Comments on NTC Document:

SAFETY ASSURANCE FOR AUTOMATED DRIVING SYSTEMS
CONSULTATION REGULATION IMPACT STATEMENT

Steven E. Shladover

Overall, it looks like a very thorough and well-thought-out document, synthesizing a great deal of information not only from Australia but also from other countries that have been active relative to road vehicle automation. Most of my comments are relatively minor and detailed, but I have one broader concern that is a bit more significant. Although the title of the report correctly discusses "Automated Driving Systems", there are many places in the report that get sloppy in terminology by discussing "automated vehicles". This is more than a semantic distinction, because a single automated vehicle could be equipped with multiple ADS features that operate at different levels of automation within different ODDs – to take the simplest example, a vehicle could have a Level 3 ADS for driving on major arterials, a Level 4 ADS for driving on limited-access motorways and a Level 4 automated valet parking system. Those are three different ADS features within one vehicle. The focus of attention should be on the ADS features, rather than the vehicles. See the very recent update to SAE J3016 for some more explanation of these issues at: https://saemobilus.sae.org/content/J3016_201806/

p. x (Executive Summary): "breaking" should be "braking"

p. 11 – "initial safety assurance – which involves the ADSE demonstrating compliance against a set of safety criteria for an ADS type on a case-by-case basis" -- that would be nice in theory but those criteria have not been defined yet and it is likely to be a long time before they are because of the complexity of the challenge.

p. 14, Level 4 definition – "all the time in defined places" is a bit misleading because it puts the ODD into strictly geographic terms, but the ODD restrictions also include important dimensions of weather and traffic conditions.

p. 15, Level 5 definition – "are undertaken by the ADS" is misleading. This should be "can be undertaken by the ADS" – the user could decide when to activate or deactivate the level 5 system, and could even drive the vehicle manually for some of the time if he or she so wished.

p. 18 – Don't assign too much importance to the Virginia Tech report on the crash rates of the Google test vehicles, because those vehicles were being test driven by test drivers who were very carefully selected and rigorously trained to take over control of the vehicle when there was even a small risk of a safety problem, so those represent mainly the skill of the test drivers rather than the capabilities of the systems that they were testing (for those you have to look at the California disengagement reports). Also in Footnote 11, for most of the time the Autopilot system has been available the driver was not required to keep their hands on the wheel, and the drivers who crashed using that system did not have their hands on the wheel.

Section 4.3.1 appears to be closely related to functional safety, but the term "functional safety' does not show up here. It would probably be better to make explicit reference to it.

Section 6.4 about the regulatory costs to industry skims past the largest such cost, which is the cost of doing the engineering development work to produce an ADS that will be sufficiently safe that it can pass the regulatory requirements. This is a cost that all developers should of course

be incurring if they are doing a proper system development job, but it should probably not be ignored in favor of the much smaller administrative costs that are discussed in this section.

Section A.1 Design risks – there is an important missing one, which is an incomplete set of system design requirements and specifications, meaning that the designer has failed to account for all the hazards that the ADS will encounter in the real world. The malfunction item in the first bullet item is too broad and vague.

p. 85 – The reference to the Swedish paper is not convincing. The authors have made naïve assumptions about the level of capability of the ADS designs that will not be achievable in practice. Also on this page, don't follow the mistake that NHTSA made when they eliminated the ethics item that was in the first version of their policy statement. The second generation statement was badly watered down compared to the far more well-conceived first statement.

Section C.3.1 Data recording and sharing – There is going to be a need to specify a minimum set of data elements and minimum sampling rates for those data elements to go into the data recording. Eventually there will industry standards to cover this, but those will take time to develop and it will probably be useful to have some placeholder requirements defined until those standards are available.

P. 90 – Privacy – Again, do not follow the mistake that NHTSA made in eliminating the requirement that was in their first policy statement, which was much better than the later version. In this case they just ducked the issue because they said it belonged to a different agency of the U.S. government. See the California requirement protecting the privacy of ADS users, and especially the requirement that any sharing of non-safety-critical data be subject to the user opting in.

p. 106, final sentence – There WILL BE vehicle automation risks ("may be" is far too weak a statement)

The Figure 7 timeline of claimed release dates needs to be taken with a huge grain of salt because there is no indication of the severe ODD restrictions that will apply to all of these systems (and the Tesla claim of level 5 is nothing more than science fiction – it was only a few months ago that Musk finally admitted that his "Autopilot" is only a Level 2 driver assistance system).

p. 115 – lidars are already available for much less than $75,000 and those costs keep coming down.