U.S. Department of Transportation
National Highway Traffic Safety Administration

NHTSA

DOT HS 812 879

November 2020

Safety of the Intended Functionality of Lane-Centering and Lane-Changing Maneuvers of a Generic Level 3 Highway Chauffeur System

DISCLAIMER

Suggested APA Format Citation:

Becker, C. J., Brewer, J. C., & Yount, L. J. (2020, November). *Safety of the intended functionality of lane-centering and lane-changing maneuvers of a generic level 3 highway chauffeur system* (Report No. DOT HS 812 879). National Highway Traffic Safety Administration.

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
DOT HS 812 879		

4. Title and Subtitle	5. Report Date
Safety of the Intended Functionality of Lane-Centering and Lane-Changing Maneuvers of a Generic Level 3 Highway Chauffeur System	November 2020
	6. Performing Organization Code
7. Authors	8. Performing Organization Report No.
Christopher Becker, John Brewer, and Larry Yount	DOT-VNTSC-NHTSA-19-02
9. Performing Organization Name and Address	10. Work Unit No. (TRAIS)
John A.Volpe National Transportation Systems Center 55 Broadway Cambridge, MA 02142	11. Contract or Grant No.
12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
National Highway Traffic Safety Administration Electronic Systems Safety Division 1200 New Jersey Avenue SE. Washington, DC 20590	Final Report
	14. Sponsoring Agency Code

15. Supplementary Notes

Paul Rau was the Contracting Officer's Representative for this project.

16. Abstract

This report describes the findings from applying Safety of the Intended Functionality (SOTIF) concepts as described in the Publicly Available Specification (PAS) ISO 21448 to the lane-changing and lane-centering maneuvers of a generic Level 3 highway chauffeur system. This report compares the SOTIF process described in PAS 21448 with the automotive industry's voluntary functional safety standard, ISO 26262. This report then develops a generalized Level 3 highway chauffeur system, and identifies potential vehicle-level hazards, triggering events, and SOTIF mitigation measures. Finally, this report presents an approach for developing candidate scenarios to evaluate safety relevant triggering events and discusses current SOTIF evaluation approaches.

17. Key Words	18. Distribution Statement
Safety of the Intended Functionality, SOTIF, PAS 21448, triggering event, highway chauffeur system, systems-theoretic process analysis, STPA	Document is available to the public from the National Technical Information Service, www.ntis.gov

19 Security Classif. (of this report)	20. Security Classif. (of this page)	21 No. of Pages	22. Price
Unclassified	Unclassified	145	

Form DOT F 1700.7 (8-72) Reproduction of completed page authorized

Table of Contents

Figures

Tables

List of Acronyms

ADS	automated driving system
ALARP	as low as reasonably practicable
ALC	automated lane centering
ASIL	Automotive Safety Integrity Level
E/E	electrical and electronic
FARS	Fatality Analysis Reporting System
FMEA	failure mode and effects analysis
FTA	fault tree analysis
GAMAB	*globalement au moins aussi bon* (translation: globally at least as good)
HAZOP	hazard and operability study
HMI	human-machine interface
HOV	high-occupancy vehicle
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
KPI	key performance index
ODD	operational design domain
OEDR	object and event detection and response
PAS	Publicly Available Specification
SAE	SAE International
SME	subject matter expert
SOTIF	Safety of the Intended Functionality
STPA	systems-theoretic process analysis

Executive Summary

The automotive industry recognized that some class of potential safety problems is not covered by the current International Organization for Standardization functional safety process, ISO 26262.[1] A new analytical approach that focuses on safety problems that can occur when driving automation systems may develop an incorrect situational awareness (e.g., through sensor or algorithm limitations) has been developed and is termed Safety of the Intended Functionality (SOTIF). SOTIF issues can affect both the system behavior as well as the interaction with the driver. SOTIF also aims to address foreseeable misuse by the driver or other people.

This project's objectives included:

- Understand the issues and current industry approaches to SOTIF,
- Provide an example application of SOTIF principles using the lane-centering and lane-changing functions of a generalized Automation Level 3 highway chauffeur System,
- Improve understanding of how SOTIF analysis results may be validated, and
- Illustrate how SOTIF analysis might overlap with the concept phase of the functional safety process providing insights on how PAS 21448 and ISO 26262 can holistically assess the safety of new vehicle systems.

This project supports NHTSA's electronics reliability research[2] in several areas:

- This study builds the knowledge base of the current state-of-the-art safety analysis processes used for driving automation systems.
- This study provides an example for implementing SOTIF concepts, including identifying triggering events and mitigation measures, and describing different SOTIF evaluation strategies. The methods and results in the SOTIF example may also provide system developers insights for efficient and effective testing and evaluation methods.

This report describes research that applies concepts from PAS 21448 to two maneuvers, lane centering and lane changing, for a generic Level 3 highway chauffeur system. In order to conduct the analysis, this report developed a process that captures key steps from PAS 21448. This process was integrated with a similar process developed for functional safety analyses, conducted in accordance with the concept phase of the voluntary industry functional safety standard, ISO 26262. This study, furthermore, maps key parts from PAS 21448 to corresponding clauses from ISO 26262 to illustrate how these two safety approaches complement each other.

[1] ISO 26262: Road Vehicles – Functional Safety. This industry standard addresses hazards that could arise as the result of failures in E/E systems.

[2] NHTSA established the electronics reliability research area to study the mitigation and safe management of electronic control system failures and operator response errors.

By applying the SOTIF process to a "reference" SAE Level-3 highway chauffer system,[3] this study identified:

- Four potential vehicle-level hazards and five related safety goals,
- 59 potential triggering events related to sensor, algorithm, and other system limitations,
- 22 potential triggering events related to foreseeable misuse, and
- 126 example SOTIF mitigation measures.

To further assist in the SOTIF analysis, this study developed a preliminary list of scenario considerations based on Fatality Analysis Reporting System crash variables. These scenario variables were integrated into an operational design domain taxonomy developed by Thorne et al. (2018). This study found that FARS data is particularly useful for capturing non-typical roadway conditions related to the behavior of other drivers and roadway users—for instance, aggressive driving, swerving/swaying/fishtailing trailers, and non-motorists with low visibility or failing to have lights on. These scenario variables could supplement the list of considerations in Annex F of PAS 21448, and could assist in deriving SOTIF trigging events related to environmental conditions. For example:

- A common strategy for lane-centering maneuvers is to track a lead vehicle in the absence of suitable lane markings. Using FARS variables, this study identified a triggering event in which the system could track a lead vehicle that is driving erratically (swerving, not staying in the lane, etc.). A possible mitigation measure might be to confirm the lead vehicle's trajectory relative to surrounding landmarks to ensure that the trajectory is appropriate.
- FARS variables include a range of environmental effects, such as crosswinds. This helped identify a triggering event in which the camera sensor is not able to detect certain environmental conditions such as wind or black ice. A possible mitigation measure could be to monitor the error between the trajectory mapped by the steerable path algorithm and the actual vehicle path reported by the vehicle position algorithm.

This research helps advance automotive safety system analysis practices by applying the SOTIF concepts to a reference Level-3 Automated Driving System design.

Finally, this report reviews current SOTIF evaluation techniques and identifies potential data needs that could support these evaluation techniques.

[3] Note that the purpose of this study was to illustrate the SOTIF process and provide examples of the types of results that the SOTIF process may yield. The findings in this study are not intended to replace the system-specific analysis that would need to be applied to an actual system. Furthermore, the mitigation measures presented in this study are not intended to represent NHTSA's official position or requirements on highway chauffeur or similar systems.

1 Introduction

1.1 Project Background

Through the ISO, the automotive industry developed the voluntary standard ISO 26262 to address functional safety for safety-relevant automotive electrical and electronic systems. ISO 26262 focuses on mitigating potential hazards in systems in motor vehicles that result from E/E failures. Hazards that arise when the system is functioning correctly (i.e., there are no E/E failures) are not covered by the current ISO 26262 process and are not addressed by functional safety requirements. One such set of hazards may arise when driving automation systems develop an incorrect situational awareness (e.g., through sensor or algorithm limitations), and can affect both the system behavior as well as the system's interaction with the driver. The automotive industry developed a process, termed SOTIF, to address these hazards.

The objectives of this project are to:

- Understand the issues and current industry approaches to SOTIF,
- Provide an example application of SOTIF principles using lane-centering and lane-changing functions of a generic SAE Automation Level 3[4] highway chauffeur system,
- Understand the state-of-the-art of evaluating SOTIF analysis results, and
- Illustrate how SOTIF might overlap with the concept phase of the functional safety process.

This report reviews current concepts on the implementation of a SOTIF analysis, develops an example of how SOTIF mitigation measures might be developed for a generic Level 3 highway chauffeur system, and provides insight on how the safety analysis process developed through prior studies on functional safety might be adapted to reflect SOTIF considerations.

1.2 Analysis Scope

This project applied the SOTIF process to a generic Level 3 highway chauffeur system in a light vehicle.[5] In particular this project focuses on the lane-centering and lane-changing maneuvers to remain consistent with the scope of prior functional safety studies on automated lane-centering systems (Brewer et al., 2018).

This study only applied analytical aspects of the SOTIF process. No simulation or testing was performed during any part of this study.

[4] SAE Recommended Practice J3016 (*Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*) defines five levels of driving automation, ranging from Level 1 (driver assistance) to Level 5 (full driving automation) (SAE International, 2018). Level 0 is used to describe vehicles with no automation [30]. Level 3 systems are conditional driving automation where the system performs sustained lateral and longitudinal vehicle motion control and also performs OEDR functions . In Level 3 systems, a fallback-ready user (e.g., driver) is available to respond to requests to intervene and to respond to performance-relevant system failures in other vehicle systems .
[5] Light vehicles include passenger cars, vans, minivans, sport utility vehicles, and pickup trucks with a gross vehicle weight rating of 10,000 pounds or less.

2 Safety of the Intended Functionality Overview

The objective of SOTIF is to assure the absence of unreasonable risk due to hazards resulting from performance limitations affecting the specified behavior of a system or from reasonably foreseeable misuse by persons (ISO, 2019). The scope of SOTIF is further described as applying to situations where proper situation awareness, based on complex sensors and algorithms, is critical for safety. The SOTIF process covers two main categories.

The first area addresses situations that exceed the performance limitations of the system and components. This report defines this category as SOTIF Type I triggering events. This category includes both sensor limitations as well as limitations in algorithms, such as machine learning and neural net algorithms. For example, a Level 3 highway chauffeur system may be operating within its ODD (e.g., highway, good weather) but then encounter a roadway configuration with glare conditions. The resulting lighting conditions may exceed the performance limitations of a front-facing camera.

The second category contains human factor limitations, particularly in relation to the human-machine interface (HMI). This report defines this category as SOTIF Type II triggering events. In general, this area broadly covers several human factors issues, such as the driver failing to keep their hands on the steering wheel (where required); the driver's understanding of the system capabilities and limitations, and the driver's responsibilities; and the driver's ability to understand and respond to warnings and alerts.[6]

The subject matter experts (SMEs) interviewed for this project emphasized that SOTIF Type II triggering events do not extend to intentional abuse of the system, such as deliberately ignoring driver takeover requests or defeating driver monitoring systems (e.g., attaching an object to the steering wheel to defeat a sensor that detects the presence of the driver's hands).

2.1 Publicly Available Specification 21448

In 2019 ISO released PAS 21448 to describe SOTIF activities. PAS 21448 covers SAE Level 1 and 2 driving automation systems, but the concepts in PAS 21448 can be considered for ADS[7] (although additional measures may be necessary) (ISO, 2019). Until PAS 21448 is officially extended to cover ADS, each manufacturer can determine which aspects of the current PAS 21448 they want to incorporate into development of ADS.

The SOTIF PAS 21448 consists of 12 clauses, which are further broken down into sub-clauses. There are eight main clauses and four supporting clauses. The relationship between SOTIF activities are described in a flowchart in PAS 21448, which supports the iterative nature of SOTIF. One way to conceptualize SOTIF is using the four-quadrant diagram shown in Figure 1 (ISO, 2019).

[6] Note that for a Level 3 system, such as the one considered in this study, the driver is considered the user and may not be required to perform some tasks such as keeping their hands on the steering wheel.
[7] Automated driving systems is the term used in SAE J3016 to refer to Level 3 to 5 driving automation systems (SAE International, 2018).

Area 1 represents the known-safe scenarios. These are scenarios that the system is capable of handling safely. For instance, these scenarios may fall well within the ODD of the system or may represent scenarios that have already been addressed through existing countermeasures.

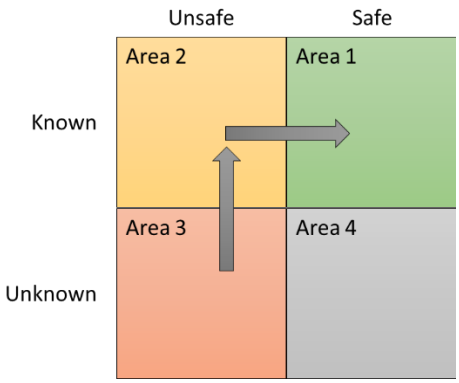

Figure 1. Four classifications of scenarios in SOTIF.

Area 2 represents known-unsafe scenarios. These are scenarios known to the system designers and under which the system cannot perform safely (e.g., the scenario exceeds the sensor limitations). SMEs provided several examples of how their organizations identify triggering events in Area 2, including:

- Analysis and guided brainstorming, using methods such as fault tree analysis, failure modes and FMEA, and systems-theoretic process analysis (STPA);
- Field data, such as accident analysis and reconstruction;
- Lessons learned from development and deployment of existing systems; and
- Existing guidance and codes of practice.

Manufacturers develop countermeasures, such as functional changes to the system or restriction of use cases, to address scenarios in Area 2 to reduce the overall risk of system use (see Section 7). As these measures are integrated into the system design and demonstrated to effectively mitigate the known-unsafe scenarios, these scenarios from Area 2 are reclassified under Area 1.

Area 3 represents unknown-unsafe scenarios. These are scenarios unknown to the system designers and under which the system cannot perform safely. SMEs indicated that unknown-unsafe triggering events are discovered through a combination of approaches, such as:

- Analysis and guided brainstorming, using methods such as FTA, FMEA, and STPA;
- On-road and track testing; and
- Simulation.

As manufacturers identify unknown-unsafe scenarios, these scenarios are then reclassified under Area 2. SMEs indicated that these different approaches are used in combination. For example, on-road testing is probabilistic (e.g., likelihood of encountering a particular combination of conditions). However, once on-road testing identifies a new type of scenario, permutations of this scenario can inform simulation testing. In general, Area 3 represents a core challenge in SOTIF and SMEs agreed that it is unlikely that Area 3 will be reduced completely (i.e., identification of all unknown-unsafe situations). Remaining unknown-unsafe scenarios would contribute to the residual risk in the system.

Area 4 represents unknown-safe scenarios. These are scenarios that the system can safely handle, for instance through existing countermeasures, even though they are unknown to the designers. The SOTIF process does not extend to trying to identify these scenarios.

2.2 Integration with Functional Safety Analysis

The core development processes in PAS 21448 (Clauses 5 through 12) and ISO 26262 (Parts 3 through 7) describe related activities. PAS 21448 presents one possible mapping between the ISO 26262 processes and the PAS 21448 activities (ISO, 2019). Glander presents a slightly different mapping between ISO 26262 and PAS 21448 (Glander, 2018). Figure 2 integrates information from these two sources to map the PAS 21448 clauses to relevant ISO 26262 sub-clauses. Specifically, Figure 2 maps each of the eight PAS 21448 core clauses to the V-model reference process model presented in ISO 26262 with the relevant sub-clauses.

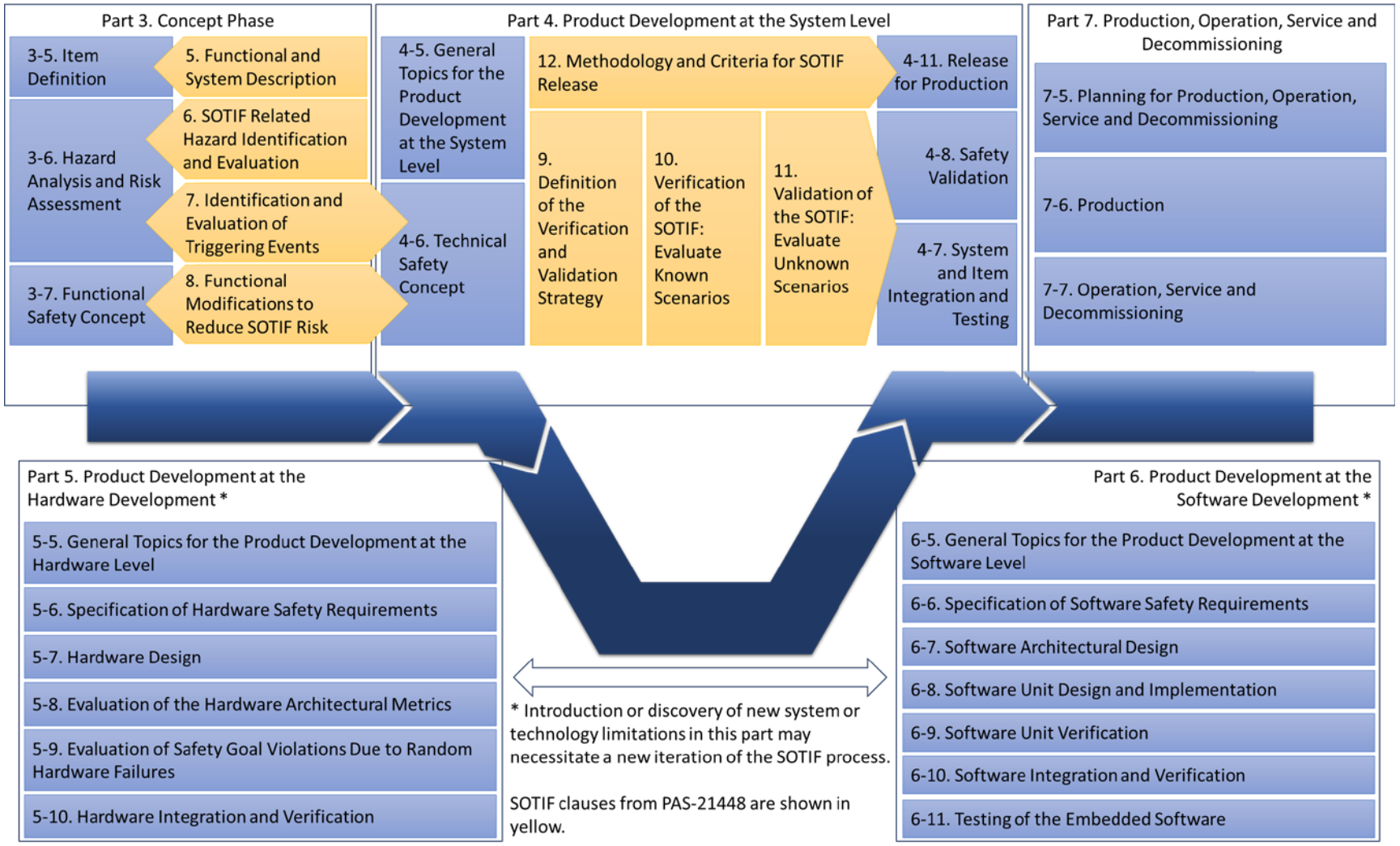

Figure 2. Possible mapping of clauses from SOTIF PAS 21448 to relevant parts and sub-clauses from ISO 26262.

As shown in Figure 2, the SOTIF clauses have strong overlap with ISO 26262 Parts 3 and 4, as suggested by Glander (2018). While Glander primarily maps the SOTIF PAS 21448 clauses to ISO 26262 Parts 3 and 4, the mapping to ISO 26262 presented in PAS 21448 extends the SOTIF clauses to the product development at the hardware and software level (Parts 5 and 6) (ISO, 2019). This research found that the preliminary SOTIF activities are aligned with ISO 26262 Parts 3 and 4, consistent with Glander. However, design implementation at the hardware and software level through ISO 26262 Parts 5 and 6 may introduce new system or technology limitations—for instance, as specific camera or radar sensors are selected. This may necessitate reapplying the SOTIF process to ensure that these new technology limitations do not lead to potential hazards. This is consistent with the iterative approach to SOTIF described by SMEs interviewed for this study.

ISO 26262, Part 3, is the Concept Phase, which includes activities such as item definition, hazard analysis, and risk assessment. The output of ISO 26262, Part 3, is the functional safety concept. The functional safety concept describes implementation-independent safety measures assigned to architectural elements that are necessary to achieve the safety goals (ISO, 2018). SOTIF does not produce a similar "safety concept" work product. Instead, SOTIF produces functional modifications that are measures developed to avoid, reduce, or mitigate SOTIF risks that result from system limitations that lead to safety violations (ISO, 2019). ISO 26262, Part 4, is the Product Development at the System Level, which decomposes the functional safety concept into the technical safety concept. ISO 26262, Part 4, also defines the validation and testing strategy, which is an important concept in the latter parts of SOTIF.

2.3 Integrated Analysis Approach

A safety analysis and safety requirements development process was developed and applied in prior research applying functional safety concepts to generic automotive electronic control systems (Brewer et al., 2018). Integrating the key SOTIF steps into this existing safety analysis process produced the updated safety analysis process shown in Figure 3. Note that each manufacturer may best decide how to integrate ISO 26262 and SOTIF activities, and Figure 3 is intended to show the process that was applied in this study.

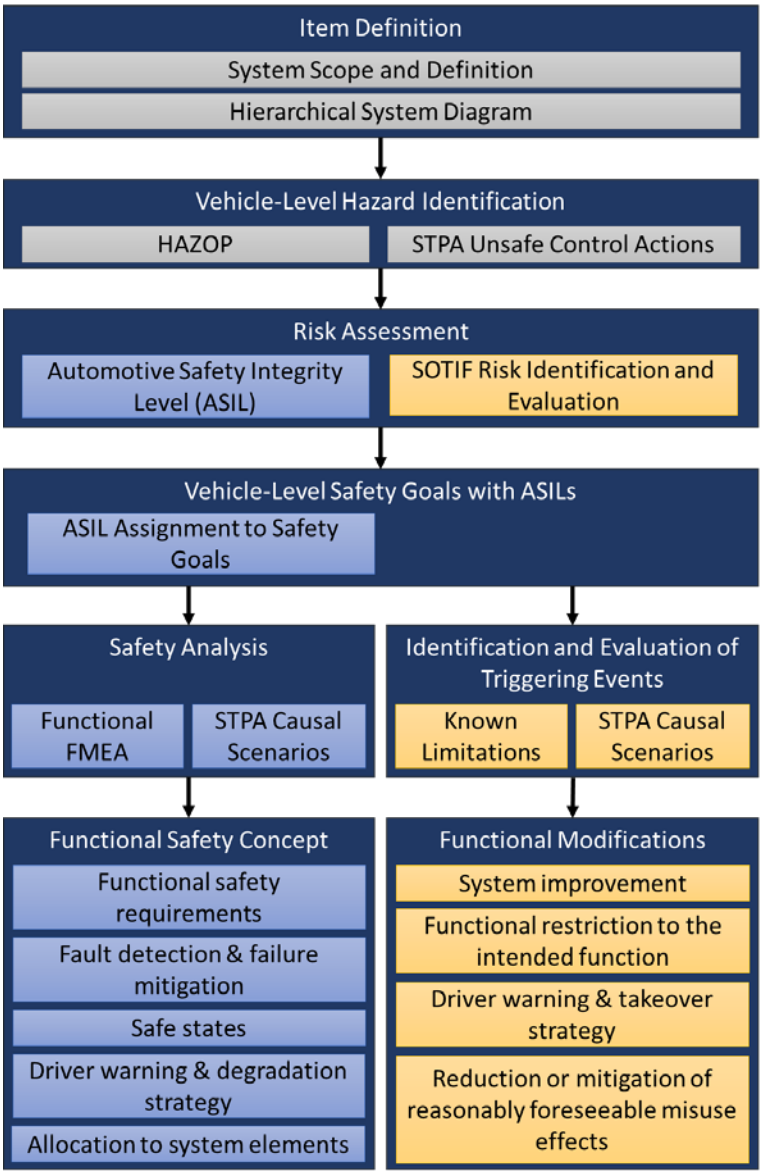

Figure 3. Updated safety analysis process integrating elements of the functional safety concept phase and SOTIF.

The steps in Figure 3 that are common to both the functional safety and SOTIF processes include:

1. Define the system by:
    - Documenting the system functions;
    - Establishing the system boundaries, including system interactions with other components and systems;
    - Identifying known system limitations; and

- Recording any assumptions about the system operation or configuration made when defining the system.

In particular, the system definition should specify the sensor types for the system and include a preliminary description of key algorithm functions. Note that the ISO 26262 item definition does not require specification of hardware or software components or technologies. However, this level of detail is necessary for the SOTIF analysis. A hierarchical system block diagram is developed to illustrate the system understanding and to assist in the analysis.

2. Identify vehicle-level hazards using both the hazard and operability study (IEC, 2001) and STPA methods (Leveson, 2012). The output of the hazard analysis step is a list of potential vehicle-level hazards. Hazards will be denoted as applying to functional safety, SOTIF, or both processes.
3. Conduct the risk assessment of the identified vehicle-level hazards. To the extent possible, the SOTIF and functional safety risk assessments can rely on similar operating situations. However, considerations such as the exposure assessment for the functional safety risk assessment may require varying the granularity of the operating situations.
    - For the functional safety part of the process, apply the ISO 26262 process to assign an Automotive Safety Integrity Level (ASIL) to each functional safety hazard as defined in ISO 26262.
4. Generate vehicle-level safety goals, which are top-level safety requirements based on the identified vehicle-level hazards. In general, the same safety goals may apply to both SOTIF and functional safety, although PAS 21448 does not require establishing safety goals for SOTIF.
    - For the functional safety part of the process, assign the ASIL associated with each functional safety hazard to the corresponding safety goal. If a safety goal applies to more than one vehicle-level hazard, the more stringent ASIL is applied to the safety goal (ISO, 2018).
5. Functional Safety – Perform safety analyses on the relevant system components and interactions as defined in the first step of this process. The safety analysis process uses both a functional FMEA (SAE, 1994) and STPA to complete the safety analysis.

   SOTIF – Identify Type I triggering events by assessing known sensor and algorithm limitations identified in Step 1 (Item Definition) and Type I and II triggering events by identifying STPA causal scenarios. Note that a single STPA assessment could extend across both the functional safety and SOTIF processes; those causal scenarios related to E/E failures can be allocated to functional safety and those causal scenarios related to foreseeable misuse and system limitations in the absence of E/E failures can be allocated to SOTIF.
6. Functional Safety – Follow the ISO 26262 process to develop the functional safety concept, including functional safety requirements at the system and component levels,

based on results from the functional FMEA and STPA, ISO 26262 guidelines, and industry practice experiences.

SOTIF – Develop functional modifications to reduce the SOTIF risk by following the steps described in PAS 21448, Clause 8.

Note that this study only applies the SOTIF-relevant steps shown in Figure 3 and described above.

3 SOTIF Scenario Development Framework

To support the SOTIF analysis and identification of Type I and Type II triggering events, this study extends a framework developed by Thorn et al. to characterize the ODD (Thorn et al., 2018). In addition, Annex F of PAS 21448 provides 8 categories of potential environmental conditions that could exacerbate system limitations and possibly trigger potentially hazardous behavior of the system (ISO, 2019). Scenarios are also an important element of the SOTIF evaluation strategies, as described in Section 8.1.

Glander suggests an approach to scenario development that imports and parameterizes real-world data to create scenario variables (Glander, 2018). The FARS coding variables could be one such publicly-available parameterization of factors contributing to real-world fatal crashes. The scenario framework presented in Appendix A uses the Thorn et al. (2018) taxonomy to categorize scenario factors presented in Annex F of PAS 21448 (ISO, 2019) and relevant parameters from the FARS user and coding manuals (NCSA, 2013, 2017). The FARS database provides coded variables based on decades of analyzing historical causes of fatal crashes. While FARS does not differentiate between human drivers and driving automation systems, the FARS variables still provide general insight into known challenging roadway conditions and behaviors that driving automation systems may need to navigate. In particular, FARS provides insight into behaviors of other drivers and roadway users that are common enough to warrant specific coding variables, including unconventional behavior (e.g., aggressive driving, disobeying signs or traffic controls).

This study developed a list of 210 variables categorized into 41 detailed subcategories that fit within the taxonomy. These variables are intended to help stimulate brainstorming to identify triggering events and scenarios, rather than to serve as a checklist or literal interpretation of variables. Furthermore, this framework is not intended to be complete, but rather could grow over time as new parameters are identified.

For some variables and situations, analysts may need to consider the appropriate "negative case" when applying the framework. For example, one variable is "pedestrians, pedal-cyclists, other non-motorist permitted in road." The corresponding "negative case" is that non-motorists are prohibited from using the roadway. Negative cases are not explicitly included in the framework. In other cases, multiple variables could be considered in conjunction to build a more complex scenario.

Table 1 provides an example of the expanded framework using roadway type variables from FARS. Appendix A provides the full framework. The scenario variables in Appendix A also include some variables from the Thorne et al. study that were not included in the FARS user and coding manuals (NCSA, 2013, 2017) or PAS 21448 Annex F (ISO, 2019).

Table 1. Example expanded SOTIF scenario taxonomy based on FARS and PAS 21448 parameters.

Top-Level Category	Immediate Subcategory	Detailed Subcategory	Scenario Variable
Physical Infrastructure	Roadway Type	Functional Class	Interstate
			Principal Arterial (Other Freeways/Expressways)
			Principal Arterial – Other
			Minor Arterial
			Major Collector
			Minor Collector
			Local
			Other
		Trafficway	Two-Way, Divided, Unprotected
			Two-Way, Divided, Positive Median Barrier
			Two-Way, Not Divided
			Two-Way, Not Divided, Continuous Left Turn Lane
			One-way Trafficway
			Non-Trafficway or Driveway Access

In order to organize the variables from FARS and PAS 21448 into a structure amenable to scenario construction, this study categorized each variable as either permanent-regional, permanent-local, a compounding event or condition, or a non-typical event or condition.

3.1 Permanent-Regional Variables

Permanent-regional variables are characteristics of the ODD and form the backdrop of scenarios. Permanent-regional variables do not change over time or over significant spatial portions of the trip. Examples of permanent-regional variables include roadway functional class, lane type, and permitted types of non-vehicle uses. Permanent-regional variables may be most amenable to geocoding because of their persistent and pervasive nature. This study identified 31 scenario variables in the permanent-regional category.

3.2 Permanent-Local Variables

Permanent-local variables persist over time, but are localized spatially. From a mobile frame of reference (e.g., a vehicle), permanent-local variables may only be encountered for brief portions of a trip. A vehicle may encounter multiple permanent-local variables over the course of a trip. Each combination of permanent-local variables may represent different variations of the backdrop defined by permanent-regional variables. Examples of permanent-local variables include curves, hills, bridges, and intersections. Since permanent-local variables are temporally

persistent, they could be geocoded—for instance, to inform vehicles of approaching intersections, tunnels, or other similar features. This study identified 45 scenario variables in the permanent-local category.

3.3 Compounding Events and Conditions

Compounding event and condition variables are temporary events or conditions that may occur within the scenario defined by permanent-regional and permanent-local variables. For a fixed point in space, compounding events or conditions are those aspects of the initial scene that can change. While a compounding event or condition may persist through an entire trip (e.g., rain), it is also possible for the same compounding event or condition to persist for only a portion of a trip (e.g., a short rain shower) or to change between trips (e.g., the weather may be clear one day and rainy the next). This study further defines compounding events or conditions as variables that are aspects of normal driving. This study identified 84 compounding event or condition variables.

3.4 Non-Typical Events and Conditions

Non-typical events and conditions are temporary events or conditions to which the system may need to respond. Unlike compounding events/conditions, this category represents unexpected behaviors or deviations from normal driving situations—for example, other vehicles disobeying signs or traffic controls or pedestrians darting out into the roadway. Threats may be static (e.g., a stalled or disabled vehicle) or dynamic (e.g., an aggressive driver). This study identified 50 non-typical event or condition variables.

Note that some variables categorized as compounding events and conditions could also be considered non-typical events and conditions—for instance, weather-related events that exist along a spectrum. Mild to heavy rain may be a compounding event or condition. However, a torrential downpour could also be considered a non-typical event or condition.

4 Generic Highway Chauffeur System Description

The first step in the SOTIF process is to establish the functional and system specification. According to PAS 21448 (ISO, 2019), the functional and system specification may include:

- Description of the system (e.g., goals, key functions, components);
- Use cases in which the system is activated or deactivated;
- Level of automation and authority over the system dynamics;
- Description of the system sensors, controllers, and actuators;
- Algorithm and sensor technology limitations;
- Dependencies or interactions with other vehicle systems and the surrounding environment;
- Assumptions on system inputs and outputs;
- Limitations and their countermeasures; and
- Degradation and driver warning strategies.

This study focuses on a generic Level 3 highway chauffeur system with the functionality and capabilities described in this section.

4.1 Functional Description

4.1.1 System Goals

Consistent with the definition of a Level 3 ADS, when engaged, the highway chauffeur system provides sustained lateral and longitudinal control in a restricted highway environment and is responsible for performing the object and event detection and response (OEDR) task (i.e., the system performs the complete dynamic driving task). The highway chauffeur system is expected to operate safely while traversing an optimal path (e.g., with respect to safety, speed, distance, and energy savings) to the desired destination (Watzenig & Horn, 2017). As a Level 3 ADS, the highway chauffeur does not need constant monitoring by the driver, but a takeover-ready driver is expected to be able to resume control after a sufficient transition period. The system is expected to continue to operate safely during this transition period.

This study specifically focuses on two tactical maneuvers of a Level 3 highway chauffeur system related to lateral control—lane centering and lane changing. Based on a study by Thorn et al. (2019), the relevant behavioral competencies for these maneuvers include:

- Lane centering;
- Lane switching, including overtaking or to achieve a minimal risk condition;
- Merge for high and low speed;
- Detect and respond to encroaching vehicles;
- Enhancing conspicuity (e.g., blinkers);
- Detect and respond to no passing zones;
- Detect and respond to lane changes, including unexpected cut-ins;
- Detect and respond to vehicle roadway entry; and
- Detect and respond to relevant adjacent vehicles.

4.1.2 Anticipated Use Cases

Level 3 highway chauffeur systems are designed to be activated on highways. Thorn et al. further specify the Level 3 highway chauffeur ODD as divided highways with clear lane markings (Thorn et al., 2018). Typically, these systems are not capable of navigating intersections, and therefore are further limited to use on restricted access highways.[8] A Level 3 highway chauffeur system also may not be capable of navigating certain features expected on a restricted access highway, such as toll plazas (Pegasus Projekt, n.d.). One SME provided tunnels and law enforcement checkpoints as additional highway features that a Level 3 highway chauffeur system may not be capable of navigating. The Pegasus Projekt team lists other potential limitations of the highway chauffeur, including navigating construction sites and operating in extreme weather conditions (e.g., low visibility, low traction).

The Pegasus Projekt team indicates that the highway chauffeur system would transfer control back to the human driver at highway junctions (Pegasus Projekt, n.d.). However, Thorn et al. (2018) suggest some highway chauffeur systems may be capable of merging at highway junctions. The highway chauffeur system considered in this study does not navigate on-ramps and off-ramps, or other highway junctions.

4.1.3 System Operation

The generic highway chauffeur system considered in this study would operate across the typical highway speed range (e.g., from 0 to 80 mph),[9] including bringing the vehicle to a complete stop (Pegasus Projekt, n.d.; Becker et al., 2017). The lane-centering feature controls the vehicle's lateral position to maintain the vehicle's position between the lane markers of the current travel lane. The highway chauffeur system requires clear lane lines to operate normally. In the absence of clear lane markings, the highway chauffeur system may use a lead vehicle or surrounding landmarks to maintain the vehicle's position in the lane until either the driver resumes control or the lane markings are re-established.

The lane-change feature allows the highway chauffeur system to steer the vehicle into a suitable space in an adjacent lane, if a lane change is necessary to achieve the system goals (e.g., to overtake a slower vehicle when conditions permit higher operating speeds). Prior to initiating a lane change, the highway chauffeur system monitors the target adjacent lane to determine if adequate free space is available. The system then engages the turn signal and executes the lane-change maneuver. Once the lane-change maneuver is complete, the highway chauffeur system transitions to the lane-centering maneuver in the new lane.

4.1.4 Authority over Vehicle Dynamics

The foundational vehicle systems provide actuation for the Level 3 highway chauffeur system. The propulsion and braking systems execute longitudinal commands by accelerating, decelerating, and braking the vehicle. However, the focus of this study is not on longitudinal motion.

[8] Restricted access is defined as having designated on- and off-ramp locations, with no at-grade intersections or access to abutting land use (e.g., driveways).

[9] The actual maximum allowable speed may differ between manufacturers, although in Becker et al. and Pegasus, the maximum speed referenced is 130 kilometers per hour (approximately 80 mph).

The steering system is the primary lateral control mechanism for the lane-changing and lane-centering tactical maneuvers of a Level 3 highway chauffeur system. The foundational steering system receives a torque request from the highway chauffeur system. The steering system then changes the orientation of the front road wheels to adjust the vehicle's heading.

Depending on the system design, the torque authority of the highway chauffeur system may be subject to torque limits. The torque limit may be established at a level that allows the driver to manually override the torque requested by the highway chauffeur system.[10] However, this torque limit may also limit the roadway curvatures where the system can operate. This study considers the highway chauffeur system to have full torque authority over the steering system, as long as the torque authority does not affect functional safety mitigation measures or safe states (as determined by applying ISO 26262).

4.1.5 Key System Dependencies

In addition to monitoring the statuses of the foundational systems described in Section 4.1.4, the Level 3 highway chauffeur system also relies on several in-vehicle sensors to provide important data regarding the host vehicle state. In particular, the system uses information from the yaw rate sensors and vehicle speed sensors.

The HMI is another key dependency of the Level 3 highway chauffeur system. The HMI allows the driver to engage or disengage the system. The HMI also provides relevant system notifications and alerts to the driver, including control transition notifications. Finally, the HMI incorporates any driver awareness monitoring subsystems, which are important for gauging the driver's attentiveness during transition of control between the system and driver.

Finally, the navigational system in the vehicle may be equipped with GPS and map information that is capable of providing additional input to the Level 3 highway chauffeur system about the host vehicle's location on the roadway. GPS and map information may be particularly important in enforcing geocoding for system operation.

4.2 System Description

4.2.1 Sensors

The vehicle sensors supporting the Level 3 highway chauffeur system is expected to be able to detect obstacles relevant to the system functions under the range of permitted use cases. The most challenging use case defines the sensor requirements (Becker et al., 2017). Object detection is expected to occur early enough such that the vehicle is able to safely execute the subsequent maneuver. For example, sensors is expected to detect the deceleration of a lead vehicle with sufficient time for the system to bring the host vehicle to a stop.

Cameras and radars are common sensors used for Level 3 highway chauffeur systems. LiDAR sensors have not yet reached widespread deployment on production vehicles, and therefore this

[10] Establishing a torque limit may be a functional safety mitigation measure to improve the driver's controllability in the event of an electronic failure that commands maximum steering torque. If the system incorporates such a functional safety mitigation measure as part of the functional safety concept, then it would be considered as part of the system limitations in SOTIF. This is one example of how the functional safety and SOTIF processes may influence each other.

study considers camera and radar as the primary sensors for the Level 3 highway chauffeur system.

4.2.1.1 Camera Sensor

Camera sensors typically face forward from behind the windshield. Rear-facing cameras may be useful for some driving automation systems, but are not considered for this study. System architectures may use a single camera (monoscopic) or dual cameras (stereoscopic) (Continental AG, 2017b, 2017c). Monoscopic camera systems can provide object detection, but typically do not support determining the distance to objects reliably. Stereoscopic cameras can support determining the distance to objects more reliably (Continental AG, 2017a).

Examples of typical camera limitations include:

- Low visibility conditions;
- Low contrast;
- Field of view limits; and
- Missing lane markings or landmarks.

4.2.1.2 Radar Sensor

Radars are typically located in the bumper at the front, rear, and four corners of the vehicle. For applications such as a Level 3 highway chauffeur system that performs lane changes, radars may also be located along each side of the vehicle to provide full coverage around the vehicle. Radar implementations may include short-range radar (e.g., 24 gigahertz range) used for detection of vehicles in adjacent lanes and long-range radar (e.g., 77 gigahertz range) used to detect objects in front of and behind the vehicle (Meinel & Bösch, 2017). In general, shorter radar ranges have wider detection fields and longer radar ranges have narrower detection fields. Radar can provide information on object range, angular position relative to the vehicle, and velocity.

Examples of typical radar limitations include:

- Field of view limits;
- Roadway curvature;
- Precipitation on the device cover; and
- Missing landmarks or vehicles.

4.2.1.3 GPS and Maps

GPS and maps supplement the other vehicle sensors to provide additional input to the system about the host vehicle's location. GPS uses signals from a constellation of satellites to provide the absolute position and velocity for the vehicle. The GPS information is paired with detailed maps to help determine where the vehicle is in relation to the roadway and other nearby features (e.g., on-ramps and off-ramps, merging lanes). This GPS information also supports geofencing, which could restrict system operation to certain roadway types that fall within the ODD. Depending on the precision of the GPS and detail of the maps, the system may be able to determine the vehicle's lane position, which could support the lane-centering and lane-changing maneuvers. However, standard commercial GPS precision is on the order 2 to 5 meters (Osterwood & Noble, 2017).

Examples of typical GPS and map limitations include:

- Physical blockage of the satellite signal (e.g., tunnels);
- Complex environments that reflect the satellite signal (e.g., urban canyons);
- Precision; and
- Accuracy of current map data.

4.2.2 Algorithms

There are different abstractions for representing the algorithms used for ADS,[11] such as a Level 3 highway chauffeur system. For instance, Watzenig and Horn (2017) categorize algorithms into three groups: localization and map building; environmental perception and modelling; and path planning and decision-making . The path planning and decision-making category is further decomposed into three steps: strategic planning, tactical planning, and reactive planning. Schubert and Obst (2017) describe four layers: sensing, perception, function, and actuation. The perception and the function layers are decomposed into two and four algorithm categories, respectively. Behere and Törngren (2017) provide a third representation, functionally decomposing the algorithms into three categories: perception, decision and control, and vehicle platform manipulation .

For the purposes of this study, the algorithms are grouped into two categories. Perception algorithms focus on ingesting raw sensor data to build a model of the environment. This may include elements such as sensor fusion, localization, and roadway modeling. Path planning algorithms determine a set of actions based on the environmental model constructed by the perception algorithms.

Examples of algorithm limitations include:

- Quality and accuracy of the raw sensor data,
- Robustness of the algorithm (e.g., quality and completeness of training data),
- Delays in obtaining sufficient sensor data to update models,
- The theoretical basis of the algorithm (e.g., the probability distribution assumptions, filtering methods),
- Considerations in calculating the confidence intervals and the acceptance limits, and
- Interpretation of complex environments (e.g., multiple vehicles in close proximity).

4.2.2.1 Perception

4.2.2.1.1 Sensor Fusion

The highway chauffeur system decision-making algorithms typically do not use the raw data from sensors. An intermediate processing layer integrates data from different sensor types (e.g., velocity from radar data and object classification from camera data) to create a more comprehensive understanding of the environment. The intermediate processing layer also helps reduce the effects of individual sensor errors, such as failure to detect an object or false detection of objects, and facilitates error estimation for individual sensors (e.g., by comparing data between sensors or against the model) (Schubert & Obst, 2017).

[11] The algorithms presented in this study are examples intended to illustrate the SOTIF process. Other possible decompositions and representations of algorithms exist.

The sensor perception algorithms considered in this study include:

- Lane Model – The lane model algorithm is responsible for receiving raw data on the lane markings and road edges from the camera sensor. The lane model algorithm processes this information to determine the lane and roadway boundaries.
- Fusion Tracker – The fusion tracker algorithm receives raw data from the vehicle sensors about objects in a defined boundary surrounding the vehicle. The fusion tracker also receives object classification data from the sensors. The fusion tracker combines the sensor data to create a fusion map that contains the instantaneous position of all detected objects within the defined boundary.

4.2.2.1.2 Localization

Localization is another set of algorithms employed by the highway chauffeur system. Localization refers to the process of determining the host vehicle position with respect to the roadway (Watzenig & Horn, 2017). Becker et al. describe three levels of precision for localization: roadway, lane, and sub-lane (Becker et al., 2017).

Roadway-level localization determines the roadway on which the vehicle is operating. Roadway-level localization may be useful for geofencing, for instance whether the driver should be able to engage the highway chauffeur system. Current map and GPS data are typically sufficient for roadway-level localization.

Lane-level localization determines which lane on the roadway the vehicle is currently occupying as well as information on adjacent lanes (e.g., are they viable travel lanes). Lane-level localization may be necessary for maneuvers such as lane changing (Becker et al., 2017). Highly detailed maps and accurate GPS may be able to provide this information, but are also data-intensive and may not be trustworthy (e.g., outdated). highway chauffeur systems may instead rely on on-board vehicle sensors, such as forward-facing cameras and radars, to perform lane-level localization.

Sub-lane-level localization determines the vehicle location within the travel lane, for instance to support lane centering (Becker et al., 2017). Similar to lane-level localization, highly detailed maps and precise GPS (e.g., centimeter-level precision) may support sub-lane-level localization. However, in the near-term, Highway Chauffeur systems would likely rely on on-board vehicle sensors as the primary mechanism for sub-lane-level localization.

Localization algorithms used in this study include:

- Host Vehicle State – The host vehicle state algorithm collects relevant data on the vehicle's operating state from other vehicle systems. This information includes vehicle speed, yaw rate, powertrain status, steering system status, and brake system status.
- Vehicle Position – The vehicle position algorithm compares GPS information with the road model developed by the road model algorithm using on-board vehicle sensors in order to determine the vehicle location and heading in the lane (lane-level localization). The vehicle position algorithm combines this information with the vehicle dynamics data provided by the host vehicle state algorithm to predict the vehicle's path. The vehicle position algorithm also provides relevant GPS data (e.g., roadway-level localization) for geofencing and other path planning or decision-making algorithms.

4.2.2.1.3 Environmental Model

Schubert and Obst (2017) describe how driving automation systems integrate sensor data to develop an environmental model that can be used for path planning and decision-making algorithms. The environmental model uses integrated perception to validate an *a priori* hypothesis about the environment. For instance, the system may use perception data to confirm that lanes follow an expected geometry (e.g., straight or curved) rather than try to determine the lane geometry from a set of all possible geometries.

In addition to detecting the current roadway environment, perception data is used by system algorithms to predict object behavior, for instance through object tracking. As an example of this approach, algorithms might assign a probability of existence to a detected object and develop a hypothesis about the object's behavior (Schubert & Obst, 2017). The algorithms then use data from each relevant sensor to update both the probability of existence and predicted object behavior.

As another perception strategy, the system might also classify areas that are free of objects as "free space." If the perception algorithms cannot reliably classify an area as either free space or occupied by an object, it may designate the area as "unknown" (Becker et al., 2017).

The environmental model algorithms used in this study include:

- Object Trail/Tracker – The object trail/tracker algorithm tracks the behavior of existing objects in the region of interest (e.g., velocity and object trail). For instance, the object trail/tracker algorithm may track the path of a lead vehicle to help the highway chauffeur system maintain its lane position in the absence of lane markings. The object trail/tracker may also help predict an object's likely future trajectory.
- Road Model – The road model integrates data from the other algorithms to develop a model of the surrounding environment. For instance, the road model classifies roadside objects, such as landmarks, barriers, and roadway signs. The road model projects the location of the lane in the roadway and populates the projection with identified objects, and their location, orientation, and speed.
- Free Space – The free space algorithm uses outputs of other algorithms to develop a grid map that predicts of areas that are free of objects, which can then be used for path planning.

4.2.2.2 Path Planning

The path planning algorithms use information from the perception algorithms to determine the behavior of the system based on the current driving situation (Becker et al., 2017). Path planning algorithms may be further categorized into several groups.

4.2.2.2.1 Situation Assessment

The situation assessment augments the environmental model with feature-specific goals and objectives. As described by Ulbrich et al., the environmental model generated by the perception algorithms may be independent of the system's goals and therefore contain more information than is immediately relevant to the driving situation (Ulbrich et al., 2015). For example, a highway chauffeur system operating in the left-most lane of traffic may track vehicles in the oncoming lane. However, since the highway chauffeur system considered in this study only operates on divided highways, this data may not be relevant to the driving situation.

4.2.2.2.2 Decision-making

Decision-making describes the process of using the information from the situation assessment to identify and select possible maneuvers to achieve the system goals. In addition to achieving the system goals, decision-making may also include behavioral reasoning (Watzenig & Horn, 2017). Becker et al. provide examples of factors that influence decision-making algorithm (Becker et al., 2017):

- Adapting the system operation based on current weather conditions. For instance, a highway chauffeur system may reduce its maximum operating speed in heavy fog that limits the vision range for the forward-facing camera. Different system architectures may impose different performance limitations, which in turn may affect the design of decision-making algorithms.
- Determining if a maneuver is necessary and can be performed safely. For instance, in order to achieve the system's objective of reaching the destination in an optimal manner the highway chauffeur system may decide to change lanes to pass a slower moving vehicle. The system might first need to ensure that there are no fast-approaching vehicles in the target lane and that the vehicle is not entering a curve that may limit the field of view (Becker et al., 2017).
- Following traffic rules and norms, such as maintaining the vehicle speed within posted limits and maintaining safe distances from other vehicles. This may also extend to driving conventions that are not immediately safety-critical. For instance, the Missouri driver education book states that "on a road with three or more lanes traveling in the same direction, stay in the right lane except to pass. If there is a considerable amount of traffic entering the right travel lane, then use the center travel lane" (Missouri Department of Revenue, 2018). To comply with this traffic norm, a highway chauffeur system might need to change back to the right-most lane after passing a slower vehicle or anticipate a heavy merge and move into the center lane.

In a Level 3 highway chauffeur system, the driver may also intervene and provide inputs directly to the foundational systems. This study considers one algorithm that monitors the driver's intent with respect to performing maneuvers, which factors into the overall system decision-making process.

- Driver intent – The driver intent algorithm evaluates the driver's inputs via the steering wheel and foot pedals to determine if the driver is attempting to resume driving manually. If the system determines the driver is performing a maneuver (e.g., evasive steering), the decision-making algorithm may suspend system operation or may support the driver's action, for instance by providing an assistive torque overlay.

4.2.2.2.3 Path Selection and Evaluation

Path selection refines the output of the decision-making step and generates the actual trajectory for completing a maneuver. Some maneuvers of a highway chauffeur system, such as lane centering and car following, may not have complex trajectories (or may not need trajectories at all) (Rupp & Stolz, 2017). Other maneuvers, such as lane changing, need to generate a specific trajectory that safely and smoothly moves the vehicle to the target lane.

Rupp and Stolz surveyed various control approaches for developing the trajectory for an ADS . A control algorithm may generate multiple possible trajectories. A common strategy when

selecting between potential trajectories is to minimize a cost function that typically incorporates elements such as obstacle avoidance, choice of lane, smoothness, desired longitudinal velocity, etc. This yields an optimal trajectory with respect to the elements in the cost function. Evaluation of different control strategies is out of scope for this project.

For the purposes of this study, the situation assessment, decision-making, and path selection and evaluation algorithms are combined into one algorithm:

- Steerable path – The steerable path algorithm uses the environmental model to determine a lateral trajectory[12] for the host vehicle based on the action selected by the system (lane centering or lane changing).

4.2.2.2.4 Motion Control

Once the highway chauffeur system selects a desired trajectory, the path is expected to be translated into lower-level commands for the foundational systems (i.e., braking, steering, and propulsion). This will depend on the selected model of vehicle dynamics as well as other particulars of the system design—for instance, which systems contribute to lateral control (e.g., steering only versus steering with active torque vectoring). One common approach is to implement lateral and longitudinal control as separate control algorithms in the controller, using the vehicle's current velocity as an input into the lateral control algorithm (Rupp & Stolz, 2017).

4.2.3 Degradation Concept

As a Level 3 ADS, the driver is the primary fallback measure for the system. However, in the event the vehicle encounters a scenario that exceeds the system limitations, the highway chauffeur system is expected to remain operational until the driver is able to resume control. If the system cannot operate with full capabilities, it may transition to a mode with reduced functionality until the driver can resume control.

Gauging the driver's reengagement with the driving task is important for a Level 3 highway chauffeur system in order to determine if the driver can safely resume control of the vehicle. One approach to monitoring driver engagement is to use inward-facing cameras to track the driver's gaze (Continental AG, 2017a). In order to alert and re-engage the driver, a Level 3 highway chauffeur system may apply an escalating series of alerts, such as those shown in Figure 4. In the event the driver does not resume control, the vehicle may transition into another fallback mode, such as stopping in the emergency lane.

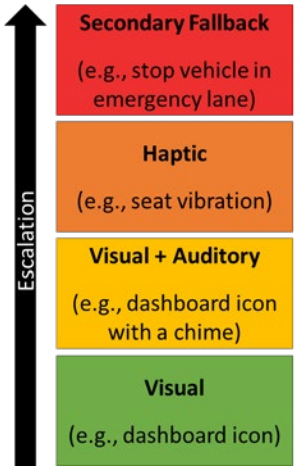

Figure 4. Example of an escalation strategy for alerts in a Level 3 Highway Chauffeur system.

The estimated time for driver takeover may vary depending on the specifics of the use case (e.g., vehicle speed, driver engagement). Becker et al. suggest an estimated 10- to 15-second driver takeover time for a Level 3 highway chauffeur system (Becker et al., 2017). This is consistent with other studies that suggest it takes approximately 10 seconds after an alert before the driver refocuses their attention on the roadway (Merat et al., 2014). However, there are

[12] As described in Section 4.4, this study assumes a constant longitudinal velocity for all maneuvers.

many factors that may affect the driver takeover notification time, and it is not the purpose of this study to establish takeover time values.

4.3 Functional Block Diagram

Figure 5 presents a hierarchical block diagram of the generic Level 3 highway chauffeur system considered in this study. The primary system components and algorithms are based on the system description provided in this section.

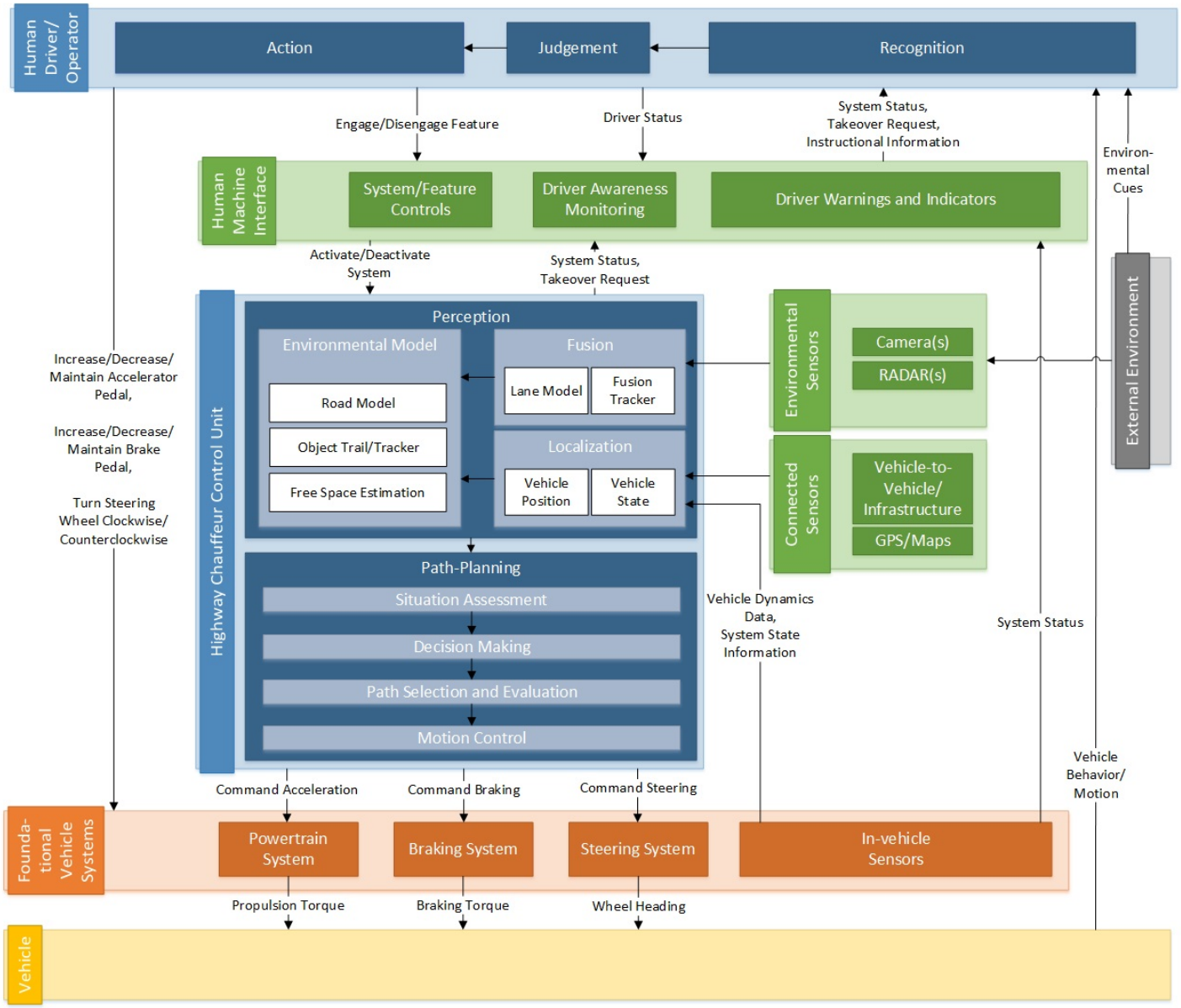

Figure 5. Block diagram of the generic Level 3 highway chauffeur system considered in this study.

4.4 Analysis Assumptions

In addition to the project scope described in Section 1.2 and the system description provided in Section 4, this analysis includes several assumptions regarding the operation of the generic Level 3 highway chauffeur system.

- Some architectures may expand the performance envelope of the system by combining active torque vectoring with steering (Meinel & Bösch, 2017). Torque vectoring may be accomplished through differentially braking or by differentially allocating propulsion torque to the wheels on the left and right side of the vehicle. In order to simplify the analysis, this study assumes that the steering system is the primary system that implements the highway chauffeur system's lateral control requests.
    - *Use of torque vectoring to supplement steering would require identification and evaluation of additional actuator-related triggering events.*
- Since this study only focuses on lateral control actions, lane-change maneuvers are assumed to be completed at constant speed.
    - *More complex lane-change maneuvers incorporating acceleration or deceleration would require additional analysis.*
- This analysis was performed on a generic Level 3 highway chauffeur system. Specific system design information, such as control algorithms or cost functions, were not available.
    - *The findings in this study represent an informative example of the SOTIF process, and do not replace a system-specific analysis.*
- The highway chauffeur system considered in this study does not navigate on-ramps and off-ramps, or other highway junctions (e.g., clover-leaf interchanges).
    - *Additional analysis of driving scenarios and potential triggering events would be necessary if the system's capabilities included navigating on-ramps, off-ramps, or other interchanges.*

5 Vehicle-Level Hazard Analysis

The next steps in the safety analysis process in Figure 3 are to identify the vehicle-level hazards, assess the risk associated with each hazard, and derive vehicle-level safety goals. A detailed description on using the STPA process for hazard identification is provided in Appendix B.

5.1 Possible Hazardous Events

SOTIF requires a systematic identification and evaluation of possible hazardous events. Hazardous events are a combination of a potential vehicle-level hazard and a credible operational situation. PAS 21448 provides the following example of a hazardous event for an automatic emergency braking system:

- Hazard: Unintended automatic emergency braking activation at x m/s^2 for y seconds.
- Operational situation: Operating on a highway.

5.1.1 Potential Vehicle-Level Losses

This study applied STPA to identify potential vehicle-level hazards associated with the lane-changing and lane-centering maneuvers of a generic Level 3 highway chauffeur system. The STPA process begins by identifying specific losses that the control system is trying to prevent. Since this project focuses on safety, the types of vehicle-level losses relevant to this study are vehicle crashes. A review of the crash type variable in the FARS coding manual revealed the following relevant crash types for the maneuvers considered in this study.

- Right/Left Roadside Departure
    - Driving off the road
    - From a control or traction loss
- Forward Impact
    - With a stationary object
    - With a pedestrian or animal
- Rear End
    - Lead vehicle is stopped
    - Lead vehicle is slower
    - Lead vehicle is decelerating
- Sideswipe/Angle
    - Host vehicle is going straight ahead (sideswipe from left or right)
    - Host vehicle is changing lanes to the left or right
- Head-on
    - Lateral move left/right

Since the system only operates on restricted access, divided highways, certain crash types are not applicable, such as forward impact with parked vehicles. The head-on crash type is not anticipated in the nominal case for divided highways, but may be applicable to reverse-lane operation, as described in Section 5.2.

5.1.2 Potential Vehicle-Level Hazard Identification

In the STPA model, losses may result from a combination of a vehicle-level hazard and worst-case environmental condition. The next step in the analysis is to identify potential vehicle-level hazards that could lead to one or more of the losses. This study develops STPA unsafe control actions to identify these potential vehicle-level hazards. The STPA UCAs are analogous to the potentially hazardous behaviors described in PAS 21448. Potentially hazardous behaviors are unexpected behaviors of the system as a result of the intended function or performance limitations that may lead to vehicle-level hazards.

To develop the UCAs, this study considers the following control actions issued by the Level 3 highway chauffeur system controller:

- Command an adjustment to change the vehicle's lateral position in the δ direction.[13]
- Command a lane change with constant speed.
- Issue a driver takeover request.

This study considers control actions at the maneuver level rather than at the foundational system command level (e.g., braking or steering commands). Since SOTIF assumes that the system is free of faults, the expectation is that the motion control algorithms will be able to correctly translate the maneuver into commands for the foundational vehicle systems. Analysis at the maneuver level more clearly illustrates the relationship between the triggering event and UCA.

In addition, this study evaluates possible driver interaction with the system by considering the following control actions taken by the human driver:

- Engage or disengage the Level 3 highway chauffeur system
- Provide a steering command
- Increase, decrease, or maintain the accelerator pedal position
- Increase, decrease, or maintain the brake pedal position

Each control action is considered in conjunction with relevant context variables and compared to the six UCA guidewords described in Appendix B. Analysis of the STPA UCAs identified the four potential vehicle-level hazards shown in Table 2.

Table 2. Potential vehicle-level hazards identified in this study.

Hazard ID	Hazard
H1	Lane or roadway departure while the system is engaged
H2	Lane change into an obstructed or occupied space in the target lane
H3	Vehicle does not complete the lane change (partially between lanes)
H4	System interferes with operation of a higher-priority safety-critical system

[13] Rather than duplicate the analysis for left and right lateral maneuvers, the variable δ is used to generally indicate the direction of the control action.

Initially, this study considered two additional potential hazards specifically related to foreseeable driver misuse—(1) improper transition of control between the driver and driving automation system, and (2) the driver unintentionally deactivating or overriding safety aspects of the system. Upon further evaluation and discussion, the analysts agreed that these potential hazards could instead be considered as categories of Type II triggering events that could lead to one of the other identified hazards.

SMEs interviewed for this study indicated that the SOTIF and functional safety processes could rely on the same set of potential vehicle-level hazards. This is consistent with the findings from this study; the four potential vehicle-level hazards shown in Table 2 are comparable to the types of potential hazards that would be identified through the functional safety process. A prior study applying the Part 3 of ISO 26262 to an ALC system identified hazards H1 and H4 (Brewer et al., 2018). The lane-changing maneuver was not considered as part of the prior study. The prior study also identified one additional hazard that was not relevant to SOTIF—unexpected loss of ALC. This hazard specifically relates to E/E failure of the system, and therefore is outside the SOTIF scope.

5.1.3 Relevant Operational Situations

In order to develop hazardous events, each vehicle-level hazard in Table 2 is considered in the context of operational situations. Operational situations are high-level scenarios that can occur during a vehicle's life, such as driving at high speed or parking on a slope (ISO, 2018). Consistent with the example provided in PAS 21448, operational situations do not include the potential causes of hazards (e.g., weather, behavior of other vehicles).

There is no standard approach in the automotive industry to identify operational situations. However, SAE Recommended Practice J2980 (SAE International, 2015) provides examples of variables to consider when developing operational situations for the ISO 26262 functional safety analysis. In the context of SOTIF, several of these variables represent triggering events that are considered later in the SOTIF analysis (e.g., road conditions, weather). Therefore, this study uses relevant permanent-regional variables from the framework provided in Appendix A to construct operational situations that are consistent with the level of detail provided in PAS 21448. The permanent-regional variables were selected because these variables describe the general roadway characteristics when the system could be activated, while providing a manageable number of operational situations to evaluate. Deviations or variations of these more general roadway characteristics (i.e., triggering events) are considered later in the analysis.

The specific permanent-regional variables considered to develop the operational situations are shown in Table 3 and denoted by a filled circle. Variables from each subcategory that are outside the ODD specified in Section 4.1 are denoted by an open circle in Table 3.

Table 3. Permanent-regional variables used to construct operational situations.

Immediate Subcategory	Detailed Subcategory	Permanent-Regional Scenario Variable	Considered for Operational Situations
Roadway Type	Functional Class	Interstate	●
		Principal Arterial (Other Freeways/Expressways)	●
		Principal Arterial – Other	●
		Minor Arterial	○
		Major Collector	○
		Minor Collector	○
		Local	○
		Other	○
	Trafficway	Two-Way, Divided, Unprotected	●
		Two-Way, Divided, Positive Median Barrier	●
		Two-Way, Not Divided	○
		Two-Way, Not Divided, Continuous Left Turn Lane	○
		One-Way Trafficway	●
		Non-Trafficway or Driveway Access	○
Roadway Surface and Features	Lane Type	Single Lane	●
		Multi-Lane	●
		Reversible Lane	●
		Shoulder Lane	●
		Managed Lane (high-occupancy vehicle, etc.)	●
	Surface Type	Concrete	●
		Blacktop, Bituminous, or Asphalt	●
		Brick or Block (including cobblestone/Belgian brick)	○
		Slag, Gravel, or Stone	○
		Dirt	○
Roadway/Lane Edges	Shoulder Type	Paved/Gravel	●
		Unpaved	●
Roadway Users	Other Non-Vehicle Users Permitted on Roadway	Pedestrian, Pedal-cyclist, Other Non-Motorist Permitted in Road	●

Immediate Subcategory	Detailed Subcategory	Permanent-Regional Scenario Variable	Considered for Operational Situations
Non-Roadway Users	Pedestrian Crosswalks/ Intersections	Crosswalks/Intersections Present in Roadway Type	○
	Other Users on Side of Roadway	Non-Motorists Permitted Along Roadway	●
Regions/States	Regional Traffic Laws	Special Regional Traffic Laws and Norms	○
	State Traffic Laws	Special State Traffic Laws and Norms	○
● – Variable considered in development of operational situations. ○ – Variable not considered in development of operational situations.			

The combinations of variables in Table 3 can be enumerated to create a comprehensive list of operational situations. Each operational situation can be assessed and the results logically reduced using techniques such the Quine-McCluskey minimization algorithm (Coudert, 1994). The operational situations can then be combined with the vehicle-level hazards to create hazardous events.

5.2 Risk Assessment

Once the hazardous events are identified, the next step in the SOTIF process is to conduct a risk assessment. Compared to the ASIL risk assessment process described in ISO 26262, PAS 21448 applies a more qualitative risk assessment. If the potentially hazardous event may lead to harm (i.e., severity parameter is non-zero; >S0)[14] and is not simply controllable (i.e., controllability parameter is non-zero; >C0),[15] then the hazardous event is considered through the SOTIF process. Unlike the ISO 26262 functional safety process, no ASIL is assigned to hazardous events in the SOTIF risk assessment process.

To the extent possible crash data was used to inform the risk assessments in Table 4 through Table 7. However, crash data could not be mapped directly to each hazardous event. For instance, the crash databases do not contain variables relating to managed lane types (e.g., HOV or reversible lanes). Crash data also does not explicitly differentiate between restricted access and unrestricted access roadways, and therefore cannot directly map to the system's ODD.[16]

[14] Severity is one dimension in the ASIL assessment process. PAS 21448 applies the ISO 26262 concept of severity to determine if a hazardous event may result in potential harm.
[15] Controllability is one dimension in the ASIL assessment process. A higher controllability number (e.g., C3) equates to a less-controllable situation. PAS 21448 applies the ISO 26262 concept of controllability to determine if a potentially hazardous event could be avoided easily. A hazardous event could result in potential harm, but because it is easily avoidable further assessment may not be necessary.
[16] Restricting the functional classification variable to interstate and principal arterial roadway types served as a proxy for restricted access roadways. However, not all principal arterial roads have controlled access.

Additionally, crash data considers a wider range of conditions and contributing factors other than those shown in Table 4 through Table 7.

In this study, the crash data from 2015 was used for a crude assessment of the maximum severity of a hazardous event to illustrate one possible approach for evaluating hazardous events. Crash data was filtered by the functional classification (FUNC_SYS) and trafficway description (VTRAFWAY) to approximate divided, restricted access roadways. Relevant precrash scenarios developed by Swanson et al. (in press) were used to approximate the hazard under consideration. Finally, the worst-case outcome was approximated using the crash type variable (ACC_TYPE). The injury severity variable (INJ_SEV) was used to determine if the combination of conditions could result in a non-zero severity.

Existing crash data also does not support the controllability assessment of hazardous events. Since this study considers a Level 3 ADS, the risk assessment used a conservative assumption that the driver was not engaged in the driving task and was unable to provide timely intervention to mitigate the hazardous events.

The current version of SOTIF PAS 21448 is only intended for Level 1 and Level 2 driving automation systems, where the driver is expected to be engaged in the driving task. Extension of the SOTIF PAS 21448 to higher levels of automation may require additional guidance for assessing controllability. For example, the controllability parameter may need to account for situations where the driver successfully re-engages with the driving task following an alert, situations where the driver unsuccessfully re-engages (e.g., is not situationally aware) or is otherwise unavailable (e.g., medical emergency), or the role of secondary fallback measures (if present) should the driver fail to resume control.

Table 4. Risk assessment of potential hazardous events for hazard H1: lane or roadway departure while the system is engaged.

Potential Hazardous Event	Potential Crash Type	Severity	Controllability
Vehicle departs the lane or roadway when traveling on a paved/gravel shoulder lane, with non-roadway users permitted on the side of the road.	Forward impact (pedestrian)	> S0	> C0
Vehicle departs the lane or roadway when traveling on a single lane roadway, with non-roadway users permitted on the side of the road.	Forward impact (pedestrian)	> S0	> C0
Vehicle departs the lane or roadway when traveling on a paved/gravel shoulder lane, with non-roadway users NOT permitted on the side of the road.	Right/left roadside departure (drive off road)	> S0	> C0
Vehicle departs the lane or roadway when traveling on a single lane roadway, with non-roadway users NOT permitted on the side of the road.	Right/left roadside departure (drive off road)	> S0	> C0
Vehicle departs the lane when traveling on a multi-lane roadway or in a managed lane (e.g., HOV lane).	Sideswipe (same direction, left/right)	> S0	> C0
Vehicle departs the lane when traveling in a reversible lane.	Head-on (lateral move left/right)	> S0[1]	> C0
[1] Crash data was not available to support this severity assessment, since reversible lanes are not explicitly identified in the crash databases.			

Table 5. Risk assessment of potential hazardous events for hazard H2: lane change into an obstructed or occupied space in the target lane.

Potential Hazardous Event	Potential Crash Type	Severity	Controllability
Vehicle changes lanes into an obstructed or occupied space when traveling on a single-lane roadway, with non-roadway users permitted on the side of the road.	Forward impact (pedestrian)	> S0[1]	> C0
Vehicle changes lanes into an obstructed or occupied space when traveling on a single-lane roadway, with non-roadway users NOT permitted on the side of the road.	Forward impact (stationary object)	> S0[1]	> C0
Vehicle changes lanes into an obstructed or occupied space when traveling on a multi-lane roadway or on a managed lane (e.g., HOV).	Rear-end (changing lanes to the right/left)	> S0	> C0
Vehicle changes lanes into an obstructed or occupied space when traveling on a paved/gravel shoulder lane.	Rear-end (changing lanes to the right/left)	> S0	> C0

Potential Hazardous Event	Potential Crash Type	Severity	Controllability
Vehicle changes lanes into an obstructed or occupied space when traveling in a reversible lane.	Head-on (lateral move left/right)	> S0[2]	> C0
[1] No data available for this crash type for the relevant pre-crash scenario (changing lanes). Non-zero severity is based on the analysts' judgement.			
[2] Crash data was not available to support this severity assessment, since reversible lanes are not explicitly identified in the crash databases.			

Table 6. Risk assessment of potential hazardous events for hazard H3: vehicle does not complete the lane change (partially between lanes).

Potential Hazardous Event	Potential Crash Type	Severity	Controllability
Vehicle does not complete the lane change and operates between lanes when traveling on a single-lane roadway, with non-roadway users permitted on the side of the road.	Forward impact (pedestrian)	> S0[1]	> C0
Vehicle does not complete the lane change and operates between lanes when traveling on a single-lane roadway, with non-roadway users NOT permitted on the side of the road.	Forward impact (stationary object)	> S0[1]	> C0
Vehicle does not complete the lane change and operates between lanes when traveling on a multi-lane roadway or on a managed lane (e.g., HOV).	Rear-end (stopped, slower, or decelerating vehicle)	> S0	> C0
Vehicle does not complete the lane change and operates between lanes when traveling on a paved/gravel shoulder lane.	Rear-end (stopped, slower, or decelerating vehicle)	> S0	> C0
Vehicle does not complete the lane change and operates between lanes when traveling in a reversible lane.	Head-on (lateral move left/right)	> S0[2]	> C0
[1] No data available for this crash type for the relevant pre-crash scenario (changing lanes). Non-zero severity is based on the analysts' judgement.			
[2] Crash data was not available to support this severity assessment, since reversible lanes are not explicitly identified in the crash databases.			

Table 7. Risk assessment of potential hazardous events for hazard H4: system interferes with operation of a higher-priority safety-critical system.

Potential Hazardous Event	Potential Crash Type	Severity	Controllability
System interferes with the operation of a higher-priority safety critical system (e.g., pedestrian avoidance or emergency steering) when the vehicle is traveling on a roadway that permits non-vehicles on the road.	Forward impact (pedestrian)	> S0	> C0
System interferes with the operation of a higher-priority safety critical system (e.g., electronic stability control) when the vehicle is traveling on a single-lane roadway or in a reversible lane, and non-vehicles are NOT permitted on the road.	Right/left roadside departure (control/traction loss)	> S0	> C0
System interferes with the operation of a higher-priority safety critical system (e.g., automatic emergency braking) when the vehicle is traveling on a multi-lane roadway or on a managed lane (e.g., HOV), and non-vehicles are NOT permitted on the road.	Rear-end (stopped, slower, or decelerating vehicle)	> S0	> C0
System interferes with the operation of a higher-priority safety critical system (e.g., automatic emergency braking) when the vehicle is traveling on a paved/gravel shoulder lane, and non-vehicles are NOT permitted on the road.	Rear-end (stopped, slower, or decelerating vehicle)	> S0	> C0

5.3 Example Safety Goals

PAS 21448 does not specify establishing safety goals for each vehicle-level hazard. In ISO 26262, safety goals represent a top-level safety requirement that become part of the safety concept. In contrast, SOTIF may result in functional modifications that could affect the item definition and result in an updated specification (e.g., the SOTIF process is iterated). Some SMEs interviewed for this study indicated that safety goals may also be applicable to SOTIF, while other SMEs indicated that safety goals are not applicable to SOTIF.

In this study, safety goals were derived from the vehicle-level hazards to provide traceability between SOTIF measures and the vehicle-level hazards those measures are intended to address. The process shown in Figure 3 derives a common set of safety goals for the functional safety and SOTIF processes. In the event a hazard only exists for the SOTIF process, deriving a safety goal may help ensure a complete set of top-level safety constraints for the system even though this step is not explicitly required in PAS 21448.

Possible safety goals for the potential vehicle-level hazards identified in this study are presented in Table 8.

Table 8. Possible vehicle-level safety goals derived from the identified hazards.

Related Hazard ID	Safety Goal ID	Possible Safety Goal
H1	SG1	Prevent lane departures while the system is engaged and executing a “lane-centering” maneuver for all ODDs.
H2	SG2	When executing a lane-change maneuver, ensure space in target lane is clear of vehicles and other obstacles adjacent to the host vehicle and TBD meters ahead of and behind the host vehicle for all ODDs.
H3	SG3	If the system is unable to complete a lane-change maneuver, safely return the vehicle to its original lane.
H1-H3	SG4	Alert the driver with sufficient takeover time (TBD seconds) prior to disengaging the system or exiting an ODD.
H4	SG5	Ensure the vehicle’s arbitration algorithm selects the highest priority system for safety.

The possible safety goals in Table 8 are consistent with the types of safety goals developed through the ISO 26262 functional safety process. For instance, safety goals SG-1 and SG-5 were also identified as possible safety goals in the functional safety assessment of a generic ALC system (Brewer et al., 2018). Of the SMEs that considered safety goals relevant to SOTIF, most agreed that the safety goals would be common to functional safety and SOTIF; one SME suggested that the safety goals derived through ISO 26262 might include statements about failure rates that would not be applicable to SOTIF. In these instances, it may be possible to derive a higher-level common safety goal, with sub-goals incorporating functional safety-specific failure rate information.

6 Example Triggering Events

After deriving the vehicle-level safety goals, the next step in the process shown in Figure 3 is to identify and evaluate triggering events. PAS 21448 describes two parallel approaches for identifying triggering events:

- Assess known limitations of system components to derive causal scenarios from those limitations that could potentially result in vehicle-level hazards.
- Assess environmental conditions and foreseeable misuse to derive causal scenarios that could potentially result in vehicle-level hazards.

This study applied both approaches to identify potential triggering events for the generic Level 3 highway chauffeur system. First the analysts identified the known limitations of the system sensors and algorithms (e.g., sensor field of view) and derived an initial set of potential triggering events. Next, the analysts applied STPA to identify additional causal scenarios. To identify possible Type I triggering events, analysts used the list of scenario variables in Appendix A to postulate potential causal scenarios that could lead to the UCAs identified in the hazard identification step (Section 5.1.2). To identify possible Type II triggering events, analysts used STPA to model the driver as a controller using the decision-making steps described in Annex E of PAS 21448.

Note although Figure 3 shows the safety analysis and identification and evaluation of triggering events as two separate steps, a single comprehensive assessment could extend across both the functional safety and SOTIF processes. Those causal scenarios related to electronic failures could be allocated to the functional safety process and those causal scenarios related to foreseeable misuse and system limitations can be allocated to SOTIF.

6.1 Type I Triggering Events

This study defines Type I triggering events as conditions that exceed the performance limitations of the system and components. These triggering events are specific to the technologies described in the functional and system specification. As described in Section 4, this study considers two primary vehicle-based sensors—camera and radar. These sensors are supplemented by GPS and maps. Finally, the system controller contains a set of perception and decision-making algorithms.

The Type I triggering events presented in this section are intended to illustrate the types of triggering events that could be identified through application of the SOTIF process to a generic Level 3 highway chauffeur system. These triggering events not intended to represent a complete set of all possible triggering events for a Level 3 highway chauffer system. Furthermore, the triggering events presented in this section are not intended to replace the system-specific analysis that would need to be performed for any systems under development.

6.1.1 Camera

This study identified 10 potential triggering events for the camera. These triggering events are listed in Table 9 along with the potential hazard or hazards that may result from the triggering event.

Table 9. Potential triggering events identified for the camera sensor.

Triggering Event ID	Triggering Event	Relevant Potential Hazard(s)
CS-1	The camera sensor may not detect the lane boundaries because the lane markings are partially or fully covered.	H1, H2, H3
CS-2	Obstructions may block the camera's view of lane markings, vehicles, or other objects.	H1, H2, H3
CS-3	The camera may have deteriorated performance in environmental conditions that reduce visibility, such as weather or low lighting.	H1, H2, H3
CS-4	Environmental noise factors, such as light reflection or shadows, may affect the camera's ability to detect lane markings, vehicles, or other objects.	H1, H2, H3
CS-5	The camera may not detect roadside landmarks, such as concrete barriers or guardrails, if there is low contrast between the landmarks and the roadway or other environmental features.	H1, H2, H3
CS-6	The camera may not detect lane markings if the lane markings have low contrast with the pavement or are below a minimum size or quality.	H1, H3
CS-7	The vehicle or object in an adjacent lane may be outside the camera's field-of-view.	H2, H3
CS-8	If lead vehicle tracking is used in the absence of clear lane markings, the lead vehicle may exceed the visual range of the camera.	H1
CS-9	The camera may have limitations individually tracking multiple objects that are close together and moving at similar speeds.	H2
CS-10	The camera may not be able to detect certain road surface or environmental conditions, such as black ice.	H1, H3

The majority of triggering events identified for the camera sensor focus on environmental and physical factors that affect the sensor's ability to detect lane markings, other vehicles and objects, and surrounding environmental features. One triggering event, CS-10, describes a limitation where the camera may not be able to detect certain roadway conditions because of limited visual cues.

6.1.2 Radar

This study identified 6 potential triggering events for the radar sensor. These triggering events are listed in Table 10 along with the potential hazard or hazards that may result from the triggering event.

Table 10. Potential triggering events identified for the radar sensor.

Triggering Event ID	Triggering Event	Relevant Potential Hazard(s)
RS-1	Water film on the radar antenna may lead to partial or total loss of the radar signal, particularly in the millimeter frequency range.	H1, H2, H3
RS-2	The roadway geometry, such as curvature or grade, may prevent the radar from correctly determining the distance to other vehicles, including the lead vehicle.	H1, H2, H3
RS-3	Reflective noise from the surrounding environment may degrade the signal quality or cause false signal detection.	H1, H2, H3
RS-4	The radar may not detect certain environmental features with sufficient confidence, such as guardrails.	H1, H2, H3
RS-5	The radar may not detect vehicles with thin profiles, such as motorcycles or bicycles, or objects below a certain size.	H2
RS-6	The radar may have limitations individually tracking multiple objects that are close together and moving at similar speeds.	H2

Four of triggering events identified for the radar sensor focus on environmental and physical factors that affect the sensor's ability to detect other vehicles and objects, and surrounding environmental features. Even if the radar does detect other vehicles, objects, or the surrounding environmental features, the system still might have low confidence in its detection or other limitations in discerning the vehicle, object, or environmental feature, as described in RS-4 and RS-6.

6.1.3 GPS/Maps

This study identified 4 potential triggering events for the GPS and map information. These triggering events are listed in Table 11 along with the potential hazard or hazards that may result from the triggering event.

Table 11. Potential triggering events identified for the GPS and maps.

Triggering Event ID	Triggering Event	Relevant Potential Hazard(s)
GM-1	A delay in the update rate for the vehicle location may cause the system to operate with an outdated host vehicle position in the lane.	H1, H2, H3
GM-2	The tolerance range for the host vehicle position may be too high causing the system to incorrectly determine the vehicle's travel lane or position in the roadway.	H1, H2, H3
GM-3	The GPS or map data may be out of date, causing the system to have an incorrect understanding of the roadway type, travel lanes, or vehicle position.	H1, H2, H3
GM-4	Information provided by the maps may be incorrect, causing algorithms to have an incorrect understanding of the roadway type or travel lane.	H1, H2, H3

Two of the GPS and maps triggering events (GM-1 and GM-2) describe short-term limitations that affect the accuracy of determining the vehicle's position on the roadway. The other two triggering events describe errors in the underlying data on which the GPS/maps are based. For instance, the maps may provide inaccurate data (e.g., incorrect coding by the map provider, outdated data) regarding roadway types or may not be updated to reflect lane closures.

6.1.4 Algorithms

The triggering events for the algorithms are categorized based on the nine algorithm types described in Section 4.2.2 and shown in Figure 5. In addition, this section also provides a general category of triggering events for highway chauffeur algorithms that do not fit into the other categories described in Section 4.2.2.

This study identified 7 potential triggering events for the lane model algorithm. These triggering events are listed in Table 12 along with the potential hazard or hazards that may result from the triggering event.

Table 12. Potential triggering events identified for the lane model algorithm.

Triggering Event ID	Triggering Event	Relevant Potential Hazard(s)
LM-1	The lane model algorithm may incorrectly determine the edges of features (e.g., Carny edge detection error).	H1, H2, H3
LM-2	The lane model algorithm may incorrectly interpolate data to determine the straightness of the lane lines (e.g., Hough transformation error).	H1, H2, H3
LM-3	The lane model algorithm may incorrectly determine the lane lines such that the perceived location infringes on adjacent lanes or is otherwise outside the current travel lane.	H1
LM-4	The lane model algorithm may incorrectly determine that the lane lines for the adjacent lane are closer to the current travel lane than they actually are (i.e., the adjacent lane is perceived as off-set toward the current travel lane).	H3, H6
LM-5	There may be a delay before the lane model algorithm updates incorrect lane line information with the correct lane line information.	H1, H2, H3
LM-6	The lane model algorithm may incorrectly categorize other roadway features, such as off-ramps or branching lanes, as a continuation of the current travel lane.	H1
LM-7	The lane model algorithm perceives other environmental features as the lane lines (e.g., skid marks, ghost markings, or other false positive lane marker detection).	H1, H2, H3

The lane model algorithm triggering events primarily focus on the ability of the system to correctly determine the boundaries of the current travel lane, or the boundaries of adjacent lanes for performing the lane-change maneuver.

This study identified 4 potential triggering events for the fusion tracker algorithm. These triggering events are listed in Table 13 along with the potential hazard or hazards that may result from the triggering event.

Table 13. Potential triggering events identified for the fusion tracker algorithm.

Triggering Event ID	Triggering Event	Relevant Potential Hazard(s)
FT-1	The fusion tracker algorithm may incorrectly combine camera and radar data from multiple objects (e.g., assign the incorrect velocity to an object in the adjacent lane).	H2, H3
FT -2	There may be a delay before the fusion tracker algorithm updates incorrectly associated object tracks from the camera and radar data.	H1, H2, H3
FT -3	The fusion tracker algorithm may not update the fusion map with sufficient frequency to capture maneuvers by other vehicles (e.g., double-lane change, high speed).	H2, H3
FT -4	The fusion tracker algorithm may incorrectly establish a vehicle in the target lane when no vehicle exists (false positive).	H3

The fusion tracker algorithm triggering events focus on the ability of the system to correctly combine camera and radar data (FT-1 and FT-2). This includes using the combined sensor data to record the presence of objects on the fusion map (FT-3). If the fusion tracker incorrectly combines data, it may also report objects that do not exist (FT-4).

This study identified 2 potential triggering events for the host vehicle state algorithm. These triggering events are listed in Table 14 along with the potential hazard or hazards that may result from the triggering event.

Table 14. Potential triggering events identified for the host vehicle state algorithm.

Triggering Event ID	Triggering Event	Relevant Potential Hazard(s)
VS-1	The vehicle state algorithms may have an incorrect model of the host vehicle size or configuration (e.g., attached trailer).	H2, H3
VS-2	The vehicle state algorithm has incorrect information leading to an incorrect time-to-collision calculation.	H2, H3, H6

The host vehicle state algorithm triggering events relate to the system's internal model of the vehicle configuration and its dynamics.

This study identified 2 potential triggering events for the host vehicle position algorithm. These triggering events are listed in Table 15 along with the potential hazard or hazards that may result from the triggering event.

Table 15. Potential triggering events identified for the host vehicle position algorithm.

Triggering Event ID	Triggering Event	Relevant Potential Hazard(s)
VP-1	The vehicle position algorithm incorrectly determines the host vehicle position in the lane.	H1, H2, H3, H6
VP-2	There may be a delay before the vehicle position algorithm updates an incorrect host vehicle position with the correct vehicle position.	H1, H2, H3

The host vehicle position algorithm triggering events relate to the system's lane-level or sub-lane-level localization model.

This study identified 9 potential triggering events for the object trail/tracker algorithm. These triggering events are listed in Table 16 along with the potential hazard or hazards that may result from the triggering event.

Table 16. Potential triggering events identified for the object trail/tracker algorithm.

Triggering Event ID	Triggering Event	Relevant Potential Hazard(s)
OT-1	In the absence of clear lane markings, the object trail/tracker algorithm may track the incorrect lead vehicle.	H1
OT-2	In the absence of clear lane markings, the object trail/tracker algorithm tracks a lead vehicle that is not staying centered in the travel lane (e.g., swerving, exiting roadway, changing lanes).	H1
OT-3	The object trail/tracker algorithm may have limitations differentiating between or tracking objects with similar speeds and that are close together.	H2, H3
OT-4	The object trail/tracker algorithm may incorrectly assign the track of an object to the incorrect lane (e.g., two lanes over instead of the adjacent lane).	H2, H3
OT-5	The object trail/tracker algorithm may incorrectly determine that a vehicle in the adjacent lane is changing to another lane (e.g., other vehicle aborts a lane change).	H2, H3
OT-6	The object trail/tracker algorithm may prematurely delete an object track or may not confirm a track for an existing object.	H2, H3
OT-7	If two objects or vehicles are close together and one object moves away (e.g., changes lanes), the object trail/tracker algorithm may incorrectly delete the track for the remaining object.	H2, H3
OT-8	The object trail/tracker algorithm may not detect an object moving in front of the host vehicle during a lane change.	H2, H3
OT-9	The object trail/tracker may not correctly detect or classify the entire vehicle or object (e.g., develops tracks for a truck cab but not a flatbed trailer).	H2, H3

The object trail/tracker algorithm triggering events primarily describe limitations in tracking other vehicles and objects (e.g., due to insufficient historical data or erratic behavior of other vehicles). One object trail/tracker algorithm triggering event further describes limitations in tracking the entirety of an object (OT-9). Two object trail/tracker algorithms relate to lead vehicle tracking (OT-1 and OT-2), which is performed when the system does not have sufficient confidence in the lane boundaries determined from lane marking data.

This study identified 4 potential triggering events for the road model algorithm. These triggering events are listed in Table 17 along with the potential hazard or hazards that may result from the triggering event.

Table 17. Potential triggering events identified for the road model algorithm.

Triggering Event ID	Triggering Event	Relevant Potential Hazard(s)
RM-1	In the absence of clear lane markings or landmarks, the road model algorithm incorrectly establishes the travel lane and/or the target lane.	H1, H2, H3
RM-2	The road model algorithm incorrectly estimates the road curvature and reports the incorrect curvature to the steerable path algorithms.	H1, H3
RM-3	There may be a delay before the road model algorithm updates incorrect lane boundary information with the correct lane boundary locations.	H1, H2, H3
RM-4	There may be a delay before the road model algorithm updates incorrect roadway curvature information with the correct roadway geometry.	H1, H2, H3

The road model algorithm triggering events relate to the system's environmental model, particularly as it relates to the current travel lane or target lane (i.e., for a lane-change maneuver).

This study identified 2 potential triggering events for the free space algorithm. These triggering events are listed in Table 18 along with the potential hazard or hazards that may result from the triggering event.

Table 18. Potential triggering events identified for the free space algorithm.

Triggering Event ID	Triggering Event	Relevant Potential Hazard(s)
FS-1	The free space algorithm may incorrectly determine the amount of free space in the target lane.	H2, H3
FS-2	There may be a delay before the free space algorithm updates incorrect free space information about the target lane with the correct data.	H2, H3

The free space algorithm triggering events relate to the system's determination of viable free space, specifically with respect to the target lane for a lane-change maneuver.

This study identified 3 potential triggering events for the driver intention algorithm. These triggering events are shown in Table 19 along with the potential hazard or hazards that may result from the triggering event.

Table 19. Potential triggering events identified for the driver intention algorithm.

Triggering Event ID	Triggering Event	Relevant Potential Hazard(s)
DI-1	The driver intention algorithm incorrectly assumes that the driver is attempting a maneuver and allows the host vehicle to get too close to other vehicles or objects on the roadway. There is a delay before the driver intention algorithm correctly determines that the driver is not performing a maneuver.	H2, H3
DI-2	The driver intention algorithm may incorrectly disregard an intended maneuver by the driver and instead maintain the vehicle on the trajectory computed by the steerable path algorithm.	H1, H2, H3
DI-3	The driver intention algorithm may incorrectly interpret a true steering input from the driver as incidental and therefore disregard an intended maneuver by the driver.	H1, H2, H3

The driver intention algorithm triggering events generally describe situations where the algorithm develops an incorrect model of the driver's behavior.

This study identified 2 potential triggering events for the steerable path algorithm. These triggering events are listed in Table 20 along with the potential hazard or hazards that may result from the triggering event.

Table 20. Potential triggering events identified for the steerable path algorithm.

Triggering Event ID	Triggering Event	Relevant Potential Hazard(s)
SP-1	The steerable path algorithm may have an incorrect model of the host vehicle trajectory (e.g., speed, yaw).	H1, H2, H3, H6
SP-2	The trajectory computed by the steerable path algorithm may become unviable partway through the maneuver.	H2, H3

In the first steerable path triggering event (SP-1), an incorrect model of the vehicle's current kinematics may affect the ability of the algorithm to compute the appropriate trajectory for the vehicle. The second steerable path triggering event (SP-2) identifies a condition where the roadway environment may change during a maneuver—for instance, during a lane-change maneuver, the lead vehicle in the target lane may brake suddenly reducing the amount of free space available in which to complete the maneuver.

6.1.5 General

In addition to triggering events for specific algorithms described in Section 6.1.4, this study also identified 4 potential triggering events that generally apply to the highway chauffeur system. These triggering events are listed in Table 21 along with the potential hazard or hazards that may result from the triggering event.

Table 21. Potential triggering events identified for the overall highway chauffeur system.

Triggering Event ID	Triggering Event	Relevant Potential Hazard(s)
HC-1	There may be a delay before the highway chauffeur system realizes that the foundational systems are not properly executing the commands to follow the charted trajectory.	H1, H2, H3
HC-2	The vehicle response may not correspond to the expected response by the path planning algorithm due to mechanical issues with the vehicle (e.g., worn tires).	H3
HC-3	The environmental or roadway conditions may change suddenly, causing the system to reach the limits of its ODD sooner than expected.	H1, H2, H3
HC-4	The highway chauffeur system may be incapable of safely bringing the vehicle to a stop in the middle of a maneuver.	H2, H3

The first two triggering events (HC-1 and HC-2) describe situations where the vehicle does not correctly execute the trajectory established by the steerable path algorithm. Even though the sensors and algorithms correctly establish a traversable trajectory, limitations in the actuation are also considered in SOTIF (ISO, 2019). The third triggering event (HC-3) broadly captures scenarios where the system may not be able to anticipate a change in the ODD, particularly affecting the ability of the system to provide the driver with an adequate transition time. This type of triggering event may be a core capability that requires detailed evaluation, particularly in situations where the driver is the only fallback. Similarly, in triggering event HC-4, the system may find itself in a scenario where the system may need to abort a lane-change maneuver, but cannot bring the vehicle safely to a stop. In this case, the system also may not be able to provide the driver with an adequate transition time.

6.2 Type II Triggering Events

The second category of triggering events contains human factor limitations, which this report defines as SOTIF Type II events. The first set of Type II triggering events are limitations in the HMI. These are potential limitations in system components, such as driver awareness monitoring or control transition algorithms. The remaining Type II triggering events relate to potential foreseeable misuse scenarios. These triggering events are based on the three decision-making process steps described in Annex E of PAS 21448, which in turn are based on the human factors analysis and classification system developed by Shappell and Wiegmann (2000).

6.2.1 Human-Machine Interface

This study identified 12 potential triggering events related to the HMI. These triggering events are listed in Table 22 along with the potential hazard or hazards that may result from the triggering event.

Table 22. Potential triggering events identified for the human-machine interface.

Triggering Event ID	Triggering Event	Relevant Potential Hazard(s)
HM-1	The highway chauffeur system may return control to the driver at the end of the control transition period, regardless of the driver's attention state.	H1, H2, H3
HM-2	The highway chauffeur system may return control to the driver in a driving situation that the driver cannot navigate or respond to in time.	H1, H2, H3
HM-3	The highway chauffeur system may delay transitioning control to the driver because it expects the environmental or roadway conditions to resolve, which may result in an insufficient transition time.	H1, H2, H3
HM-4	The highway chauffeur system may return control to the driver, but the foundational brake system may then respond to a request from another system.	H2
HM-5	The highway chauffeur system may return control to the driver, but the foundational powertrain system may then respond to a request from another system.	H2
HM-6	The highway chauffeur system may return control to the driver, but the foundational steering system may then respond to a request from another system.	H1, H2, H3
HM-7	The driver awareness monitoring subsystem may incorrectly gauge the driver's attention status.	H1, H2, H3
HM-8	If the driver awareness monitoring system cannot reliably determine the driver's level of engagement, then the system may not know the appropriate amount of transition time to provide the driver.	H1, H2, H3
HM-9	The driver may have difficulty accessing the system controls (e.g., if the system controls are located in sub-menus).	H2, H3
HM-10	The driver may lose access to the system controls because the console screen changes (e.g., passenger switches head unit screen to a media screen).	H2, H3
HM-11	The feature control may not provide any feedback to the driver when the system state is changed, affecting the driver's interaction with the controls.	H1, H2, H3
HM-12	The feature control may change or become disabled during the transition of control from the highway chauffeur system to the driver.	H2, H3

The first four triggering events (HM-1 to HM-4) describe instances where the highway chauffeur system incorrectly transitions control to the driver. Initially, this category of Type II triggering events was considered a separate hazard, as discussed in Section 5.1.2. However, upon further consideration, they were categorized as Type II triggering events that may lead to one of the identified vehicle-level hazards. Three triggering events (HM-5 to HM-7) also describe potential

confusion that may result during transition of control to the driver. In these triggering events the highway chauffeur system indicates the driver has control of the vehicle, but another safety system then actuates one or more of the foundational systems.

Two of the triggering events (HM-8 and HM-9) relate to the driver awareness monitoring subsystem, and four of the triggering events (HM-10 to HM-13) relate to the physical feature controls used to engage or disengage the system.

6.2.2 Driver Recognition

Recognition-based misuse scenarios in Annex E of PAS 21448 are akin to the perceptual errors described by Shappell and Wiegmann (2000). These misuse scenarios describe cases where the driver's perception of the environment differs from reality. Example guidewords for the recognition process provided in Annex E of PAS 21448 include "not understanding" and "false recognition."

This study identified 4 potential triggering events related to the driver's recognition process. These triggering events are listed in Table 23 along with the potential hazard or hazards that may result from the triggering event.

Table 23. Potential triggering events identified for the driver's recognition process.

Triggering Event ID	Triggering Event	Relevant Potential Hazard(s)
DR-1	The driver does not understand the system operation, including controls, warnings, system states, and control transition process and timing.	H1, H2, H3
DR-2	The driver may confuse actions taken by other vehicle systems, including warnings issued by other systems, with the behavior of the highway chauffeur system. As a result, the driver may interact with the highway chauffeur system controls rather than the controls of these other systems.	H3
DR-3	The driver does not have adequate situational awareness when requested to resume control.	H1, H2, H3
DR-4	In the absence of an alert, it may take longer for a disengaged driver to recognize that the highway chauffeur system is not going to respond appropriately to the driving scenario.	H1, H2, H3

The first driver recognition-related triggering event (DR-1) captures misuse scenarios based on the driver's incorrect understanding of the system capabilities and operation, system warnings, or expected driver actions. The second triggering event (DR-2) describes false recognition situations where the driver confuses other vehicle systems and the highway chauffeur system. Finally, two driver recognition-related triggering events (DR-3 and DR-4) relate to the driver's understanding of the roadway environment following a transfer of control from the highway chauffeur system to the human driver.

6.2.3 Driver Judgement

Judgement-based misuse scenarios in Annex E of PAS 21448 are akin to the decision errors described by Shappell and Wiegmann (2000). These misuse scenarios describe cases where the driver decides on an incorrect behavior for the given situation (e.g., a poor choice) . Example guidewords for the recognition process provided in Annex E of PAS 21448 include "judgement errors."

This study identified 3 potential triggering events related to the driver's recognition process. These triggering events are listed in Table 24 along with the potential hazard or hazards that may result from the triggering event.

Table 24. Potential triggering events identified for the driver's judgement process.

Triggering Event ID	Triggering Event	Relevant Potential Hazard(s)
DJ-1	The driver may choose to keep their hands on the steering wheel (or feet on pedals) in a manner that may unintentionally deactivate the system.	H2, H3
DJ-2	The driver may try to engage the highway chauffeur system while it is outside of the system ODD.	H1
DJ-3	The driver may decide to disengage the system when they are unable to safely control the vehicle (e.g., driver doesn't realize objects or vehicles are near-by).	H2

All three driver judgement-related misuse scenarios describe situations where the driver selects an action with an outcome that differs from the driver's expectation.

6.2.4 Driver Action

Action-based misuse scenarios in Annex E of PAS 21448 are akin to the skill-based errors described by Shappell and Wiegmann (2000). These misuse scenarios include attention errors, memory errors, or technique errors. Example guidewords for the recognition process provided in Annex E of PAS 21448 include "slip/mistake," "intentional," and "unable."

This study identified 3 potential triggering events related to the driver's action process. These triggering events are listed in Table 25 along with the potential hazard or hazards that may result from the triggering event.

Table 25. Potential triggering events identified for the driver's action process.

Triggering Event ID	Triggering Event	Relevant Potential Hazard(s)
DA-1	The driver may unintentionally deactivate the system by incorrectly interacting with the foundational systems (reflexively, intentionally, or accidentally).	H1, H2, H3
DA-2	The driver may unintentionally deactivate the system by incorrectly interacting with the feature controls in the head unit (intentionally or accidentally).	H1, H2, H3
DA-3	The driver may be incapacitated or otherwise unable to resume control of the vehicle at the end of the control transition period (e.g., medical emergency, asleep).	H1, H2, H3

The first two triggering events (DA-1 and DA-2) describe misuse scenarios where the driver unintentionally deactivates the system. If the driver is not situationally aware or ready to resume control, then this could affect their ability to safely control the vehicle. The third triggering event (DA-3) describes a situation where the driver is physically unable to resume control of the vehicle at the end of the control transition period.

6.3 Example Triggering Event Scenario Development

The appropriate level of detail for triggering events is not well specified in PAS 21448. The example in Annex A of PAS 21448 provides generalized triggering events that are consistent with the level of detail for the triggering events presented in Sections 6.1 and 6.2. For instance, Annex A provides an example triggering event: special road conditions can give radar echoes that could be interpreted as obstacles. In contrast, Clause 7, Sub-clause 7.2.2, provides a more detailed triggering event. The example in this clause is: heavy woolen coats can affect the performance of ultrasonic sensors (as opposed to more general wording such as "soft material").

The absence of clear guidance on the level of detail for triggering events presents a challenge—should the analysis comprise a more comprehensive set of high-level triggering events and defer specific scenarios to the evaluation (see Section 8), or should the analysis attempt to develop a set of detailed triggering events from among nearly infinite possibilities. One SME interviewed for this study indicated that their organization develops triggering events at both the general and specific level.

The higher level potential triggering events presented in Sections 6.1 and 6.2 could be refined to create more specific triggering events by using the scenario variables in Section 3. Table 26 provides an example of how the more general triggering events presented in this study could be refined into more detailed triggering events.

Table 26. Example of refining a generalized triggering event into detailed triggering events.

Generalized Triggering Event	Detailed Triggering Event
The camera may not detect lane markings if the lane markings have low contrast with the pavement or are below a minimum size or quality (CS-6)	The camera may not detect Bott's Dots or Cat's Eye lane markings.
	The camera may not detect non-traditional lane markings.
	The camera may not detect lane markings following a change in surface type from asphalt to concrete.
	The camera may not detect short lane markings in a construction or maintenance area.
	…

Alternatively, the triggering events can remain in a generalized form, and the variables presented in Appendix A can be used to construct detailed scenarios as part of the evaluation strategy, as described in Section 8.

7 Generic Mitigation Considerations

In order to develop possible SOTIF mitigation measures for the Level 3 highway chauffeur system, this study applied the mitigation strategies outlined in PAS 21448 to the triggering events in Section 6. The mitigation strategies in PAS 21448 include:

- Mitigation strategies based on functional restriction (ISO, 2019):
  - Restrict system operation or authority for specific use cases (e.g., degraded operation).
  - Prevent system operation for specific use cases.

- Mitigation strategies based on design improvement:
  - Improve algorithm performance.
  - Improve or diversify sensor technology.
  - Modify sensor locations.
  - Detect and react to sensor disturbances.
  - Recognize approaching limits of the ODD.
  - Improve actuator technology, including response, accuracy, durability, and authority capability.
  - Detect and respond to known unsupported use cases.
  - Mitigate and resolve functional interference or conflicts.
  - Improve system and component testability against known-unsafe scenarios.

- Mitigation strategies to improve (human) fallback operation and reduce foreseeable misuse:
  - Improve the HMI.
  - Improve the warning and degradation strategy.
  - Improve driver understanding of the system limitations.

7.1 Example Functional Restriction Mitigation Measures

One approach for developing SOTIF mitigations is to prevent the system operation for specific use cases. This approach may be useful for eliminating classes of triggering events (e.g., weather-related), or eliminating hazards and accident types. To illustrate this approach, Table 27 provides example mitigation measures based on further restricting the ODD for the system.

Table 27. Example mitigation measures based on functional restriction.

Mitigation Measure ID	Example Mitigation Measure	Relevant Safety Goals
MM-1	Prevent operation on reversible lanes that do not provide adequate physical barriers with on-coming traffic.	SG-1, SG-2, SG-3
MM-2	Prevent operation on roadways that allow non-motorists on the roadway or adjacent to the roadway.	SG-1, SG-2, SG-3, SG-5
MM-3	Prevent operations on roadways with no lane markings, inadequate landmarks, and no reliable lead vehicles to track.	SG-1

Two mitigation measures (MM-1 and MM-2) are derived from the risk assessment in Section 5.2 and can help eliminate potential crash types for the specified hazards. For instance, the system is intended for use on divided highways (Section 4.1.2). Divided highways might include reversible lanes that are separated from on-coming traffic by different types of barriers, which raises the possibility of head-on crash types. By restricting operation in reversible lanes to those lanes that are divided from on-coming traffic,[17] this could significantly reduce or eliminate the risk of head-on crash types. Similarly, certain restricted access roadways may allow non-vehicle use (e.g., interstates in rural areas).[18]

One challenge with mitigation strategies focused on restricting the ODD is that the driver may not always be aware of or fully understand these ODD restrictions. For instance, a foreseeable driver misuse scenario for the above reversible lane example is that the driver engages the system on an unsuitable reversible lane (DJ-2 in Table 24)—the driver may not know what constitutes a suitable barrier from on-coming traffic. It therefore becomes incumbent on the Level 3 highway chauffeur system to appropriately determine if the reversible lane falls within the allowable ODD (e.g., through a combination of GPS/maps and camera or radar data).

7.2 Example Design Improvement Mitigation Measures

Mitigation measures may also focus on design improvements that improve the system's ability to detect and respond to SOTIF triggering events. These measures might include ensuring a minimum confidence level in the output of a sensor or algorithm. In the example mitigation measures presented in this section, the confidence level is expressed as a key performance index. Other mitigation measures may help define performance boundaries for the sensors or algorithms, which in turn can help enable detection of scenarios that exceed these performance boundaries.

7.2.1 Sensor Mitigation Measures

In this study, sensors are assumed to only detect the surrounding environment and provide raw sensor data to the system algorithms. The algorithms are responsible for evaluating the reliability of the raw sensor data through sensor fusion and other modelling techniques. Therefore, considerations such as KPI do not exist at the individual sensor level; confidence in the raw sensor data is determined at the algorithm level. Additionally, sensors are expected to physically operate and provide data across the full range of environmental conditions. If certain environmental conditions sufficiently degrade the sensor data, this would again be determined by the algorithms.

This study identified 11 potential mitigation measures for the camera sensor. These mitigation measures are shown in Table 28.

[17] A more conservative approach may be to prevent operation on reversible lanes altogether.
[18] For example, the *Oregon Bicyclist Manual* (2016) specifies only portions of interstates where bicycle travel is prohibited.

Table 28. Example mitigation measures for the camera sensor.

Mitigation Measure ID	Example Mitigation Measure	Relevant Safety Goals
MM-4	Detect and distinguish individual vehicles, other road users, and other objects.	SG-1, SG-2, SG-3
MM-5	Detect vehicles, other road users, and other objects in the field-of-view and transmit the data to the control unit. a. Vehicles include large and small motor vehicles. b. Vehicles and objects may either be stationary or moving.	SG-1, SG-2, SG-3
MM-6	Detect vehicles, other road users, and other objects between a minimum of TBD meters from the vehicle to a maximum range of TBD meters from the vehicle.[19]	SG-1, SG-2, SG-3
MM-7	Provide a horizontal field-of-view that supports the maximum roadway curvature allowed in the ODD, including view of the adjacent lanes to the specified range. a. If the roadway curvature exceeds the camera horizontal field-of-view, notify the control unit.	SG-1, SG-2, SG-3
MM-8	Provide a vertical field-of-view that supports the maximum roadway grade allowed in the ODD. a. If the roadway grade exceeds the camera vertical field-of-view, notify the control unit.	SG-1, SG-2, SG-3
MM-9	Provide a field of view that supports the number of lanes and roadway width specified in the ODD.	SG-2, SG-3
MM-10	Minimize false positive or incorrect detection under the following conditions: full field-of-view blockage, partial field-of-view blockage, smeared spots, and blurred image conditions. a. If obstructions or other conditions reduce the camera's ability to detect objects, then notify the control unit.	SG-1, SG-2, SG-3
MM-11	Detect windshield camera obstructions. a. If an obstruction reduces the camera's ability to detect objects, then notify the control unit.	SG-1, SG-2, SG-3
MM-12	Detect the curvature of the roadway.	SG-1, SG-2, SG-3
MM-13	Operate in all road conditions, including partially covered lane markings, construction zones, areas with faded lane markings, multiple lane markings, or extraneous roadway markings. a. Report deteriorated functionality in these conditions to the control unit.	SG-1, SG-2, SG-3
MM-14	Operate in all weather conditions including rain, snow, fog, dust, sand, and smoke.	SG-1, SG-2, SG-3

[19] This range could be established iteratively to achieve the necessary performance requirements based on evaluation against plausible scenarios and on-road testing. An example range might extend from 0.5 meters to 60 meters from the vehicle.

This study identified 8 potential mitigation measures for the radar sensor. These mitigation measures are shown in Table 29.

Table 29. Example mitigation measures for the radar sensor.

Mitigation Measure ID	Example Mitigation Measure	Relevant Safety Goals
MM-15	Detect vehicles, other road users, and other objects in the region of interest and transmit the data to the control unit. a. Vehicles include large and small motor vehicles. b. Vehicles and objects may either be stationary or moving.	SG-1, SG-2, SG-3
MM-16	Detect all moving objects surrounding the host vehicle, including motorcycles, mopeds, bicycles, and similar objects.	SG-2
MM-17	Provide a vertical field-of-view that supports detection of vehicles and objects of varying heights above the road surface within the ODD.[20]	SG-2
MM-18	Detect guardrails, concrete barriers, and other lane or roadway boundaries, as well as roadside landmarks (e.g., traffic signs, telephone poles).	SG-1, SG-2, SG-3
MM-19	Minimize reporting of ghost objects.	SG-1, SG-2, SG-3
MM-20	Minimize false positive detection of objects.	SG-1, SG-2, SG-3
MM-21	Recognize conditions in which reliable detection of vehicles, other road users, and other objects on the roadway is not possible (high false detection possibility), and report “detection not available” to the control unit.	SG-1, SG-2, SG-3
MM-22	Operate in all weather conditions, including rain, snow, fog, dust, sand, and smoke.	SG-1, SG-2, SG-3

This study identified 5 potential mitigation measures for the GPS and maps. These mitigation measures are shown in Table 30.

Table 30. Example mitigation measures for the GPS and maps.

Mitigation Measure ID	Example Mitigation Measure	Relevant Safety Goals
MM-23	Update the vehicle position information every TBD seconds.	SG-1, SG-2, SG-3
MM-24	Locate the vehicle position to within TBD centimeters in the travel lane.	SG-1, SG-2, SG-3
MM-25	Verify the correctness of the GPS and map data by comparing the data to models produced by the system algorithms (e.g., vehicle position and road model).	SG-1, SG-2, SG-3
MM-26	Detect a loss of connectivity for a duration longer than TBD milliseconds. a. Report loss of connectivity to the control unit.	SG-1, SG-2, SG-3

[20] Note that this example mitigation measure could also be covered elsewhere, for instance in the object trail/tracker mitigation measures.

Mitigation Measure ID	Example Mitigation Measure	Relevant Safety Goals
MM-27	Verify the current map version on start-up of the vehicle. a. Operate at a reduced Level 2 functionality if the GPS/map system has not been verified in TBD days. b. Notify the driver of reduced functionality.	SG-1, SG-2, SG-3

7.2.2 Algorithm Mitigation Measures

The system algorithms evaluate the reliability of the raw sensor data through sensor fusion and other modelling techniques, and assign a confidence to the fused data or resultant model. Therefore, the algorithm mitigation measures feature a KPI threshold for this confidence. If the confidence in the algorithm output is below the KPI threshold for a specified duration, the system may begin implementing the degradation concept described in Section 4.2.3.[21] KPI can be established for true positives, true negatives, false positives, and false negatives.

This study identified 20 potential mitigation measures for the lane model algorithm. These mitigation measures are shown in Table 31.

Table 31. Example mitigation measures for the lane model algorithm.

Mitigation Measure ID	Example Mitigation Measure	Relevant Safety Goals
MM-28	Satisfy a true positive KPI of TBD percent to allow the system to operate. a. If the confidence metric is below this KPI, the system may continue to operate for TBD seconds by tracking lead vehicles or landmarks before transitioning control back to the driver. b. If the confidence metric is below this KPI, the system is to operate with restricted functionality by not allowing a lane-change maneuver until the confidence metric is above the KPI.	SG-1, SG-2, SG-3
MM-29	Satisfy a true negative KPI of TBD percent to allow the system to operate. a. If the confidence metric is below this KPI, the system may continue to operate for TBD seconds by tracking lead vehicles or landmarks before transitioning control back to the driver. b. If the confidence metric is below this KPI, the system is to operate with restricted functionality by not allowing a lane-change maneuver until the confidence metric is above the KPI.	SG-1, SG-2, SG-3
MM-30	Satisfy a false positive KPI of TBD percent to allow the system to operate. a. If the false positive KPI is not met at any time, transition control back to the driver.	SG-1, SG-2, SG-3, SG-4
MM-31	Establish minimum performance criteria for the edge detection function, such that combining the minimum criteria for the edge detection function with other lane model functions satisfies the true positive KPI.	SG-1, SG-2

[21] For example, the KPI threshold might be 98 percent confidence with an allowance of 1 second of operation below the KPI before initiating a control transition. Note that the KPI and associated duration for which the system can operate below the KPI threshold would need to be determined on a system-specific basis.

Mitigation Measure ID	Example Mitigation Measure	Relevant Safety Goals
MM-32	Establish minimum performance criteria for the line straightness function, such that combining the minimum criteria for the line straightness function with other lane model functions satisfies the true positive KPI.	SG-1, SG-2, SG-3
MM-33	Operate correctly (as measured by the true positive KPI) in the presence of double lane markings, where the distance between the markings is less than or equal to TBD centimeters.	SG-1
MM-34	Operate correctly (as measured by the true positive KPI) when the longitudinal distance between lane markings is less than or equal to TBD meters.	SG-1, SG-2
MM-35	Operate correctly (as measured by the true positive KPI) when the lane markings are greater than or equal to TBD centimeters in width.	SG-1, SG-2, SG-3
MM-36	Operate correctly (as measured by the true positive KPI) when at least TBD percent of the lane marking is visible.	SG-1, SG-2, SG-3
MM-37	Operate correctly (as measured by the true positive KPI) when the lane markings have TBD contrast ratio with the surrounding road surface.	SG-1, SG-2, SG-3
MM-38	Operate correctly (as measured by the true positive KPI) in lighting conditions of greater than or equal to TBD lux.	SG-1, SG-2, SG-3
MM-39	Operate correctly (as measured by the true positive KPI) when the lighting conditions change from any lux value to the minimum lux conditions within TBD milliseconds. a. This includes shadows, tree cover, and entering or exiting a tunnel.	SG-1, SG-2, SG-3
MM-40	Operate correctly (as measured by the true positive KPI) when the lane markings are not fully visible due to a camera lens blockage of less than or equal to TBD percent.	SG-1, SG-2, SG-3
MM-41	Operate correctly (as measured by the true positive KPI) in rain, snow, or other environmental conditions that are at or below the maximum acceptable noise limits for the camera. a. Establish the maximum acceptable noise limits based on the noise level that causes the KPI to drop below TBD percent with TBD frequency.[22]	SG-1, SG-2, SG-3
MM-42	Operate correctly (as measured by the true positive KPI) in the absence of lane markings that satisfy the minimum criteria for a distance of TBD kilometers if any of the following exist at a level that satisfies the lane model algorithm true positive KPI: a. Road edges that separate two different types of road surfaces. b. Curbs. c. Roadway barriers, including cement barriers or guard rails. If none of the above conditions exist and the lane markings do not satisfy the minimum criteria, initiate control transition to the driver.	SG-1, SG-3
MM-43	Correctly distinguish (as measured by the false positive KPI) between lane lines and lane boundaries, versus tire tread marks, shadows, and other extraneous road surface markings.	SG-1, SG-2, SG-3

[22] This may require data that maps the intensity of rain, snow, or other weather conditions to camera noise levels.

Mitigation Measure ID	Example Mitigation Measure	Relevant Safety Goals
MM-44	Track the correct lane markings for the vehicle's intended path when the lane markings diverge (e.g., exit ramp, branching road).	SG-1, SG-3
MM-45	Perform a plausibility check to ensure the target lane lines are correct prior to initiating a lane-change maneuver (e.g., by relying on data from the object trail/tracker or road model algorithms).	SG-3
MM-46	If the lane model algorithm is unable to operate within the ODD, send a "data not available" signal to the state manager.	SG-1, SG-2, SG-3
MM-47	If the lane model algorithm does not have the necessary data to operate, send a "data not available" signal to the state manager.	SG-1, SG-2, SG-3

This study identified 9 potential mitigation measures for the fusion tracker algorithm. These mitigation measures are shown in Table 32.

Table 32. Example mitigation measures for the fusion tracker algorithm.

Mitigation Measure ID	Example Mitigation Measure	Relevant Safety Goals
MM-48	Satisfy a true positive KPI of TBD percent for the fusion tracker algorithm input to the object trail/tracker algorithm.	SG-1, SG-2, SG-3
MM-49	Satisfy the true positive KPI when identifying a vehicle based on fused sensor data, or individual camera or radar data.	SG-1, SG-2, SG-3
MM-50	Incorporate the time duration a vehicle is assigned to a track when determining the true positive KPI.	SG-1, SG-2, SG-3
MM-51	Satisfy a true negative KPI of TBD (this is associated with the absence of a vehicle in the target lane).	SG-1, SG-2, SG-3
MM-52	Cross-reference the object detection and classification from the camera with object size and presence information from the radar.	SG-1, SG-2
MM-53	Update the fusion map at a minimum of TBD times per second (equivalent to TBD frames per second updates from the camera).	SG-2, SG-3
MM-54	Detect all objects within the region of interest, including the number of relevant lanes in the ODD, and update the fusion map accordingly.	SG-2, SG-3
MM-55	Distinguish between similar and dissimilar objects reported by the camera moving at the same speed (within +/- TBD kph) and at a distance greater than TBD meters.	SG-2, SG-3
MM-56	Distinguish between similar and dissimilar objects reported by the radar moving at the same speed (within +/- TBD kph) and at a distance greater than TBD meters.	SG-2, SG-3

This study identified 5 potential mitigation measures for the host vehicle state algorithm. These mitigation measures are shown in Table 33.

Table 33. Example mitigation measures for the host vehicle state algorithm.

Mitigation Measure ID	Example Mitigation Measure	Relevant Safety Goals
MM-57	Confirm the use of the primary (i.e., manufacturer default) vehicle configuration parameters file. a. Prevent activation if the system detects modifications to the vehicle dimensions (e.g., trailer attachment) or other modifications that block the sensors' field-of-view for the regions of interest.	SG-2, SG-3, SG-5
MM-58	Detect the addition to or connection of objects to the host vehicle that increase the total vehicle length by more than TBD centimeters.	SG-2, SG-3, SG-5
MM-59	Determine the vehicle speed to an accuracy of +/- TBD kph.	SG-2, SG-3, SG-5
MM-60	Perform a plausibility check of key host vehicle state parameters with the object trail/tracker and path planning algorithms.	SG-5
MM-61	Compare the time-to-collision computed by the highway chauffeur system with the TTC computed by higher priority vehicle systems.	SG-5

This study identified 4 potential mitigation measures for the host vehicle position algorithm. These mitigation measures are shown in Table 34.

Table 34. Example mitigation measures for the host vehicle position algorithm.

Mitigation Measure ID	Example Mitigation Measure	Relevant Safety Goals
MM-62	Detect the speed of the host vehicle to an accuracy of +/- TBD kph.	SG-1, SG-2, SG-3, SG-5
MM-63	Detect the host vehicle yaw rate to an accuracy of TBD radians per second.	SG-1, SG-2, SG-3, SG-5
MM-64	Ensure the correctness of the host vehicle position (e.g., by comparing the output of the vehicle position algorithm to the GPS and map data, and road model algorithm). a. If the correctness of the host vehicle position cannot be determined, the system is to operate at reduced functionality by restricting lane changes. b. If the correctness of the host vehicle position cannot be determined for more than TBD seconds, transition control to the driver.	SG-1, SG-2, SG-3, SG-5
MM-65	Update the host vehicle position with a frequency of TBD seconds.	SG-1, SG-2, SG-3, SG-5

This study identified 15 potential mitigation measures for the object trail/tracker algorithm. These mitigation measures are shown in Table 35.

Table 35. Example mitigation measures for the object trail/tracker algorithm.

Mitigation Measure ID	Example Mitigation Measure	Relevant Safety Goals
MM-66	Satisfy a true positive KPI of TBD percent for associating objects with tracks in order to allow the system to operate. a. If there is a hysteresis time[23] for the true positive KPI, establish the hysteresis time to allow sufficient time to transfer control to the driver.	SG-1, SG-2, SG-3
MM-67	Satisfy a false positive KPI of TBD percent in order to allow the system to operate.	SG-1, SG-2, SG-3
MM-68	Do not delete an object track unless the true negative KPI of TBD is met.	SG-2, SG-3
MM-69	Confirm the fusion tracker input satisfies the true positive KPI of TBD percent in order to operate.	SG-1, SG-2, SG-3
MM-70	Identify and track the lead vehicle to a distance up to TBD meters.	SG-1
MM-71	Follow the lead vehicle maintaining a vehicle centerline offset of no more than TBD centimeters.	SG-1
MM-72	Communicate the lane boundaries determined from the lead vehicle trajectory to the path planning algorithms.	SG-1
MM-73	Confirm the lane boundaries determined from the lead vehicle trajectory against the host vehicle lane boundaries determined by the road model algorithm. a. If the lane boundaries do not align by +/- TBD centimeters for more than TBD seconds, transition control to the driver.	SG-1, SG-2
MM-74	Identify and track vehicles in the adjacent lanes on either side of the host vehicle's current travel lane (if the lanes exist), and other lanes as appropriate to satisfy the lane-change maneuver.	SG-1, SG-2, SG-3
MM-75	Differentiate between similar and dissimilar objects that are moving at a differential speed from each other at greater than TBD kph and separated by a distance greater than TBD meters.	SG-2, SG-3
MM-76	Do not delete an object track until the hysteresis time elapses.	SG-2, SG-3
MM-77	If an object was tracked and deleted, and is tracked again within TBD seconds (e.g., a vehicle aborting a lane change), build the confidence metric on previously established data. a. Object track history may need to be maintained for TBD seconds to support this.	SG-2, SG-3
MM-78	Detect and track objects that are moving at a differential speed up to TBD kph.	SG-2, SG-3
MM-79	Establish a spatial region of interest that supports returning to the original lane in the event of an aborted lane-change maneuver.	SG-2, SG-3
MM-80	Detect and track objects that move within the region of interest and ODD, regardless of the object's travel lane.	SG-2, SG-3

[23] Due to the probabilistic nature of the perception functions, a hysteresis time allows the confidence metric to temporarily drop below the KPI without triggering the degradation strategy. This filters out transition effects and false instantenous measurements.

This study identified 5 potential mitigation measures for the road model algorithm. These mitigation measures are shown in Table 36.

Table 36. Example mitigation measures for the road model algorithm.

Mitigation Measure ID	Example Mitigation Measure	Relevant Safety Goals
MM-81	Satisfy a true positive KPI of TBD percent for locating the host vehicle in the travel lane in the absence of a lead vehicle or road markings in order to allow the system to operate. a. If there is a hysteresis time[24] for the true positive KPI, establish the hysteresis time to allow sufficient time to transfer control to the driver.	SG-1, SG-2, SG-3
MM-82	Compare the output from radar and camera data to the output of the GPS/maps and vehicle position algorithm. a. Consider the results of this comparison in the true positive KPI confirmation.	SG-1, SG-2, SG-3
MM-83	Detect unsupported roadway conditions, and report such conditions to the highway chauffeur decision making algorithm. a. Unsupported roadway conditions include the absence of lane markings and surrounding landmarks.	SG-1, SG-2, SG-3
MM-84	Detect and confirm the curvature of the road (e.g., through plausibility checks based on the tracks of other vehicles or landmarks).	SG-3
MM-85	Track the location of roadway shoulders and emergency breakdown lanes to support a safe state that includes moving the vehicle out of traffic.	SG-1, SG-2, SG-3, SG-5

This study identified 3 potential mitigation measures for the free space algorithm. These mitigation measures are shown in Table 37.

Table 37. Example mitigation measures for the free space algorithm.

Mitigation Measure ID	Example Mitigation Measure	Relevant Safety Goals
MM-86	Satisfy a true positive KPI of TBD percent for determining the size and occupancy status of a space in the target lane in order to allow a lane-change maneuver.	SG-2
MM-87	Ensure the object trail/tracker algorithm KPI is satisfied before allowing a lane-change maneuver.	SG-2
MM-88	Update the free space at the same rate as the fusion tracker algorithm (TBD times per second).	SG-2

This study identified 9 potential mitigation measures for the driver intention algorithm. These mitigation measures are shown in Table 38.

[24] Due to the probabilistic nature of the perception functions, a hysteresis time allows the confidence metric to temporarily drop below the KPI without triggering the degradation strategy. This filters out transition effects and false instantaneous measurements.

Table 38. Example mitigation measures for the driver intention algorithm.

Mitigation Measure ID	Example Mitigation Measure	Relevant Safety Goals
MM-89	Satisfy a false negative KPI of TBD percent.	SG-1, SG-2, SG-3
MM-90	Determine the likelihood that the driver intentionally intends to regain control of the vehicle or execute a maneuver when one or more of the foundational systems are operated.	SG-1, SG-2, SG-3
MM-91	If the driver intention algorithm true positive KPI is not met when the driver actuates one or more foundational systems, communicate via audible and visual messages to the driver that a foundational system is actuated, and request confirmation that the driver is requesting to take control. a. If the driver continues to actuate the foundational system, and does not respond to the driver intention module's request for confirmation, move the vehicle out of traffic, bring the speed to zero, place the vehicle in park, and turn on hazard light indicators.	SG-1, SG-2, SG-3
MM-92	Satisfy a true positive KPI of TBD percent when determining the intention of the driver to take control or execute a maneuver based on the actuation of one or more of the foundational systems.	SG-1, SG-2, SG-3
MM-93	Immediately transfer control back to the driver if the true positive KPI is met under all operating conditions.	SG-1, SG-2, SG-3
MM-94	Request confirmation from the driver that a maneuver is being executed if the true positive KPI falls between TBD and TBD percent. a. If the driver confirms an intended maneuver, immediately transfer control back to the driver.	SG-1, SG-2, SG-3
MM-95	Immediately transfer control back to the driver if the steering input from the driver exceeds TBD Newton-meters.	SG-1, SG-2, SG-3
MM-96	Request confirmation from the driver that a maneuver is being executed if the steering input from the driver falls between TBD and TBD Newton-meters. a. If the driver confirms an intended maneuver, immediately transfer control back to the driver.	SG-1, SG-2, SG-3
MM-97	Relinquish control to the driver, but issue an audio or visual warning, if the driver confirms the intent to take control but the driver's input is potentially unsafe for the roadway environment.	SG-1, SG-2, SG-3

This study identified 4 potential mitigation measures for the steerable path algorithm. These mitigation measures are shown in Table 39.

Table 39. Example mitigation measures for the steerable path algorithm.

Mitigation Measure ID	Example Mitigation Measure	Relevant Safety Goals
MM-98	Verify that the lane model or road model (or both) algorithm satisfies its respective true positive KPI for the roadway environment.	SG-1, SG-2
MM-99	Verify that the vehicle position algorithm satisfies its true positive KPI.	SG-1, SG-2
MM-100	Abort the lane-change maneuver and safely return the vehicle to its original lane in the event any of the following conditions occur: a. The steerable path algorithm becomes unavailable. b. The confidence metric for the charted trajectory (as determined by the vehicle position, lane model, or road model algorithms) drops below the KPI. Communicate the host vehicle status to other vehicle systems as required by the vehicle system architecture, and communicate to the driver that the system aborted the lane-change maneuver.	SG-2, SG-5
MM-101	Monitor the error between the trajectory mapped by the steerable path algorithm and the actual vehicle path reported by the vehicle position algorithm (e.g., comparing the host vehicle state algorithm and path planning algorithm). a. If the error exceeds a safe limit of TBD percent, then transition control to the driver.	SG-1, SG-2, SG-3

7.2.3 Other Design Improvement Mitigation Measures

In addition to the potential mitigation measures for specific sensors and algorithms, this study identified potential mitigation measures that address some of the general Type I triggering events in Section 6.1.5.

This study identified 9 potential mitigation measures for the actuating foundational systems and other interfacing systems. These mitigation measures are shown in Table 40.

Table 40. Example mitigation measures for the actuating foundational systems and other interfacing systems.

Mitigation Measure ID	Example Mitigation Measure	Relevant Safety Goals
MM-102	Include the highway chauffeur input as part of the steering system controller arbitration strategy.	SG-1, SG-2, SG-3
MM-103	Use the necessary host vehicle state algorithm data in the steering system control strategy when the highway chauffeur system is activated.	SG-1, SG-2, SG-3
MM-104	Provide a steering response within +/- TBD radians per second from the time of the steering request from the highway chauffeur system. a. Report to the highway chauffeur system if the response is outside this threshold.	SG-1, SG-2, SG-3
MM-105	Include the highway chauffeur input as part of the brake system controller arbitration strategy.	SG-1, SG-2, SG-3
MM-106	Use the necessary host vehicle state algorithm data in the brake system control strategy when the highway chauffeur system is activated.	SG-1, SG-2, SG-3
MM-107	Report differential braking events to the highway chauffeur host vehicle state algorithm.	SG-1, SG-2, SG-3
MM-108	Ensure that the vehicle system architecture and arbitration strategy provides for safe transition of control between the highway chauffeur system and other vehicle systems.	SG-2, SG-3
MM-109	Allow higher-priority safety systems to override the highway chauffeur system.	SG-5
MM-110	Bring the vehicle to an appropriate safe state when required regardless of the state of the system operation, including during a lane-change maneuver.	SG-2, SG-3

7.3 Example Fallback and Foreseeable Misuse Mitigation Measures

The third category of mitigation measures presented in PAS 21448 address fallback measures and instances of foreseeable misuse by the driver. For the generic Level 3 highway chauffeur system considered in this study, the driver is the primary fallback measure as described in Section 4.2.3. This study identified 9 potential mitigation measures to help improve the likelihood of successful driver takeover during a control transition through measures that improve the HMI, notifications and warnings, and system understanding. These mitigation measures are shown in Table 41.

Table 41. Example mitigation measures to improve successful driver takeover.

Mitigation Measure ID	Example Mitigation Measure	Relevant Safety Goals
MM-111	Establish distinct levels of driver engagement in the driver awareness monitoring system, including levels that differentiate between physical and cognitive engagement.	SG-4
MM-112	Determine the driver's level of engagement regardless of the driver's physical characteristics (e.g., sunglasses, hats).	SG-4
MM-113	If the lane model algorithm cannot establish the lane boundaries (e.g., due to the absence of adequate lane markings), adjust the measured level of driver engagement one level lower (i.e., as if the driver were less engaged).	SG-4
MM-114	Establish an escalating warning strategy, distinct from other vehicle system warnings, to alert the driver to regain awareness of the situation. a. Set the escalating warning strategy based on the level of driver engagement determined by the driver awareness monitoring system.	SG-4
MM-115	Clearly communicate to the driver when the system starts control and when the system stops control at the end of the control transition period. a. Clearly display the current system state (i.e., on, off, transitioning, or degraded operation) to the driver at all times.	SG-4
MM-116	Ensure a safe operating envelope of TBD seconds to provide sufficient time to transition control to the driver in the event the limits of the ODD are reached. a. Initiate the control transition at a time greater than or equal to TBD seconds. b. Ensure the road model algorithm supports operation for the entire duration of TBD seconds based on the current operating speed. The vehicle speed may be reduced to achieve the TBD seconds.	SG-4
MM-117	Set the control transition time for driver takeover as a dynamic parameter that depends on the level of engagement determined by the driver awareness monitoring system.	SG-4
MM-118	During the control transition process, clearly communicate via audible and visual messaging, distinct from other vehicle system warnings, the time remaining for the drive to take control.	SG-4
MM-119	During the control transition process, clearly communicate to the driver via audible and visual messaging the immediate step required by the driver as a part of regaining control depending on the state of the vehicle (speed, lateral angle, and traffic conditions).	SG-4

This study identified 7 potential mitigation measures to help address foreseeable misuse scenarios. These mitigation measures aim to improve driver understanding of the system operation and reduce the likelihood of inadvertent system interaction. These mitigation measures are shown in Table 42.

Table 42. Example mitigation measures to address potential foreseeable misuse.

Mitigation Measure ID	Example Mitigation Measure	Relevant Safety Goals
MM-120	Provide an in-vehicle, on-screen training on the controls and operation of the highway chauffeur system, including operation, warnings, methods to transfer control between the system and the driver, duration of the control transition process, actions required by the driver, and response of the system to actuation of foundational systems when the feature is engaged. a. Ensure the training program is completed at least once before allowing the system to be engaged on the roadway.	SG-1, SG-2, SG-3
MM-121	In the system interface, provide the driver with an easily accessible control to turn the feature off at any point. a. Periodically confirm that the HMI controls are active, including during the transition process.	SG-1, SG-2, SG-3
MM-122	Clearly indicate any changes to the system capabilities during nominal operation or during the control transition period, including reduced functionality or reduced authority.	SG-1, SG-2, SG-3
MM-123	Clearly communicate to the driver the system availability based on the ODD. a. If the driver attempts to activate the system outside its ODD, do not engage the system and alert the driver that the system is not available.	SG-1, SG-2, SG-3
MM-124	When a foundational system is actuated, clearly communicate to the driver via audible and visual messages that the system is going to relinquish control to the driver. a. Continue operating for the full control transition period of TBD seconds if the driver intention module confidence metric does not satisfy the true positive KPI. b. Provide the driver with an option to cancel the control transfer if the system is still within its ODD.	SG-1, SG-2, SG-3
MM-125	If the driver does not resume control by the end of the control transition period, transition to a safe state that includes moving the vehicle out of traffic, bringing the vehicle speed to zero, placing the vehicle in park, and turning on the hazard light indicators.	SG-1, SG-2, SG-3, SG-5
MM-126	Provide warnings and messages for the highway chauffeur system that are distinct from those warnings and messages of other vehicle systems.	SG-1, SG-2, SG-3

8 Overview of Risk Evaluation Approaches

8.1 Evaluation Approaches

8.1.1 Approaches to Evaluate Area 2: Known-Unsafe Scenarios

As unsafe scenarios are identified and thus become known-unsafe scenarios, countermeasures are developed and incorporated into the system design to mitigate the resultant unintended behavior. These SOTIF mitigation measures might include strategies such as restricting the system's ODD, providing additional sensor coverage, or implementing redundancy in sensing or in the algorithms. The purpose of evaluating the system against known-unsafe scenarios is to ensure that the system does not present unreasonable risk that could lead to hazardous events in known scenarios, given the SOTIF mitigation measures (ISO, 2019).

These evaluation techniques focus on targeted testing of the sensors, algorithms, and actuators against the known system limitations. In addition, these techniques also test the integrated system against known-unsafe scenarios. Targeted testing against known-unsafe scenarios typically includes testing perturbations of those scenarios to extend coverage (e.g., varying levels of rainfall). Koopman and Wagner (2018) suggest biasing such tests to favor perturbations that create more challenging scenarios rather than a more normal distribution centered on the nominal case.

PAS 21448 identifies a set of tests to consider when evaluating the known-unsafe scenarios (Table 43). These tests could be performed using a combination of analysis, simulation, and vehicle-level testing as described previously. Each test presented in PAS 21448 focuses on either the integrated system or a particular subsystem (e.g., sensors, actuators).

Table 43. Possible approaches in PAS 21448 for testing known-unsafe scenarios.

Test Type	System or Subsystem Under Test
Controllability tests (e.g., reasonably foreseeable misuse)	Integrated System
Injection of system inputs to trigger unintended behavior	Sensor, Algorithm
In-the-loop testing (HIL/SIL/MIL) against select SOTIF use cases and scenarios	Sensor, Algorithm, Actuator, Integrated System
Randomized input tests	Integrated System
Requirements based test	Sensor, Algorithm, Actuator, Integrated System
Testing against different environmental conditions	Sensor, Actuator, Integrated System
Vehicle testing against select SOTIF use cases and scenarios	Sensor, Algorithm, Actuator, Integrated System
Verification of component characteristics	Sensor, Actuator
Verification of aging effects	Sensor, Actuator, Integrated System
Evaluation of architectural properties (e.g., independence)	Algorithm
Verification of robustness to interference from other sources	Algorithm
Robustness to signal-to-noise ratio degradation (e.g., noise injection)	Integrated System
Verification of vehicle-mounted sensing system characteristics (e.g., sensor overlap)	Sensor

Applying these tests to the perception and decision-making algorithms in a Level 3 highway chauffeur system is not always straightforward. It may not always be possible for safety engineers to fully understand the system's decision-making process (Koopman & Wagner, 2018). For instance, when evaluating a lane-centering maneuver in a scenario with extraneous roadway markings, testing is expected to be able to differentiate between outcomes where the system detects the correct lane markings with sufficient confidence and outcomes where the system has low confidence but follows the correct lane markings by chance.

8.1.2 Approaches to Evaluate Area 3: Unknown-Unsafe Scenarios

Initially, SOTIF mitigation measures are based on the known-unsafe scenarios identified through analysis. However, these represent only a fraction of the potential driving scenarios that could be encountered in the real world. Additional techniques are used to identify potential unknown-unsafe scenarios and make them known-unsafe scenarios for which system engineers can develop additional SOTIF mitigation measures.

SMEs interviewed for this study apply a combination of structured techniques (e.g., guided brainstorming) and unstructured techniques (e.g., on-road testing within the ODD) to expose new unknown-unsafe scenarios. However, the extent of testing required to identify unknown-unsafe scenarios is still an unresolved issue in the SOTIF process and there is no guarantee that all unknown-unsafe scenarios will be identified through any amount of testing. PAS 21448 only recommends that safety engineers determine a test length and provide rationale supporting the selected test length. SMEs generally indicated that this remains a gap.

SMEs also emphasized the importance of ensuring that all testing used to evaluate the system against unknown-unsafe scenarios occurs within the ODD and provides coverage across the range of parameters within the ODD. In particular, this type of testing only provides value if the system encounters the specific set of conditions that constitute an unknown-unsafe scenario. Combining structured analysis with on-road testing may help uncover new scenarios that are expected to be challenging but may not occur frequently on the road. For instance, on-road testing may reveal a new combination of environmental parameters to consider. SMEs indicated that structured analysis could then introduce a known challenging behavior of another vehicle (e.g., cut-ins) into this combination of environmental parameters to create a new scenario without having to encounter it on the roadway.

It is also important to distinguish between testing intended to identify new unknown-unsafe scenarios (e.g., data and requirements gathering) and testing with the intent to demonstrate safe operation within the ODD (e.g., system validation) (Koopman & Wagner, 2018). In particular, if testing to demonstrate safe operation within the ODD results in discovery of many new unknown-unsafe scenarios, this suggests that either additional data and requirements gathering is necessary or there are problems with other aspects of the validation approach. Annex C of PAS 21448 describes an approach based on establishing a target value for the number of miles traveled without encountering a new unknown-unsafe scenario. However, as unknown-unsafe scenarios are addressed through SOTIF mitigation measures, it may be necessary to restart this type of testing to ensure that the modifications to the design did not introduce new unknown-unsafe scenarios.

PAS 21448 provides examples of tests to evaluate unknown-unsafe scenarios (Table 2). Unlike those tests shown in Table 43, the tests in Table 44 are typically conducted at the integrated system level using vehicle testing and simulation.

Table 44. Possible approaches in PAS 21448 for testing unknown-unsafe scenarios.

Test Type
Robustness to signal-to-noise ratio degradation (e.g., noise injection)
Evaluation of architectural properties (e.g., independence)
In-the-loop testing on randomized test cases
Randomized input tests
Vehicle testing against select SOTIF use cases and scenarios
Long-term vehicle test
Fleet tests
Tests derived from field experience
Tests of corner cases and reasonably foreseeable misuse
Comparison with existing systems
Simulation of selected scenarios
Analysis of worst-case scenarios

8.1.3 Example of Integrated Evaluation Approaches

A SOTIF evaluation strategy could incorporate multiple approaches as described in Sections 8.1.1 and 8.1.2. For instance, one possible approach to SOTIF evaluation could begin by analyzing the system design with the incorporated SOTIF mitigations measures. Examples include:

- Evaluation of architectural properties (e.g., independence)
- Verification of vehicle-mounted sensing system characteristics (e.g., sensor overlap)

Next, the system designers could test the SOTIF mitigation measures against known-unsafe scenarios through simulation. Simulation models would need to be verified against real-world data to provide confidence in the accuracy of the simulation (Glander, 2018).

As described in Section 6.3, individual triggering events may be in a form with enough detail to directly generate scenarios. Alternatively, if triggering events are in a more generalized form, additional analysis may be necessary to develop detailed scenarios to support scenario-focused evaluation approaches. To illustrate this concept, Appendix C provides an example of how the high-level triggering events in Section 6 could be mapped to the scenario variables described in Section 3. There is active research to develop a minimum set of testable cases and scenarios that provides coverage of the ODD and could support the SOTIF evaluation. Glander also emphasizes the importance of a complete scenario data set.

Simulation strategies could include:

- Testing sensor and algorithm limitations against environmental conditions (e.g., weather conditions, roadway geometry, lighting) to ensure performance remains within the acceptable system limits,[25]
- Injection of system inputs, including those based on known triggering events, random inputs across the range of values possible within the ODD, and simulated noise inputs.
- Testing against select known-unsafe SOTIF scenarios and use cases, and combinations of scenarios and use cases.
- Testing against both randomly generated scenarios and targeted "worst-case" scenarios.

The results of simulation could then be verified through vehicle testing, including track testing and on-road testing. This testing may also provide additional confidence in the extent to which unknown-unsafe scenarios have been identified. However, as discussed previously, this testing cannot prove the absence of additional unknown-unsafe scenarios.

Vehicle testing could include:

- Track testing to verify components behave in accordance with simulation models and are robust to interference from other sources,
- Long-term testing to verify that aging effects do not result in unintended behavior, and
- On-road testing to identify potential unknown-unsafe scenarios.

Based on the outcome of testing, additional SOTIF measures may be necessary. As these additional SOTIF measures are incorporated into the system design, the evaluation process could be repeated until no credible scenarios remain or the triggering events are deemed acceptable based on the risk evaluation targets.

8.2 Potential Risk Targets and Evaluation Techniques

8.2.1 Comparison to Crash Statistics

PAS 21448 presents crash statistics as a possible metric against which safety engineers can evaluate the effectiveness of SOTIF measures and assess residual risk. One approach may be to consider the typology developed by Swanson et al., which provides a comprehensive set of pre-crash scenarios supported by U.S. traffic statistics (Swanson et al., in press). In addition, pre-crash scenarios are further evaluated against relevant conditions, such as environmental conditions, road geometry, crash location, and other contributing factors. Additional variables in the crash databases could also be used to develop known-unsafe scenarios, which in turn could support comparison of these scenarios against crash data.

In the context of the lane-centering maneuver of a Level 3 highway chauffeur system, relevant pre-crash scenarios might include roadway departure and sideswipe. The lane-change maneuver has a dedicated pre-crash scenario (lane change). Crash rates for the relevant pre-crash scenarios may provide risk evaluation targets—for instance, operation of the Level 3 highway chauffeur system should not result in a higher incidence of crashes per billion miles than vehicles without the Level 3 highway chauffeur.

[25] Acceptable system limits could be defined by the minimum required true positive and true negative KPIs.

To illustrate this, the lane-change pre-crash scenario has a frequency of 43 crashes per billion light vehicle miles traveled on highways[26] (a frequency on the order of 10^{-8} crashes per mile traveled) (Swanson et al., in press). The sum of the probabilities of all SOTIF events given the likelihood of their respective scenarios could then be compared to this value (Glander, 2018). However, there is no guarantee that the definition of highway used in this analysis aligns with the precise definition of a highway used in the ODD for a particular system (e.g., restricted versus unrestricted, managed lanes). Furthermore, these statistics would need to remove any irrelevant factors that may not apply to a Level 3 highway chauffeur system.

Crash data might also be useful to compare against specific SOTIF scenarios—for instance, the frequency of crashes related to lane changes in rainy weather could be compared against the frequency of SOTIF events resulting from rain. However, crash data may become sparse when many variables are combined to create highly specific scenarios. Crash data also only captures crashes reported to the police with property damage or injury—minor crashes may not be reflected in the crash data. Additionally, certain data categories in the crash data (e.g., rain) may not have sufficient resolution to effectively compare against specific system limitations—for instance, there is a spectrum of rain intensity that is not captured in the crash data (e.g., a system may be capable of operating up to a certain level of rain).

8.2.2 Comparison to Human Behavior

SMEs suggested an alternative approach to evaluating residual risk could involve comparing the system performance against the capabilities of human drivers (i.e., assessing whether an ADS is as effective as a human driver in avoiding crashes and resolving driving conflict situations). At the core of this approach is the assumption that if a human driver cannot avoid a crash, it may not be reasonable to expect the ADS to avoid a crash under identical circumstances.

An important consideration for this approach is to ensure that if the system cannot resolve a driving conflict situation or avoid a crash, it at least had the correct situational awareness and evaluated similar avoidance maneuvers as the human driver (i.e., the system did not "miss" something or "not consider" a potential maneuver). Similarly, this approach should ensure that a system is avoiding hazards for the correct reasons (Koopman & Wagner, 2018). One technique may be to output established "test-points" in the system design—for instance, confidence level outputs from the perception system to determine if the system is detecting the correct objects with sufficient confidence. Koopman and Wagner also propose a "think-out-loud" documentation of the system's decision-making process during testing to ensure that the system is responding to the scenario in accordance with the design intent.

A challenge with this approach is that no such set of human performance data is readily available against which to compare system performance behavior. An approach like this may also need a complete set of behavioral requirements and competencies to evaluate using pass/fail testing criteria (Koopman & Wagner, 2018). For instance, data may also be needed that describes the full set of explicit and implicit traffic laws and norms navigated by human drivers so that ADS can be evaluated on their ability to follow these traffic laws and norms. This would allow for a more accurate comparison between system and human responses.

[26] Based on crash data from 2011-2015. See Swanson et al. (in press) for details for determining this value.

8.2.3 Probabilistic Evaluation

The approaches in Sections 8.2.1 and 8.2.2 focus on comparing system behavior against metrics derived from human competencies. This comparison may be suitable for Level 4 and Level 5 ADS where the system is wholly responsible for all elements of the OEDR as well as providing for a safe fallback (SAE International, 2018). In addition to the approaches in Sections 8.2.1 and 8.2.2 , Level 3 systems (e.g., a Level 3 highway chauffeur system) also need to consider the potential for safe driver takeover of the system after a suitable transition period—and the potential for foreseeable misuse. If the system can safely transition control to the driver, the driver may be able to avoid a crash or resolve a driving conflict even if the ADS cannot.

For a Level 3 system, this type of evaluation might consider elements such as:

- P1 = the probability of encountering a SOTIF triggering event scenario requiring driver takeover;
- P2 = the probability the system does not recognize that the SOTIF unintended behavior is occurring and does not alert the driver;
- P3 = the probability of no driver mitigation without a driver alert; and
- P4 = the probability of no driver mitigation with a driver alert.

Given a SOTIF event occurs (*P1*), this approach allows for consideration of two outcomes:

- *P2 x P3* - The system does not recognize an unintended behavior due to a SOTIF triggering event (e.g., system is tracking the wrong lane markings with high confidence) and therefore does not alert the driver. Mitigation of this event depends on the driver's ability to recognize the SOTIF event and intervene without an alert.
- *(1-P2) x P4* – The system does recognize an unintended behavior and properly alerts the driver and initiates transfer of control. However, due to foreseeable driver misuse or other situations, the driver fails to intervene.

The probabilities could be combined in an equation:

$$F \geq \text{P1 x [P2 x P3} + (1 - \text{P2}) \text{ x P4]}$$

where *F* is a critical value that could be determined using the approaches in Sections 8.2.1 and 8.2.2, or from other sources.[27]

In order to correctly perform such an evaluation, data is needed for all four variables. Such data is not readily available and may be system-specific. For instance, the probability of encountering a SOTIF triggering event scenario may depend on the level of scenario detail and the system-specific ODD. Similarly, the probability of the system not recognizing a SOTIF unintended behavior may be system-specific. These data may be more suitable for individual manufacturers to collect through a combination of simulation and on-road or track testing, as described in Section 8.1. However, if a universal minimum set of scenarios could be developed, then it could be possible to establish a common data set for P1. Additionally, developing a common set of data

[27] This equation illustrates one possible concept of how driver behavior may be incorporated into the SOTIF evaluation and assumes independence of the parameters, which may not always be the case. Application of such a concept should include evaluating the independence of parameters and modification of the equation as appropriate.

that supports evaluation of the driver takeover in both alerted an unalerted situations could help establish a consistent evaluation across industry.

8.2.4 Risk Management Rationale

In the event that sufficient crash data, field data, or other relevant statistics are not available, Sub-clause 6.5 of PAS 21448 states that appropriate evaluation targets can be selected with appropriate rationale. PAS 21448 presents two examples of such targets—the French concept *globalement au moins aussi bon* (GAMAB; *translation:* globally at least as good) and as low as reasonably practicable. Both approaches are discussed below.

Additional guidance may be necessary to ensure application of these approaches do not result in unreasonable risk. For instance, establishing a minimum risk level would help ensure that application of GAMAB does not increase the risk of one hazard to an unacceptable level, even though that increased risk is offset by reductions elsewhere in the system. Similarly, a minimum risk level would help ensure that application of ALARP does not result in releasing a system with unacceptable risk levels simply because cost-effective solutions were not available.

8.2.4.1 GAMAB

The GAMAB principle states that the overall residual safety risk of the system under consideration should not be higher than that of a comparable existing system with similar functionality. The concept is based on the overall tradeoff between risks and hazards. While the introduction of the new system might increase the residual risk associated with some hazards, this increase in risk might be offset by a more significant decrease in residual risk associated with other hazards (ISO, 2019).

8.2.4.2 ALARP

The ALARP principle requires that any risk be reduced so far as is reasonably practicable, considering both the benefits resulting from the system and the costs of any further reduction in risk (ISO, 2019). The ALARP principle is based on evaluating the overall tradeoff between risk reduction and cost. Part 5, Annex C, of the International Electrotechnical Commission (IEC) functional safety standard IEC 61508 describes the ALARP principle in more detail. According to IEC 61508, certain risks are categorized as “intolerable” and cannot be justified except in extraordinary circumstances (IEC, 2005). Beneath the intolerable region are tolerable risks, which are acceptable only if further risk reduction is impracticable or if the cost is greatly disproportionate to the level of risk reduction. Within the tolerable region, the ALARP principle should be used to show that risk cannot be reduced further. Finally, there is a broadly acceptable region, where the level of risk is low enough that further reduction is not necessary. In this region, it is important to demonstrate that risk remains at this level.

8.2.5 Example of Integrated Risk Targets and Evaluation Techniques

The risk targets and evaluation techniques in Sections 8.2.1 to 8.2.4 are not mutually exclusive and could be combined to create a more comprehensive strategy. One such approach is outlined below:

- First, identify if it is more appropriate to compare the system performance to crash data or human driving behavior. This may depend on factors such as availability of data and system goals.

- Next, if the system allows for driver takeover, evaluate the probability of safe driver takeover using the approach described in Section 8.2.3. If the system does not allow for driver takeover, the likelihood of the system failing to safely transition to a fallback state could be compared directly to the metric selected above.
- Then iterate the SOTIF process and improve the SOTIF mitigation measures until the system satisfies the metric selected above.
- Finally, further improve the system by applying additional risk mitigation measures using an ALARP technique. That is, as long as cost-effective measures exist to further reduce risk, those measures should be incorporated into the system design even though the system may meet the target metrics established by crash data or human driving behavior.

9 Conclusions

This study applied concepts from the recently released SOTIF PAS 21448 to the lane-centering and lane-changing maneuvers for a generic Level 3 highway chauffeur system. This study is intended to illustrate the SOTIF process and highlight some comparisons with the functional safety process. While the results may be informative, this study was performed on a generic Level 3 highway chauffeur system with limited technical details. Any potential application of these findings to actual systems would require a system-specific analysis.

This study found consistency between the vehicle-level hazards identified for SOTIF and the functional safety approach using ISO 26262. However, some hazards may only apply to one approach—for instance, if a hazard could only result from an E/E failure. Although SOTIF does not require establishing safety goals, this study found that similar safety goals could support both SOTIF and functional safety. Safety goals may support traceability between the SOTIF mitigation measures and vehicle-level hazards the measures are intended to mitigate. However, some SMEs interviewed for this study indicated that safety goals are not appropriate for SOTIF; other SMEs concurred that the SOTIF and functional safety processes may share safety goals.

Application of the SOTIF risk assessment approach to a Level 3 system indicates that additional guidance to practitioners may be helpful to more consistently evaluate controllability for ADS. The risk assessment in this study adopted the most conservative approach and assumed that the driver was not engaged in the driving task or available to intervene. Therefore, the controllability factor in the risk assessment was assigned ">C0" for all hazardous events. Guidance could provide illustrative examples for assessing controllability by considering the role of other vehicle systems or considering system performance during a transition period, and assessing the likelihood of successful driver takeover at the end of the transition period.

This report provides 81 examples of triggering events for the lane-centering and lane-changing maneuvers of a Level 3 highway chauffeur system. Specifically, this study identified:

- 59 Type I triggering events, which focus on system limitations, and
- 22 Type II triggering events, which focus on HMI and foreseeable driver misuse situations.

The triggering events were used to derive 126 potential mitigation measures using guidance provided in PAS 21448.

PAS 21448 does not provide guidance on the level of specificity for triggering events. Triggering events could be described broadly, capturing many specific events in a single category. This approach would rely on identifying the specific SOTIF scenarios as part of a future evaluation process, as described in Section 6.3. Alternatively, an analysis could derive detailed triggering events at the outset. Regardless, it is unlikely that an analysis would capture all triggering events or scenarios, particularly as triggering events are refined to have greater specificity. This becomes more apparent when considering the possible combinations of scenario variables presented in Appendix A (which itself is only a subset of possible scenario variables that could be encountered on the roadway).

Finally, this study provides an overview of current risk evaluation approaches identified by SMEs interviewed for this study, in literature, and discussed in PAS 21448. This report presents one possible approach for integrating these evaluation approaches. A common theme in

reviewing these evaluation approaches is that current data collection and evaluation methods based on human driving are not readily applicable to ADS.

- Existing crash data does not necessarily map well to ODDs, for instance differentiating between restricted and unrestricted highways, or managed lane types. Crash data also does not include data on minor crashes or "near misses," although this data might be available from naturalistic driving studies. If a common scenario framework exists, it may be possible to map existing crash data and naturalistic driving data to this framework, and identify remaining data gaps and other information on the types of crashes relevant to ADS.
- Human driving performance data is not readily available, but may be an alternative metric against which to compare ADS performance. In particular, this type of data may be useful for evaluating ADS decision-making against human decision-making—for instance, is an ADS detecting the correct objects with sufficient confidence and is the ADS selecting maneuvers based on the correct situational awareness.
- Data on human takeover in both alerted and unalerted situations would assist in incorporating driver takeover and foreseeable driver misuse into the evaluation of Level 2 and Level 3 ADS. This type of data may also evaluate whether the driver responds appropriately when resuming control (i.e., does the driver select the appropriate control action for the situation after being disengaged?).

Another remaining challenge for the SOTIF process is determining that sufficient testing of the unknown-unsafe problem space has been performed. Annex C of PAS 21448 provides one example for determining a sufficient level of testing to identify potential unintended behaviors. However, additional data or guidance could improve this part of the SOTIF process.

10 References

Becker, J., Helmle, M., & Pink, O. (2017). System architecture and safety requirements for automated driving. In D. Watzenig & M. Horn, Eds., *Automated driving: safer and more efficient future driving* (pp. 265-283). Springer International Publishing.

Behere, S., & Törngren, M. (2017). Systems engineering and architecting for intelligent autonomous systems. In D. Watzenig & M. Horn, Eds., *Automated driving: safer and more efficient future driving* (pp. 313-351). Springer International Publishing.

Brewer, J., Becker, C., Yount, L., & Pollard, J. (2018). *Functional safety assessment of a generic automated lane centering (ALC) system and related foundational vehicle systems* (Report No. DOT HS 812 572). National Highway Traffic Safety Administration.

Continental AG. (2017a, July 13). *Cruising chauffeur: Continental demonstrates the future of highly automated driving on highways* (Press release). Author. www.continental.com/en/press/press-releases/cruising-chauffeur-71302

Continental AG. (2017b). Mono camera. (Web page). Author. www.continental-automotive.com/en-gl/Passenger-Cars/Chassis-Safety/Advanced-Driver-Assistance-Systems/Cameras/Mono-Camera

Continental AG. (2017c). Stereo camera (Web page). Author. www.continental-automotive.com/en-gl/Passenger-Cars/Chassis-Safety/Advanced-Driver-Assistance-Systems/Cameras/Stereo-Camera

Coudert, O. (1994). Two-level logic minimization: An overview. *Integration, the VLSI Journal, 17*(2), 97-140.

Dubey, A. (2015, October 14). EDN Network: The challenges and opportunities for ADAS stereo vision applications, part I. www.edn.com/Pdf/ViewPdf?contentItemId=4440597

Federal Highway Administration. (2013). *Highway functional classification concepts, criteria and procedures, 2013 edition* (Publication No. FHWA-PL-13-026). Author. Available at www.fhwa.dot.gov/planning/processes/statewide/related/highway_functional_classifications/fcauab.pdf

Glander, K. H. (2018, August 28). *Case study by Karl-Heinz Gander ZF Group: It's all about safety and validation* [Video]. YouTube. https://youtu.be/qxfwkC7Mpgc

International Electrotechnical Commission. (2001). *IEC 61882-2001: Hazard and operability studies (HAZOP Studies) - Application Guide, Edition 1.0.*

International Electrotechnical Commission. (2005). *IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems.*

International Organization for Standardization. (2019). *PAS 21448: Road vehicles— Safety of the intended functionality*.

International Organization for Standardization. (2018). *ISO 26262: Road vehicles— Functional safety*.

Koopman, P., & Wagner, M. (2018, April 10-12). *Toward a framework for highly automated vehicle safety validation* (Report No. SAE 2018-01-1071). 2018 SAE World Congress, Detroit, MI.

Leveson, N. (2012). *Engineering a safer world*. MIT Press.

Meinel, H. H., & Bösch, W. (2017). Radar Sensors in Cars. In D. Watzenig & M. Horn, Eds., *Automated driving: safer and more efficient future driving* (pp. 245-261). Springer International Publishing.

Merat, N., Jamson, A. H., Lai, F. C., Daly, M., & Carsetn, O. M. (2014). Transition to manual: Driver behavior when resuming control from a highly automated vehicle. Elsevier: *Transportation Research, Part F(27)*, 274-282.

Missouri Department of Revenue. (2018, August). *Missouri driver guide: A guide to understanding Missouri motor vehicle laws and licensing requirements*. https://dor.mo.gov/pdf/Chapter3.pdf

National Center for Statistics and Analysis. (2013, November). *2012 Fatality Analysis Reporting System (FARS) and National Automotive Sampling System (NASS) General Estimates System (GES) coding and validation manual* (Report No. DOT HS 811 854). National Highway Traffic Safety Administration. Available at https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/811854

National Center for Statistics and Analysis. (2017, October). *Fatality Analysis Reporting System (FARS) Analytical User's Manual 1975-2016* (Report No. DOT HS 812 447). National Highway Traffic Safety Administration. Available at https://www.nhtsa.gov/filebrowser/download/163441

Oregon Department of Transportation. (2016). *Oregon bicyclist manual*. www.oregon.gov/ ODOT/Programs/TDD%20Documents/Oregon-Bicyclist-Manual.pdf

Osterwood, C., & Noble, F. (2017, May 26). *Localization for the next generation of autonomous vehicles*. www.swiftnav.com/sites/ default/files/whitepapers/localization_white_paper_052617.pdf

Pegasus Projekt. (n.d.). Requirements & conditions - Stand 3: The highway-chauffeur. (PowerPoint). www.pegasusprojekt.de/files/tmpl/PDF-Symposium/03_The-Highway-Chauffeur.pdf

Rupp, A., & Stolz, M. (2017). *Survey on control schemes for automated driving on highways. in automated driving: Safer and more efficient future driving*. Springer International Publishing.

SAE International. (2018). *SAE J3016: Taxonomy and definitions for terms related to on-road motor vehicle automated driving systems*.

SAE International. (2015). *SAE J2980: Considerations for ISO 26262 ASIL hazard classification*.

Schubert, R., & Obst, M. (2017). The role of multisensor environmental perception for automated driving. In D. Watzenig & M. Horn, Eds., *Automated driving: Safer and more efficient future driving* (pp. 161-182). Springer International Publishing.

Shappell, S. A., & Wiegmann, D. A. (2000). *The human factors analysis and classification system*. Federal Aviation Administration.

Society of Automotive Engineers. (1994). *SAE J1739: Potential failure mode and effects analysis in design and potential failure mode and effects analysis in manufacturing and assembly processes*.

Swanson, E. D., Foderaro, F., Yanagisawa, M., Najm, W. G., & Azeredo, P. (in press). *Statistics of light-vehicle pre-crash scenarios based on 2011-2015 national crash data.* National Highway Traffic Safety Administration.

Thorn, E., Kimmel, S., & Chaka, M. (2018). *A framework for automated driving system testable cases and scenarios* (Report No. DOT HS 812 623). National Highway Traffic Safety Administration.

Ulbrich, S., Menzel, T., Reschka, A., Schuldt, F., & Maurer, M. (2015). *Defining and Substantiating the terms scene, situation, and scenario for automated driving*. Proceedings of the IEEE 18th International Conference on Intelligent Transportation Systems.

Watzenig, D., & Horn, M. (2017). Introduction to automated driving. In D. Watzenig & M. Horn, Eds., *Automated driving: Safer and more efficient future driving* (pp. 3-16). Springer International Publishing.

Appendix A: Scenario Framework

Table 45. List of permanent-regional scenario variables.

Top-Level Category	Immediate Subcategory	Detailed Subcategory	Permanent-Regional Scenario Variable
Physical Infrastructure	Roadway Type	Functional Class	Interstate
			Principal Arterial (Other Freeways/Expressways)
			Principal Arterial – Other
			Minor Arterial
			Major Collector
			Minor Collector
			Local
			Other
		Trafficway	Two-Way, Divided, Unprotected
			Two-Way, Divided, Positive Median Barrier
			Two-Way, Not Divided
			Two-Way, Not Divided, Continuous Left Turn Lane
			One-way Trafficway
			Non-Trafficway or Driveway Access
	Roadway Surface and Features	Lane Type	Single Lane
			Multi-lane
			Reversible Lane
			Shoulder Lane
			Managed Lane (HOV, etc.)
		Surface Type	Concrete
			Blacktop, Bituminous, or Asphalt
			Brick or Block (including cobblestone/Belgian brick)
			Slag, Gravel, or Stone
			Dirt
	Roadway/Lane Edges	Shoulder Type	Paved/Gravel
			Unpaved
Objects	Roadway Users	Other Non-Vehicle Users Permitted on Roadway	Pedestrian, Pedal-cyclist, Other Non-motorist Permitted in Road

Top-Level Category	Immediate Subcategory	Detailed Subcategory	Permanent-Regional Scenario Variable
Objects (Cont.)	Non-Roadway Users	Pedestrian Crosswalks/ Intersections	Crosswalks/Intersections Present in Roadway Type
		Other Users on Side of Roadway	Non-motorists Permitted Along Roadway
Zones	Regions/States	Regional Traffic Laws	Special Regional Traffic Laws and Norms
		State Traffic Laws	Special State Traffic Laws and Norms

Table 46. List of permanent-local scenario variables.

Top-Level Category	Immediate Subcategory	Detailed Subcategory	Permanent-Local Scenario Variable
Physical Infrastructure	Roadway Surface and Features	Intersection	Median Crossover Road
			Tollbooth/Tollgate
			Entrance/Exit Ramp
			Four-way Intersection
			T-intersection
			Y-intersection
			Traffic Circle
			Roundabout
			Five-point or More
			L-intersection
		Surface Type	Local Change in Surface (e.g., concrete bridge)
			Step Difference/Uneven
		Roadway Condition	Manhole Cover
	Roadway/Lane Edges	Lane Marking Type/Quality	Bott's Dots or Cat's Eye
			Other Non-Traditional Markings
		Lane Type	Narrow Lane
			Wide Lane
			Merging
			Branching
		Road Edge Type/Quality	Median
			Curb
			Concrete Barrier

Top-Level Category	Immediate Subcategory	Detailed Subcategory	Permanent-Local Scenario Variable
Physical Infrastructure (cont.)	Roadway/Lane Edges (cont.)	Road Edge Type/Quality (cont.)	Guardrails
			Grating
			Telephone Poles
	Roadway Geometry	Alignment	Straight
			Curve Right
			Curve Left
		Grade	Level
			Grade, Unknown Slope
			Hillcrest
			Sag (Bottom)
			Uphill
			Downhill
			Banked
Operational Constraints	Speed Limit	Speed Limit Signage	Posted Speed Limit
Zones	Traffic Management Zone	Variable Speed Zone	Variable Speed Zone
		Loading/Unloading Zone	Loading/Unloading Zone
	School/ Construction Zone	School Zone	Within Designated School Zone
	Interference Zones	Structures	Tunnels
			Bridges (double-deck, covered, viaduct, etc.)
			Tall Buildings (e.g., urban canyon)
			Parking Garage
		Natural Conditions	Geologic Formations (e.g., canyons, overhang)
			Mountainous Regions

Table 47. List of compounding event or condition scenario variables.

Top-Level Category	Immediate Subcategory	Detailed Subcategory	Compounding Event or Condition Scenario Variable
Physical Infrastructure	Roadway Surface and Features	Roadway Condition	Ruts, Holes, Bumps in Road
			Other Maintenance or Construction-Related Condition
			Shoulder-Related (design or condition)

Top-Level Category	Immediate Subcategory	Detailed Subcategory	Compounding Event or Condition Scenario Variable
Physical Infrastructure (cont.)	Roadway Surface and Features (cont.)	Roadway Condition (cont.)	Extraneous Road Surface Markings (e.g., skid marks)
			Inadequate Construction or Poor Design of Roadway, Bridge, etc.
	Roadway/Lane Edges	Road Edge Type/Quality	Cones
Operational Constraints	Speed Limit	Operating Speed	Posted Maximum Limit Below Minimum System Operating Speed
			Posted Minimum Limit Above Maximum System Operating Speed
			Relative Speed Above Surrounding Traffic
			Relative Speed Below Surrounding Traffic
			Speed Inappropriate for Conditions (e.g., surface, geometry)
		Speed Limit Signage	None (inferred speed limit)
	Traffic Conditions	Standard Traffic	Light or No Traffic
			Backup Due to Regular Congestion
		Altered Traffic Flow	Tollbooth/Plaza Related
			Backup Due to Prior Non-Recurring Incident
			Backup Due to Prior Crash
Objects	Signals and Signage	Local Traffic Control Type	No Control or Uncontrolled
			Flashing Traffic Control Signal
			Traffic Signal With/Without Pedestrian Crossing Signal
			Regulatory Sign
			Warning/Information/Temporary Sign
			Railroad Crossing Device/Gate
			Traffic Officer/Flag Person/Hand Signs
	Roadway Users	Standard Vehicles	Compact Sedan
			Mid-Size Sedan
			Large Sedan
			Van
			Pickup Truck
			Sport Utility Vehicle
			Sub-Compact Sedan

Top-Level Category	Immediate Subcategory	Detailed Subcategory	Compounding Event or Condition Scenario Variable
Objects (cont.)	Roadway Users (cont.)	Standard Vehicles (cont.)	Motorcycle
		Non-Standard Vehicles	Special Cargo Body Type (e.g., garbage, gravel, flatbed, auto transporter)
			Large Vehicle Configuration (bus, tractor-trailer, single unit truck, etc.)
			Towed Vehicle (Fixed or Non-Fixed Linkage)
			Multiple Trailing Units
			Wide-Load Vehicle
			Mini-Compact Sedan
		Other Non-Vehicle Users Permitted on Roadway	Pedestrian, Bicyclist, Other Cyclist or Person on Personal Conveyances in Travel Lane
			Pedestrian, Bicyclist, Other Cyclist or Person on Personal Conveyances on Paved Shoulder/Bicycle Lane/Parking Lane
			Pedestrian Jogging/Running in Roadway
	Non-Roadway Users	Pedestrians	Pedestrian, Bicyclist, Other Cyclist, or Person on Personal Conveyances in Intersection Area
			Pedestrian, Bicyclist, Other Cyclist, or Person on Personal Conveyances in Crosswalk Area
			Pedestrian, Bicyclist, Other Cyclist, or Person on Personal Conveyances in Median/Crossing Island
			Pedestrian, Bicyclist, Other Cyclist, or Person on Personal Conveyances Waiting to Cross Roadway
		Other Users on Side of Roadway	Pedestrian, Bicyclist, Other Cyclist, or Person on Personal Conveyances on Sidewalk/Shared-Use Path/Driveway Access
			Pedestrian, Bicyclist, Other Cyclist, or Person on Personal Conveyances in Unpaved Right-of-Way
			Pedestrian, Bicyclist, Other Cyclist, or Person on Personal Conveyances in Non-Trafficway (Driveway)
			Pedestrian, Bicyclist, Other Cyclist, or Person on Personal Conveyances in Non-Trafficway (Parking Lot/Other)
			Pedestrian, Bicyclist, Other Cyclist, or Person on Personal Conveyances Adjacent to Roadway (e.g., shoulder, median)
			Pedestrian Jogging/Running Adjacent to Roadway

Top-Level Category	Immediate Subcategory	Detailed Subcategory	Compounding Event or Condition Scenario Variable
Environmental Conditions	Weather	Wind	Severe Crosswind
			Wind From Passing Truck
		Precipitation	Clear/Cloudy
			Rain
			Sleet/Hail
			Snow
			Blowing Snow
			Freezing Rain or Drizzle
		Particulate Matter	Fog, Smog, Smoke
			Blowing Sand, Soil, Dirt
	Weather-Induced Roadway Condition	Roadway Obscured	Surface Under Water
			Splash or Spray From Another Vehicle
		Surface Condition (Including Low-μ)	Wet
			Snow
			Ice/Frost
			Sand
			Water (standing or moving)
			Mud, Dirt, Gravel
			Slush
			Surface Washed Out (e.g., cave-in, road slippage)
			Loose or Slippery Surface (mud, gravel, sand, wet leaves)
	Light Conditions	Ambient Light	Daylight
			Dark (lighted)
			Dark (unlighted)
			Dawn
			Dusk
		External Lighting	Reflected Glare, Bright Sunlight, Headlights
Zones	Special Zone	Special Zone	Special Zone
	School/ Construction Zone	School Zone	Pedestrian, Bicyclist, Other Cyclist, or Person on Personal Conveyances Going to or From School (K-12)
		Construction Zone	Construction
			Utility Work

Top-Level Category	Immediate Subcategory	Detailed Subcategory	Compounding Event or Condition Scenario Variable
Zones (cont.)	School/ Construction Zone (cont.)	Construction Zone (cont.)	Maintenance
	Interference Zone	Natural Conditions	Dense Foliage

Table 48. List of non-typical event or condition scenario variables.

Top-Level Category	Immediate Subcategory	Detailed Subcategory	Non-Typical Event and Condition Scenario Variable
Physical Infrastructure	Roadway/Lane Edges	Lane Marking Type/Quality	No Markings or Obscured Lane Markings
Operational Constraints	Traffic Conditions	Altered Traffic Flow	Recent Previous Crash Scene Nearby
			Police Pursuit
			Stalled/Disabled Vehicle or Vehicle Fire
Objects	Signals and Signage	Local Traffic Control Missing	Inadequate Warning of Exits, Narrowing Lanes, Traffic Controls, etc.
			Traffic Controls Not Functioning Properly
	Roadway Users	Standard Vehicles	[Other Vehicle] Aggressive Behavior by Non-Contact Vehicle Owner
			[Other Vehicle] Overloading or Improper Loading of Vehicle with Passengers or Cargo
			[Other Vehicle] Following Improperly
			[Other Vehicle] Traveling on Prohibited Trafficways
			[Other Vehicle] Passing Through or Around Barrier
			[Other Vehicle] Failure to Observe Warnings or Instructions on Vehicles Displaying Them
			[Other Vehicle] Failure to Signal Intentions
			[Other Vehicle] Driving Wrong Way or on Wrong Side
			[Other Vehicle] Other Bad Driving
			[Other Vehicle] Disobeying Signs or Traffic Controls
			[Other Vehicle] Other Driving in the Wrong Place (e.g., bike lane)
			[Other Vehicle] Other Misbehavior – Moving (e.g., not dimming headlights)
			[Other Vehicle] Other Misbehavior – Fixed (e.g., open door into trafficway)

Top-Level Category	Immediate Subcategory	Detailed Subcategory	Non-Typical Event and Condition Scenario Variable
Objects (cont.)	Roadway Users (cont.)	Standard Vehicles (cont.)	Jackknife of Articulated Vehicle
			Nearby Trailer (swerving, swaying, or fishtailing)
			[Vision Obscured by] In-Transport Motor Vehicle (including load)
		Other Non-Vehicle Users Permitted on Roadway	Non-Occupant Struck Vehicle
			Non-Motorist Inattentive, Careless, Distracted
			Non-Motorist Failure to Yield Right-of-Way
		Other Non-Vehicle Users Permitted on Roadway (cont.)	Non-Motorist Failure to Obey Traffic Signs, Signals, or Officer
			Non-Motorist Improper or Erratic Lane Changing
			Non-Motorist Failure to Keep in Proper Lane or Running Off Road
			Non-Motorist Passing With Insufficient Distance or Inadequate Visibility, or Failing to Yield to Overtaking Vehicle
			Non-Motorist Making Improper Entry to or Exit From Trafficway
			Non-Motorist Making Improper Turn or Merge
			Non-Motorist Improper Passing
			Non-Motorist Not Visible (dark clothing, no lighting, etc.) or Failing to Have Lights on When Required
			Non-Motorist Operating without Required Equipment
			Non-Motorist in Roadway Improperly (standing, lying, working, playing)
			Non-Motorist Wrong-Way Riding or Walking
			Non-Motorist Working in Roadway (incident response)
			Non-Motorist Entering/Exiting Parked or Stopped Vehicle
			Disabled Vehicle Related (working on, pushing, leaving/approaching)
	Non-Roadway Users	Stationary Object	Debris or Objects in Road
			[Vision Obscured by] Curve, Hill, or Other Roadway Design Features
			[Vision Obscured by] Building, Billboard, etc.
			[Vision Obscured by] Trees, Crops, Vegetation

Top-Level Category	Immediate Subcategory	Detailed Subcategory	Non-Typical Event and Condition Scenario Variable
Objects (cont.)	Non-Roadway Users (cont.)	Stationary Object (cont.)	[Vision Obscured by] Not-in-Transport Motor Vehicle (parked, working)
		Dynamic Object	Struck by Falling Cargo or Something That was Set in Motion by Vehicle
			Non-Occupant Struck by Cargo/Debris
			Animal in Road
		Pedestrian	Pedestrian, Bicyclist, Other Cyclist, or Person on Personal Conveyances Dart-out
			Pedestrian, Bicyclist, Other Cyclist, or Person on Personal Conveyances Improper Crossing of Roadway or Intersection (jaywalking)
			Pedestrian, Bicyclist, Other Cyclist, or Person on Personal Conveyances Crossing Expressway

Appendix B: Systems-Theoretic Process Analysis Approach

B.1 STPA Process Overview

The STPA is a top-down systems engineering approach to system safety (Leveson, 2012). In STPA, the system is modelled as a dynamic control problem, where proper controls and communications in the system ensure the desired outcome for emergent properties such as safety. In the STPA framework, a system will not enter a hazardous state unless a UCA is issued by a controller, or a control action needed to maintain safety is not issued. Figure 6 shows a process flow diagram for the STPA method.

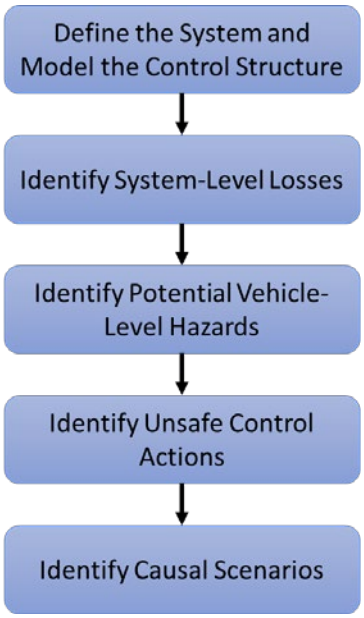

Figure 6. Key steps in the STPA process.

B.2 STPA Unsafe Control Action Derivation

This study identifies potential UCAs issued by each of the system controllers that could lead to hazardous states for the system. Specifically, this study considered two system controllers—the Level 3 highway chauffeur control module and the human driver/operator. Four sub-steps were performed to identify UCAs.

1. For each controller in the scope of the system, list all of the relevant control actions it can issue. Since this system only considered the lane change and lane-centering maneuvers of the Level 3 highway chauffeur system, only the following control actions were considered for the highway chauffeur control module:
   - Adjust lateral position in the δ direction – This control action returns the vehicle to the center of the lane. Rather than duplicate the analysis for left and right lateral maneuvers, the variable δ is used to generally indicate the direction of the control action.

- Change lanes while maintaining speed – This control action captures a lane-change maneuver at constant speed. Lane-change maneuvers with increasing and decreasing speed were initially considered, but later removed from the analysis since other longitudinal motion control was considered out-of-scope.
- Issue takeover request – This control action describes the initiating of the control transition process from the highway chauffeur controller to the human driver/operator.

For the human driver/operator, this study considered the following control actions.

- Engage/Disengage the feature – This control action describes the driver's action with a feature button—either on the head unit, steering wheel, or elsewhere—to activate or deactivate the system.
- Input steering command – This control action describes the driver's action with the foundational steering system via the steering wheel.
- Increase/decrease/maintain the accelerator pedal position – This control action describes the driver's action with the foundational propulsion system via the accelerator pedal.
- Increase/decrease/maintain the brake pedal position – This control action describes the driver's action with the foundational braking system via the brake pedal.

2. For each control action, develop a set of context variables.[28] Context variables and their states describe the relevant external control inputs to the control system and the external environment that the control system operates in, which may have an impact on the safety of the control action of interest. The combinations of context variable states are enumerated to create an exhaustive list of possible states. The context variables considered for each control action for the highway chauffeur control module are shown in Table 49.

Table 49. Highway Chauffeur control action context variables considered in STPA.

Control Action	Context Variable	Variable States
Adjust Lateral Position in δ Direction	Movement Relative to Lane Center	δ direction is away from lane center
		δ direction is toward lane center
	Lateral Commands From Other Systems	None
		In same direction as δ
		In opposite direction of δ
		In multiple directions
Change Lanes while Maintaining Speed	Target Lane Space	Clear of vehicles/objects
		Object/vehicle adjacent to host vehicle
		Object/vehicle adjacent rear of host vehicle

[28] The context variables describe the context in which a controller issues a control action. For example, the control command "disengage ALC system" may operate in the context of the driver's request to disengage the ALC system, the driver's attentiveness, and disengage or suspend requests from other vehicle systems.

Control Action	Context Variable	Variable States
		Object/vehicle adjacent front of host vehicle
	Current Lane Space	Clear of vehicles/objects
		Vehicle/object ahead
Issue Takeover Request	Driver Status	Attentive
		Not attentive
		Unknown
	ODD Status	At limit
		Approaching limit
		Fully within

The context variables considered for each control action for the human driver/operator are shown in Table 50.

Table 50. Human driver/operator control action context variables considered in STPA.

Control Action	Context Variable	Variable States
Press button to enable/disable the system	Highway Chauffeur System Status	Enabled
		Transitioning Control to Driver
		Disabled
Input steering command	Highway Chauffeur System Status	Enabled
		Transitioning Control to Driver
		Disabled
	Highway Chauffeur System Maneuver	Maintain Lane Position
		Lane Change
Increase/decrease/maintain accelerator pedal position	Highway Chauffeur System Status	Enabled
		Transitioning Control to Driver
		Disabled
	Highway Chauffeur System Maneuver	Maintain Lane Position
		Lane Change
Increase/decrease/maintain brake pedal position	Highway Chauffeur System Status	Enabled
		Transitioning Control to Driver
		Disabled
	Highway Chauffeur System Maneuver	Maintain Lane Position
		Lane Change

3. Apply the UCA guidewords to each control action. The original STPA literature includes four such guidewords (Leveson, 2012). This study uses a set of six guidewords for the identification of UCAs as illustrated in Figure 7.

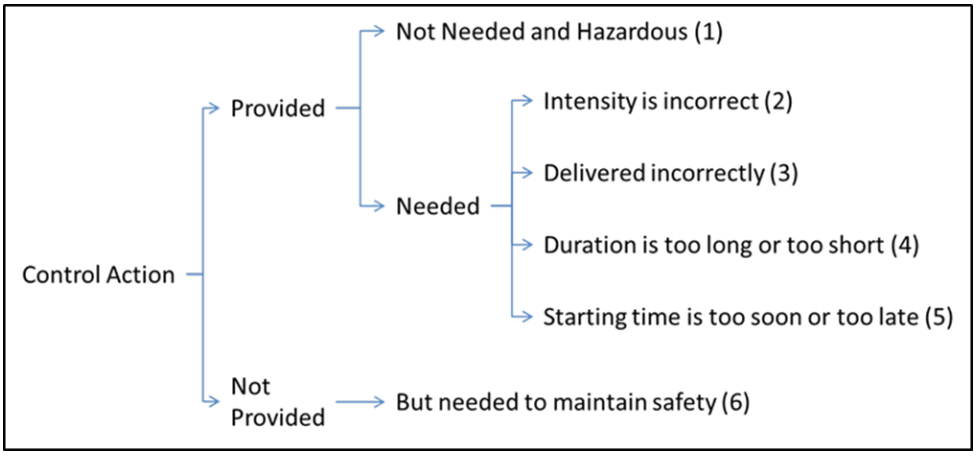

Figure 7. Guidewords used to derive UCAs in this study.

For each control action, assess each of the six guidewords against each of the context variable combinations to determine if it could lead to any of the preliminary vehicle-level hazards. If this step identifies new hazards, add them to the vehicle-level hazard list.

4. Apply logical reduction to the resulting UCA matrix using the Quine-McCluskey minimization algorithm (Coudert, 1994) in order to reduce the number of UCA statements.

Table 51 provides examples of UCAs for the highway chauffeur control module and driver derived using the above process.

Table 51. Example UCAs derived for this study.

Unsafe Control Action	Potential Vehicle-Level Hazard
The highway chauffeur system adjusts the lateral position in the δ direction during a lane following maneuver when: - the direction of δ is away from the lane center.	H1
The highway chauffeur system initiates a lane change with constant speed when: - the target lane is clear, or the target lane has a vehicle or object slightly ahead of or behind the host vehicle, and - there is a vehicle or object ahead of the host vehicle in the current lane, but the lateral adjustment is executed too late.	H3
The driver increases the brake pedal position when: - the system is enabled or transitioning control to the driver, and - the system is executing a lane change.	H2, H3

Comparing the UCAs derived in this study with those derived for a prior study of the functional safety for a generic ALC system (Brewer et al., 2018), finds that a common set of UCAs could support both the functional safety and SOTIF processes. This is reflected in the analysis process shown in Figure 3.

B.3 STPA Causal Scenario Derivation

Causal scenarios are developed for each identified UCA, based on the components and interactions in the control structure representation of the system. In the context of SOTIF, causal scenarios are similar to triggering events. By considering both the human driver/operator and technical system, STPA allows identification of both Type I and Type II triggering events.

This study adopted the following approach in deriving causal scenarios.

1. Each component and connection in the system, including the actuating foundational systems and controlled process (i.e., vehicle), were evaluated to identify limitations that could lead to potential unintended behavior (i.e., UCAs). In order to compete this analysis, the highway chauffeur control module was decomposed into various perception and path-planning algorithm components, as shown in Figure 5. Table 52 provides examples of causal scenarios derived for the UCA examples in Table 51.

Table 52. Example causal scenarios based on system limitations.

Unsafe Control Action and Causal Scenarios		Potential Vehicle-Level Hazard
The highway chauffeur system adjusts the lateral position in the δ direction during a lane following maneuver when: - the direction of δ is away from the lane center.		H1
LM-3	The lane model algorithm may incorrectly determine the lane lines such that the perceived location infringes on adjacent lanes or is otherwise outside the current travel lane.	
LM-7	The lane model algorithm perceives other environmental features as the lane lines (e.g., skid marks, ghost markings, or other false positive lane marker detection).	
The highway chauffeur system initiates a lane change with constant speed when: - the target lane is clear, or the target lane has a vehicle or object slightly ahead of or behind the host vehicle, and - there is a vehicle or object ahead of the host vehicle in the current lane, but the lateral adjustment is executed too late.		H3
FS-2	There may be a delay before the free space algorithm updates incorrect free space information about the target lane with the correct data.	
VP-1	The vehicle position algorithm incorrectly determines the host vehicle position in the lane.	

2. Next, the causal scenario analysis identified environmental factors that may lead to UCAs. This was performed by considering environmental factors both at a general level (e.g., weather effects) and at a specific level. This study used the list of scenario variables in Appendix A to guide the identification of relevant environmental factors. Table 53 provides examples of these causal scenarios.

Table 53. Example causal scenarios based on environmental factors.

Unsafe Control Action and Causal Scenarios		Potential Vehicle-Level Hazard
The highway chauffeur system adjusts the lateral position in the δ direction during a lane following maneuver when: - the direction of δ is away from the lane center.		H1
CS-2	Obstructions may block the camera's view of lane markings, vehicles, or other objects.	
VP-1	The vehicle position algorithm incorrectly determines the host vehicle position in the lane.	
The highway chauffeur system initiates a lane change with constant speed when: - the target lane is clear, or the target lane has a vehicle or object slightly ahead of or behind the host vehicle, and - there is a vehicle or object ahead of the host vehicle in the current lane, but the lateral adjustment is executed too late.		H3
RS-1	Water film on the radar antenna may lead to partial or total loss of the radar signal, particularly in the millimeter frequency range.	
CS-3	The camera may have deteriorated performance in environmental conditions that reduce visibility, such as weather or low lighting.	

3. Finally, this study identified causal scenarios related to foreseeable misuse (Type II triggering events). In this study, the foreseeable misuse causal scenarios typically focused on UCAs related to the human driver/operator. That is, foreseeable misuse is described by potentially unsafe actions taken by the driver/operator. The causal scenarios were derived by modelling the human driver/operator decision-making according to Annex E of PAS 21448 and as shown in Figure 5. Table 54 provides examples of these causal scenarios based on the human driver/operator UCA example in Table 51.

Table 54. Example foreseeable misuse causal scenarios.

Unsafe Control Action and Causal Scenarios		Potential Vehicle-Level Hazard
The driver increases the brake pedal position when: - the system is enabled or transitioning control to the driver, and - the system is executing a lane change.		H2, H3
DR-1	The driver does not understand the system operation, including controls, warnings, system states, and control transition process and timing.	
DA-1	The driver may unintentionally deactivate the system by incorrectly interacting with the foundational systems (reflexively, intentionally, or accidentally).	

Each causal scenario could be refined into a set of more detailed scenarios, as described in Section 6.3.

Appendix C: Allocation of Scenario Variables to Triggering Events

● - Indicates a scenario variable that could directly cause a triggering event to occur.

○ - Indicates a secondary variable that could help assess the impact of the triggering event against a more challenging scenario.

Camera Sensor Triggering Events and Example Scenario Variables Based on Crash Database Variables

Camera sensor does not detect lane lines because the lane markings are partially or fully covered.	**CS-1**
Scenario Variable	
Entrance/Exit Ramp	○
Narrow Lane	○
Merging	○
Branching	○
Curve Right	○
Curve Left	○
Other Maintenance or Construction-Related Condition	●
Surface Under Water	●
Snow	●
Sand	●
Water (standing or moving)	●
Mud, Dirt, Gravel	●
Slush	●
No Markings or Obscured Lane Markings	●
Debris or Objects in Road	●

Obstructions in the camera's field of view may block lane markings or other vehicles.	**CS-2**
Scenario Variable	
Median Crossover Road	○
Tollbooth/Tollgate	○
Entrance/Exit Ramp	○
Narrow Lane	○
Merging	○

Obstructions in the camera's field of view may block lane markings or other vehicles.	**CS-2**
Branching	o
Curb	o
Concrete Barrier	o
Guardrails	o
Grating	o
Telephone Poles	o
Curve Right	o
Curve Left	o
Other Maintenance or Construction-Related Condition	o
Cones	o
Tollbooth/Plaza Related	o
Regulatory Sign	o
Warning/Information/Temporary Sign	o
Traffic Officer/Flag Person/Hand Signs	o
Compact Sedan	o
Mid-size Sedan	o
Large Sedan	o
Van	o
Pickup Truck	o
SUV	o
Sub-Compact Sedan	o
Motorcycle	o
Special Cargo Body Type (e.g., garbage, gravel, flatbed, auto transporter)	o
Large Vehicle Configuration (e.g., bus, tractor-trailer, single-unit truckv, etc.)	o
Towed Vehicle (fixed or non-fixed linkage)	o
Multiple Trailing Units	o
Wide-Load Vehicle	o
Mini-Compact Sedan	o
Pedestrian, Bicyclist, Other Cyclist or Person on Personal Conveyances in Travel Lane	o
Sleet/Hail	●
Snow	●
Blowing Snow	●
Freezing Rain or Drizzle	●

Obstructions in the camera's field of view may block lane markings or other vehicles.	**CS-2**
Splash or Spray From Another Vehicle	●
Construction	●
Utility Work	●
Maintenance	●
[Vision Obscured by] In-Transport Motor Vehicle (including load)	●
Debris or Objects in Road	●
[Vision Obscured by] Curve, Hill, or Other Roadway Design Features	●
[Vision Obscured by] Building, Billboard, etc.	●
[Vision Obscured by] Trees, Crops, Vegetation	●
[Vision Obscured by] Not-in-Transport Motor Vehicle (parked, working)	●
Pedestrian, Bicyclist, Other Cyclist, or Person on Personal Conveyances Crossing Expressway	○

The camera may have deteriorated performance in environmental conditions that reduce visibility, such as weather or low lighting.	**CS-3**
Scenario Variable	
Median Crossover Road	○
Tollbooth/Tollgate	○
Entrance/Exit Ramp	○
Narrow Lane	○
Merging	○
Branching	○
Median	○
Curb	○
Concrete Barrier	○
Guardrails	○
Grating	○
Telephone Poles	○
Curve Right	○
Curve Left	○
Cones	○
Tollbooth/Plaza Related	○
Regulatory Sign	○

The camera may have deteriorated performance in environmental conditions that reduce visibility, such as weather or low lighting.	**CS-3**
Warning/Information/Temporary Sign	○
Traffic Officer/Flag Person/Hand Signs	○
Compact Sedan	○
Mid-size Sedan	○
Large Sedan	○
Van	○
Pickup Truck	○
SUV	○
Sub-Compact Sedan	○
Motorcycle	○
Special Cargo Body Type (e.g., garbage, gravel, flatbed, auto transporter)	○
Large Vehicle Configuration (bus, tractor-trailer, single-unit truckv, etc.)	○
Towed Vehicle (fixed or non-fixed linkage)	○
Multiple Trailing Units	○
Wide-Load Vehicle	○
Mini-Compact Sedan	○
Pedestrian, Bicyclist, Other Cyclist or Person on Personal Conveyances in Travel Lane	○
Rain	●
Sleet/Hail	●
Snow	●
Blowing Snow	●
Freezing Rain or Drizzle	●
Fog, Smog, Smoke	●
Blowing Sand, Soil, Dirt	●
Dark (lighted)	●
Dark (unlighted)	●
Dawn	●
Dusk	●
Construction	○
Utility Work	○
Maintenance	○
Dense Foliage	●

The camera may have deteriorated performance in environmental conditions that reduce visibility, such as weather or low lighting.	**CS-3**
Debris or Objects in Road	○
Pedestrian, Bicyclist, Other Cyclist, or Person on Personal Conveyances Crossing Expressway	○
Non-Motorist Not Visible (dark clothing, no lighting, etc.) or Failing to Have Lights on When Required	○

Environmental noise factors, such as light reflection or shadows, may affect the camera's ability to detect lane markings, vehicles, or other objects.	**CS-4**
Scenario Variable	
Median Crossover Road	○
Tollbooth/Tollgate	○
Entrance/Exit Ramp	○
Narrow Lane	○
Merging	○
Branching	○
Curb	○
Concrete Barrier	○
Guardrails	○
Grating	○
Telephone Poles	●
Curve Right	○
Curve Left	○
Hillcrest	○
Tunnels	●
Bridges (double-deck, covered, viaduct, etc.)	●
Tall Buildings (e.g., urban canyon)	●
Geologic Formations (e.g., canyons, overhang)	●
Extraneous Road Surface Markings (e.g., skid marks)	●
Cones	○
Tollbooth/Plaza Related	○
Regulatory Sign	○
Warning/Information/Temporary Sign	○
Traffic Officer/Flag Person/Hand Signs	○

Environmental noise factors, such as light reflection or shadows, may affect the camera's ability to detect lane markings, vehicles, or other objects.	**CS-4**
Compact Sedan	○
Mid-size Sedan	○
Large Sedan	○
Van	○
Pickup Truck	○
SUV	○
Sub-Compact Sedan	○
Motorcycle	○
Special Cargo Body Type (e.g., garbage, gravel, flatbed, auto transporter)	●
Large Vehicle Configuration (e.g., bus, tractor-trailer, single-unit truckv, etc.)	●
Towed Vehicle (fixed or non-fixed linkage)	○
Multiple Trailing Units	●
Wide-Load Vehicle	●
Mini-Compact Sedan	○
Pedestrian, Bicyclist, Other Cyclist or Person on Personal Conveyances in Travel Lane	○
Dark (unlighted)	○
Dawn	○
Dusk	○
Reflected Glare, Bright Sunlight, Headlights	●
Dense Foliage	●
[Other Vehicle] Other Misbehavior – Moving (e.g., not dimming headlights)	●
Pedestrian, Bicyclist, Other Cyclist, or Person on Personal Conveyances Crossing Expressway	○

The camera may not detect roadside landmarks, such as concrete barriers or guardrails, if there is low contrast between the landmarks and the roadway or other environmental features.	**CS-5**
Scenario Variable	
Entrance/Exit Ramp	○
Narrow Lane	○
Merging	○
Branching	○
Curb	○

The camera may not detect roadside landmarks, such as concrete barriers or guardrails, if there is low contrast between the landmarks and the roadway or other environmental features.	**CS-5**
Concrete Barrier	○
Guardrails	○
Grating	○
Telephone Poles	○
Curve Right	○
Curve Left	○
Tall Buildings (e.g., urban canyon)	○
Clear/Cloudy	●
Snow	●
Dark (unlighted)	●
Dawn	●
Dusk	●
Dense Foliage	●
No Markings or Obscured Lane Markings	○

The camera may not detect lane markings if the lane markings have low contrast with the pavement or are below a minimum size or quality.	**CS-6**
Scenario Variable	
Entrance/Exit Ramp	○
Local Change in Surface (e.g., concrete bridge)	●
Bott's Dots or Cat's Eye	●
Other Non-Traditional Markings	●
Narrow Lane	○
Wide Lane	○
Merging	○
Branching	○
Curve Right	○
Curve Left	○
Tunnels	○
Other Maintenance or Construction-Related Condition	●
Shoulder Related (design or condition)	●

The camera may not detect lane markings if the lane markings have low contrast with the pavement or are below a minimum size or quality.	**CS-6**
Inadequate Construction or Poor Design of Roadway, Bridge, etc.	●
Wet	●
Snow	●
Slush	●

The vehicle or object in an adjacent lane may be outside the camera's field-of-view.	**CS-7**
Scenario Variable	
Entrance/Exit Ramp	●
Wide Lane	●
Merging	●
Curve Right	●
Curve Left	●
Motorcycle	○
Special Cargo Body Type (e.g., garbage, gravel, flatbed, auto transporter)	○
Mini-Compact Sedan	○
Pedestrian, Bicyclist, Other Cyclist or Person on Personal Conveyances in Travel Lane	○
Pedestrian, Bicyclist, Other Cyclist or Person on Personal Conveyances on Paved Shoulder/Bicycle Lane/Parking Lane	○
[Vision Obscured by] In-Transport Motor Vehicle (including load)	●
[Vision Obscured by] Curve, Hill, or Other Roadway Design Features	●

If lead vehicle tracking is used in the absence of clear lane markings, the lead vehicle may exceed the visual range of the camera.	**CS-8**
Scenario Variable	
Entrance/Exit Ramp	○
Branching	○
Curve Right	●
Curve Left	●
Hillcrest	●
Relative Speed Below Surrounding Traffic	●
Light or No Traffic	●

Rain	○
Sleet/Hail	○
Snow	○
Blowing Snow	○
Freezing Rain or Drizzle	○
Fog, Smog, Smoke	○
Blowing Sand, Soil, Dirt	○
Dark (lighted)	○
Dark (unlighted)	○
Dawn	○
Dusk	○
No Markings or Obscured Lane Markings	●

The camera may have limitations individually tracking multiple objects that are close together and moving at similar speeds.	**CS-9**
Scenario Variable	
Backup Due to Prior Non-Recurring Incident	●
Backup Due to Prior Crash	●
Backup Due to Regular Congestion	●
Tollbooth/Plaza Related	●
Compact Sedan	○
Mid-size Sedan	○
Large Sedan	○
Van	○
Pickup Truck	○
SUV	○
Sub-Compact Sedan	○
Motorcycle	○
Special Cargo Body Type (e.g., garbage, gravel, flatbed, auto transporter)	○
Large Vehicle Configuration (e.g., bus, tractor-trailer, single-unit truckv, etc.)	○
Towed Vehicle (fixed or non-fixed linkage)	○
Multiple Trailing Units	○
Wide-Load Vehicle	○
Mini-Compact Sedan	○

The camera may have limitations individually tracking multiple objects that are close together and moving at similar speeds.	**CS-9**
Pedestrian, Bicyclist, Other Cyclist or Person on Personal Conveyances in Travel Lane	○
Pedestrian, Bicyclist, Other Cyclist or Person on Personal Conveyances on Paved Shoulder/Bicycle Lane/Parking Lane	○
Construction	●
Recent Previous Crash Scene Nearby	●
Stalled/Disabled Vehicle or Vehicle Fire	●
[Other Vehicle] Following Improperly	●
[Other Vehicle] Other Bad Driving	●
Struck by Falling Cargo or Something That Was Set in Motion by Vehicle	●

The camera may not be able to detect certain road surface or environmental conditions, such as black ice.	**CS-10**
Scenario Variable	
Local Change in Surface (e.g., concrete bridge)	○
Step Difference/Uneven	●
Ruts, Holes, Bumps in Road	●
Other Maintenance or Construction-Related Condition	●
Severe Crosswind	●
Wind From Passing Truck	●
Surface Under Water	●
Wet	●
Ice/Frost	●
Water (standing or moving)	●
Slush	●
Loose or Slippery Surface (mud, gravel, sand, wet leaves)	●
Dark (lighted)	○
Dark (unlighted)	○
Dawn	○
Dusk	○

Radar Sensor Triggering Events and Example Scenario Variables Based on Crash Database Variables

Water film on the radar antenna may lead to partial or total loss of the radar signal, particularly in the millimeter frequency range.	**RS-1**
Scenario Variable	
Tollbooth/Tollgate	o
Concrete Barrier	o
Guardrails	o
Cones	o
Tollbooth/Plaza Related	o
Compact Sedan	o
Mid-size Sedan	o
Large Sedan	o
Van	o
Pickup Truck	o
SUV	o
Sub-Compact Sedan	o
Motorcycle	o
Special Cargo Body Type (e.g., garbage, gravel, flatbed, auto transporter)	o
Large Vehicle Configuration (e.g., bus, tractor-trailer, single-unit truckv, etc.)	o
Towed Vehicle (fixed or non-fixed linkage)	o
Multiple Trailing Units	o
Wide-Load Vehicle	o
Mini-Compact Sedan	o
Pedestrian, Bicyclist, Other Cyclist or Person on Personal Conveyances in Travel Lane	o
Pedestrian, Bicyclist, Other Cyclist or Person on Personal Conveyances on Paved Shoulder/Bicycle Lane/Parking Lane	o
Rain	●
Sleet/Hail	●
Snow	●
Blowing Snow	●
Freezing Rain or Drizzle	●
Splash or Spray From Another Vehicle	●
Wet	●

Water film on the radar antenna may lead to partial or total loss of the radar signal, particularly in the millimeter frequency range.	**RS-1**
Snow	●
Water (standing or moving)	●
Slush	●
Pedestrian, Bicyclist, Other Cyclist, or Person on Personal Conveyances Crossing Expressway	○

The roadway geometry, such as curvature or grade, may prevent the radar from correctly determining the distance to other vehicles, including the lead vehicle.	**RS-2**
Scenario Variable	
Curve Right	●
Curve Left	●
Grade, Unknown Slope	●
Hillcrest	●
Sag (Bottom)	●
Compact Sedan	○
Mid-size Sedan	○
Large Sedan	○
Van	○
Pickup Truck	○
SUV	○
Sub-Compact Sedan	○
Motorcycle	○
Special Cargo Body Type (e.g., garbage, gravel, flatbed, auto transporter)	○
Large Vehicle Configuration (e.g., bus, tractor-trailer, single-unit truckv, etc.)	○
Towed Vehicle (fixed or non-fixed linkage)	○
Multiple Trailing Units	○
Wide-Load Vehicle	○
Mini-Compact Sedan	○
Pedestrian, Bicyclist, Other Cyclist or Person on Personal Conveyances in Travel Lane	○
Pedestrian, Bicyclist, Other Cyclist or Person on Personal Conveyances on Paved Shoulder/Bicycle Lane/Parking Lane	○
Stalled/Disabled Vehicle or Vehicle Fire	○
[Vision Obscured by] Curve, Hill, or Other Roadway Design Features	●

Reflective noise from the surrounding environment may degrade the signal quality or cause false signal detection.	**RS-3**
Scenario Variable	
Tollbooth/Tollgate	●
Step Difference/Uneven	●
Manhole Cover	●
Grating	●
Bridges (double-deck, covered, viaduct, etc.)	●
Tall Buildings (e.g., urban canyon)	●
Geologic Formations (e.g., canyons, overhang)	●
Ruts, Holes, Bumps in Road	●
Other Maintenance or Construction-Related Condition	●
Special Cargo Body Type (e.g., garbage, gravel, flatbed, auto transporter)	●
Wide-Load Vehicle	●
Blowing Sand, Soil, Dirt	●
Construction	●

The radar may not detect certain environmental features with sufficient confidence, such as guardrails.	**RS-4**
Scenario Variable	
Tollbooth/Tollgate	●
Entrance/Exit Ramp	○
Merging	○
Branching	○
Curb	●
Concrete Barrier	●
Guardrails	●
Grating	●
Telephone Poles	●
Curve Right	○
Curve Left	○
Hillcrest	○

The radar may not detect certain environmental features with sufficient confidence, such as guardrails.	**RS-4**
Bridges (double-deck, covered, viaduct, etc.)	○
Other Maintenance or Construction-Related Condition	●
Shoulder Related (design or condition)	●
Cones	●

The radar may not detect vehicles with thin profiles, such as motorcycles or bicycles, or objects below a certain size.	**RS-5**
Scenario Variable	
Entrance/Exit Ramp	○
Merging	○
Tollbooth/Plaza Related	○
Motorcycle	●
Special Cargo Body Type (e.g., garbage, gravel, flatbed, auto transporter)	●
Pedestrian, Bicyclist, Other Cyclist or Person on Personal Conveyances in Travel Lane	●
Pedestrian, Bicyclist, Other Cyclist or Person on Personal Conveyances on Paved Shoulder/Bicycle Lane/Parking Lane	●
[Other Vehicle] Aggressive Behavior by Non-Contact Vehicle Owner	○
[Other Vehicle] Other Bad Driving	○
Pedestrian, Bicyclist, Other Cyclist, or Person on Personal Conveyances Crossing Expressway	●

The radar may have limitations individually tracking multiple objects that are close together and moving at similar speeds.	**RS-6**
Scenario Variable	
Backup Due to Prior Non-Recurring Incident	●
Backup Due to Prior Crash	●
Backup Due to Regular Congestion	●
Tollbooth/Plaza Related	●
Compact Sedan	○
Mid-size Sedan	○
Large Sedan	○
Van	○

The radar may have limitations individually tracking multiple objects that are close together and moving at similar speeds.	**RS-6**
Pickup Truck	○
SUV	○
Sub-Compact Sedan	○
Motorcycle	○
Special Cargo Body Type (e.g., garbage, gravel, flatbed, auto transporter)	○
Large Vehicle Configuration (e.g., bus, tractor-trailer, single-unit truckv, etc.)	○
Towed Vehicle (fixed or non-fixed linkage)	○
Multiple Trailing Units	○
Wide-Load Vehicle	○
Mini-Compact Sedan	○
Pedestrian, Bicyclist, Other Cyclist or Person on Personal Conveyances in Travel Lane	○
Pedestrian, Bicyclist, Other Cyclist or Person on Personal Conveyances on Paved Shoulder/Bicycle Lane/Parking Lane	○
Construction	●
Recent Previous Crash Scene Nearby	●
Stalled/Disabled Vehicle or Vehicle Fire	●
[Other Vehicle] Following Improperly	●
[Other Vehicle] Other Bad Driving	●
Struck by Falling Cargo or Something That Was Set in Motion by Vehicle	●

GPS/Maps Triggering Events and Example Scenario Variables Based on Crash Database Variables

A delay in the update rate for the vehicle location may cause the system to operate with an outdated host vehicle position in the lane.	**GM-1**
Scenario Variable	
Entrance/Exit Ramp	○
Narrow Lane	○
Merging	○
Branching	○
Curve Right	○
Curve Left	○
Tunnels	●
Bridges (double-deck, covered, viaduct, etc.)	●
Tall Buildings (e.g., urban canyon)	●
Geologic Formations (e.g., canyons, overhang)	●
Tollbooth/Plaza Related	○

The tolerance range for the host vehicle position may be too high causing the system to incorrectly determine the vehicle's travel lane or position in the roadway.	**GM-2**
Scenario Variable	
Entrance/Exit Ramp	○
Narrow Lane	○
Merging	○
Branching	○
Curve Right	○
Curve Left	○
Tunnels	●
Bridges (double-deck, covered, viaduct, etc.)	●
Tall Buildings (e.g., urban canyon)	●
Geologic Formations (e.g., canyons, overhang)	●
Tollbooth/Plaza Related	○

The GPS or map data may be out of date, causing the system to have an incorrect understanding of the roadway type, travel lanes, or vehicle position.	**GM-3**
Scenario Variable	
Parking Garage	●
Other Maintenance or Construction-Related Condition	o
Shoulder Related (design or condition)	o
Construction	o
Utility Work	o
Maintenance	o

Information provided by the maps may be incorrect, causing algorithms to have an incorrect understanding of the roadway type or travel lane.	**GM-4**
Scenario Variable	
Median Crossover Road	o
Tollbooth/Tollgate	o
Entrance/Exit Ramp	o
Narrow Lane	o
Wide Lane	o
Merging	o
Branching	o
Straight	o
Curve Right	o
Curve Left	o
Posted Speed Limit	o
Variable Speed Zone	o
Other Maintenance or Construction-Related Condition	o
Shoulder Related (design or condition)	o
Construction	o
Inadequate Warning of Exits, Narrowing Lanes, Traffic Controls, etc.	o

Lane Model Algorithm Triggering Events and Example Scenario Variables Based on Crash Database Variables

The lane model algorithm may incorrectly determine the edges of features (e.g., Carny edge detection error).	**LM-1**
Scenario Variable	
Curb	○
Concrete Barrier	○
Guardrails	○
Ruts, Holes, Bumps in Road	●
Other Maintenance or Construction-Related Condition	●
Extraneous Road Surface Markings (e.g., skid marks)	●
Debris or Objects in Road	○
Struck by Falling Cargo or Something That Was Set in Motion by Vehicle	○

The lane model algorithm may incorrectly interpolate data to determine the straightness of the lane lines (e.g., Hough transformation error).	**LM-2**
Scenario Variable	
Local Change in Surface (e.g., concrete bridge)	○
Step Difference/Uneven	○
Bott's Dots or Cat's Eye	●
Other Non-Traditional Markings	●
Narrow Lane	●
Wide Lane	●
Merging	●
Branching	●
Straight	○
Curve Right	○
Curve Left	○
Ruts, Holes, Bumps in Road	●
Other Maintenance or Construction-Related Condition	●
Extraneous Road Surface Markings (e.g., skid marks)	●
No Markings or Obscured Lane Markings	●

The lane model algorithm may incorrectly determine the lane lines such that the perceived location infringes on adjacent lanes or is otherwise outside the current travel lane.	**LM-3**
Scenario Variable	
Tollbooth/Tollgate	○
Entrance/Exit Ramp	○
Bott's Dots or Cat's Eye	●
Other Non-Traditional Markings	●
Narrow Lane	○
Wide Lane	○
Merging	○
Branching	○
Other Maintenance or Construction-Related Condition	●
Extraneous Road Surface Markings (e.g., skid marks)	●
Inadequate Construction or Poor Design of Roadway, Bridge, etc.	●
Cones	●
No Markings or Obscured Lane Markings	●

The lane model algorithm may incorrectly determine the lane lines for the adjacent lane are closer to the current travel lane than they actually are (i.e., the adjacent lane is off-set toward the current travel lane).	**LM-4**
Scenario Variable	
Narrow Lane	●
Other Maintenance or Construction-Related Condition	○
Tollbooth/Plaza Related	○
Construction	○
No Markings or Obscured Lane Markings	●

There may be a delay before the lane model algorithm updates incorrect lane line information with the correct lane line information.	**LM-5**
Scenario Variable	
Entrance/Exit Ramp	●
Bott's Dots or Cat's Eye	●
Other Non-Traditional Markings	●

There may be a delay before the lane model algorithm updates incorrect lane line information with the correct lane line information.	**LM-5**
Narrow Lane	○
Wide Lane	○
Merging	○
Branching	●
Hillcrest	○
Tunnels	○
Other Maintenance or Construction-Related Condition	●
Extraneous Road Surface Markings (e.g., skid marks)	●
Cones	●
No Markings or Obscured Lane Markings	●

The lane model algorithm may incorrectly categorize other roadway features, such as off-ramps or branching lanes, as a continuation of the current travel lane.	**LM-6**
Scenario Variable	
Entrance/Exit Ramp	●
Branching	●
Curve Right	○
Curve Left	○
Hillcrest	○
Other Maintenance or Construction-Related Condition	○
Shoulder Related (design or condition)	○
Extraneous Road Surface Markings (e.g., skid marks)	○
No Markings or Obscured Lane Markings	○
Inadequate Warning of Exits, Narrowing Lanes, Traffic Controls, etc.	○

The lane model algorithm perceives other environmental features as the lane lines (e.g., skid marks, ghost markings, or other false positive lane marker detection).	**LM-7**
Scenario Variable	
Telephone Poles	●
Other Maintenance or Construction-Related Condition	●
Extraneous Road Surface Markings (e.g., skid marks)	●

The lane model algorithm perceives other environmental features as the lane lines (e.g., skid marks, ghost markings, or other false positive lane marker detection).	**LM-7**
Inadequate Construction or Poor Design of Roadway, Bridge, etc.	●
Dense Foliage	●
No Markings or Obscured Lane Markings	●

Fusion Tracker Algorithm Triggering Events and Example Scenario Variables Based on Crash Database Variables

The fusion tracker algorithm may incorrectly combine camera and radar data from multiple objects (e.g., assign the incorrect velocity to an object in the adjacent lane).	**FT-1**
Scenario Variable	
Narrow Lane	O
Wide Lane	O
Merging	O
Branching	O
Curve Right	O
Curve Left	O
Tollbooth/Plaza Related	O
Compact Sedan	O
Mid-size Sedan	O
Large Sedan	O
Van	O
Pickup Truck	O
SUV	O
Sub-Compact Sedan	O
Motorcycle	O
Special Cargo Body Type (e.g., garbage, gravel, flatbed, auto transporter)	O
Large Vehicle Configuration (e.g., bus, tractor-trailer, single-unit truckv, etc.)	O
Towed Vehicle (fixed or non-fixed linkage)	O
Multiple Trailing Units	O
Wide-Load Vehicle	O
Mini-Compact Sedan	O
Pedestrian, Bicyclist, Other Cyclist or Person on Personal Conveyances in Travel Lane	O
[Other Vehicle] Aggressive Behavior by Non-Contact Vehicle Owner	O
[Other Vehicle] Following Improperly	O
[Other Vehicle] Driving Wrong Way or on Wrong Side	O
[Other Vehicle] Other Bad Driving	O
Nearby Trailer (Swerving, Swaying, or Fishtailing)	O
Non-Motorist Improper or Erratic Lane Changing	O

The fusion tracker algorithm may incorrectly combine camera and radar data from multiple objects (e.g., assign the incorrect velocity to an object in the adjacent lane).	**FT-1**
Non-Motorist Passing With Insufficient Distance or Inadequate Visibility, or Failing to Yield to Overtaking Vehicle	O
Non-Motorist Making Improper Entry to or Exit From Trafficway	O
Non-Motorist Improper Passing	O
Struck by Falling Cargo or Something That Was Set in Motion by Vehicle	O

There may be a delay before the fusion tracker algorithm updates incorrectly associated object tracks from the camera and radar data.	**FT-2**
Scenario Variable	
Narrow Lane	O
Wide Lane	O
Merging	O
Branching	O
Curve Right	O
Curve Left	O
Tollbooth/Plaza Related	O
Compact Sedan	O
Mid-size Sedan	O
Large Sedan	O
Van	O
Pickup Truck	O
SUV	O
Sub-Compact Sedan	O
Motorcycle	O
Special Cargo Body Type (e.g., garbage, gravel, flatbed, auto transporter)	O
Large Vehicle Configuration (e.g., bus, tractor-trailer, single-unit truckv, etc.)	O
Towed Vehicle (fixed or non-fixed linkage)	O
Multiple Trailing Units	O
Wide-Load Vehicle	O
Mini-Compact Sedan	O
Pedestrian, Bicyclist, Other Cyclist or Person on Personal Conveyances in Travel Lane	O
[Other Vehicle] Aggressive Behavior by Non-Contact Vehicle Owner	O

There may be a delay before the fusion tracker algorithm updates incorrectly associated object tracks from the camera and radar data.	**FT-2**
[Other Vehicle] Following Improperly	O
[Other Vehicle] Driving Wrong Way or on Wrong Side	O
[Other Vehicle] Other Bad Driving	O
Nearby Trailer (Swerving, Swaying, or Fishtailing)	O
Non-Motorist Improper or Erratic Lane Changing	O
Non-Motorist Passing With Insufficient Distance or Inadequate Visibility, or Failing to Yield to Overtaking Vehicle	O
Non-Motorist Making Improper Entry to or Exit From Trafficway	O
Non-Motorist Improper Passing	O
Struck by Falling Cargo or Something That Was Set in Motion by Vehicle	O

The fusion tracker algorithm may not update the fusion map with sufficient frequency to capture maneuvers by other vehicles (e.g., double-lane change, high speed).	**FT-3**
Scenario Variable	
Entrance/Exit Ramp	O
Merging	O
Curve Right	O
Curve Left	O
Backup Due to Prior Non-Recurring Incident	O
Backup Due to Prior Crash	O
Backup Due to Regular Congestion	O
Tollbooth/Plaza Related	O
Recent Previous Crash Scene Nearby	O
Police Pursuit	O
Stalled/Disabled Vehicle or Vehicle Fire	O
[Other Vehicle] Aggressive Behavior by Non-Contact Vehicle Owner	O
[Other Vehicle] Following Improperly	O
[Other Vehicle] Passing Through or Around Barrier	O
[Other Vehicle] Driving Wrong Way or on Wrong Side	O
[Other Vehicle] Other Bad Driving	O
Non-Motorist Improper or Erratic Lane Changing	O
Non-Motorist Improper Passing	O

The fusion tracker algorithm may incorrectly establish a vehicle in the target lane when no vehicle exists (false positive).	**FT-4**
Scenario Variable	
Merging	O
Branching	O
Curve Right	O
Curve Left	O
Bridges (double-deck, covered, viaduct, etc.)	O
Tall Buildings (e.g., urban canyon)	O
Other Maintenance or Construction-Related Condition	O
Shoulder Related (design or condition)	O
Cones	O
Fog, Smog, Smoke	O
Blowing Sand, Soil, Dirt	O
Construction	O
Utility Work	O
Maintenance	O

Host Vehicle State Algorithm Triggering Events and Example Scenario Variables Based on Crash Database Variables

The vehicle state algorithms may have an incorrect model of the host vehicle size or configuration (e.g., attached trailer).	**VS-1**
Scenario Variable	
Merging	O
Backup Due to Prior Non-Recurring Incident	O
Backup Due to Prior Crash	O
Backup Due to Regular Congestion	O

The vehicle state algorithm has incorrect information leading to an incorrect time-to-collision calculation.	**VS-2**
Scenario Variable	
Narrow Lane	O
Merging	O
Backup Due to Prior Non-Recurring Incident	O
Backup Due to Prior Crash	O
Backup Due to Regular Congestion	O
Severe Crosswind	O
Wind From Passing Truck	O

Host Vehicle Position Algorithm Triggering Events and Example Scenario Variables Based on Crash Database Variables

The vehicle position algorithm incorrectly determines the host vehicle position in the lane.	**VP-1**
Scenario Variable	
Tollbooth/Tollgate	O
Entrance/Exit Ramp	O
Narrow Lane	O
Wide Lane	O
Merging	O
Branching	O
Curve Right	O
Curve Left	O
Severe Crosswind	O
Wind From Passing Truck	O
No Markings or Obscured Lane Markings	●

There may be a delay before the vehicle position algorithm updates an incorrect host vehicle position with the correct vehicle position.	**VP-2**
Scenario Variable	
Entrance/Exit Ramp	O
Wide Lane	O
Branching	O
Tunnels	O
Bridges (double-deck, covered, viaduct, etc.)	O
Tall Buildings (e.g., urban canyon)	O
Extraneous Road Surface Markings (e.g., skid marks)	O
Severe Crosswind	O
Wind From Passing Truck	O
No Markings or Obscured Lane Markings	●

Object Trail/Tracker Algorithm Triggering Events and Example Scenario Variables Based on Crash Database Variables

In the absence of clear lane markings, the object trail/tracker algorithm may track the incorrect lead vehicle.	**OT-1**
Scenario Variable	
Entrance/Exit Ramp	●
Merging	●
Branching	●
Curve Right	●
Curve Left	●
Hillcrest	○
Extraneous Road Surface Markings (e.g., skid marks)	○
Cones	○
Light or No Traffic	○
Backup Due to Prior Non-Recurring Incident	○
Backup Due to Prior Crash	○
Backup Due to Regular Congestion	○
Tollbooth/Plaza Related	●
Motorcycle	○
Special Cargo Body Type (e.g., garbage, gravel, flatbed, auto transporter)	○
Wide-Load Vehicle	○
Pedestrian, Bicyclist, Other Cyclist or Person on Personal Conveyances in Travel Lane	○
Construction	○
Utility Work	○
Maintenance	○
No Markings or Obscured Lane Markings	●
Police Pursuit	○

In the absence of clear lane markings, the object trail/tracker algorithm tracks a lead vehicle that is not staying centered in the travel lane (e.g., swerving, exiting roadway, changing lanes).	**OT-2**
Scenario Variable	
Entrance/Exit Ramp	●
Merging	●

In the absence of clear lane markings, the object trail/tracker algorithm tracks a lead vehicle that is not staying centered in the travel lane (e.g., swerving, exiting roadway, changing lanes).	**OT-2**
Branching	●
Curve Right	●
Curve Left	●
No Markings or Obscured Lane Markings	●
[Other Vehicle] Traveling on Prohibited Trafficways	●
[Other Vehicle] Passing Through or Around Barrier	●
[Other Vehicle] Failure to Observe Warnings or Instructions on Vehicles Displaying Them	●
[Other Vehicle] Driving Wrong Way or on Wrong Side	●
[Other Vehicle] Other Bad Driving	●
[Other Vehicle] Disobeying Signs or Traffic Controls	●
[Other Vehicle] Other Driving in the Wrong Place (e.g., bike lane)	●

The object trail/tracker algorithm may have limitations differentiating between or tracking objects with similar speeds and which are close together.	**OT-3**
Scenario Variable	
Narrow Lane	●
Backup Due to Prior Non-Recurring Incident	●
Backup Due to Prior Crash	●
Backup Due to Regular Congestion	●
Tollbooth/Plaza Related	●
Compact Sedan	O
Mid-size Sedan	O
Large Sedan	O
Van	O
Pickup Truck	O
SUV	O
Sub-Compact Sedan	O
Motorcycle	O
Special Cargo Body Type (e.g., garbage, gravel, flatbed, auto transporter)	O
Large Vehicle Configuration (e.g., bus, tractor-trailer, single-unit truckv, etc.)	O
Towed Vehicle (fixed or non-fixed linkage)	O

The object trail/tracker algorithm may have limitations differentiating between or tracking objects with similar speeds and which are close together.	**OT-3**
Multiple Trailing Units	○
Wide-Load Vehicle	○
Mini-Compact Sedan	○
Pedestrian, Bicyclist, Other Cyclist or Person on Personal Conveyances in Travel Lane	○
[Other Vehicle] Following Improperly	●
Non-Motorist Passing With Insufficient Distance or Inadequate Visibility, or Failing to Yield to Overtaking Vehicle	●

The object trail/tracker algorithm may incorrectly assign the track of an object to the incorrect lane (e.g., two lanes over instead of the adjacent lane).	**OT-4**
Scenario Variable	
Wide Lane	●
Merging	●
Curve Right	○
Curve Left	○
Other Maintenance or Construction-Related Condition	●
Extraneous Road Surface Markings (e.g., skid marks)	●
Tollbooth/Plaza Related	○
[Other Vehicle] Other Bad Driving	●
[Other Vehicle] Other Driving in the Wrong Place (e.g., bike lane)	○
Nearby Trailer (Swerving, Swaying, or Fishtailing)	●
Non-Motorist Improper or Erratic Lane Changing	●

The object trail/tracker algorithm may incorrectly anticipate that a vehicle in the adjacent lane is changing to another lane (e.g., other vehicle aborts a lane change).	**OT-5**
Scenario Variable	
Entrance/Exit Ramp	○
Wide Lane	○
Branching	○
Other Maintenance or Construction-Related Condition	○
Extraneous Road Surface Markings (e.g., skid marks)	○
Tollbooth/Plaza Related	○

The object trail/tracker algorithm may incorrectly anticipate that a vehicle in the adjacent lane is changing to another lane (e.g., other vehicle aborts a lane change).	**OT-5**
Severe Crosswind	○
Wind From Passing Truck	○
Construction	○
Utility Work	○
Maintenance	○
[Other Vehicle] Aggressive Behavior by Non-Contact Vehicle Owner	○
[Other Vehicle] Following Improperly	○
[Other Vehicle] Failure to Signal Intentions	●
[Other Vehicle] Other Bad Driving	●
Nearby Trailer (Swerving, Swaying, or Fishtailing)	●
Non-Motorist Improper or Erratic Lane Changing	●

The object trail/tracker algorithm may prematurely delete a track or may not confirm a track for an existing object.	**OT-6**
Scenario Variable	
Entrance/Exit Ramp	●
Wide Lane	●
Branching	●
Curve Right	●
Curve Left	●
Other Maintenance or Construction-Related Condition	●
Tollbooth/Plaza Related	●
Motorcycle	●
Special Cargo Body Type (e.g., garbage, gravel, flatbed, auto transporter)	●
Multiple Trailing Units	●
Wide-Load Vehicle	●
Pedestrian, Bicyclist, Other Cyclist or Person on Personal Conveyances in Travel Lane	●
[Other Vehicle] Following Improperly	○
[Other Vehicle] Passing Through or Around Barrier	○
[Vision Obscured by] In-Transport Motor Vehicle (including load)	●
Non-Motorist Improper or Erratic Lane Changing	●

If two objects or vehicles are close together and one object moves away (e.g., changes lanes), the object trail/tracker algorithm may incorrectly delete the track for the remaining object.	**OT-7**
Scenario Variable	
Entrance/Exit Ramp	○
Branching	○
Compact Sedan	○
Mid-size Sedan	○
Large Sedan	○
Van	○
Pickup Truck	○
SUV	○
Sub-Compact Sedan	○
Motorcycle	●
Special Cargo Body Type (e.g., garbage, gravel, flatbed, auto transporter)	●
Large Vehicle Configuration (e.g., bus, tractor-trailer, single-unit truckv, etc.)	○
Towed Vehicle (fixed or non-fixed linkage)	○
Multiple Trailing Units	○
Wide-Load Vehicle	○
Mini-Compact Sedan	○
Pedestrian, Bicyclist, Other Cyclist or Person on Personal Conveyances in Travel Lane	●

The object/trail tracker algorithm may not detect an object moving in front of the host vehicle during a lane change.	**OT-8**
Scenario Variable	
Entrance/Exit Ramp	○
Merging	○
Other Maintenance or Construction-Related Condition	○
Backup Due to Prior Non-Recurring Incident	○
Backup Due to Prior Crash	○
Backup Due to Regular Congestion	○
Tollbooth/Plaza Related	○
Compact Sedan	●
Mid-size Sedan	●

The object/trail tracker algorithm may not detect an object moving in front of the host vehicle during a lane change.	**OT-8**
Large Sedan	●
Van	●
Pickup Truck	●
SUV	●
Sub-Compact Sedan	●
Motorcycle	●
Special Cargo Body Type (e.g., garbage, gravel, flatbed, auto transporter)	●
Large Vehicle Configuration (e.g., bus, tractor-trailer, single-unit truckv, etc.)	●
Towed Vehicle (fixed or non-fixed linkage)	●
Multiple Trailing Units	●
Wide-Load Vehicle	●
Mini-Compact Sedan	●
Pedestrian, Bicyclist, Other Cyclist or Person on Personal Conveyances in Travel Lane	●
Rain	○
Sleet/Hail	○
Snow	○
Blowing Snow	○
Freezing Rain or Drizzle	○
Fog, Smog, Smoke	○
Blowing Sand, Soil, Dirt	○
Dark (unlighted)	○
Dawn	○
Dusk	○
Reflected Glare, Bright Sunlight, Headlights	○
[Other Vehicle] Aggressive Behavior by Non-Contact Vehicle Owner	●
[Other Vehicle] Following Improperly	●
[Other Vehicle] Passing Through or Around Barrier	●
[Other Vehicle] Driving Wrong Way or on Wrong Side	●
[Other Vehicle] Other Bad Driving	●
Non-Motorist Improper or Erratic Lane Changing	●
Non-Motorist Failure to Keep in Proper Lane or Running Off Road	●
Non-Motorist Making Improper Entry to or Exit From Trafficway	●

The object/trail tracker algorithm may not detect an object moving in front of the host vehicle during a lane change.	**OT-8**
Non-Motorist Improper Passing	●

The object trail/tracker may not correctly detect or classify the entire vehicle or object (e.g., develops tracks for a truck cab but not a flatbed trailer).	**OT-9**
Scenario Variable	
Special Cargo Body Type (e.g., garbage, gravel, flatbed, auto transporter)	●
Large Vehicle Configuration (e.g., bus, tractor-trailer, single-unit truckv, etc.)	●
Towed Vehicle (fixed or non-fixed linkage)	●
Multiple Trailing Units	●
Wide-Load Vehicle	●

Road Model Algorithm Triggering Events and Example Scenario Variables Based on Crash Database Variables

In the absence of clear lane markings or landmarks, the road model algorithm incorrectly establishes the travel lane and/or the target lane.	**RM-1**
Scenario Variable	
Tollbooth/Tollgate	●
Entrance/Exit Ramp	●
Bott's Dots or Cat's Eye	○
Other Non-Traditional Markings	○
Merging	●
Branching	●
Median	○
Curb	○
Grating	○
Curve Right	●
Curve Left	●
Hillcrest	○
Other Maintenance or Construction-Related Condition	○
Extraneous Road Surface Markings (e.g., skid marks)	○
Light or No Traffic	●
Tollbooth/Plaza Related	●
No Markings or Obscured Lane Markings	●
Recent Previous Crash Scene Nearby	○
Stalled/Disabled Vehicle or Vehicle Fire	○

The road model algorithm incorrectly estimates the road curvature and reports the incorrect curvature to the steerable path algorithms.	**RM-2**
Scenario Variable	
Merging	○
Branching	○
Curve Right	●
Curve Left	●
Hillcrest	○
Extraneous Road Surface Markings (e.g., skid marks)	●

The road model algorithm incorrectly estimates the road curvature and reports the incorrect curvature to the steerable path algorithms.	**RM-2**
[Vision Obscured by] Trees, Crops, Vegetation	○

There may be a delay before the road model algorithm updates incorrect lane boundary information with the correct lane boundary locations.	**RM-3**
Scenario Variable	
Entrance/Exit Ramp	●
Narrow Lane	●
Wide Lane	●
Merging	●
Branching	●
Hillcrest	●
Tunnels	●
Other Maintenance or Construction-Related Condition	●
Extraneous Road Surface Markings (e.g., skid marks)	●
Cones	●
Tollbooth/Plaza Related	○
No Markings or Obscured Lane Markings	●

There may be a delay before the road model algorithm updates incorrect roadway curvature information with the correct roadway geometry.	**RM-4**
Scenario Variable	
Merging	○
Branching	○
Curve Right	●
Curve Left	●
Hillcrest	○
Extraneous Road Surface Markings (e.g., skid marks)	●
[Vision Obscured by] Trees, Crops, Vegetation	○

Free Space Algorithm Triggering Events and Example Scenario Variables Based on Crash Database Variables

The free space algorithm may incorrectly determine the amount of free space in the target lane.	**FS-1**
Scenario Variable	
Narrow Lane	○
Wide Lane	○
Curve Right	○
Curve Left	○
Speed Inappropriate for Conditions (e.g., surface, geometry)	○
Backup Due to Prior Non-Recurring Incident	●
Backup Due to Prior Crash	●
Backup Due to Regular Congestion	●
Tollbooth/Plaza Related	○
Motorcycle	●
Special Cargo Body Type (e.g., garbage, gravel, flatbed, auto transporter)	●
Multiple Trailing Units	●
Wide-Load Vehicle	●
Pedestrian, Bicyclist, Other Cyclist or Person on Personal Conveyances in Travel Lane	●
Dark (lighted)	○
Dark (unlighted)	○
Dawn	○
Dusk	○
Dense Foliage	○
[Other Vehicle] Following Improperly	○
[Other Vehicle] Failure to Signal Intentions	○
[Other Vehicle] Other Bad Driving	○
Non-Motorist Improper or Erratic Lane Changing	○
Non-Motorist Failure to Keep in Proper Lane or Running Off Road	○

There may be a delay before the free space algorithm updates incorrect free space information about the target lane with the correct data.	**FS-2**
Scenario Variable	
Entrance/Exit Ramp	O
Wide Lane	O
Merging	O
Other Maintenance or Construction-Related Condition	O
Tollbooth/Plaza Related	O
Construction	O
[Other Vehicle] Aggressive Behavior by Non-Contact Vehicle Owner	O
[Other Vehicle] Other Bad Driving	O
Non-Motorist Improper or Erratic Lane Changing	O
Non-Motorist Making Improper Entry to or Exit From Trafficway	O

Driver Intention Algorithm Triggering Events and Example Scenario Variables Based on Crash Database Variables

The driver intention algorithm incorrectly assumes that the driver is attempting a maneuver and allows the host vehicle to get too close to other vehicles or objects on the roadway. There is a delay before the driver intention algorithm correctly determines that the driver is not performing a maneuver.	**DI-1**
Scenario Variable	
Tollbooth/Tollgate	O
Entrance/Exit Ramp	O
Narrow Lane	O
Merging	O
Curve Right	O
Curve Left	O
Tollbooth/Plaza Related	O
Construction	O
Utility Work	O
Maintenance	O

The driver intention algorithm may incorrectly disregard an intended maneuver by the driver and instead maintain the vehicle on the trajectory computed by the steerable path algorithm.	**DI-2**
Scenario Variable	
Entrance/Exit Ramp	O
Merging	O
Branching	O
Straight	O
Curve Right	O
Curve Left	O
Tollbooth/Plaza Related	O
Construction	O
Utility Work	O
Maintenance	O
Recent Previous Crash Scene Nearby	O
Police Pursuit	O

The driver intention algorithm may incorrectly disregard an intended maneuver by the driver and instead maintain the vehicle on the trajectory computed by the steerable path algorithm.	**DI-2**
Stalled/Disabled Vehicle or Vehicle Fire	O
[Other Vehicle] Driving Wrong Way or on Wrong Side	O
[Other Vehicle] Other Bad Driving	O
Nearby Trailer (Swerving, Swaying, or Fishtailing)	O
Debris or Objects in Road	O
Struck by Falling Cargo or Something That Was Set in Motion by Vehicle	O

The driver intention algorithm may incorrectly interpret a true steering input from the driver as incidental and therefore disregard an intended maneuver by the driver.	**DI-3**
Scenario Variable	
Entrance/Exit Ramp	O
Branching	O
Straight	O
Curve Right	O
Curve Left	O

Steerable Path Algorithm Triggering Events and Example Scenario Variables Based on Crash Database Variables

The steerable path algorithm may have an incorrect model of the host vehicle trajectory (e.g., speed, yaw).	**SP-1**
Scenario Variable	
Curve Right	○
Curve Left	○
Banked	○
Snow	●
Ice/Frost	●
Water (standing or moving)	●
Slush	●
Loose or Slippery Surface (mud, gravel, sand, wet leaves)	●

The trajectory computed by the steerable path algorithm may become unviable partway through the maneuver.	**SP-2**
Scenario Variable	
Entrance/Exit Ramp	○
Merging	○
Other Maintenance or Construction-Related Condition	○
Speed Inappropriate for Conditions (e.g., surface, geometry)	○
Tollbooth/Plaza Related	○
Special Cargo Body Type (e.g., garbage, gravel, flatbed, auto transporter)	○
Large Vehicle Configuration (e.g., bus, tractor-trailer, single-unit truckv, etc.)	○
Towed Vehicle (fixed or non-fixed linkage)	○
Multiple Trailing Units	○
Wide-Load Vehicle	○
Construction	●
Utility Work	○
Maintenance	○
Police Pursuit	○
[Other Vehicle] Aggressive Behavior by Non-Contact Vehicle Owner	●
[Other Vehicle] Following Improperly	●
[Other Vehicle] Traveling on Prohibited Trafficways	●

The trajectory computed by the steerable path algorithm may become unviable partway through the maneuver.	**SP-2**
[Other Vehicle] Passing Through or Around Barrier	●
[Other Vehicle] Driving Wrong Way or on Wrong Side	●
[Other Vehicle] Other Bad Driving	●
[Other Vehicle] Disobeying Signs or Traffic Controls	●
[Other Vehicle] Other Misbehavior – Fixed (e.g., open door into trafficway)	○
Nearby Trailer (Swerving, Swaying, or Fishtailing)	●
[Vision Obscured by] In-Transport Motor Vehicle (including load)	○
Non-Motorist Failure to Yield Right-of-Way	●
Non-Motorist Improper or Erratic Lane Changing	●
Non-Motorist Failure to Keep in Proper Lane or Running Off Road	●
Non-Motorist Making Improper Entry to or Exit From Trafficway	●
Non-Motorist Making Improper Turn or Merge	●
Non-Motorist Improper Passing	●
Non-Motorist Not Visible (dark clothing, no lighting, etc.) or Failing to Have Lights on When Required	○
Debris or Objects in Road	●
[Vision Obscured by] Curve, Hill, or Other Roadway Design Features	○
Struck by Falling Cargo or Something That Was Set in Motion by Vehicle	●

DOT HS 812 879
November 2020

U.S. Department
of Transportation

**National Highway
Traffic Safety
Administration**

14623-110520-v3