Public Comment on Federal Automated Vehicles Policy Document

Docket Number NHTSA-2016-0090

Summary

I discuss the need for NHTSA to mandate specific performance standards for operation in fault-free state and in cases where systems have reconfigured to deal with fault conditions.

I also raise four other issues: psychological perceptions of safety; need for unified approach to solutions for the Trolley Problem; need for guidance on vehicle condition with respect to its effect on system performance, and need for coordinated policies to resolve unstructured or deadlock scenarios. All of these issues require NHTSA to provide further guidance.

Discussion

While the potential safety benefits of increased automation are highlighted and stated in a qualitative way in the document, it is essential that actual benefits are realized. There are system engineering issues that must be recognized and the necessary additional guidance provided:

> **Put simply, crudely and at its most basic, the issue is how many people these vehicles will be allowed/designed to kill.**

There are two important aspects to this – fault free performance, and performance with faults:

1. Fault-Free Performance

Among human drivers there is a competency or performance gradation, ranging from highly engaged/competent/experienced/expert, down to highly impaired/inattentive/inexperienced/unskilled. A similar performance scale can be visualized for Highly Automated Vehicles. The realized benefits of highly automated vehicles depend on where in this gradation the actual performance of the vehicle falls, and that in turn principally depends on what level of competency the specific design aims for.

We may reasonably assume that there will be rather small realized benefits in death reduction/injury reduction/vehicle damage and property damage reduction if the performance level of the automation only rises to the level of an "average" human driver.[1] [2] I therefore contend that the standard must be higher, and of course the higher the better.

However I foresee a problem specifying an overall performance standard for self driving vehicles because their ultimate performance is the combination of many functions. The well-proven traditional way would be to specify performance targets on a function-by-function basis.

---

[1] The benefits accrue only when the automation prevents an accident that a particular (inattentive, etc.) driver would have had if the automation had not been engaged.

[2] Also, the self driving vehicles will some of the time be carrying the otherwise high functioning drivers, so the balance of users in the road system may change.

Consider for a somewhat simple example the increasingly popular collision prevention function of modern cruise controls. Clearly these perform better than inattentive, impaired and distracted drivers, but do they reach the standard (i.e. prevent as many collisions) as a highly engaged, short reaction time driver? Should they? Or are they only as good as an average driver? What operational regimes (e.g. weather) do they function in? Do they have false operations that increase risk in other areas (e.g. rear end collisions with the equipped vehicle)? Perhaps the individual manufacturers have design performance criteria (and performance test evidence) and have some idea of the answers, but I am pretty sure that NHTSA does not, and neither do we, the users of this function (although I do recall that Consumer Reports has performed some basic functional tests).

For self driving vehicles these questions are the same but the answers are much harder to determine, because the "function" of driving itself is so complex. Perhaps every sub-function can be defined and performance standards specified? The Policy is mute on this issue as far as I can tell, so guidance as to what the answers ought to be needs to be added.

When I question my own experiential point of reference and ask "How does the FAA (NHTSA's sister Administration) handle these questions?" the answers are in the performance requirements in the Federal Airworthiness Regulations (FARs). As I have commented before, NHTSA is so far behind FAA in this area it is hard to see how it can catch up. However there should at least be some evidence in the Policy that the problem has even been recognized.

I note that – as I have previously advocated – NHTSA did look at FAA's pre-entry-to-service process, mentions the Agency man-hours involved and the use of Designated Engineering Representatives within the manufacturers' organizations. But it states no conclusions and without further discussion adopts self-certification as its policy.

It is clear to me that performance standards are essential and they cannot be left to the discretion and often cynical cost vs. benefit calculations of the vehicle manufacturers. Self-certification may (perhaps) be made to work, but only if what is being certified is conformance to an explicit standard.

2. Performance with Faults

The Policy does recognize that guidance is needed in this respect, using the somewhat obscure phrase "fall back minimal risk condition", but covers it in insufficient depth. What is missing is a target for the probability of occurrence of (performance degradation resulting from) a given failure state resulting in a specific hazardous situation.

Once again I look to the FARs and Advisory Circulars and find the topic covered (e.g. FAR 25.1309 and AC 25.1309). Top down analysis determines conditions that could occur. These are then classified as to the associated danger (Hazard) level. Probability targets are defined for each band in the range of Hazard levels ranging from minor to catastrophic[3]. Designs are defined and analyzed and equipment is developed using specified processes to meet and exceed these targets.

It may be that automotive industry standards documents cover these processes and define the probabilities to be met. Even so, I believe it is not sufficient to leave it at that. As I stated above, compliance levels cannot be left to the discretion and often cynical cost vs. benefit calculations of the vehicle manufacturers. The Policy document – or perhaps Roadworthiness Requirements documents – must specify actual targets to be met.

[3] A key aspect of policy that needs to be developed is whether "No single fault that is not extremely improbable shall lead to a catastrophe" (paraphrasing AC 25.1309-1A paragraph 5.a(1)) is a requirement for road transport, as it is for air transport. This is a fundamental, defining safety requirement that I believe should be imposed.

3. I have four further, more general, comments:

3.1 For various reasons road travel is often perceived as being less frightening than air travel, even though by any measure road travel is much more dangerous. One reason for this perception is the feeling of being in control, rather than a passive, powerless recipient of a service. I think there will be a shift towards the airline travelers' feeling when road travelers cede full control to self driving vehicles - I know there would for me. I believe it will become a defining factor in requiring NHTSA to set defined standards for self driving vehicle safety.

3.2 The Trolley Problem is alluded to in a generic way as an ethical issue in the Policy. For me, a given vehicle's policies for resolving Trolley Problem type scenarios would be an important factor in my choice of self driving vehicle. As public awareness increases I think it will become a general concern. NHTSA must lead the industry in the development of policies for rationalized resolution of Trolley Problem type scenarios across the range of vehicles.

3.3 Vehicle condition influences the performance that is actually achieved in service. I note that there is guidance on the need for configuration control of the automation's software and hardware, but, for example, for how long is a system degraded by a failure condition allowed to be on the road pending repair? And how influenced will the performance of the automation be by, for example, the state of the tires or wear and tear of the suspension?[4] I believe it will be necessary to have mandatory maintenance procedures and intervals to assure minimum in-service performance. NHTSA must add system-wide configuration control considerations to the Policy.

3.4 I have seen John Walsh's public submission questioning whether vehicles will be able to deal with unstructured – typically emergency, possibly also deadlock – situations. Since self driving vehicles will have to coordinate among themselves and with other involved entities in such situations I think NHTSA will have to define specific policies to be applied across the board to ensure satisfactory resolution of such scenarios. NHTSA must add clarification and guidance on this to the Policy document.

Submitted:

Geoff Barrance

October 12, 2016

[4] Or for that matter, wear and tear of the systems' own sensors, such as degradation of optical windows for cameras (perhaps like clouded headlight lenses, so common now).