Analysis

Rationale for Inclusion of This Topic as Part of Core Safety Information

Post-collision vehicle response relates to the ADS's ability to minimize harm and mitigate residual risk. Thorough data collection and analysis of the causes of incidents and how an ADS-DV responds during and after a collision are important for mitigating immediate outcomes and developing strategies for mitigating risk of future instances. Presenting evidence of a well-designed and executed vehicle response and established data collection and analysis processes can support trust between stakeholders.

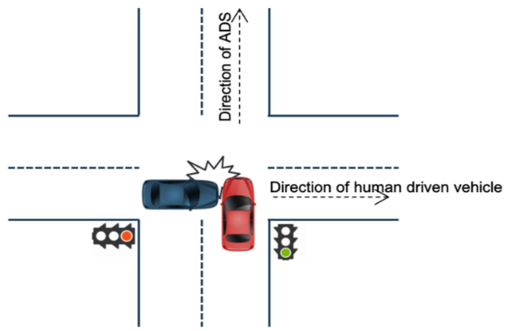
Data collected from the ADS provides insights into the real-world operating conditions and challenges faced by ADS-DVs. Post-incident analysis—driven by collected data—enables the detection of potential anomalies and irregularities, which can inform safety measures. Incorporating this as part of core safety information demonstrates the provider's proactive approach and their dedication to safety and continuous improvement in autonomous systems.

Example

An ADS-DV is transporting a passenger in a busy urban area. At an intersection, a human-driven vehicle runs a red light and collides with the ADS-DV.

The ADS immediately performs a fallback, maneuvering to achieve a minimal risk condition (MRC), and notifies the control center to contact the passenger. The control center contacts the appropriate first responders, continues to monitor the situation, and stays in contact with the passengers until their arrival.

FIGURE 9 Vehicle collision response



Description of Information That Can Be Included in This Example

Information included in post-collision vehicle response, data collection, and analysis will be specific to the provider and the deployment context. The following are example topics providers may include as part of core safety information:

- **Description of the process for communicating the incident internally and externally:** Such as to the ride-hailing/freight ADS operator's control center, first responders, and passengers.
- **Explanation of the processes and steps taken to support the passenger or other actors involved after the collision:** Such as arrangements for the passenger's continued journey.
- **Description of processes for collecting and managing subject collision-related data.**

References and Industry Examples

The following best practices and standards can be utilized to prepare content for this topic:

- AVSC00004202009: Provides guidelines and recommendations for collecting and managing data from ADS-DVs, especially in the context of safety incidents like collisions.
- AVSC-I-01-2024: Provides insights into establishing protocols for first responder interactions with ADS-DVs during incidents.
- SAE J1698 and SAE J2728-1: Standards to guide data collection and reporting follow industry-accepted practices (EDR), thereby enhancing the reliability and consistency of incident analysis.
- SAE J3197: Standardized approach to data collection (ADS data logger) and analysis, facilitating a thorough examination of the incident's causes and safety system performance.

6.12 First Responder Safety Interactions

Rationale for Inclusion of This Topic as Part of Core Safety Information

First responder safety interactions encompass various aspects, including communication and coordination between ADS-DVs, ADS operators, and first responders during emergency situations. ADS manufacturers, developers, and operators demonstrate their commitment to public safety and their readiness to collaborate with emergency services by including this topic as part of core safety information.

Well-defined protocols and procedures for interactions between ADS-DVs and first responders ensure that both parties can respond efficiently and effectively in emergency scenarios, reducing the likelihood and severity of harm. Clear communication channels and coordinated processes may help first responders effectively address incidents, ensure passenger safety, and improve overall emergency preparedness in areas where ADS-DVs operate. This topic can also help in building trust with stakeholders by showcasing the commitment to safety and proactive collaboration with public safety agencies.

Example

While an ADS ride hailing vehicle is in transit, law enforcement signals the vehicle to pull over as it approaches an active scene. The vehicle complies with the request to pull over. When the vehicle is pulled over, the vehicle provides indication, in accordance with its first responder interaction plan, that it is safe to approach. The first responder approaches the vehicle and follows the interaction plan to initiate communication with a remote operator.

After the interaction, the first responder indicates to the remote operator that the vehicle should avoid a certain area to leave the scene. When the ADS-DV is released and determines that the driving environment is clear, it follows the guidance of the remote operator and leaves the scene.

Description of Information That Can Be Included in This Example

Information included in first responder safety interactions will be specific to the provider and the deployment context. The following are example topics providers may include as part of core safety information:

- **Description of procedures for interactions with first responders in various emergency scenarios:** Such as medical emergencies, collisions, or system failures.
- **Description of established communication channels and protocols for connecting the ADS-DV with local emergency services or first responders:** Such as dedicated frequencies, data exchange formats, and alert triggers.
- **Procedures for the creation, distribution, and maintenance of training materials for first responders.**

References and Industry Examples

The following best practices can be utilized to prepare content for this topic:

- AVSC-I-01-2024: Provides guidelines and best practices for facilitating interactions between first responders and ADS-DVs.
- AVSC00003202006: Provides guidance on handling emergency situations initiated by passengers during an ADS trip. It offers insights into the procedures for addressing passenger emergencies, which can complement the protocols outlined as part of core safety information for public safety interactions.

6.13 Safety-Relevant Cybersecurity

Rationale for Inclusion of This Topic as Part of Core Safety Information

ADS companies should demonstrate to stakeholders an established, formal, comprehensive, and effective methodology to manage safety-relevant cybersecurity, communicating a reasonable level of residual safety risk has been maintained. Cybersecurity is an integral part of AV safety. Its role is to ensure the output of all safety approaches remain intact during the lifecycle of the product or service.

Companies may develop their own techniques for assessing and managing cybersecurity risks, in addition to cybersecurity standards and best practices which serve as a foundation for a cybersecurity management system (CSMS). **An ADS company's CSMS should address all relevant value-chain functions related to the creation and operation of an AV product or service.** Figure 10 shows the functions encompassed by *The NIST Cybersecurity Framework (CSF) 2.0*, which highlights and organizes appropriate cybersecurity outcomes at a high level. Frameworks, standards, and best practices, such as the NIST CSF, give guidance towards the foundational elements of a CSMS.

Example

An ADS-DV's cybersecurity system detects an attempted intrusion into its network while driving on the road. The intrusion is instantly identified, blocked, and reported to the fleet's control center. Simultaneously, the vehicle switches to a backup communication network to ensure passenger safety and uninterrupted service. The incident is analyzed, and appropriate updates are made. Countermeasures are then deployed to enhance the cybersecurity system.

FIGURE 10 NIST CSF framework encompassed functions [30]

Description of Information That Can Be Included in This Example

Information included in safety relevant cybersecurity will be specific to the provider and the deployment context. The following are example topics providers may include as part of core safety information:

- **Describe the company's security goals, outlining its commitment to cybersecurity at the policy level.**
- **Highlight how the CSMS addresses the full ADS lifecycle:** Such as in-use monitoring.
- **Describe the foundational elements of the established methodology for managing cybersecurity risk through the CSMS.**
- **Describe how the CSMS addresses all relevant functions within the value chain:** Such as development, manufacturing, testing, and operations.

References and Industry Examples

The following standards and examples can be utilized to prepare content for this topic:

- ISO 27001 [29]: Can be used to establish a robust framework for safeguarding data and ensuring the security of the vehicle's software and communication systems.
- ISO/SAE21434: Outlines the requirements for assessing and mitigating cybersecurity risks in automotive systems. It provides a structured approach to identify and manage cybersecurity threats in the automotive domain.
- *The NIST Cybersecurity Framework (CSF) 2.0* [30]: Best practices for cybersecurity framework, risk management, and incident response strategies.
- SAE J3061: Provides a set of high-level guiding principles for cybersecurity relating to cyber-physical vehicle systems.
- NHTSA's *Cybersecurity Best Practices for the Safety of Modern Vehicles* [31].

6.14 Misuse Mitigation

Rationale for Inclusion of This Topic as Part of Core Safety Information

Addressing potential public misuse (by both ADS-DV users and other road users) not only safeguards the well-being of the public, but also reinforces the cooperative nature of ADS-DV operations and enhances public trust in ADS technology.

Comprehensive education (e.g., training videos, educational information, promotional campaigns, etc.) before/during/after operations and effective safety features can help avoid potential harm arising from misuse by in-vehicle users and other road users alike. Monitoring systems of both the in-vehicle cabin and the vehicle surroundings help prevent misuse, ensuring that ADS-DVs are operated in a safe and responsible manner.

Including these aspects as part of core safety information demonstrates a commitment to promoting responsible use and positive public interactions in the deployment of ADS technology.

Example

In an urban setting, an ADS ride-hailing vehicle has just picked up a passenger and is about to start its journey. Before starting the ride, the passenger is shown an educational video of appropriate behavior, including not touching the vehicle controls. The video is accompanied by a warning that touching the vehicle controls may terminate the ride. The passenger watches the video, fastens their seatbelt, and starts the ride.

During the ride, the passenger attempts to sound the horn out of curiosity. The ADS determines that the signal can be ignored and does not change its driving behavior. The ADS reports to customer support that a tampering event has been detected. A customer support agent immediately contacts the passenger through the in-vehicle communication system and informs the passenger that vehicle-control tampering has been identified, which violates the terms of service agreement as such behavior is not permissible. A terms-of-service violation is flagged on the rider’s profile. Should this reoccur, the rider may face additional consequences.

Description of Information That Can Be Included in This Example

Information included in misuse mitigation will be specific to the provider and the deployment context. The following are example topics providers may include as part of core safety information:

- **List safety guidelines for passengers:** Such as actions to take in various scenarios. These guidelines can include information about seatbelts, emergency procedures, and responsible in-vehicle behavior.
- **Describe educational programs or materials provided to passengers:** Such as safety tutorials or onboarding processes, aimed at raising awareness about proper in-vehicle conduct.
- **Explain features that enable passengers to seek assistance during the ride:** Such as the availability of remote operators, or a digital in-vehicle help-center guide.
- **Describe the AV's general response in situations where misuse has been detected to facilitate safety of the riders and the public.**

References and Industry Examples

The following standards can be utilized to prepare content for this topic:

- ISO 21448 [17]: Standard providing guidance relating to safety of the intended functionality and reasonably foreseeable misuse by persons.

7. Summary

This best practice provides guidance for ADS manufacturers, developers, and operators to share safety-relevant information in a consistent, clear, and explainable manner. It outlines topics helpful to communicating ADS safety information and provides illustrative examples, where appropriate. This can facilitate communicating use-case-relevant ADS safety information between relevant parties preparing for and deploying ADS-DV systems.

8. About Automated Vehicle Safety Consortium™

The objective of the Automated Vehicle Safety Consortium™ (AVSC) is to provide a safety framework around which automated vehicle technology can responsibly evolve in advance of the broad use of commercialized vehicles. The consortium will leverage the expertise of its current and future members and engage government and industry groups to establish safety principles and best practices. These technology-neutral principles are key considerations for deploying SAE level 4 and level 5 automated vehicles on public roads.

AVSC Vision:
Public acceptance of SAE level 4 and level 5 automated driving systems as a safe and beneficial component of transportation through industry consensus.

AVSC Mission:
The mission of the Automated Vehicle Safety Consortium™ (AVSC) is to quickly establish safety principles, common terminology, and best safety practices, leading to standards to engender public confidence in the safe operation of SAE level 4 and level 5 light-duty passenger and cargo on-road vehicles ahead of their widespread deployment.

The AVSC will:

- Develop and prioritize a roadmap of precompetitive topics.
- Establish working groups to address each of the topics.
- Engage the expertise of external stakeholders.
- Share output/information with the global community.
- Initially focus on fleet service applications.

9. Contact Information

To learn more about the Automated Vehicle Safety Consortium™, please visit https://avsc.sae-itc.org.

Contact: AVSCinfo@sae-itc.org.

10. Acknowledgements

The Automated Vehicle Safety Consortium™ would like to acknowledge the contributions of the member organizations during the development of this document:

Aurora, GM/Cruise, Daimler/Torc Robotics, Motional, Uber, Volkswagen, Waymo, and Zoox, including collaboration from Edge Case Research.

11. Abbreviations

ADS	Automated driving system
ADS-DV	Automated driving system-dedicated vehicle
AEB	Automatic emergency braking
AV	Automated vehicle
AVSC	Automated Vehicle Safety Consortium™
CSF	Cybersecurity framework
CSMS	Cybersecurity management system
EDR	Event data recorder
FMVSS	Federal Motor Vehicle Safety Standard
FOC	Fleet operations center
HMI	Human machine interface
ISO	International Organization for Standardization
MRC	Minimal risk condition
MRM	Minimal risk maneuver
ODD	Operational design domain
RA	Remote assistance
RO	Remote operations
SA	Safety assurance
SAE ITC	SAE Industry Technologies Consortia®
SMS	Safety management system
SP	Safety promotion
SPI	Safety performance indicator
SPO	Safety policy objectives
SRM	Safety risk management
VRU	Vulnerable road user
V&V	Verification and validation
VSSA	Voluntary Safety Self-Assessment

APPENDIX A. Best Practice Quick Look

- Automated driving systems (ADSs) manufacturers, developers, and operators may choose to share aspects of the safety-relevant lifecycle process as appropriate (Section 4). This may include: safety-by-design practices, deployment readiness (Section 4.1), deployment readiness criteria and decision processes (Section 4.2), feedback loops across the safety lifecycle process, and continuous monitoring strategies. (Section 4.3)

- ADS manufacturers, developers, and operators may choose to include safety metrics as part of core safety information as appropriate (Section 5). Safety metrics should be used to measure safety performance improvement throughout the product lifecycle and should be context-relevant, clear, and unambiguous (Section 5.1). If included, safety metrics information should be evaluated within the intended context and use case. (Section 5.2)

- Core safety information should, at minimum, include the specified topics; any exclusions or changes should be explained. (Section 6)

  - **Use-case descriptions** should be clear, appropriately defined, and describe how an automated driving system-dedicated vehicle (ADS-DV) will be utilized in public-facing operations. (Section 6.1)

  - **Operational design domain (ODD) information** should demonstrate a comprehensive understanding of the ADS-DV's operational conditions and careful consideration of related safety aspects. (Section 6.2)

  - **High-level aspects of system design** information should outline the interaction between key elements within the system of systems, clarify aspects of the functional design, and highlight a systematic design approach. (Section 6.3)

  - **Information on vehicle integration** should highlight compliance with regional legislative and regulatory safety requirements for both upfitted and ground-up designs. (Section 6.4)

  - **Verification and validation (V&V) testing** information should include a description of the process for testing and analysis, ensuring completion of testing and analysis and addressing test failures. (Section 6.5)

  - **Safety-relevant human-machine interactions (HMI)** information should showcase facilitation of information exchange among vehicle occupants, remote operators, and other road users for safety-related functions. (Section 6.6)

  - Information shared about an ADS company's **safety management system (SMS)** should address relevant functions of development, manufacture, testing, monitoring, and operations. It should communicate the provider's approach to governance and decision-making and its effectiveness to manage and avoid unreasonable safety risks. (Section 6.7)

  - **Fleet operations and maintenance** information should highlight the proactive measures for maintaining safe and consistent operation of an ADS-DV fleet. This may include preventive measures to preemptively address potential issues and the ability to accommodate evolving operating conditions and unforeseen situations in a timely manner. (Section 6.8)

  - **Remote operations (RO), including remote assistance (RA),** support safe, efficient, and reliable ADS operations and should be included as part of core safety information. This may include remote monitoring, supporting ADS response to unforeseen challenges, supporting coordination of care of passengers and freight, real-time communications between ADS and human operators, as well as the selection, training, and oversight of RO staff. (Section 6.9)

  - **Incident response and post-incident analysis** information should showcase processes for timely response to incidents and the post-incident ability to identify and address issues appropriately. (Section 6.10)

- Core safety information should include evidence of a well-designed and executed **post-collision vehicle response and data collection and analysis processes**. (Section 6.11)

- **First responder safety interaction** information should highlight protocols and procedures that allow for collaboration with emergency services and demonstrate a commitment to public safety. (Section 6.12)

- Core safety information should communicate **safety-relevant cybersecurity** information and that an acceptable level of residual safety risk has been maintained. This can be documented in a cybersecurity management system (CSMS) which should address all relevant value-chain functions related to the creation and operation of an AV product or service. (Section 6.13)

- **Misuse mitigation** information should demonstrate established misuse prevention and mitigation policies and procedures. These may include safety features and education. (Section 6.14)

APPENDIX B. AVSC Best Practices Mapped to Safety-Relevant Lifecycle Processes

Table 2 shows how published AVSC best practices can be mapped to safety-relevant lifecycle processes as described in Section 4.

TABLE 2 AVSC best practices mapped to safety-relevant lifecycle processes

Development	
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*
AVSC00007202107	*AVSC Information Report for Adapting a Safety Management System (SMS) for Automated Driving System (ADS) SAE Level 4 and 5 Testing and Evaluation*
Deployment Readiness	
AVSC00006202103	*AVSC Best Practice for Metrics and Methods for Assessing Safety Performance of Automated Driving Systems (ADS)*
AVSC00008202111	*AVSC Best Practice for Evaluation of Behavioral Competencies for Automated Driving System Dedicated Vehicles (ADS-DVs)*
AVSC-I-04-2023	*AVSC Best Practice for ADS Remote Assistance Use Case*
Continuous Improvement	
AVSC-I-01-2024	*AVSC Best Practice for First Responder Interactions with Fleet-Managed Automated Driving System-Dedicated Vehicles (ADS-DVs)*
AVSC00009202208	*AVSC Best Practice for Interactions Between ADS-DVs and Vulnerable Road Users (VRUs)*
AVSC00010202304	*AVSC Information Report for Change Risk Management*
AVSC00011202307	*AVSC Best Practice for Continuous Monitoring and Improvement after Deployment*
AVSC00012202308	*AVSC Best Practice for Developing ADS Safety Performance Thresholds Based on Human Driving Behavior*