NCC Group response to the NTC Regulation Impact Statement:

In-service safety for automated vehicles

About NCC Group

NCC Group is a global expert in cyber security and risk mitigation, working with businesses to protect their brand, value and reputation against the ever-evolving threat landscape.

Through an unrivalled suite of services, we provide organisations with peace of mind that their most important assets are protected, available and operating as they should be at all times.

With our knowledge, experience and global footprint, we are best placed to help businesses identify, assess, mitigate & respond to the risks they face.

We are passionate about making the Internet safer and revolutionising the way in which organisations think about cyber security.

Headquartered in Manchester, UK, with over 35 offices across the world, NCC Group employs more than 2000 people and is a trusted advisor to 15,000 clients worldwide.

Prepared by:

Dean Hardcastle, APAC Automotive Assurance Practice Lead

Anthony Caulfield, APAC Transport Assurance Practice Lead

Level 13, 92 Pitt Street

Sydney, NSW 2000, Australia

Phone: +61 2 9552 4451

Website: www.nccgroup.com

NTC Consultation Questions

NTC Q1. Have we correctly identified the parties with an influence on the in-service safety of automated vehicles and accurately described their role? If you identify additional parties, please explain what their role is.

NCC Group Response:

Does section “4.5.10 Component (not ADS) manufacturers” include aftermarket third-party device manufacturers or distributors, such as insurance companies distributing on-board diagnostics (ODB) devices to customers?

Given the more widespread of use "black boxes" and other driver monitoring devices, these should be considered an influencing factor. The additional attack surface exposed by third party devices, either issued by an insurance company or otherwise, has been shown to be vulnerable to compromise even when there has not been any end-user modification.

Although a vehicle manufacturer may have implemented a diagnostics interface with a documented specification, this does not mean that a third-party device will adhere to that specification. Since an ODB device is connected directly to the Controller Area Network (CAN) bus of a vehicle, it could have the same influence on in-service safety as any other component that was implemented with the ADS at the design stage.

NTC Q2. Have we accurately assessed each party’s influence on the in-service safety of automated vehicles? If not, please provide details.

NCC Group Response:

Does section “4.4.2 Road managers (public and private)” include law enforcement?

In the case of SAE level 3, 4 and 5 automated vehicles, law enforcement may require a means to forcibly stop, or query information from, a moving vehicle without involving a driver. This is also likely to be a consideration in instances where a driver is not able or willing to comply with an instruction to stop.

When self-certifying against the safety criteria and demonstrating compliance with “A.1.10 Cybersecurity”, are ADSE’s required to demonstrate that any technical assurance has been performed of the ADS?

For example, does the requirement to “minimise the risk of cyber-intrusion” include a specific technical validation, such as independent security testing?

NTC Q5. Do you think there are any new risks posed by second-hand ADS components, after-market modifications or the transfer of ownership of automated vehicles, which may not be adequately addressed by existing regulation designed for conventional vehicles?

NCC Group Response:

Whose responsibility is it to ensure that ADS components are compliant with the regulations when the ADS is resold, either within an entire vehicle or as individual components?

Although an ADS or component may have once met the required safety requirements, it is unclear if there is any responsibility on any specific parties to ensure that the safety requirements are still met when it is resold. Insurance companies may require this information from the new owner in order to assess the in-service safety of the ADS.

Scenario 2 of section 3.3.1 describes accidental damage to a sensor, which goes unreported by the vehicle, and results in a crash. The same could apply to a third-party after-market safety component, which does not report the fault and cannot respond to an action, such as applying the brakes. It would be difficult for someone buying a used car to know whether all of the components are genuine and operating safely if no "errors" are reported by any of the self-diagnostics the vehicle performs.

As is currently the case with conventional vehicles, an owner looking to sell a vehicle might spend as little money as possible to return the car to a minimum working state, however that does not always mean the "repairs" have actually fixed the issues. This currently comes in the form of resetting fault codes that are known to be intermittent, removing bulbs/LEDs from the instrument cluster to prevent a fault being displayed, or shorting the connection on a sensor so that it appears to be working despite getting no actual reading.

Undisclosed modifications that affect the safety of a second-hand vehicle are not a new risk. However, their impact may present new and unique safety implications for an automated vehicle.