Establishing a Standard List of Hazards for Automatic Driving

Robert C. Hammett; Draper; Cambridge, MA, USA

Keywords: Automatic Driving, Autonomous Vehicles, Safety Assessment, Hazards

Abstract

Fully automatic (self-driving) automobiles (SAE level 5 - steering wheel optional) safety assessment begins with an analysis to identify potential hazards. Examples of hazards include failure to sense an obstacle in the vehicle's path, incorrect determination of an obstacle's location or boundary box, incorrect prediction of a moving obstacle's future location, etc. These types of hazards are not unique to one system developer and establishing a standardized list would be useful for developers, safety professionals, system buyers and for legal use. The paper presents a proposed list of standard hazards and some discussion of their consequences, risks levels and mitigation's. The author believes there is value in maintaining and evolving a list of standard hazards to be used in all phases of automatic driving system design, development and verification.

Introduction

Self-driving or Autonomous Vehicles (AV) are attracting a lot of interest. Virtually all car manufactures, major technology companies and transportation companies such as GM (Hawkins, 2018), Ford, Google, Apple and Uber are making large investments towards their development. The argument is being made that that AV’s will reduce the large US fatal accident rate (40,000/year) associated with highway travel by eliminating human driver error. There are many economic benefits from driverless taxi and trucking services, improved use of commuting time, and perhaps reduced traffic congestion. The convenience of self-parking cars and cars that respond to a summons for pickup are appealing.

Can the goal of exceeding the safety levels of human drivers be exceeded? Can they be as safe as human driver? In a self-driving AV, even with an experience driver onboard with access to controls, it is unrealistic to assume that he/she can take over control should the automation fail. And since the goal is to provide robotic taxi services, self-parking cars, and to transport non-drivers, this is not even an option in those cases. The AV can’t rely upon a human back-up for safety. It must also be assumed that self-driving vehicles must share the road with human driven vehicles and with all of the usual difficulties such as weather conditions, road construction, human errors, pedestrians, and mechanical failures remain unchanged.

Designing these vehicles is very challenging. They are made possible by recent advances in electronics for high-speed computing and sensing. Success would be an extraordinary accomplishment in mobile robotics and artificial intelligence. Our proudest human accomplishments in aerospace control systems have not had to operate in chaotic environment of our streets and highways.

Summary

Operating motor vehicles on public roadways is an inherently risky activity. The potential for collisions that can cause injury and death are always present. Mil-Std-882 (Mil-Std-882E, 2012) states The objective of system safety is to achieve acceptable mishap risk through a systematic approach of hazard analysis, risk assessment, and risk management.
Developers of AVs are understandably concerned about the potential for accidents and their underlying causes. The prevention of accidents is the goal and this is accomplished by reducing exposure to hazardous operating conditions. It is easy to get lost in the details and conditions that may lead to accidents and the underlying causes can be confused with the hazards they create. The objective of this work was to identify and document a proposed list of standard hazards that can be applied to the design and safety evaluation of AV’s. The magnitude and difficulty of this task was underestimated and the goal was only partially reached. But it is believed the progress made is worth presenting and the process used of interest. The author would like to continue the effort, perhaps with collaboration from others. The effort would be informed by a detailed study of traffic laws (AAA, Digest of Motor Laws, 2018), traffic control devices (MUTCD, 2009), and established practices for student driver training (AAA, How to Drive Guide, 2013).

The original premise for the work remains unchanged. The bedrock of safety engineering such as is outlined in Mil-Std-882E (Mil-Std-882E, 2012) is identification of system hazards and, at least in public literature, it does not appear that a complete and organized list of AV hazards has been published.

In this work, a standard hazard is defined as one that is generic and not specific to a particular AV design. In fact, these hazards are generally applicable to vehicles with human drivers. Identification of standard hazards can serve to guide the process of identifying the lower level causes of these hazards with the goal of providing mitigations. Although road vehicles potentially have many types of hazards such flammable gasoline or lithium batteries, the focus here is upon AV hazards that lead to a collision mishap (accident). Collisions include impacts with other vehicles, with stationary objects including terrain, and with other moving objects such as bicycles or pedestrians. Note that a hazard does not always result in a mishap, but increases the likelihood of a mishap occurrence. For example, driving off of the road surface will only result in a collision if a roadside obstacle is in its path. Figure 1 illustrates how the identification of standard hazards, and causes for them can be used to generate a hierarchy (tree) of lower level causes, ultimately down to the root cause(s) of the hazard.
This work did not attempt to assign risk levels to the identified AV hazards. This would require assessing the probability of the cause(s) of the hazard condition and the likelihood that the hazard will lead to a mishap and the severity of the consequences. And these probabilities are influenced by external variables such as weather conditions that result in a loss of traction leading to a loss of control. The likelihood that a hazard such as a loss of control leading to a mishap depends upon the presence of obstacles that might be impacted. The severity of the consequences depend upon the speeds involved and obstacle being impacted. Loss of control could result in minor consequences or a major collision.

Developing a complete hazard hierarchy for an AV design is a challenging task. Driving is a complex task that requires years for a human driver to master. The human driver learns much about the hazards, understands their causes and is able to weigh the relative risks associated with different hazards.

**Approach to Generic Hazard Identification**

There are many possible collision hazards associated with AVs and a systematic approach is needed to identify them. The systematic approach selected for this effort was a series of use cases based upon the analogy of a student driver being introduced to new and progressively more challenging driving situations. The analogy begins with the student driver beginning his training by driving on simple and uncongested roads in clear daytime weather with only simple traffic laws and signals to obey. As the training progresses, he/she are introduced to progressively more difficult
driving situations of increased traffic and more complex roadways, more elaborate traffic laws and signals, pedestrians, bicycles, construction, nighttime, poor weather and mechanical malfunctions.

Although the student driver analogy is a useful approach, there are many specialized use cases involved in mastering the task of driving. There are many scenarios such safe driving with obstructed views, traffic rotaries, construction, urban conditions, tunnels, bridges, one-way streets, and many others that must be included for complete hazard identification.

**Use case 1 - Operate on back roads without other traffic (empty back road)**

To identify potential hazards, the starting use case is analogous to that of a student driver, leaning to negotiate hazards in the least hazardous of driving conditions, operating on empty back roads in clear weather, ideally with no other moving objects present. In this scenario, the student driver takes the wheel on the side of a quiet back road with simple signs, signals, pavement markings, and driving laws and assuming no other vehicles, pedestrians, bicycles or animals. There is some potential for stationary obstacles (parked vehicles, debris) in the roadway. The route is selected to avoid complex intersections and with clear lines of sight. The vehicle being driven is assumed to remain in good operating condition. The task is to maintain the posted speed, remain within the lane boundaries (usually centered), avoid any stationary objects, stop at intersections with stop signs and make turns at intersections. Intersection hazards and associated traffic law observance only become safety concerns when other traffic is introduced, but should become habit for the student driver. Similarly, turning lane pathes through intersections only become important when other vehicles are making turns in the same intersection but the student should develop good habits. Regardless of posted speeds, the vehicle must be operated at speeds safe for making turns and without loss of traction that could lead to a loss of control. Assuming no other traffic, the proposed standard hazards are: departure from road surface, departure from travel/turning lane, fail to avoid stationary objects in roadway, fail to obey traffic signs, fail to observe intersection traffic laws, exceeding vehicle performance limits (traction, stopping distance, cornering), not become a slow/stopped road obstacle.

And although task at hand is hazard identification, it is noted that perhaps the most severe hazard consequence in this situation might be departure from travel/turning lane where the roadway centerline is crossed with the potential for a head on collision with other vehicles. Yet to avoid the hazard fail to avoid stationary objects in roadway, it may become necessary to temporarily cross the roadway centerline to avoid another vehicle stopped and partially blocking the travel lane. So in some cases, it may become necessary to increase exposure to one hazard to avoid another.

Once the student becomes proficient on the back roads, more complex roads (again without other traffic) can be attempted. More complex roads introduce more complex intersections with traffic lights, multiple lanes and multiple lane markings. The additional standard hazards include fail to obey traffic signals and fail to obey lane markings. Table 1 summarizes the hazards that were identified from the first student driver use case.

<table>
<thead>
<tr>
<th>Table 1 — Empty Back Road Hazards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Departure from road surface</td>
</tr>
<tr>
<td>Departure from travel/turning lane</td>
</tr>
<tr>
<td>Fail to avoid stationary objects in roadway</td>
</tr>
<tr>
<td>Fail to obey traffic signs</td>
</tr>
</tbody>
</table>
Fail to observe intersection traffic laws
Exceeding vehicle performance limits
Do not become a slow/stopped road obstacle
Fail to obey traffic signals
Fail to obey lane markings

**Use case 2 - Include other vehicles on back roads in clear weather** (back road with other traffic)

As the student driver becomes more adept at the basic tasks of lane keeping, speed control and responding to intersection markings, the difficulty level (hazard potential) can be increased by including other vehicles being operated by (hopefully) responsible drivers driving in a safe and predictable manor.

The added tasks of operating on back roads with other vehicles include maintaining a safe following distance, stopping behind stopped vehicles (at intersections or other reasons), maintaining a safe distance from vehicles entering or exiting the roadway, negotiating with other vehicles at intersections (includes signaling intent) and overtaking slow moving vehicles. An added task is to recognize and negotiate unmarked intersections (no stop sign or signal). These added tasks generate additional proposed standard hazards: *failure to maintain safe separation distance from other vehicles, failure to stop for other vehicles, failure to yield to other vehicles, improper passing, fail to signal for turns, fail to follow intersection rules of the road*.

<table>
<thead>
<tr>
<th>Table 2 — Back road with other traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure to maintain safe separation distance from other vehicles</td>
</tr>
<tr>
<td>Failure to stop for other vehicles</td>
</tr>
<tr>
<td>Failure to yield to other vehicles</td>
</tr>
<tr>
<td>Improper passing</td>
</tr>
<tr>
<td>Fail to signal for turn</td>
</tr>
<tr>
<td>Fail to follow intersection rules of the road</td>
</tr>
</tbody>
</table>

Each of these standard hazards has a rich set of casual conditions. The identification of the hazard provides the framework for the task of elaborating these.

**Use case 3 - Include pedestrians, bicycles and animals on back roads in clear weather**

The inclusion of Pedestrians, Bicycles and Animals (PBA) adds new hazards to the back road scenario. Other vehicles such as cars and motorcycles are subject to motor vehicle laws and in general will behave in predictable manor. Pedestrians, bicycles and animals may not be as predictable and it is the task of the student driver to learn how to safely interact. In some cases, such as pedestrians crossing the road in a crosswalk, the driver is required to stop and wait for pedestrians to cross. In other settings not involving a crosswalk or pedestrians, it may still be safest to stop and wait for the object to move safely away. But this is often impractical and introduces new hazards if the vehicle becoming a stationary obstacle hazard to other vehicles. An appropriate action can become a very nuanced task that requires understanding the potential motions of these non-vehicle moving objects and predicting the intended motion. Potential
motions can include consideration of age (old people or children), disabilities (a white cane) and animal behavior (turkeys take their time, squirrels dart about randomly). Consequences vary. Hitting a squirrel is sad. Hitting a person is may be manslaughter crime. Once the motion is predicted, a plan to maximize the safe separation distance must be developed and executed. During execution of this plan, actual motion of the object is observed and if necessary a new prediction and plan developed and executed. The hazards become: failure to properly predict motion of pedestrians, bicycles and animals, failure to maintain safe separation from pedestrians, bicycles and animals.

**Operate in darkness or adverse weather**

The introduction of darkness or adverse weather impact visibility. Adverse weather can also impact vehicle performance by reducing road surface friction. Darkness and adverse weather will also impact the behavior and performance of other nearby vehicles. Although these elements elevate the risk associate with previously identified hazards, they do not generate new hazards. Arguably, the risk associated with operating too fast for the vehicle to safely stop is covered under a standard hazard such as failure to stop for other vehicles and is introduced in the casual factors for the standard hazard.

**Operate on hazardous roadways**

The design of the roadway can increase the risk of the previously established standard hazards, can contribute the causal factors for these hazards and can introduce unique standard hazards. For example, a roadway without a safe roadside buffer region will increase the severity of a depart road surface incident. The lack of clearly painted road edge lane marking can be a casual factor in a depart road surface incident. The addition of one-way streets introduces a new standard hazard wrong direction of travel. Road design features such as obstructed views, traffic rotaries, tunnels, bridges, and ferry boats all will introduce. Inadequate or confusing road signs and signals will also introduce new hazards.

**Future Work**

The limited number of use cases examined by this work and presented in this paper are inadequate to produce a comprehensive list of standard hazards. The author acknowledges that there is much more work to be done. A detailed investigation of driver training approaches, traffic laws, highway design standards and traffic control devices would all help inform developing a comprehensive list of hazards. It is also apparent that once a comprehensive list of hazards is developed, there is also a large effort to identify potential causes for these hazard to exist. Some of these causes will be generic to all AV’s while others will be specific to an AV’s design. It is at this level of detail that the design can include hazard mitigations to reduce the probability of occurrence. For example, if fog or dust obscuring the view of a visual sensor results in various hazards associated with not seeing, localizing or identifying objects, perhaps an additional RADAR sensor can mitigate the hazard(s).

Finally, determine if the risks have been adequately mitigated, the risk levels must be at least approximately quantified. The overall goal is to develop systems that once placed in service will result in a decrease in annual highway fatalities and other accident statistics.
References

Hawkins, A. J. (2018, January 12). Retrieved from The Verge:


AAA. (2013). HOW TO DRIVE INSTRUCTOR GUIDE.