OPERATIONAL DESIGN DOMAIN (ODD) FRAMEWORK FOR DRIVER-AUTOMATION SYSTEMS

HongSeok Cho and R. John Hansman

Project Final Report for Ford-MIT Alliance Project: Understanding Driver’s Trust in Automation and Its Impact on Driver’s Decisions and System Safety

This report is based on the Thesis of HongSeok Cho submitted to the Department of Aeronautics and Astronautics in partial fulfillment of the requirements for the degree of Engineer in Aeronautics and Astronautics (EAA) at the Massachusetts Institute of Technology

Report No. ICAT-2020-10
December 2020

MIT International Center for Air Transportation (ICAT)
Department of Aeronautics & Astronautics
Massachusetts Institute of Technology
Cambridge, MA 02139 USA
Operational Design Domain (ODD) Framework for Driver-Automation Systems

By HongSeok Cho and R. John Hansman

Executive Summary

Current driving automation systems have technical limitations which restrict their capability based on operating conditions. This is recognized in the SAE levels of automation which uses the concept of the Operational Design Domain (ODD) to define the conditions under which a given driving automation system is designed to function. There is not yet a clear standard and a systematic process to evaluate an automation system in order to determine its ODD. In addition, inappropriate use of the automation outside the ODD has been a major cause of accidents related to driving automation systems. This project investigated a risk based approach to defining the ODD. The project also evaluated approaches to assuring driving automation systems are used within the ODD through automated or human ODD management.

![Figure 1: Risk-based ODD Transform](image)

A risk-based framework was developed, to define the ODD in a conditional hyperspace in terms of risk related to an automation system’s failure to perform its intended function. In the framework shown in Figure 1. The automation system is evaluated to identify potential unreliable behaviors of the automation system and a preliminary hazard analysis is conducted to identify potential resulting hazards. The impact of external conditions on both the reliability of the
automation system and the consequences of unreliable behavior are evaluated. The area of acceptable level of risk in a traditional risk matrix can be transformed to an acceptable volume in the ODD hyperspace for each identified hazard. The overall system ODD is the union of the acceptable volumes in the ODD hyperspace.

Figure 2: ODD Management

Once an ODD is determined for a driving automation system, it should be adequately managed so that the use of the automation outside the ODD is avoided. The key role of ODD management is to observe available information and assess whether the observed conditions are inside or outside the ODD. This role may be performed automatically by the system (for SAE Level 3 or 4 systems) or performed by the human operator (for SAE Level 1 or 2 systems) as shown in Figure 2 above.

An analysis of recent accidents involving driving automation system’s failures to perform its intended function was conducted to investigate how failures in ODD management by drivers. A model was developed and used to identify potential failure modes of human ODD management. These include: 1) perception failure, 2) comprehension failure, and 3) projection failure. Based on the findings, a set of recommendations for improving the driver-automation systems that would support to improve the ODD management are suggested.
Acknowledgements

This research would not have been possible without funding from the Ford Motor Company.
[Page Intentionally Left Blank]
Outline

1. Introduction and Objectives ................................................................. 11
   1.1. Research Motivation and Objectives ............................................ 11
   1.2. Report Overview ................................................................. 15

2. Risk-based ODD Determination Methodology ........................................ 17
   2.1. Past Studies on the ODD Definition ............................................ 17
   2.2. ODD Conditional Hyperspace .................................................... 19
       2.2.1. Hyperspace Dimension Determination .................................... 20
       2.2.2. Risk-based Threshold Determination .................................... 21
   2.3. Risk-Based ODD Determination Process ...................................... 22
       2.3.1. Preliminary Hazard Identification ....................................... 23
       2.3.2. Modeling of the Relevant Events ....................................... 24
       2.3.3. Hazard Evaluation (Conditional Risk Assessment) ................. 26
       2.3.4. ODD Determination ........................................................ 27
   2.4. Example Application of the Methodology ..................................... 28
       2.4.1. System description .......................................................... 28
       2.4.2. Preliminary Hazard Identification ....................................... 29
       2.4.3. Modeling of the Relevant Events ....................................... 31
       2.4.4. Hazard Evaluation (Conditional Risk Assessment) ................. 34

3. ODD Management ............................................................................ 39
   3.1. ODD Management Overview ..................................................... 39
       3.1.1. Automated ODD Management ......................................... 41
       3.1.2. Shared ODD Management .................................................. 42
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.3 Human ODD Management</td>
<td>43</td>
</tr>
<tr>
<td>3.2. Historical Accident Analysis</td>
<td>45</td>
</tr>
<tr>
<td>3.2.1. Analysis Overview</td>
<td>46</td>
</tr>
<tr>
<td>3.2.2. Review of the Involved Driving Automation Systems</td>
<td>47</td>
</tr>
<tr>
<td>3.2.3. Analysis Result</td>
<td>49</td>
</tr>
<tr>
<td>4.2.4. Analysis Summary</td>
<td>53</td>
</tr>
<tr>
<td>3.3. Human ODD Management</td>
<td>54</td>
</tr>
<tr>
<td>3.4. Human ODD Management Failures</td>
<td>56</td>
</tr>
<tr>
<td>3.4.1. Not Observable ODD Violation: Failure of Perception</td>
<td>57</td>
</tr>
<tr>
<td>3.4.2. Ignored ODD Violation: Failure of Comprehension</td>
<td>59</td>
</tr>
<tr>
<td>3.4.3. Not Observed ODD Violation: Failure of Projection</td>
<td>61</td>
</tr>
<tr>
<td>4. Recommendation to Support Improved ODD Management</td>
<td>65</td>
</tr>
<tr>
<td>5. Summary and Conclusion</td>
<td>73</td>
</tr>
<tr>
<td>Reference</td>
<td>77</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction and Objectives

1.1 Research Motivation and Objectives

Driving automation systems expect to provide various benefits including increased safety and efficiency and a reduction of driver workload (Kalra, 2017). There is a great interest in developing automation systems that would perform various driving related \textit{intended functions} including longitudinal, lateral control of the vehicle and responding to specific driving event/situation or obstacles.

In order to achieve the potential benefit of the driving automation systems the automation needs to be sufficiently reliable to perform the intended driving functions in order to be trusted by the driver and be acceptably safe. However, most current driving automation systems have technical limitations which restrict their reliability to perform in certain conditions. For example, a vision-based obstacle detection system becomes less reliable in dark and inclement weather conditions. Recent experiments (AAA 2019, IIHS 2018) showed a change in the reliability of
driving automation systems for driving conditions such as curves, hills and higher vehicle speed. Because the reliability can depend on driving conditions, the variable reliability of automation to perform its intended functions is defined conditional reliability in this report.

Table 1-1: SAE Levels of Driving Automation

<table>
<thead>
<tr>
<th>Level</th>
<th>Name</th>
<th>Dynamic Driving Task</th>
<th>Fallback</th>
<th>ODD</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Sustained Lateral &amp; Longitudinal Vehicle Motion Control</td>
<td>Object and Event Detection and Response</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>No Driving Automation</td>
<td>Driver</td>
<td>Driver</td>
<td>N/A</td>
</tr>
<tr>
<td>1</td>
<td>Driver Assistance</td>
<td>Driver and System</td>
<td>Driver</td>
<td>Limited</td>
</tr>
<tr>
<td>2</td>
<td>Partial Driving Automation</td>
<td>System</td>
<td>Driver</td>
<td>Limited</td>
</tr>
<tr>
<td>3</td>
<td>Conditional Driving Automation</td>
<td>System</td>
<td>Driver</td>
<td>Limited</td>
</tr>
<tr>
<td>4</td>
<td>High Driving Automation</td>
<td>System</td>
<td>System</td>
<td>Limited</td>
</tr>
<tr>
<td>5</td>
<td>Full Driving Automation</td>
<td>System</td>
<td>System</td>
<td>Unlimited</td>
</tr>
</tbody>
</table>

National Highway Traffic Safety Administration (NHTSA) adopted the Society of Automotive Engineers (SAE) levels of driving automation as a formal taxonomy for driving automation systems (NHTSA, 2017) as shown in Table 1-1. In the taxonomy, the SAE implicitly deals with the conditional reliability through a concept called the Operational Design Domain (ODD), which provides operational boundaries for the use of driving automation. The ODD is defined as “Operating conditions under which a given driving automation system or feature thereof is specifically designed to function, including, but not limited to, environmental, geographical, and time-of-day restrictions, and/or the requisite presence or absence of certain traffic or roadway characteristics.” (SAE J3016, 2018). As shown in the Table, the ODD is limited to specific driving conditions except for the level 5 category of SAE levels of driving automation, full driving...
The unlimited ODD indicates that the system can perform the driving tasks in all
driver-manageable on-road driving situations.

The ODD concept, at this point, does not have a clear standard for its definition, nor there
a systematic process to evaluate driving automation systems to determine what the ODD would be
A clear standard with a formal process will determine the ODD that would accurately capture the
technical limitations of the driving automation system and define operating conditions where the
performance of the automation is acceptably reliable.

These clearly defined acceptable operating conditions provides an approach to safely
manage the use of the driving automation system by limiting their use within the acceptable
conditions. In this report automation use can be managed by ODD management which determines
automation use based on whether the operating conditions are within the ODD. If the ODD is
correctly defined ODD management will support an acceptable level reliability of the automation
system.

At a high level, the ODD management can be represented in the feedback control model in
Figure 1-1 below. On the right is a vehicle operated by a driving automation system within a certain
driving environment. On the left is the ODD manager who is responsible for managing the ODD.
The ODD manager makes an ODD management decision regarding whether to use or do not use
the automation system. The decision is based on the feedback of information observed by the ODD
manager, which may include the states in the external environment (e.g. roadway, infrastructure,
other vehicles and objects, weather), behavior of the vehicle (e.g. acceleration, braking), and driver
feedback provided by the vehicle and the automation (e.g. vehicle speed, automation activation
status).
Figure 1-1. ODD Management Feedback Model

The ODD management role can be performed by the human driver or in some systems can be done automatically. The assignment of ODD management responsibility maps to the levels of driving automation proposed by the SAE in Table 1-1. For the SAE Level 2 driving automation systems, the systems does not have the capability to observe the ODD states and to make appropriate the ODD management decisions, therefore, the ODD management responsibility belongs on the human operator. For the SAE Level 3 and 4, the automation systems have the capability to observe critical ODD states and determine if conditions are acceptable to use the automation. When the automated ODD manager detects conditions that are not acceptable the automation in an SAE level 3 systems request the driver to intervene to end automation use. In an SAE level 4 system the driver is automatically prevented from using the automation outside the ODD.

An example of inappropriate ODD management which allowed the use of the automation in conditions outside the ODD occurred in a fatal accident on May 7, 2016 at Williston, Florida. A Tesla Model S failed to detect a crossing traffic due to technical limitations and ended up in a fatal collision. The vehicle was operating outside an access-limited highway which is outside the
ODD indicated as a do-not-use condition in the Tesla’s owner’s manual. Because this was an SAE Level 2 system, the automation did not prevent use in the “do-not-use condition”. It is unknown if the driver was aware of this do-not-use condition but this does indicate a failure of ODD management and the need to better understand the process of ODD.

To improve the definition and management of the ODD in driving automation systems this report set the following research objectives: 1) to develop a framework to define the ODD with a principled basis and a systematic methodology, and 2) to understand how drivers make decisions to use the automaton and support adequate management of ODD the automation use within the ODD.

1.2 Report Overview

Chapter 2 introduces the risk-based methodology that determines an ODD of a driving automation system. The steps of the methodology are explained in detail including hazard and relevant event identification, ODD condition identification, modeling of the events and the risk assessment. The methodology was applied to a simple example automation system in order to illustrate the use of the methodology. Chapter 3 discusses the ODD management process in detail and its implications on overall system safety. Then, recent accidents involving existing driving automation systems were analyzed to understand the types of accidents occurred and their relation to the ODD management. A human cognitive process model for ODD management was developed to understand the key processes and to identify potential causes of the ODD management failures. Based on the understanding from this model, Chapter 4 provided recommendation that would support to improve the ODD management. Chapter 5 provides a summary of the report and future work.
Chapter 2

Risk-based ODD Determination Methodology

2.1 Past Studies on ODD Definition

With the introduction of automated driving systems, there have been various studies that focused on identifying and classifying the structure and elements of the driving environment. Geyer et al (2013) proposed an ontology to provide a unified terminology for generating test and use-case catalogues for requirements. They defined and order the term ego vehicle, scenery, scene, situation, scenario, driving mission and route. Czarnecki (2017) represented this ontology using “Operational World Model” that includes operational road environment model, subject vehicle model.

Based on this ontology, Schuldt (2017) proposed a layered model to represent a driving scene, which consist of road, traffic infrastructure, temporary manipulation, object and environment, as shown in Figure 2-1. Colwell et al. suggested that models based on ontology can
be used as a reference for creating an ODD. Seppelt et al. (2017) classified the conditions and elements used to create an ODD into “static ODD” and Dynamic ODD” Static ODD is defined as the set of environmental and roadway conditions with a fixed location and/or those that can be anticipated from knowledge of a particular route. Dynamic ODD is the set of environment and roadway conditions that require on-board sensing to detect changes in state relative to vehicle position at a second-to-minute rate.

Wittmann et al (2015) used a term “functional boundary” in a similar fashion to the ODD concept. They highlighted the need for monitoring the functional boundary in order to ensure safe operation. The functional boundaries were specified in terms of five subspaces including static environment, traffic dynamics, environmental conditions, state of the subject vehicle, and passenger actions.
In summary, these past studies provide conditional categories and scientific community thought process of what an ODD should consist of. However the gap in the literature is clear - there has not been a formal method to evaluate the safety and risk associated with the conditional variables.

### 2.2 ODD Conditional Hyperspace

![Conditional Hyperspace Diagram](image)

**Figure 2-2: Illustration of the Conditional Hyperspace and the ODD Boundary**

In order to formally represent the ODD, this study defined a *conditional hyperspace* which is the space of conditions which influence the reliability of driving automation system. The ODD is then defined as the volume of the hyperspace where the reliability of the automation is acceptable. Figure 2-2 shows a simple example of the conditional hyperspace with two dimensions for illustration. The actual conditional hyperspace would have multiple dimensions with each dimensions corresponding to a specific condition that influence the reliability of the automation system. For driving automation systems that are technically limited and are only conditionally reliable, the performance of the automation system will vary within the conditional hyperspace.
The conditions within the boundary comprise the ODD of the driving automation system and the conditions that are outside the boundary are defined as the *ODD violation conditions*.

The report propose to develop a methodology to determine the ODD boundaries within the ODD hyperspace. In order to achieve this goal the method needs to: 1) determine the appropriate dimensions of the ODD conditional hyperspace in which the ODD is defined, and 2) set the thresholds that determines the boundary between the acceptable and unacceptable conditions.

### 2.2.1 Hyperspace Dimension Determination

Having the appropriate dimensions of the ODD hyperspace is critical. The dimensions need to include the most important relevant conditions that influence on automation systems’ performance of the intended function. If important dimensions of the hyperspace are missed, the ODD would fail to capture the conditions that separates the acceptable and unacceptable conditions. Therefore the formation of the hyperspace need to consider the technical limitations of the driving automation system and identify the relevant conditions that have significant influence on the automation’s conditional reliability.

In addition, the identification of the hyperspace dimensions need to consider ODD management by the human driver or the automation system. Therefore, the hyperspace dimensions used to define the ODD need to be both observable and understandable to the human or automated ODD manager.
2.2.2 Risk-based Threshold Determination

Once the dimensions of the conditional hyperspace are defined it is necessary to determine the threshold between acceptable and unacceptable conditions shown in the simple example in FIG 2-X. This report proposed a risk-based methodology to determine the thresholds of ODD acceptable use. (ISO/DIS, 2009). The risk based approach is effectively used in other safety-critical fields such as aircraft certification where it provides a principled methodology to determine the certification criteria (FAA, 2009).

The methodology assesses a level of risk associated with specific hazards that are identified for the system being analyzed. The methodology represents the level of risk associated a hazard of a system or a procedure in terms of two variables: 1) occurrence probability (likelihood) of a hazard, and 2) consequence severity of the hazard. Using these two variables, a desired threshold which determines the acceptable level of risk can be represented in a matrix format, called the risk matrix.

Figure 2-3 shows a risk matrix using the certification standard applicable for Part 23 small general aviation aircraft (ASTM 3230). These aircraft are owner operated and with passenger levels similar to automobiles so the level of societally acceptable risk are likely to be similar.

In the risk matrix, the severity levels of consequence are categorized into 5 descriptive levels in terms of adverse events’ effect on the aircraft, the occupants and the flight crew. The occurrence probabilities are categorized into 5 quantitative probability thresholds for each severity level, which are set by the certification standard. In the ASTM certification standard, there are the probability thresholds depending on the types of the aircraft and the number of passengers. Aircraft with more passengers have higher certification thresholds. The probability thresholds shown in the figure are associated with the small aircraft with less than 6 passengers, which most closely resembles the size and the capacity of automobiles.
In the risk matrix, the acceptable level of risk is indicated with green, and the unacceptable level of risk is indicated with red. This formalism is adopted to determine the boundaries that demarcate acceptable and unacceptable conditions of the driving automation systems.

**Figure 2-3: A Risk Matrix with the Aviation Certification Standard for Small Aircraft (ASTM 3230)**

<table>
<thead>
<tr>
<th>Consequence Severity</th>
<th>No effect</th>
<th>Slight reduction in capability</th>
<th>Significant reduction in capability</th>
<th>Large reduction in capability</th>
<th>Normally with hull loss</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Inconvenience</td>
<td>Physical discomfort</td>
<td>Physical distress or injury</td>
<td>Impaired performance</td>
<td>Multiple fatalities</td>
</tr>
<tr>
<td></td>
<td>No Effect</td>
<td>Slight increase in workload</td>
<td>Significant increase in workload</td>
<td>Fatal injury or incapacitation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Negligible</td>
<td>Minor</td>
<td>Major</td>
<td>Hazardous</td>
<td>Catastrophic</td>
</tr>
</tbody>
</table>

### 2.3 Risk-Based ODD Determination Process

A systematic methodology using the risk based approach described above was developed to determine the ODD of driving automation systems as shown in Figure 2-4.

The methodology consists of following steps:

1. Preliminary Hazard Identification
2. Occurrence and Consequence Modeling

3. Hazard Evaluation (Conditional Risk Assessment)

4. ODD Determination

2.3.1 Preliminary Hazard Identification

In this report, a *hazard* is defined as an unreliable behavior of the driving automation system that would result in a failure of its intended function. Once a hazard is identified for a given driving automation system based on the system definition, two types of events that are related to
the hazard are identified. Occurrence Events are defined as events that leads to the occurrence of the hazard (i.e. unreliable behavior). Consequence Events are defined as events that follows the unreliable behavior and result in adverse consequence. This sequence of occurrence event(s) – unreliable behavior (hazard) – consequence event(s) are defined as a “causal-chain.” The illustration of a causal-chain is shown in Figure 2-5 below.

Figure 2-5: Illustration of a Causal-Chain and Relevant Condition for a Hazard

Once a causal-chain is identified for a hazard, the hyperspace dimension determination process identifies the relevant conditions. The relevant conditions are derived from the known technical limitations of the driving automation system. The relevant conditions are the conditions that: 1) affect the occurrence events and influence the probability of the unreliable behavior, and/or 2) affect the consequence events and influence the severity of its consequence. Relevant condition identification is a key process of the methodology because the classes of the identified relevant conditions becomes the dimensions of the condition hyperspace where the ODD will be determined.

Because the ODD must be managed by the driver and/or the automation which is responsible for the ODD management, it is desirable for the conditions to be observable/distinguishable by the ODD manager. When certain conditions are not clearly
observable, *surrogate conditions* needs to be identified which are observable or understandable by the ODD manager. For example, if the presence of a pedestrian may not be observable sufficiently in to adequately determine automation use, then in some condition it may be possible to use road type (e.g. limited access highway) as a surrogate variable which influences the probability of a pedestrian being present. If appropriate observable or surrogate relevant conditions cannot be identified for a hazard that is itself sufficiently likely to occur than the automation system cannot be adequately managed and is not assured to be sufficiently reliable.

Another factor to consider is granularity of condition variables needed to define the ODD. For example, in the condition class of ambient light condition, simple day and night categories are less granular than daylight, dark but lighted road, dark unlighted road, dawn, and dusk categories are more granular. More granularity may make it harder to distinguish an ODD, whereas less granularity may be required to capture important condition variables influence the likelihood or consequences of a hazard.

2.3.2 Modeling of the Relevant Events

The modeling of occurrence event and consequence events can be done to identify functional relationships (e.g. mathematical function, discrete mapping, and probability distributions) between the input conditions and resulting states and associated conditional probabilities. The output of the occurrence model is relevant attributes of the unreliable behavior (e.g. impact speed) and their conditional probability. The output of the consequence model is different levels of consequence severity (e.g. injury severity) and their conditional probability.
2.3.3 Hazard Evaluation (Conditional Risk Assessment)

The output of the preliminary hazard identification process is a causal-chain including a hazard and related events, and a set of relevant conditions that may influence the occurrence probability and/or the consequence severity. In the illustrated in Figure 2-6, for a hazard $H_1$, three relevant condition classes are identified (Condition A, B, and C). The combination of the condition variables comprises sets of conditions ($C_1$, $C_2$, $C_3$, $C_4$ ...). Based on the functional relationship identified through the modeling of the events, the risk associated with different set of conditions for the hazard $H_1$ ($H_1|C_1$, $H_1|C_2$, $H_1|C_3$, $H_1|C_4$ ...) can be evaluated in terms of the probability and the consequence.

![Figure 2-6: Conditional Risk Framework (Illustration)](image)

The benefit of this framework is that the evaluated risk can be mapped into a risk matrix with a desired safety standard to assess the acceptability of the set of relevant conditions in an objective manner. In the illustration, the condition sets $C_1$ and $C_2$ has the acceptable levels of risk, whereas the condition sets $C_3$ and $C_4$ are unacceptable for the hazard $H_1$. 

26
2.3.4 ODD Determination

Based on the modeled causal-chain, the level risk associated with a set of conditions can be evaluated for the hazard. The conditional risk framework provides a clear boundary between the acceptable and unacceptable set of conditions. This operating boundary can be represented in conditional hyperspace. The relevant condition classes become the dimensions of the hyperspace, in which a set of acceptable conditions for a specific hazard can be represented as a volume in the hyperspace. As illustrated in Figure 2-7, the volume of acceptable condition for a hazard represents a sub-ODD.

![Figure 2-7: ODD Determination Process (Illustration)](image)

The conditional risk evaluation will be conducted for all identified hazards of an automation system. The sub-ODD related to each hazard are combined in order to determine the ODD of an overall system. The most restricting boundaries will dominate to form ODD boundaries.
2.4 Example Application of the Methodology

In order to demonstrate the use of the framework, the methodology was applied to a simple example driving automation system. The example system consists of a longitudinal control system (adaptive cruise control and automatic emergency braking) and a lateral motion control (automated lane keeping) system. This case study looked at the automatic emergency braking system’s forward collision avoidance function.

2.4.1 System description.

The intended function of the example driving automation system is “to detect obstacles with sufficient time/distance and avoid a forward collision by braking” as illustrate in Figure 2-8. The system uses a visual (camera) sensor and a radar sensor to detect forward objects. Once the system algorithm detects an object and classifies it as a threat which requires braking, it applies the brake to avoid a potential forward collision.

![Figure 2-8: Example System’s Forward Collision Avoidance Function](image_url)

Figure 2-8: Example System’s Forward Collision Avoidance Function
This longitudinal system has known technical limitations on the detection of a forward object. The radar sensor is limited by targets’ radar-cross-section and may perform poorly for the object with small radar-cross-section such as a pedestrian. Also, the radar sensor used for driving automation systems based on Doppler estimation can detect moving objects better than stationary objects due to high background noise. The camera sensor used to aid object detection can be affected by low visibility due to light conditions. The braking system has a fundamental limitation on its deceleration rate which depends on the road surface condition.

2.4.2 Preliminary Hazard Identification

A hazard is defined in section 2.3.1 as a failure of the intended function (i.e. unreliable behavior). In this case the intended function is “to detect obstacles with sufficient time/distance and avoid a forward collision by braking”. The identified hazard is “a failure to adequately detect obstacle.”

The occurrence events that are related to the hazard are identified. First, there is a presence of an object (threat) for which the automation needs to detect and respond. Then there is a detection event where the automation detects a forward object target as a threat. Once a threat is detected, there is a braking event where the automation applies the brake to avoid a projected collision. The consequence event that result in harmful consequence, injury, is a forward collision with the threat. The identified causal-chain is shown in Figure 2-9.

![Figure 2-9: Identified Hazard and Related Events (Causal-Chain)](image-url)
Next, relevant conditions that influence the events are identified. As discussed earlier, it is desirable that the relevant conditions are observable, because the conditions are potential dimensions of the ODD that needs to be managed. For this example, it was assumed that the human operator is responsible observing the conditions. For the object presence event, the presence of a threat object (e.g. pedestrian) is a driving condition that directly influence the outcome of the event, however the presence of a threat object is not a condition that can be observed by the human a priori. Instead, the likelihood of a presence of certain types of threat object varies depending on the road type. For example, it is more likely to experience a pedestrian threat in a city street than to experience it in a limited-access highway. Therefore the road type was chosen as a surrogate condition that influence the object presence event. Based on the assumed technical limitation of the example system, the detection distance is influenced by light conditions and threat object type. The braking event is influenced by the travel speed prior to braking and the road surface conditions which affect the friction coefficient. Since the road surface condition can be difficult to observe, the weather condition was used as a surrogate condition.

<table>
<thead>
<tr>
<th>Table 2-1: Identified Relevant Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Condition Classes</strong></td>
</tr>
</tbody>
</table>
| Road Type | • Limited-Access Highway  
• Rural Highway  
• Urban Arterials/City Street |
| Light Condition | • Day  
• Night |
| Weather Condition | • Clear  
• Precipitation |
| Prior Speed | • Velocity (Continuous) |
The granularity of each conditions are chosen so that it is clearly observable and distinguishable by the human operator. The road type was classified into 1) limited-access highways, 2) rural highways, and 3) urban arterials and city streets, which are defined based on a review (Nowakowski et al., 2015). The light condition was categorized into day and night, and the weather condition was categorized in to clear and precipitation conditions. The travel speed prior to braking was continuous variable since it can be observed through information feedback. The identified conditions and the condition variables are summarized in Table 2-1.

2.4.3 Modeling of the Relevant Events

Based on the identified hazard (unreliable behavior), related events, and associated relevant conditions in the causal-chain shown in Figure 2-9, each of the identified events was modeled by defining the relationship between the input relevant conditions and the event outputs as represented in Figure 2-10 below.

Figure 2-10: Identified Causal Chain Model of for a Hazard of the Example System

For the modeling of the object presence event, the probability of object presence was assumed for different road types as shown in Table 2-2. The target objects identified for this
analysis are a pedestrian and stationary vehicle. These were crude assumptions for the overall methodology demonstration. These probabilities may be updated with better estimations based on accident statistics or expert reviews.

For the detection event, the relationship between the detection range for the threat objects and affecting conditions (light and weather) were estimated and listed in Table 2-3. These were estimations based on the assumptions that the darkness and precipitation condition both have adverse effects on the detection distance, and pedestrian targets are harder to detect compared to stationary vehicle targets.

Table 2-2: Assumed Occurrence Rate of Object Presence for Different Road Types

<table>
<thead>
<tr>
<th>Road Type</th>
<th>Object Type</th>
<th>Pedestrian</th>
<th>Stationary Vehicle</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limited-Access Highway</td>
<td></td>
<td>Every 10,000 hr. (1X10^4)</td>
<td>Every 10 hr. (1X10^-1)</td>
</tr>
<tr>
<td>Rural Highway</td>
<td></td>
<td>Every 1,000 hr. (1X10^3)</td>
<td>Every 10 Hr. (1X10^-1)</td>
</tr>
<tr>
<td>City Streets</td>
<td></td>
<td>Every 10 hr. (1X10^-1)</td>
<td>Every hour. (1)</td>
</tr>
</tbody>
</table>

Table 2-3: Assumed Detection Distance for Different Obstacle Types, Weather and Light Conditions

<table>
<thead>
<tr>
<th>Weather Condition</th>
<th>Light Condition</th>
<th>Pedestrian</th>
<th>Night</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear</td>
<td>Day</td>
<td>200 ft.</td>
<td>100 ft.</td>
</tr>
<tr>
<td></td>
<td>Night</td>
<td>100 ft.</td>
<td>50 ft.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Weather Condition</th>
<th>Light Condition</th>
<th>Day</th>
<th>Night</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear</td>
<td>Day</td>
<td>400 ft.</td>
<td>200 ft.</td>
</tr>
<tr>
<td></td>
<td>Night</td>
<td>200 ft.</td>
<td>100 ft.</td>
</tr>
</tbody>
</table>

The braking event was modeled with a simple kinematic equation of velocity which calculates a final speed based on the prior speed, brake initiation distance from the target (detection
distance) and deceleration rates. The deceleration rate was assumed to be a constant that is influenced by the weather condition. The typical deceleration rate for automatic emergency braking systems for dry road surface was 0.8g, and it was assumed that it would be reduced to 0.4g for the slippery road condition due to precipitation weather conditions. (Bosma et al, 2017, Graci.V, et al., 2019).

The consequence event was modeled to provide a relationship between the impact speed, and the consequence as shown in the graphs in Figure 2-11. The severity of the harmful consequence was categorized into four levels of injury: fatal, major, minor and negligible. For a range of impact speed, the probability distribution for each level of injury was identified based on past crash-injury models and past accident statistics for both pedestrian and vehicle targets. (Bahouth et al., 2014, Jurewicz et al., 2016, Richard, 2009). The identified probability distributions are shown in Figure 9 below.

**Figure 2-11: Probability distributions of Injury Levels for Impact Speed (mph)**
2.4.4 Hazard Evaluation (Conditional Risk Assessment)

Based on the constructed causal-chain for the identified hazard, a conditional risk assessment was conducted in order to identify acceptable sets of conditions, a sub-ODD of the example system in this case study.

<table>
<thead>
<tr>
<th></th>
<th>Negligible</th>
<th>Minor</th>
<th>Major</th>
<th>Fatal</th>
</tr>
</thead>
<tbody>
<tr>
<td>$&lt;10^{-6}$</td>
<td>Extremely Remote</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$&lt;10^{-5}$</td>
<td>Remote</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$&lt;10^{-3}$</td>
<td>Probable</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$&gt;10^{-3}$</td>
<td>Frequent</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 2-12: Risk matrix with a standard adopted from the aviation certification standard for small aircraft (ASTM 3230)**

A standard for the acceptable level of risk was adapted from the aviation standard. The ASTM F3230 provides the industry standard for the safety assessment of systems and equipment in small aircraft that is acceptable for the part 23 federal regulations. The standard provides acceptable quantitative probabilities for different assessment levels. The assessment level for airplanes with a maximum seating configuration of 2 to 6 passengers was chosen for this analysis for it best resembles the small passenger cars. The acceptable occurrence probabilities, in terms of per driving hour, for different levels of consequence, in terms of injury severity are shown in Figure 2-12.

Based on the models of the causal-chain events, the risk associated with each set of conditions comprised of the four condition classes (road type, light condition, weather condition,
and prior speed) is calculated. The risk was calculated in terms of the probability for each of the injury severity categories (negligible, minor, major and fatal). The calculated probabilities were assessed against the risk matrix in order to determine the acceptability of the relevant set of conditions.

![Figure 2-13: Preliminary case study result: Identified ODD of the hazard](image)

For each set of conditions, the occurrence probabilities of the injury severities were calculated differently depending on the object type. Therefore the acceptable set of conditions was compared between the object types and the ODD of the hazard was determined by the object type with a more restricting acceptable condition. The determined ODD is represented in green in the condition hyperspace as shown in Figure 2-13.

The determined ODD shows the influence of the condition variables on the condition acceptability. The conditions become unacceptable for higher prior speed, and the acceptable
speed thresholds vary depending on ambient light and the weather condition. The clear daylight condition has the highest speed thresholds and it is reduced the most in the dark and the precipitation conditions. The difference in thresholds for different road types was minimal.

In Figure 2-13, the prior speed thresholds set by the risk involving stationary vehicle are indicated with blue numbers, and the thresholds set by pedestrian are indicated with black numbers. For all road types, the determination of the ODD was dominated by the risk involving the forward collision with the pedestrian. The analysis also allows identifying the severity level of the consequence that determines the ODD. For the limited-access highway and the rural highway, the collision with the pedestrian resulting major injury determined the acceptable boundaries. The boundaries for the city street were determined by the collision with the pedestrian resulting minor injury.

The determined ODD is characterized with the four dimensions of the hyperspace identified during the preliminary hazard identification process including: the road type, weather condition, light condition and the travel speed. The dimensions are identified assuming that the human operator will be responsible for the ODD management. Thus the granularity of the conditions are chosen so that they are easily distinguishable by the human. For example the road type is difficult for the human to distinguish if the granularity is higher than the three broad categories chosen: limited-access highway, rural highway and urban streets. Also, the weather condition, light condition are categorized into binary categories for the human to easily determine the ODD conditions. The travel speed was a continuous variable because the human can observe the exact speed through the information displayed in the dashboard.

If this ODD is automatically managed by the automation system, the conditions needs to be observable to the sensors, and all of the four conditions are generally detectable through existing
sensors. For examples, the road type can be detected by the automation through detailed map data and the navigation system such as GPS. The light condition can be sensed through vision sensor which calculates the total illumination. For the weather conditions it could use the humanity as a surrogate condition to detect the precipitation condition.

Depending on who will be responsible for the ODD management, the dimensions of the hyperspace and their granularity will be influenced which will alter how the ODD will be characterized. It will also influence the performance requirements of the automation system when certain ODD conditions are required to be observed automatically. Next chapter will discuss the importance of the ODD management, the detailed process, and the limitations of the ODD manager, either the human or the automation, in order to think about the how the defined ODD should be managed.
Chapter 3

ODD Management

3.1 ODD Management Overview

The risk-based ODD determination methodology provides an ODD boundary that demarcates the conditions with acceptable level of risk within a conditional hyperspace. Thus, the automation use within the properly defined ODD assures that the automation will perform its intended functions with a sufficient reliability. However, the ODD itself does not assure the safe operation of the driving automation system because there remains the possibility of the inappropriate automation use outside the ODD. Therefore the use of the driving automation systems must be limited to its ODD through the ODD management.

The processes of ODD management is described in the simple feedback control model as shown in Figure 3-1. In the model, the ODD manager, the agent(s) who is responsible for the ODD
management, perceives of the available information in order to observe the conditions that are relevant to the ODD. The observed relevant conditions are assessed using the ODD hyperspace. The observed set of relevant conditions can be represented in a point in the conditional hyperspace, and the ODD boundaries in the hyperspace provide clear criteria to decide whether the condition set is inside and outside of the ODD.

Based on this assessment the ODD manager enables or limits the use of the automation. This can be accomplished by actions such as deactivating the driving automation system and transferring the control over to the human driver, or automatically maneuvering (e.g. change route, reduce speed) to avoid exiting the ODD. Successful ODD management requires the ODD manager to perceive the necessary information and to make an accurate judgement of the driving condition. Depending on the system, the responsibility of the ODD management may belong to the automation or the human operator.
The different allocations of the ODD management responsibilities depending on the capabilities of the automation and the human operator, and their corresponding SAE driving automation levels are summarized in Table 3-1.

Table 3-1: ODD Management Responsibility and the SAE Levels of Driving Automation

<table>
<thead>
<tr>
<th>SAE Levels</th>
<th>ODD Management Tasks</th>
<th>Condition Observation</th>
<th>ODD Management Decision</th>
<th>ODD Management Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 &amp; 2</td>
<td>Human Operator</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Automation System</td>
<td></td>
<td></td>
<td>Human Operator</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td>Automation System</td>
</tr>
</tbody>
</table>

3.1.1 Human ODD Management

The Human ODD management process represented by SAE Level 1 and 2 systems is shown in Figure 3-4. In human ODD management, the human operator observes information
through human sensory perception which is influenced by the operator’s attention. From this information, the operator needs to observe the conditions that are relevant to the defined ODD of the driving automation system. For example, the operator visually observes the external driving scene and detects a traffic sign which indicates the presence of the construction zone.

Based on the observed relevant conditions, the operator needs to determine if the conditions are inside or outside the ODD. The decision is based on the human operator’s mental model of the automation system which represents the operator’s understanding of the automation system’s ODD boundaries in the conditional hyperspace. Based on the ODD management decision, the operator will either use or do not use the automation in the observed relevant conditions.

3.1.2 Shared ODD Management
If the automation does not have the adequate capabilities to perform the ODD management actions, the ODD management task is shared between the human and the automation, which corresponds to an SAE Level 3 system. One way to share the ODD management task is to provide an alert or a notification to request the human operator intervene, once an ODD violation is automatically detected or anticipated, as shown in Figure 3-3 below. The human operator then must perform necessary actions to safely end the automation use. For example, the human operator may take manual control or adjust the automation control parameters such as target speed or target lane of travel in order to avoid ODD violation conditions, or the human may resume to full manual control in order to prevent the automation use outside the ODD.

Effective shared ODD management, requires both that the automation system anticipate the ODD violation in time and that the human driver responds to the request in a timely manner. In some cases the human operators latency may be low and may need more time than the automation can provide. This is exacerbated when the operator is “out of the loop” and not engaged with the driving tasks. Recent literature suggests that the average time required to respond to a request to intervene during automation driving is around 5 seconds (Gold, C. et al 2016 & Radlmayr, J. et al 2014). If the automation cannot sufficiently anticipate the ODD violation to provide adequate time for the human operator to take necessary actions, the shared ODD management is will not be effective.

3.1.3 Automated ODD Management

In an SAE Level 4 or above the ODD management is accomplished by automation which must observe the necessary conditions to make appropriate automation use decisions according to
the defined ODD of the driving automation system. The automated ODD management process is shown in Figure 3-2.

![Figure 3-4: Automated ODD Management](image)

In automated ODD management, the automation collects necessary data to determine the ODD conditions through various sensor systems. The sensor data is processed to detect the conditional states that are relevant to the ODD. For examples, an automation may collect images of the surrounding environment through vision sensors and use an image classification process to classify road signs to determine a presence of the construction zone, or an automation may use the GPS to collect its location data and use a stored map data to determine the types of the road in the planned travel path.

The ODD library represents an abstraction of the conditional hyperspace with the defined ODD boundaries of the driving automation system. The automation uses the ODD library as a decision criteria to determine whether the detected relevant conditions are inside or outside the ODD. Assuming that the ODD definition is valid, the feasibility of automated ODD management depends on the capability of the automation’s sensors to adequately observe necessary information to accurately determine an ODD violation. If the automation cannot observe an important ODD
violation conditions than a Level 4 or 5 system is not possible and the human operator needs to be ODD manager by observing those conditions to prevent the inappropriate automation use.

Once the automation determines whether the observed conditions are appropriate or inappropriate to use the automation, necessary actions may be necessary to safely activate or deactivate the automation system. This ODD management actions may be performed either by the automation or the human depending on the level of the automation system.

For the automation to safely perform the ODD management actions, the automation need to automatically control the vehicle to prevent entering the conditions which violates the ODD, which corresponds to the SAE level 4 automation system. For example, if an ODD is defined so that it has a lower speed threshold for the raining condition, the automation can slow down the vehicle to the lower speed threshold for the detected raining condition. If an ODD only includes a limited access highway, the automation need to be able to change lanes in order to prevent exiting from the traveling highway. When there isn’t an alternative routes or options to prevent the vehicle from entering the ODD violation conditions, the automation needs to be able to safely stop the vehicle to a minimal risk condition, such as stopping in the lane shoulders.

3.2 Historical Accident Analysis

The feasibility of human ODD management depends on the capability of the human to adequately observe necessary information, and the accuracy of the mental model of the automation to accurately assess the observed relevant conditions. Most current driving automation system rely on the human operator to manage the ODD, however the operator may fail to accurately determine the ODD condition and allow the use of the automation outside the ODD which may result in
accidents. The following explores recent accidents involving driving automation system to understand how human ODD management may fail.

3.2.1. Analysis Overview

In order to understand accidents related to the driving automation systems, historical accidents were analyzed. The analysis reviewed accidents which occurred within the US between 2016 and 2019. The criteria for review was if the accident:

- Involving a vehicle operated by driving automation system.
- Related to the driving automation system’s unreliable behavior that resulted in a failure to perform its intended function.
- Had sufficient public documentation of the accident to assess the behaviors of the automation and the driver.

<table>
<thead>
<tr>
<th>#</th>
<th>Date</th>
<th>Automation System</th>
<th>Vehicle</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2/14/2016</td>
<td>Google</td>
<td>Lexus SUV</td>
<td>Mountain View, CA</td>
</tr>
<tr>
<td>2</td>
<td>5/7/2016</td>
<td>Tesla Autopilot</td>
<td>Model S</td>
<td>Williston, FL</td>
</tr>
<tr>
<td>3</td>
<td>2/27/2017</td>
<td>Tesla Autopilot</td>
<td>Model S</td>
<td>Dallas, TX</td>
</tr>
<tr>
<td>4</td>
<td>1/22/2018</td>
<td>Tesla Autopilot</td>
<td>Model S</td>
<td>Culver City, CA</td>
</tr>
<tr>
<td>5</td>
<td>3/18/2018</td>
<td>Uber ATG</td>
<td>Volvo XC90</td>
<td>Tempe, AZ</td>
</tr>
<tr>
<td>6</td>
<td>3/23/2018</td>
<td>Tesla Autopilot</td>
<td>Model X</td>
<td>Mountain View, CA</td>
</tr>
<tr>
<td>7</td>
<td>5/11/2018</td>
<td>Tesla Autopilot</td>
<td>Model S</td>
<td>South Jordan, UT</td>
</tr>
<tr>
<td>8</td>
<td>5/29/2018</td>
<td>Tesla Autopilot</td>
<td>Model S</td>
<td>Laguna Beach, CA</td>
</tr>
<tr>
<td>9</td>
<td>3/1/2019</td>
<td>Tesla Autopilot</td>
<td>Model 3</td>
<td>Delray Beach, FL</td>
</tr>
</tbody>
</table>

The analysis identified 9 accidents that involved unreliable behaviors of the driving automation system as shown in Table 3-2 below. This analysis reviewed how the ODD was defined for the automation system involved and the conditions at the time of the accident with respect to
the defined ODD. The analysis reviewed available information for the driver related the ODD and the response behavior of the driver.

3.2.2. Review of the Involved Driving Automation Systems

Out of the 9 accidents that were analyzed, 7 accidents involved Tesla’s driving automation system, “Autopilot”. The Autopilot consists of two automation features 1) Traffic-Aware Cruise Control (TACC) and 2) Autosteer. Autopilot utilizes a sensor and imaging suite (cameras, radar and ultrasonic sensors) to monitor the travel path. Based on the input data from the sensors, Autopilot 1) maintains the set cruise speed, 2) brakes when it detects slower objects ahead of the Tesla, 3) decelerates and follows a slower-moving vehicle in front of the Tesla at a preset time-based headway, and 4) maintains the vehicle’s lateral position in the travel lane.

While the Tesla’s Owner’s Manual does not specifically describe an ODD, it does state the Autopilot’s recommended use conditions and do-not-use condition. In addition, the manual lists specific limiting conditions where the performance of the Autopilot is limited and thus requires the driver to intervene for potentially unreliable behaviors. The limiting conditions includes roadway features/conditions (hills, toll booths, difficult lane markings), environmental conditions (bright light, extreme temperature), specific traffic conditions (stationary object, high travel speed, cut-out scenario) for which automation system may not work properly. For this analysis, the recommended use conditions were considered as the ODD of Tesla Autopilot, and the do-not-use conditions and the existence of specified limiting conditions were considered as outside the ODD, as shown in Table 3-3.
Table 3-3: The Assumed ODD and the ODD Violation Conditions of the Tesla Autopilot

<table>
<thead>
<tr>
<th>ODD Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Limited-Access Divided Highways/Freeways</td>
</tr>
<tr>
<td>- Straight Road</td>
</tr>
<tr>
<td>- Dry Road Surface</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ODD Violation Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>- City Streets</td>
</tr>
<tr>
<td>- Sharp Curves</td>
</tr>
<tr>
<td>- Icy or Slipper Road Surface</td>
</tr>
<tr>
<td>- Adverse Weather Conditions (heavy rain, snow, fog)</td>
</tr>
<tr>
<td>- Areas where bicyclists/pedestrians may be present</td>
</tr>
<tr>
<td>- Construction Zone</td>
</tr>
<tr>
<td>- Hills</td>
</tr>
<tr>
<td>- Lane Marking that are Difficult to Detect</td>
</tr>
<tr>
<td>- Faded/Worn</td>
</tr>
<tr>
<td>- Visible Previous Markings</td>
</tr>
<tr>
<td>- Temporary Adjusted</td>
</tr>
<tr>
<td>- High-Contrast Lines (Shadows, Pavement Seams)</td>
</tr>
<tr>
<td>- Bright Light</td>
</tr>
<tr>
<td>- Direct Headlight</td>
</tr>
<tr>
<td>- Direct Sunlight</td>
</tr>
<tr>
<td>- Extreme Temperature</td>
</tr>
<tr>
<td>- Sensor/Damage/Obstructions</td>
</tr>
<tr>
<td>- Stationary Objects</td>
</tr>
<tr>
<td>- Travel Speed &gt; 50 mph</td>
</tr>
<tr>
<td>- Cut-Out Scenario</td>
</tr>
<tr>
<td>- Objects Partially in the Travel Lane</td>
</tr>
<tr>
<td>- Toll Booths</td>
</tr>
</tbody>
</table>

In the Tesla Autopilot, the use of the automation is only automatically restricted when the vehicle is unable to determine the path due to lack of visual lane markings or the absence of a lead vehicle to follow. In other conditions, it is the human operator’s responsibility to observe the condition in order to determine if the condition is appropriate to use the automation and to activate or deactivate the Autopilot accordingly.

The other two accidents that were reviewed involved vehicles equipped with driving automation systems that were being tested by trained operators within designated routes. One of the accidents involved a Lexus SUV vehicles equipped with a driving automation system
developed by Google (Waymo), and the other accident involved a Volvo XC90 vehicle which had been modified and equipped with a driving automation system that was being developed by Uber ATG. In that accident the Volvo’s advanced driver assistance system (ADAS) components were deactivated while operating in ATG’s autonomous mode. Because these driving automation systems were not in public, there was no information regarding the ODD of those systems and the specific roles of the driver regarding the use of the automation. However a post-accident interviews revealed that the testing operators of the Uber ATG automation systems were being trained specifically to respond to the situations such as the presence of the pedestrian in the path for a possible unreliable behaviors. Therefore the presence of the pedestrian was considered as ODD violation condition for the Uber ATG.

3.2.3. Analysis Result

Table 3-4: Summary of the Results

<table>
<thead>
<tr>
<th>#</th>
<th>Location</th>
<th>Driving Condition</th>
<th>ODD Violation Conditions</th>
<th>ODD Violation Observability</th>
<th>Driver Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Mountain View, CA</td>
<td>N/A</td>
<td>-</td>
<td>-</td>
<td>None</td>
</tr>
<tr>
<td>2</td>
<td>Williston, FL</td>
<td>Outside ODD</td>
<td>- Not Limited Access Road</td>
<td>Observable</td>
<td>None</td>
</tr>
<tr>
<td>3</td>
<td>Dallas, TX</td>
<td>Outside ODD</td>
<td>- Construction Zone</td>
<td>Observable</td>
<td>None</td>
</tr>
<tr>
<td>4</td>
<td>Culver City, CA</td>
<td>Outside ODD</td>
<td>- Stationary Objects (Cut-Out Scenario)</td>
<td>Unknown</td>
<td>None</td>
</tr>
<tr>
<td>5</td>
<td>Tempe, AZ</td>
<td>Outside ODD</td>
<td>- Presence of Pedestrian</td>
<td>Observable</td>
<td>0.02 s.</td>
</tr>
<tr>
<td>6</td>
<td>Mountain View, CA</td>
<td>Outside ODD</td>
<td>- Lane Marking that are Difficult to Detect</td>
<td>Unknown</td>
<td>None</td>
</tr>
<tr>
<td>7</td>
<td>South Jordan, UT</td>
<td>Outside ODD</td>
<td>- Stationary Objects (Cut-Out Scenario)</td>
<td>Unknown</td>
<td>None</td>
</tr>
<tr>
<td>8</td>
<td>Laguna Beach, CA</td>
<td>Outside ODD</td>
<td>- Not Limited Access Road</td>
<td>Observable</td>
<td>None</td>
</tr>
<tr>
<td>9</td>
<td>Delray Beach, FL</td>
<td>Outside ODD</td>
<td>- Not Limited Access Road</td>
<td>Observable</td>
<td>None</td>
</tr>
</tbody>
</table>
First, the driving conditions during the accidents were reviewed to determine whether the automation systems were being used within the ODD. All of the accidents except the accident which involved Google’s automation system (#1), occurred outside the defined ODD. For those 8 ODD violation accidents: 3 accidents (#2, 8, 9) occurred outside the limited-access divided highway, 3 accidents (#4, 5, 7) occurred at the presence of objects which violated the ODD (2 accidents (#4, 7) involved stationary vehicles and 1 accident (#5) involved a pedestrian), 1 accident (#6) occurred on road with lane markings that were difficult to detect, and 1 accident (#3) occurred within a construction zone. The results are summarized in Table 3-4.

For the 8 accidents that occurred outside the ODD, the available information was reviewed in order to evaluate the observability of the ODD violation conditions. For the ODD violation conditions which violated the limited-access highway conditions (#2, 8, 9), there was no automated support and the operators needed to visually observe the external driving environment to determine if they were on a limited-access highway. Visual information indicating that they were not on a limited access highway was clearly observable to the drivers due to the presence of multiple at-grade intersections in clear daylight condition prior to the accidents.

For the ODD violation conditions related to the presence of specific objects (#4, 5, 7), there was also no automated support. The information was only observable to the human when the objects were within the visual field of the driver. Two accidents (#4, 7) involved the presence of a stationary vehicle in a cut-out scenario. A cut-out scenario which refers to a specific driving situation when a leading vehicle moves out of the driving path revealing a stationary or slow-moving vehicle or object is in front. Although the exact observability of the stationary vehicle during the accidents is unknown, the stationary vehicles may have been visually observable only after the lead vehicle had moved. In one of the two accidents, the post-event investigation
concluded that the lead vehicle moved out 3.5 seconds prior to the crash, the exact timing in the other accident was unknown (NTSB 2019). Similarly, in the accident involved the presence of a pedestrian (#5), the post-event investigation concluded that the pedestrian was visually observable 5.6 seconds prior to the crash (NTSB 2019).

In accident #3, there was no automation support to provide a feedback to the driver regarding the presence of the construction zone, therefore it was the human operator’s role to determine the presence of the construction zone by observing the traffic signs or other relevant cues such as temporary barriers (e.g. drums, cones and tubes). It is likely that the construction zone had been visually observable to the attentive human operator.

One accident (#6) occurred within the ODD violation condition related to lane markings that are difficult to detect due to faded lane markings. Although the post-accident analysis found that the quality of the lane markings at the accident location were partially degraded, the markings were not completely faded. It is unknown if the condition was salient enough for the operator to be able to distinguish at the time of the accident. In addition, the ODD violation condition is defined as “lane markings that are difficult to detect”. Because it is unclear how much degradation of the lane markings is difficult for the automation to detect, it may have been ambiguous for the operator to observe the ODD violation condition.

Next, the behavior of the human operator related to the ODD management prior to each of the accidents was reviewed, including the operator’s attention to available ODD information and the operator’s actions prior to the accident.

In the accident involving the Uber ATG automation system, the vehicle was equipped with an inward-facing camera which allowed a direct observation of the operator’s behavior through a recorded video. The post-accident analysis shows that the operator spent nearly a third of the
trip looking down at a personal cell phone and only intermittently observed the driving scene. Examination of the operator’s cell phone records show that the operator was streaming a video for the entire trip. About 6 seconds prior to crash, the operator again looked down and their gaze remained down for the next 5 seconds. The operator returned their gaze to the road about 1 second prior to the impact, and applied a steering input 0.02 seconds prior to the impact which was insufficient to avoid the crash. (NTSB, 2019).

The Tesla Autopilot monitors the changes in steering wheel torque applied by the operator as a surrogate means of assessing the level of engagement of the operator. In 4 out of the 7 Tesla accidents, the record of the steering wheel torque prior to the crash were available in the accident reports (NTSB 2017, 2019, 2019, 2020). For these accidents the record indicated prolonged lack of engagement of the human operator during the use of the automation. Also the hands were not detected for a length of time prior to the impact as shown in Table 3-5 below.

<table>
<thead>
<tr>
<th>Location</th>
<th>Total Trip Period</th>
<th>Automation Use Period</th>
<th>Hands on the Steering Wheel Period</th>
<th>Last Hands on the Steering Wheel Prior to Crash</th>
</tr>
</thead>
<tbody>
<tr>
<td>Williston, FL</td>
<td>41 min</td>
<td>37 min</td>
<td>25 s.</td>
<td>1 min. 51 s.</td>
</tr>
<tr>
<td>Culver City, CA</td>
<td>66 min.</td>
<td>29 min. 4s.</td>
<td>1 min. 18 s.</td>
<td>3 min. 41 s.</td>
</tr>
<tr>
<td>Mountain View, CA</td>
<td>29 min.</td>
<td>21 min. 25 s.</td>
<td>7 min. 22 s.</td>
<td>6 s.</td>
</tr>
<tr>
<td>Delray Beach, FL</td>
<td>Unknown</td>
<td>Unknown</td>
<td>Unknown</td>
<td>8 s.</td>
</tr>
</tbody>
</table>

Lastly, in all of the 7 Tesla accidents, none of the drivers perform any type of action (e.g. braking, turning steering wheel, adjust/deactivate automation functions) to mitigate the consequence, which indicates distraction and/or potential overreliance on automation.
3.2.4. Analysis Summary

Based on the analysis, the failures the human ODD management in the accidents were categorized into 3 types: 1) ODD violation was not observable, 2) ODD violation was ignored, and 3) ODD violation not observed. The possible failure types for each accidents are summarized in Table 3-6.

**Table 3-6: Possible Failures of the Human ODD Management in the Accidents**

<table>
<thead>
<tr>
<th>#</th>
<th>Location</th>
<th>Driving Condition</th>
<th>Not Observable ODD Violation</th>
<th>Ignored ODD Violation</th>
<th>Not Observed ODD Violation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Mountain View, CA</td>
<td>N/A</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>Williston, FL</td>
<td>Outside ODD</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>3</td>
<td>Dallas, TX</td>
<td>Outside ODD</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>4</td>
<td>Culver City, CA</td>
<td>Outside ODD</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Tempe, AZ</td>
<td>Outside ODD</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Mountain View, CA</td>
<td>Outside ODD</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>South Jordan, UT</td>
<td>Outside ODD</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Laguna Beach, CA</td>
<td>Outside ODD</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Delray Beach, FL</td>
<td>Outside ODD</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
</tbody>
</table>

The analysis found that most of the accidents (8/9) occurred outside the defined ODD of the driving automation system. This indicates that one causal path is the inappropriate use of automation outside the ODD. In some of these cases (4/8) the ODD violation conditions may have *not observable* for the human operator to observe with a sufficient time to safely end the automation use due to an obstruction of the visual field or poorly defined ODD condition. This indicates that ODD observability is a key issue in mitigating automation accidents. In the remainder of the accidents accident (4/8), the ODD violation conditions were clearly observable.
by the operator but the operator decided use the automation outside the ODD. This result indicate that the operator either ignored the observed ODD violation conditions or did not observed the observable ODD violation condition due to lack of attention. This indicates potential issues with regard to over trust, lack of understanding of the automation and the potential distracted attention due to overreliance on the automation.

3.3 Human ODD Management

In order to adequately manage the ODD, the operator needs to make an assessment on whether the operating conditions are within or outside the defined ODD of the driving automation system. As shown in the accident analysis in the previous chapter, if the driver does not recognize an ODD violation, the automation may be inappropriately. Therefore it is important to understand the human’s underlying process for making the automation use decisions. This chapter will explore the underlying cognitive process by which the human operators make the ODD management decisions. Based on this understanding, the potential causes of the ODD management failures are identified.

In order to understand how the human operator manages the ODD, a human cognitive process model was developed based on the Endsley’s situational awareness model (Endsley, 1995). Endsley represented the human’s awareness of the situation in three stages: 1) perception of the relevant information in the operational environment, 2) comprehension of their meanings, and 3) projection of the future state. This framework was adopted to represent the situation awareness of the human operator regarding the ODD management. The developed model is shown in Figure 3-2 below.
In the model, the human operator uses sensory perception to observe the information, which includes: 1) visual perception of the driving scene, visual display of vehicle and/or automation system status (e.g. vehicle dashboard, human-automation interface), 2) auditory perception of the external environment (e.g. honking, emergency vehicle siren) and in vehicle alerts or notification) and 3) vestibular and somatosensory perception of the behaviors of the vehicle (e.g. acceleration, control feedback). The observation of the information is limited by human sensory system’s physiological limitations. For example, the visual perception has a limited visual range and field of view that is susceptible to conditions such as adverse weather, dark light conditions, or a presence of obstructions. In addition, it is difficult to observe less salient or ambiguous information.

The observable information is observed by the human operator when the operator allocates adequate cognitive attention to the information. Attention is a process of directing attention resource to perceive specific information. The control of attention can be done involuntarily or voluntarily. Involuntary control of attention is driven by salient stimulus such as flashing lights or sudden sound such as alerts. Voluntary control of attention intentionally directs the attention resource to perceive specific information of interest. The primary intention to perceive information
from the driving environment is to resolve uncertainty. (Senders et al., 1967). For example the
drivers perceive the driving environment to resolve the uncertainty of the vehicle current position
respect to the lane boundaries. In addition, the attention is influenced by the human operator’s
physical and emotional conditions. For example, operator fatigue may results in lack of attention
resource for the operator to pay attention to the roadway.

The human operator comprehends the observed information in order to, among other things,
make ODD management decisions. The decisions are made by assessing the relevant conditions
based on the operator’s mental model of the automation. The mental model is a cognitive
representation of the human’s awareness and knowledge of a process (Rouse & Morris 1985;
Seppelt & Lee 2015). In this context, the mental model of automation represents the human
operator’s knowledge of the automation system including its defined ODD. The accuracy of the
ODD management decisions depends on the accuracy of the operator’s mental model of the
automation.

Based on the information comprehended, the human operator may project the future
conditions in order to predict possible future ODD violations. The accuracy of the ODD prediction
depends on the accuracy of the projected future conditions and accuracy of the mental model of
the automation system. If the human operator incorrectly predicts that the operating conditions
will remain with the ODD, the operator may not allocate adequate attention to the important
information and is at risk for distraction.

### 3.4 Human ODD Management Failures

Based on the review of the accidents in section 3.2.4, the report identified three types of
ODD management failures: 1) ODD was not observable, 2) ODD was ignored, and 3) ODD not
observed. These three failure types correspond to the failures of each stage in the Endsley’s situational awareness model: 1) failure of perception 2) failure of comprehension, and 3) failure of projection. This chapter will discuss the details and the possible causes of those failures using the situational awareness model for the ODD management.

3.4.1 ODD Violation Not Observable: Failure of Perception

![Diagram of Perception Failure Represented in the Situation Awareness Model]

**Figure 3-6: Perception Failure Represented in the Situation Awareness Model**

In order to make an ODD management decision, the human operator observes information necessary to recognize the conditions that are relevant to the ODD of the driving automation system. The operator needs to perceive the presence of the conditions which violate the ODD (e.g. presence of a construction zone) or perceive the absence of the conditions that constitute the ODD (e.g. absence of the visual lane markings) in order to determine that the driving conditions is outside of the defined ODD. If the necessary information is *not observable* to the human, the
operator cannot recognize ODD violation adequately to prevent the use of the automation in the unacceptable operating conditions.

The ODD violations are not observable when the relevant conditions are not physically perceivable to the human sensory systems. For example, internal states of the automation are not observable if the information is not displayed through a display or other input. Also the human’ vision has limited range and field of view, and the limited range and the field of view may be further reduced due to adverse weather conditions or obstructions by vehicles or object.

ODD violations are ambiguous for the human to observe, when the difference between the acceptable ODD and ODD violation conditions are not distinguishable. For example, the slow change in the ambient light condition may lead the operator to not realize that the condition is too dark for the automation to be used. In the past accident, the subtle degradation of the lane markings may not had been distinguishable to the operator.

If ODD violation conditions appear too quickly, the operator may not be able to project the presence of violation conditions with sufficient time for the operator to respond. For example, when the presence of a pedestrian is an ODD violation condition, a sudden appearance of a crossing pedestrian between parked cars may not be observable for the operator to safely intervene.

A potential cause of lack of observability is an inappropriately defined ODD which does not carefully consider the limitations of the human sensory systems and situation awareness process as well as potential situations that may influence the observability of the ODD violation conditions. The information necessary to make ODD management decisions directly depends on how the ODD is defined for a given driving automation system. If the ODD is defined with environmental conditions that are not physically observable to human sensory perception then it is not observable. For example, violation conditions could be outside of the visible range or field
of view due to visibility reducing environmental conditions (e.g. heavy rain, fog). Another potential cause of observability is an ambiguously defined ODD threshold or criteria.

3.4.2 ODD Violation Ignored: Failure of Comprehension

![Diagram of the Situation Awareness Model with a red arrow indicating Ignored ODD Violation]

**Figure 3-4: Comprehension Failure Represented in the Situation Awareness Model**

In ODD management, the human operator evaluates the observed information in order to evaluate whether the conditions is acceptable to use the automation or not. The basis for the evaluation is the operator mental model of the automation. If the mental model is inaccurate, the operator may falsely assume that the automation is acceptable to be used outside the ODD and ignore the ODD violation. The report identified two causes of the inaccurate mental model of the automation: 1) lack of understanding, 2) over-trust in automation.

In the past accidents that involved the use of the automation outside the limited-access highway, it is likely that the operators were able to easily observe that the roadway is not a limited-access highway. However the operators ignored the observed ODD violation and decided to use
the automation. The use decision may have been made due to a lack of understanding of not knowing that the automation use is only acceptable within the limited-access highway. Or, the operators may have over-trusted the automation to perform reliably in the conditions outside the limited-access highway based on their experience of testing the automation in those ODD violation conditions.

The human operator may also develop an inaccurate mental model if the operator has a lack of understanding of the driving automation system and its ODD. Lack of understanding is when the operator does not understand or is not aware of the limitations of the automation system or the ODD. The lack of understanding may induce the operator to unintentionally ignore the ODD violation. For example, if the operator does not know that a sharp curve violates the ODD, even if the operator observes a sharp curve in the path, the operator may choose to use the automation.

The understanding of the driving automation system is obtained various sources including training, experience with similar systems, and education by dealers or reading the manual. One of the challenges with driver automation systems is that the systems are used by operators with a wide range of general and technical competency and there is often no required training or demonstration of competency for use of automation systems. Driver mental models are often developed through operating experience and are vulnerable to lack of understanding.

The human operator may also have an inaccurate mental model of the automation if the operator develops over-trust, which creates a gap between the operator’s knowledge of the automation’s capabilities and its actual capabilities. This may lead the operator to make a false assumption that the automation is reliable and can be used in certain conditions outside of the defined ODD.
The operator may develop over-trust through incorrect learning via experience with the use of the automation. Learning through experience is a process of developing the mental model by which the information obtained from a recent experience is assessed to create, confirm or modify the driver’s prior knowledge. It is shown in past studies (Beggiato et al, 2013, 2015) that experience can modify prior understandings.

If the use of the automation is not automatically prohibited for conditions outside the ODD, the human operator may choose to test and explore the limits of the automation by activating the automation outside the ODD. The operator may not be exposed to the unreliable behaviors of the automation, because, due to the conservative safety standard, the automation is likely to be relatively reliable even in the conditions outside the ODD. Repeated experience of this reliable automation performance outside the ODD may lead the operator to modify the prior knowledge of automation and assume that the automation is acceptable to be used outside the ODD.

3.4.3 ODD Violation Not Observed: Failure of Projection

![Figure 3-7: Projection Failure Represented in the Situation Awareness Model](image-url)
The primary cause of lack of observation of perceptible ODD violation conditions by the operator appears to be due to lack of attention. The lack of attention is the result of insufficient allocation resources. Lack of attention appeared in all of the evaluated accidents that occurred outside the ODD, which highlights the importance of understanding the cause of the lack of attention.

The lack of attention may due to poor physiological or emotional conditions of the operator. For example, the human may fall asleep due to fatigue or become unconscious due to poor health condition. This result in the involuntary lack of attention. The lack of attention may also arise if the human voluntarily allocates their attention to the information that not relevant to the ODD management such as texting or watching a movie on a cellphone.

Literature on human attention during driving suggest that the primary motivation for paying attention to the information relevant to the driving task is to resolve uncertainty (Senders et al., 1967). For examples, the human may monitor the vehicle position relative to the driving environment in order to resolve the uncertainty in the vehicle’s lateral position relative to the lane boundaries, or the human may monitor the forward path of the vehicle in order to resolve the uncertainty in the presence of obstacles in the path, or a change in speed of a lead vehicle. Conversely, if the human has low uncertainty on the information, the human has no motivation to observe the information, which leads to the lack of attention during the period of low uncertainty. And as the uncertainty builds up over time, the human relocates the attention back to the information to resolve the uncertainty. This attention cycle time depends on the rate of the uncertainty build up which is influenced by the driving situation. Past experiment showed that as the speed increases, the occlusion time (i.e. time of between of the sampling of visual information) was reduced (Senders et al, 1967).
In the ODD management context, the motivation for paying attention to the driving conditions is uncertainty in the potential changes in the conditions that may violate the ODD. If an operator projects that the driving conditions will be within the ODD during a projected period of time, the projection may lead to a lack of motivation for the operator to allocate attention to the available information (Cummings, M.L. & Ryan, J.C., 2014). And if the operator’s ODD projection is inaccurate, the lack of attention may lead the operator to not be able to observe the ODD violation. The report identified two causes of the inaccurate ODD projection: 1) inaccurate projection of the future conditions, and 2) Inaccurate mental model of the automation.

As a part of the situation awareness process, the human projects future situation based on the observed and comprehended information. In the ODD management, the operator may project the future driving conditions that are relevant to the ODD. An inaccurate projection of the future conditions may create a gap between the operator’s projected conditions and the actual future conditions. Even if an operator has an accurate mental model of the automation, an incorrect projection that excludes the actual presence of ODD violation conditions may induce the operator to falsely assume that the driving condition will remain within the ODD during the projected period of time. For example, even if an operator knows that the automation should not be used near construction zone, the operator may fail to project a construction zone in the path. This may allow the operator to use the automation without paying attention to the relevant conditions and failed to observe the ODD violation conditions.

It is difficult for the human to accurately project events or condition that are less probable such as temporary change in the driving environment, or presence of objects or conditions that are less common. It is because rather than making a rational judgement by considering the probability of every relevant conditions, the human uses heuristics to form expectations which are often
associated with bias (Klein 1998, Simon, 1990 Tversky & Kahneman 1974, Parasuraman & Riley 1997). The heuristic may underestimate the likelihood of less probable event and neglect them in the future projection. The accuracy of the projection may vary largely across individual depending on their sophistication of the mental model of the environment, familiarity with the driving environment and experience.

The human operator evaluates the projected information in order to determine whether the projected conditions include the ODD violation conditions or not. The basis for the evaluation is the operator mental model of the automation. If the human has an inaccurate mental model, the operator may ignore the projected ODD violations and falsely assume future conditions will remain acceptable. This leads to an inaccurate ODD projection despite the accurate projection of the future conditions by the operator. The two causes of the inaccurate mental model of the automation: 1) lack of understanding, 2) over-trust in automation are discussed in detail in the previous section 3.4.2.
Chapter 4

Recommendations to Support Improved ODD Management

In the previous chapters, the ODD management process was explored. The accident analysis and modeling of the situational awareness process related to the cause of ODD management failures provided an understanding of these failures and motivated approaches to improve the driver-automation systems to support ODD management.

- Clearly Define the ODD considering the Human or Automated ODD Manager

  The risk-based framework provided a principle based methodology to determine the ODD by assessing the risk associated with sets of conditions that are relevant to the technical limitations of the driving automation systems. The ODD determined through this method is confined by the relevant conditions that are used to construct the conditional space in which the sets of conditions
are evaluated. Therefore it is important to consider the feasibility of the ODD management at this preliminary stage where the relevant conditions are identified.

The identification of the ODD hyperspace of relevant conditions must consider the observability and those conditions to the agent who is responsible for the ODD management, either the human operator or the automation. Because the human operator and automation have different capabilities, it is necessary to determine who will be responsible for managing the ODD, and then identify the relevant conditions accordingly.

- **Automate ODD Management When Possible**

  The review of past accidents indicated that the human operator’s lack of understanding or over-trust in automation or poor future projection can lead to lack of attention and overreliance which can result in ODD management failures. Because of these numerous vulnerabilities of human ODD management, it appears desirable when possible to automate ODD management. This requires that the ODD be defined in a way that the relevant conditions can be reliably observed by the automation.

  In addition, in automated ODD management, because the ODD definition is not limited by the human’s sensory or memory capabilities, it can be more complex and higher resolution than can be communicated and managed by a human driver. For example, when the road type is considered as a surrogate condition to define an ODD, for the human it is limited to only a few categories such as limited-access highway, rural highway or urban streets. For the automation, the level of risk could be assigned to specific road segments in a high resolution “ODD map”.

  The ODD can also be defined with conditions that are ambiguous to the human operator. For example, for light conditions, it could be ambiguous for the human to distinguish how dark
would be considered outside the ODD. For the automation this ODD condition could be defined with an exact illumination level of the external environment.

It is important for the automation to have the sufficient capability to make an accurate observation of the relevant conditions in order to make accurate ODD management decisions (e.g. sensor performance to detect ODD violation conditions). Because the ODD requires the probability of unreliable behavior due to the automation use outside the ODD to be reduced to an acceptable level. This provides a standard to determine the minimum performance requirements for the both the automation and the ODD management sensors use to determine the ODD violation conditions.

Some relevant conditions could be difficult or ambiguous for the automation system to observe and comprehend. When an ODD is defined with relevant conditions that are not reliably observable by the automation, the human operator needs to manage the ODD, or the ODD needs to be redefined with surrogate conditions that are observable to the automation. For example, a stopped car next to the road that is about to pull out from a driveway may be difficult for an automation to detect because the automation may have the capability detect subtle cues to comprehend the intention of the other driver. Whereas for the human, the other road user’s intention could be easily comprehended.

Automated ODD management with SAE level 4 requires the automation to safely deactivate the automation use in the ODD violation conditions. Therefore it is important to determine the capability of the automation to perform the deactivation. If the automation does not have the capability to take necessary actions, the automation must request the human operator intervene and let the human decide the necessary actions and execute them which is required for SAE level 3 automation systems. However this requires the automated ODD management to
determine ODD violation with a sufficient leeway for the human operator to return to the control loop. The human intervention may require longer leeway than the automated ODD management can provide since the human need to regain the situational awareness due to being out-of-the-loop.

- Provide Feedback to Support the Human Mental Model for SAE Level 3 Systems

  Display of information such as automation’s internal logic criteria for the ODD determination may support the operator to mental model of the automation. The information provided through a display informs the human what ODD violation conditions the automation has detected through sensors (e.g. the display may represent high curvature, presence of construction zone, or a road with higher likelihood of the presence of hazards). In addition, providing such information along with an alert (i.e. request to intervene) has a potential to mitigate the loss of trust in the automation system by supporting the operator’s understanding of the cause of the alert so that the driver can understand if the alert was issued on a reasonable basis.

  For example, when an alert is issued without any other information regarding why the alert was issued, the operator may not comprehend the potential changes in the driving conditions that would violate the ODD, especially if the ODD violation conditions are not salient to the human perception. As a result, the operator may lose trust in the alert if the alert does not lead to an actual unreliable behavior of the automation. Conversely, if supporting information is provided (e.g. provide an information to the operator that the alert was issued based on the detection of degraded/faded lane markings), the operator may understand that the automation is using the clarity of the lane markings as a cue to determine the ODD. With the understanding, the operator can consider the alert was issued reasonably.
• Define ODD for SAE Level 1 & 2 Systems Considering Human Limitations

If the automation cannot reliably detect the ODD relevant conditions, the human operator need to manage the ODD, which corresponds to the SAE level 1 & 2 automation systems. In order to support human ODD management, the ODD must be defined with a careful consideration of the limitations of the human operator.

The ODD needs to be defined with the relevant conditions that are observable to human sensory systems. When conditions that are directly related to the technical limitations of the automation systems are not observable to the human, observable surrogate conditions need to be identified to describe the ODD. When the ODD conditions that are the internal states of the automation/vehicle system, the information must be displayed to the human through appropriate feedback. These consideration for the observability needs to be addressed when potential relevant conditions are identified during the preliminary hazard identification stage in the overall ODD determination process.

In addition, the ODD definition for the human must be comprehensible and clear, considering the human’s limited cognitive capacity. The human has limited capacity to understand and recall information. If the list of relevant conditions are beyond human capability, it would result in lack of understanding for the human to adequately manage the ODD. Also, if the ODD is complex and defined with multiple combinations of the driving conditions the human may not be able to comprehend the ODD due to limited information the human can process in real-time. Therefore, the complexity and the granularity of the relevant conditions need to be carefully chosen.
• Be aware of the Potential Human Operator’s Over-Trust in Automation

It is difficult to avoid the development of over-trust in automation for systems where ODD management relies on the human operator because it is difficult for a human operator to accurately infer the reliability of an automation system from experience. This is because any reasonable driver automation system will work most of the time, even for short excursions outside the ODD and it is difficult for the driver to safely observe automation failure conditions which would calibrate them on the ODD validity. Some mitigation of this risk can be achieved by communicating and making examples of automation failures outside the ODD and in training materials but this may not be fully appreciated by many drivers in the general population. As a result, potential driver automation systems which rely on human ODD management should be used with caution and evaluated for the clarity and understanding of the ODD and the risk (probability and consequences) if over-trust develops.

• Teach Human Mental Model to Support Accurate ODD Knowledge

In order to develop a mental model with accurate knowledge of the ODD, the human needs to be provided with opportunities for appropriate learning. The learning opportunities may include: training materials such as owner’s manual, online user manual content; car dealer training for demonstration; instructional videos.

One of the challenges in developing a teaching material is the broad range of driver experience and sophistication in the driver’s mental models. The goal of designing manuals or training materials is to clearly inform the defined ODD of the automation system so that even operators with the lowest level mental model can adequately observe and determine the ODD violation conditions.
One approach for developing an effective teaching material is to carefully consider the apriori mental model. Vakil and Hansman (1998) proposed the “operator directed process” as an attempt to redefine the design process to incorporate and specify the expected operator mental model of the automation system as a design requirement. One version of this approach to support ODD management is to write the teaching material for the ODD conditions before the system is developed and use it as part of the automation system requirements as opposed to the traditional approach of developing the system and then attempting to develop the teaching material. Vakil suggested that “by constraining the design process to implementations which can be used effectively by operators at the basis of a robust mental representation, it is expected that less error prone automation systems will be developed.”
Chapter 5

Summary and Conclusion

A risk-based framework was developed leveraging on the traditional risk theory to formally provide a principled basis to define the ODD in terms of risk related to a system’s failure of intended function as a function of: 1) occurrence probability and 2) consequence severity. The framework allowed to assess the acceptability of the risk associated with a set of conditions using a threshold provided by the risk matrix with a desired safety standard.

Based on the framework, the report developed a methodology to determine the ODD by determining the conditional boundary that demarcates the sets of conditions with acceptable level
of risk. The method identified the importance of finding the appropriate relevant conditions, because the conditions form the dimensions of the conditional hyperspace in which the ODD boundary is determined. The methodology was applied to a simple example driving automation system in order to demonstrate the use of the proposed framework.

The analysis of the historical accidents involving driving automation systems identified the failure mechanisms of the human ODD management related to each stage of the Endsley’s situational awareness model: failure in perception (not observable ODD violation), failure in comprehension (ignored ODD violation) and failure in projection (not observed ODD violation). The identified failures were explored to identify potential causes of those failures including, lack of observability of the relevant conditions, the human operator’s lack of understanding and over-trust in automation, and the inaccurate projection of the future conditions. Based on the understanding, the report provided a set of recommendations to support improved ODD management including the ways to appropriately defining the ODD considering the limitations of the human or the automated ODD manager, and the ways to support accurate mental model of the human operator.

The report identified numerous vulnerabilities of the human operator that would result in inappropriate automation use outside the ODD which highlights concerns with human ODD management. Human operator’s over-trust in automation was a natural consequence of monitoring highly reliable automation systems due to the human’s low exposure to the automation’s unreliable behaviors. Together with the human operator’s limited capability to project unexpected future states, the human operator’s potential lack of attention and overreliance on automation seemed difficult to prevent.
The findings emphasized the need for automated ODD management when possible and the importance of defining the required level of performance of the automation to adequately perform both the automated driving tasks and the tasks related to the management of the ODD. The risk-based methodology proposed in the report provides a structure to formally evaluate the driving automation system to determine the minimum performance requirements for the automation to be used in specific operating conditions.

Although the proposed risk-based framework sets the foundation for the evaluation of driving automation system, the details in the processes of the methodology have rooms to improve. The application of methodology was limited to a hazard of a simple driving automation system, partially because of the lack of detailed information of real driving automation systems due to the proprietary reasons. Applications of the methodology to real systems with a greater complexity will provide opportunities to enhance the methodology.
Reference


Czarnecki K. *Operational World Model Ontology for Automated Driving Systems*, Waterloo Intelligent Systems Engineering Lab (WISE), 2018


Cummings, M.L.; Ryan, J.C, Shared Authority Concerns in Automated Driving Applications, MIT, HAL Reports, 2014


IIHS, *Road, track tests to help IIHS craft ratings program for driver assistance features*. Insurance Institute for Highway Safety Status Report, 53(4), 3-6, 2018


Kalra, N., *Challenges and Approaches to Realizing Autonomous Vehicle Safety*. RAND Corporation, Santa Monica, February 14, 2017


NTSB, *Collision between a Car Operating with Automated Vehicle Control Systems and a Tractor-Semitrailer Truck near Williston, Florida, May 7, 2016*, National Transportation Safety Board, NTSB/HAR-17/02, Washington, DC., September 12, 2017

NTSB, *Collision between Vehicle Controlled by Developmental Automated Driving System and Pedestrian, Tempe, Arizona, March 18, 2018*, National Transportation Safety Board, NTSB/HAR-19/03, Washington, DC., November 19, 2019


Rouse, W. B., and N. M. Morris. *On looking into the black box: Prospects and limits in the search for mental models* (DTIC #AD-A159080). Atlanta, GA: Center for Man-Machine Systems Research, Georgia Institute of Technology, 1985

Schuldt, F. Towards testing of automated driving functions in virtual driving environments, Ph.D. dissertation, Technische Universitat Braunschweig, 2017


