Australian Government
Department of Infrastructure, Transport, Regional Development, Communications and the Arts

National Transport Commission

Third-party interference with an ADS

This paper **expands** on previous policy work

April 2024

Overview

An Automated Driving System Entity (ADSE) is responsible for the safety of its Automated Driving System (ADS). Despite this, other parties could interfere with an ADS in a way that creates safety risks. This risk will be addressed through third-party interference offences, along with certain ADSE safety duties and requirements.

This topic paper explores the proposed third-party interference offences and seeks feedback.

Key points

An ADSE is responsible for the safety of its ADS for the duration of the ADS's design life.

Interference with an ADS can either be inadvertent or deliberate. It could include unauthorised work on an ADS or ADS components (both hardware and software) and it could also be an intentional act to affect ADS safety.

Both the Automated Vehicle Safety Law (AVSL) and state and territory law will include provisions for third-party interference offences. These offences would be intended to operate concurrently to enable a flexible approach, depending on the nature of the third-party interference attempt. To support consistency across state and territory laws, model third-party interference offence provisions could be developed.

ADSEs will also be required to take actions to prevent third-party interference attempts as far as reasonably practicable, and to notify the automated vehicle in-service regulator of any detected third-party interference attempts on its ADSs.

Consultation questions

We welcome feedback on all elements of the regulatory framework. In relation to third-party interference, we are especially interested in the following.

16. Do you support third-party interference offences being included in both the AVSL and state and territory law?

Risk of third-party interference

Given the complex nature of ADSs, there are a number of ways in which ADS safety could be compromised through intentional and unintentional actions. Such actions include:

- an unauthorised person performing any repairs, maintenance or modifications on an ADS including:
  - ADS component maintenance or repair of ADS hardware or software
  - ADS modifications, such as installation of ADS hardware or software that does not meet the ADSE's specifications
  - changing the operational design domain, that is, the conditions in which the ADS's features can be used
- deliberate engagement of an ADS that has been disengaged by an ADSE
- action intended to impair ADS operation or impact ADS safety (such as hacking ADS software)
- performing maintenance or repair of non-ADS components that affect ADS safety.

A third-party interference offence in the AVSL

To address this risk, we propose that the AVSL include measures designed to prevent people performing unauthorised works on an ADS, or deliberately compromising ADS safety. The broad prohibition on third-party interference would cover matters such as:

- unauthorised access to, or modification or impairment of, the existing ADS software, for example overriding settings or configurations specified by the ADSE or the new regulator
- unauthorised installation of new software, including spyware, malware, gridlockware[1], or other software or updates not authorised by the ADSE or the regulator
- unauthorised access to, or modification or impairment of, the ADS hardware, including disabling or modifying a sensor, camera or other ADS components
- unauthorised installation of new hardware as part of the ADS, for example installing sensors that are not approved by the ADSE
- deliberate engagement of an ADS that has been disabled by an ADSE or at the direction of the regulator
- repairs to an ADS or its components that have not been authorised by the ADSE or the regulator, or that are not performed by an authorised repairer, maintainer or modifier (see the *Additional measures for repairers, maintainers, modifiers* paper)
- making changes to an ADS's operational design domain that have not been authorised by the ADSE or the regulator

---

[1] Gridlockware refers to code intended to disable a vehicle until a ransom is paid.

- interference with non-ADS components of an automated vehicle, if this affects ADS safety.

It is proposed that the AVSL will also have an offence for unauthorised aftermarket ADS installation. This offence is related to third-party interference, but is not identical, as aftermarket installation is not interference with an existing ADS. An entity that installs an ADS aftermarket but is not certified as an ADSE by the new regulator would commit an aftermarket installation offence. More information on aftermarket ADS installation is in the *Automated Driving System Entity certification* paper.

The automated vehicle policy framework set out in the National Transport Commission's 2022 paper identified that third-party interference offences should be included in state and territory law and be enforced by state and territory governments.[2] We now consider that including third-party interference offences both in the Commonwealth AVSL and in state and territory law would provide the most appropriate level of regulatory coverage. Having third-party interference offences in the AVSL will enable simplified enforcement of third-party interference offences that occur fleet-wide or in more than one jurisdiction.

The new regulator will be able to provide guidance on what types of work or action would consistitute a third-party interference offence under the AVSL. Guidance will help educate people who work with ADSs to ensure they are aware of the risk of interfering with an ADS when performing works on an automated vehicle, as well as point them towards relevant information on automated vehicles (for example, in the automated vehicle register). More information is in the *Establishing an automated vehicle register* paper.

State and territory third-party interference offences

In addition to including third-party interference offences in the AVSL, states and territories will also introduce third-party interference offences in their laws. The two sets of offences would operate concurrently to provide comprehensive coverage of third-party interference.

To support consistency across states and territories, and complementary operation with the proposed AVSL offence, we intend to develop model third-party interference offence provisions.

The **types** of action that would constitute a third-party interference offence are likely to be broadly similar between Commonwealth and state and territory law.

However, third-party interference offences are likely to vary in size and scope, and having provisions in both the AVSL and in state and territory laws will enable an appropriate enforcement response. States and territories are more likely to handle those third-party interference offences that are committed by an individual, affect individual ADSs, or have impacts limited to a single jurisdiction. Where third-party interference offences occur in more than one jurisdiction, it may be more suitable to use the third-party interference offences in Commonwealth law.

Consultation questions

16. Do you support third-party interference offences being included in both the AVSL and state and territory law?

---

[2] National Transport Commission (NTC), *The regulatory framework for automated vehicles in Australia*, NTC, Melbourne, 2022, accessed March 2024.

Safety duties and other requirements

The AVSL will include a safety duty requiring ADSEs to consider and protect against third-party interference with its ADSs. While ADSEs are not responsible for the actions of third parties, the AVSL will require the ADSE to notify the regulator of any third-party interference attempts that it becomes aware of.

Preventing ADS interference

The AVSL will place safety duties on ADSEs by identifying the safety outcomes they are expected to achieve. These will include a duty for the ADSE to make efforts to ensure that the ADS cannot be interfered with by third parties, so far as is reasonably practicable.

This duty is intended to require an ADSE to consider potential external risks to the safe operation of the ADS, such as interference with the vehicle or the ADS. The duty does not mean the ADSE will be held responsible for the actions of third parties, which are covered by third-party interference offences.

To meet this duty, an ADSE would need to:

- actively consider third-party interference risks and take steps to address or mitigate risks arising from the potential interference
- protect the networks and facilities with which its ADS interfaces from unauthorised interference or access, to prevent third-party interference (for example, encrypting software updates or making hardware physically tamper-proof).

Notifying the regulator

Where a third-party interference attempt is detected, it will be beneficial for the regulator to be notified of this as soon as practicable so prompt action can be taken. Reporting this information can also help the regulator to identify and track any patterns of third-party interference.

Examples of these include:

- hacking attempts potentially indicating involvement of a coordinated group across state and territory lines
- patterns of particular interference indicating that owners or operators are not sufficiently informed or aware of what works they may perform on a vehicle with an ADS.

An ADSE will be required to notify the regulator of any detected third-party interference attempts made on its ADS, including the range of deliberate or unintentional actions as described above.

The regulator may notify state and territory law enforcement of the third-party interference attempt where it relates to third-party interference offences in state and territory law. Commonwealth law enforcement agencies may also be notified where the third-party interference attempt relates to offences in Commonwealth law.