

4.2. The ADS shall interact safely with the user in the vehicle¹

Until now it has always been clear who's driving, who is responsible for performing the driving task, not only for controlling the vehicle but also for perceiving and interpreting the environment and for choosing a cause of action. That clarity is fading with the introduction of automation in the vehicle and will become even less clear with the introduction of automated driving systems (ADSs) where it concerns vehicles equipped with ADS that can also be driven by a human being inside the vehicle.

In vehicles that can still be driven by a human every part of the driving task that is not automated needs to be performed by a human and every part of the driving task that is not 'perfectly' automated needs to be compensated for by a human. It therefore has to be clear who performs which part of the driving task during a trip. It has to be clear what a human can and cannot do while the ADS performs (a part of) the driving task. It has to be clear when the ADS can no longer perform the driving task and the human has to take over. It has to be clear if the ADS is activated or can be activated. This kind of clarity is essential for safety, essential for a safe use of the ADS. And this clarity is provided through the interaction between the human and the ADS. The interaction is more than the interface and includes for example how an ADS 'behaves' in the perception of its user (e.g., if braking then standby mode; not only how much it decelerates).

The following recommendations mainly focus on vehicles that can also be driven by a human. The recommendations applying to vehicles that cannot be driven by a human being will be indicated in ????

Considerations

Vehicle that can (still) be driven by a user

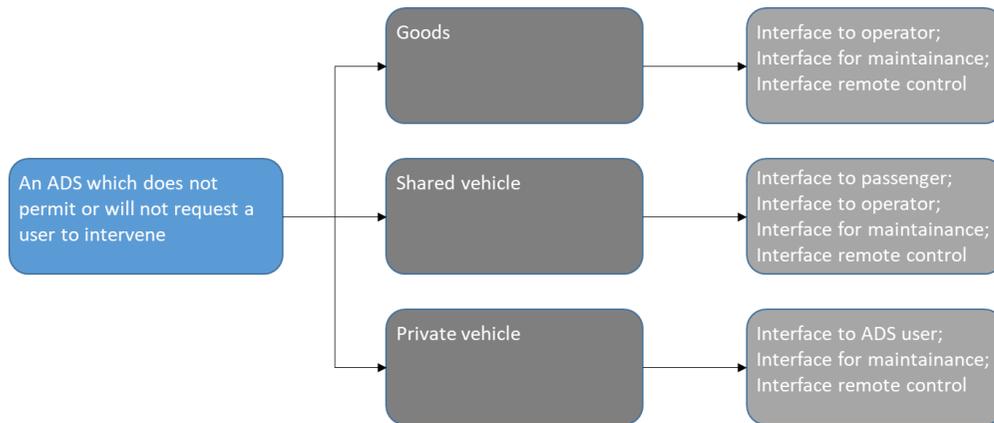
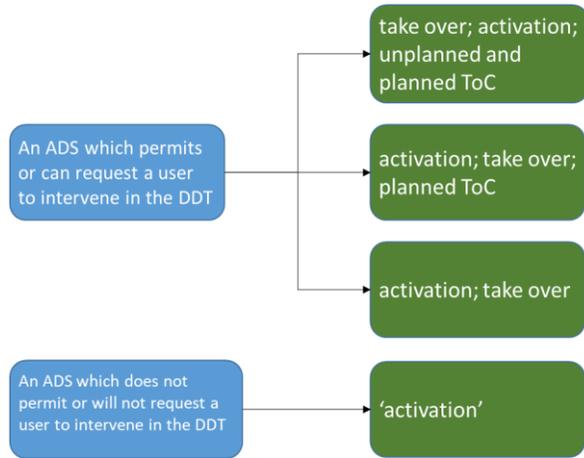
Vehicle that can be driven by maintenance personnel (not 'ordinary' user) or steward

Vehicle that can be driven by remote operator

¹ The Human Centred Design Process is an important process to achieve a safe interaction between a vehicle with and its users. Any process should encompass

- Analyses of user needs and risk, setting safety and usability objectives, as well as specifying user requirements and ensuring user understanding and context]
- Producing design solutions to meet these requirements
- Conducting evaluations, particularly real world testing on real users (i.e., not the people who are developing the products)
- Competent personnel; human factors design and testing activities should be assigned to qualified personnel, with clearly defined roles and responsibilities, including process oversight and sign-off.
- Monitoring; device performance should be monitored in the field and this information should be used to set future design targets and evaluate designs against these requirements.

This part should be integrated in the safety management system of the organization (for audit) (ISO 13407: 1999)



4.2.1. The ADS and its features shall have a high-level commonality of design of the user interaction, and the interface.

4.2.1.1 The ADS should be designed to foster a level of trust that is aligned with its capabilities and limitations to ensure proper use of the system

Commented [BR(1)]: avoid over reliance?

4.2.1.2 The operation of the interaction shall at least have in common:

- a) The sequence of actions and states in the activation of the ADS
- b) The sequence of actions and states in the transition of control process from the ADS to the user
- c) The sequence of actions and states in the de-activation of the ADS
- d) The role of the user after a transition of control from the ADS to the user or after the deactivation of the ADS. This role shall normally be a fully engaged driver without any control assistance (temporarily intervening safety systems such as ESC will remain activated)

Commented [BR(2)]: Canada: why normally?

4.2.1.3 The interaction should be simplified:

- a)
- b) [Limit the number of potential transitions]
- c) [Limit the number of settings]
- d) [Limit the number of different interaction modes]

A high-level commonality in the interaction processes between the vehicle and a user for all brands and models helps drivers to develop and apply a single mental model of how their responsibilities relate to the level of automation and of how to interact with the systems. It also helps to reduce the risk of user confusion (e.g., mode confusion) when changing vehicle.

4.2.2. The ADS HMI shall provide clear, conspicuous and unambiguous information to support comprehension by the user.

- 4.2.2.1 The vehicle shall indicate its ADS capabilities in terms of their automated [features] and their ODD.
- 4.2.2.2 The ADS shall inform the user on the current conditions:
 - a) ADS status information
 - b) The availability of automated features
 - c) Responsibility
 - d) Permitted NDRA or not-permitted NDRA
 - e) Potential roles to activate
 - f) “Standard” information
 - i) [.....]
 - g) ADS failure information
- 4.2.2.3 The ADS shall inform the user in time on the upcoming conditions:
 - a) ODD boundaries
 - b) Upcoming actions or change in roles
 - c) Oncoming decisions/manoeuvres
 - d) Estimated time until take over in normal conditions
 - e) Transition-related communication.
- 4.2.2.4 The ADS shall ensure that safety related information is prioritised and presented in a clear and unambiguous manner.

Commented [BR(3): Canada: Not sure if ODD boundary information is essential for the user because b) already addresses the need to inform the user of upcoming actions.

To ensure that there is no mode confusion or a lack of clarity about responsibilities of the ADS and the user or a lack of clarity about the capabilities of the ADS it is essential that specific kind of information needs be presented such that the information is well received and well understood.

4.2.3. The ADS shall be designed to prevent misuse and errors in operation by the user.

- 4.2.3.1 The controls dedicated to the ADS shall be clearly distinguishable from other controls
- 4.2.3.2 The ADS shall be designed to prevent inadvertent activation or deactivation
- 4.2.3.3 The ADS shall provide feedback when the user attempts to enable unavailable functions

For a safe use of the ADS mode confusion needs to be avoided. Therefore it is essential that an ADS cannot be activated by mistake within the ODD nor that it can de-activated. Misuse of the ADS can for example be that a fall-back user is sleeping while the ADS performs the driving task.

4.2.4. The ADS shall ensure safe ADS feature activation.

- 4.2.4.1 The ADS shall inform the user that preconditions for activation are met
- 4.2.4.2 The activation shall follow a common sequence of actions and states
- 4.2.4.3 The ADS shall provide confirmation that the system is activated

4.2.4, 4.2.5 and 4.2.6 strongly rely on the commonality concept. That's why some of the detailed provisions are also presented 4.2.1. To avoid mode confusion after a transition of control the transition should be to a fully engaged driver without any assistance. If assistance would still be possible this could, for example, be indicated and the user could activate that specific kind of ADAS.

4.2.5. An ADS which permits a transition of control shall be designed to ensure safe transitions of control.

- 4.2.5.1 The Transition of control process shall follow a common sequence of actions and states
- 4.2.5.2 Transition of control shall return to a common default user role
 - a) The role of the user after a transition of control from the ADS to the user or after the deactivation of the ADS. This role shall normally be a fully engaged driver without any control assistance (temporarily intervening safety systems such as ESC will remain activated,
- 4.2.5.3 The ADS shall continuously verify whether the user is available for the Transition of Control and
 - a) adapt the Transition of Control process, including the time budget where feasible, to the state of the user and/or to the ADS.
 - b) warn the user if not available when required
 - c) register user response indicating readiness for transfer of control
- 4.2.5.4 The ADS shall verify that the user is in stable control of the vehicle to complete the Transition of Control process
- 4.2.5.5 During transition, the ADS shall remain active until the Transition of control has been completed or the ADS reaches a minimal risk condition

Commented [BR(4)]: Canada: why normally?

4.2.6. An ADS which permits user-initiated takeovers of control shall be designed to ensure a safe user-initiated takeover process.

- 4.2.6.1 Such ADS shall allow the user to initiate a take-over process.
- 4.2.6.2 The deactivation shall follow a common sequence of actions and states in the transition of control (change of user roles)
- 4.2.6.3 The ADS shall momentarily delay deactivation of driving control when immediate human resumption of control could compromise safety.
- 4.2.6.4 The ADS shall provide clear, specific feedback of the completion of a user initiated take over.
- 4.2.6.5 The user initiated take over shall return to a common default user role being the driver.
 - a) The role of the user after a transition of control from the ADS to the user or after the deactivation of the ADS. This role shall normally be a fully engaged driver without any control assistance (temporarily intervening safety systems such as ESC will remain activated,

Commented [BR(5)]: Canada: why normally?

4.2.7. The ADS shall be supported by documentation and tools to facilitate user understanding of the functionality and operation of the system.

- 4.2.7.1 The ADS manufacturer / vehicle manufacturer (as appropriate) shall provide documentation available for audit on:
 - 4.2.7.1.1 The details of their user-centred design process
 - 4.2.7.1.2 Its intended educational approach:
 - a) Theoretical and practical training
 - b) How its HMI design aligns with common HMI and interaction
 - 4.2.7.1.3 Owner's manual describing at least:
 - a. An operational description of ADS' (features) capabilities and limitations (the information should also refer to specific scenarios)
 - b. A description of the roles and responsibility of driver/user and ADS when an ADS (feature) is on/off
 - c. A description on the permitted transitions of roles and the procedure for those transitions
 - d. A general overview of NDRA allowed when an ADS feature is active
- 4.2.7.2 The ADS manufacturer / vehicle manufacturer (as appropriate) shall create the following in-vehicle tools such that
 - 4.2.7.2.1 the ADS supports the user in correct operation (coaching)
 - 4.2.7.2.2 the ADS gives prompt feedback on erroneous operation

Commented [BR(6)]: Suggested by Canada

The documentation and tools that are provided by the ADS manufacturer / vehicle manufacturer on the ADS will ensure that the user of an ADS can develop a general mental model of how the system functions, its

capabilities, the user responsibilities and a more specific mental model of how to interact with the systems. A correct mental model is necessary for correct usage and expectations of the ADS.

4.2.8 The HMI of an ADS which permits a transition of control shall be integrated with the entire vehicle HMI

4.2.8.1 The vehicle and ADS HMI need to take into account potential impairments of users (such as colour blindness, impaired hearing) which do not require specific hardware adaptations of the vehicle.

To avoid mode confusion it has to be clear to the user the differences between the different levels of automation that can be available in a vehicle so that an ADAS mode can never be confused with an ADS mode.

4.2.9 A dedicated ADS vehicle shall provide vehicle occupants with means to request a minimal risk manoeuvre to stop the fully automated vehicle.

Commented [BR(7): Based on EU regulation

4.2.10 A dedicated ADS shall ensure that it operates within operational relevant legal boundaries.

Commented [BR(8): This is to ensure that with no driver an ADS checks whether seat belt is on, within load limits, within # of passengers, etc. That's why it says operational relevant. We don't mean that the ADS needs to check it is insured. For dual mode vehicles this needs to be arranged

Annex ?

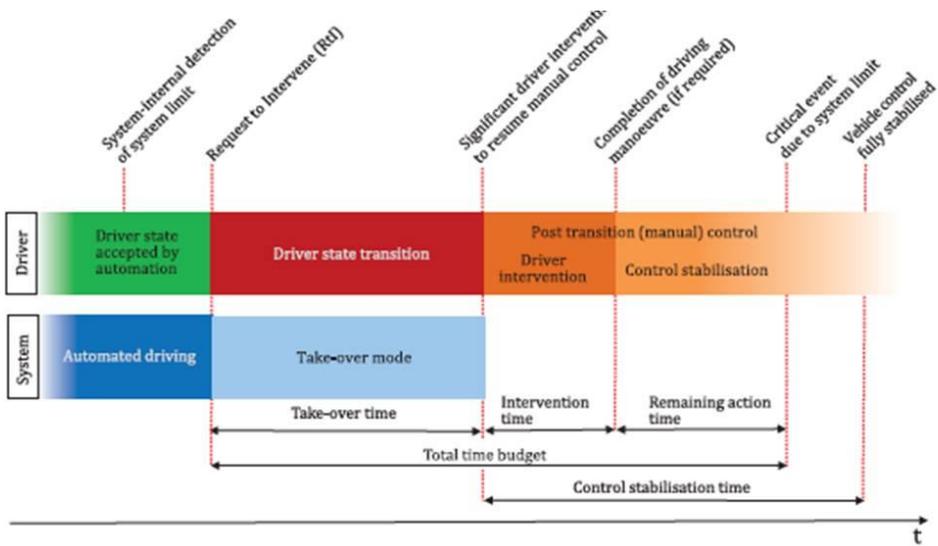
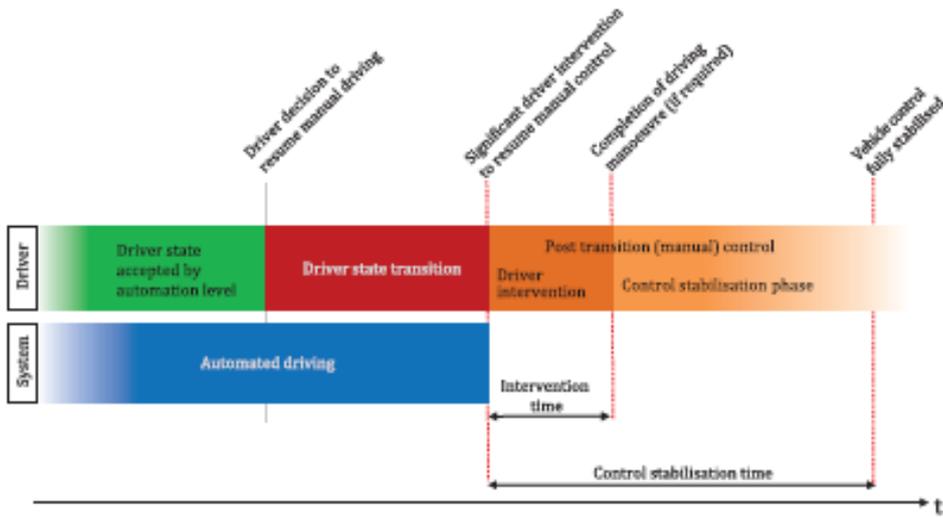


Figure 2 — System-initiated transition from automated to manual driving

Annex ??



(ISO/TR 21959-1:2020(E))