Automated Vehicle Safety Consortium™
A Program of SAE ITC

Automated Vehicle Safety Consortium™ Information Report

AVSC00010202304

Issued 2023-04

AVSC Information Report for Change Risk Management

Citation: Automated Vehicle Safety Consortium. 2023. AVSC Information Report for Change Risk Management. SAE Industry Technologies Consortia.

Rationale

The operation of any SAE level 4 or 5 automated vehicle on private or public roads inherently involves the assessment of safety risks to property or persons. Additionally, changes introduced after an automated driving system-dedicated vehicle (ADS-DV) has been deployed can introduce new risks or alter the assumptions for existing risks that arise from changes in the ADS-DV's design and operations. Developers may benefit from knowledge regarding how safety risks resulting from changes can be systematically identified, evaluated, and managed at every stage of the ADS's lifecycle. Though there are a variety of existing standards that cover risk identification, evaluation, and management for conventional road vehicles, they do not explicitly cover the risk management process for either planned changes or unplanned changes in ADS-DV design and/or operations.

This document outlines potential risk management strategies developers can consider when addressing risks that may occur due to planned and unplanned ADS changes.

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 5 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 5 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.

SAE Industry Technologies Consortia™ provides that: "This AVSC information report is published by the SAE ITC to advance the stage of technical and engineering sciences. The use of this information report is entirely voluntary and its suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user."

Introduction

During the development of an ADS-DV, various standards are used to address safety risks in domains such as functional safety, safety of the intended functionality, cybersecurity, design safety, etc. These standards are useful tools and address safety risks during various aspects of the initial design, development, and testing of ADS-DVs. Following their deployment, ADS-DVs will likely experience both planned and unplanned changes based on previously identified and managed safety risks. These changes may lead to new safety risks to be assessed and managed. All changes have the potential to introduce risk or alter the assumptions associated with existing risks. A change risk management (CRM) process would address these eventualities.

CRM is a process for identifying, evaluating, and managing risks that arise from planned (e.g., added functions, cybersecurity preventive measures, ODD changes) or unplanned (e.g., identifying new on-road scenarios, cybersecurity countermeasures) changes in the ADS-DV's design and/or operations.

The CRM process differs from classical risk assessment processes[1] in that the focus is on managing changes and generally includes the following steps:

- Analyze the CRM triggers.
- Identify hazards that may be generated by the change(s).
- Analyze and identify new risks based on defined hazards related to the change.
- Evaluate and assess new risks for each hazardous event that can be identified out of defined hazards related to the change.
- Identify and evaluate potential safety measures for the newly outlined hazardous events and associated safety risks related to the change.
- Implementing and validating safety measures as appropriate.
- Continue iterating, as needed.

CRM is an iterative process. If a new change is identified or an assumption is refined, then the CRM would be performed again.

[1] AVSC0000720210 provides an example of a classic risk assessment process.

Table of Contents

1. Scope

This Automated Vehicle Safety Consortium™ (AVSC) information report provides a process for change risk management for fleet-operated ADS-DVs using level 4 or 5 automation. The document addresses risks resulting from planned and unplanned changes in an ADS-DV design and/or operation.

This process assumes initial risk assessment and management associated with design, development, testing, and operations have been conducted for the ADS-DV according to relevant standards. The document is not intended to be used for the initial risk management in functional safety, safety of the intended functionality (SOTIF), cybersecurity-related safety, design safety and other safety-related domains. This information report does not establish specific risk levels for developers and manufacturers or establish requirements for the specific risk management tools.

1.1 Purpose

This AVSC information report is based on the concept of risk-informed decision making. This means the processes and tools outlined below are intended to help developers and manufacturers make determinations about risks not captured in the initial risk assessment and decide if further design and/or operational safety measures could be applied. This information report addresses the risks that are implicit to working in a changing environment. A failure to recognize, assess, and adjust to new risks creates the possibility of new vulnerabilities.

Making risk management decisions such as safety and change management, safety analysis, and safety assurance are especially applicable when moving from concept to production intent for the ADS-DV. CRM does not replace best practices or other methods for managing safety anomalies or change management processes. It may instead be viewed as an additional resource that elaborates on how safety anomaly management and change management can be performed.

This information report is intended for use by developers, product/program managers, safety managers, and safety assurance teams, as well as states, municipalities, infrastructure owner-operators (IOOs), and the public, as applicable. These stakeholders can compare the information and processes identified in this report against their procedures or use them as a benchmark. This information report is not a substitute for the sound judgment, accountability, and ethical decision making of engineers, risk management professionals, and leaders. Industry standards and processes still apply, where applicable.

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 issue 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.

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

SAE J3016_202104	Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles
SAE J3187_202202	System Theoretic Process Analysis (STPA) Recommended Practices for Evaluations of Automotive Related Safety-Critical Systems

2.1.2 Other Documents

[1] ICAO 9859. (2018). Safety management manual, fourth edition. *International Civil Aviation Organization (ICAO)*. Available: https://www.skybrary.aero/bookshelf/books/5863.pdf.

[2] MIL-STD-882E. (2012). "Department of Defense standard practice: System safety." *U.S. Department of Defense (DoD)*. Available: https://www.dau.edu/cop/armyesoh/DAU%20Sponsored%20Documents/MIL-STD-882E.pdf.

[3] ISO 45001. (2022). "Occupational health and safety management systems—Requirements with guidance for use." *International Organization for Standardization (ISO)*. Available: https://www.iso.org/standard/63787.html.

[4] ISO 26262. (2018). "Road vehicles—Functional safety—Part 1: Vocabulary. *International Organization for Standardization (ISO)*. Available: https://www.iso.org/standard/68383.html.

[5] ISO 26262. (2018). "Road vehicles—Functional safety—Part 8: Supporting processes. *International Organization for Standardization (ISO)*. Available: https://www.iso.org/standard/68390.html.

[6] ISO 21448. (2022). "Road vehicles—Safety of the intended functionality." *International Organization for Standardization (ISO).* Available: https://www.iso.org/standard/77490.html.

[7] ISO/SAE 21434. (2021). "Road vehicles—Cybersecurity engineering." *International Organization for Standardization (ISO) and the Society for Automotive Engineers (SAE)*. Available: https://www.iso.org/standard/70918.html.

[8] IEC 61508. (2010). "Functional safety of electrical/electronic/programmable electronic safety-related systems—Parts 1 to 7." *International Electrotechnical Commission (IEC)*. Available: https://webstore.iec.ch/publication/22273.

[9] DOE O 210.2A. (2011). "DOE corporate operating experience program." *U.S. Department of Energy (DOE)*. Available: https://www.directives.doe.gov/directives-documents/200-series/0210.2-BOrder-a.

[10] ISO 55001. (2014). "Asset Management". *International Organization for Standardization (ISO).* Available: https://www.iso.org/standard/55089.html

3. Definitions

These definitions are provided for reader convenience and are not intended to supplant or replace established legal or "terms of art" definitions.

3.1 CRM Trigger

Any planned or unplanned changes in ADS-DV design and/or operation.

3.2 Frequency

The count of historical occurrences, which must be modified by the expected changes to the system design and control scheme effectiveness to determine likelihood or probability.

3.3 Harm

Physical injury or damage to the health of persons. [4]

3.4 Hazard

Potential source of harm caused by malfunctioning behavior of the item. [4]

3.5 Hazardous Events

Combination of a hazard and an operational situation. [4]

3.6 Likelihood

A function of probability and exposure to harm given known or reasonably foreseeable operational conditions.

3.7 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, and/or the requisite presence or absence of certain traffic or roadway characteristics.

3.8 Planned Change

An expected or known alteration in the ADS-DV's design and/or operations.

NOTE: Examples may include added functions, cybersecurity preventive measures, and ODD changes.

3.9 Residual Risk

Risk remaining after the deployment of safety measures. [4]

3.10 Risk

The combination of the probability of occurrence of harm and the potential severity of that harm. [4]

3.11 Safety Anomaly

Conditions that deviate from expectations and can lead to harm. [4]

3.12 Safety Measure

Any technical, operational, organizational, or administrative action that prevents or mitigates a hazardous event, thus constraining the risk or severity of a hazardous event. The acceptable level of risk or severity is typically defined by the organization that performs CRM.

3.13 Severity

Estimate of the extent of harm to one or more individuals that can occur in a potentially hazardous event. [4]

3.14 Subject-Matter Expert (SME)

An individual with qualifications and experience in a particular field or work process; an individual who by education, training, and/or experience is a recognized expert on a particular subject, topic, or system. [9]

3.15 Unplanned Change

An unexpected alteration in the ADS-DV's design and/or operations.

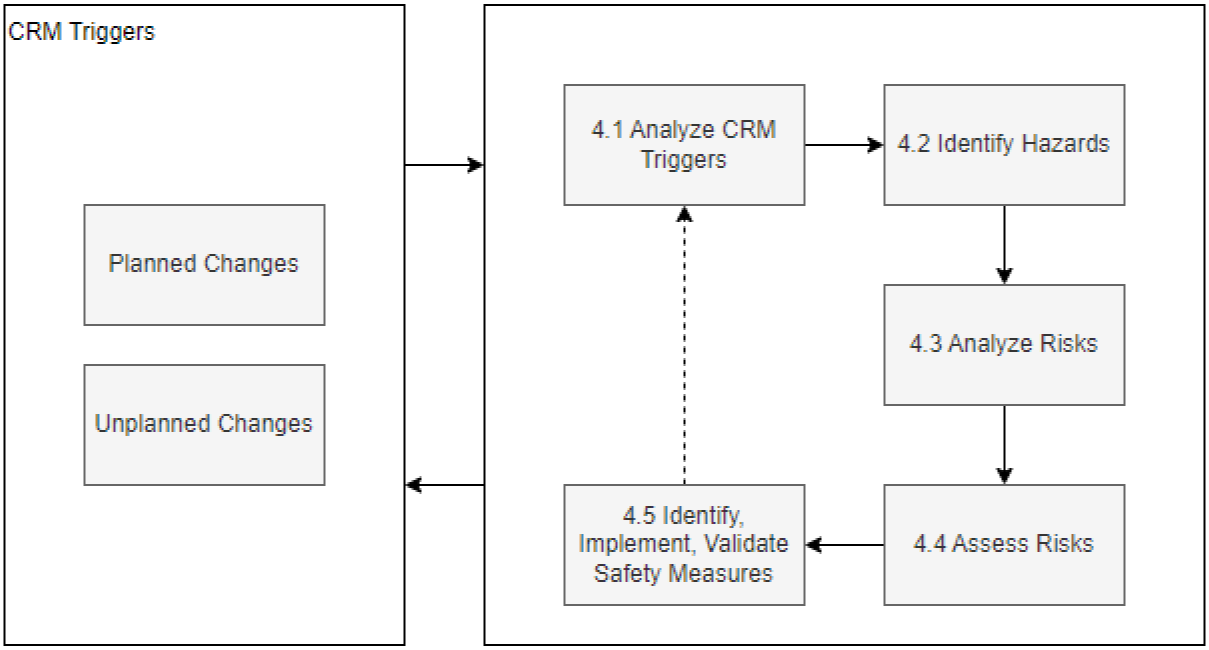
3.16 Vehicle Platform

Vehicle platform is usually an original equipment manufacturer (OEM) vehicle but can also be an experimental vehicle created for the testing of ADS-DV prototypes.

4. Introduction to Change Risk Management (CRM)

Change risk management (CRM) is a process where ADS-DV manufacturers, developers, and fleet operators may evaluate if and how ADS-DV changes affect previously identified and managed safety risks. They may also identify, assess, and manage new safety risks resulting from those changes. Figure 1 illustrates this process.

FIGURE 1 The iterative relationship between change risk management triggers and the CRM process flow



A similar flow is reflected in the AVSC SMS information report (AVSC00007202107), which breaks down the risk management process into five steps and is one way the CRM process flow can be implemented in an organization. [5]

4.1 CRM Triggers Identification and Impact Analysis

CRM triggers help ADS-DV manufacturers and developers identify changes that impact safety risks.

As shown in Figure 1, the CRM process is initiated by the input from the CRM triggers which can arrive from multiple sources. These sources can include analysis of field operations data, results of the safety assurance process, and intentional changes in the ADS-DV design/operations made by the organization. Regardless of the cause, an engineering team could begin with classification and analysis of the CRM triggers to determine the parts of the ADS-DV's design and operations which might be impacted. Some examples of changes and safety anomaly triggers are listed in Table 1.

TABLE 1 Types and examples of CRM triggers

Example List of Potential Triggers
• Functions and capabilities changed/added
• Component degradation
• Use cases/demo scenarios changed
• Technology change (introduction of new software or hardware)
• Vehicle platform change
• Supplier/source change
• Assurance/test procedure change
• Release procedure change
• ODD intentional change/expansion
• Fleet expansion (increase of the number of vehicles)
• Test route change
• Personnel change (e.g., safety drivers)
• Regulation/law changes introduced
• Safety/quality assurance failed
• Newly discovered operational scenarios
• Unexpected behavior of ADS-DV observed from field data
• Unexpected behavior of other road users observed from field data
• Safety process/culture issues discovered at audit/survey

ADS-DV manufacturers and developers may consider utilizing a list or map of the dependencies between CRM triggers and aspects of the ADS-DV project that may be impacted by the change.

These aspects include, but are not limited to:

- ADS software, hardware, architecture, requirements, design, behaviors, etc.

- ADS-DV ODD.

- Vehicle platform.

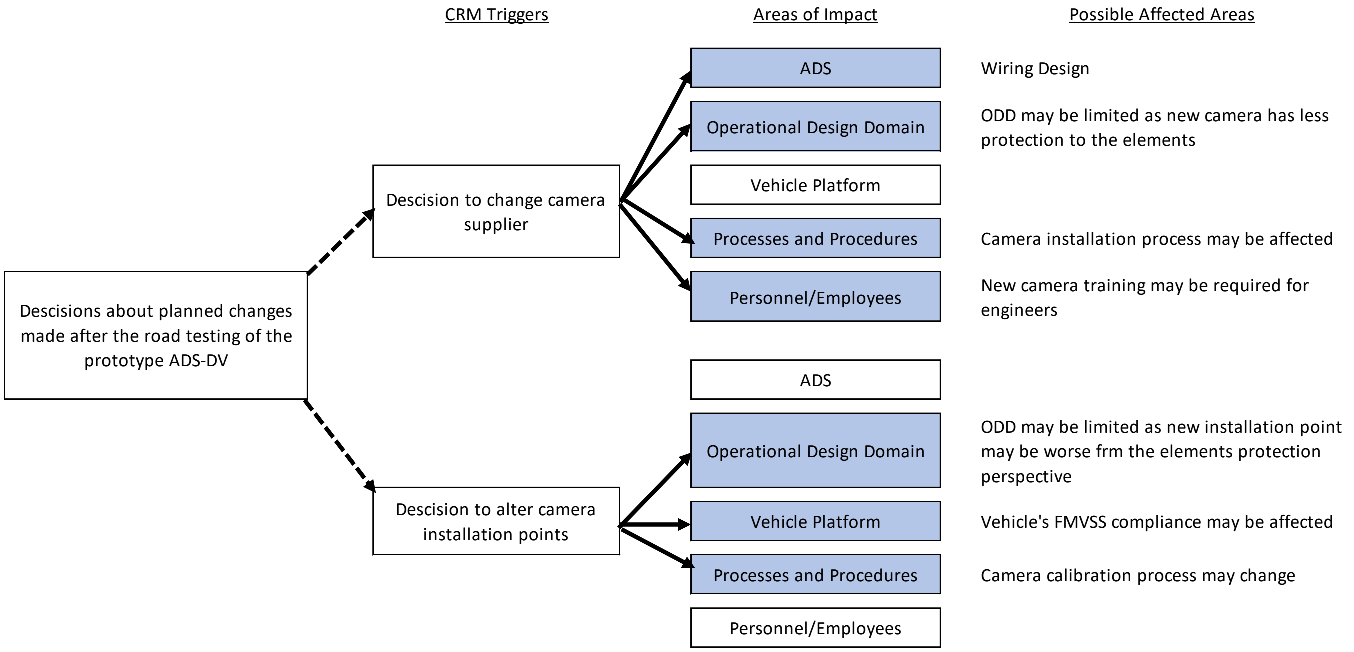
- Processes and procedures used to engineer, test, produce, operate, and service the ADS-DV or fleet.

- Personnel involved in the engineering, testing, production, operation, and service of the ADS-DV or fleet.

Various methods of facilitation and analysis can be used for the CRM triggers and impact analysis. Examples of these methods include model-based system engineering, bowtie, event sequence diagram, and subject-matter expert (SME) brainstorming.

Figure 2 is an illustrative example of how SME brainstorming may be applied to conduct an impact analysis, ensuring coverage of all mentioned aspects. Blue boxes indicate project aspects that could be affected by the CRM trigger.

FIGURE 2 Illustrative example of CRM triggers impact analysis


CRM Triggers
Areas of Impact
Possible Affected Areas
Descisions about planned changes made after the road testing of the prototype ADS-DV
Descision to change camera supplier
ADS
Operational Design Domain
Vehicle Platform
Processes and Procedures
Personnel/Employees
Wiring Design
ODD may be limited as new camera has less protection to the elements
Camera installation process may be affected
New camera training may be required for engineers
Descision to alter camera installation points
ADS
Operational Design Domain
Vehicle Platform
Processes and Procedures
Personnel/Employees
ODD may be limited as new installation point may be worse frm the elements protection perspective
Vehicle's FMVSS compliance may be affected
Camera calibration process may change

4.2 Hazard Identification

Results of the CRM triggers and impact analysis are then used to complete the hazard analysis.

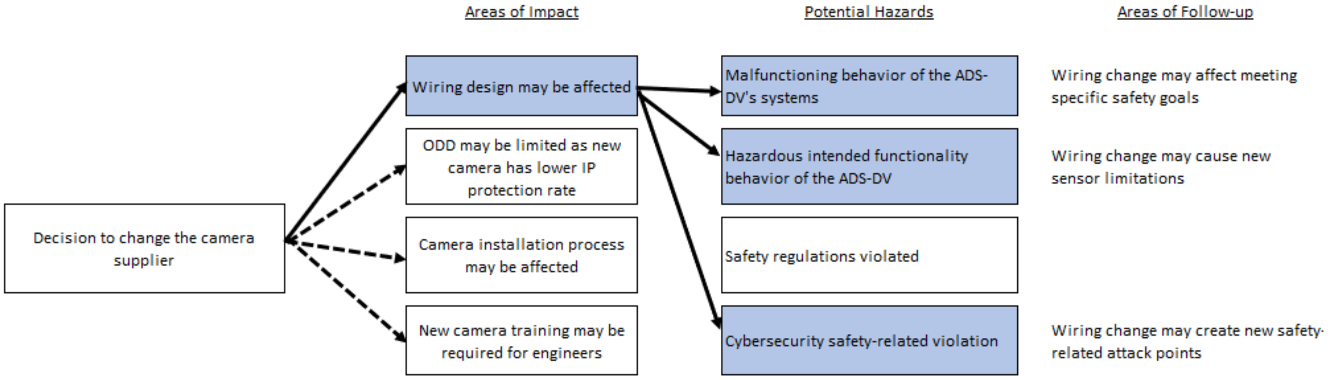
The same methods of analysis used for CRM triggers and impact analysis may be used for hazard identification. Hazards may be identified from past events or data (reactive), audits and evaluations (proactive), or from analyzing system processes and the environment to identify potential future hazards (predictive). Predictive hazard identification is typically important when implementing new systems or processes due to a lack of data.

The hazard identification method each company chooses is dependent on the ADS-DV project and organizational needs. ADS-DV developers and manufacturers typically identify hazards relevant to their system, use case, and ODD. Lists may vary. Some general examples include hazards associated with:

- Malfunctioning behavior of the ADS-DV system.
- Safety regulations violation.
- Cybersecurity-related safety violations.
- Unintended behavior of the ADS-DV not related to the previous items.

The hazards listed above can be expanded further by replacing the generalized hazards with a list of safety goals, cybersecurity goals, or specific standards or regulation violations. The level of granularity of the hazard analysis depends on the purpose and is left up to the responsible organization. It is given that identification of every possible hazard is not possible. Figure 3 shows potential hazards pertaining to a specific area of impact.

FIGURE 3 Example of impact analysis leading to hazards list


Areas of Impact
Potential Hazards
Areas of Follow-up
Decision to change the camera supplier
Wiring design may be affected
ODD may be limited as new camera has lower IP protection rate
Camera installation process may be affected
New camera training may be required for engineers
Malfunctioning behavior of the ADS-DV's systems
Hazardous intended functionality behavior of the ADS-DV
Safety regulations violated
Cybersecurity safety-related violation
Wiring change may affect meeting specific safety goals
Wiring change may cause new sensor limitations
Wiring change may create new safety-related attack points

4.3 Risk Analysis

Risk analysis follows hazard identification and is the analytical process of estimating the likelihood of a hazard occurrence and the severity of its effect. Risk analysis is not to be confused with SRA, covered in the next section. Risk analysis is the analytical process of determining severity and likelihood of a hazardous event. SRA, in contrast, is the process of combining severity and likelihood for a particular hazardous event to determine the level of risk. SRA involves a decision regarding the acceptability of operation in the presence of an identified hazard and the associated level of risk.

There are many ways to approach the analytical aspects of risk analysis. For some risks, the number of variables and the availability of suitable data and mathematical models may lead to credible results with quantitative methods. However, not all hazards lend themselves to credible analysis solely through numerical methods. Typically, these are supplemented qualitatively through critical and logical analysis of the known variables and system relationships.

4.4 Safety Risk Assessment (SRA)

The SRA is a process that includes a panel of SME stakeholders evaluating the safety risks associated with each identified safety concern or potential hazard. SRA can be achieved through various methods leveraging qualitative and quantitative approaches. An overview of examples follows in 4.4.1 and 4.4.2. AVSC00007202107 provides additional SRA information

ADS-DV manufacturers and developers typically have traceability as referenced in UL4600 and IATF 16949 of risk-related decisions, including an escalation path. The escalation path for risks evaluated in the SRA may vary depending on each organization's process.

The SRA end products may include a risk registry with a running list of hazards and a list of key safety measures which the organization has put in place to mitigate those hazards. If used, the risk registry/registries could be shared across the ADS-DV organization whenever new hazards are identified or safety measures are updated.

4.4.1 Qualitative SRA Methods

Utilizing a qualitative SRA is an expedient approach to assess risk scores for identified hazards. It can be further used as a foundation to build the quantitative approach. ADS-DV manufacturers and developers may choose to utilize a qualitative SRA method to assess change-related safety risks when first integrating CRM. This approach heavily relies on subject-matter expertise and experience to assess the level of risk associated with a hazard. It does not depend on availability of quantitative inputs, such as large data sets, to produce actionable SRA outputs.

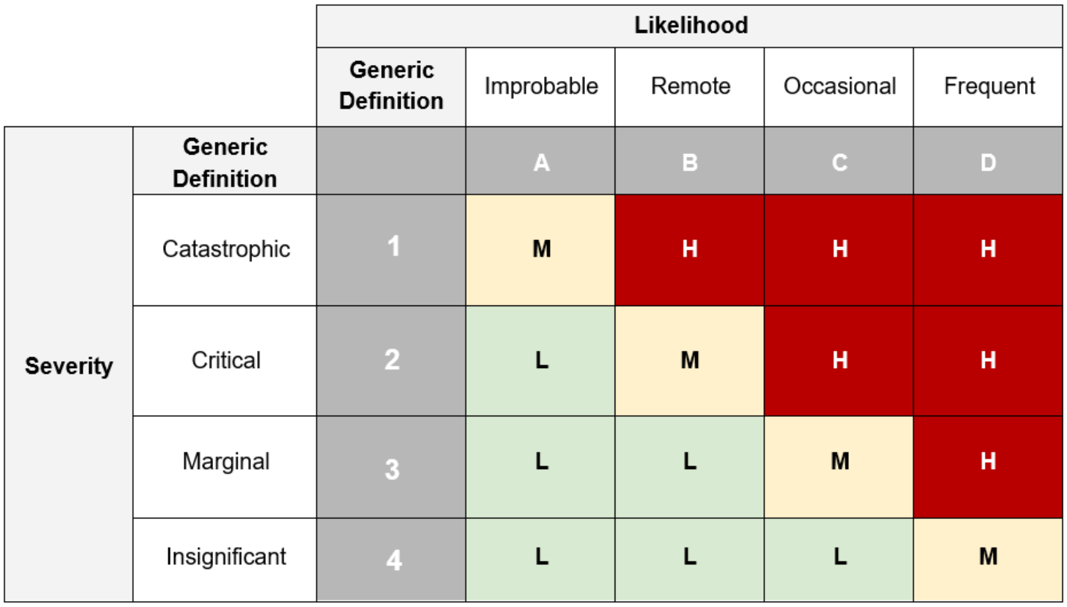
The risk matrix is an example of a tool ADS-DV developers may use to subjectively guide SRA using the definitions of severity and likelihood provided in this document (see Figure 4). It maps severity and likelihood to risk levels to assign a risk score. Although standard risk matrices exist in certain contexts [2, 5, 8], organizations may create their own or tailor an existing risk matrix to support risk-informed decision making effectively, where the decision risk matrix acts as a support tool to inform the level of residual risk.

It is the goal of Figure 4 to make explicit the established risk in relation to the severity and likelihood rankings; specifically, to make use of the matrix by assessing the level of risk.

This indicates the level of management required to accept a given level of risk as established by the risk acceptance criteria, and the formal process of risk acceptance.

NOTE: Definitions from [4] for "severity" and "likelihood" are utilized in Figure 4. The illustration itself is modified and may not match the risk matrices in the standard. Conformance to [4] is not implied.

FIGURE 4 Example of a conceptual risk matrix with illustrative categories



		Likelihood				
		Generic Definition	Improbable	Remote	Occasional	Frequent
Severity	Generic Definition		A	B	C	D
	Catastrophic	1	M	H	H	H
	Critical	2	L	M	H	H
	Marginal	3	L	L	M	H
	Insignificant	4	L	L	L	M

Table 2 illustrates an example of the SRA executed based on the risk matrix from Figure 4.

TABLE 2 SRA example

Hazard	Severity Estimation	Likelihood Estimation	Risk Score
New camera interface causes failure of camera to meet its objective	Catastrophic Viewing objects in pathway is critical for ADS-DV	Frequent High-speed driving occurs more than 10% of the ADS-DV's operational time	High
New attack point occurred due to interface change that allows attacker to manipulate perception	Catastrophic Potential perception manipulation may lead to the inability to detect certain road traffic participants and collide with them	Frequent The contact with road traffic participants is permanent, which supports frequent likelihood argument	High

In the example from Table 2, it does not make sense to perform the full risk assessment. An understanding of which safety or cybersecurity goal may be violated gives an appropriate understanding of the risk level that will be assigned to this change. Understanding the hazard source and associated risk score will drive design and implementation of safety measures to be added due to this change.

4.4.2 Quantitative SRA Methods

Organizations that develop ADS-DVs may consider quantitative methods in addition to conducting qualitative SRAs. The quantitative SRA approach requires the availability of adequate data to support analysis using mathematical and probabilistic methods. Robust safety risk scores then can be derived in a systematic and evidence-based manner.

Methods to quantify risk include the use of data sets. These may include performance data, predictive safety metrics, and outcome-related safety metrics—such as crashes and traffic citations[2]—in conjunction with a probabilistic model to determine the likelihood of a safety event. Quantitative SRA methods also require developing a model to determine the predicted severity of the hazardous event. For this purpose, closing velocity, potential point of impact, road actor behavior, and other parameters could be utilized to model collisions. Models can vary based on operational use cases and available objective data. Quantitative approaches from other safety critical industries such as military, energy, and aviation can be adapted to create the SRA models and methods.

4.5 Safety Measures

ADS-DV manufacturers and developers may identify, implement, and validate safety measures as appropriate to address identified safety risks.

The CRM process typically results in identification of potential safety measures to apply, if appropriate, and provides an additional reduction in risk after the changes are implemented. Safety measures help to maintain an overall acceptable level of risk if a need is identified for the hazards analyzed for that activity.

Safety measures are then prioritized by their impact to manage unreasonable safety risks. The following is an example of how safety measures can be grouped:

- Complete hazard elimination—This action entails either reverting the change or applying other actions to eliminate the hazard that triggers the hazardous event.

- Hazard substitution—This entails substituting the existing hazard with one that may still trigger the hazardous event or may trigger a different hazardous event but with a lower severity or likelihood.

- Technical safety measures—This measure is a technical solution that is focused on detecting, controlling, or mitigating the consequences of a hazardous event.

- Operational, organizational, and administrative safety measures—These measures and actions are focused on reducing the risk score by lowering the likelihood of a hazardous event (e.g., occurrence frequency or exposure). They can include instructions and/or warnings for the ADS-DV occupants and other road traffic participants.

- Personal protection equipment—This measure is a combination of a technical solution and enforcing the use of the technical solution. In this example this would be the least efficient safety measure.

[2] Refer to AVSC00006202103 for a description of some recommended metrics that may constitute datasets available to manufacturers.

The higher the safety measure is on this list, the higher the efficiency of said safety measure. For example, complete hazard elimination may include fleet grounding, which effectively eliminates the likelihood of a hazardous event occurring. Whereas hazard replacement which may include ODD limitation in terms of lowering operation speed may reduce the overall severity of a crash bringing the overall assessment of the risk to an acceptable level. Additionally, technical safety measures such as limiting vehicle dynamics can be more effective than administrative policies, which may rely on a safety driver to respond.

Deciding which safety measure group to implement may require an appropriate balance of utility and functionality. Often a combination of safety measures is used to maximize their total risk minimization effect. It is possible that a combination of lower order safety measures may help reduce the risk level more than a single higher order safety measure. The organization typically would perform a study or assessment every time safety measures are selected.

There are various approaches that may help an organization estimate the overall effectiveness of safety measure implementation. One approach is probabilistic metric for random hardware failures (PMHF). Others include goal structured analysis (GSA) or layers of protection analysis (LOPA) if technical measures are used. Alternatively, risk reassessment can be conducted on new safety measures that have been added. If the residual risk score is reduced to an acceptable level, the safety measures applied are considered sufficient. Table 3 shows examples of potential safety measures.

TABLE 3 Safety measures example

Hazard	Risk Score	Safety Measures	Notes
New camera interface causes failure of camera to meet its objective	H	Update ODD to address the hazard severity/likelihood	Replacing hazard as high speed changed with low speed
New attack point occurred due to interface change that allows attacker to manipulate perception	H	Add an additional layer of end-to-end (E2E) data consistency check between the camera and computer to detect any camera data alterations	Technical measure added

Every safety measure is validated before release and monitored afterwards. Failure to validate a safety measure’s effectiveness is treated as a CRM trigger and initiates another iteration of the CRM.

Design, implementation, and validation of the safety measures to address functional safety, safety of the intended function, and cybersecurity violation topics typically follow organization-specific processes and policies. Organizations may also collect their own lists of safety measures to be (re)used in other projects, such as re-introducing a fallback safety operator or driver following an ODD expansion or an increase in the size of the vehicle fleet

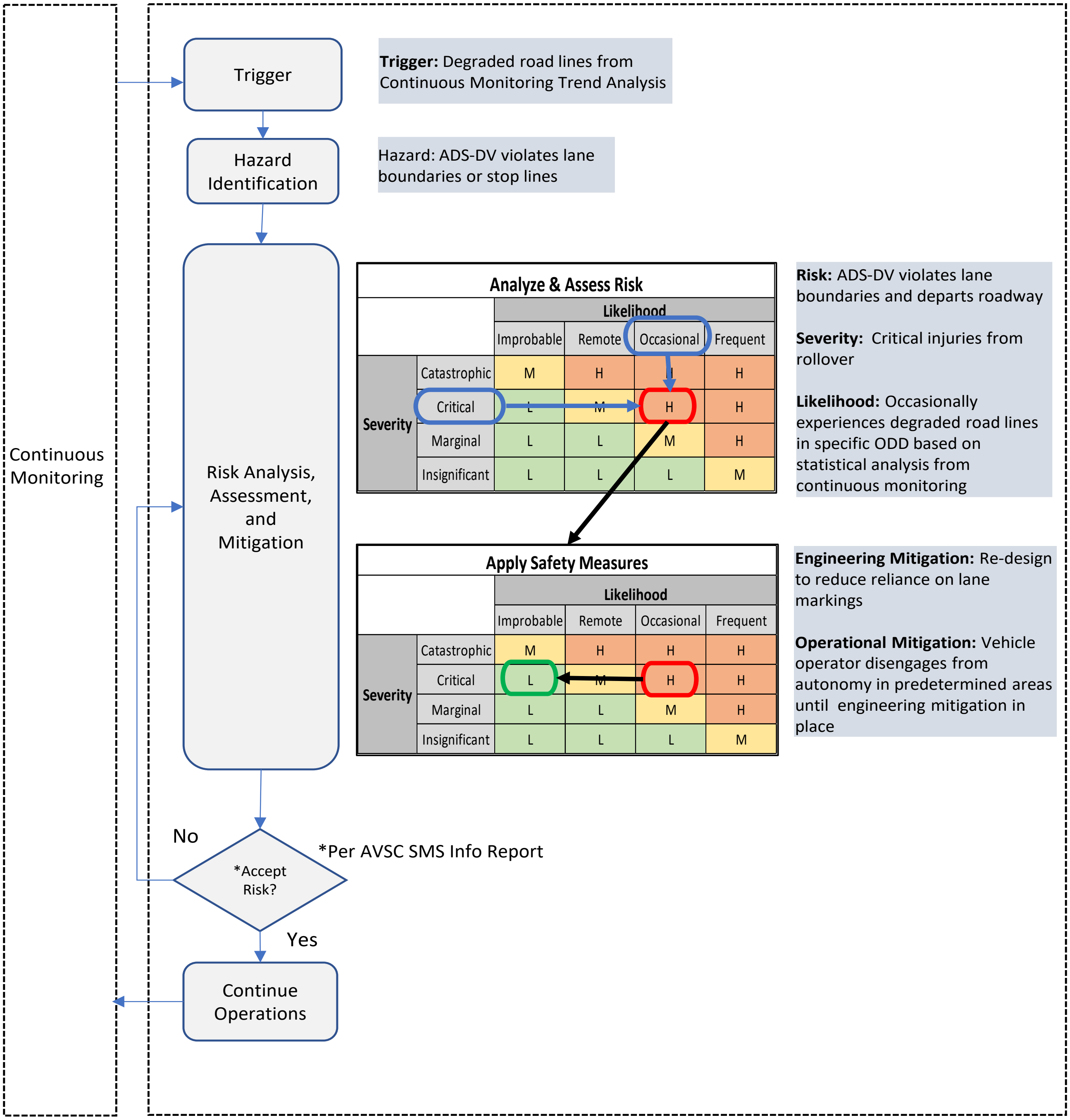
4.6 Confirmation of Residual Risk

The final function of CRM is to make sure the change has been properly addressed and the final residual risk has been accepted. An unacceptable residual risk score usually results in reverting the change and/or rejecting the safety measures applied. Additional product outputs may also be considered as noted in [5].

5. EXAMPLES

Figure 5 illustrates SRA for trend analysis during ADS-DV perception of degraded road signages (e.g., stop signs), fading lane markings, or deteriorating roadways. It further shows the reduction in severity after safety measures have been applied.

FIGURE 5 Change risk management process for trend analysis



Trigger: Degraded road lines from Continuous Monitoring Trend Analysis

Hazard: ADS-DV violates lane boundaries or stop lines

Analyze & Assess Risk

		Likelihood			
		Improbable	Remote	Occasional	Frequent
Severity	Catastrophic	M	H	H	H
	Critical	L	M	H	H
	Marginal	L	L	M	H
	Insignificant	L	L	L	M

Risk: ADS-DV violates lane boundaries and departs roadway

Severity: Critical injuries from rollover

Likelihood: Occasionally experiences degraded road lines in specific ODD based on statistical analysis from continuous monitoring

Apply Safety Measures

		Likelihood			
		Improbable	Remote	Occasional	Frequent
Severity	Catastrophic	M	H	H	H
	Critical	L	M	H	H
	Marginal	L	L	M	H
	Insignificant	L	L	L	M

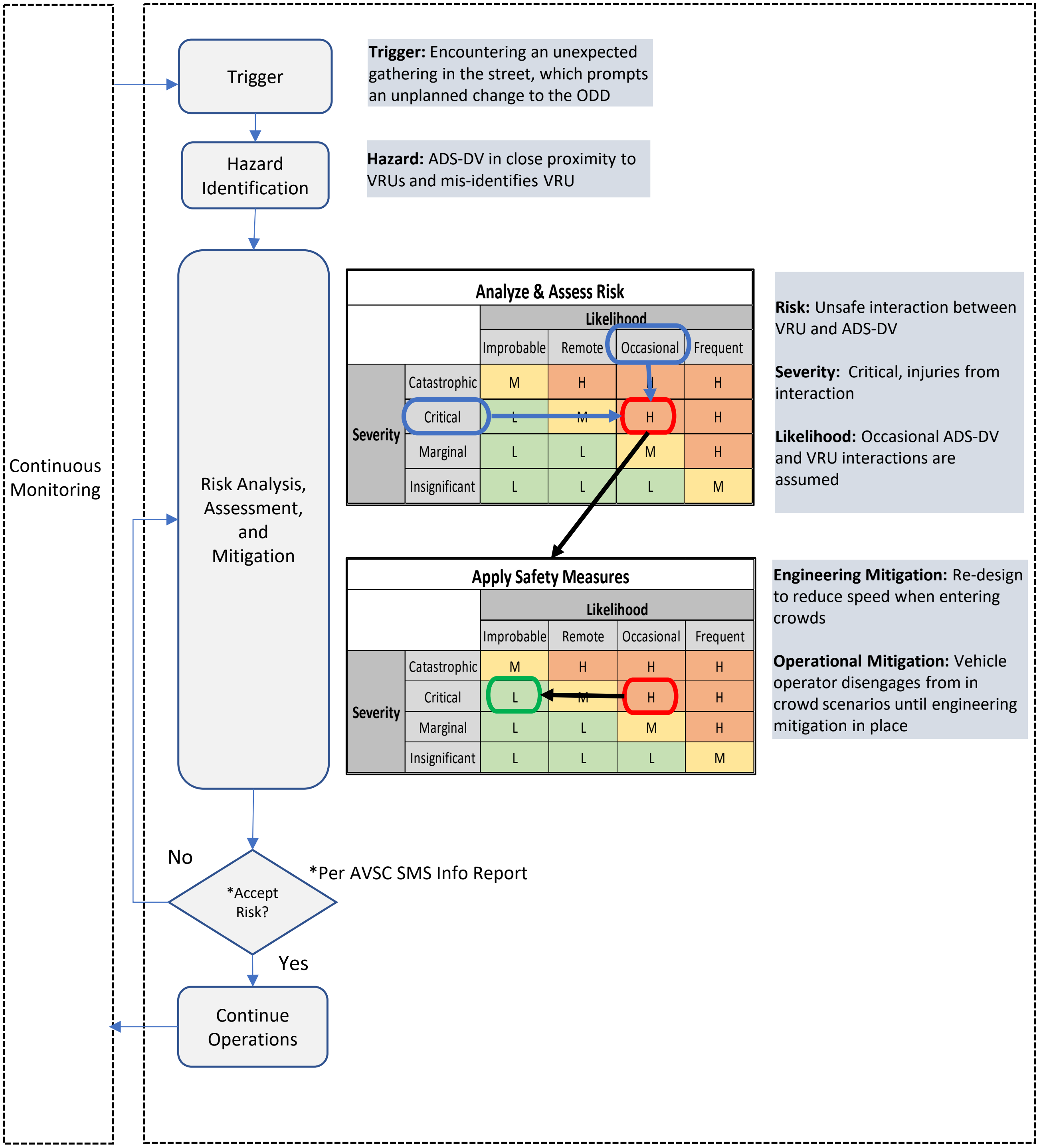
Engineering Mitigation: Re-design to reduce reliance on lane markings

Operational Mitigation: Vehicle operator disengages from autonomy in predetermined areas until engineering mitigation in place

*Per AVSC SMS Info Report

Figure 6 illustrates an ADS-DV encountering an “unknown” event such as a crowd in the middle of the street, along with the relevant ratings after completing the assessment and mitigation steps.

FIGURE 6 Change risk management process for an unknown event



Trigger: Encountering an unexpected gathering in the street, which prompts an unplanned change to the ODD

Hazard: ADS-DV in close proximity to VRUs and mis-identifies VRU

Analyze & Assess Risk

		Likelihood			
		Improbable	Remote	Occasional	Frequent
Severity	Catastrophic	M	H	H	H
	Critical	L	M	H	H
	Marginal	L	L	M	H
	Insignificant	L	L	L	M

Risk: Unsafe interaction between VRU and ADS-DV

Severity: Critical, injuries from interaction

Likelihood: Occasional ADS-DV and VRU interactions are assumed

Apply Safety Measures

		Likelihood			
		Improbable	Remote	Occasional	Frequent
Severity	Catastrophic	M	H	H	H
	Critical	L	M	H	H
	Marginal	L	L	M	H
	Insignificant	L	L	L	M

Engineering Mitigation: Re-design to reduce speed when entering crowds

Operational Mitigation: Vehicle operator disengages from in crowd scenarios until engineering mitigation in place

*Per AVSC SMS Info Report

6. Summary

Several standards are available that address different facets of risk identification, evaluation, and management and can be applied to the development of ADS-DVs. This information report addresses risk management related to planned or unplanned changes that may occur across the post-deployment ADS lifecycle. These changes may result from the addition of ADS features, functions, or new scenarios in the operating environment.

The CRM concepts described in this information report complement the initial risk management ADS developers and manufacturers conduct using relevant standards and best practices. This information report provides steps for analysis and identification of risks related to changes. It outlines both qualitative and quantitative safety risk assessment processes with examples and key categories. It also provides a list of top safety measures for consideration when implementing and validating actions to address any safety risks identified during the assessment process.

7. 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 members and engage government and industry groups to establish best practices and provide stakeholders with ADS safety-related information. This technology-neutral content can form the foundation for 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 pre-competitive 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.

8. Contact Information

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

Contact: AVSCinfo@sae-itc.org.

9. Acknowledgements

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

Aurora, GM, Honda, Lyft, Motional, VW, and Waymo.

10. Abbreviations

ADS	Automated Driving System
ADS-DV	Automated Driving System-Dedicated Vehicle
AVSC	Automated Vehicle Safety Consortium™
CRM	Change Risk Management
DDT	Dynamic Driving Task
GSA	Goal Structured Analysis
IEEE	Institute of Electrical and Electronics Engineers
IOO	Infrastructure Owner-Operators
LOPA	Layers of Protection Analysis
NHTSA	National Highway Traffic Safety Administration
ODD	Operational Design Domain
OEDR	Object and Event Detection and Response
OEM	Original Equipment Manufacturer
PMHF	Probabilistic Metric for random Hardware Failures
SAE	Society of Automotive Engineers
VRU	Vulnerable Road User
SME	Subject-Matter Expert
SMS	Safety Management System
SRA	Safety Risk Assessment

APPENDIX A. Quick Look

- Change risk management (CRM) is a process where ADS-DV manufacturers, developers, and fleet operators may evaluate if and how ADS-DV changes affect previously identified and managed safety risks. They may also identify, assess, and manage new safety risks resulting from those changes. (Section 4)

- The CRM process is initiated by the input from the CRM triggers which can arrive from multiple sources. These sources can include analysis of field operations data, results of the safety assurance process, and intentional changes in the ADS-DV design/operations made by the organization. (4.1)

- ADS-DV manufacturers and developers may consider utilizing a list or map of the dependencies between CRM triggers and aspects of the ADS-DV project that may be impacted by the change (4.1)

- Various methods of facilitation and analysis can be used for the CRM triggers and impact analysis. Examples of these methods include model-based system engineering, bowtie, event sequence diagram, and subject-matter expert (SME) brainstorming. (4.1)

- The same methods of analysis used for CRM triggers and impact analysis may be used for hazard identification. Hazards may be identified from past events or data (reactive), audits and evaluations (proactive), or from analyzing system processes and the environment to identify potential future hazards (predictive). (4.2)

- It is given that identification of every possible hazard is not possible. (4.2)

- Risk analysis follows hazard identification and is the analytical process of estimating the likelihood of a hazard occurrence and the severity of its effect. (4.3)

- The SRA is a process that includes a panel of SME stakeholders evaluating the safety risks associated with each identified safety concern or potential hazard. SRA can be achieved through various methods leveraging qualitative and quantitative approaches. (4.4)

- ADS-DV manufacturers and developers typically have traceability as referenced in UL4600 and IATF 16949 of risk-related decisions, including an escalation path. The escalation path for risks evaluated in the SRA may vary depending on each organization’s process. (4.4)

- ADS-DV manufacturers and developers may choose to utilize a qualitative SRA method to assess change-related safety risks when first integrating CRM. This approach heavily relies on subject-matter expertise and experience to assess the level of risk associated with a hazard. It does not depend on availability of quantitative inputs, such as large data sets, to produce actionable SRA outputs. (4.4.1)

- ADS-DV manufacturers and developers may identify, implement, and validate safety measures as appropriate to address identified safety risks. (4.5)

- The CRM process typically results in identification of potential safety measures to apply, if appropriate, and provides an additional reduction in risk after the changes are implemented. (4.5)

- Design, implementation, and validation of the safety measures to address functional safety, safety of the intended function, and cybersecurity violation topics typically follow organization-specific processes and policies. (4.5)

- The final function of CRM is to make sure the change has been properly addressed and the final residual risk has been accepted. (4.6)