Minimal Risk Condition Behaviors based on Environmental and Vehicle Conditions

Introduction

By definition, a Minimal Risk Condition (MRC) is a condition to which a user or an Automated Driving System (ADS) may bring a vehicle to after performing the dynamic driving task (DDT) fallback in order to reduce the risk of a crash when a given trip cannot or should not be completed (SAE J3016).

While this definition provides a general description of MRC, it does not define acceptance criteria for any particular MRC in a given fallback situation.

In general, the MRC can be binned to two broad categories:

- A "park vehicle" category where the ADS cannot sufficiently perform the DDT to complete the current trip but has enough DDT operability (steering, braking, propulsion, and Object Event Detection and Response (OEDR) capability) to exit from a driving lane and park the vehicle.

- A "stop-in-path" category where the ADS is unable to complete the trip, or "park the vehicle" outside of an active driving lane, but the ADS does maintain the ability to implement a controlled stop in its present travel path or lane. Reasons why the ADS is unable to complete the trip could be due to vehicle or environmental conditions (e.g., road flooding, a broken axle).

Figure 1 depicts the possible outcomes if ADS nominal operation is interrupted. Note that a "stop-in-path" can result either from ADS fallback and MRC achievement, or from a failure mitigation strategy in the event the ADS has been incapacitated (e.g., loss of backup power to the ADS after initial power failure or incapacitation of the ADS's computing capability) and is thus unable to achieve an MRC.[1]

[1] For a more complete description of the difference between MRC and failure mitigation strategy, please refer to section 8.6 of SAE J3016 (June 2018).

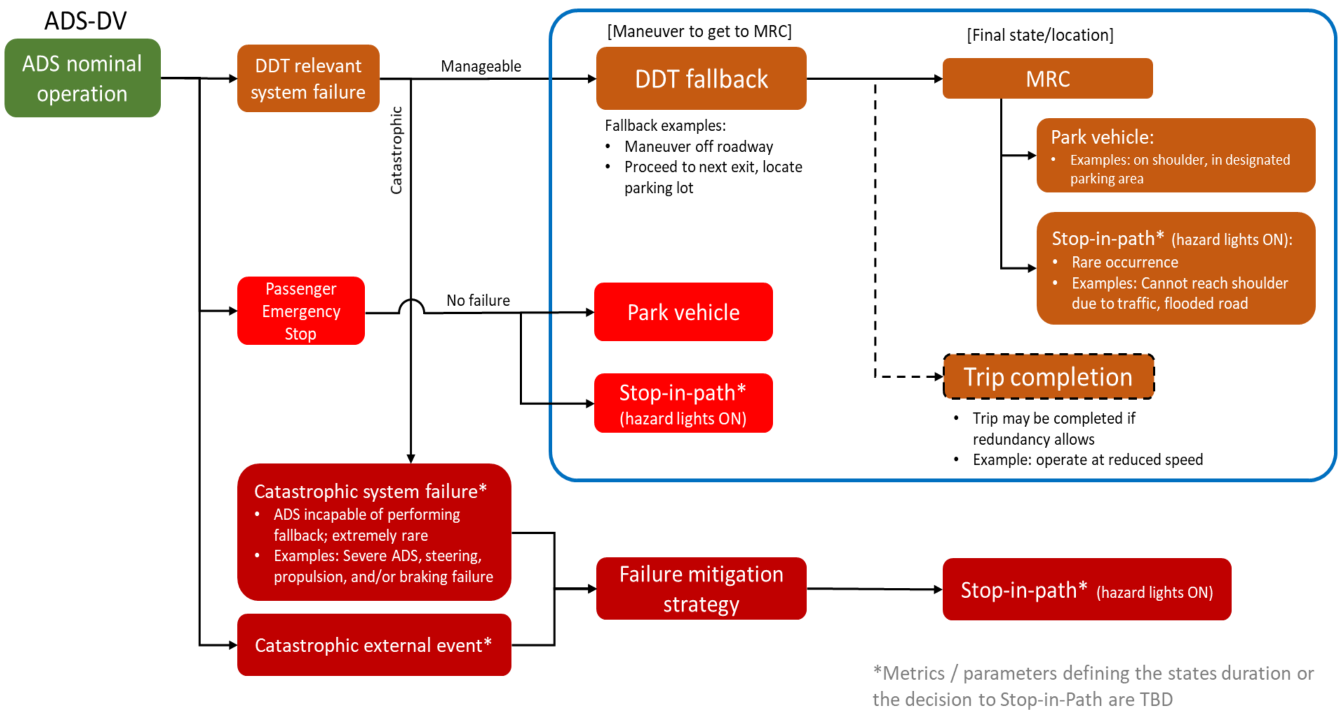

Figure 1: ADS Actions for DDT System Failures or a Passenger Emergency Stop

Figure 1 illustrates that, in some cases, occurrence of certain DDT relevant system failures may still result in trip completion (possibly at a lower speed or only on certain road types) due to redundant system features. When this is not the case, the ADS should execute a “park vehicle” procedure. However, a “stop-in-path” MRC under some conditions may be the appropriate or the only available course of action and must be considered.

For the purpose of this report, we will concentrate on the conditions where a “stop-in-path” MRC is the appropriate or the only available outcome, given a DDT performance-relevant system failure (ADS or vehicle), or given environmental factors that do not allow the current trip to continue.

Sample conditions where an MRC or failure mitigation strategy action of stop-in-path is either the preferred action, or the only possible action, given the circumstances.

1 Traffic-related Conditions - Heavy, Slow-moving Traffic

There may be situations where an Automated Driving System-Dedicated Vehicle (ADS-DV) encounters a DDT-relevant system failure but is unable to perform a "park vehicle" fallback and reach the associated MRC state of being parked out of an active lane of traffic due to traffic or other road conditions around the vehicle. For example, stop-and-go traffic may prevent the ADS-DV from reaching the side of the road before it exhausts its reserve electrical power storage (in the case of a primary power system failure).

This situation is depicted in Figure 2.

2 Certain ADS and/or Vehicle Failure Types (Catastrophic System Failures)

There are certain, albeit rare, types of ADS and/or vehicle failures where an MRC or failure mitigation strategy of "stop in path" may be either the safest action to employ, or the only option available, given incapacitation of the ADS. An exemplar list of such conditions is provided below:

2.1 Severe mechanical failure (e.g., broken axle). Control issues that prevent the sustained lateral and longitudinal vehicle motion control aspects of the DDT in order to achieve a "park vehicle" MRC or a "degraded mode condition." The result being a MRC; ADS commands controlled stop-in-path.

2.2 A vehicle motion control actuator fails to successfully execute its given command (after having used any failure countermeasures). The result being a MRC; ADS commands controlled stop-in-path.

2.3 Large-scale sensor/data conflict (several redundant sensors reporting conflicting information). The result being an MRC; ADS commands controlled stop-in-place.

2.4 Simultaneous loss of functionality for multiple sensors caused by rare environmental events (e.g., insect swarm). The result being a failure mitigation strategy of stop-in-path. ADS functionality is incapacitated and stop-in-path is better than allowing the vehicle to exhaust its momentum and possibly collide with another object.

2.5 Cybersecurity watchdog detects attack without known preventable countermeasure. The result being a failure mitigation strategy of stop-in-path. ADS is incapacitated and stop-in-path is better than allowing the vehicle to exhaust its momentum and possibly collide with another object.

2.6 Failure (or exhaustion) of redundant power source following failure of primary power source. The result being a failure mitigation strategy of stop-in-path. ADS functionality is incapacitated and stop-in-path is better than allowing the vehicle to exhaust its momentum and possibly collide with another object.

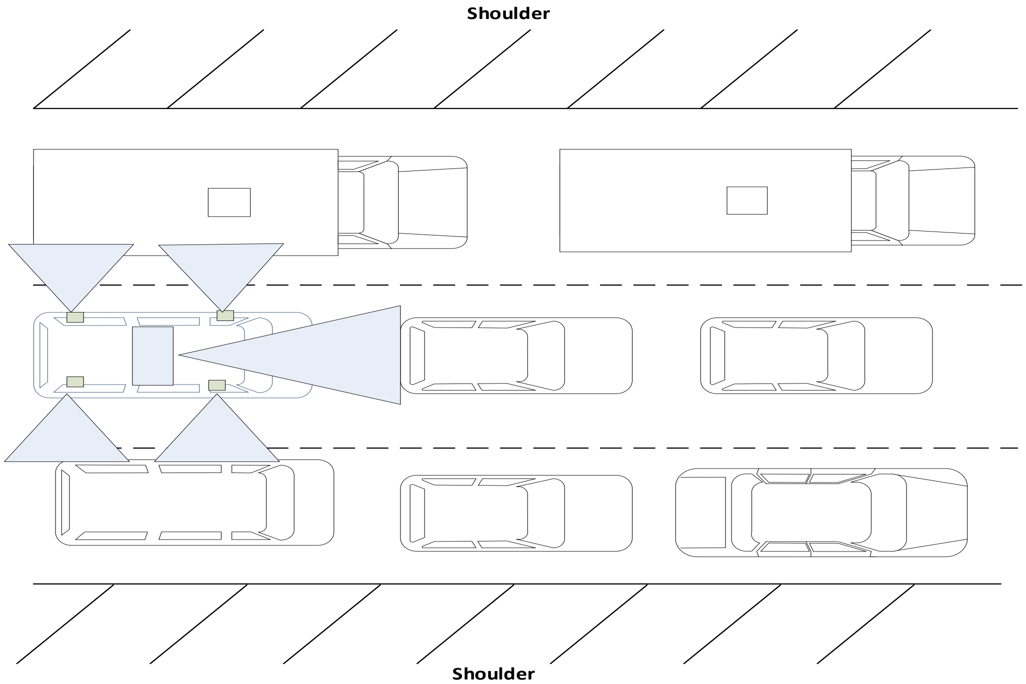

Figure 2: ADS Vehicle Experiences a Critical Failure while in Heavy Traffic

3 First Responder Motivations

As depicted in Figure 3, the ADS-DV could be involved in an accident and is no longer able to move out of traffic due to the damage it sustained.

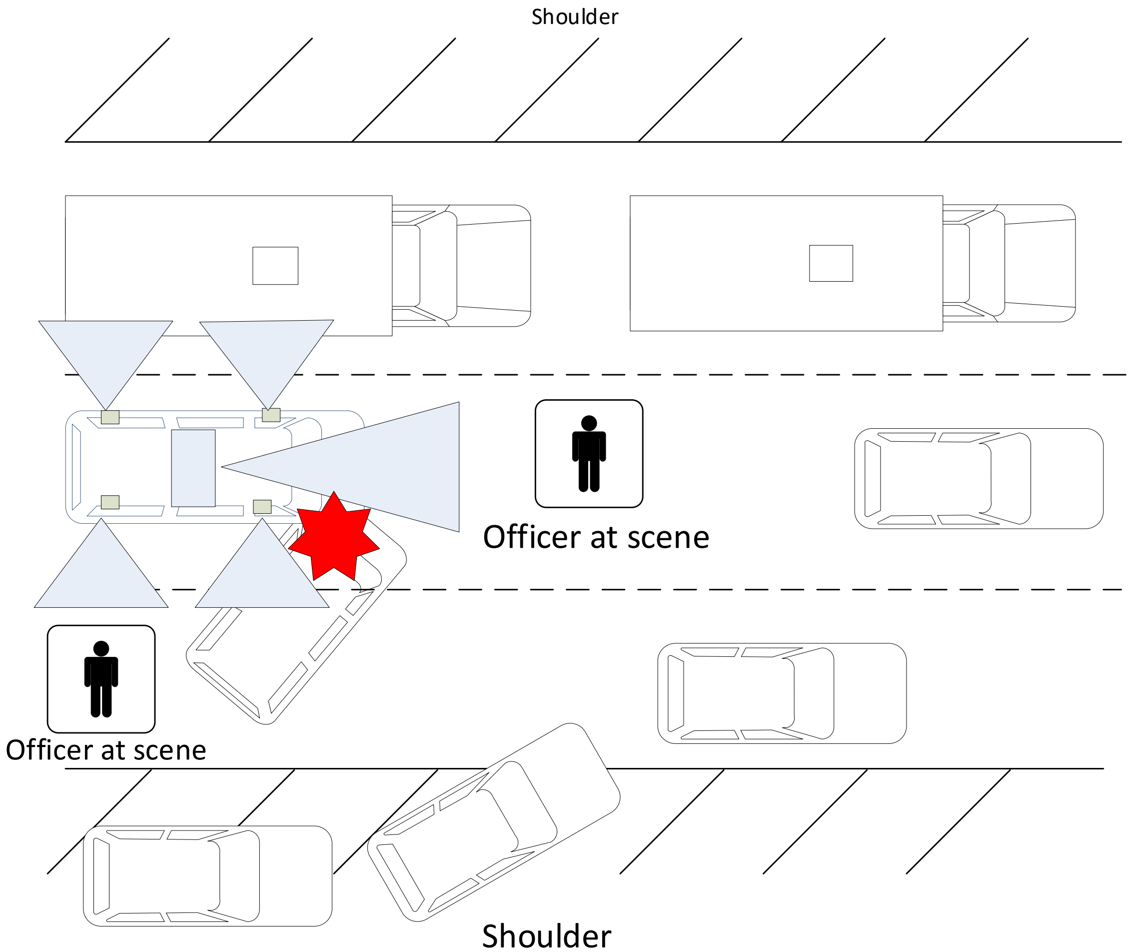

Figure 3: ADS-equipped Vehicle Involved in a Traffic Accident

4 Environmental / Out-of- Operational Design Domain Condition Occurs

There are environmental conditions that could prompt an out-of-Operational Design Domain (ODD) condition that would necessitate an MRC "stop in path" procedure. A non-exhaustive list of these conditions is as follows:

4.1 Extreme Weather Conditions
- 4.1.1 Sudden heavy snow/white-out conditions
- 4.1.2 Extremely heavy rain/monsoon

4.2 Road Impassable (bridge out, sinkhole, tree blockage, etc.)
- 4.2.1 Road is blocked, and road shoulder is unavailable or blocked
- 4.2.2 Flooded road

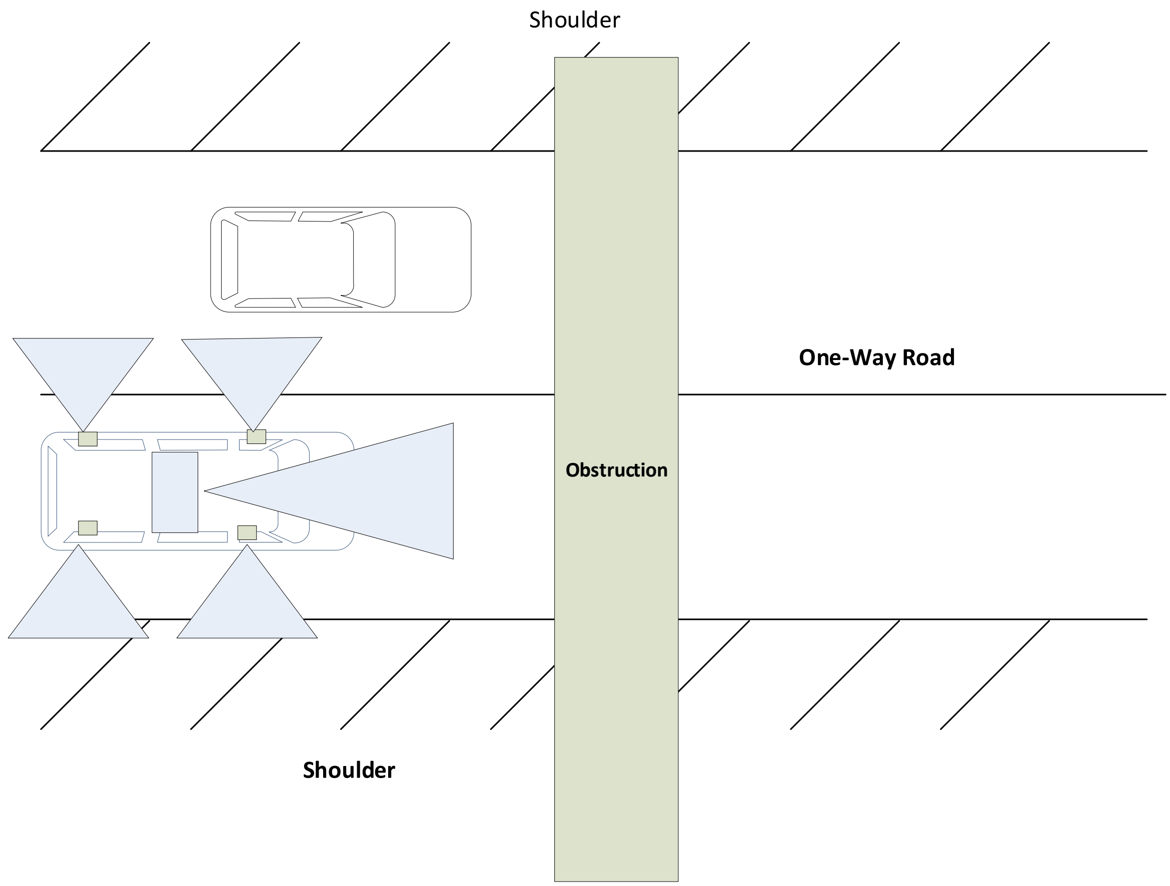

Figure 4: ADS Encounters an Obstruction

As depicted in Figure 4, the ADS could encounter an out-of-ODD condition that prohibits further movement on the path. In which case, the best course of action would be to stop in path and wait for the obstruction to be cleared or wait for a fleet operator to address the situation.

5 Passenger-initiated Emergency Stop (PES)

While riding in an ADS-DV [2] dispatched by a commercial enterprise that offers a ride hailing service for a fee, a passenger may activate a Passenger-initiated Emergency Stop (if available) due to a perceived hazardous situation that they believe necessitates an immediate stopping of the vehicle, such as fire in the cabin, threat of passenger-on-passenger violence, or an external hazardous event/threat. Please note that automated stopping due to a PES activation is not considered "fallback performance." Therefore, the resultant stop does not constitute a MRC or a failure mitigation strategy as defined in SAE J3016 (June 2018).

6 Summary and Next Steps

Given a DDT relevant system failure that prevents trip completion, the preferred action of an ADS is to perform a "park vehicle" procedure resulting in the ADS-DV reaching an MRC outside of an active lane of traffic. However, a "stop-in-path" MRC under the conditions outlined in sections 1 through 5 must be considered as a valid MRC state.

With this in mind, the standards development community should develop acceptance criteria regarding when to transition to "stop-in-path" after unsuccessfully attempting a "park vehicle" MRC procedure. In the future, the ADS community may agree on a standardized test framework to verify safe functionality in the presence of a DDT relevant system failure.

Given that a "stop-in-path" could be necessary in the event of a DDT-relevant system failure, designs should ensure that all ADS-equipped vehicles maintain the ability (from an ADS sensing and ADS sustained lateral and longitudinal control standpoint) to enact a controlled stop at all times during fallback performance and during failure mitigation strategy execution.

Designs should also ensure that ADS-equipped vehicles maintain the ability to perform a controlled stop-in-path at all points of operation within the ODD if, while attempting to complete the trip or to reach a "park vehicle" MRC, the operating conditions change to where these actions cannot be successfully implemented (e.g., the road floods or the ADS-DV comes under cyber-attack). As an example, if the ADS-DV is capable of speeds on the order of 120 kph, it should maintain sufficient power to decelerate the vehicle to a controlled complete stop. It is expected that when the vehicle comes to a controlled stop, there should be a "standstill management" strategy to keep the vehicle stationary that is not dependent on the ADS-DV maintaining power.

[2] ADS-DV is defined in SAE J3016 (June 2018) as "A vehicle designed to be operated exclusively by a level 4 or level 5 ADS for all trips within its given ODD limitations (if any)."