SAFETY ASSESSMENT
for Automated Driving Systems in Canada

JANUARY 2019

Transport Canada Transports Canada

Canada

Cette publication est aussi disponible en français sous le titre *Évaluation de la sécurité des systèmes de conduite automatisés au Canada*

TP 15402E
TC 1006019 E

PRINT
Cat. No. T86-52/2018E-PDF
ISBN 978-0-660-28478-1

PDF
Cat. No. T86-52/2018E-PDF
ISBN 978-0-660-28478-1

TABLE OF CONTENTS

MESSAGE FROM THE MINISTER OF TRANSPORT

It is my great pleasure to introduce the Safety Assessment for Automated Driving Systems (ADS) in Canada, a tool developed by Transport Canada to support ADS developers in their responsibilities for ensuring the safety of highly automated vehicle technologies.

ADS technologies hold great potential to improve the safety of Canadians by reducing the number and severity of collisions on our roads. To ensure we realize this, Transport Canada is exploring new approaches that maintain safety as the top priority while also supporting innovation. If we introduce conventional regulatory approaches too early, we could impede the development of new technologies—ones that could very much enhance the safety of Canadian road users. To address the complex challenges ADS-equipped vehicles pose, we need to work with a diverse range of stakeholders on how to keep pace with emerging trends and develop sound policies.

Publishing the Safety Assessment tool is one of the ways we are seeking to do this. This assessment process aligns with our country's self-certification regulatory regime, a system that, since its start over 40 years ago, has helped to significantly lower the number of fatal collisions in Canada.

Public confidence in ADS technologies will be key to their successful adoption. This tool brings consistency to the safety evaluation parameters that ADS developers will consider as they prepare to deploy vehicles with higher levels of automation. Information we collect in safety assessment reports will also help federal and provincial/territorial governments to closely follow the evolution of ADS technologies, building a body of evidence that will inform future policies, and contribute to safe and secure Canadian roadways.

The Canadian Safety Assessment tool is closely aligned with similar policies in the United States. This approach will continue to support the close integration of our automotive industries, promoting cross-border trade and a common market for motor vehicles in North America.

I would like to thank our provincial and territorial colleagues, and all the stakeholders who provided feedback as we developed this document. The Safety Assessment is an integral part of a broader suite of initiatives we are creating to promote the safe use of ADS-equipped vehicles in Canada. In keeping with our Transportation 2030 strategic plan, the Government of Canada will continue to work with other levels of government, international colleagues, and a wide range of stakeholders, to ensure all Canadians benefit from this transformative technology.

The Honourable Marc Garneau, P.C., M.P.
Minister of Transport

EXECUTIVE SUMMARY

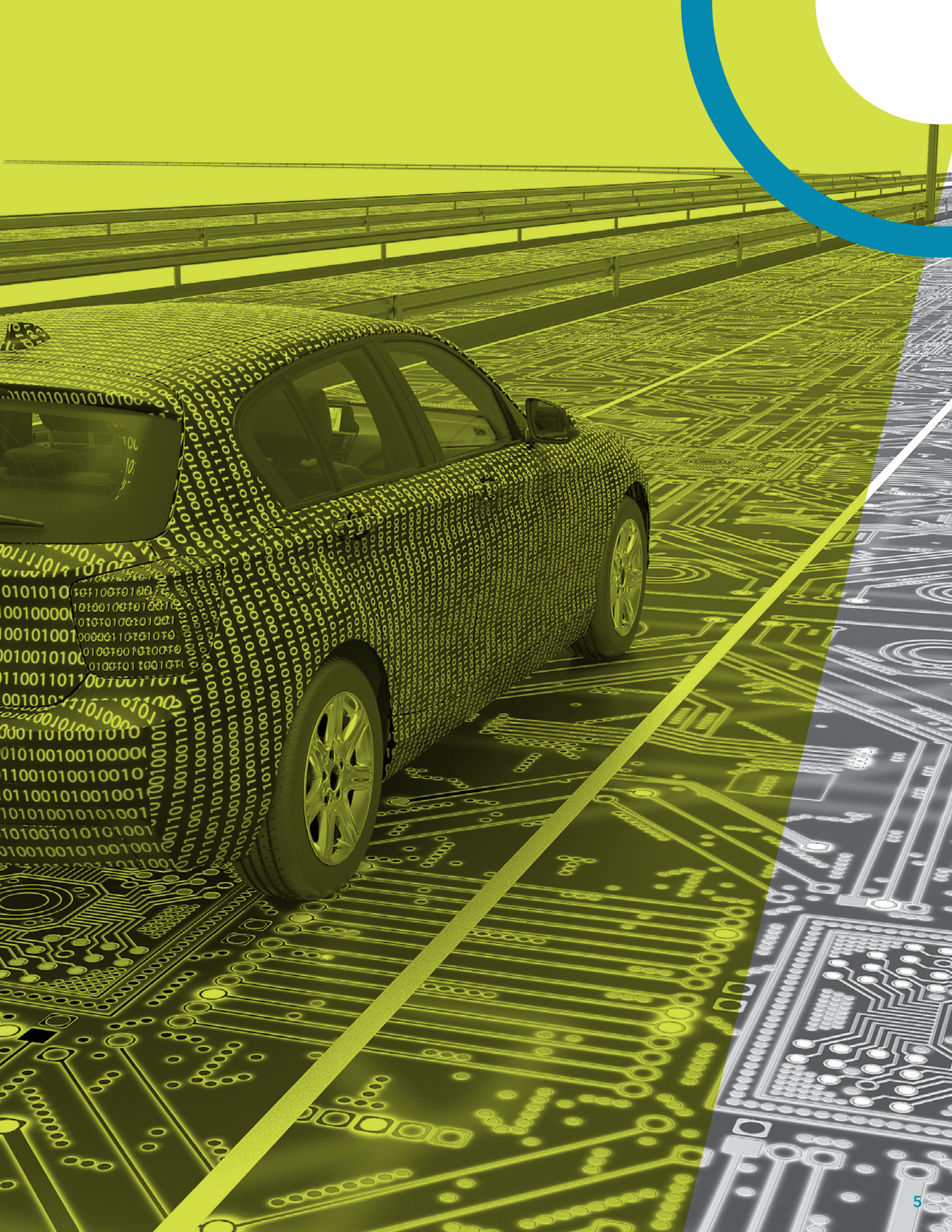
The Safety Assessment for Automated Driving Systems (ADS) in Canada is a voluntary tool to help ADS developers review the safety of vehicles equipped with SAE level 3 to 5 ADS features, which they intend to manufacture, import, operate and/or sell in Canada.

This tool has been designed as a policy measure to provide guidance on safety at a time when ADS technology is evolving and it is not yet appropriate to consider conventional regulatory approaches. As such, Transport Canada has identified 13 outcomes that vehicles equipped with ADS features should be able to perform. The outcomes are organized under three categories:

- ADS capabilities, design, and validation
- user-centered safety
- cyber security and data management

Information provided in the Safety Assessment reports will be collected by Transport Canada. ADS developers are encouraged to make their Safety Assessment reports available to the public to promote consumer awareness. Ultimately, information in these reports will help inform the ongoing development of Transport Canada's safety regime for ADS-equipped vehicles, including future safety requirements (where appropriate), and policies adopted by the provinces and territories.

As with conventional vehicles, developers of vehicles equipped with ADS features have full responsibility for ensuring the safety and security of their products and compliance with applicable Canadian safety standards and regulations. While the Safety Assessment is a risk-mitigation policy tool, defect and non-compliance provisions outlined in the *Motor Vehicle Safety Act* also apply to vehicles equipped with ADS features and will be used as a responsive measure to address any safety concerns that arise as these vehicles are deployed on Canadian roads.



INTRODUCTION

PURPOSE OF THE SAFETY ASSESSMENT TOOL

The Safety Assessment is a voluntary tool that provides a non-exhaustive list of factors for industry to consider as they review the safety and security of vehicles equipped with SAE level 3 to 5 automated driving systems (ADS)[1] before they are deployed on Canadian roads.

The Safety Assessment is a policy measure focusing on vehicle safety issues that are not addressed in existing regulations, recognising that ADS technologies are currently evolving at a pace that is not conducive to conventional regulatory approaches. By developing the Safety Assessment tool, Transport Canada is following the example of other international partners and aligning our safety policies with those of the United States to promote an integrated North American motor vehicle market. By providing a list of performance-based outcomes that ADS equipped vehicles are expected to achieve, Transport Canada is creating an environment for ADS developers to innovate while also ensuring they take responsibility for the safety of the technologies they deploy on Canadian roads.

Transport Canada's ultimate objective in developing the Safety Assessment is to promote safety. This tool will help facilitate the safe introduction of ADS technologies in Canada's transportation system and foster dialogue between industry and all levels of government in Canada.

The Safety Assessment tool has been developed by Transport Canada's Mult-Modal and Road Safety Programs Directorate, which is responsible for administering the *Motor Vehicle Safety Act* and its regulations. The Directorate's key responsibilities as they relate to motor vehicle safety include compliance and enforcement activities, the development of regulations, the conduct of research, and the development of motor vehicle safety policies and non-regulatory guidance.

SCOPE

The Safety Assessment tool should be used by entities that are designing vehicles equipped with ADS features that are intended for use on public roadways in Canada. This includes all vehicles equipped with ADS features that meet the SAE definitions for automation levels 3 through 5 that are to be manufactured, imported, operated and/or sold in Canada. Safety Assessment reports should be updated as the ADS features are refined through software updates and as newer models with novel capabilities are released.

Transport Canada strongly encourages ADS developers to make their Safety Assessment reports publically available to promote awareness of the current state of new vehicle technologies. Transport Canada may also look to information provided in Safety Assessment reports to inform the development of future vehicle safety requirements. As such, ADS developers are encouraged to provide a more comprehensive technical report which could include sensitive information (confidential business information or intellectual property) to Transport Canada. At the request of the ADS developer, Transport Canada will take all reasonable measures to ensure sensitive information is protected by entering into nondisclosure agreements[2] or through other means deemed appropriate in consultation with the ADS developer.

ADS developers are encouraged to begin using the Safety Assessment tool on the date of its publication.

1 Sourced with permission from SAE International's *Surface Vehicle Recommended Practice: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*, J3016 (2018). This document can be accessed for free at the SAE International website: www.sae.org.

Authors of the Safety Assessment referred to the June 2018 version of J3016 throughout the drafting process. Transport Canada recognizes that this standard will continue to evolve. ADS developers are encouraged to consult the latest version of J3016 available when developing their Safety Assessment reports.

2 The information is subject to release pursuant to Access to Information and Privacy or when Transport Canada is required to authorize by law to disclose the information.

LEVELS OF DRIVING AUTOMATION

LEVEL 0

NO AUTOMATION
The human driver performs all aspects of the dynamic driving task.

LEVEL 1

DRIVER ASSISTANCE
The vehicle's driver assistance features support the driver with **either** steering **or** acceleration/deceleration **under specific conditions**. The human driver is expected to perform all remaining aspects of the dynamic driving task, including monitoring and responding to the driving environment.

LEVEL 2

PARTIAL AUTOMATION
The vehicle's driver assistance features support the driver with **both** steering **and** acceleration/deceleration **under specific conditions**. The human driver is still expected to perform all remaining aspects of the dynamic driving task, including monitoring and responding to the driving environment.

LEVEL 3

CONDITIONAL AUTOMATION
The vehicle's automated driving system (ADS) features perform all aspects of the dynamic driving task, including monitoring and responding to the driving environment, **under specific conditions**. The human driver must **be alert and ready** to perform the dynamic driving task when the system requests the human driver to intervene.

LEVEL 4

HIGH AUTOMATION
The ADS-equipped vehicle performs all aspects of the dynamic driving task, including monitoring and responding to the driving environment, **under specific conditions**. The vehicle is designed to respond safely without human action to all situations, including when it reaches the limits of its operating environment.

LEVEL 5

FULL AUTOMATION
The ADS-equipped vehicle performs all aspects of the dynamic driving task, including monitoring and responding to the driving environment, **in all conditions**.

SITUATING THE SAFETY ASSESSMENT IN THE BROADER FEDERAL POLICY CONTEXT

Canada's Safety Framework for Automated and Connected Vehicles (AV/CV) outlines the ways Transport Canada is ensuring safe testing and deployment of new types of vehicles and emerging technologies. The Safety Framework situates the emergence of AV/CV in relation to existing legislation and regulations, as well as non-regulatory interventions.

To date, have two non-regulatory guidance documents for AV/CVs have been issued. Transport Canada published *Testing Highly Automated Vehicles in Canada: Guidelines for Trial Organizations* in June 2018, which focuses exclusively on temporary automated vehicle trials and outlines minimum safety considerations for trial organizations. The Canadian Council for Motor Transport Administrators (CCMTA), in collaboration with Transport Canada and provincial/territorial governments, also developed the *Canadian Jurisdictional Guidelines for the Safe Testing and Deployment of Highly Automated Vehicles*. These guidelines offer recommendations for provincial/territorial jurisdictions to consider as they develop policies for automated vehicles related to registration, licencing, and insurance, among others.

The Safety Assessment is the third non-regulatory tool for AV/CVs captured under the broader Safety Framework and focuses more specifically on the safe performance of vehicles that are imported into or manufactured within Canada for deployment purposes (i.e. sale or operation).

Together, the Safety Assessment, Guidelines for Trial Organizations, and the CCMTA Jurisdictional Guidelines are non-regulatory interventions that foster innovative collaboration between all levels of government in Canada and facilitate engagement with industry and other stakeholders to promote understanding of the rapid evolution of emerging technologies. This, in turn, allows governments to better position future safety requirements, including potential regulations and legislative amendments.

The Safety Assessment will continue to be adapted as ADS technologies mature and the broader policy context evolves. Transport Canada may also consider other non-regulatory guidance, including for specific issues related to commercial vehicles.

LINKS TO EXISTING FEDERAL MOTOR VEHICLE SAFETY LAWS AND REGULATIONS

The Safety Assessment has been developed in the same spirit of Canada's broader self-certification regulatory regime. Although its purpose is to provide ADS developers with a tool to assess the safety of technologies for which there are no existing regulations and standards, all vehicles equipped with ADS features must continue to comply with applicable legislation at the federal and provincial/territorial levels, including the *Motor Vehicle Safety Act*.

There are two provisions within the *Motor Vehicle Safety Act* that can be leveraged to address vehicles that may not be compatible with existing regulations and standards, including those equipped with ADS features. The first is the Section 7(1)(a) importation exception, which applies to vehicles that are temporarily imported for the purposes of exhibition, demonstration, evaluation or testing. The second is the Section 9 exemption process, which applies to vehicles being deployed in Canada.

IMPORTATION

Vehicles imported into Canada must comply with the *Motor Vehicle Safety Regulations* (MVSR) and the *Canada Motor Vehicle Safety Standards* (CMVSS) applicable to their class.

If a non-compliant vehicle is imported solely for the purposes of exhibition, demonstration, evaluation, or testing, **the person importing the vehicle** may apply for an importation exception as described in section 7(1) (a) of the *Motor Vehicle Safety Act* using a Schedule VII declaration. The Schedule VII process allows for temporary importations for periods up to one year or such other periods as specified by the Minister of Transport. A Safety Assessment report would not have to be developed for these vehicles, though they would be captured by the Transport Canada document *Testing Highly Automated Vehicle in Canada: Guidelines for Trial Organizations*.

EXEMPTIONS

Section 9 of the *Motor Vehicle Safety Act* describes a process that allows **companies**[3] to be exempt from conforming to a prescribed standard for a specified period if the exemption would promote new safety features or new kinds of vehicles, technologies, or systems. To be granted an exemption, companies must submit an application along with supporting documentation, which includes a risk assessment, to Transport Canada. When granting an exemption, the Minister may specify conditions the company must meet to promote the safe operation of the vehicle.

The applicant may consider developing a Safety Assessment report to serve as a supporting document for the Section 9 exemption process when appropriate. Please note that the Safety Assessment tool is not intended to replace or act as a risk assessment methodology required for the exemption process. In addition to Canadian safety standards and regulations, manufacturers are responsible for ensuring compliance with other relevant federal, provincial/territorial, and municipal legislation.

DEFECTS

As with conventional motor vehicles, ADS developers are ultimately responsible for ensuring the safety of their vehicles. While the MVSR do not currently account for ADS technologies, provisions in the *Motor Vehicle Safety Act* related to defects (Section 10) apply to all vehicles, regardless of their level of automation. These authorities allow Transport Canada to mandate testing and analysis (Section 8.1) and order companies to take corrective actions once a notice of defect has been given (Section 10.5).

3 The *Motor Vehicle Safety Act* defines a company as a person: a) who is engaged in the business of manufacturing vehicles or equipment in Canada, b) who is engaged in the business of selling to other persons, for the purpose of resale by those persons, vehicles or equipment obtained directly from a person described in (a) or the agent of such a person, or c) who imports a vehicle or article of equipment into Canada for the purpose of sale.

SHARED RESPONSIBILITIES FOR MOTOR VEHICLE SAFETY

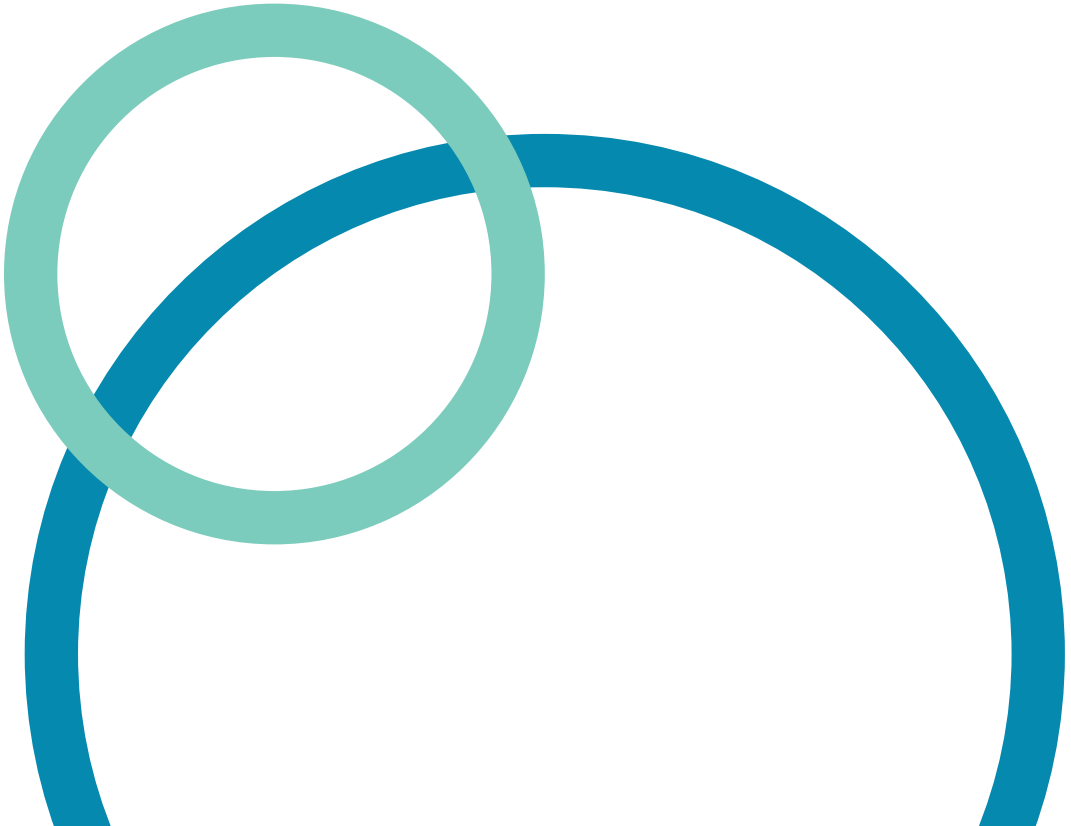
Federal, provincial/territorial and municipal levels of government share responsibility for motor vehicle safety in Canada.

Under the *Motor Vehicle Safety Act* (MVSA), Transport Canada establishes safety regulations that apply to the importation of motor vehicles and designated motor vehicle equipment, and the shipment of newly manufactured motor vehicles and designated equipment across provincial/territorial boundaries. The objective of these regulations is to reduce the risk of death, injury, and damage to property and the environment. In addition to conducting motor vehicle safety research, investigations and managing recalls of safety-related motor vehicle defects, Transport Canada also has a responsibility to exercise leadership and offer guidance on new and emerging technologies to promote motor vehicle safety in this rapidly changing environment.

Through Innovation, Science and Economic Development Canada (ISED), the federal government also sets and enforces compliance with technical standards and licencing requirements for wireless technologies integrated in vehicles and roadside infrastructure.

Provincial and territorial governments oversee many of the laws and regulations governing the use of vehicles on public roads. These responsibilities include driver licensing; vehicle registration; motor vehicle insurance and liability; vehicle maintenance standards; and enacting traffic laws. Municipalities are responsible, to varying degrees, for managing passenger transportation, including public transit and taxis; parking; traffic control; and enacting and enforcing by-laws. Municipalities and provincial/territorial governments share responsibility for enforcing traffic laws, and for adapting infrastructure to support the deployment of connected and automated vehicles. Some responsibilities, such as those for public education and awareness are shared across all three levels of government.

The Safety Assessment tool has been developed by Transport Canada in recognition of the need for federal leadership and guidance to support other levels of government as they consider policy measures related to ADS-equipped vehicles in their respective jurisdictions. Completed Safety Assessment reports can provide insight and offer assurance on the safety features of ADS-equipped vehicles, at a time when there are no safety standards or regulations for these technologies.



COMPONENTS OF THE SAFETY ASSESSMENT

The Safety Assessment outlines 13 expected outcomes ADS-equipped vehicles should be capable of performing. The expected outcomes have been identified based on a review of available evidence and are aligned with existing Transport Canada policies. Canadian studies and reports including the Report of the Standing Senate Committee on Transport and Communications *Driving Change: Technology and the Future of the Automated Vehicle* (January 2018), the report presented to the Council of Ministers of Transportation and Highway Safety *The Future of Automated Vehicles in Canada* (January 2018), and the overarching objectives of *Transportation 2030: A Strategic Plan for the Future of Transportation in Canada* (2016) have all influenced the choice of expected outcomes presented in the Safety Assessment tool. Similar policies in place in other countries and work underway at the Global Forum for Road Traffic Safety (WP.1) related to automated vehicles were also considered.

The Safety Assessment's 13 expected outcomes have been organized into three sections:

- **ADS capabilities, design, and validation:** reviews vehicle design considerations linked to the specific level of automation, intended use, operational design domain (ODD), basic vehicle functions, as well as testing, verification and validation that has been conducted.
- **User-centered safety: focuses on safety systems;** the accessibility of the controls; driver/user knowledge of capabilities, limitations, and maintenance requirements; and ADS operation in the event of collisions or system failures.
- **Cyber security and data management:** focuses on strategies used to manage cyber security risks, safe functioning of the vehicle as it is deployed, data collection by the ADS, including considerations for the sharing of data with government, and protection of personal information.

When writing Safety Assessment reports, ADS developers should clearly describe how their vehicles and ADS features meet each of the expected outcomes. A Writer's Guide which lists specific questions for each of the identified outcome statements, is provided in Annex A. This tool is meant to provide further guidance, and may be referred to by ADS developers who are drafting Safety Assessment reports.

For clarity on definitions of technical concepts used throughout the Safety Assessment, including the levels of automation, readers can refer to SAE International *Surface Vehicle Recommended Practice* J3016[4].

4 Authors of the Safety Assessment referred to the June 2018 version of J3016 throughout the drafting process. Transport Canada recognizes that this standard will continue to evolve. ADS developers are encouraged to consult the latest version of J3016 available when developing their Safety Assessment Reports.

OVERVIEW OF SAFETY ASSESSMENT EXPECTED OUTCOMES

3. Object Event Detection and Response
The vehicle has object event detection and response (OEDR) capabilities adapted to its ODD that enable safe and appropriate actions to be taken when subjected to day-to-day traffic conditions, as well as unexpected events.

1. ADS Level of Automation and Intended Use
The ADS features' level(s) of automation is/are clearly defined based on the levels of automation found in SAE J3016, as this will determine what behaviors are expected of drivers/users. Some vehicles may be capable of operating at different levels of automation in different modes.

5. Testing and Validation
Safety risks were considered throughout the development of the vehicle and the ADS technologies. Sufficient pre-deployment testing has been conducted and validation methods have been employed to verify performance, safety of the intended functionality, occupant safety, and failure handlings. Validation and verification have been used to ensure safe integration and operation of the vehicle and ADS features in day-to-day traffic and in response to unexpected events and various weather conditions.

2. Operational Design Domain
The ADS(s) has/have a clearly defined Operational Design Domain (ODD). Domain constraints are known, and the vehicle will respond safely and predictably when the ODD is exceeded.

6. Safety Systems
The vehicle is equipped with safety systems with appropriate redundancies that continuously monitor system performance, perform fault detection, hazard analysis, signal any malfunctions, and ultimately take corrective actions or revert to a minimal risk condition when needed.

4. International Standards and Best Practices
Where they apply, and as much as possible, the vehicle and ADS comply with relevant standards and best practices, such as those developed by SAE International and the International Organization for Standardization (ISO).

ADS CAPABILITIES, DESIGN, AND VALIDATION

USER-CENTRED SAFETY

CYBER SECURITY AND DATA MANAGEMENT

9. User Protections during Collisions or System Failures
The vehicle is equipped with adequate active and passive safety features to protect occupants and other road users, and mitigate injuries and damages in the event of a collision or system failure. The vehicle will be brought to a safe state following a collision or system failure, and will convey safety critical information to passengers, first responders, and emergency services.

11. System Updates and After-Market Repairs/ Modifications
In the event of a system update or after-market repair or modification, measures are in place to verify all vehicle systems continue to operate safely, and as intended.

7. Human-Machine Interface and Accessibility of Controls
Vehicle controls are accessible to users (i.e. intuitive/easy to understand). The vehicle can communicate critical messages to passengers and other road users when needed, taking into account relevant accessibility factors, needs of different occupants, and the intended use of the vehicle.

12. User Privacy
Measures are in place to safeguard the information collected by the vehicle and ADS to protect the personal information and privacy of occupants and other road users.

8. Public Education and Awareness
Concrete actions have been taken to ensure awareness of the capabilities and limitations of the ADS features of the vehicle, as well as the vehicle's safe fallback conditions. Drivers/users are aware of what is expected of them in relation to the dynamic driving task under different conditions and of the vehicle and ADS features maintenance requirements. Drivers/users will be informed of any changes in these expectations that arise following a system update.

13. Collaboration with Government Agencies and Law Enforcement
In the event of a collision or other incident, data collected by vehicles and ADS features is shared with federal, provincial/territorial, and municipal law enforcement and government agencies to support investigations, including defect and collision investigations.

10. Cyber Security
Adequate design and mitigation strategies have been developed to protect the ADS-equipped vehicle from cyber security threats. Programs, plans, and/or operating procedures have been established to manage cyber events. Consideration should also be given to how these events are communicated to other stakeholders, including government agencies, to prevent similar events in the future.

ADS CAPABILITIES, DESIGN, AND VALIDATION

This first section of the Safety Assessment aims to collect general information about the ADS features. Points articulated under this section should be used to inform responses in all sections of the Safety Assessment, recognizing that vehicle safety features should be adapted to the intended use, level of automation and overall risks the vehicle will likely encounter while it is in use. Descriptions of relevant standards that have been incorporated into the ADS features design, and the testing methods that have been employed to verify and validate performance are also requested.

1. ADS LEVEL OF AUTOMATION AND INTENDED USE

Expected outcome: The ADS features' level(s) of automation is/are clearly defined based on SAE levels of automation found in J3016. The definition of the level of automation identifies the agent responsible for the dynamic driving task (DDT) under different circumstances and the vehicle's intended use is clearly stated.

It is important for ADS developers to clearly define the ADS feature(s) level(s) of automation based on SAE J3016, as this will determine what behaviors are expected of drivers/users. Some vehicles may be capable of operating at different levels of automation in different modes.

Examples of potential intended uses of the vehicle could include private ownership, ride-share fleet, service vehicles, public transportation, etc. Each of these scenarios presents different safety risks that should be considered throughout the subsequent responses. Understanding the vehicle's intended use and its level(s) of automation will provide context for the Safety Assessment report and help situate the responses to the subsequent expected outcomes, showing that safety measures reflect relative risks the vehicle is likely to encounter.

2. OPERATIONAL DESIGN DOMAIN

Expected outcome: The ADS feature(s) has/have a clearly defined Operational Design Domain (ODD). Domain constraints are known, and the vehicle will respond safely and predictably when the ODD is exceeded.

It is important for ADS developers to clearly define and document the ODD of the vehicle. This demonstrates a strong understanding of the circumstances in which the ADS will be able to operate, including, but not limited to, any constraints related to road types, weather, speed restrictions, and traffic conditions, among others. Developers are encouraged to design the ADS features in a way that prohibits users from engaging or activating their functions when the ODD is exceeded. Throughout its operation, the ADS should be able to comply with traffic rules and should prioritize actions that will maintain the safe flow of traffic. In unforeseen circumstances or when the boundary conditions of the ODD are crossed, the ADS should react in a way that minimizes danger to passengers and other road users. Information provided for this expected outcome should reflect testing and validation (5) described below. The ODD and its constraints should be taken into account when considering the intended use of the vehicle (1), the object event detection and response (OEDR) (3) capabilities, human-machine interface and accessibility of controls (7), as well as the approach taken to address public and consumer awareness (8).

3. OBJECT AND EVENT DETECTION AND RESPONSE

Expected outcome: The vehicle has OEDR capabilities adapted to its ODD that enable safe and appropriate actions to be taken when subjected to day-to-day traffic conditions, as well as unexpected events.

Description of the OEDR capabilities provided in Safety Assessment reports should focus on how the ADS perceives and navigates its surroundings and include information on the sensor suite and integration, as well as the recognition and decision software. A nonexhaustive list of different actors, vehicles, and road-users that vehicles equipped with ADS features should be able to identify and react safely to is enumerated in the Writer's Guide (see Annex A). This outcome statement is closely linked to those related to the ODD (2) and to safety systems (6), which together allow for a clearer understanding of how the ADS will perform the driving task, particularly in a dynamic environment where it will encounter various other road users.

4. INTERNATIONAL STANDARDS AND BEST PRACTICES

Expected outcome: Where they apply, and as much as possible, the vehicle and ADS comply with relevant standards and best practices, such as those developed by SAE International and the International Organization for Standardization (ISO).

ADS developers are encouraged to document how existing standards have been integrated into the design of the vehicle and ADS; ADS developers are also invited to provide a rationale in instances when they have chosen to deviate from existing standards. Having a clear understanding of what existing international standards and best practices focused on system safety, security, data protection and others that are already being integrated into the vehicle will support government agencies as they consider and draft future safety requirements for vehicles equipped with ADS features.

The response to this outcome statement provides assurance that systems integrated in the vehicle and ADS have been developed based on the most recent and up-to-date safety practices.

5. TESTING AND VALIDATION

Expected outcome: Safety risks were considered throughout the development of the vehicle and the ADS technologies. Sufficient pre-deployment testing has been conducted and validation methods have been employed to verify performance, safety of the intended functionality, occupant safety, and failure handlings. Validation and verification have been used to ensure safe integration and operation of the vehicle and ADS features in day-to-day traffic and in response to unexpected events and various weather conditions.

To meet this outcome statement, ADS developers are requested to describe the testing and validation methods that were employed to ensure the vehicle is able to operate safely and securely, and to meet all 12 other expected outcomes listed in the Safety Assessment, taking into account its intended use. Descriptions of the arrangements made to ensure testing and validation methods were adhered to throughout the development of the vehicle are also welcome.

Information listed for this expected outcome will provide assurances that the vehicle's various systems operate safely in an integrated manner under various conditions. Testing and validation methods can also be used to justify the safety of novel features and systems for which no international best practices or standards exist. Information provided for this expected outcome may be reviewed to inform the eventual development of future safety requirements for vehicles equipped with ADS features.

USER-CENTRED SAFETY

This second section of the Safety Assessment is focused on safety elements incorporated to protect drivers/users and passengers of the vehicle, as well as other road users, including in the event of a collision or system failure. Emphasis is placed on ensuring the ADS features are intuitive, accessible and adapted to user needs. Considerations on how the vehicle will interact with other road users, including vulnerable road users (e.g., pedestrians, cyclists, etc.) and emergency responders are also highlighted.

Transport Canada recognizes that safety features and risk mitigation strategies should be adapted to the vehicle's intended use. Driver/users and owner/operators need to be well informed of the capabilities and limitations of the technologies in their vehicles, and understand their roles and responsibilities related to the vehicle's safe operation and maintenance. Outcomes related to consumer awareness and public education have also been included in this section.

6. SAFETY SYSTEMS

Expected outcome: The vehicle is equipped with safety systems with appropriate redundancies that continuously monitor system performance, perform fault detection and hazard analysis, signal any malfunctions, and ultimately take corrective actions or revert to a minimal risk condition when needed.

For this outcome statement, ADS developers are invited to describe how the vehicle's safety systems were designed, and how various interdependent systems interact. Responses for this expected outcome may include information on how the system's performance is monitored throughout operation and what happens when faults are detected. The information provided should also focus on the safe fallback state of the vehicle, and describe how systems will determine when a minimal risk condition is achieved.

When responding to this expected outcome, ADS developers may include information on quality management systems that were employed throughout the development of the vehicle and ADS according to relevant standards. Safety systems should be based on a hazard analysis and risk assessment, whereby the ADS developer can document that they have considered and controlled risks to an acceptable level, based on the ADS's design and intended functionality.

7. HUMAN MACHINE INTERFACE AND ACCESSIBILITY OF CONTROLS

Expected outcome: Vehicle controls are accessible to users (that is, intuitive and easy to understand). The vehicle can communicate critical messages to occupants and other road users when needed, taking into account relevant accessibility factors, needs of different occupants, and the intended use of the vehicle.

This outcome statement aims to prevent safety hazards that could arise from the accidental misuse or misinterpretation of the ADS features. If the driver/user needs to intervene, insufficient time to respond and/or confusing signalling could create safety risks. If we further consider that some vehicles equipped with ADS features may be used as part of a ride-sharing or car-sharing service, drivers/users may be exposed to various types of ADS features with differing interfaces, which could lead to further confusion. ADS developers are encouraged to provide information on strategies that will be employed to ensure controls are accessible to drivers/users across various vehicle models. Vehicles equipped with ADS features should clearly show when they are available, when they are operational, and when they are not available for use. If the dynamic driving task is shared, the vehicle must clearly communicate the need for the driver to assume control, and provide sufficient warning time to facilitate a safe transition, with due consideration given to factors like driver distraction.

Methods used to validate the safe transition between the ADS and the driver should be described in testing and validation (5). The selected strategies should be informed by risk analyses and consider the needs of the intended use population. In ADS dedicated vehicles, additional consideration should be given to the integration of accessibility features for passengers with special needs.

Due consideration should be given to how the vehicle will signal its intentions to other road users, including vulnerable road users (e.g. through visual and/or auditory cues). To the extent possible, Transport Canada encourages the development of and adherence to industry standards and best practices to promote a degree of consistency in the ways vehicles signal their intent to other road users to promote safety and minimize confusion.

8. PUBLIC EDUCATION AND AWARENESS

Expected outcome: Concrete actions have been taken to ensure awareness of the capabilities and limitations of the ADS features of the vehicle, as well as the vehicle's safe fallback conditions. Drivers/users are aware of what is expected of them in relation to the dynamic driving task under different conditions and of the vehicle and ADS features maintenance requirements. Drivers/users will be informed of any changes in these expectations that arise following a system update.

This outcome statement has been included to address safety risks that could arise from the misuse of the ADS(s). To achieve this, drivers/users of vehicles equipped with ADS features need to have a clear understanding of how and when the vehicle will perform the dynamic driving task, and what behaviours are expected of them under different circumstances. Vehicles equipped with ADS features may also have different maintenance requirements that need to be performed to ensure systems continue to operate as intended. These requirements should be clearly communicated to the driver/user and owner/operator.

Other road users, including vulnerable road users, should also be kept informed of how the vehicle will react to them, and how they should react to the vehicle. To address this expected outcome, ADS developers are encouraged to provide information on how each of these considerations will be met.

9. USER PROTECTIONS DURING COLLISIONS OR SYSTEM FAILURES

Expected outcome: The vehicle is equipped with adequate active and passive safety features to protect occupants and other road users, and mitigate injuries and damages in the event of a collision or system failure. The vehicle will be brought to a safe state following a collision or system failure, and will convey safety critical information to passengers, first responders, and emergency services.

Vehicles equipped with ADS features, particularly ADS-dedicated vehicles, present opportunities for novel seat configurations and other vehicle layout options that are not available in conventional vehicles. This outcome statement seeks to ensure that as these new options are considered, ADS developers remain mindful of possible collisions with other road users and existing vehicle designs. ADS developers should always integrate appropriate active and passive safety features in their vehicles to protect occupants and other road users.

This expected outcome also seeks to ensure that during a collision, occupants and other road users are cared for and damages and injuries are prevented to the extent possible. When first responders and law enforcement respond to collisions involving vehicles equipped with ADS features, any precautionary measures they need to take should be evident. In addition to these considerations, ADS developers are encouraged to describe how vehicles will be brought to a safe state following a collision, and how necessary actions, including system tests, will be performed before the vehicle returns to circulation.

CYBER SECURITY AND DATA MANAGEMENT

This third and final section of the Safety Assessment has been developed to address cyber security concerns related to ADS features, and the unprecedented amount of data that will likely be collected by ADS-equipped vehicles. Potential OTA software updates also present new safety risks that need to be appropriately mitigated. Outcomes in this section aim to ensure these risks are anticipated to help ensure the safe operation of vehicles equipped with ADS features, the protection of user data and personal information, and collaboration with government agencies to support investigations.

10. CYBER SECURITY

Expected outcome: Adequate design and mitigation strategies have been developed to protect the ADS-equipped vehicle from cyber security threats. Programs, plans, and/or operating procedures have been established to manage cyber events. Consideration should also be given to how these events are communicated to other stakeholders, including government agencies, to prevent similar events in the future.

As more advanced technologies are included in vehicles, particularly those equipped with ADS(s), the risk of external interference by malicious actors increases. This expected outcome is intended to ensure ADS developers are mindful of cyber security risks throughout the development and deployment of their vehicles. To manage cyber risks, ADS developers should use relevant international best practices and standards throughout the design of the vehicle and ADS features. ADS developers should also consider how to address software and/or hardware vulnerabilities that emerge as their vehicles are deployed. Recognizing that cyber events experienced by one vehicle may also be repeated and perpetrated against others, ADS developers are also invited to share information when cyber events occur to promote awareness and collaborative approaches to address safety and security risks

11. SYSTEM UPDATES AND AFTER-MARKET REPAIRS/ MODIFICATIONS

Expected outcome: Expected outcome: In the event of a system update or after-market repair or modification, measures are in place to verify all vehicle systems continue to operate safely, and as intended.

Vehicles equipped with ADS features have complex integrated sensor suites and other systems that are co-dependent and calibrated to operate safely. System updates, OTA updates, after-market repairs, or modifications may introduce safety risks by interfering and compromising the safe operation of the systems. Furthermore, ADS developers may identify software and/or hardware issues after vehicles are deployed, and require the installation of updates to ensure the integrity of safety critical systems.

For this expected outcome, ADS developers are invited to describe measures that are in place to ensure systems continue to function as intended throughout the vehicle's lifecycle over a reasonable timeline defined at their discretion. Due consideration should be given to how updates that affect the performance of the ADS features will be shared with end-users (see public education and awareness (8)). If certain ADS functions can no longer be safely supported by the developer (e.g., deployed hardware cannot support new software updates), vehicles should revert to a "fail-safe" mode (that is, certain ADS functions may need to be disabled).

12. USER PRIVACY

Expected outcome: Measures are in place to safeguard the information collected by the vehicle and ADS to protect the personal information and privacy of occupants and other road users.

Vehicles equipped with ADS features have the potential to collect unprecedented amounts of data on passenger movements and mobility habits. For this expected outcome, ADS developers are requested to describe the measures that are in place to protect occupant and road users' personal information. ADS developers are also invited to describe how they intend to ensure Canadian privacy laws at the federal and provincial/territorial levels will be respected.

13. COLLABORATION WITH GOVERNMENT AGENCIES AND LAW ENFORCEMENT

Expected outcome: In the event of a collision or other incident, data collected by vehicles and ADS features is shared with federal, provincial/territorial, and municipal law enforcement and government agencies to support investigations, including defect and collision investigations.

Vehicles equipped with ADS features will likely include more devices that record data on the performance of the vehicle in the lead-up to a collision. This data can help law enforcement and government agencies understand what happened as they investigate collision scenes, including for the attribution of fault and investigations of possible defects. For this expected outcome, ADS developers are asked to describe what type of data may be available in vehicles equipped with ADS features, and how this data could be accessed.

ADS developers should also consider means to share data on vehicle performance with vehicle owners and/or users upon request (i.e. to support insurance claim processes). ADS developers are also invited to work with government agencies to share anonymized data, including on mobility patterns, which could inform programming, including urban planning activities.

SUBMITTING SAFETY ASSESSMENTS TO TRANSPORT CANADA

The Safety Assessment provides a non-exhaustive list of considerations to inform broader risk assessment, testing and other safety management processes conducted by ADS developers. Mitigation strategies and safety features described in Safety Assessment reports should reflect the intended use of the vehicle, according to its ODD, and be adapted to relative risks and potential hazards.

Completed Safety Assessment reports will be collected by Transport Canada. Safety Assessment reports should be submitted by entities that are designing vehicles equipped with ADS features for use on public roadways in Canada, before they are deployed. Transport Canada will monitor industry's submission of Safety Assessments, and may explore future measures to require the submission of these reports, in alignment with practices adopted by international counterparts such as the United States.

A designated point of contact should be identified in the Safety Assessment report to answer any questions related to the information provided. By submitting a Safety Assessment report to Transport Canada, manufacturers are providing a written account of the safety measures that have been incorporated in the design of vehicles with ADS features[5].

Transport Canada encourages ADS developers to make a version and/or summary of their Safety Assessment reports available to the public to promote transparency and consumer awareness.

Provincial and territorial governments may refer to information provided in Safety Assessment reports to inform decisions related to motor vehicle safety policies for automated vehicles within their jurisdictions.

If ADS developers choose to submit detailed technical reports to Transport Canada, which contain sensitive information, the department will take all reasonable measures to ensure the information provided is protected. Non-disclosure agreements[6] and other options deemed appropriate to protect confidential business information can be explored at the request of the ADS developer.

Completed Safety Assessment reports as well as any questions or requests for more information on the Safety Assessment process can be directed to:
tc.avcv-vcva.tc@tc.gc.ca

5 ADS developers may wish to submit Safety Assessment reports prepared for other jurisdictions. If this option is chosen, Transport Canada requests that an information note or cover page be added to address any Canada-specific additions and identify where different outcomes are addressed in the report.

6 The information is subject to release pursuant to Access to Information and Privacy or when Transport Canada is required to authorize by law to disclose the information.

CONCLUSION

This Safety Assessment tool has been developed in recognition of Transport Canada's primary mandate to promote the safety and security of Canada's transportation system. As technologies facilitating higher levels of vehicle automation continue to evolve, policies will need to provide space for innovation and novel approaches without compromising safety. Our hope is that information provided in Safety Assessment reports will offer insight into the evolution of technology to inform the development of future policy tools and support provincial and territorial governments as they manage road safety policies within their jurisdictions.

ADS-equipped vehicles have tremendous potential to address a wide variety of mobility and transport challenges faced by all Canadians. All levels of government have a key role to play in shaping the ways ADS technologies will be deployed to meet the needs of citizens and provide new opportunities to create greener, safer, and more accessible communities.

As ADS technologies mature and best practices and standards emerge, the Safety Assessment tool may be updated and streamlined as longer-term policy options are developed. Transport Canada remains committed to working with all stakeholders across different levels of government, industry, non-governmental organizations and academia to ensure our policy approaches to ADS technologies meet the needs of Canadians, adhere to national values, promote Canadian interests, and build on the best available evidence.

ANNEX A: SAFETY ASSESSMENT WRITER'S GUIDE

Questions identified in the Safety Assessment Writer's Guide are meant to provide further clarity and direction to ADS developers as they review the safety of their ADS equipped vehicles. The questions provide a non-exhaustive list of considerations that ADS developers are encouraged to reflect upon as they produce their Safety Assessment reports. Specific questions have been developed for each of the 13 expected outcomes identified in the Safety Assessment tool.

Transport Canada recognizes that not all questions may be relevant or applicable to all ADS technologies, and it is incumbent upon ADS developers to produce reports that reflect their unique products. Some ADS developers may choose to focus their Safety Assessment reports on the safety elements they deem most critical. However, entities are encouraged to provide some minimal explanation as to how they have achieved each of the 13 expected outcomes.

ADS CAPABILITIES, DESIGN, AND VALIDATION

1. ADS Level of Automation and Intended Use

a. What ADS features is the vehicle equipped with? What is their level of automation?

b. How is the ADS identified (e.g., does it have a specified hardware version, software version, etc.)?

c. Is the driver/user responsible for any portion of the DDT including fallback? Under what conditions?

d. What is the intended use of the vehicle (transportation of goods vs. people; highway vs. low-speed; urban vs. rural; etc.)? Is the vehicle intended for private ownership or will it be managed by a ride-share program? Will you, the ADS developer, be operating the ride-share program, or will the vehicles be marketed to a third-party for this purpose?

2. Operational Design Domain

a. How is ODD of each ADS feature defined? Please include any domain constraints (weather, road type, speed restrictions, traffic conditions, etc.).

b. How does the vehicle respond when the limits of the ODD are exceeded?

c. Is it possible to activate or engage the ADS outside of the ODD?

3. Object Event Detection and Response

a. What systems are used for OEDR? How does the vehicle perceive its surroundings to determine if there is an object or event (computer vision, sensor fusion, sensor suite and integration, localization/recognition and decision software/route planning)?

b. What is the range of view of the sensors? What is the range of object detection?

c. How does the system treat unknown objects or objects it cannot classify?

d. What are the known sources of interference with the operation of your system?

e. Can the vehicle identify and react safely to:

   i. Pedestrians (adults, children, individuals with mobility devices)

   ii. Other vulnerable road users (cyclists, motorcycles)

   iii. Law enforcement or emergency services vehicles and officers

   iv. Canadian signs and road infrastructure

   v. Vehicle types that are commonly found on Canadian roadways (logging trucks, snow plows, etc.)

vi. Other service providers (e.g., construction workers, crossing guards, utility service providers, waste collection, snow plows, public transit vehicles, school buses, etc.) with occasional responsibilities to direct traffic, or that require specific behaviours (e.g., stopping, yielding right-of-way)

vii. Other vehicles or road users that do not respect traffic laws (e.g., vehicles that are speeding, do not stop, do not signal, etc.)

viii. Animals/wildlife

4. International Standards and Best Practices

a. What safety risks were considered in the design of the vehicle? Which industry standards, voluntary guidance, best practices, design principles and original approaches were employed to mitigate safety risks (e.g., ISO 26262 functional safety process standard for road vehicles, etc.)? If applicable, please describe the subsystems to which the standards were applied.

b. Have you deviated from international standards in the design of the ADS-equipped vehicle? If so, why?

5. Testing and Validation

a. What design and validation processes have been used to manage safety risks (e.g., critical systems test scenarios, on-road testing, lab testing, model in the loop, software in the loop, hardware in the loop, driver in the loop, etc.)?

b. Snow, ice, freezing rain, low temperatures, snow/ice accumulation on sensors/vehicles, gravel and dirt roads, among others, are all common conditions in Canada that could pose additional risks to the safe operation of the vehicle and the ADS features. What measures have been taken to mitigate these risks?

c. How have factors related to extreme seasonal variability (changing topography due to snow accumulation, variable light conditions due to changes in foliage, road markings hidden by snow and ice, etc.) been factored into the testing and validation of the vehicle?

d. How did you arrive at the determination that testing was sufficient and safety risks were appropriately mitigated?

USER-CENTERED SAFETY

6. Safety Systems

a. What safety-critical systems are provided with redundancies and why? How are the redundant systems designed (sensor level, hardware level, software level), and how do they interact? Do they continually contribute to decision-making, or are they only activated in the event of a malfunction?

b. How do the ADS features perform fault detection? What will happen in the event of a fault detection, sub-system malfunction or failure (e.g., limp mode, restricted ODD, ADS becomes unavailable)? Will the driver/user be able to take over at any point? Is there an emergency override built into the system?

c. What does the vehicle consider to be a minimal risk condition? Recognizing the choices will be situation dependent, what options will the vehicle consider for its minimal risk condition (e.g., stop in-lane; stop on shoulder; stop at next available rest-stop)?

d. How will the vehicle determine that a minimal risk condition is achieved? What actions will the vehicle take after a minimal risk condition is achieved? If this is an ADS-dedicated vehicle, how will the vehicle be put back into service? Does it need a signal from an occupant to resume or will it do so when the conditions place it back within its ODD?

7. Human-Machine Interface and Accessibility of Controls

a. What processes and best practices were used to ensure vehicle controls are intuitive and easy for drivers/users to understand? What measures are in place to prevent the unsafe misuse of the vehicle's features?

b. How does the vehicle communicate critical messages to users/drivers and other passengers? How will indicators show:

i. When the ADS is functioning as intended?

ii. When the system is malfunctioning, or sensors need to be recalibrated?

iii. When the ADS is on?

iv. When ADS functions are available/unavailable for use (if applicable)?

v. A request for the operator to resume/assume the dynamic driving task (if applicable)?

c. Is the vehicle equipped with systems that allow occupants to seek assistance in the event of an emergency or when more information is needed?

d. Is the vehicle accessible to passengers with special needs (e.g., with mobility impairments, hearing/vision impairments, service animals, children, mobility devices)? What design features have been developed to meet the needs of these users?

e. What measures have been taken to ensure vehicle actions are intuitive to other road users?

Additional questions for vehicles equipped with SAE level 3 ADS features:

e. If the ODD boundaries are exceeded or if the driver must take over dynamic driving task, how much time is given for a take-over request?

f. Is the system equipped with risk mitigation features that will bring the vehicle to a minimal risk condition if the driver does not take over the dynamic driving task?

g. How will the vehicle react in the event of a critical situation involving an imminent hazard when there is not enough time to facilitate a safe transition of the dynamic driving task?

h. Is the vehicle equipped with systems to monitor the availability of a take-over-ready driver (e.g., weight in the driver seat, fastened seat belt, eye-movement monitoring, etc.)?

8. Public Education and Awareness

a. What measures have been/will be taken to ensure drivers/users are aware of the capabilities and limitations of the vehicle's ADS, including any domain constraints?

b. How will drivers/users and owner/operators be informed of critical tasks related to safe operation and maintenance of the vehicle (e.g., in-car tutorials, training or education programs for sales representatives)?

c. How will drivers/users be informed of critical system updates, and particularly how system updates may change or affect the way they are expected to operate the vehicle?

d. Have measures been taken to ensure other road users (drivers, pedestrians, cyclists, etc.) know:

i. That the vehicle is equipped with ADS(s)?

ii. How to interact with the vehicle?

iii. How the vehicle will react to them?

9. User Protections during Collisions or System Failures

a. What are the vehicle's crash avoidance design features and capabilities? What pre-crash scenarios can the vehicle detect?

b. What active and passive safety measures are in place to protect occupants and other road users?

c. What design considerations have been used to ensure crash compatibility with existing vehicles on roadways?

d. What actions/system responses will occur immediately before, during, and after a crash to protect occupants? Will the actions/system responses vary depending on the severity of the crash?

e. How will the vehicle systems be brought to a safe state following a crash?

f. Does the ADS seek to minimize external damages and impacts on pedestrians or vulnerable road users during a crash?

g. How will first responders and emergency service providers be protected and informed about the hazards and procedures associated with the vehicle? Consideration should be given to how safety messages will be transmitted to emergency responders and first on scene (members of the public).

CYBER SECURITY AND DATA MANAGEMENT

10. Cyber Security

a. What methods are available to interface external systems or software with the vehicle through wired (ODB, USB, memory card, etc.) or wireless (V2X, Wifi, 4G/LTE, etc.) means?

b. What testing has been done to ensure system intrusion safety? How segregated are the various systems?

c. In addition to any international standards adhered to (see Expected Outcome 4), are additional measures in place to address cyber security threats (e.g., self-audits, regular software updates, forensic support, aftermarket risk mitigation, etc.)?

d. How will the vehicle systems detect a potentially malicious cyber event?

e. What action will the vehicle take in the event of a cyber incident? Does the vehicle have means of executing safe behaviours when encountering unsafe or compromised sensor information (i.e., GPS spoofing, sensor modification etc.)? How will vulnerabilities and/or safety risks be communicated to occupants?

f. Will government agencies (Transport Canada, Canadian Centre for Cyber Security) be informed of cyber incidents, including those occurring outside of Canada?

g. Is there a vehicle cyber security program and/or plan in place to support the response to a cyber event affecting the vehicle and ADS (e.g., a designated team, governance structure, protocols, testing, training, etc.)?

h. How will vulnerabilities (software and/or hardware) that are observed as vehicles are deployed be addressed?

11. System Updates and After-Market Repairs/ Modifications

a. Is the vehicle equipped with an auditable version control system that shows the system version in operation, past and/or pending updates? How is the information presented or accessed?

b. In the event of a system update, after-market repair or modification to the software or hardware of the vehicle, what tests will be performed to ensure other systems are not compromised and continue to function as intended (i.e., that subsystems still interact correctly and existing functions are not affected)?

c. In the event of an update conducted by the ADS developer, what regression testing will be conducted to ensure system performance is not degraded by the update prior to its implementation (e.g., simulation, track test, real-world)?

d. What measures are in place/will be taken to ensure OTA updates are completed securely, safely and in full (e.g., the integrity of the communication link to the vehicle is safeguarded and maintained throughout the update; the vehicle is not in operation while the update is being performed, etc.)? How will the ADS developer ensure the update is legitimate and/or that no code has been modified, added or removed from the update?

e. Does the vehicle need to be off for a certain period of time during or after the update is installed? If the vehicle is electric, does it need to have a certain level of power remaining? How will this information be conveyed to drivers/users?

12. User Privacy

a. Is personal information of occupants or other road users transmitted to the ADS developer during normal operation, or only during servicing? What kind of personal information is being transmitted (video, sound, GPS, other sensor data)?

b. How will drivers/users consent to the collection and use of their personal information? What processes are in place to ensure drivers/users are aware of what personal information is being collected and how it is being used?

c. What measures are in place to safeguard occupants' and road users' personal information and prevent its loss, theft, or unauthorised access, use or disclosure?

d. How will occupants and other road users be made aware of any loss, theft, or unauthorised access, use, or disclosure of their personal information?

13. Collaboration with Government Agencies and Law Enforcement

a. What systems within the vehicle collect and store data on the vehicle's operation? Where are these systems located? What tools are required to retrieve this data?

b. Is data collection constant, or it is triggered by a set of events (rapid lateral or longitudinal change, ADS disengagement, etc.)? If the latter, what is the amount of time pre and post event that is captured? How long is this information stored?

c. What assistance will be provided to law enforcement or collision investigators to retrieve data needed to support investigations?

d. Are there processes in place to enable data sharing with vehicle owner/operators when requested, for example, to facilitate insurance claims? How will vehicle owners be made aware of these processes?


omous
ng
unication
ery
gation
rorless
logy
00m
48
mph
/Autonomous
/Sensing
/Communication
/Battery
/Navigation
/Mirrorless
/Ecology