More comments for Docket No. NHTSA-2020-0106

David Gelperin
david@clearspecs.com

What would increase the confidence of a safety engineer in ADS safety?

Answer: An **industry-wide**:

- glossary of ADS phrases e.g., definitions of “clear/obstructed view”, “erratic driving”, “near the roadway” and “defensive driving” [More terms appear on page 3] – **Unrecognized Ambiguity is very dangerous**
- inventory of hazards both to (see example below) an ADS and from an ADS (e.g., UA)
- requirements and suggestions for ADS hazard mitigations

Clear definitions of the safety challenges is in everyone’s best interest. Those who ignore some hazards or implement ineffective mitigations would likely and appropriately be punished in the courts. Unfortunately, **some innocents will die**.

All ADS software requirements should be publicly available or independently reviewed including quality attributes, basic function sets, design constraints and implementation constraints. Without skeptical reviews, such requirements are likely to be seriously flawed for many reasons.

The current non-collaborative environment is very dangerous and ignores most of what we know about human behavior.

Various forms of hazard analysis might identify the following hazards to an ADS and their combinations:

System failures

- all/some sensors fail
- classifier fails e.g., misclassifies
- effector logic fails
- platform with guidance software dies
- GPS signal lost
- software causes unintended acceleration or erratic behavior
- software enables hacking
- software fails to adapt to new environments e.g. passage from England to France or entry into school zone

Vehicle conditions

- motor dies
- tires go flat
- brakes fail
- battery fails
- vehicle catches fire
- top is sheared off
- vehicle skids (e.g., on ice)
- vehicle is submerged

Roadway conditions

- different zones e.g., school, hospital, or work
- large, heavy, stationary object (e.g., fire truck) blocking the roadway or lane
- spills, floods, fires, or heavy smoke
- ice and snow
- roadway collapses (e.g. bridge or sink hole)
- downed powerline
- kangaroo on or near roadway
- large animal on roadway e.g. moose
- large rocks, mud slide, or fallen tree
- traffic light outages
- stale yellow light

Traffic conditions

- wrong way or encroaching vehicle
- vehicle ahead/beside drives erratically
- vehicle tailgating
- traffic-obscured hazard e.g., stalled truck

Weather conditions

- heavy snow, hail, or dust storms
- heavy fog or dark moonless nights
- hurricanes or tornadoes

Hazard lists to and from an ADS can be used to guide requirements development or check the completeness of existing requirements. To guide requirements development, each hazard can be put into the following template and then refined into specific situations and responses.

If <hazard>, then the system must safely respond.

For example:
If the "motor dies" and the vehicle is stopped, then …
If the "motor dies" and the vehicle is moving and emergency parking is feasible, then …
If the "motor dies" and the vehicle is moving and emergency parking is not feasible, then …

Terminology missing from BSI Connected and automated vehicles – Vocabulary

BSI Flex 1890 v3.0:2020-10

This vocabulary seems to focus on solution terminology. **Problem terminology** is critically important as well. Most of it is missing. I'm sure I have missed some.

- Defensive driving
- Destination – only appears in a Note about what DDT is not
- Emergency stopping
- Erratic driving
- Glide path
- Near the roadway
- Obstructed/Obscured view
- Origin
- Parking lot
- Pedestrian indicator e.g., baby buggy, rolling ball
- Roadway barrier e.g., mud slide
- Roadway hazard
- Roadway user e.g., kangaroo
- Safe following
- Safe merging
- Safe parking
- Safe stopping
- Safe turning
- School/Work zone
- Tailgating
- Traffic cone
- Unintended acceleration
- Warning sign