Applied EV submission

Received 16 May 2024

To Whom It May Concern,

To gradually increase the public's trust in automated vehicles and allow for technology improvements over time, please consider the following recommendations when introducing automated / autonomous vehicles into Australia…

COVERED COMPLETELY OR IN PART BY UN ECE R1426 FRAMEWORK:

1. Steering, Braking and energy/power subsystems need to have appropriate safety integrity levels – as does the whole of vehicle "system". Typically in the automotive field, these ratings are described in ISO 26262 (for electronics and software). It's highly recommended that qualified 3rd parties audit designs to a standard such as ISO 26262.
   Note that for SAE Level 4 and beyond, where a highly alert driver who could normally push through system failures does not need to be present, managing failed systems must be done through redundant mechanisms. Consider short fail operational times (eg, less than 250m) rather than back-to-base options when a system fails to avoid the potential for the failure to also occur on the redundant system (which is more likely in the event of non-diversified hardware and/or software).
   Consider motion control / steering/braking/energy/connectivity certification (deterministic so ISO 26262 applicable) should be separate to AD software / planning & perception certification (subject to SOTIF audits due to the nature of AI usage).
   An alternative to being prescriptive on how to achieve safety, regulators could define a minimum set of safety goals and OEMs could choose how to meet those safety goals for autonomous vehicles.

2. Initially limit physical intervention of teleops to eStopping a vehicle. Attempting control of steering, braking, etc. will be very difficult for some years due to latency issues with cloud / mobile network integrations.

3. CyberSecurity & Privacy: Vulnerabilities need to be protected against within the whole vehicle control system including its connectivity infrastructure. It is highly recommended that qualified 3rd parties audit designs to appropriate CyS (ref UN 155) and Privacy best practices. Vehicles must never be weaponised against the public or have their sensor sets encroach on the publics' privacy.

4. V2x/V2I considerations: Establish a common communications protocol so that vehicles can effectively utilise each other's data to maximise protection of the public.
   Rationale: Fleet sizes won't initially be big enough in Australia to provide enough data per brand. Cross-brand communication is recommended. Consider minimum data logging and storage expectations (UN ECE working group details publicly available). Roll-outs of tech should not adversely influence other road users (preferably improve their experience through correct road usage).

CONSIDERATIONS NOT COVERED OR POTENTIALLY INSUFFICIENTLY COVERED BY UN ECE R1426 FRAMEWORK:

5. Highly recommended to avoid SAE Level 3 (especially in the first 10 years until full acceptance and increased capability). Go straight from Level 2/2+ to Level 4.
   Rationale: Expecting drivers to regain control of a vehicle ad hoc doesn't work well. Note also that the reason the driver will be expected to take over is because something is wrong with the vehicle. This means that not only does the driver have to become alert and regain control, he/she will have to fault-find within a few seconds to push through an issue which could be related to a brake system OR a steering system OR an energy system, etc. This is too much to expect of a driver who has not had to intervene before.

6. Visually identify vehicles running autonomously (especially in the first 10 years until full acceptance and increased capability).
   This is a recommended "state light" colour scheme for vehicle identification:

Condition	State Light Colour	Flash Rate	Comment
AD Control	Turquoise	none	SAE J3134
DbW Control	OFF	none	
EV Charging Fault *	TBD	none	avoid red R48
EV Charging *	Green	Normal	eg, Tesla

EV Charged *	Green	none	eg, Tesla

** information is included about existing EVs just to show colours used*

DbW = Drive-by-Wire (applicable to vehicles that can also be human operated only).
RC = Remote Control (applicable to logistics vehicles moving in confined spaces into maintenance areas, for example).

Note also that state lights need their own diagnostics / fail operational mode.

Additionally, existing indicators/hazard lights are recommended to exhibit the following:

Condition	Hazard Lights Status	Flash Rate
Remote Control (RC) – line of sight	On	none
Emergency Stop (eStop)	On	Normal
MRM / Exit Path underway	On	Normal
System Error	On	Normal

MRM / "Exit Path" could be considered the fail operational portion of the mission as described in Point 1 above. Also see patents applicable in this area due to its importance.

Additionally, for automated passenger vehicles, a light at eye level (approx) and an audible warning that a vehicle is about to move off automatically is recommended:

Condition	Warning Light Colour	Flash Rate	Comment
AD-controlled Vehicle Movement commencing	TBD	none	avoid red R48

This is essentially advising passengers to either get in or get out (don't get caught halfway in when the vehicle moves off). Audible warning should accompany the Warning Light.

Options could include occupant sensing or soft-close doors for autonomous vehicles.

7. Minimise technical exposure: It's highly recommended that the first years of approved/production exposure to automated vehicles are Level 4 for cargo only – no passengers. This effectively reduces the risk and the need for occupant protection strategies. Risk is limited to people outside of the vehicle ONLY.
   Early/pre-production trials, of course, will need to have internal supervision ready to take over. Consider AD provider "L" plates.

8. Ensure switchable eSIMs or redundant telecommunications methods are allowable by telecommunications providers and utilised by the vehicle. In the event of outages such as the extended Optus outage, you don't want fleets of vehicles stranded on our road systems when plausible mission status signals stop being transmitted to vehicles.

9. Determine how to deal with accessories / peripherals responsibly. They will often be added after vehicle sale to enable use-cases (with or without the OEMs cooperation for the integration). Examples include robot arms to enact some of the functions that a human driver would have otherwise conducted. Peripherals can extend beyond the perimeter of the vehicle (ideally only when the vehicle is stationary). Peripherals can also draw significant power from the vehicle detracting from the effective range required to achieve a mission/task successfully.

10. Consider harsh penalties for parties that deliberately interfere with autonomous vehicles. Interference can endanger members of the public or cause significant societal inconvenience. Rectification of issues can be very costly and witnesses may not be available for unattended autonomous vehicles.

I hope this information assists.

Best regards,