FTA RESEARCH

FEDERAL TRANSIT ADMINISTRATION

Hazard and Safety Analysis of Automated Transit Bus Applications

Final Report

APRIL 2020

FTA Report No. 0161
Federal Transit Administration

PREPARED BY
Christopher Becker
Ahmad Nasser
John Brewer
John A Volpe National Transportation Systems Center

U.S. Department of Transportation
Federal Transit Administration

COVER PHOTO

Image courtesy of Volpe Center

DISCLAIMER

Hazard and Safety Analysis of Automated Transit Bus Applications

Final Report

APRIL 2020

FTA Report No. 0161

PREPARED BY

Christopher Becker
Ahmad Nasser
John Brewer
John A Volpe National Transportation Systems Center
55 Broadway
Cambridge, MA 02142-1093

SPONSORED BY

Federal Transit Administration
Office of Research, Demonstration and Innovation
U.S. Department of Transportation
1200 New Jersey Avenue, SE
Washington, DC 20590

AVAILABLE ONLINE

https://www.transit.dot.gov/about/research-innovation

Metric Conversion Table

SYMBOL	WHEN YOU KNOW	MULTIPLY BY	TO FIND	SYMBOL
LENGTH				
in	inches	25.4	millimeters	mm
ft	feet	0.305	meters	m
yd	yards	0.914	meters	m
mi	miles	1.61	kilometers	km
VOLUME				
fl oz	fluid ounces	29.57	milliliters	mL
gal	gallons	3.785	liters	L
ft^3	cubic feet	0.028	cubic meters	m^3
yd^3	cubic yards	0.765	cubic meters	m^3
NOTE: volumes greater than 1000 L shall be shown in m^3				
MASS				
oz	ounces	28.35	grams	g
lb	pounds	0.454	kilograms	kg
T	short tons (2000 lb)	0.907	megagrams (or "metric ton")	Mg (or "t")
TEMPERATURE (exact degrees)				
^oF	Fahrenheit	5 (F-32)/9 or (F-32)/1.8	Celsius	^oC

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY	2. REPORT DATE April 2020	3. REPORT TYPE AND DATES COVERED Final Report

4. TITLE AND SUBTITLE Hazard and Safety Analysis of Automated Transit Bus Applications, Final Report	5. FUNDING NUMBERS HW11A1

6. AUTHOR(S)
Christopher Becker, Ahmad Nasser, John Brewer

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Department of Transportation John A Volpe National Transportation Systems Center 55 Broadway, Cambridge, MA 02142-1093	8. PERFORMING ORGANIZATION REPORT NUMBER DOT-VNTSC-FHWA-20-07

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSORING/MONITORING AGENCY REPORT NUMBER
U.S. Department of Transportation Federal Transit Administration Office of Research, Demonstration and Innovation East Building 1200 New Jersey Avenue, SE Washington, DC 20590	U.S. Department of Transportation Federal Highway Administration Intelligent Transportation System Joint Program Office 1200 New Jersey Avenue, SE Washington, DC 20590	FTA Report No. 0161

11. SUPPLEMENTARY NOTES [https://www.transit.dot.gov/about/research-innovation] [https://doi.org/10.21949/1518333]
Suggested citation: Federal Transit Administration. Hazard and Safety Analysis of Automated Transit Bus Applications. Washington, D.C.: United States Department of Transportation, 2020. https://doi.org/10.21949/1518333

12A. DISTRIBUTION/AVAILABILITY STATEMENT Available from: National Technical Information Service (NTIS), Springfield, VA 22161. Phone 703.605.6000, Fax 703.605.6900, email [orders@ntis.gov]	12B. DISTRIBUTION CODE TRI-30

13. ABSTRACT

In December 2018, the International Organization for Standardization (ISO) released Edition 2 of the industry's functional safety standard for road vehicles, ISO 26262. Although the previous edition of ISO 26262 focused on light-duty passenger vehicles, this new edition includes considerations for buses. This report presents the findings from an analysis that applies key concepts from Edition 2 of the ISO 26262 standard to a set of Level 0 to Level 2 driving automation systems in the context of a generic 40-ft transit bus. Although this study found that many of the same basic hazards exist for transit buses as for other vehicles, specific aspects of transit bus operations resulted in additional hazards and associated functional safety measures. The results of this research provide a useful reference for manufacturers on the application of hazard analysis and risk assessment concepts in the context of transit bus applications and for comparison of the results from internal system-specific hazard and safety analyses.

14. SUBJECT TERMS Transit buses, functional safety, ISO 26262, concept phase, automotive safety integrity level, ASIL, automation, object detection and collision avoidance, lane keeping/ lane centering, steering assist, docking, park assist, park out, yard park, automatic emergency braking, reverse brake assist, full park assist, valet parking (bus yard), adaptive cruise control with/without stop and go, traffic jam assist with lane keeping/ lane centering	15. NUMBER OF PAGES 154

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	Unlimited

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Abstract

In December 2018, the International Organization for Standardization (ISO) released Edition 2 of the industry's functional safety standard for road vehicles, ISO 26262. Although the previous edition of ISO 26262 focused on light-duty passenger vehicles, this new edition includes considerations for buses. This report presents the findings from an analysis that applies key concepts from Edition 2 of the ISO 26262 standard to a set of Level 0 to Level 2 driving automation systems in the context of a generic 40-ft transit bus. Although this study found that many of the same basic hazards exist for transit buses as for other vehicles, specific aspects of transit bus operations resulted in additional hazards and associated functional safety measures. The results of this research provide a useful reference for manufacturers on the application of hazard analysis and risk assessment concepts in the context of transit bus applications and for comparison of the results from internal system-specific hazard and safety analyses.

EXECUTIVE SUMMARY

The extension of driving automation systems to transit buses has the potential to alter the urban transportation landscape. This project helps accelerate the development and safe deployment of driving automation systems in transit buses by identifying potential hazards and safety measures related to these technologies. Specifically, this project considered nine categories of driving automation systems derived from the *Transit Bus Automation Project: Transferability of Automation Technologies Final Report* [1]. These driving automation systems operate at Automation Levels 0 to 2, as defined in SAE International Recommended Practice J3016 [2].

To identify the potential hazards and safety measures, this project applied key concepts from the International Organization for Standardization (ISO) voluntary functional safety standard, ISO 26262. Functional safety is the automotive industry's process for ensuring the absence of unreasonable risk due to hazards caused by malfunctioning behavior (i.e., failures) of electrical and electronic systems [3]. In 2018, ISO published the second edition of ISO 26262, which provides additional guidance on applying the functional safety process to transit buses, including guidance related to the risk assessment.

This study tailored the hazard analysis and risk assessment to transit buses in two ways. First, it considered system interfaces with transit bus-specific systems that are not present on light or commercial vehicles, such as the door control system. Second, it considered unique aspects of transit bus operations, in particular the presence of standing and unrestrained passengers and the fact that transit buses operate in traffic environments with a high number of vulnerable road users (VRUs). Transit buses may need to more reliably detect and safely respond to VRUs in situations such as operating in large crowds, driving toward pedestrians, and responding to unconventional VRU behavior. These interactions with VRUs may be less common for light and commercial vehicles.

This study found that many of the vehicle-level hazards and functional safety measures for light vehicles and heavy trucks also apply to transit buses. This will facilitate transfer of these Level 0 to Level 2 driving automation system technologies to transit buses, since many of these functional safety measures would not require significant modification.[1] However, this study also found that transit bus operations do lead to some unique vehicle-level hazards and additional safety measures that are specific to transit buses.

[1] Note that this study does not assess technological challenges (e.g., availability of electronically-actuated braking systems) with transferring these Level 0 to Level 2 driving automation system technologies to transit buses. The reader is referred to the *Transit Bus Automation Project: Transferability of Automation Technologies Final Report* for an assessment of technological challenges with transferability.

This research identified a total of 18 potential vehicle-level hazards for the driving automation systems considered in the study. Two of the identified vehicle-level hazards relate to functions that do not exist for light vehicles and are therefore unique to transit buses:

- The hazard "vehicle motion when passenger door is open" is relevant to systems that operate the propulsion system while the vehicle is in service, such as adaptive cruise control (ACC) or traffic jam assist. This hazard covers instances where the driving automation system causes the bus to resume moving or continue moving when the passenger door is open.
- The hazard "vehicle too far from the curb at station/stop" is relevant to the docking system and covers instances where the docking system does not bring the bus close enough to the curb for passengers, particularly mobility-impaired passengers, to safely embark or disembark.

One additional vehicle-level hazard, "excessive vehicle roll," is common to both transit buses and light vehicles but is more likely to occur in transit buses because of the different vehicle dimensions.

The ISO 26262 risk assessment process was applied to each of the identified vehicle-level hazards. The risk assessment considers three dimensions—severity, exposure, and controllability. Severity is an estimation of the potential harm that could result from a hazard. Exposure is an estimation of the likelihood that the bus is in a particular operating situation when a hazard occurs. Controllability is an estimation of how easily the bus driver or some other individual can avert the hazard. If the combination of these dimensions meets a certain threshold, the hazard is assigned one of four Automotive Safety Integrity Levels (ASILs). The ASILs range from ASIL A (least stringent) to ASIL D (most stringent).

The risk assessment found that the ASILs for the driving automation systems considered in this study were generally comparable between light vehicles and transit buses. This means that, in general, the level of design rigor used when developing these systems for light vehicles should be sufficient for transit bus applications. The one exception was for steering-related hazards, which were determined to have slightly more stringent ASILs (rated ASIL C) than their light vehicle counterparts (rated ASIL B).

Although the ASILs were generally comparable between light vehicles and transit buses, the risk assessment showed that severity and exposure ratings involving VRUs were typically higher for transit buses. However, this increased severity and exposure was offset by the presence of a skilled and trained transit bus operator,[2]

[2] In this context, an improved controllability rating could mean, for instance, that 90–99% of trained/skilled drivers can avert the hazard (C2 rating) as opposed to fewer than 90% of average drivers of passenger vehicles (C3 rating). For example, a skilled driver may feather the breaks to slow the bus when there are standing passengers but may feel comfortable braking more aggressively if all passengers are seated.

which improved the controllability rating.[3] This tradeoff, however, may not hold at higher levels of automation (i.e., Level 4 and Level 5) where a trained operator may not be present.

When applying the risk assessment, this study found that the current version of ISO 26262 does not provide guidance on how to consider exposure in the context of potential outlier conditions with low exposure for light vehicles but that are encountered more frequently by a transit bus that repeatedly runs a specific route. For instance, driving over railroad tracks might have a low exposure rating in a generic operating environment. However, if those railroad tracks are located on a transit bus route, then the exposure would be much higher.

In the ISO 26262 process, functional safety measures are developed to mitigate the risk of the identified hazards. This study provides examples of these high-level risk mitigation techniques. In general, this study found that many of the functional safety measures for light vehicles would be applicable to driving automation systems for transit buses. However, these functional safety measures may require some modification as these systems are transferred to transit buses. For instance, transit buses have longer stopping distances than light vehicles; therefore, a transit bus may require additional time to safely bring the vehicle to a stop in the event of a failure.

This study also identified functional safety measures that are unique to transit buses. These functional safety measures generally fell into two categories:

- **Functional safety measures that address transit bus-specific vehicle-level hazards**; for instance, these functional safety measures would help mitigate failures that could prevent the ACC system from monitoring the passenger door status.
- **Functional safety measures that support acceleration and deceleration limits intended to protect passengers**. Occupants of light vehicles are presumed to be wearing seatbelts, allowing light vehicles to accelerate or decelerate more aggressively than transit buses, which have standing and unbelted passengers. These additional functional safety measures help mitigate failures that could, for example, allow the ACC system to request a level of deceleration that causes standing passengers to fall over.

Incorporating engineered safety measures may be more effective at mitigating risks than providing improved operator training [4]. Thus, functional safety measures should be incorporated into the design of driving automation systems for transit buses rather than rely primarily on additional operator training to mitigate the effects of potential system failures.

[3] The controllability assessment in ISO 26262 assumes that the driver is in the appropriate condition to drive and has the appropriate driver training [3]. In the context of transit buses, this includes obtaining a commercial driver's license (CDL).

Functional safety focuses on mitigating the effect of failures in the system, but it does not address design considerations for the safe operation of the system under normal (i.e., non-failure) conditions. This study identified several safety-relevant design considerations that fall outside the scope of ISO 26262 but are nevertheless relevant to promoting the safe transfer of driving automation systems from light vehicles and commercial trucks to transit buses. These safety-relevant design considerations address areas such as:

- Ensuring proper interfaces between driving automation systems and other transit bus systems to protect passengers and allow for safe embarkation and disembarkation.
- Establishing acceleration and deceleration limits (including lateral acceleration) that protect unrestrained standing and seated passengers.
- Modifying algorithms to account for larger transit bus dimensions and the associated vehicle behaviors, such as wide right turns.

This research supports the safe transfer of Level 0 to Level 2 driving automation systems to transit buses by documenting some of the unique safety measures relevant to transit buses and by providing an example for applying ISO 26262 concepts to transit buses. As manufacturers and transit agencies consider pilot deployments to demonstrate these driving automation systems on transit buses, the results of this study may serve as an informative baseline against which to compare the results of their own internal system-specific hazard and safety analyses. This research may also provide a useful reference for manufacturers that wish to pursue different hazard analysis strategies to ensure the safety of their products prior to deployment.

SECTION 1

Introduction

Project Background

The extension of driving automation systems[4] to transit buses has the potential to alter the urban transportation landscape. However, public acceptance of these systems is dependent, in part, on their safe deployment. This study explored how unique aspects of transit bus operations and use cases could contribute to new hazards or safety challenges. In particular, this project builds upon a prior study that identified Level 0 to Level 2 driving automation systems developed for light vehicles and commercial trucks that are potentially transferrable to 40-ft city transit buses [1].

This study applied hazard analysis techniques to identify vehicle-level hazards that could potentially result from failures of these systems. It then assessed the risk posed by these hazards in accordance with the International Organization for Standardization (ISO) standard ISO 26262 [3], the state-of-the-art functional safety standard for road vehicles including buses. Finally, this study provides high-level risk mitigation techniques to facilitate the safe deployment of driving automation systems on transit buses.

Research Objective

The goal of this project was to accelerate the development and safe deployment of Level 0 to Level 2 driving automation systems by identifying potential hazards and safety measures for these technologies in the context of transit bus applications. As manufacturers and transit agencies consider pilot deployments to demonstrate these driving automation systems on transit buses, the results of this study may serve as an informative baseline against which to compare the results of their own internal system-specific hazard and safety analyses. The results of this research effort may also be a useful reference for manufacturers that wish to pursue different hazard analysis strategies to ensure the safety of their products prior to deployment.

[4] Driving automation systems is the generic term defined in SAE International Recommended Practice J3016 (*Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*) to broadly refer to any vehicle system or feature that operates from SAE Automation Level 1 to Level 5 [17]. SAE International Recommended Practice J3016 defines five levels of automation. Level 1 and 2 systems are referred to as driver support features, where the system provides sustained control but only for part of the driving task; the human operator is responsible for supervising the system's performance as well as monitoring the surrounding environment. Level 3 to Level 5 systems are referred to as Automated Driving Systems (ADS), wherein the system provides sustained control of the entire driving task. In Level 3 systems, the human operator may be used a fallback; Level 0 defines systems with no automation (i.e., there is no sustained control).

Specifically, the objectives of this project were to:

- Identify potential vehicle-level hazards and top-level safety goals for a generic 40-ft transit bus system equipped with Level 0 to Level 2 driving automation systems.
- Derive generic top-level safety measures and safe states to support potential testing and evaluation of transit buses equipped with these systems and identification of driver warning needs.

SECTION 2

Analysis Approach

Functional safety is one component of the overall system safety. The functional safety process is intended to mitigate risks resulting from failures in electrical and electronic (E/E) systems.[5] For road vehicles, including transit buses, the functional safety process is described in ISO 26262—a 12-part, voluntary functional safety standard. Certain parts of the standard correspond to specific phases in system development, such as product development at the hardware level (Part 5) or management of functional safety (Part 2).

Part 3 of ISO 26262 is called the "concept phase." It describes the steps for applying functional safety principles during the concept of operations stage of the development process. At this stage of the development process, the system is defined functionally, but specific design details are not yet selected. For example, the concept of operations may describe the function of environmental sensors, which is to provide sensor fusion algorithms with raw data on the vehicle's surrounding environment. However, this stage may not assume a specific technology is used by the system (e.g., camera or radar). This allows for an implementation-independent analysis. Consistent with this approach, this study used a conceptual description of the system that describes general functions rather than detailed system-specific designs.

The concept phase is an important part of the overall functional safety process because it includes key steps, such as the hazard analysis and risk assessment (HARA), that drive much of the downstream development process. For instance, the HARA informs the development of top-level safety measures known as "safety goals." Conducting an analysis based on the concept phase improved the broad applicability of this study by allowing the results to remain implementation-independent.

The analysis approach in this study was adopted from the concept phase (Part 3) of ISO 26262 [3]. Figure 2-1 depicts the key steps in the analysis approach. Figure 2-1 also shows the sections of this report that correspond to each step of the analysis. Each step is described as follows:

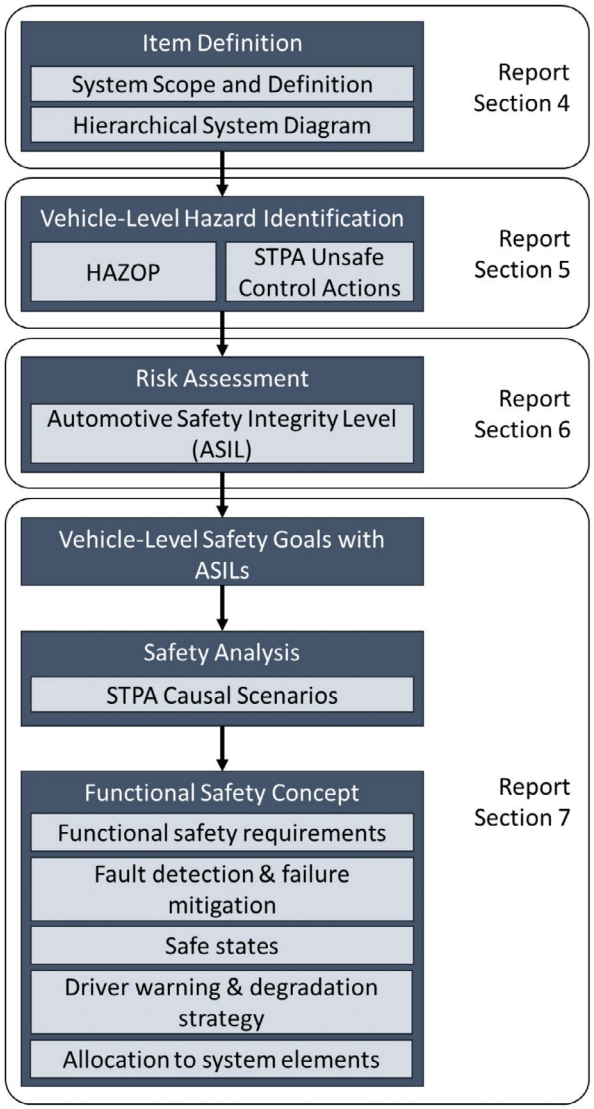
- **Item Definition** (ISO 26262, Part 3, Clause 5 [3]) – The first step in the approach is to clearly define the system and identify the system boundary. This enables identification of components and interactions within the system boundary as well as interactions with other vehicle systems outside the boundary. This step includes describing the system functions and any

[5] Other hazards may exist in systems that are not the result of E/E faults, such as fire or toxicity. These hazards are outside the scope of ISO 26262 [3].

assumptions about the system operation or configurations. A hierarchical system diagram may help illustrate the system structure and assist analysts in the rest of the process.

Figure 2-1

Analysis approach used in this study with corresponding report sections



HAZOP: Hazard and Operability Analysis
STPA: Systems Theoretic Process Analysis

- **Vehicle-Level Hazard Identification** (ISO 26262, Part 3, Clause 6.4.2 [3]) – The second step in the approach applies two hazard analysis techniques—the Hazard and Operability Analysis (HAZOP) [5] and the Systems-Theoretic Process Analysis (STPA) [6] methods. The output of the hazard analysis step is a list of potential vehicle-level hazards. If the HAZOP and STPA methods do not produce a consistent list of hazards at the outset, an additional step may be necessary to synthesize the hazards identified using the two methods.

- **Risk Assessment** (ISO 26262, Part 3, Clause 6.4.3 [3]) – Each identified hazard is then combined with one or more operating situations (e.g., roadway conditions, vehicle speed) to generate a set of hazardous events [3]. Each hazardous event and its worst-case outcome (e.g., a type of crash) is assessed along three dimensions—severity,[6] exposure,[7] and controllability.[8] These three dimensions are combined to generate an Automotive Safety Integrity Level (ASIL), which gives an indication of the level of design stringency necessary under ISO 26262 to avoid unreasonable risk.[9] ASILs range from A (least stringent) to D (most stringent). If the combination of severity, exposure, and controllability is sufficiently low (e.g., no injuries result), then no ASIL is assigned and the hazardous event is designated as quality management (QM). QM implies that appropriate quality management techniques in the production of system components should be sufficient to eliminate unreasonable risk.
- **Vehicle-Level Safety Goals** (ISO 26262, Part 3, Clause 6.4.4 [3]) – The next step in the approach derives vehicle-level safety goals, which are top level safety objectives intended to mitigate one or more of the identified vehicle-level hazards. The vehicle-level safety goal inherits the most stringent ASIL for the associated vehicle-level hazard. If a safety goal satisfies more than one vehicle-level hazard, the more stringent ASIL is applied to the safety goal [3].
- **Safety Analysis** (ISO 26262, Part 3, Clause 7.4.2.4 [3]) – This study applies STPA to identify component failures and unsafe interactions that may lead to one or more of the identified vehicle-level hazards. The safety analysis is conducted at the functional level, meaning that it considers failures in the functions of system components. For instance, a signal may not be provided from a sensor to the controller. However, the safety analysis does not focus on failures modes of a specific technology (e.g., why the signal was not provided).
- **Functional Safety Concept** (ISO 26262, Part 3, Clause 7 [3]) – The functional safety concept describes the functional safety measures, fault detection and mitigation strategies, safe states, and driver warning strategies that support the identified safety goals. Functional safety requirements are derived from the component failures and unsafe interactions identified in the safety analysis. For this study, the functional safety concept will focus on areas specific to transit buses.

---

[6] Severity is the estimated extent of harm that may result because of the hazardous event under consideration [3].

[7] Exposure is the potential for the vehicle to be in the operating situation for the hazardous event under consideration [3].

[8] Controllability measures the potential for one or more persons involved in a hazardous event to avoid harm [3]. Note that a higher controllability parameter value implies a higher risk that the operator will be unable to safely control the outcome of the scenario.

[9] Unreasonable risk is defined as "risk judged to be unacceptable in a certain context according to valid societal moral concepts" [3].

SECTION 3

Transit Bus Considerations for Analysis

To understand the unique aspects of transit buses that are relevant to the hazard and safety analysis, this study began with a review of the transit bus considerations included in the most recent edition of ISO 26262; interviews with transit bus manufacturers, suppliers, and transit agencies; and a literature review of driving automation systems for transit buses.

Inclusion of Transit Buses in ISO 26262

In 2018, ISO published the second edition of the ISO 26262 standard. Among other changes, the second edition includes specific considerations for trucks and buses. The truck and bus considerations introduced into the vocabulary (Part 1) and concept phase (Part 3) sections of ISO 26262 are most applicable to this study.

ISO 26262 broadly defines a bus as a "motor vehicle which, because of its design and appointments, is intended for carrying persons and luggage, and which has more than nine seating places, including the driving seat" [3].

ISO 26262 acknowledges that characteristics of a truck or bus may change during operation. Specifically, ISO 26262 defines the variant in truck and bus vehicle operation as the "use of a truck or bus vehicle with different dynamic characteristics influenced by cargo or towing during the service life of the vehicle" [3]. For instance, the variations in bus operation might include different handling characteristics between an empty bus and a fully-loaded bus.

The second edition of ISO 26262 also provides added requirements and guidance for applying the ISO 26262 risk assessment to transit buses. In particular, Part 3 provides guidance for evaluating the exposure parameter for different types of buses (e.g., city, interurban, and coach) and the controllability parameter. For instance, Tables B.4 and B.5 in Part 3 [3] provide some general examples of exposure ratings for transit buses.

Subject Matter Expert Interviews

Interviewed Organizations

This study included a series of interviews with subject matter experts (SMEs) at suppliers, manufacturers, and transit agencies. SMEs provided insight into aspects of transit buses and their operation that were relevant to this study, as described in this section. SMEs from the following organizations were interviewed:

- Continental Corporation (supplier)
- Mobileye (supplier)
- ZF/TRW (supplier)
- New Flyer (manufacturer)
- Proterra (manufacturer)
- Blacksburg Transit (transit agency)
- Jacksonville Transportation Authority (transit agency)
- LYNX (transit agency)
- Minnesota Valley Transit Authority (transit agency)
- Pierce County Public Transportation Benefit Area Corporation (transit agency)

Insights on Transit Bus Operations

Transit Bus Dimensions

Several SMEs highlighted challenges related to the larger dimensions of a transit bus. The sensor placement on transit buses necessarily differs from that on light vehicles, which may, in turn, necessitate retraining machine-learning algorithms to detect objects (e.g., vehicles, pedestrians) based on the different perspective. Similarly, transit buses have different vehicle dynamics, such as stopping distance and handling response, which may require modification of response algorithms. In particular, the increased stopping distance for transit buses could require earlier object detection with an associated increase in the false-positive detection rate.

The larger dimensions of a transit bus also present challenges for driving maneuvers such as right-hand turns. Transit buses make wide right-hand turns, which may cause the bus to depart the travel lane as they enter the turn. When the bus is preparing to turn right, transit bus operators may also choose to straddle lane markings to discourage other vehicles from attempting to turn to the right of the bus. This may have relevance to systems designed to keep the vehicle within a lane.

The effects of transit bus dimensions were considered as part of the safety analysis and in the derivation of the safety-relevant design considerations in Section 7.

Increased Vulnerable Road User Exposure

By their nature, transit buses operate in traffic environments with a high number of vulnerable road users (VRUs).[10] Interactions with VRUs that might be rare for light vehicles could be common occurrences for transit buses. Therefore, driving

[10] VRUs include pedestrians, pedalcyclists, motorcyclists, and other roadway users that do not benefit from any appreciable external protective devices that would absorb energy in a collision [23].

automation systems in transit buses may need to more reliably detect and safely respond to these situations. Nonetheless, driving automation systems should be minimally susceptible to false-positive activation in these situations. SMEs indicated that high false-positive alarm rates reduce bus driver acceptance of and trust in driving automation systems.

SMEs shared several important examples of these pedestrian-centric situations:

- **Operating in large crowds** – Transit buses may need to navigate around or potentially collect passengers in large crowds (e.g., after cultural or sporting events). Crowd members may not exhibit typical pedestrian behavior; for example, there may be numerous people walking in the travel lanes, even intoxicated people walking erratically, which can test the limits of an algorithm's ability to reliably predict pedestrian behavior.
- **Driving toward pedestrians** – Transit buses are expected to approach groups of pedestrians waiting at bus stops. Systems should be able to reliably differentiate between situations in which the bus can safely approach a group of pedestrians and those in which emergency braking or other system intervention may be necessary.
- **Passenger activity around the bus** – Systems designs should be able to anticipate and respond to otherwise unexpected pedestrian behavior around transit bus stops. For instance, pedestrians may dart out into the road to catch a bus, chase after a departing bus, or immediately cross in front of a bus after disembarking.

Unconventional behavior from VRUs may also present challenges for driving automation systems on transit buses. Human operators can usually anticipate certain VRU behaviors, particularly on fixed bus routes in which particular locations may be prone to unconventional VRU behaviors. Examples shared by SMEs include:

- **Bicycles suddenly entering the roadway** – One transit agency operates buses on a university campus where bicyclists can use the sidewalk. However, once bicyclists leave the campus, they must leave the sidewalk and enter the roadway. Often, bicyclists enter the roadway in an uncontrolled manner (e.g., hopping off the sidewalk). Human operators can anticipate and understand this behavior; however, a driving automation system may need to be able to respond appropriately to the sudden appearance of a bicycle within the limits of the roadway.
- **Wrong-way operation** – One transit agency shared that its buses go through a tourist area. Tourists renting bicycles are sometimes unfamiliar with the local roadways, and the transit bus operators often encounter bicyclists going the wrong way down a one-way street. Driving automation systems should be able to anticipate such behaviors similar to human operators.

The effects of both increased pedestrian exposure and unconventional VRU behavior were evaluated in the risk assessment (Section 6).

Passenger-Related Safety Considerations

In most motor vehicles, passengers are seated and wearing seat belts. However, in transit buses, passengers do not typically wear seatbelts, and many will be standing. Passengers might even be navigating the aisles, whether to change seats, pay the fare, or prepare to disembark. Unsecured passengers are more vulnerable to sudden changes in motion such as hard braking or steering. Transit agency SMEs indicated that human operators regularly check their interior mirror to gauge the status of passengers in case the need arises to respond to an immediate driving situation. For instance, if all passengers are seated, the driver may feel more comfortable braking aggressively. Alternatively, a driver may feather the brakes if passengers are standing. Generally, transit agency SMEs indicated that individual operators are responsible for determining how hard to brake or steer; there is no universal policy. Driving automation systems would need to be capable of determining the appropriate level of steering, braking, and acceleration to prevent possible injury to passengers. If the system is capable of braking aggressively for an extended period, it may require sensors and algorithms to assess the status of passengers.

Transit bus operators sometimes assist passengers with disabilities who are embarking or disembarking the bus. At the lower levels of automation considered in this study, the human operator would presumably still perform these assistance roles. However, there are potentially safety considerations around accessibility related to the docking system; this system must reliably steer the vehicle into a relatively flat, obstacle-free location from which mobility-impaired passengers can safely disembark with minimal or no assistance.

Considerations related to passengers were addressed in both the hazard identification (Section 5) and risk assessment (Section 6) portions of the analysis.

Bus Stop Interactions

When approaching a bus stop, transit buses may encroach on or cross the right-most lane marking to pick up passengers. Lateral control systems should account for and accommodate this behavior to ensure that the bus can get close enough to the curb, especially if ramps or lifts need to be deployed.

Transit buses may also cross into or over bike lanes to enter or exit a bus stop. Lateral control systems should be able to cross into the bike lane safely, accounting for lane markings and the presence of bicyclists. When departing a bus stop, transit bus driving automation systems may also need to detect bicyclists passing the bus on the left.

Concerns around entering bus stops were specifically considered in the hazard identification (Section 5) and safety analysis and derivation of safety-relevant design considerations in Section 7.

Urban Environment Considerations

Driving automation systems for transit buses would need to navigate complex urban environments with numerous intersections, cross streets, and unsignaled crosswalks. Sensing systems are challenged by numerous line-of-sight occlusions (e.g., buildings, crowds, vehicles). Practically, human operators can signal to other road users in times of ambiguity or confusion.

In some jurisdictions, transit buses operate in dedicated bus lanes. Dedicated lanes may facilitate deployment of driving automation systems by providing a more controlled environment in which transit buses can operate. However, several SMEs indicated that other vehicles and VRUs frequently infringe on bus lanes. Thus, even driving automation systems operating in dedicated bus lanes may still need to detect and respond to the full range of roadway users.

Consideration of bus lanes was included as part of the risk assessment (Section 6). Other urban environment considerations were considered in the safety analysis and derivation of the non-ISO 26262 safety measures (Section 7).

Literature Review of Potential Transit Bus Driving Automation Systems

To develop the system description and construct the hierarchical control diagram (Figure 4-1, Step 1), this study included a high-level literature review to understand notional configurations and applications of driving automation systems for bus applications.

Transferability of Automation Technologies Study

The *Transferability of Automation Technologies Final Report* [1] identifies light vehicle and commercial truck technologies that are potentially transferrable to 40-ft transit buses. Table 3-1 summarizes the technologies identified in the transferability study.

Table 3-1

Summary of Technologies in Transferability of Automation Technologies Final Report

System	Category	Description
Adaptive Cruise Control (ACC) with/ without Stop-and-Go	Braking, Powertrain	Controls gap between vehicles and controls speed down to 0 miles per hour (mph)
Automatic Emergency Braking (AEB)	Braking	Provides automatic braking in case of an imminent collision
Docking	Steering	Steers vehicle into a bus stop or station (e.g., at a curb)
Full Park Assist/Valet Parking (Bus Yard)*	Steering, Braking, Powertrain	Parks vehicle in a slot selected by driver, with driver inside or outside of vehicle
Lane Keeping/Lane Centering/Steering Assist†	Steering	Provides steering assistance to prevent unintended lane departure or to keep vehicle in center of lane
Object Detection and Collision Avoidance	Human-Machine Interface (HMI)	Alerts or warns driver or higher-level automation systems of nearby objects and potential collisions
Park Assist/Park Out/ Yard Park‡	Steering	Steers vehicle into or out of a parking slot or to other driver-designated locations in a specified area
Reverse Brake Assist	Braking	Detects objects or pedestrians behind vehicle, brakes automatically during backing maneuvers
Traffic Jam Assist (TJA) with Lane Keeping/Lane Centering	Steering, Braking, Powertrain	Controls gap between vehicles in stop-and-go traffic while keeping vehicle in lane

**The* Transferability of Automation Technologies Final Report *lists these as two separate systems, but they are combined in this study since they are functionally similar. These technologies provide steering, braking, and powertrain control intended to park the bus in a designated spot.*

† The Transferability of Automation Technologies Final Report *lists these as two separate systems, but they are combined in this study since they are functionally similar. These technologies provide steering-only control intended to keep the vehicle centered in the lane.*

‡ The Transferability of Automation Technologies Final Report *lists these as three separate systems, but they are combined in this study since they are functionally similar. These technologies provide steering-only control in maintenance yards and other limited access areas.*

The technologies in Table 3-1 form the basis of the system descriptions and hierarchical control diagram in Section 4. As part of the *Transferability of Automation Technologies Final Report*, the researchers performing that study reviewed a series of pilot studies and deployments and integrated the findings from these studies into their report. Therefore, this study did not explicitly include an additional review of those sources.

Several of the technologies in Table 3-1 may be specific to restricted zones when employed on buses. For instance, the yard park and valet park systems would operate only in maintenance yards. Similarly, SMEs indicated that transit buses typically do not reverse when in service, and technologies such as reverse brake assist would be used primarily in maintenance yards. Furthermore, some technologies in Table 3-1 may be specific to certain use cases. For instance, the driver would engage the docking system only when the vehicle approaches a bus stop.

The *Transferability of Automation Technologies Final Report* broadly assessed light vehicle and commercial truck technologies for their applicability to transit buses. However, when integrating these systems into a single vehicle, some of the identified technologies might be mutually exclusive in their operation. For example, the steering assist and lane keeping/lane centering systems both provide steering to keep the vehicle within the travel lane; the only difference between the systems is whether the steering system operates independent of the driver (steering assist) or in conjunction with the driver's input (lane keeping/lane centering). Therefore, it is unlikely that a bus design would allow the operator to engage both systems concurrently.

American Public Transportation Association Bus Procurement Guidelines

The American Public Transportation Association (APTA) produces bus procurement guidelines. Although no guidelines exist for driving automation systems on transit buses, the June 2013 guidelines provide information on other transit bus systems that could potentially interact with the driving automation systems considered in this study:

- **Backup lights and alarms** – This system provides visible and audible warnings to alert other vehicles or pedestrians when the bus is performing a reverse operation [7]. It has potential interactions with systems that provide longitudinal control in the reverse direction, such as parking assist systems.
- **Door control** – The driver operates the door controls for both the front and rear passenger doors. In some configurations, the driver may also be able to allow passengers to open the rear door themselves [7]. The door control system may feature an interlock that prevents operation of the propulsion system if the door is opened more than three inches from the fully-closed position [7]. The door control system has potential interactions with longitudinal control systems that operate while the vehicle is in service (e.g., ensure doors are closed before the vehicle resumes motion).
- **Lift and kneeling systems** – This system provides access for mobility-impaired individuals. An interlock system typically prevents the bus from moving during the loading or unloading cycle while the lift is deployed [7]. This system has potential interactions with systems that control the longitudinal motion of the bus.

SECTION
4

System Overview

Systems Considered for Analysis

This study grouped the driving automation system technologies from the *Transferability of Automation Technologies Final Report* into nine categories by combining similar functions. For instance, the lane keeping/lane centering system and steering assist system provide similar functions for transit buses and are, therefore, considered jointly as a single category. The nine categories evaluated in this study are described in this section.

Adaptive Cruise Control with/without Stop-and-Go

The ACC system controls the speed of the bus to maintain a gap between the bus and the vehicle in front of it. It controls propulsion and braking, but the driver is responsible for steering the bus. In some applications, ACC may be paired with a lateral control system (e.g., steering assist) to allow for Level 2 automation. The ACC system may also control speed based on speed limit signs or geocoded speed limit data [1].

ACC systems may be equipped with a "stop-and-go" feature, which allows the system to operate down to a speed of 0 mph and can shut off the engine. The stop-and-go feature restarts the bus under certain conditions (e.g., the vehicle in front of the bus moves by a set distance) [1].

Automatic Emergency Braking

According to the *Transferability of Automation Technologies Final Report*, the AEB system monitors the path ahead of the transit bus for vehicles, pedestrians, and other objects [1]. In the event of a potential collision between the transit bus and a detected object, the AEB system will implement a tiered strategy to mitigate the collision:

- First, the AEB system will issue a warning to the driver via the HMI [1].
- At the first distance or time-to-collision (TTC) threshold, the AEB system will pressurize the brakes to reduce the time it takes for the brakes to engage when the driver presses the brake pedal [1].
- At the next distance or TTC threshold, the AEB system will apply a brake jerk to gain the driver's attention [1].
- At the final distance or TTC threshold, the AEB system will bring the propulsion torque to zero and apply the brakes with sufficient force to avoid or reduce the severity of the collision [1].

Transit buses have an increased time to stop relative to light vehicles. According to SMEs, there are tradeoffs between activating the AEB system early enough to mitigate all collisions and an increased rate of false positives (i.e., activating the system when a potential collision does not exist).

Docking

The *Transferability of Automation Technologies Final Report* describes the docking system as capable of steering the bus into a bus stop at a pre-determined distance from the curb [1]. The driver selects the distance from the curb and controls the propulsion and braking. That is, the docking system controls only the steering function. The docking system must be able to detect the curb and lane boundaries [1].

For the docking system to steer the bus close enough to the curb, the system may need to disengage or suspend other lateral control systems that may be active, such as the lane keeping/lane centering/steering assist system.

Full Park Assist/ Valet Parking

Full park assist and valet parking are two parking systems that provide propulsion, braking, and steering control to maneuver a bus into a designated parking spot. These systems were described separately in the *Transferability of Automation Technologies Final Report* but are combined in this study since they are both parking features that provide lateral and longitudinal control.

For the full park assist system, the operator is inside the vehicle and selects the parking spot [1]. For the valet parking system, the operator may be outside the vehicle while the system parks the vehicle; the operator may even activate the system using a remote device such as a smartphone or tablet [1].

Lane Keeping/ Lane Centering/ Steering Assist

This study considered the lane keeping/lane centering and steering assist systems jointly, since these systems are mutually exclusive (i.e., either steering assist or lane keeping/lane centering will be active). These systems all maintain the vehicle position in the lane and differ primarily on whether the driver is permitted to take his/her hands off the steering wheel; lane keeping/lane centering requires the driver to keep his/her hands on the steering wheel, whereas steering assist does not.

As described in the *Transferability of Automation Technologies Final Report*, these systems determine the lane boundaries directly or by interpolating the lane boundaries based on landmarks or surrounding traffic [1]. As the bus approaches a lane boundary, the system steers the bus back toward the center of the lane. If the operator is not engaged or if the system is unable to detect the lane

boundaries, the system will prompt the operator to resume control and will disengage after a specified period [1].

Lane keeping/lane centering/steering assist systems must be able to recognize (or at least not interfere with) intended lane departures necessary for maneuvering the bus in urban environments. For instance, SMEs indicated that bus drivers might intentionally depart the travel lane to make wide right-hand turns. Activation of the lane keeping/lane centering/steering assist systems may also need to be coordinated with the docking system (Section 4, Docking).

Object Detection and Collision Avoidance

According to the *Transferability of Automation Technologies Final Report*, the object detection and collision avoidance system supports the other driving automation systems by identifying and classifying stationary and moving objects around the vehicle [1]. The object detection and collision avoidance system provides this information to the driver via the HMI as well as to other driving automation systems [1].

SMEs interviewed for this study indicated that transit buses currently have object detection and collision avoidance systems (also referred to as driver assistance systems). However, these systems primarily alert and warn the driver of surrounding objects rather than support other driving automation systems.

Park Assist/ Park Out/ Yard Park

Park assist, park out, and yard park are a collection of parking-related systems that provide steering-only assistance to the driver when parking the bus. The driver is responsible for controlling the propulsion and braking, which differentiates this class of systems from the full park assist/yard park systems described in Section 4, Full Park Assist/Valet Parking. Although considered separately in the *Transferability of Automation Technologies Final Report*, this study considered these technologies jointly as parking systems that only provide lateral control.

The park assist system steers the vehicle into a driver-selected perpendicular, angular, parallel, or back-in parking spot [1]. The park out system steers the vehicle out of a parking spot [1]. The yard park system steers the vehicle into a pre-designated "home" position in the maintenance yard [1]. The yard park feature might be engaged immediately upon entering the maintenance yard, necessitating steering around fixed objects and other obstacles in the yard [1].

Reverse Braking Assist

The reverse brake assist system detects objects behind the vehicle when the vehicle is operating in reverse. In the event of a potential collision, the system issues warnings to the driver and applies the brakes. The reverse brake assist

may also detect cross-traffic behind the bus and alert the driver as vehicles, pedestrians, and other objects approach the bus's path [1].

According to transit agency SMEs, transit buses typically do not operate in reverse, except in maintenance yards where personnel can provide assistance. However, technologies such as reverse brake assist might allow buses to operate in reverse under more conditions and without assistance.

Traffic Jam Assist with Lane Keeping/ Lane Centering

As described in the *Transferability of Automation Technologies Final Report*, traffic jam assist (TJA) controls propulsion, braking, and steering in heavy traffic situations [1]. Similar to ACC, the TJA system maintains a set distance between the bus and the vehicle in front of the bus. The system can control the bus speed down to 0 mph and is capable of starting and stopping the bus in certain conditions [1]. The TJA system may be activated in conjunction with the lane keeping/lane centering/steering assist system to provide lateral control as well as longitudinal control. The lane keeping/lane centering/steering assist system will maintain the bus position between the lane boundaries as described in Section 4, Lane Keeping/Lane Centering/Steering Assist.

System Interfaces

Transit Bus Operator

A human driver is responsible for operating the bus and monitoring the external environment for potential threats. The human driver operates the vehicle based on inputs from the dashboard display (i.e., HMI) as well as visual cues from the external environment and the motion of the bus. The human driver can interact directly with the foundational vehicle systems (e.g., steering, braking, propulsion) and other transit bus systems (e.g., door control) and also with driving automation systems through the HMI. The human driver also performs additional non-driving tasks such as ensuring passenger safety and security.

Human Machine Interface

The HMI serves as the intermediary between the human driver and driving automation systems. In addition to allowing the driver to engage and disengage various driving automation systems, the HMI provides feedback through dashboard displays and audio and haptic alerts. The HMI informs the driver when it is safe to engage a system and displays notifications such as system unavailability (e.g., as a result of a fault).

System Controllers and Perception Algorithms

Section 4 provides brief descriptions of the driving automation systems considered in this study. These systems typically do not use raw sensor data.

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. This 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) [8].

The perception and sensor fusion layer develops an environmental model that can be employed by the driving automation systems. In addition to detecting the current roadway environment, perception data are used by system algorithms to predict object behavior (e.g., through object tracking). Algorithms might assign a probability of existence to a detected object and develop a hypothesis about an object's behavior (e.g., from existing models) [8]. The algorithms then use relevant sensor data to update both the probability of existence and predicted object behavior many times each second. For example, after letting passengers off at a stop, these algorithms would be responsible for detecting each person to a certain level of confidence and assessing the likelihood that the person will cross in front of the bus.

Foundational Vehicle Systems

The driving automation systems issue requests for lateral and longitudinal control to the foundational vehicle systems via the vehicle's communication network. The foundational braking, steering, and propulsion systems then provide the actuation for the driving automation systems. The foundational systems found on transit buses are described in more detail in the *Transferability of Automation Technologies Final Report* [1].

System Diagram

The hierarchical diagram shown in Figure 4-1 is based on the system description in Section 4. In addition to elements of driving automation systems that are common to light vehicles, Figure 4-1 shows potential interactions with other transit bus systems, including door controls, kneeling/lift systems, and back-up alerts. As suggested by SMEs, Figure 4-1 also explicitly depicts the on-board passengers and their interaction with both driving automation systems and the bus motion.

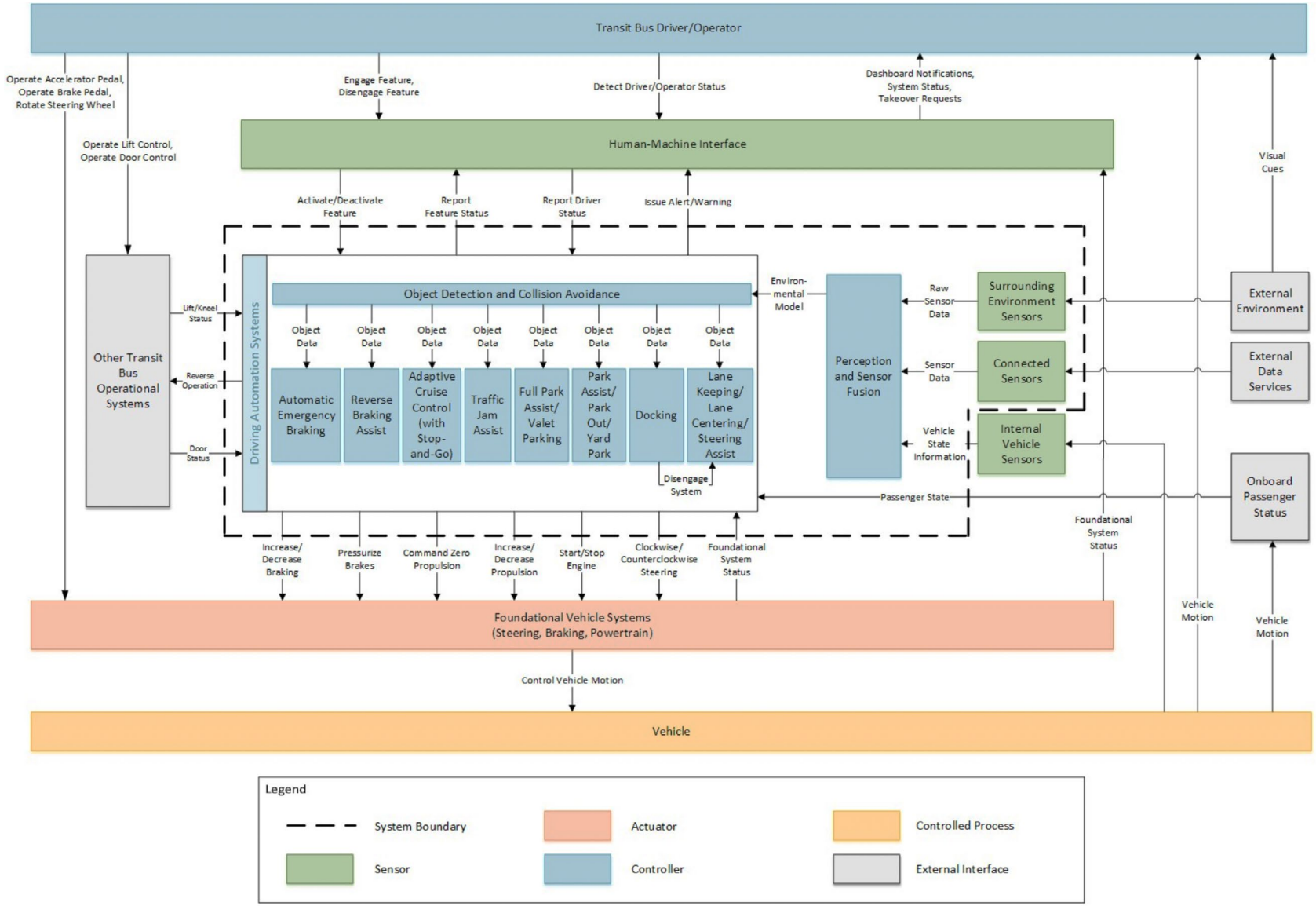


Figure 4-1 *Hierarchical block diagram for driving automation systems considered in this study*

SECTION 5

Hazard Identification

ISO 26262 defines a hazard as "a potential source of harm caused by malfunctioning behavior of the item" [3]. In ISO 26262, potential hazards are identified at the vehicle-level, which denotes that the hazards describe an effect on the overall vehicle if the malfunctioning behavior is not mitigated [9]. In contrast, other standards describe hazards that could be defined at the system, subsystem, or component level [4].

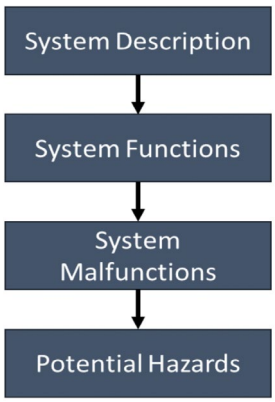
ISO 26262 does not recommend or endorse specific methods to identify vehicle-level hazards. In this study, the HAZOP and STPA methods were used to identify potential vehicle-level hazards. Both methods are routinely used in the automotive industry to conduct the hazard and safety analysis. Other techniques, such as Fault Tree Analysis and Failure Modes and Effects Analysis, are also routinely used in the automotive industry to support the functional safety process.

Hazard and Operability Analysis

Hazard and Operability Analysis Method (HAZOP)

HAZOP is a method for identifying vehicle-level hazards based on an analysis of system functions. In the HAZOP method, hazards potentially result from deviations of the system's functions from the design intent. These is referred to as a system malfunction. Figure 5-1 illustrates the four analytical steps of the HAZOP.

Figure 5-1
HAZOP method as applied in this study



The steps in HAZOP include:

- **System Description** – Define the system of study and the scope of the analysis. This step is accomplished as the first step of the overall analysis approach, as shown in Figure 1.

- **System Functions** – List the functions that the system components need to perform. This step is also accomplished in the first step of the overall analysis. A list of the HAZOP functions considered in this study is provided in Appendix A.
- **System Malfunctions** – For each of the identified functions, apply a set of guidewords that describe the various ways in which the function may deviate from its design intent (i.e., a malfunction). The HAZOP standard IEC 61882:2001 lists 11 suggested guidewords but notes that the guidewords can be tailored to the particular system being analyzed [5].[11] The HAZOP method implemented in this project uses the following seven malfunction guidewords, based on SAE International (SAE) Recommended Practice J2980 [9]:
  - Loss of function
  - More than intended
  - Less than intended
  - Intermittent
  - Incorrect direction
  - When not requested
  - Locked or stuck function

  The combination of a system function and guideword may have more than one interpretation. In such a situation, an analyst may identify more than one resulting malfunction.

- **Potential Hazards** – Assess the effect of these malfunctions at the vehicle level. If a malfunction potentially could result in a vehicle-level hazard, the hazard is documented. A malfunction can result in more than one vehicle-level hazard.

Hazard and Operability Analysis Results

Table 5-1 shows examples from applying the HAZOP method. This example considers two functions of the ACC system from the list of functions provided in Appendix A.

[11] IEC 61882:2001 also gives guidance on application of the technique and on the HAZOP procedure, including definition, preparation, examination sessions, and resulting documentation.

Table 5-1
Example Application of HAZOP from This Study

Function	Guideword	Resultant Malfunction	Potential Vehicle-Level Hazard
Accelerates and decelerates to maintain distance between the bus and the vehicle ahead	Delivers more than required	System accelerates more than required to maintain distance between bus and vehicle ahead	Excessive vehicle propulsion
		System decelerates more than required to maintain distance between bus and vehicle ahead	Excessive vehicle deceleration
	Delivers less than required	System accelerates less than required to maintain distance between bus and vehicle ahead	Insufficient vehicle propulsion
		System decelerates less than required to maintain distance between bus and vehicle ahead	Insufficient vehicle deceleration
Detects vehicles ahead of the bus	Delivers intermittently	System intermittently detects vehicles ahead of the bus	Excessive vehicle propulsion

Overall, this study considered a total of 55 functions and identified 235 malfunctions that could potentially lead to vehicle-level hazards. The total number of functions and identified malfunctions broken down by system are shown in Table 5-2.

Table 5-2
Summary of HAZOP Results

System	Functions	Identified Malfunctions
Adaptive Cruise Control with Stop-and-Go	6	29
Automatic Emergency Braking	6	25
Docking	6	27
Full Park Assist/ Valet Parking	8	35
Lane Keeping/ Lane Centering/Steering Assist	6	25
Object Detection and Collision Avoidance	5	19
Park Assist/ Park Out/ Yard Park	6	22
Reverse Braking Assist	6	24
Traffic Jam Assist with Lane Keeping/ Lane Centering	6	29

Systems-Theoretic Process Analysis (STPA)

Systems-Theoretic Process Analysis Method

STPA is a top-down systems engineering approach to system safety [6]. In STPA, the system is modeled as a dynamic control problem in which proper controls and communications in the system ensure the desired outcome for emergent properties such as safety. In the context of this study, each system had a control module responsible for issuing the appropriate control actions to the propulsion, braking, or steering systems, as described in Section 4.

In the STPA framework, a hazard would not occur unless a system controller issues an unsafe control action (UCA) or fails to issue a control action needed to maintain safety. That is, a hazard may result when the system issues a control action that is not appropriate for the current driving situation. Figure 5-2 shows the process flow diagram for the STPA method used in this study.

Figure 5-2
STPA method as applied in this study

In this project, STPA was implemented using the following steps:

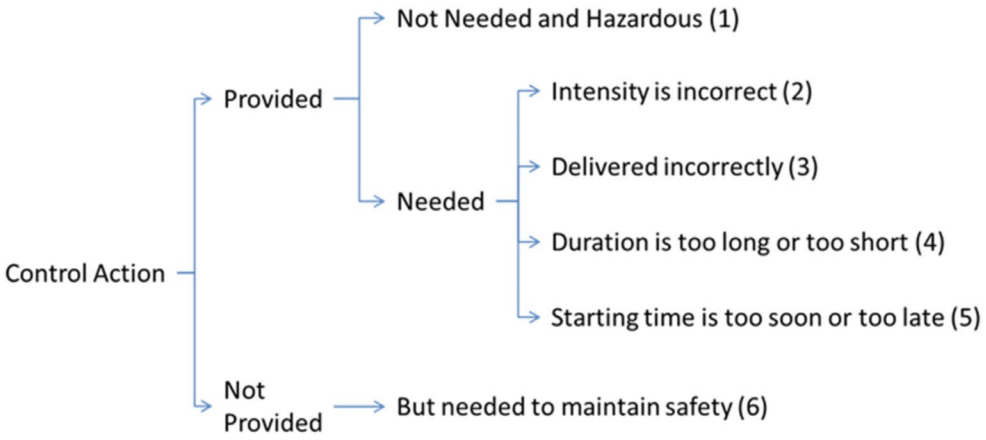
- **System Description** – Define the system under study and the scope of the analysis. This includes identifying system controllers and the control actions issued by these controllers. This step is accomplished in the first step of the overall analysis, as shown in Figure 2-1.
- **Vehicle-Level Losses** – Define the loss or losses at the vehicle level that should be mitigated. The STPA method broadly defines losses as undesired and unplanned events that result in the loss of human life or injury, property damage, environmental pollution, etc. [6]. However, this project considered only safety-relevant losses, such as injury to vehicle occupants or other roadway users.
- **Hazards** – Identify a preliminary list of vehicle-level hazards that could lead to the losses of interest. A preliminary hazard list can be generated based on engineering experience and a literature search. For instance, the SAE Recommended Practice J2980 Considerations for ISO 26262 ASIL Hazard Classification provides a list of hazards related to vehicle motion [9]. The preliminary hazard list is then refined by identifying UCAs in the next part of the STPA process.
- **Unsafe Control Actions** – Identify potential UCAs issued by each of the system controllers that could lead to potential vehicle-level hazards. Four sub-steps are involved:

  - List all relevant control actions that each controller in the scope of the study can issue. A list of control actions for the systems considered in this study is provided in Appendix B.
  - Develop a set of context variables[12] for each control action. Context variables and their states describe the relevant external inputs and conditions that 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 under which the control action could be issued. The context variables considered for each control action in this study are provided in Appendix B.
  - Apply the UCA guidewords to each control action. The original STPA literature includes four such guidewords [6]. This study uses a set of six guidewords for the identification of UCAs. These six guidewords are based on experience from prior studies applying STPA to automotive systems [10]. The six guidewords are shown in Figure 5-3.
  - Assess each control action against each of the six guidewords and the context variable combinations to determine if the combination could lead to one or more vehicle-level hazards. If this step identifies new hazards, they are added to the preliminary list of vehicle-level hazards generated in the previous step.

- **Causal Scenarios** – Determine causal scenarios that may lead to each identified UCA. Each component and interaction in the hierarchical system diagram (Figure 4-1) is evaluated to determine if a component failure or interaction could result in one of the identified UCAs. More than one component or interaction may be involved in a causal scenario.

Figure 5-3

Guidewords used in this study to derive UCAs



[12] The context variables describe the context in which a controller issues a control action. For example, the control action to "disengage the system" may be issued in the context of the driver's request to disengage the system, the driver's attentiveness, and disengage or suspend requests from other vehicle systems. The context variables should be informative, but too many context variables can create an unmanageable set of conditions to evaluate.

Systems-Theoretic Process Analysis Results

Table 5-3 shows an example result from applying STPA using the approach described in Section 5, Systems-Theoretic Process Analysis Method. This example considers the ACC control action to "request an increase in braking torque" (Section 4) paired with the guideword "provided, but intensity is incorrect" from Figure 5-3.

Table 5-3
Example STPA Results from This Study

Potential Vehicle-Level Hazard	Excessive Vehicle Deceleration or Braking
Unsafe Control Action	ACC system issues request to increase brake torque when gap with lead vehicle is below distance gap set point, but braking is provided with too much force.
Causal Scenario	ACC controller has an incorrect measurement for current vehicle speed.
	ACC system may select a speed decrease profile not suitable for unsecured passengers or cargo.
	Perception and sensor fusion algorithms may misjudge the distance between the host vehicle and another object (e.g., pedestrian, lead vehicle).

Overall, this study considered 59 control actions and identified a total of 476 UCAs that could potentially lead to vehicle-level hazards. This study also identified 694 causal scenarios that could potentially lead to UCAs. Note that not all of the identified causal scenarios are specific to transit buses; only the transit bus-specific causal scenarios were used to develop the safety measures presented in Section 7.

The total number of control actions, UCAs, and causal scenarios identified for each system in this study are shown in Table 5-4.

Table 5-4
Summary of STPA Results

System	Control Actions	Identified UCAs	Identified Causal Scenarios
Adaptive Cruise Control with Stop-and-Go	11	70	83
Automatic Emergency Braking	8	60	81
Docking	4	36	56
Full Park Assist/ Valet Parking	10	85	122
Lane Keeping/ Lane Centering/ Steering Assist	3	21	44
Object Detection and Collision Avoidance	1	7	33
Park Assist/ Park Out/ Yard Park	3	39	67
Reverse Braking Assist	6	58	81
Traffic Jam Assist with Lane Keeping/ Lane Centering	13	100	127

Potential Vehicle-Level Hazards

The vehicle-level hazards identified through the HAZOP and STPA methods were compared to each other to formulate a comprehensive list of potential vehicle-level hazards. The result of this comparison was a list of 18 potential vehicle-level hazards relevant to the driving automation systems considered in this study. These hazards are presented in Appendix C; descriptions of each hazard are also provided in Appendix C.

This study found that most of the vehicle-level hazards identified in this study are common to both light vehicles and transit buses. This is expected since the underlying system functions are similar for light vehicles and transit buses. Therefore, the vehicle-level effects of malfunctions are similar. For instance, the malfunctions shown in Table 5-1 and UCA shown in Table 5-3 would result in the same hazards regardless of whether the system is operating in a light vehicle or transit bus.

Analysts noted that one of the identified vehicle-level hazards—"excessive vehicle roll"—may apply only to certain types of light vehicles (e.g., large sport utility vehicles or vans). However, this hazard may be more broadly applicable to transit buses because of their higher center of gravity.

This study also identified two vehicle-level hazards that are unique to transit buses. These hazards derive from considering malfunctions and UCAs in the context of embarking and disembarking passengers at bus stops. This is a core transit bus-specific operation that does not exist for light vehicles. These hazards are described in more detail as follows:

- **Vehicle motion while passenger door is open** – describes conditions where the driving automation system moves the vehicle from a stop while the door is still open or fails to bring the vehicle to a stop if the passenger door opens inadvertently, increasing the risk of passengers being injured.
- **Vehicle too far from curb at bus station/stop** – describes a situation in which the docking system does not steer the bus close enough to the curb to safely disembark passengers, particularly those passengers that may have mobility limitations.

SECTION
6

Risk Assessment

Each potential vehicle-level hazard identified in this study was assessed for risk in accordance with the ISO 26262 functional safety process. The ISO 26262 risk assessment process considers three parameters—severity, exposure, and controllability. The combination of severity, exposure, and controllability values typically results in one of four ASILs using the matrix shown in Appendix D. ASILs range from A (lowest) to D (highest). In instances in which the assessed risk does not reach the threshold of an ASIL, ISO 26262 denotes a QM rating, which indicates that the organization's internal quality management process applies and the hazard does not need to be mitigated through the ISO 26262 process [3].

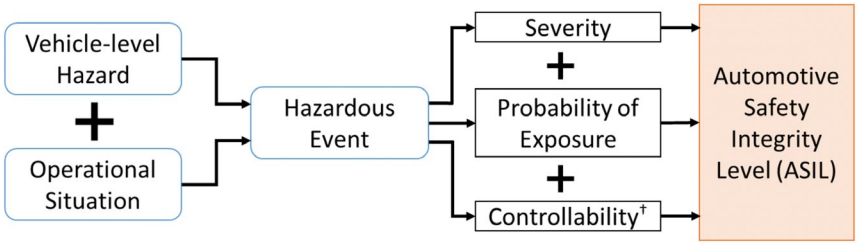
The goal of the risk assessment process is to use a systematic method to determine the most stringent ASIL that applies to each identified vehicle-level hazard. In the context of the overall ISO 26262 functional safety process, the designated ASIL will dictate the level of design rigor required to mitigate the hazard (e.g., redundant components, external system monitors).

Hazardous Event Development

The identified vehicle-level hazards require context in order to be assessed. That is, the conditions under which the hazard is occurring may affect the value assigned to each risk assessment parameter. For instance, the hazard "excessive vehicle propulsion" may have a lower severity rating when considered in the context of an open, straight road versus an intersection with pedestrians present.

To determine the worst-case ASIL, ISO 26262 describes a process for systematically evaluating hazards in different contexts by developing hazardous events. A "hazardous event" is a combination of a vehicle-level hazard and a particular operational situation, as shown in Figure 6-1. ISO 26262 defines an operational situation as a "scenario that can occur during a vehicle's life" [3]. Operational situations must provide enough detail to allow analysts to assess each dimension for the risk assessment but must also be sufficiently broad to avoid inappropriate lowering of the ASIL [3].[13]

Figure 6-1
ISO 26262 risk assessment process



[13] A highly-detailed operational situation may result in a combination of conditions that, when considered together, result in a very low probability of occurrence.

To develop operational situations, this study started by examining six top-level use cases for advanced driver assistance systems[14] described in *Transit Bus Automation: Technology Packages and Use Cases* [11]:

- Smooth Acceleration and Deceleration
- Automatic Emergency Braking and Collision Avoidance
- Curb Avoidance
- Precision Docking
- Narrow Lane/ Shoulder Operations
- Platooning

In addition, this study examined a seventh top-level use case from that report that deals with unique operations in restricted access bus maintenance and yard facilities [11]:

- Automated Parking Operations

The driving automation systems analyzed in this study were mapped to each of these seven use cases, as shown in Appendix E. This allowed analysts to map the vehicle-level hazards identified for each system to the use cases applicable to each system. However, these use cases are too broad for direct use in the risk assessment, as they do not provide enough detail to evaluate severity or exposure.

This study refined the use cases by allocating a subset of 13 operational situation categories to each use case.[15] These categories were based on industry guidance for light vehicles from SAE Recommended Practice J2980 [9] and from information obtained from SMEs interviewed as part of this study. The operational situation categories used in this study include:

- Vehicle Speed (Forward)
- Vehicle Speed (Reverse)
- Traffic Conditions
- VRU Traffic
- Road Geometry
- Road Conditions
- Road Types
- Weather Conditions

[14] Advanced driver assistance systems typically operate at Level 1 or 2 automation, as defined in SAE International Recommended Practice J3016 [17].

[15] Note that this is not a comprehensive list of all possible operational situation categories, as some use cases may depend on specific transit agency needs. Instead, it provides a generic set of common elements relevant to this study and which could be refined by future users of this report.

- Ambient Conditions
- Bus Stop Location
- Bus Passenger State
- Bus Loading
- Parking Facility Characteristics

To illustrate this approach, Table 6-1 shows the operational situation categories considered for the use case "smooth acceleration and deceleration." Note that some operational situation categories, such as vehicle speed (reverse) and parking facility characteristics, were not applicable to this use case.

Table 6-1

Example Application of Operational Situation Categories to Transit Bus Use Case

Use Case	Detailed Category	Parameters for Risk Assessment
Smooth Acceleration and Deceleration	Vehicle Speed (Forward)	• 0–5 mph
		• 5–15 mph
		• 15–30 mph
		• Over 30 mph
	Traffic Conditions	• Light traffic
		• Heavy traffic
	VRU Traffic	• Light VRU traffic
		• Heavy VRU traffic
		• VRUs with unconventional behavior
	Road Geometry	• Straight to moderate curvature
		• Sharp curvature
		• Level to low grade
		• Moderate to steep grade
	Road Conditions	• Slippery
		• Moderate to good road conditions
	Road Types	• City
		• Expressway
		• Dedicated bus lanes
	Weather Conditions	• Rain/snow/ice
		• Fog/smoke/particulates/precipitation
		• Sunny/overcast
	Ambient Conditions	• Low lighting
		• Good lighting
	Bus Passenger State	• Seated and buckled
		• Seated and unbuckled
		• Standing
	Bus Loading	• Light
		• Heavy
		• Unstowed objects (e.g., luggage, bags)

Appendix F shows the resulting framework used to develop the hazardous events for this study. The framework can be further refined or modified based on the specific needs of transit agencies or manufacturers developing driving automation systems. The framework in Appendix F provides a traceable link between the use cases, driving automation systems, and risk assessment.

Risk Assessment Dimensions

After defining the hazardous events, each is assessed along the three dimensions of severity, exposure, and controllability. ISO 26262 and SAE J2980 provide guidance for evaluating each dimension, with additional guidance specific to transit buses available in ISO 26262 Edition 2. Figure 6-1 illustrates how these parameters are used in conjunction with the hazardous event to derive an ASIL.

Severity is defined as the estimate of the extent of harm to one or more individuals that can occur in a hazardous event (Part 1 Clause 1.120 in ISO 26262 [3]). Table 6-2 shows the severity assessment values from ISO 26262 Part 3.

Table 6-2
Severity Assessment Values from ISO 26262

	Class			
	S0	**S1**	**S2**	**S3**
Description	No injuries	Light and moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries

S = Severity

Severity ratings may be influenced by transit bus-specific considerations, such as the presence of standing and unbuckled passengers. In addition, larger transit bus dimensions may increase the severity of crashes. For example, there is the potential for increased harm to VRUs from collisions with transit buses compared to light vehicles.

Exposure represents the likelihood of being in the operational situation described in the hazardous event when the hazard occurs (Part 1 Clause 1.37 in ISO 26262 [3]). For example, when considering a hazardous event related to passengers embarking or disembarking the bus, exposure may consider the frequency at which the bus is at a bus stop (i.e., almost every drive cycle, equating to high probability). Table 6-3 shows the exposure assessment values from Part 3 of the ISO 26262 standard.

Table 6-3
Exposure Assessment Values from ISO 26262

	Class				
	E0	**E1**	**E2**	**E3**	**E4**
Description	Incredible	Very low probability	Low probability	Medium probability	High probability

E = Exposure

Transit buses have increased exposure to hazardous events involving VRUs compared to light vehicles. Transit buses typically operate in urban environments that have a high number of VRUs using the roadway. Pedestrians also tend to cluster around the target destinations for buses (e.g., bus stops).

In conducting the exposure assessment for transit buses, another important consideration is that potential outlier conditions with low exposure for light vehicles could have much higher exposure for a transit bus that repeatedly runs a specific route. For instance, driving on a steep grade might have low exposure for a light vehicle, but a transit bus with a route that includes a steep grade might have much higher exposure to that condition. As this study is not based on any particular service route, the exposure parameter was assessed using national average frequencies, based on guidance in ISO 26262 Edition 2, SAE Recommended Practice J2980, and engineering judgment.

Controllability is defined as the "ability to avoid a specified harm or damage through the timely reactions of the persons[16] involved, possibly with support from external measures" (Part 1 Clause 1.19 in ISO 26262 [3]). Table 6-4 is ISO 26262's approach to assessing controllability (Table 3 in Part 3 in ISO 26262 [3]).

Table 6-4
Controllability Assessment Values from ISO 26262

	Class			
	C0	C1	C2	C3
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable

C = Controllability

When considering Level 1 and Level 2 driving automation systems, a key differentiator between light vehicles and transit buses is the presence of a trained operator. In transit bus applications, the bus operators are considered experts and can better control the bus in the event of a failure in the system compared to non-expert operators of light vehicles. This leads to a lower rating for the controllability parameter—that is, the bus operator has more control and, therefore, the resultant ASIL is lower.

Risk Assessment Results

Table 6-5 shows the range of ASILs identified in this study for each system using the ISO 26262 risk assessment process. The most stringent ASIL determined through the risk assessment was ASIL C; no systems were rated with ASIL D. Note that this analysis was performed on generic system architectures, assuming generalized operational situations. A system-specific analysis by manufacturers may yield different ASILs. Appendix C provides a breakdown of the identified ASILs by system and hazard.

[16] Persons involved can include the driver, passengers, or persons in the vicinity of the vehicle's exterior.

Table 6-5
Identified ASIL Ranges by System

Driving Automation System	Identified ASIL Range
Adaptive Cruise Control with Stop-and-Go	A-C
Automatic Emergency Braking	A-C
Docking	A-C
Full Park Assist/ Valet Park	A
Lane Keeping/ Lane Centering/ Steering Assist	A-C
Object Detection and Collision Avoidance	QM*
Park Assist/ Park Out/ Yard Park	A
Rear Brake Assist	A
Traffic Jam Assist with Lane Keeping/ Lane Centering	A-C

**QM is not considered an ASIL and denotes that the ISO 26262 process does not apply. ASIL A = least stringent, ASIL D = most stringent*

Five systems had ASILs ranging from ASIL A to ASIL C. All five operate while the bus is in service, meaning that they operate in an environment in which the bus has a higher exposure to VRUs and other motorists. In contrast, systems that generally operate in maintenance yards, parking lots, and other restricted access facilities had ASIL A ratings. These systems have lower exposure to VRUs and other motorists and also operate at lower speeds.

When conducting the risk assessment, the same hazard may be assigned different ASILs depending on the associated system. For instance, "excessive vehicle propulsion" was assigned ASIL C for the ACC system since it could very likely result in the bus striking a VRU at speeds over 30 mph. The same hazard was assigned ASIL A for the full park assist/valet park system since it operates at a lower speed, which both reduces the severity and improves the controllability by giving the operator more time to react.

The risk assessment performed in this study does not consider the effect of independent vehicle systems or other external measures on improving the controllability of a certain hazard. Per ISO 26262, these external measures can be considered during the assessment of controllability and must be independent of the system being analyzed. That is, a common failure would not affect both the system being analyzed and the system or measure that improves controllability. A system-specific analysis by manufacturers may consider the effect of any such measures included in their transit bus architecture.

Comparison of Light Vehicle and Transit Bus ASILs

This study attempted to compare the ASILs identified for driving automation systems considered in this study with ASILs for their light vehicle counterparts. However, for competitive and liability reasons, most light-vehicle original equipment manufacturers (OEMs) do not publicly share the ASIL classifications for the E/E and driving automation systems used in their vehicles.

Instead, this study compared the identified ASILs against guidelines on ASIL classifications for foundational vehicle systems in light vehicles (i.e., steering, propulsion, and braking) available from SAE J2980.[17] The driving automation systems considered in this study request actuation from one or more of the bus's foundational systems, so there are similarities between some of the hazards identified in this study and the hazards in SAE J2980. This may allow some comparison between the ASILs identified for transit buses and light vehicles, although it is not a direct comparison, as the underlying systems are different. That is, some hazards, such as "loss of vehicle deceleration or braking," may be easier to avert when they affect a driving automation system rather than a foundational vehicle system; in the former situation, the assumption is that the brake system would still be able to stop the vehicle if the driver presses the brakes.

The SAE J2980 ASIL classification guidelines for hazards related to the propulsion system and braking system are widely used in the automotive industry. For example, a paper by members of an automotive staffing company assigned ASIL C classification to hazards related to the propulsion and braking systems in their publications, which is aligned with the guidelines in SAE J2980 [12]. A survey covering the ASIL classification of hazards related to these systems also shows close resemblance to the guidelines provided by SAE J2980 [13].

Propulsion-related Hazards

The comparison of the ASILs for propulsion-related hazards are presented in Table 6-6.

Table 6-6

Comparison of Transit Bus and Light Vehicle Propulsion-related Hazards

Potential Vehicle-level Hazard	Transit Bus Risk Assessment	Comparable SAE J2980 Range
Excessive Vehicle Propulsion	ASIL A-C*	ASIL B-C
Insufficient Vehicle Propulsion	QM-ASIL A*	QM

**Specific ASIL is system-dependent, as shown in Appendix C, Table C-1.*

The ASIL classification for transit bus driving automation systems is comparable to the ASIL range for propulsion-related hazards in SAE J2980. ASIL A for "excessive vehicle propulsion" is slightly lower than the comparable range in SAE J2980. This is attributed to differences in the transit bus operational situations for some systems, such as low-speed operation in a parking lot or maintenance yard. These situations have more favorable severity and controllability ratings.

[17] Note that the ASILs in SAE J2980 are only guidelines, and, in many instances, SAE J2980 provides a range of ASIL classifications. Furthermore, not all hazards in Appendix C are included in SAE J2980.

Braking-related Hazards

Comparison of braking-related hazard is presented in Table 6-7.

Table 6-7

Comparison of Transit Bus and Light Vehicle Braking-related Hazards

Potential Vehicle-level Hazard	Transit Bus Assessment	Comparable SAE J2980 Range
Excessive Vehicle Deceleration or Braking	QM-ASIL C*	ASIL B-C
Insufficient Vehicle Deceleration or Braking	QM-ASIL B*	QM-ASIL D

**Specific ASIL is system-dependent, as shown in Appendix C, Table C-1.*

The ASILs for braking-related hazards determined in this study are lower for transit buses compared to the ASILs assigned to braking-related hazards for light vehicles in SAE J2980. One factor behind the lower ASILs was differences in the operational situations. For instance, for "excessive vehicle deceleration or braking," the lower classifications in this study (QM and ASIL A) for transit buses are associated with driving automation systems that operate at low speeds and are restricted to bus parking and maintenance facilities. The controllability and severity ratings in these settings are lower than other passenger vehicle applications.

For "insufficient vehicle deceleration or braking," the ASIL classifications for transit buses were at the lower end of the range specified in SAE J2980. This was largely due to the improved controllability afforded by skilled transit bus operators. SAE J2980 also considers instances of this hazard that affect the underlying brake system, meaning that a failure may prevent the brake system from responding to driver input. However, since the risk assessment performed in this study focuses on driving automation systems rather than the foundational vehicle system, this study assumes that the brake system is able to respond to the driver's input.

Steering-related Hazards

The comparison of steering-related hazards is presented in Table 6-8.

Table 6-8

Comparison of Transit Bus and Light Vehicle Steering-related Hazards

Potential Vehicle-level Hazard	Transit Bus Assessment	Comparable SAE J2980 Range
Excessive Lateral Motion/Yaw	ASIL A-C*	ASIL B
Insufficient Lateral Motion/Yaw	ASIL A-C*	ASIL B

**Specific ASIL is system-dependent, as shown in Appendix C, Table C-1.*

The risk assessment included ASIL classifications for steering-related hazards that were both slightly higher and lower for transit buses compared to light vehicles. The factors affecting the ASILs are similar to those described previously.

The severity rating for collisions between a bus and VRUs was higher than the severities for light vehicles but was not necessarily offset by improved controllability. For instance, the narrower margins between a bus and lane lines due to the wider bus dimension could mean that the driver may not have as much time to respond if the bus suddenly veers into a bike lane. In other instances, the presence of an experienced transit bus operator provided more favorable controllability ratings compared to light vehicles, resulting in a lower ASIL.

SECTION

7

Safety Measures

The ISO 26262 functional safety process uses a top-down approach to derive safety measures. Each level of safety measure is then decomposed into a set of more detailed safety measures. Figure 7-1 illustrates this top-down approach to deriving safety measures.

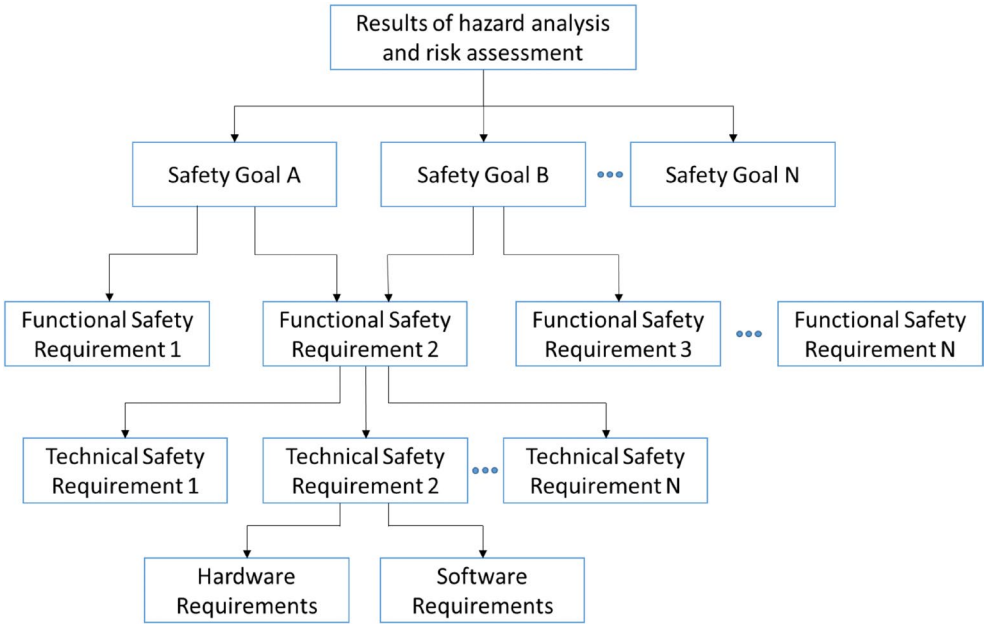


Figure 7-1

Hierarchical relationship between safety goals and safety requirements supporting safety goals at different levels of decomposition

Adapted from ISO 26262 Part 3, Figure 2

The top-most level of safety measures are called "safety goals." ISO 26262 defines safety goals as "top-level safety requirements as a result of the hazard analysis and risk assessment at the vehicle level" [3]. The safety goals are typically broadly stated and describe objectives of mitigating or preventing the identified vehicle-level hazards. The HARA results from Sections 5 and 6 were used to derive safety goals for each driving automation system in this study.

Since the safety goals are stated broadly, they do not provide a much detail. Therefore, the functional safety process decomposes the safety goals into functional safety requirements,[18] which are implementation-independent and function-based safety measures.

[18] Although the term is "safety requirement," it was not the purpose of this study to develop requirements for any particular system. Rather, this study intended to illustrate concepts in the ISO 26262 functional safety process as they apply to transit buses and to provide examples of different types of safety considerations that may need to be taken into account when transferring certain light vehicle driving automation system technologies to transit buses.

Whereas this report follows the ISO 26262 functional safety process to derive safety goals and functional safety requirements, the objective of this study was not to specify requirements. Rather, the purpose was to describe only those additional safety measures that may be necessary as these driving automation system technologies are transferred to transit buses. Therefore, this report refers to these as "functional safety measures" instead of "functional safety requirements."

The safety measures described herein include both functional safety (i.e., ISO 26262) and non-functional safety measures (i.e., safety-relevant design considerations) that arise as a result of transit bus operations, interactions with transit bus-specific systems, or transit bus physical characteristics. These transit bus-specific safety measures may provide insight to those seeking to transfer driving automation system technologies to transit buses.

Top-Level Safety Goals

This study derived a total of 21 safety goals. As these safety goals are derived directly from the vehicle-level hazards, there is often a one-to-one mapping between safety goals and hazards. However, it is possible for one safety goal to address multiple hazards or for multiple safety goals to address a single hazard, which is why the total number of safety goals identified in this study (21) is greater than the number of identified vehicle-level hazards (18). One safety goal might also apply to more than one system. The number of safety goals identified for each driving automation system considered in this study is shown in Table 7-1. A breakdown of the safety goals by hazard and system is provided in Appendix G.

Table 7-1
Number of Identified Safety Goals by System

System	Number of Identified Safety Goals*
Adaptive Cruise Control with Stop-and-Go	12
Automatic Emergency Braking	8
Docking	7
Full Park Assist/ Valet Parking	15
Lane Keeping/ Lane Centering/ Steering Assist	7
Object Detection and Collision Avoidance	1
Park Assist/ Park Out/ Yard Park	5
Reverse Braking Assist	8
Traffic Jam Assist with Lane Keeping/ Lane Centering	16

**A safety goal may be relevant to more than one system. For instance, the safety goal "prevent excessive vehicle propulsion under all vehicle operating conditions" is applicable to three systems and, thus, is counted three times in the list above.*

Safety goals inherit the highest ASIL classification for the hazard or hazards that the safety goal is intended to mitigate. Essentially, the risk assessment determines the level of design rigor needed to mitigate a particular hazard. That level of

design rigor then transfers from the hazard to the safety goal and from the safety goal to all subordinate safety measures. As with the vehicle-level hazards, a safety goal may be relevant to multiple systems and may have different ASIL for each system.

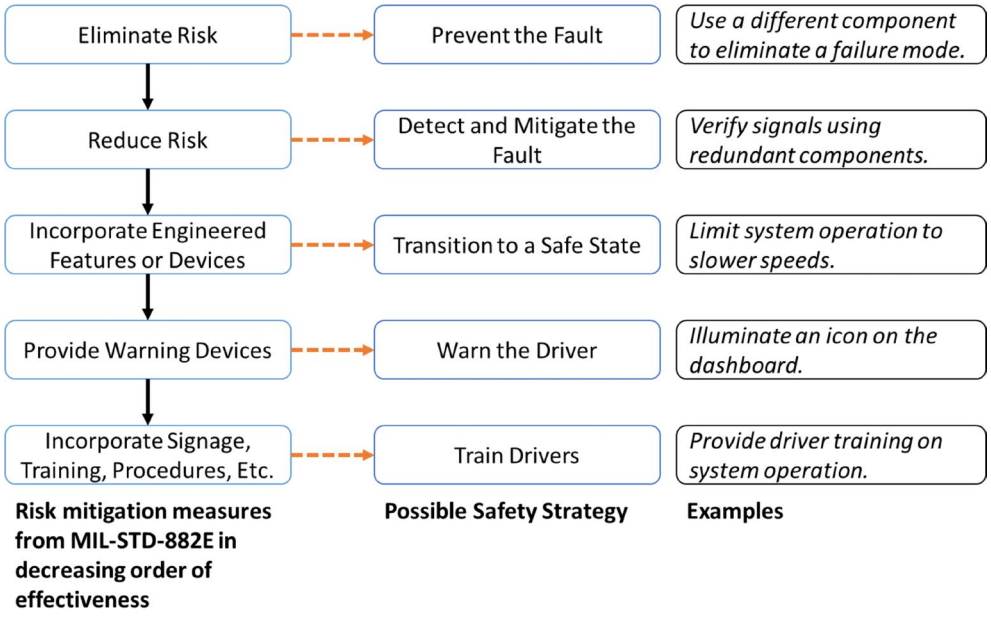
This study derived two safety goals that were specific to transit buses. These safety goals correspond to the two unique hazards identified for transit buses:

- Prevent continued vehicle motion while the passenger door is open.
- Ensure that the vehicle stops at the driver-specified distance from the curb at a bus station/stop.

General Safety Strategy

In general, the purpose of a safety goal is to mitigate risk at the hazard level. The safety goals are achieved through decomposition to functional safety requirements (as shown in Figure 7-2) in accordance with a safety strategy. One such safety strategy could be derived from the approach to establishing risk mitigation measures described in Military Standard (MIL-STD) 882E [4]. In Figure 7-2, the general risk mitigation measures from MIL-STD-882E are interpreted for functional safety.

Figure 7-2
Example safety strategy based on MIL-STD-882E



MIL-STD-882E presents five risk mitigation measures in order of decreasing effectiveness, from eliminating risk to incorporating signage, training procedures, etc. [4]. In the context of driving automation systems for transit buses, this suggests that, in the event of a failure during system operation, safety mechanisms incorporated into the system design may be more effective at mitigating risks than relying on extensive driver training.

ISO 26262 outlines typical safety strategy elements that can be mapped to the first through fourth steps in the MIL-STD-882E risk mitigation measures, including:

1. Eliminate risk by:
   - Changing the technology to eliminate failure modes (e.g., switching to a different sensor type).
2. Reduce risk by:
   - Ensuring that the system elements are functioning correctly.
   - Ensuring that the critical sensors' inputs to the main controller are valid and correct (e.g., redundant measurements paths).
   - Validating[19] the health of the main controller (e.g., using an auxiliary processor).
   - Ensuring the validity and correctness[20] of critical parameters identified through the safety analysis (e.g., using periodic checks to detect corrupted parameters and other latent faults).
   - Ensuring the validity and correctness of the critical communication signals internal and external to the system (e.g., quality factors[21]).
   - Ensuring the correct system request, in terms of magnitude, direction, and timing, is delivered to the foundational systems.
   - Ensuring the correctness and timeliness of the arbitration strategy.
3. Incorporate engineered features or safety devices by:
   - Mitigating the potential hazards when an unsafe condition is detected.
   - Ensuring that the safe state is reached on time when a potentially hazardous condition is detected.
   - Ensuring that low-voltage power is available until the safe state is reached under all potentially hazardous conditions.
4. Provide warning devices by:
   - Ensuring driver warnings are delivered when an unsafe condition is detected.

The general safety strategy outlined in this section can be applied to each safety goal to develop a safety strategy. An example of this approach is shown in Table 7-2. Appendix G shows how the safety strategy could be applied to each of the safety goals derived for the driving automation systems considered in this study.

[19] "Validate" means to ensure that the value of a parameter or the state of an element falls within a valid set of values or states.

[20] "Correctness" means that the value of a parameter is the correct one from the valid set.

[21] Quality factors refer to techniques for error detection in data transfer and communication, including checksums, parity bits, cyclic redundancy checks, error correcting codes, etc.

Table 7-2
Example Application of Safety Strategy

System	Adaptive Cruise Control
Potential Vehicle-level Hazard	Vehicle motion while the passenger door is open.
Safety Goal	Prevent continued vehicle motion while the passenger door is open through design and validation techniques in accordance with the ASIL A classification.
Safety Strategy	
Reduce Risk	• Prevent all faults that could prevent the ACC system from determining the passenger door state.* Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262. - If a fault that could prevent the ACC system from determining the passenger door state cannot be prevented, then detect and mitigate the fault. • Acknowledge all faults communicated by other vehicle systems that may prevent the ACC system from responding to an open passenger door, including faults communicated by the door control system. - Communication of the passenger door state from the door control system to the ACC system should be designed and validated in accordance with the specified ASIL.
Incorporate Engineered Features or Safety Devices	• If a failure that could allow the bus to continue moving while the passenger door is open occurs, transition into a safe state within the fault tolerant time interval (FTTI).**
Provide Warning Devices	• If a failure that could allow the bus to continue moving while the passenger door is open occurs, warn the driver and communicate any necessary actions to the driver (e.g., manually stop the vehicle, close the passenger door).

**This assumes that the ACC system design includes measures to prevent vehicle motion when the doors are open during nominal (i.e., un-faulted) operation.*

***FTTI is the minimum time span from the occurrence of a fault in a system to a possible occurrence of a hazardous event, if safety mechanisms are not activated [1].*

As part of the safety strategy, Appendix G provides examples of potential safe states for each driving automation system in the study. ISO 26262 defines safe states as an "operating mode, in case of failure, of an item without an unreasonable level of risk" [3]. Examples of safe states provided in ISO 26262 include switched off, locked, reduced functionality, or vehicle stationary and position maintained [3]. The example safe states presented for each system in Appendix G follow a tiered disengagement strategy, with different levels of system functionality depending on the failure type and supported safety goal(s).

Table 7-3
Example Safe State Strategy

System	Adaptive Cruise Control	Possible Triggering Condition
Example Safe States	Limit system operation to speeds below TBD* mph.	Failure in one sensor of multiple sensors that monitor the distance to the lead vehicle. Remaining sensor(s) are operational.
	Issue notifications through multiple channels.	Failure in communication between the ACC system and HMI.
	Disable the system and return control back to the driver.	Failure in all sensors that monitor the distance to the lead vehicle.

**An appropriate limit on the operational speed for this safe state would be determined as part of the system design or based on results of future testing.*

Transit Bus-Specific Considerations for Safety

Functional Safety Measures

This study found that the functional safety measures for light vehicles would generally be applicable to driving automation systems for transit buses. However, slight modifications to these functional safety measures may be necessary—for instance, adjusting the FTTI if different timing is necessary to bring the bus to a safe state because of longer stopping distances for buses.

The application of the ISO 26262 process to the driving automation systems in this study identified several transit bus-specific functional safety measures. Note that these functional safety measures are intended to illustrate the additional safety measures that may be necessary when developing a functional safety concept for transit buses and are not intended to constitute specific design requirements.

Several transit bus-specific functional safety measures were the result of new interfaces between the driving automation systems and other vehicle systems that are unique to transit buses, such as passenger doors. For instance, APTA's *Standard Bus Procurement Guidelines* describes a passenger door interlock that would preclude movement of the bus if the mid or rear door panel is open more than three inches [7]. If such an interlock is installed on a transit bus, a driving automation system that controls the bus's longitudinal motion would need to support the interlock. Examples of these types of functional safety measures developed for the ACC system are presented in Table 7-4. A complete list of the transit bus-specific functional safety measures identified in this study is provided in Appendix H.

Table 7-4

Example Functional Safety Measures for Interfaces with Other Systems Unique to Transit Buses

System	Adaptive Cruise Control
Safety Goal	Prevent continued vehicle motion while the passenger door is open.
Example Functional Safety Measure(s)	Ensure that the ACC system controller detects right passenger door state at all times.
	Ensure that door control system reports the correct door position state to the ACC system.
	Monitor the response time of the ACC controller to changes in the passenger door status. If the permissible response time is exceeded, the ACC system is to alert the driver and/or transition to an appropriate safe state.

This study also found that there may be new safety-relevant design considerations unique to transit buses, such as limiting the system acceleration or deceleration rates to protect passengers (see the following subsection). Additional functional safety measures are needed to ensure that failures related to these safety-relevant design considerations do not result in hazards. Examples of these types of functional safety measures are provided in Table 7-5.

Table 7-5

Example Functional Safety Measures Supporting Unique Transit Bus Safety-relevant Design Considerations

System	Adaptive Cruise Control
Safety Goal	Prevent excessive vehicle propulsion under all vehicle operating conditions.
Example Functional Safety Measure(s)	Verify the correctness of the acceleration rate limit for the ACC system.
	Verify the correctness of the vehicle acceleration profile.
	Ensure that the correct speed profile is selected at all times depending on the passenger and cargo status.

Safety-relevant Design Considerations

ISO 26262 focuses on mitigating hazards that result from failures in the system. However, ISO 26262 does not establish safety-relevant design considerations relevant to normal operation. Over the course of this study, several other safety-relevant design considerations were identified. The considerations described below are intended to help illustrate some of the unique safety challenges related to transferring driving automation system technologies from light vehicles to transit buses. These considerations are not intended to represent a comprehensive set of safety measures for transit buses or to replace a comprehensive system-specific safety analysis that would be performed as part of the system design process.

Passenger Embarkation/Disembarkation

Unlike light vehicles, transit buses have large passenger doors and unrestrained passengers. This presents a potential risk to passengers during certain bus movements. For example, the ACC or TJA system theoretically could resume accelerating while passengers are still embarking/disembarking. As noted, APTA's *Standard Bus Procurement Guidelines* provides guidelines for accelerator and brake interlocks intended to preclude movement while the passenger door is open [7]. Therefore, the following safety measures help to ensure the design for these systems allows passengers to embark and disembark the bus safely:

- The ACC and TJA algorithms may need real-time awareness of the passenger door status.
- ACC and TJA system algorithms may need to incorporate specialized behavior for various passenger door states.
- The docking system may need additional mechanisms to help ensure that the bus position allows for safe ingress and egress (particularly for passengers with disabilities) after completing the docking maneuver.

Acceleration/Deceleration Limits

The presence of unrestrained passengers and unsecured cargo presents a potential safety risk during aggressive acceleration or deceleration, including lateral acceleration (i.e., steering and cornering). Acceleration and deceleration

may need to be limited to levels that do not displace passengers or cargo in a potentially harmful manner.

Numerous studies through the years have addressed the issue of acceptable acceleration and deceleration levels on buses and trains [14–19]. The two main components of acceptability are maximum acceleration/deceleration level and the time derivative of acceleration ("jerk"). Jerk is typically quantified in units of m/s^3 but is most commonly conceived as a measure of how quickly the acceleration rises from zero to its maximum. Hoberock recommended that maximum acceleration levels do not exceed 1.1 to 1.5 m/s^2 (0.11 to 0.15 g) with jerk limited to 3 m/s^3 (0.3 g/s) [17]. This acceleration level is consistent with early work by Hirshfeld which found that passengers in the worst-case configuration (forward-facing unsupported standees) lost their balance at an average deceleration of 0.13 g [16]. The 0.3 g/s jerk level provides for a rise time to maximum acceleration of at least 0.36 seconds. Allum et al. found that minimum passenger reaction time was on the order of 0.12–0.13 seconds [15], and Simoneau and Corbeil estimated the time for a passenger to make gross body adjustments to retain balance at about 1 second [20].

Therefore, the following safety measures are intended to ensure that system design considers the effects of acceleration and deceleration levels on passengers:

- Driving automation systems that control propulsion and braking (e.g., ACC, AEB) may need to establish a limit on acceleration and deceleration that ensures the safety of unsecured standing or seated passengers as well as safety from objects displaced in a way that could cause harm to the passengers or the driver. Similarly, driving automation systems that control steering (e.g., docking, lane keeping/lane centering/steering assist) should establish a limit on lateral acceleration[22] that ensures the safety of unsecured standing or seated passengers as well as safety from displacement of objects in a way that could cause harm to the passengers or driver. The permissible acceleration or deceleration could vary, provided the driving automation system can accurately determine the passenger states, bus loading, and other pertinent characteristics. However, this may be technically challenging. A worst-case assumption might be that an unrestrained passenger or cargo might strike a solid surface or other passenger that has already been decelerated to rest.
- Certain systems, such as AEB, may need to brake sooner to ensure that the system achieves the desired level of speed reduction without exceeding the deceleration level established to protect passengers. However, a control system capable of a faster reaction time may have an inherently higher rate

[22] In general, lateral accelerations, even in an avoidance maneuver, will be of lower magnitude than those associated with significant longitudinal events (e.g., crashing, emergency braking).

of false positives. The acceptable false positive rate for these systems should be established.

- Establishing a maximum permissible deceleration that protects passengers may also limit the ability for the bus to avoid striking an (external) VRU. That is, the system may find itself in a scenario in which it is not feasible to avoid an injurious outcome. Careful evaluation in advance must be undertaken to understand the most likely implications of candidate deceleration levels. System developers will likely need to agree to *a priori* guiding principles (e.g., minimizing the most likely maximum injury severity).

Note that resolutions to such scenarios may have numerous potential options, of which none may be generally acceptable. Operators may find themselves with choices that could include, for example, striking a vehicle, striking a pedestrian, striking a fixed object (such as infrastructure, a tree, a trash can, a hedge), or hitting a curb at speed. The implications for occupants and VRUs may not be readily-assessable. Conversely, in the Level 0 to Level 2 systems in scope for this report, the time interval over which the automation system begins to de-throttle propulsion and engage the brakes may be sufficient for the human operator to evaluate the situation and decide upon the most reasonable and safe response. Under such conditions, the system will have provided a quicker reaction without itself initiating a maneuver with unreasonably unsafe consequences for unsecured passengers.

Vehicle Dimensions and Dynamics

The dimensions and vehicle dynamics of transit buses are significantly different from those of light vehicles. As described in ISO 26262, variations in the loading condition and changes to the position of the center of gravity should be considered in the hazard analysis [3]. Although ISO 26262 addresses only mitigation measures where failures may be exacerbated by these dynamics, the following safety measures are intended to help ensure the effects of the bus dynamics are considered by the relevant systems:

- The larger bus dimensions may affect several calibration parameters that affect the operation of driving automation systems. For instance, the default width of a transit bus is approximately 8.5 ft [7]. In comparison, the average width of a mid-size passenger car is approximately 6.5 ft [21]. Thus, on narrow roadways, a driving automation system such as lane keeping or lane centering might have a smaller margin during which the system can intervene. Although this is a typical part of the system design process, manufacturers may need to take added measures when transferring driving automation systems to transit buses to ensure that calibration parameters, including those related to sensor locations, are updated to reflect the different physical dimensions of the bus.

- Transit buses may require greater stopping distance than light vehicles. For example, in Table 2 of Federal Motor Vehicle Safety Standard (FMVSS) 105, which applies to hydraulic brake systems, the stopping distance for a passenger vehicle traveling at 35 mph is 74 ft, and the stopping distance a transit bus (i.e., a gross vehicle weight rating over 10,000 pounds) is 132 ft [22]. In Table 2 of FMVSS 121, which applies to pneumatic brake systems, the stopping distance for a transit bus traveling at 35 mph is 96 ft [23]. Furthermore, to ensure the safety of passengers and the driver, the deceleration rate may be inherently limited. These limitations may affect the ability of the ACC or TJA system to respond to sudden changes in speed of the lead vehicle at close following distances. Therefore, the ACC and TJA system's permissible following distances may need to be established to provide the bus with adequate stopping distance.
- Transit buses may make wide turns that require the bus to deviate from the current travel lane, as indicated by SMEs. Lateral control components of transit bus driving automation systems should not interfere with lane deviations required to make wider turns.

The physical dimensions of a bus may also present challenges for placing sensors in manner that minimizes blind spots. For example, a forward-looking camera situated to provide medium-distance coverage ahead of the vehicle may not provide good coverage immediately in front of the vehicle. Conversely, a camera mounted high on the bus and angled downward to provide coverage immediately in front of the vehicle may not provide longer-range coverage. This becomes increasingly important if multiple sensor types are needed to provide robust and redundant coverage around the bus. The following safety measures are intended to help ensure adequate sensor coverage around the bus:

- Pedestrian detection algorithms should have sufficient robustness and integrity in terms of function and performance. For instance, the pedestrian detection algorithms should have a low false negative rate and high robustness for determining the correct braking distance.
- Sensor coverage should be evaluated to minimize blind spots for systems relying on those sensors (e.g., ACC, AEB, TJA). Additional measures may be necessary to ensure sensor coverage is sufficiently robust.

SECTION 8

Summary and Conclusions

This project report describes the results of applying a hazard and safety analysis to nine categories of Level 0 to Level 2 driving automation systems that potentially are transferrable from light vehicles and heavy trucks to transit buses. The analysis approach was based on the functional safety process for road vehicles, ISO 26262.

This study found that:

- The majority of vehicle-level hazards and functional safety measures for Level 0 to Level 2 driving automation systems would be similar for light vehicles, heavy trucks, and transit buses. In general, this will facilitate transfer of these technologies to transit buses.
- Unique vehicle-level hazards exist for Level 0 to Level 2 driving automation systems in transit buses based on transit bus-specific operations, such as embarking and disembarking passengers. System-specific hazard analyses should be performed when transferring these systems to transit buses to ensure that any transit bus-specific hazards are identified.
- For hazards common to both light vehicles, heavy trucks, and transit buses, additional safety-relevant design considerations specific to transit buses exist—for instance, new safety measures may be needed to protect standing and unrestrained passengers. As with the hazard analysis, a system-specific safety analysis should be performed to identify these additional safety-relevant design considerations.

This study identified 18 potential vehicle-level hazards, of which 15 are common to both transit bus driving automation systems and light vehicles. Two hazards were unique to transit buses—"vehicle motion when passenger door is open" and "vehicle too far from curb at station/stop." A third hazard—"excessive vehicle roll"—is common to both light vehicles and transit buses, although it has greater applicability to transit buses because of their higher center of gravity.

The ISO 26262 risk assessment process was applied to each of the 18 vehicle-level hazards. In general, the ASILs assigned to the hazards identified in this study were consistent with the ASIL ratings for comparable hazards in light vehicles. In some instances, the ASILs assigned to hazards for transit bus driving automation systems were lower than their light vehicle counterparts. This was primarily influenced by more favorable controllability ratings based on the presence of a trained (i.e., skilled) bus driver and consideration of transit bus use cases, such as a lower speed range for transit bus operation. Two steering-related hazards

had ASILs that were more stringent than their light vehicle counterparts, largely due to the increased severity of the bus striking a VRU; in some operational situations, even a skilled transit bus driver may not have sufficient time to react.

The favorable controllability ratings in the risk assessment generally offset higher severity and exposure ratings related to a transit bus's operation in high VRU environments. However, higher levels of automation (i.e., Level 3 to Level 5) may not benefit from the favorable controllability ratings from an experienced transit bus operator but may still have the higher severity and exposure ratings, and, therefore, higher ASILs.

This study found that an important consideration for assessing exposure is that potential outlier conditions with low exposure for light vehicles could have much higher exposure for a transit bus that repeatedly runs a specific route. That is, if a condition exists along a transit route (e.g., train tracks, steep hill) that would typically be rated with a low exposure for light vehicles, a transit bus may encounter that condition much more frequently as it repeatedly runs the same bus route. The current edition of ISO 26262 does not provide guidance or examples for considering exposure in the context of repeated operation along a fixed route. The ramifications of this issue on system design are unknown—for instance, a system may need different levels of design for different regions, or a system may not be suitable for some regions if the difference in exposure results in significantly different ASILs from the ASILs to which the system was designed.

Several SMEs indicated the importance of preventing injury to passengers because of sudden changes in the vehicle's motion (e.g., hard braking). In traditional transit buses, the operator continually gauges the state of passengers (e.g., standing vs. seated) and operates the bus accordingly. The risk assessment performed in this study explicitly considered the implications for on-board passengers. However, standing or unbuckled passengers had a smaller influence on the ASIL assessment than anticipated. In general, injury resulting from displacement of passengers did not outweigh the severity from other hazardous events that drove the ASIL rating, such as collision with a VRU.

Consideration of on-board passengers, however, did factor into the transit bus-specific safety measures identified in this study. In particular, driving automation systems for transit buses may need to limit acceleration and deceleration rates (including lateral acceleration) to prevent displacement of passengers. This is a unique consideration for transit buses; in light vehicles, occupants are typically restrained (i.e., by seatbelts) and can therefore safely tolerate higher accelerations or decelerations.

The transit bus-specific functional safety measures identified in this study fell into two categories. The first describes measures that mitigate failures in the driving automation systems that could lead to violation of the acceleration and

deceleration rate limits, described above, and the second focuses on functional safety measures addressing failures that could lead to one of the transit bus-specific hazards. Outside of these two categories, this study found that the functional safety measures for light vehicles would generally transfer to driving automation systems for transit buses. However, some modification of the light vehicle functional safety measures may be necessary. For instance, the increased stopping distance for transit buses compared to light vehicles could mean that the transition time to a safe state needs to be adjusted for systems in transit buses.

This study also derived several transit bus-specific safety-relevant design considerations that fall outside of the scope of ISO 26262. These safety measures arise as a result of specific transit bus operations, interactions with transit bus specific systems, or transit bus physical characteristics. For instance, ACC and TJA systems may need new interfaces with the door control system to ensure that they do not cause the transit bus to resume moving while the passenger doors are open.

As transit agencies and bus manufacturers consider integrating driving automation systems into transit buses, new approaches may be necessary to ensure the safety of these electronic systems. ISO 26262 is one such approach, which is used extensively for light vehicles and has since been extended to cover transit buses. This report may serve as an example of how the ISO 26262 concepts may be applied to transit buses. Furthermore, the combination of ASILs, safety goals, and general safety strategy presented herein may be informative to transit agencies and manufacturers as they conduct pilot programs and other studies to transfer light vehicle driving automation system technologies to transit buses.

APPENDIX

A

HAZOP Functions

Adaptive Cruise Control with Stop-and-Go:

- Activate the system via the HMI.
- Detect vehicles ahead.
- Accelerate/decelerate to maintain distance between the bus and vehicle ahead.
- Start/stop the bus.
- Detect faults and warn the driver when the system is inactive.
- Request the driver to take over.

Automatic Emergency Braking:

- Activate the system via the HMI.
- Detect objects and/or pedestrians.
- Deliver a driver warning to apply brakes.
- Request braking when objects are present at a specified distance.
- Detect faults and warn the driver when the system is inactive.
- Inform the driver that the system is inactive.

Docking:

- Activate the system via the HMI.
- Detect the curb, and lane markings and/or lane boundaries.
- Request steering torque to align the bus with the curb.
- Deactivate when the operator steers during the docking maneuver at a certain torque level.
- Detect faults and warn the operator that the system is inactive.
- Request the operator to take over

Full Park Assist and Yard Park:

- Activate the system via the HMI.
- Detect parking spot/slot.
- Request steering to maneuver the vehicle along the computed trajectory.
- Request propulsion to maneuver the vehicle along the computed trajectory.
- Request braking to maneuver the vehicle along the computed trajectory.
- Deactivate when the driver applies steering, propulsion, or braking above a specified limit (for full park assist).
- Detect faults and warn the driver when the system is inactive.
- Request the driver to take over.

Lane Keeping, Lane Centering, and Steering Assist:

- Activate the system via the HMI.
- Detect lane markings and/or lane boundaries.
- Request steering to maintain the vehicle within/at the center of the lane boundaries.
- Deactivate when the driver applies steering that counters the system's steering request by a specified limit.
- Detect faults and warn the driver when the system is inactive.
- Request the driver to take over.

Object Detection and Collision Warning Alert:

- Activate the system via the HMI.
- Detect objects, including pedestrians.
- Deliver warnings to the driver.
- Provide data on near-by objects to other vehicle systems.
- Detect faults and warn the driver when the system is inactive.

Park Assist, Park Out, and Yard Park:

- Activate the system via the HMI.
- Detect parking spot (for park assist) or designated location (for yard park).
- Request steering to maneuver the vehicle along the computed trajectory.
- Deactivate when the driver applies steering above a specified limit.
- Detect faults and warn the driver when the system is inactive.
- Request the driver to take over.

Reverse Brake Assist:

- Activate the system via the HMI.
- Detect objects and/or pedestrians.
- Deliver a driver warning to apply brakes.
- Request braking when objects are present at a specified distance.
- Detect faults and warn the driver when the system is inactive.
- Request the driver to take over.

Traffic Jam Assist with Lane Keeping/Lane Centering:

- Activate the system via the HMI.
- Detect vehicles ahead.
- Accelerate or decelerate to maintain distance between the bus and the vehicle ahead.
- Start/stop the bus.
- Detect faults and warn the driver when the system is inactive.
- Request the driver to take over.

APPENDIX

B

STPA Control Actions and Context Variables

Adaptive Cruise Control with Stop-and-Go

Request an increase/decrease in propulsion torque	
Driver's distance set point	Gap with lead vehicle above set point Gap with lead vehicle at set point Gap with lead vehicle below set point
Driver's speed set point	Vehicle speed below set point Vehicle speed at set point Vehicle speed above set point
Passenger door status	Door status is open Door status is closed
Lift system status	Lift system is stowed Lift system is deployed
Bus height status	Bus is kneeling Bus is at full height
Request an increase/decrease in brake torque	
Driver's distance set point	Gap with lead vehicle above set point Gap with lead vehicle at set point Gap with lead vehicle below set point
Driver's speed set point	Vehicle speed below set point Vehicle speed at set point Vehicle speed above set point
Engage/disengage parking brake	
Bus motion	Host vehicle stopped Host vehicle moving
Lead vehicle motion	Lead vehicle stopped Lead vehicle moving
Brake status	Service brake engaged Service brake disengaged
Engine start/stop	
Bus motion	Host vehicle stopped Host vehicle moving
Lead vehicle motion	Lead vehicle stopped Lead vehicle moving
Engage/disengage feature	
Driver request	Driver activates feature Driver deactivates feature
Vehicle operating speed	Vehicle speed above maximum operating speed Vehicle speed at maximum operating speed Vehicle speed below maximum operating speed
Issue driver warning via HMI	
System status	Feature available Feature not available

Automatic Emergency Braking

Increase/decrease brake torque	
Distance to object	Object in path at first TTC threshold Object in path at second TTC threshold Object in path at third TTC threshold No object in path
Vehicle speed	Vehicle speed above minimum threshold Vehicle speed at minimum threshold Vehicle speed below minimum threshold
Driver braking input	Brake input from driver controls No brake input from driver controls
Driver propulsion input	Propulsion input from driver controls No propulsion input from driver controls
Request zero propulsion torque	
Distance to object	Object in path at first TTC threshold Object in path at second TTC threshold Object in path at third TTC threshold No object in path
Vehicle speed	Vehicle speed above minimum threshold Vehicle speed at minimum threshold Vehicle speed below minimum threshold
Driver braking input	Brake input from driver controls No brake input from driver controls
Driver propulsion input	Propulsion input from driver controls No propulsion input from driver controls
Pre-charge brakes	
Distance to object	Object in path at first TTC threshold Object in path at second TTC threshold Object in path at third TTC threshold No object in path
Vehicle speed	Vehicle speed above minimum threshold Vehicle speed at minimum threshold Vehicle speed below minimum threshold
Driver braking input	Brake input from driver controls No brake input from driver controls
Engage/disengage feature	
Driver request	Driver activates feature Driver deactivates feature
Issue driver warning via HMI	
System status	Feature available Feature not available

Docking

Request clockwise/counterclockwise steering	
Driver-specified distance from curb	Vehicle is further from curb than driver-specified distance Vehicle is at driver-specified distance from curb Vehicle is closer to curb than driver-specified distance
Vehicle alignment with curb	Vehicle alignment is toward curb Vehicle is aligned parallel to curb Vehicle alignment is away from curb
Driver steering input	Driver steering input in clockwise direction Driver steering input in counterclockwise direction No driver steering input
Request suspension of other lane guidance systems	
Docking system status	Docking system engaged Docking system disengaged
Engage/disengage feature	
Driver request	Driver activates feature Driver deactivates feature
Issue driver warning via HMI	
System status	Feature available Feature not available

Full Park Assist and Yard Park

Request clockwise/counterclockwise steering	
Lateral trajectory computed by system	Trajectory curves to left Trajectory is straight Trajectory curves to right
Longitudinal trajectory computed by system	Trajectory is ahead of vehicle Trajectory is behind vehicle
Request an increase/decrease in braking	
Object presence	Object in vehicle path within specified distance Object in vehicle path outside specified distance No object in vehicle path
Longitudinal trajectory computed by system	Trajectory requires speed increase Trajectory requires constant speed Trajectory requires speed decrease
Request an increase/decrease in propulsion	
Object presence	Object in vehicle path within specified distance Object in vehicle path outside specified distance No object in vehicle path
Longitudinal trajectory computed by system	Trajectory requires speed increase Trajectory requires constant speed Trajectory requires speed decrease
Request transmission to shift to park/reverse/drive	
Location relative to designated parking spot	Vehicle within designated parking spot Vehicle not within designated sparking spot
Vehicle speed	Vehicle speed is zero Vehicle speed is above zero

Longitudinal trajectory computed by system	Trajectory is ahead of vehicle Trajectory is behind vehicle
Engage/disengage feature	
Driver request	Driver activates feature Driver deactivates feature
Issue driver warning via HMI	
System status	Feature available Feature not available

Lane Keeping, Lane Centering, and Steering Assist

Request clockwise/counterclockwise steering	
Location relative to lane center	Vehicle lateral position is at lane center Vehicle lateral position is offset to right of lane center Vehicle lateral position is offset to left of lane center
Driver steering input	Driver steering input in clockwise direction Driver steering input in counterclockwise direction No driver steering input
Engage/disengage feature	
Driver request	Driver activates feature Driver deactivates feature
Issue driver warning via HMI	
System status	Feature available Feature not available

Object Detection and Collision Warning Alert

Provide object data to other systems	
Object location	Object present in front of vehicle Object present to front-right of vehicle Object present to front-left of vehicle Object present to right of vehicle Object present to left of vehicle Object present to rear of vehicle Object present to rear-right of vehicle Object present to rear-left of vehicle No object present within specified distance of vehicle
Issue driver warning via HMI	
System status	Feature available Feature not available
Object location	Object present in front of vehicle Object present to front-right of vehicle Object present to front-left of vehicle Object present to right of vehicle Object present to left of vehicle Object present to rear of vehicle Object present to rear-right of vehicle Object present to rear-left of vehicle No object present within specified distance of vehicle

Park Assist, Park Out, and Yard Park

Request clockwise/counterclockwise steering	
Lateral trajectory computed by system	Trajectory curves to left Trajectory is straight Trajectory curves to right
Longitudinal trajectory computed by system	Trajectory is ahead of vehicle Trajectory is behind vehicle
Driver steering input	Driver steering input in clockwise direction Driver steering input in counterclockwise direction No driver steering input
Engage/disengage feature	
Driver request	Driver activates feature Driver deactivates feature
Issue driver warning via HMI	
System status	Feature available Feature not available

Reverse Brake Assist

Increase/decrease brake torque	
Transmission position	Transmission is in park Transmission is in reverse Transmission is in neutral Transmission is in drive/low
Distance to object	Object in path at first TTC threshold Object in path at second TTC threshold Object in path at third TTC threshold No object in path
Vehicle speed	Vehicle speed above minimum threshold Vehicle speed at minimum threshold Vehicle speed below minimum threshold
Driver braking input	Brake input from driver controls No brake input from driver controls
Driver propulsion input	Propulsion input from driver controls No propulsion input from driver controls
Request zero propulsion torque	
Transmission position	Transmission is in park Transmission is in reverse Transmission is in neutral Transmission is in drive/low
Distance to object	Object in path at first TTC threshold Object in path at second TTC threshold Object in path at third TTC threshold No object in path
Vehicle speed	Vehicle speed above minimum threshold Vehicle speed at minimum threshold Vehicle speed below minimum threshold
Driver braking input	Brake input from driver controls No brake input from driver controls

Driver propulsion input	Propulsion input from driver controls No propulsion input from driver controls
Engage/disengage feature	
Driver request	Driver activates feature Driver deactivates feature
Issue driver warning via HMI	
System status	Feature available Feature not available

Traffic Jam Assist with Lane Keeping/ Lane Centering

Request clockwise/counterclockwise steering	
Location relative to lane center	Vehicle lateral position is at lane center Vehicle lateral position is offset to right of lane center Vehicle lateral position is offset to left of lane center
Vehicle operating speed	Vehicle speed above maximum operating speed Vehicle speed at maximum operating speed Vehicle speed below maximum operating speed
Driver steering input	Driver steering input in clockwise direction Driver steering input in counterclockwise direction No driver steering input
Request an increase/decrease in propulsion torque	
Driver's distance set point	Gap with lead vehicle above set point Gap with lead vehicle at set point Gap with lead vehicle below set point
Vehicle operating speed	Vehicle speed above maximum operating speed Vehicle speed at maximum operating speed Vehicle speed below maximum operating speed
Driver's speed set point	Vehicle speed below set point Vehicle speed at set point Vehicle speed above set point
Passenger door status	Door status is open Door status is closed
Lift system status	Lift system is stowed Lift system is deployed
Bus height status	Bus is kneeling Bus is at full height
Request an increase/decrease in brake torque	
Driver's distance set point	Gap with lead vehicle above set point Gap with lead vehicle at set point Gap with lead vehicle below set point
Vehicle operating speed	Vehicle speed above maximum operating speed Vehicle speed at maximum operating speed Vehicle speed below maximum operating speed
Driver's speed set point	Vehicle speed below set point Vehicle speed at set point Vehicle speed above set point

Engage/disengage parking brake	
Bus motion	Host vehicle stopped Host vehicle moving
Lead vehicle motion	Lead vehicle stopped Lead vehicle moving
Brake status	Service brake engaged Service brake disengaged
Engine start/stop	
Bus motion	Host vehicle stopped Host vehicle moving
Lead vehicle motion	Lead vehicle stopped Lead vehicle moving
Engage/disengage feature	
Driver request	Driver activates feature Driver deactivates feature
Vehicle operating speed	Vehicle speed above maximum operating speed Vehicle speed at maximum operating speed Vehicle speed below maximum operating speed
Issue driver warning via HMI	
System status	Feature available Feature not available

APPENDIX

C

Potential Vehicle-Level Hazards

This study identified 18 vehicle-level hazards as shown in Table C-1. The identified ASILs for each hazard, based on the applicable system, are also shown in Table C-1. Note that some hazards were not applicable to certain systems; these are designated in the table as "N/A."

Table C-1 *Identified ASILs for Each Potential Vehicle-level Hazard by System*

	Potential Vehicle-Level Hazard	ACC	AEB	Dock	FPA	LK/ LC	ODCA	PA	RBA	TJA
H1	Excessive vehicle propulsion	C	N/A	N/A	A	N/A	N/A	N/A	N/A	C
H2	Insufficient vehicle propulsion	QM	A	N/A	QM	N/A	N/A	N/A	QM	A
H3	Loss of vehicle propulsion	B	B	N/A	QM	N/A	N/A	N/A	QM	QM
H4	Vehicle movement in the wrong longitudinal direction	A	N/A	N/A	A	N/A	N/A	N/A	N/A	A
H5	Excessive vehicle deceleration or braking	C	C	N/A	QM	N/A	N/A	N/A	A	A
H6	Insufficient vehicle deceleration or braking	B	B	N/A	A	N/A	N/A	N/A	QM	QM
H7	Loss of vehicle deceleration or braking	C	C	N/A	A	N/A	N/A	N/A	A	B
H8	Vehicle rollaway	QM	N/A	N/A	QM	N/A	N/A	N/A	N/A	QM
H9	Excessive lateral motion/yaw	N/A	N/A	B	A	C	N/A	A	N/A	B
H10	Insufficient lateral motion/yaw	N/A	N/A	B	A	C	N/A	A	N/A	B
H11	Vehicle movement in the wrong lateral direction	N/A	N/A	C	A	C	N/A	A	N/A	C
H12	Excessive vehicle roll	N/A	N/A	N/A	N/A	B	N/A	N/A	N/A	N/A
H13	Vehicle motion when passenger door is open	A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	A
H14	Vehicle too far from curb at bus station/stop	N/A	N/A	A	N/A	N/A	N/A	N/A	N/A	N/A
H15	Lane/roadway departure while system is engaged	N/A	N/A	N/A	N/A	C	N/A	N/A	N/A	C
H16	Inadequate alerting of driver	N/A	QM	N/A	QM	N/A	QM	N/A	QM	N/A
H17	Improper transition of control between the driver and driving automation system	A	A	A	A	A	N/A	A	QM	A
H18	Improper transition of control between vehicle systems	N/A	N/A	QM	N/A	N/A	N/A	N/A	QM	N/A

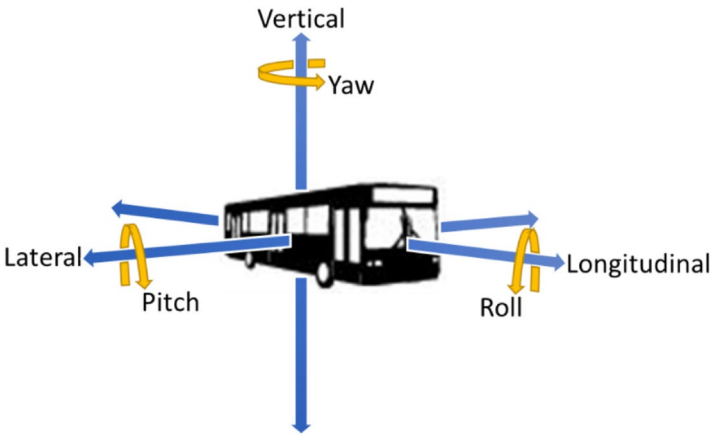
N/A = Hazard was not identified for the associated system
ASIL A = least stringent
ASIL D = most stringent
Dock = Docking system
FPA = Full park assist and valet parking system
LK/LC = Lake keeping, lane centering, and steering assist system
PA = Park assist, park out, and yard park system

Motion-Related Hazards

In general, motion-related hazards are derived from the six degrees of freedom, as shown in Figure C-1. This category of vehicle-level hazards is consistent with the types of hazards described in SAE Recommended Practice J2980 [9]. Two of the degrees of freedom—motion along the vertical axis and pitch (rotation around the lateral axis)—were not relevant to this study.

Figure C-1

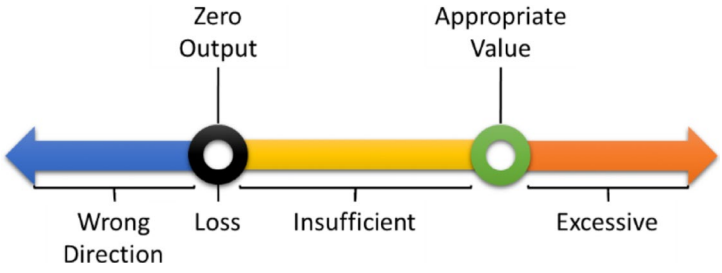
Six degrees of freedom for vehicle motion



The motion-related hazards can further be described in relation to a reference point, as shown in Figure C-2. The reference point is the "appropriate" or "correct" amount of motion required from either from the driving automation system or the human driver to maintain the safety of the vehicle. For instance, when ACC is engaged, the appropriate amount of longitudinal motion would maintain the gap between the bus and the lead vehicle while maintaining the bus speed at or below the levels set by the driver. However, a malfunction might result in the ACC system requesting more propulsion than necessary to achieve this goal (i.e., excessive propulsion).

Figure C-2

Depiction of different motion-related hazards relative to reference point



The motion-related hazards are described in more detail below.

Longitudinal-related Hazards

Longitudinal-related hazards describe hazards related to the bus's longitudinal axis of motion, as shown in Figure C-2. These hazards typically are associated with bus's propulsion or braking systems. This study identified eight longitudinal-related hazards:

- **Excessive vehicle propulsion** encompasses any situation in which the amount of propulsion exceeds the appropriate value, including situations in which the appropriate value may be zero propulsion. For example, the ACC system may request more propulsion than needed to maintain the gap with the lead vehicle.
- **Insufficient vehicle propulsion** encompasses any situation in which propulsion is provided, but at a value below the appropriate value (i.e., the vehicle does not accelerate enough). For example, the ACC system might only request a fraction of the propulsion required to bring the vehicle back to the driver's selected speed set point.
- **Loss of vehicle propulsion** encompasses any situation in which propulsion is reduced to levels between zero and the idle creep speed[23] but the appropriate value for propulsion is higher. For example, a failure in the ACC system might prevent the system from requesting propulsion while the vehicle is travelling at city speeds.
- **Vehicle movement in the wrong longitudinal direction** encompasses any situation in which propulsion is provided in the opposite direction of the appropriate direction of motion (e.g., the vehicle moves in reverse instead of forward). This may be the result of an incorrect transmission position (e.g., reverse instead of drive) or incorrect execution of a command by an electric powertrain.
- **Excessive vehicle deceleration or braking** encompasses any situation in which the vehicle decelerates by an amount that exceeds the appropriate value, including situations in which the appropriate value may be zero braking. For example, the AEB system may request braking when there are no objects in the vehicle's path.
- **Insufficient vehicle deceleration or braking** encompasses any situation in which the vehicle decelerates but at a level that is below the appropriate value (i.e., the vehicle does not decelerate enough). For example, the ACC system might request reduced propulsion in response to the lead vehicle slowing, but the propulsion may not be reduced enough.
- **Loss of vehicle deceleration or braking** describes any situation in which no deceleration or braking is provided but some level of deceleration or braking is appropriate. For example, a failure in the AEB system may prevent the AEB system from issuing a braking request to the braking system.
- **Vehicle rollaway** describes any situation in which the vehicle begins moving from a stopped position as a result of gravitational forces or from idle creep speed. For example, a full park assist/valet park system may not correctly shift the vehicle into "park" at the end of the maneuver, allowing the vehicle to begin rolling away.

[23] Idle creep speed is the low-level speed that results from engine idling while the transmission is still engaged.

Lateral- and Yaw-related Hazards

Lateral- and yaw-related hazards typically are associated with the bus's steering system. The steering system is responsible for both producing lateral acceleration (related to the bus's lateral axis of motion, as shown in Figure C-1, and changing the vehicle heading by changing the yaw rate (related to the rotation around the bus's vertical axis of motion, as shown in Figure C-1). This study identified three lateral- and yaw-related hazards.

- **Excessive lateral motion/yaw** describes any situation in which the vehicle turns or moves laterally by an amount that exceeds the appropriate value, including situations in which the vehicle turns or moves laterally when it should be going straight (i.e., zero steering). For example, the lane centering system may request steering when the bus is already centered in the lane.
- **Insufficient lateral motion/yaw** describes any situation in which the vehicle turns or moves laterally but at a level that is below the appropriate value. For example, the lane centering system might not request sufficient steering to maintain the vehicle within the lane on a curved roadway.
- **Vehicle movement in the wrong lateral direction** describes any situation in which the steering is in the opposite direction of the appropriate steering direction. For example, the lane keeping/lane centering system may request steering in the clockwise direction when the roadway curves to the left (i.e., counterclockwise steering is appropriate).

Roll-related Hazards

Roll-related hazards typically are associated with rotation around the bus's longitudinal axis, as shown in Figure C-1. This may result from a build-up of lateral forces—for instance, as a result of steering and counter-steering actions or from large steering forces at higher vehicle speeds. Since transit buses have a higher center of gravity than light vehicles, they may be more susceptible to roll incidents.

- **Excessive vehicle roll** describes any situation in which the vehicle roll exceeds the appropriate value needed to maintain vehicle stability and avoid rollover.[24]

Mission-related Hazards

The second category of identified hazards is mission-related hazards, which refer to the safety-relevant functions of a system and identify potentially unsafe system states that may arise if the system does not satisfy the relevant mission

[24] Vehicle rollovers are complex and may result from a number of factors, including vehicle type, speed, steering maneuvers (e.g., steer/counter-steer), or tripping forces [22]. For transit buses, additional factors may include bus configuration (e.g., body type, center of gravity, wheel base) as well as variations due to operation, such as loading.

requirements. Unlike motion-related hazards, mission-related hazards are not defined relative to an appropriate quantitative value; rather, they result from failure to fully and successfully complete complex maneuvers or interactions such as steering the bus into a bus stop.[25]

- **Vehicle motion while passenger door is open** describes conditions in which the driving automation system moves the vehicle from a stop while the door is still open or fails to bring the vehicle to a stop if the passenger door opens inadvertently, increasing the risk of passengers being injured during embarkation or disembarkation. For example, if a passenger requests an unplanned stop when the ACC stop-and-go feature has stopped the bus, the ACC stop-and-go feature might inappropriately accelerate the bus if the lead vehicle moves regardless of whether the door has been closed.
- **Vehicle too far from curb at bus stop** describes a situation in which the bus does not stop close enough to the curb to safely disembark passengers, particularly passengers that may have mobility limitations. The docking maneuver includes multiple steering maneuvers to bring the bus into the designated location. It may be difficult to characterize individual maneuvers with hazards such as excessive or insufficient lateral motion/yaw, since these may be compensated for by subsequent maneuvers; rather, the final positioning of the bus relative to the stop is what may create a hazard.
- **Lane or roadway departure while system is engaged** describes a situation in which the bus moves out of the desired travel lane or off the roadway when a lane guidance feature is supposed to be keeping the bus within that travel lane. Lane keeping, lane centering, and steering assist systems may be designed to provide varying levels of control. For example, some systems allow the vehicle to drift away from the center of the lane and only provide intervention as the vehicle approaches the lane boundary. This may make it difficult to characterize hazardous behavior for some systems as strictly excessive or insufficient lateral motion or yaw.

Control-related Hazards

Control-related hazards are particularly relevant to driving automation systems that may receive multiple control commands. Level 1 to Level 3 driving automation systems may be subject to potential conflict resulting from transition of control between the operator and the automation system. Two control-related hazards result from human factor issues that are considered outside the scope of ISO 26262; however, these hazards are included in this study for completeness:

- **Inadequate alerting of the driver** results when the system does not provide a necessary alert to the driver about surrounding vehicles or objects. For this hazard to apply, a system function must be to alert the driver to

[25] In contrast, an ACC system violating the gap between the bus and a lead vehicle could be more simply described with hazards such as excessive propulsion or insufficient deceleration.

threats—for instance, the object detection and collision avoidance system may fail to alert the driver of an object ahead of the bus. This hazard does not include notifications of system availability.[26]

- **Improper transition of control between the driver and driving automation system** results when either the driving automation system or human driver has an incorrect understanding of which entity is performing the motion control subtasks of the dynamic driving task. For instance, a driving automation system may not suspend operation or relinquish control to the human driver when the driver provides a countermanding steering input.[27]
- **Improper transition of control between vehicle systems** results from incorrect transition of control authority from one driving automation system to a different driving automation system. For example, when the docking system engages, the lane centering system should be suspended to allow the bus to get close enough to the curb. This hazard may also result from incorrect application of the vehicle's system arbitration strategy.

[26] Failure to notify the driver if a system becomes unavailable may be better described by the hazard "improper transition of control between the driver and driving automation system" since the purpose of this notification is to ensure the driver resumes control of the vehicle.

[27] Some driving automation systems may be designed to disengage when the driver provides a control input. Other driving automation systems may be designed to only suspend operation when the driver provides a control input; the system resumes operation once the driver stops providing a control input.

APPENDIX

D

ASIL Determination Matrix

Table D-1 *ASIL Determination Matrix from ISO 26262*

Severity Class	Probability Class (Exposure)	Controllability Class		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

QM = Quality Management
ASIL A = least stringent
ASIL D = most stringent
E = Exposure
S = Severity
C = Controllability

APPENDIX

E

Allocation of Driving Automation Systems to Identified Transit Bus Use Cases

FTA's *Transit Bus Automation: Technology Packages and Use Cases* identifies potential top-level use cases for advanced driver assistance systems[28] in transit buses [11]. In a separate document, Transferability of Automation Technologies, FTA identifies 13 light vehicle driving automation systems that could potentially be deployed in transit buses [1]. The transit bus use cases identified in *Technology Packages and Use Cases* can be implemented through combinations of the driving automation system technologies identified in the *Transferability of Automation Technologies* study. The matrix in Table E-1 represents one such approach for allocating specific driving automation systems to seven relevant top-level use cases.

Table E-1 *Allocation of Driving Assistance Systems to Top-level Use Cases*

	Smooth Acceleration and Deceleration	Automatic Emergency Braking and Collision Avoidance	Curb Avoidance	Precision Docking	Narrow Lane/Shoulder Operations	Platooning	Automated Parking Operations
Adaptive Cruise Control with/without Stop-and-Go	●	x	x	x	x	●	x
Automatic Emergency Braking	x	●	x	x	x	●	●
Docking	x	x	●	●	x	x	x
Full Park Assist/ Valet Parking (Bus Yard)	x	x	x	x	x	x	●
Lane Keeping/ Lane Centering/ Steering Assist	x	x	●	○	●	●	x
Object Detection and Collision Avoidance Alerts	x	●	x	x	x	x	●
Park Assist/ Park Out/ Yard Park	x	x	x	x	x	x	●
Reverse Brake Assist	x	●	x	x	x	x	●
TJA with Lane Keeping/ Lane Centering	●	x	●	x	●	●	x

● = *Potentially supports use case*
○ = *Potentially supports use case but may require modification or may depend on use case implementation*
x = *Not applicable to use case*

[28] Advanced driver assistance systems typically operate at Level 1 or 2 automation, as defined in SAE International Recommended Practice J3016 [17].

APPENDIX

F

Detailed Operational Scenario Framework

Table F-1 *Transit Bus Use Case Parameters for Risk Assessment*

Use Case	Detailed Category	Parameters for Risk Assessment
Smooth Acceleration and Deceleration	Vehicle Speed (Forward)	0–5 mph, 5–15 mph, 15–30 mph, over 30 mph
	Traffic Conditions	Light traffic, Heavy traffic
	VRU Traffic	Light VRU traffic, heavy VRU traffic, VRUs with unconventional behavior
	Road Geometry	Straight to moderate curvature, sharp curvature, level to low grade, moderate to steep grade
	Road Conditions	Slippery, moderate to good road conditions
	Road Types	City, expressway, dedicated bus lanes
	Weather Conditions	Rain/snow/ice, fog/smoke/particulates/ precipitation, sunny/overcast
	Ambient Conditions	Low lighting, good lighting
	Bus Passenger State	Seated and buckled, seated and unbuckled, standing
	Bus Loading	Light, heavy, unstowed objects (e.g., luggage, bags)
Automatic Emergency Braking and Collision Avoidance	Vehicle Speed (Forward)	5–15 mph, 15–30 mph, over 30 mph
	Vehicle Speed (Reverse)	0–5 mph, 5–15 mph
	Traffic Conditions	Light traffic, heavy traffic
	VRU Traffic	Light VRU traffic, heavy VRU traffic, VRUs with unconventional behavior
	Road Geometry	Straight to moderate curvature, sharp curvature, level to low grade, moderate to steep grade
	Road Conditions	Slippery, moderate to good road conditions
	Road Types	City, expressway, dedicated bus lanes
	Weather Conditions	Rain/snow/ice, fog/smoke/particulates/ precipitation, sunny/overcast
	Ambient Conditions	Low lighting, good lighting
	Bus Passenger State	Seated and buckled, seated and unbuckled, standing
	Bus Loading	Light, heavy, un-stowed objects (e.g., luggage, bags)
Curb Avoidance	Vehicle Speed (Forward)	0–5 mph, 5–15 mph, 15–30 mph, over 30 mph
	Road Geometry	Straight to moderate curvature, sharp curvature, level to low grade, moderate to steep grade
	Road Conditions	Slippery, moderate to good road conditions
	Road Types	City, expressway, dedicated bus lanes
	Weather Conditions	Rain/snow/ice, fog/smoke/particulates/ precipitation, sunny/overcast
	Ambient Conditions	Low lighting, good lighting
	Bus Stop Location	On a curve, on a grade, along a straight road
	Bus Passenger State	Seated and buckled, seated and unbuckled, standing
	Bus Loading	Light, heavy, unstowed objects (e.g., luggage, bags)

Use Case	Detailed Category	Parameters for Risk Assessment
Precision Docking	Vehicle Speed (Forward)	0–5 mph, 5–15 mph, 15–30 mph
	Traffic Conditions	Light traffic, heavy traffic
	VRU Traffic	Light VRU traffic, heavy VRU traffic, VRUs with unconventional behavior
	Road Geometry	Straight to moderate curvature, sharp curvature, level to low grade, moderate to steep grade
	Road Conditions	Slippery, moderate to good road conditions
	Road Types	City, expressway, dedicated bus lanes
	Weather Conditions	Rain/snow/ice, fog/smoke/particulates/ precipitation, sunny/overcast
	Ambient Conditions	Low lighting, good lighting
	Bus Stop Location	On a curve, on a grade, along a straight road
	Bus Passenger State	Seated and buckled, seated and unbuckled, standing
	Bus Loading	Light, heavy, un-stowed objects (e.g., luggage, bags)
Narrow Lane/ Shoulder Operations	Vehicle Speed (Forward)	0–5 mph, 5–15 mph, 15–30 mph, over 30 mph
	Traffic Conditions	Light traffic, heavy traffic
	VRU Traffic	Light VRU traffic, heavy VRU traffic, VRUs with unconventional behavior
	Road Geometry	Straight to moderate curvature, sharp curvature, level to low grade, moderate to steep grade
	Road Conditions	Slippery, moderate to good road conditions
	Road Types	City, expressway, dedicated bus lanes
	Weather Conditions	Rain/snow/ice, fog/smoke/particulates/ precipitation, sunny/overcast
	Ambient Conditions	Low lighting, good lighting
	Bus Passenger State	Seated and buckled, seated and unbuckled, standing
	Bus Loading	Light, heavy, un-stowed objects (e.g., luggage, bags)
Platooning	Vehicle Speed (Forward)	0–5 mph, 5–15 mph, 15–30 mph, over 30 mph
	Traffic Conditions	Light traffic, heavy traffic
	VRU Traffic	Light VRU traffic, heavy VRU traffic, VRUs with unconventional behavior
	Road Geometry	Straight to moderate curvature, sharp curvature, level to low grade, moderate to steep grade
	Road Conditions	Slippery, moderate to good road conditions
	Road Types	City, expressway, dedicated bus lanes
	Weather Conditions	Rain/snow/ice, fog/smoke/particulates/ precipitation, sunny/overcast
	Ambient Conditions	Low lighting, good lighting
	Bus Passenger State	Seated and buckled, seated and unbuckled, standing
	Bus Loading	Light, heavy, unstowed objects (e.g., luggage, bags)

Use Case	Detailed Category	Parameters for Risk Assessment
Bus Yard and Parking Operations	Vehicle Speed (Forward)	0–5 mph, 5–15 mph
	Vehicle Speed (Reverse)	0–5 mph, 5–15 mph
	Traffic Conditions	Light traffic, heavy traffic
	VRU Traffic	Light VRU traffic, heavy VRU traffic, VRUs with unconventional behavior
	Road Conditions	Slippery, moderate to good road conditions
	Weather Conditions	Rain/snow/ice, fog/smoke/particulates/ precipitation, sunny/overcast
	Ambient Conditions	Low lighting, good lighting
	Parking Facility Characteristics	Lined parking spots, unlined parking spots, fencing

APPENDIX

G

Safety Goals by System

This study identified 21 safety goals, as shown in Table G-1. The identified ASILs for each safety goal, based on the applicable system, are also shown in Table G-1. Note that some safety goals were not applicable to certain systems; these are designated in the table as "N/A."

Table G-1 *Identified Safety Goals and Associated ASILs by System*

Assoc. Hazard	Top-Level Safety Goal	ACC	AEB	Dock	FPA	LK/LC	ODCA	PA	RBA	TJA
H1	Prevent excessive vehicle propulsion*under all vehicle operating conditions.	C	N/A	N/A	A	N/A	N/A	N/A	N/A	C
H2	Ensure that the system provides the correct level of propulsion.	QM	A	N/A	QM	N/A	N/A	N/A	QM	A
H3	Prevent the stop-and-go subsystem from shutting off the engine while the vehicle is in motion.	B	N/A	N/A	N/A	N/A	N/A	N/A	N/A	QM
H3	Prevent the system from requesting unintended zero propulsion torque.	N/A	B	N/A	QM	N/A	N/A	N/A	QM	N/A
H4	Ensure that vehicle motion occurs in the intended longitudinal direction.	A	N/A	N/A	A	N/A	N/A	N/A	N/A	A
H5	Prevent excessive vehicle deceleration† or braking under all operating conditions.	C	C	N/A	QM	N/A	N/A	N/A	A	A
H6	Ensure that the system provides the correct level of deceleration or braking.	B	B	N/A	A	N/A	N/A	N/A	QM	QM
H7	Prevent loss of vehicle deceleration or braking.	C	C	N/A	A	N/A	N/A	N/A	A	B
H8	Prevent vehicle rollaway under all operating conditions.	QM	N/A	N/A	QM	N/A	N/A	N/A	N/A	QM
H8	Prevent unintended vehicle motion under all operating conditions.	QM	N/A	N/A	QM	N/A	N/A	N/A	N/A	QM
H9	Prevent excessive lateral motion/yaw.	N/A	N/A	B	A	C	N/A	A	N/A	B
H10	Ensure that the system provides the correct level of lateral motion/yaw.	N/A	N/A	B	A	C	N/A	A	N/A	B
H11	Ensure that lateral motion/yaw is provided in the correct direction.	N/A	N/A	C	A	C	N/A	A	N/A	C
H12	Prevent excessive vehicle roll‡ resulting from steering maneuvers.	N/A	N/A	N/A	N/A	B	N/A	N/A	N/A	N/A
H13	Prevent continued vehicle motion while the passenger door is open.	A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	A
H14	Ensure that the vehicle stops at the driver-specified distance from the curb at a bus station/stop.	N/A	N/A	A	N/A	N/A	N/A	N/A	N/A	N/A
H15	Prevent a lane or roadway departure while the system is engaged.	N/A	N/A	N/A	N/A	C	N/A	N/A	N/A	C
H16	Ensure that the system issues driver alerts.	N/A	QM	N/A	QM	N/A	QM	N/A	QM	N/A
H17	Ensure that the system status is properly conveyed to the driver.	QM	QM	QM	QM	A	N/A	QM	QM	A
H17	Ensure that the driver is capable of overriding the system.	A	A	A	A	A	N/A	A	A	A
H18	Ensure that the system communicates its operational status to other vehicle systems (e.g., lane keeping, lane centering, or steering assist).	N/A	N/A	QM	N/A	N/A	N/A	N/A	N/A	N/A

**Excessive vehicle propulsion is TBD m/s^2 above the design intent.*
† Excessive vehicle deceleration is TBD m/s^2 above the design intent.
‡ Excessive vehicle roll is defined as TBD above the design intent and can be determined based on conditions that increase the risk of rollover
N/A = Hazard was not identified for the associated system.
ASIL A = least stringent
ASIL D = most stringent
Dock. = Docking system
FPA = Full park assist and valet parking system
LK/LC = Lake keeping, lane centering, and steering assist system
PA = Park assist, park out, and yard park system

Adaptive Cruise Control

Safety Goal, Adaptive Cruise Control–1

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to excessive vehicle propulsion in the ACC system. For example, excessive vehicle propulsion may occur from failures that cause the ACC system to command more propulsion, when instead the bus should be slowing down.

- Prevent excessive vehicle propulsion under all vehicle operating conditions through design and validation techniques in accordance with the ASIL C classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification below may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the ACC system commanding excessive vehicle propulsion. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the ACC system commanding excessive vehicle propulsion cannot be prevented (i.e., eliminated), then detect and mitigate the faults.
- When the ACC system is active, prevent all faults that increase propulsion torque when additional propulsion is not requested by the driver, the ACC system, or higher priority safety systems.
- Prevent unintended activation of the ACC system.
- Ensure that the validity and correctness of signals provided by the environmental sensors and other critical sensors for the ACC system.
- Ensure that the validity and correctness of communication signals from other vehicle systems to the ACC system.
- If a failure that could lead to excessive vehicle propulsion occurs, transition into a safe state within the FTTI.[29]
- If a failure that could lead to excessive vehicle propulsion occurs, warn the driver and communicate any necessary actions to the driver (e.g., manually disengage the system).

[29] FTTI is the minimum time span from the occurrence of a fault in a system to a possible occurrence of a hazardous event, if safety mechanisms are not activated [I].

- Ensure that the acceleration resulting from failures[30] does not exceed TBD m/s^2. The allowable acceleration should be determined so that it does not cause displacement of unsecured standing or seated passengers, or displacement of objects in a way that could cause harm to the passengers or driver.

Safety Goal, Adaptive Cruise Control–2

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to insufficient vehicle propulsion from the ACC system. For example, insufficient vehicle propulsion could result from failures that cause the ACC system to command less propulsion than needed to match the speed of surrounding traffic.

- Ensure that the system provides the correct level of propulsion through design and validation techniques in accordance with the QM[31] classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the ACC system commanding insufficient vehicle propulsion. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the ACC system commanding insufficient vehicle propulsion cannot be prevented (i.e., eliminated), then detect and mitigate the fault.
- Ensure the validity and correctness of signals provided by the environmental sensors and other critical sensors for the ACC system.
- Acknowledge all faults communicated by other vehicle systems that may prevent the vehicle from achieving the intended increase in speed, including faults communicated by the powertrain system.
- If a failure that could lead to insufficient vehicle propulsion occurs, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.

[30] Establishing an acceptable acceleration rate for nominal system performance that ensures the safety of passengers and the driver would be part of the system design and would not be covered by ISO 26262.

[31] Note that safety goals assigned "QM" typically are not shown in the functional safety concept, as internal quality management processes rather than ISO 26262 concepts apply to these safety goals. However, in this study, these safety goals are shown for completeness.

- If a failure that could lead to insufficient vehicle propulsion occurs, warn the driver and communicate any necessary actions to the driver (e.g., manually disengage the system).

Safety Goal, Adaptive Cruise Control–3

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to loss of vehicle propulsion when the ACC system is active. For example, loss of vehicle propulsion may result from failures that cause the stop-and-go system to shut off the engine while the vehicle is moving at higher speeds.

- Prevent the stop-and-go subsystem from shutting off the engine while the vehicle is in motion through design and validation techniques in accordance with the ASIL B classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the ACC system shutting off the engine while the vehicle is in motion. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the ACC system shutting off the engine while the vehicle is in motion cannot be prevented, then detect and mitigate the fault.
- Ensure the validity and correctness of signals provided by the environmental sensors and other critical sensors for the ACC system.
- Acknowledge all faults communicated by other vehicle systems that may cause propulsion loss, including faults communicated by the powertrain system.
- If a failure that could lead to loss of vehicle propulsion occurs, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.
- If a failure that could lead to loss of vehicle propulsion occurs, warn the driver and communicate any necessary actions to the driver (e.g., manually disengage the system).

Safety Goal, Adaptive Cruise Control–4

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to the ACC system commanding vehicle movement in the wrong longitudinal direction. This safety goal is applicable only for ACC systems with the stop-and-go feature equipped on buses with electric powertrains. For example, a failure may cause the electric powertrain system to incorrectly execute the ACC system commands in the reverse direction.

- Ensure that vehicle motion occurs in the intended longitudinal direction through design and validation techniques in accordance with the ASIL A classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Acknowledge all faults communicated by other vehicle systems that may cause the vehicle to move in the wrong longitudinal direction, including faults communicated by the powertrain system.
- Prevent propulsion commands from the ACC system when the transmission is in a position other than drive.
- If a failure that could lead to vehicle movement in the wrong direction occurs, transition into a safe state within the FTTI.
- If a failure that could lead to vehicle movement in the wrong direction occurs, warn the driver and communicate any necessary actions to the driver (e.g., apply the brakes).

Safety Goal, Adaptive Cruise Control–5

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to excessive vehicle deceleration or braking by the ACC system. For example, a failure may cause the ACC system to decelerate the bus more than necessary when the vehicle ahead of the bus slows down.

- Prevent excessive vehicle deceleration or braking under all operating conditions through design and validation techniques in accordance with the ASIL C classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the ACC system commanding excessive vehicle deceleration or braking. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the ACC system commanding excessive vehicle deceleration or braking cannot be prevented, then detect and mitigate the fault.
- Prevent unintended activation of the ACC system.
- Ensure the validity and correctness of signals provided by the environmental sensors and other critical sensors for the ACC system.
- Ensure the validity and correctness of communication signals from other vehicle systems to the ACC system.
- When the ACC system is active, prevent all faults that cause deceleration or braking when deceleration is not requested by either the driver, the ACC system, or higher priority safety systems.
- Ensure that the vehicle speed is at zero before shutting off the engine.
- If a failure that could lead to excessive vehicle deceleration or braking occurs, transition into a safe state within the FTTI.
- If a failure that could lead to excessive vehicle deceleration or braking occurs, warn the driver and communicate any necessary actions to the driver (e.g., manually disengage the system).
- Ensure that deceleration resulting from failures[32] does not exceed TBD m/s^2. The allowable deceleration should be determined so that it does not cause displacement of unsecured standing or seated passengers, or the displacement of objects in a way that could cause harm to the passengers or driver.

Safety Goal, Adaptive Cruise Control–6

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to insufficient vehicle deceleration or braking by the ACC system. For example, a failure may cause the ACC system to command less braking than necessary when the lead vehicle slows down.

[32] Establishing an acceptable deceleration rate for nominal system performance that ensures the safety of passengers and the driver would be part of the system design and would not be covered by ISO 26262.

- Ensure that the system provides the correct level of deceleration or braking through design and validation techniques in accordance with the ASIL B classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the ACC system commanding insufficient vehicle deceleration or braking. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the ACC system commanding insufficient vehicle deceleration or braking cannot be prevented, then detect and mitigate the fault.
- Ensure the validity and correctness of signals provided by the environmental sensors and other critical sensors for the ACC system.
- Acknowledge all faults communicated by other vehicle systems that may prevent the vehicle from achieving the intended decrease in speed, including faults communicated by the powertrain system or the braking system.
- If a failure that could lead to insufficient vehicle deceleration or braking occurs, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.
- If a failure that could lead to insufficient vehicle deceleration or braking occurs, warn the driver and communicate any necessary actions to the driver (e.g., apply the brakes).

Safety Goal, Adaptive Cruise Control–7

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could prevent the ACC system from stopping the bus when at zero speed. For example, a failure in the stop-and-go subsystem may cause a delay in shutting off the engine when the bus is stopped.

- Prevent loss of vehicle deceleration or braking through design and validation techniques in accordance with the ASIL C classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the ACC system incorrectly stopping the engine or inadvertently restarting the engine when the vehicle is stopped. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the ACC system commanding insufficient vehicle deceleration or braking cannot be prevented, then detect and mitigate the fault.
- Acknowledge all faults communicated by other vehicle systems that may prevent the vehicle from properly stopping the engine, including faults communicated by the powertrain system.
- If a failure that could prevent the ACC system from stopping the bus at zero speed occurs, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.
- If a failure that could prevent the ACC system from stopping the bus at zero speed occurs, warn the driver and communicate any necessary actions to the driver (e.g., apply the brakes).

Safety Goal Adaptive Cruise Control–8

These safety goals are intended to establish a set of safety requirements that detect and mitigate potential failures that could cause the vehicle to roll away when the ACC system is active. For example, in system designs in which the ACC system engages the parking brake during prolonged stops, a failure may cause the ACC system to disengage the parking brake before the service brake is re-engaged.

- Prevent vehicle rollaway under all operating conditions through design and validation techniques in accordance with the QM[33] classification.
- Prevent unintended vehicle motion under all operating conditions through design and validation techniques in accordance with the QM[34] classification.

These safety goals are common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

[33] Note that safety goals assigned "QM" typically are not shown in the functional safety concept, as internal quality management processes rather than ISO 26262 concepts apply to these safety goals. However, in this study, these safety goals are shown for completeness.

[34] *Ibid.*

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the ACC system allowing the vehicle to roll away. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the ACC system allowing the vehicle to roll away cannot be prevented, then detect and mitigate all faults.
- Acknowledge all faults communicated by other vehicle systems that may prevent the vehicle from remaining stopped, including faults communicated by the powertrain system and braking system.
- Ensure that sufficient brake force is provided to keep the vehicle stopped for all combinations of bus loading and roadway grade.
- If a failure that could lead to the vehicle rolling away occurs, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.
- If a failure that could lead to the vehicle rolling away occurs, warn the driver and communicate any necessary actions to the driver.

Safety Goal, Adaptive Cruise Control–9

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could allow the ACC system to continue providing propulsion while the passenger door is open. For example, a failure may prevent the ACC system from recognizing that the passenger door was inadvertently opened.

- Prevent continued vehicle motion while the passenger door is open through design and validation techniques in accordance with the ASIL A classification.

This safety goal is specific to transit buses, since light vehicles do not have centrally-operated passenger doors.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could prevent the ACC system from determining the passenger door state.[35] Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.

[35] This assumes that the ACC system design includes measures to prevent vehicle motion when the doors are open during nominal (i.e., un-faulted) operation.

  - If a fault that could prevent the ACC system from determining the passenger door state cannot be prevented, then detect and mitigate the fault.
- Acknowledge all faults communicated by other vehicle systems that may prevent the ACC system from responding to an open passenger door, including faults communicated by the door control system.
  - Communication of the passenger door state from the door control system to the ACC system should be designed and validated in accordance with the specified ASIL.
- If a failure that could allow the bus to continue moving while the passenger door is open occurs, transition into a safe state within the FTTI.
- If a failure that could allow the bus to continue moving while the passenger door is open occurs, warn the driver and communicate any necessary actions to the driver (e.g., close the passenger door).

Safety Goal, Adaptive Cruise Control–10

These safety goals are intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to improper transition of control between the driver and the ACC system. For example, a failure may affect the ACC system from disengaging when the driver presses the brake pedal.

- Ensure that the system status is properly conveyed to the driver through design and validation techniques in accordance with the QM[36] classification.
- Ensure that the driver is capable of overriding the system through design and validation techniques in accordance with the ASIL A classification.

These safety goals are common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could prevent the ACC system from responding to the driver's request or displaying the ACC system status. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that could prevent the ACC system from responding to the driver's request or displaying the ACC system status cannot be prevented, then detect and mitigate the fault.

[36] Note that safety goals assigned "QM" typically are not shown in the functional safety concept, as internal quality management processes rather than ISO 26262 concepts apply to these safety goals. However, in this study, these safety goals are shown for completeness.

- Acknowledge all faults communicated by other vehicle systems that may prevent the ACC system from responding to the driver's request or displaying the ACC system status, including faults communicated by the instrument panel and head unit systems.
- If a failure that could prevent the ACC system from responding to the driver's request or displaying the ACC system status occurs, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.
- If a failure that could prevent the ACC system from responding to the driver's request or displaying the ACC system status occurs, warn the driver and communicate any necessary actions to the driver.

Potential Safe States

For the ACC system, potential safe states could be achieved through driver takeover via a tiered system disengagement, such as:

- Limit system operation to speeds below TBD mph. (Relevant Adaptive Cruise Control Safety Goals: 1, 2, 5, 6)
  - The driver should be notified of the limited operation.
- Issue all notifications through multiple channels (e.g., visual and audio). (Relevant Adaptive Cruise Control Safety Goals: 10)
- Disable the system and return control back to the driver. (Relevant Adaptive Cruise Control Safety Goals: All)
  - The driver should be notified of system disengagement.
  - The system should command zero propulsion input.

Automatic Emergency Braking

Safety Goal, Automatic Emergency Braking–1

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures in the AEB system that could lead to insufficient vehicle propulsion. For example, insufficient vehicle propulsion could result from failures that prevent the AEB system from releasing the brake pressure when the driver is trying to resume accelerating.

- Ensure that the system provides the correct level of propulsion through design and validation techniques in accordance with the ASIL A classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could cause the AEB system to maintain the brake pressure when the driver confirms an acceleration command. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the AEB system commanding insufficient vehicle propulsion cannot be prevented, then detect and mitigate the fault.
- Acknowledge all faults communicated by other vehicle systems that may prevent the AEB system from releasing the brake pressure, including faults communicated by the powertrain system and braking system.
- If a failure that could lead to insufficient vehicle propulsion occurs, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.
- If a failure that could lead to insufficient vehicle propulsion occurs, warn the driver and communicate any necessary actions to the driver.

Safety Goal, Automatic Emergency Braking–2

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures in the AEB system that could lead to loss of vehicle propulsion. For example, a failure in the AEB system may cause the system to command zero propulsion torque at the wrong time to collision (TTC) threshold.

- Prevent the system from requesting unintended zero propulsion torque through design and validation techniques in accordance with the ASIL B classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could cause the AEB system to request zero propulsion torque when the AEB system is not braking. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the AEB system requesting zero propulsion torque when not braking cannot be prevented, then detect and mitigate the fault.

- Ensure the validity and correctness of communication signals from other vehicle systems to the AEB system.
- If a failure that could lead to loss of vehicle propulsion occurs, transition into a safe state within the FTTI.
- If a failure that could lead to loss of vehicle propulsion occurs, warn the driver and communicate any necessary actions to the driver (e.g., disengage the system).

Safety Goal, Automatic Emergency Braking–3

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to excessive vehicle deceleration by the AEB system. For example, a failure in the AEB system may cause the system to apply the brakes when no object is in the bus's path.

- Prevent excessive vehicle deceleration or braking under all operating conditions through design and validation techniques in accordance with the ASIL C classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the AEB system commanding excessive vehicle deceleration or braking. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the AEB system commanding excessive vehicle deceleration or braking cannot be prevented, then detect and mitigate the fault.
- Prevent unintended activation of the AEB system.
- Ensure the validity and correctness of signals provided by the environmental sensors and other critical sensors for the AEB system.
- If a failure that could lead to excessive vehicle deceleration or braking occurs, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.
- If a failure that could lead to excessive vehicle deceleration or braking occurs, warn the driver and communicate any necessary actions to the driver.

- Ensure that deceleration resulting from failures[37] does not exceed TBD m/s^2. The allowable deceleration should be determined so that it does not cause displacement of unsecured standing or seated passengers, or the displacement of objects in a way that could cause harm to the passengers or driver.

Safety Goal, Automatic Emergency Braking–4

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to insufficient vehicle deceleration or braking by the AEB system. For example, a failure may cause the AEB system to command less braking than necessary for the driving situation.

- Ensure that the system provides the correct level of deceleration or braking through design and validation techniques in accordance with the ASIL B classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the AEB system commanding insufficient vehicle deceleration or braking. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the AEB system commanding insufficient vehicle deceleration or braking cannot be prevented, then detect and mitigate the fault.
- Ensure the validity and correctness of signals provided by the environmental sensors and other critical sensors for the AEB system.
- Acknowledge all faults communicated by other vehicle systems that may prevent the AEB system from achieving the intended decrease in speed, including faults communicated by the powertrain system or the braking system.
- If a failure that could lead to insufficient vehicle deceleration or braking occurs, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.

[37] Establishing an acceptable deceleration rate for nominal system performance that ensures the safety of passengers and the driver would be part of the system design and would not be covered by ISO 26262.

- If a failure that could lead to insufficient vehicle deceleration or braking occurs, warn the driver and communicate any necessary actions to the driver (e.g., apply the brakes).

Safety Goal, Automatic Emergency Braking–5

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to loss of vehicle deceleration or braking by the AEB system. For example, a failure may prevent the AEB system from applying the brakes at the final TTC threshold.

- Prevent loss of vehicle deceleration or braking through design and validation techniques in accordance with the ASIL C classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could prevent the AEB system from applying the brakes at the final TCC threshold. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that lead to loss of vehicle deceleration or braking cannot be prevented, then detect and mitigate the fault.
- Acknowledge all faults communicated by other vehicle systems that may prevent the AEB system from applying the brakes, including faults communicated by the braking system.
- If a failure that could lead to loss of vehicle deceleration or braking occurs, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.
- If a failure that could lead to loss of vehicle deceleration or braking occurs, warn the driver and communicate any necessary actions to the driver (e.g., apply the brakes).

Safety Goal, Automatic Emergency Braking–6

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to inadequate alerting of the driver by the AEB system. For example, a failure may prevent the AEB system from issuing a driver alert at the appropriate TTC thresholds.

- Ensure that the system issues driver alerts through design and validation techniques in accordance with the QM[38] classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could prevent the AEB system from issuing driver alerts at the appropriate TCC thresholds. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to inadequate alerting of the driver cannot be prevented, then detect and mitigate the fault.
- Ensure the validity and correctness of signals provided by the environmental sensors and other critical sensors for the AEB system.
- Acknowledge all faults communicated by other vehicle systems that may prevent the system from alerting the driver, including faults communicated by the instrument panel and head unit systems.
- If a failure that could lead to inadequate alerting of the driver occurs, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.

Safety Goal, Automatic Emergency Braking–7

These safety goals are intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to improper transition of control between the driver and the AEB system. For example, a failure may affect the AEB system status notification to the driver.

- Ensure that the system status is properly conveyed to the driver through design and validation techniques in accordance with the QM[39] classification.
- Ensure that the driver is capable of overriding the system through design and validation techniques in accordance with ASIL A classification.

These safety goals are common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

---

[38] Note that safety goals assigned "QM" typically are not shown in the functional safety concept, as internal quality management processes rather than ISO 26262 concepts apply to these safety goals. However, in this study, these safety goals are shown for completeness.

[39] Note that safety goals assigned "QM" typically are not shown in the functional safety concept, as internal quality management processes rather than ISO 26262 concepts apply to these safety goals. However, in this study, these safety goals are shown for completeness.

General Safety Strategy Considerations

Top-level considerations to help achieve these safety goals include:

- Prevent all faults that could prevent AEB system override or displaying the AEB system status. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that could prevent AEB system override or displaying the AEB system status cannot be prevented, then detect and mitigate the fault.
- Acknowledge all faults communicated by other vehicle systems that may prevent AEB system override or displaying the AEB system status, including faults communicated by the powertrain system, braking system, instrument panel, and head unit systems.
- If a failure that could prevent AEB system override or displaying the AEB system status, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.
- If a failure that could prevent AEB system override or displaying the AEB system status, warn the driver and communicate any necessary actions to the driver (e.g., manually disengage the AEB system).

Potential Safe States

For the AEB system, potential safe states include:

- Limit system operation to operating scenarios that can be supported with only one sensor type. (Relevant Automatic Emergency Braking Safety Goals: 1, 2, 3, 4, 5)
  - In these operating scenarios, the system would have sufficient confidence in the data provided by one sensor type to safely activate.
  - The driver should be notified of the limited operation.
- Limit system operation to braking-only. (Relevant Automatic Emergency Braking Safety Goals: 6)
  - The driver should be notified of the limited operation.
- Issue all notifications through multiple channels (e.g., visual and audio). (Relevant Automatic Emergency Braking Safety Goals: 6, 7)
- Disable active braking and provide warnings via a brake jerk and the HMI.[40] (Relevant Automatic Emergency Braking Safety Goals: 2, 4, 5, 6, 7)
  - The driver should be notified of the limited operation.

[40] In addition to visual warnings, the HMI may also include other types of warnings such as haptic and audio.

- Disable active braking and provide warnings via the HMI only. (Relevant Safety Goals: All)
  - The driver should be notified of the limited operation.

Docking

Safety Goal, Docking–1

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to the docking system commanding excessive lateral motion. For example, excessive lateral motion may occur from failures that cause the docking system to apply steering torque that brings the bus into contact with the curb.

- Prevent excessive lateral motion/yaw through design and validation techniques in accordance with the ASIL B classification.

This safety goal is unique to transit buses since light vehicles do not perform the docking maneuver.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the docking system commanding excessive lateral motion/yaw. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the docking system commanding excessive lateral motion/yaw cannot be prevented, then detect and mitigate the fault.
- When the docking system is active, prevent all faults that increase steering torque when additional steering is not requested by the driver, the docking system, or higher priority safety systems.
- Prevent unintended activation of the docking system.
- Ensure the validity and correctness of signals provided by the environmental sensors and other critical sensors for the docking system.
- Ensure the validity and correctness of communication signals from other vehicle systems to the docking system.
- If a failure that could lead to excessive lateral motion/yaw occurs, transition into a safe state within the FTTI.
- If a failure that could lead to excessive lateral motion/yaw occurs, warn the driver and communicate any necessary actions to the driver (e.g., manually disengage the system).

- Ensure that the lateral acceleration resulting from failures[41] does not exceed TBD m/s^2. The allowable lateral acceleration should be determined so that it does not cause displacement of unsecured standing or seated passengers, or displacement of objects in a way that could cause harm to the passengers or driver.

Safety Goal, Docking–2

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to insufficient lateral motion by the docking system. For example, insufficient lateral motion may occur from failures that cause the docking system to command less steering than appropriate to align the vehicle with the curb.

- Ensure that the system provides the correct level of lateral motion/yaw through design and validation techniques in accordance with the ASIL B classification.

This safety goal is unique to transit buses since light vehicles do not perform the docking maneuver.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the docking system commanding insufficient lateral motion/yaw. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the docking system commanding insufficient lateral motion/yaw cannot be prevented, then detect and mitigate all faults.
- Ensure the validity and correctness of signals provided by the environmental sensors and other critical sensors for the docking system.
- Acknowledge all faults communicated by other vehicle systems that may prevent the vehicle from achieving the intended level of steering, including faults communicated by the steering system and braking system.
- If a failure that could lead to insufficient lateral motion/yaw occurs, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.

[41] Establishing an acceptable acceleration rate for nominal system performance that ensures the safety of passengers and the driver would be part of the system design and would not be covered by ISO 26262.

- If a failure that could lead to insufficient lateral motion/yaw occurs, warn the driver and communicate any necessary actions to the driver (e.g., resume steering).

Safety Goal, Docking–3

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to the docking system commanding vehicle movement in the wrong direction. For example, a failure might cause the docking system to invert the steering requests to the steering system.

- Ensure that lateral motion/yaw is provided in the correct direction through design and validation techniques in accordance with the ASIL C classification.

This safety goal is unique to transit buses, as light vehicles do not perform the docking maneuver.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the docking system commanding lateral motion/yaw in the wrong direction. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the docking system commanding lateral motion/yaw in the wrong direction cannot be prevented, then detect and mitigate the fault.
- Ensure the validity and correctness of signals provided by the environmental sensors and other critical sensors for the docking system.
- Ensure the validity and correctness of communication signals from other vehicle systems to the docking system.
- If a failure that could lead to lateral motion/yaw in the wrong direction occurs, transition into a safe state within the FTTI.
- If a failure that could lead to lateral motion/yaw in the wrong direction occurs, warn the driver and communicate any necessary actions to the driver (e.g., manually disengage the system).

Safety Goal, Docking–4

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to the docking system stopping the bus too far from the curb at a station/stop. For example, a failure might cause the docking system to incorrectly determine the distance to the curb.

- Ensure that the vehicle stops at the driver-specified distance from the curb at a bus station/stop through design and validation techniques in accordance with the ASIL A classification.

This safety goal is unique to transit buses since light vehicles do not perform the docking maneuver.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the docking system stopping too far from the curb at a bus station/stop. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the docking system stopping too far from the curb at a bus station/stop cannot be prevented, then detect and mitigate the fault.
- After each maneuver, compute the future trajectory of the docking system and, given any limits on steering authority, determine if the docking system can achieve the driver-specified distance from the curb at the bus station/stop.
- Ensure the validity and correctness of signals provided by the environmental sensors and other critical sensors for the docking system.
- Acknowledge all faults communicated by other vehicle systems that may lead to the docking system stopping too far from the curb at a bus station/stop, including faults communicated by the steering system and braking system.
- If a failure that could lead to the docking system stopping too far from the curb at a bus station/stop occurs, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.
- If a failure that could lead to the docking system stopping too far from the curb at a bus station/stop occurs, warn the driver and communicate any necessary actions to the driver (e.g., manually disengage the system).

Safety Goal, Docking–5

These safety goals are intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to improper transition of control between the driver and the docking system. For example, a failure may affect the docking system status notification to the driver.

- Ensure that the system status is properly conveyed to the driver through design and validation techniques in accordance with the QM[42] classification.

- Ensure that the driver is capable of overriding the system through design and validation techniques in accordance with the ASIL A classification.

These safety goals are unique to transit buses since light vehicles do not perform the docking maneuver.

General Safety Strategy Considerations

Top-level considerations to help achieve these safety goals include:

- Prevent all faults that could prevent the docking system from responding to the driver's request or displaying the docking system status. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that could prevent the docking system from responding to the driver's request or displaying the docking system status cannot be prevented, then detect and mitigate the fault.
- Acknowledge all faults communicated by other vehicle systems that may prevent the docking system from responding to the driver's request or displaying the docking system status, including faults communicated by the steering system, instrument panel, and head unit systems.
- If a failure that could prevent the docking system from responding to the driver's request or displaying the docking system status occurs, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.
- If a failure that could prevent the docking system from responding to the driver's request, warn the driver and communicate any necessary actions to the driver (e.g., manually disengage the system).

Safety Goal, Docking–6

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to improper transition of control between another vehicle system and the docking system. For example, a failure may prevent communication between the docking system and the lane centering system.

[42] Note that safety goals assigned "QM" typically are not shown in the functional safety concept, as internal quality management processes rather than ISO 26262 concepts apply to these safety goals. However, in this study, these safety goals are shown for completeness.

- Ensure that the system communicates its operational status to other vehicle systems (e.g., lane keeping, lane centering, or steering assist) through design and validation techniques in accordance with the QM[43] classification.

This safety goal is unique to transit buses since light vehicles do not perform the docking maneuver.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could prevent the docking system from communicating its status to other vehicle systems. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that could prevent the docking system communicating its status to other vehicle systems cannot be prevented, then detect and mitigate the fault.
- Acknowledge all faults communicated by other vehicle systems that may prevent these systems from suspending operation while the docking system is active, including faults communicated by other driving automation systems (e.g., lane keeping, lane centering, or steering assist), or other active steering system functions.
- If a failure that could prevent the docking system from communicating its status to other vehicle systems occurs, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.
- If a failure that could prevent the docking system from communicating its status to other vehicle systems occurs, warn the driver and communicate any necessary actions to the driver (e.g., manually disengage the other system).

Potential Safe States

For the docking system, potential safe states could be achieved through driver takeover via a tiered system disengagement, such as:

- Restrict the level of steering provided to a steering overlay that only assists the driver, rather than full steering. (Relevant Docking Safety Goals: 1, 2)
  - Notify the driver of the limited operation.

[43] Note that safety goals assigned "QM" typically are not shown in the functional safety concept, as internal quality management processes rather than ISO 26262 concepts apply to these safety goals. However, in this study, these safety goals are shown for completeness.

- Pause system operation and instruct driver to manually disable other driver assistance systems. (Relevant Docking Safety Goals: 6)
- Issue all notifications through multiple channels (e.g., visual and audio). (Relevant Docking Safety Goals: 5)
- Disable active steering and provide visual trajectory guidance only (no active steering). (Relevant Docking Safety Goals: 1, 2, 3, 5)
  - Notify the driver of the limited operation.
- Disable the system. (Relevant Safety Goals: All)
  - Notify the driver of system unavailability.

Full Park Assist/ Valet Parking

Safety Goal, Full Park Assist/ Valet Parking–1

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to the full park assist system commanding excessive vehicle propulsion. For example, excessive vehicle propulsion may occur from failures that cause the full park assist system to command additional propulsion once the bus is already in the selected parking spot.

- Prevent excessive vehicle propulsion under all operating conditions through design and validation techniques in accordance with the ASIL A classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification below may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the full park assist system commanding excessive vehicle propulsion. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the full park assist system commanding excessive vehicle propulsion cannot be prevented, then detect and mitigate the faults.
- When the full park assist system is active, prevent all faults that increase propulsion torque when additional propulsion is not requested by the driver, the full park assist system, or higher priority safety systems.
- Prevent unintended activation of the full park assist system or unintended selection of a parking space.

- Ensure the validity and correctness of signals provided by the environmental sensors and other critical sensors for the full park assist system.
- Ensure the validity and correctness of communication signals from other vehicle systems to the full park assist system.
- If a failure that could lead to excessive vehicle propulsion occurs, transition into a safe state within the FTTI.
- If a failure that could lead to excessive vehicle propulsion occurs, warn the driver and communicate any necessary actions to the driver (e.g., manually disable the system).

Safety Goal, Full Park Assist/ Valet Parking–2

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to insufficient vehicle propulsion from the full park assist system. For example, insufficient vehicle propulsion could result from failures that cause the full park assist system to receive less propulsion than requested.

- Ensure that the system provides the correct level of propulsion through design and validation techniques in accordance with the QM[44] classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the full park assist system commanding insufficient vehicle propulsion. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the full park assist system commanding insufficient vehicle propulsion cannot be prevented, then detect and mitigate the fault.
- Ensure the validity and correctness of signals provided by the environmental sensors and other critical sensors for the full park assist system.
- Acknowledge all faults communicated by other vehicle systems that may prevent the vehicle from achieving the intended increase in speed, including faults communicated by the powertrain system.

[44] Note that safety goals assigned "QM" typically are not shown in the functional safety concept, as internal quality management processes rather than ISO 26262 concepts apply to these safety goals. However, in this study, these safety goals are shown for completeness.

- If a failure that could lead to insufficient vehicle propulsion occurs, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.
- If a failure that could lead to insufficient vehicle propulsion occurs, warn the driver and communicate any necessary actions to the driver.

Safety Goal, Full Park Assist/ Valet Parking–3

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to the full park assist system commanding vehicle movement in the wrong longitudinal direction. For example, a failure may cause the full park assist system to increase propulsion while the transmission is in the wrong position.

- Ensure that vehicle motion occurs in the intended longitudinal direction through design and validation techniques in accordance with the ASIL A classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the full park assist system commanding vehicle propulsion in the wrong direction. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the full park assist system commanding vehicle propulsion in the wrong direction cannot be prevented, then detect and mitigate the fault.
- Acknowledge all faults communicated by other vehicle systems that may cause vehicle propulsion in the wrong longitudinal direction, including the powertrain system.
- If a failure that could lead to vehicle movement in the wrong direction occurs, transition into a safe state within the FTTI.
- If a failure that could lead to vehicle movement in the wrong direction occurs, warn the driver and communicate any necessary actions to the driver.

Safety Goal, Full Park Assist/ Valet Parking–4

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to excessive vehicle deceleration or braking. For example, a failure may cause the full park assist system to decelerate the vehicle suddenly when in a queue with other buses.

- Prevent excessive vehicle deceleration or braking under all vehicle operating conditions through design and validation techniques in accordance with the QM[45] classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the full park assist system commanding excessive vehicle deceleration or braking. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the full park assist system commanding excessive vehicle deceleration or braking cannot be prevented, then detect and mitigate the fault.
- When the full park assist system is active, prevent all faults that cause deceleration or braking when deceleration is not requested by either the driver, the full park assist system, or higher priority safety systems.
- Ensure the validity and correctness of signals provided by the environmental sensors and other critical sensors for the full park assist system.
- Ensure the validity and correctness of communication signals from other vehicle systems to the full park assist system.
- If a failure that could lead to excessive vehicle deceleration or braking occurs, transition into a safe state within the FTTI.
- If a failure that could lead to excessive vehicle deceleration or braking occurs, warn the driver and communicate any necessary actions to the driver (e.g., manually disengage the system).

[45] Note that safety goals assigned "QM" typically are not shown in the functional safety concept, as internal quality management processes rather than ISO 26262 concepts apply to these safety goals. However, in this study, these safety goals are shown for completeness.

Safety Goal, Full Park Assist/ Valet Parking–5

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to insufficient vehicle deceleration or braking by the full park assist system. For example, a failure may cause the full park assist system to brake with too little force to stop the bus after the system completes the parking maneuver.

- Ensure that the system provides the correct level of deceleration or braking through design and validation techniques in accordance with the ASIL A classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the full park assist system commanding insufficient vehicle deceleration or braking. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the full park assist system commanding insufficient vehicle deceleration or braking cannot be prevented, then detect and mitigate the fault.
- Ensure the validity and correctness of signals provided by the environmental sensors and other critical sensors for the full park assist system.
- Acknowledge all faults communicated by other vehicle systems that may prevent the vehicle from achieving the intended decrease in speed, including faults communicated by the powertrain system or the braking system.
- If a failure that could lead to insufficient vehicle deceleration or braking occurs, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.
- If a failure that could lead to insufficient vehicle deceleration or braking occurs, warn the driver and communicate any necessary actions to the driver.

Safety Goal, Full Park Assist/ Valet Parking–6

These safety goals are intended to establish a set of safety requirements that detect and mitigate potential failures that could cause the full park assist system to allow the vehicle to roll away. For example, a failure may prevent the full park assist system from shifting the vehicle into park at the end of a maneuver.

- Prevent vehicle rollaway under all operating conditions through design and validation techniques in accordance with the QM[46] classification.
- Prevent unintended vehicle motion under all operating conditions through design and validation techniques in accordance with the QM[47] classification.

These safety goals are common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve these safety goals include:

- Prevent all faults that could lead to the full park assist system allowing the vehicle to roll away. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the full park assist system allowing the vehicle to roll away cannot be prevented, then detect and mitigate the fault.
- Acknowledge all faults communicated by other vehicle systems that may prevent the vehicle from properly shifting into the correct gear or keeping the vehicle stopped, including faults communicated by the powertrain system, transmission system, and braking system.
- If a failure that could lead to the vehicle rolling away occurs, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.
- If a failure that could lead to the vehicle rolling away occurs, warn the driver and communicate any necessary actions to the driver (e.g., apply the brakes).

Safety Goal, Full Park Assist/ Valet Parking–7

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to the full park assist system commanding excessive lateral motion. For example, excessive lateral motion may occur from failures that cause the full park assist system to steer more than necessary when entering the selected parking space.

- Prevent excessive lateral motion/yaw through design and validation techniques in accordance with the ASIL A classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

[46] Note that safety goals assigned "QM" typically are not shown in the functional safety concept, as internal quality management processes rather than ISO 26262 concepts apply to these safety goals. However, in this study, these safety goals are shown for completeness.

[47] *Ibid.*

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the full park assist system commanding excessive lateral motion/yaw. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the full park assist system commanding excessive lateral motion/yaw cannot be prevented, then detect and mitigate the fault.
- When the full park assist system is active, prevent all faults that increase steering torque when additional steering is not requested by the driver, the full park assist system, or higher priority safety systems.
- Prevent unintended activation of the full park assist system or unintended selection of a parking space.
- Ensure the validity and correctness of signals provided by the environmental sensors and other critical sensors for the full park assist system.
- Ensure the validity and correctness of communication signals from other vehicle systems to the full park assist system.
- If a failure that could lead to excessive lateral motion/yaw occurs, transition into a safe state within the FTTI.
- If a failure that could lead to excessive lateral motion/yaw occurs, warn the driver and communicate any necessary actions to the driver.

Safety Goal, Full Park Assist/ Valet Parking–8

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to insufficient lateral motion by the full park assist system. For example, insufficient lateral motion may occur from failures that cause the full park assist system to command less steering than needed to align the bus with the selected parking space.

- Ensure that the system provides the correct level of lateral motion/yaw through design and validation techniques in accordance with the ASIL A classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the full park assist system commanding insufficient lateral motion/yaw. Such faults and their root causes may be

determined through a comprehensive safety analysis in accordance with ISO 26262.

  - If a fault that leads to the full park assist system commanding insufficient lateral motion/yaw cannot be prevented, then detect and mitigate the fault.
- Acknowledge all faults communicated by other vehicle systems that may prevent the vehicle from achieving the intended level of steering, including faults communicated by the steering system and braking system.
- If a failure that could lead to insufficient lateral motion/yaw occurs, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.
- If a failure that could lead to insufficient lateral motion/yaw occurs, warn the driver and communicate any necessary actions to the driver (e.g., manually disengage the system).

Safety Goal, Full Park Assist/ Valet Parking–9

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to the full park assist system commanding vehicle movement in the wrong lateral direction. For example, a failure might cause the full park assist system to steer in the wrong direction for the current transmission position.

- Ensure that lateral motion/yaw is provided in the correct direction through design and validation techniques in accordance with the ASIL A classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the full park assist system commanding lateral motion/yaw in the wrong direction. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the full park assist system commanding lateral motion/yaw in the wrong direction cannot be prevented, then detect and mitigate the fault.
- Acknowledge all faults communicated by other vehicle systems that may cause vehicle movement in the wrong lateral direction, including faults communicated by the powertrain system or the steering system.

- If a failure that could lead to lateral motion/yaw in the wrong direction occurs, transition into a safe state within the FTTI.
- If a failure that could lead to lateral motion/yaw in the wrong direction occurs, warn the driver and communicate any necessary actions to the driver (e.g., manually deactivate the system).

Safety Goal, Full Park Assist/ Valet Parking–10

These safety goals are intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to improper transition of control between the driver and the full park assist system. For example, for systems with remote operation (i.e., driver outside the cab) a failure may affect the driver's ability to override the full park assist system.

- Ensure that the system status is properly conveyed to the driver through design and validation techniques in accordance with the QM[48] classification.
- Ensure that the driver is capable of overriding the system through design and validation techniques in accordance with the ASIL A classification.

These safety goals are common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve these safety goals include:

- Prevent all faults that could prevent the driver from overriding the full park assist system or receiving information on the full park assist system status, including in instances of remote operation. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that could prevent full park assist system override or displaying the full park assist system status cannot be prevented, then detect and mitigate the fault.
- Acknowledge all faults communicated by other vehicle systems that may prevent the driver from overriding the full park assist system, including faults in the brake system, steering system, or telematics system (in the case of remote operation).
- Acknowledge all faults communicated by other vehicle systems that may prevent the full park assist system from displaying the system status, including

[48] Note that safety goals assigned "QM" typically are not shown in the functional safety concept, as internal quality management processes rather than ISO 26262 concepts apply to these safety goals. However, in this study, these safety goals are shown for completeness.

faults communicated by the instrument panel, head unit system, or telematics system (in the case of remote operation).

- If a failure occurs that could prevent overriding the full park assist system or displaying the full park assist system status, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.
- If a failure occurs that could prevent overriding the full park assist system or displaying the full park assist system status, warn the driver and communicate any necessary actions to the driver (e.g., manually disengage the system).

Potential Safe States

For the full park assist system, potential safe states could be achieved through driver takeover via a tiered system disengagement, such as:

- Limit system operation to operating scenarios that can be supported with only one sensor type (Relevant Full Park Assist/Valet Parking Safety Goals: 1, 2, 3, 4, 5, 6, 7, 8, 9)
  - In these operating scenarios, the system would have sufficient confidence in the data provided by one sensor type to safely activate.
  - The driver should be notified when activating the system in an unsupported operating scenario.
- Disable longitudinal control and provide steering assistance only. (Relevant Full Park Assist/Valet Parking Safety Goals: 1, 2, 3, 4, 5)
  - Notify the driver of the limited operation.
- Issue all notifications through multiple channels (e.g., visual and audio). (Relevant Full Park Assist/Valet Parking Safety Goals: 10)
- Provide trajectory guidance only (no active steering, propulsion, or braking). (Relevant Full Park Assist/Valet Parking Safety Goals: 7, 8, 9)
  - This safe state may depend on availability of certain sensing technologies (e.g., front-facing camera).
  - Notify the driver of the limited operation.
- Disable the system. (Relevant Safety Goals: All)
  - Notify the driver that the full park assist system is not available.
  - The system should command zero propulsion input.

Lane Keeping/ Lane Centering/ Steering Assist

Safety Goal, Lane Keeping/ Lane Centering/ Steering Assist–1

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to the lane keeping or lane centering system commanding excessive lateral motion. For example, excessive lateral motion may occur from failures that cause the lane keeping or lane centering system to steer suddenly when the bus is travelling on a straight roadway.

- Prevent excessive lateral motion/yaw through design and validation techniques in accordance with the ASIL C classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the lane keeping or lane centering system commanding excessive lateral motion/yaw. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the lane keeping or lane centering system commanding excessive lateral motion/yaw cannot be prevented, then detect and mitigate the fault.
- When the lane keeping or lane centering system is active, prevent all faults that increase steering torque when additional steering is not requested by the driver, the lane keeping or lane centering system, or higher priority safety systems.
- Prevent unintended activation of the lane keeping or lane centering system.
- Ensure the validity and correctness of signals provided by the environmental sensors and other critical sensors for the lane keeping or lane centering system.
- Ensure the validity and correctness of communication signals from other vehicle systems to the lane keeping or lane centering system.
- If a failure that could lead to excessive lateral motion/yaw occurs, transition into a safe state within the FTTI.

- If a failure that could lead to excessive lateral motion/yaw occurs, warn the driver and communicate any necessary actions to the driver (e.g., manually disengage the system).
- Ensure that the lateral acceleration resulting from failures[49] does not exceed TBD m/s^2. The allowable lateral acceleration should be determined so that it does not cause displacement of unsecured standing or seated passengers, or displacement of objects in a way that could cause harm to the passengers or driver.

Safety Goal, Lane Keeping/ Lane Centering/ Steering Assist–2

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to insufficient lateral motion by the lane keeping or lane centering system. For example, insufficient lateral motion may occur from failures that cause the lane keeping or lane centering system to command less steering than needed to follow the road curvature.

- Ensure that the system provides the correct level of lateral motion/yaw through design and validation techniques in accordance with the ASIL C classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the lane keeping or lane centering system commanding insufficient lateral motion/yaw. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the lane keeping or lane centering system commanding insufficient lateral motion/yaw cannot be prevented, then detect and mitigate the fault.
- Ensure the validity and correctness of signals provided by the environmental sensors and other critical sensors for the lane keeping or lane centering system.
- Acknowledge all faults communicated by other vehicle systems that may prevent the vehicle from achieving the intended level of steering, including faults communicated by the steering system and braking system.

[49] Establishing an acceptable acceleration rate for nominal system performance that ensures the safety of passengers and the driver would be part of the system design and would not be covered by ISO 26262.

- If a failure that could lead to insufficient lateral motion/yaw occurs, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.
- If a failure that could lead to insufficient lateral motion/yaw occurs, warn the driver and communicate any necessary actions to the driver (e.g., resume steering).

Safety Goal, Lane Keeping/ Lane Centering/ Steering Assist–3

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to the lane keeping or lane centering system commanding vehicle movement in the wrong lateral direction. For example, a failure might cause the lane keeping or lane centering system to issue a steering command in the opposite direction of the road curvature.

- Ensure that lateral motion/yaw is provided in the correct direction through design and validation techniques in accordance with the ASIL C classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the lane keeping or lane centering system commanding lateral motion/yaw in the wrong direction. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the lane keeping or lane centering system commanding lateral motion/yaw in the wrong direction cannot be prevented, then detect and mitigate the fault.
- Ensure the validity and correctness of signals provided by the environmental sensors and other critical sensors for the lane keeping or lane centering system.
- Ensure the validity and correctness of communication signals from other vehicle systems to the lane keeping or lane centering system.
- If a failure that could lead to lateral motion/yaw in the wrong direction occurs, transition into a safe state within the FTTI.
- If a failure that could lead to lateral motion/yaw in the wrong direction occurs, warn the driver and communicate any necessary actions to the driver (e.g., manually disengage the system).

Safety Goal, Lane Keeping/ Lane Centering/ Steering Assist–4

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to the lane keeping or lane centering system creating excessive vehicle roll conditions. For example, excessive vehicle roll may occur from failures that cause the lane keeping or lane centering system to steer suddenly when travelling at high speeds.

- Prevent excessive vehicle roll resulting from steering maneuvers through design and validation techniques in accordance with the ASIL B classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the lane keeping or lane centering system commanding steering that leads to excessive vehicle roll. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the lane keeping or lane centering system creating an excessive vehicle roll condition cannot be prevented, then detect and mitigate the fault.
- Prevent failures that result in lateral acceleration forces above TBD m/s^2, where TBD m/s^2 is a critical threshold that leads to excessive roll given the bus's dimensions, speed, center of gravity, and loading.
- Acknowledge all faults communicated by other vehicle systems that may affect the vehicle dynamics or steering, including faults communicated by the steering system, powertrain system, suspension system, and braking system.
- If a failure that could lead to the system creating an excessive vehicle roll condition occurs, transition into a safe state within the FTTI.
- If a failure that could lead to the system creating an excessive vehicle roll condition occurs, warn the driver and communicate any necessary actions to the driver (e.g., apply the brakes and reduce the steering input).

Safety Goal, Lane Keeping/ Lane Centering/ Steering Assist–5

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to a lane or roadway departure while the lane keeping or lane centering system is engaged. For example, a failure

might prevent the lane keeping or lane centering system from recognizing that the vehicle is approaching a lane boundary.

- Prevent a lane or roadway departure while the system is engaged through design and validation techniques in accordance with the ASIL C classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to a lane or roadway departure while the lane keeping or lane centering system is engaged. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to a lane or roadway departure while the lane keeping or lane centering system is engaged cannot be prevented, then detect and mitigate the fault.
- Ensure the validity and correctness of signals provided by the environmental sensors and other critical sensors for the lane keeping or lane centering system.
- Acknowledge all faults communicated by other vehicle systems that may lead to a lane or roadway departure while the lane keeping or lane centering system is engaged, including faults communicated by the steering system and braking system.
- If a failure occurs that could lead to a lane or roadway departure while the lane keeping or lane centering system is engaged, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.
- If a failure occurs that could lead to a lane or roadway departure while the lane keeping or lane centering system is engaged, warn the driver and communicate any necessary actions to the driver (e.g., resume steering).

Safety Goal, Lane Keeping/ Lane Centering/ Steering Assist–6

These safety goals are intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to improper transition of control between the driver and the lane keeping or lane centering system. For example, a failure may prevent the driver from overriding the steering force exerted by the lane keeping or lane centering system.

- Ensure that the system status is properly conveyed to the driver through design and validation techniques in accordance with the ASIL A classification.
- Ensure that the driver is capable of overriding the system through design and validation techniques in accordance with the ASIL A classification.

These safety goals are common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve these safety goals include:

- Prevent all faults that could prevent the driver from overriding the lane keeping or lane centering system or receiving information on the lane keeping or lane centering system status. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that could prevent the driver from overriding the lane keeping or lane centering system or receiving information on the lane keeping or lane centering system status cannot be prevented, then detect and mitigate the fault.
- Acknowledge all faults communicated by other vehicle systems that may prevent the driver from overriding the lane keeping or lane centering system, including faults in the steering system.
- Acknowledge all faults communicated by other vehicle systems that may prevent the lane keeping or lane centering system from displaying the system status, including faults communicated by the instrument panel or head unit system.
- If a failure occurs that could prevent overriding the lane keeping or lane centering system or displaying the lane keeping or lane centering system status, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.
- If a failure occurs that could prevent overriding the lane keeping or lane centering system or displaying the lane keeping or lane centering system status, warn the driver and communicate any necessary actions to the driver (e.g., resume steering).

Potential Safe States

For the lane keeping or lane centering system, potential safe states could be achieved through driver takeover via a tiered system disengagement, such as:

- Disable lane centering (i.e., continuous control) and provide lane keeping only (i.e., short intervention near lane boundaries. (Relevant Lane Keeping/Lane Centering/Steering Assist Safety Goals: 2, 5, 6)
  - Notify the driver of the limited operation.
- Issue all notifications through multiple channels (e.g., visual and audio). (Relevant Lane Keeping/Lane Centering/Steering Assist Safety Goals: 6)
- Provide trajectory guidance only (no active steering). (Relevant Lane Keeping/Lane Centering/Steering Assist Safety Goals: 1, 2, 3, 4, 5)
  - Notify the driver of the limited operation.
- Disable active steering and provide lane departure warnings only. (Relevant Lane Keeping/Lane Centering/Steering Assist Safety Goals: All)
  - Notify the driver that the lane keeping or lane centering system is not available.
  - The system should command zero steering (i.e., return to center).

Object Detection and Collision Avoidance

Safety Goal, Object Detection and Collision Avoidance–1

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to inadequate alerting of the driver by the object detection and collision avoidance system. For example, a failure may prevent the object detection and collision avoidance system from issuing a driver alert when it detects an object.

- Ensure that the system issues driver alerts through design and validation techniques in accordance with the QM[50] classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could prevent the object detection and collision avoidance system from issuing driver alerts when an object is detected. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.

[50] Note that safety goals assigned "QM" typically are not shown in the functional safety concept, as internal quality management processes rather than ISO 26262 concepts apply to these safety goals. However, in this study, these safety goals are shown for completeness.

  - If a fault that leads to inadequate alerting of the driver cannot be prevented, then detect and mitigate the fault.
- Ensure the validity and correctness of signals provided by the environmental sensors and other critical sensors for the lane keeping or lane centering system.
- Acknowledge all faults communicated by other vehicle systems that may prevent the system from alerting the driver, including faults communicated by the instrument panel and head unit systems.

Park Assist/Park Out

Safety Goal, Park Assist/ Park Out–1

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to the park assist or park out system commanding excessive lateral motion. For example, excessive lateral motion may occur from failures that cause the park assist or park out system to steer the vehicle when the bus does not have sufficient clearance from adjacent objects.

- Prevent excessive lateral motion/yaw through design and validation techniques in accordance with the ASIL A classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the park assist or park out system commanding excessive lateral motion/yaw. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the park assist or park out system commanding excessive lateral motion/yaw cannot be prevented, then detect and mitigate the fault.
- When the park assist or park out system is active, prevent all faults that increase steering torque when additional steering is not requested by the driver, the park assist or park out system, or higher priority safety systems.
- Prevent unintended activation of the park assist or park out system, or unintended selection of a parking space.
- Ensure the validity and correctness of signals provided by the environmental sensors and other critical sensors for the park assist or park out system.

- Ensure the validity and correctness of communication signals from other vehicle systems to the park assist or park out system.
- If a failure that could lead to excessive lateral motion/yaw occurs, transition into a safe state within the FTTI.
- If a failure that could lead to excessive lateral motion/yaw occurs, warn the driver and communicate any necessary actions to the driver (e.g., manually disengage the system).

Safety Goal, Park Assist/ Park Out–2

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to insufficient lateral motion by the park assist or park out system. For example, insufficient lateral motion may occur from failures that cause the park assist or park out system to command less steering than appropriate for the driving situation.

- Ensure that the system provides the correct level of lateral motion/yaw through design and validation techniques in accordance with the ASIL A classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the park assist or park out system commanding insufficient lateral motion/yaw. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the park assist or park out system commanding insufficient lateral motion/yaw cannot be prevented, then detect and mitigate the fault.
- Ensure the validity and correctness of signals provided by the environmental sensors and other critical sensors for the park assist or park out system.
- Acknowledge all faults communicated by other vehicle systems that may prevent the vehicle from achieving the intended level of steering, including faults communicated by the steering system and braking system.
- If a failure that could lead to insufficient lateral motion/yaw occurs, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.

- If a failure that could lead to insufficient lateral motion/yaw occurs, warn the driver and communicate any necessary actions to the driver (e.g., resume steering).

Safety Goal, Park Assist/ Park Out–3

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to the park assist or park out system commanding vehicle movement in the wrong lateral direction. For example, a failure might cause the park assist or park out system to issue a steering command when the vehicle's transmission is in the wrong position.

- Ensure that lateral motion/yaw is provided in the correct direction through design and validation techniques in accordance with the ASIL A classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the park assist or park out system commanding lateral motion/yaw in the wrong direction. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the park assist or park out system commanding lateral motion/yaw in the wrong direction cannot be prevented, then detect and mitigate the fault.
- Ensure the validity and correctness of signals provided by the environmental sensors and other critical sensors for the park assist or park out system.
- Acknowledge all faults communicated by other vehicle systems that may lead to vehicle movement in the wrong lateral direction, including faults communicated by the steering system and powertrain (transmission) system.
- If a failure that could lead to lateral motion/yaw in the wrong direction occurs, transition into a safe state within the FTTI.
- If a failure that could lead to lateral motion/yaw in the wrong direction occurs, warn the driver and communicate any necessary actions to the driver (e.g., manually disengage the system).

Safety Goal, Park Assist/ Park Out–4

These safety goals are intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to improper transition of control between the driver and the park assist or park out system. For example,

a failure may prevent the driver from overriding the steering force exerted by the park assist or park out system.

- Ensure that the system status is properly conveyed to the driver through design and validation techniques in accordance with the QM[51] classification.
- Ensure that the driver is capable of overriding the system through design and validation techniques in accordance with the ASIL A classification.

These safety goals are common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve these safety goals include:

- Prevent all faults that could prevent the driver from overriding the park assist or park out system or receiving information on the park assist or park out system status. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that could prevent the driver from overriding the park assist or park out system or receiving information on the park assist or park out system status cannot be prevented, then detect and mitigate the fault.
- Acknowledge all faults communicated by other vehicle systems that may prevent the driver from overriding the park assist or park out system, including faults in the steering system.
- Acknowledge all faults communicated by other vehicle systems that may prevent the park assist or park out system from displaying the system status, including faults communicated by the instrument panel or head unit system.
- If a failure occurs that could prevent overriding the park assist or park out system or displaying the park assist or park out system status, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.
- If a failure occurs that could prevent overriding the park assist or park out system or displaying the park assist or park out status, warn the driver and communicate any necessary actions to the driver.

Potential Safe States

For the park assist or park out system, potential safe states could be achieved through driver takeover via a tiered system disengagement, such as:

[51] Note that safety goals assigned "QM" typically are not shown in the functional safety concept, as internal quality management processes rather than ISO 26262 concepts apply to these safety goals. However, in this study, these safety goals are shown for completeness.

- Restrict the level of steering provided to a steering overlay that only assists the driver, rather than full steering. (Relevant Park Assist/ Park Out Safety Goals: 1, 2)
  - Notify the driver of the limited operation.
- Limit system operation to operating scenarios that can be supported with only one sensor type. (Relevant Park Assist/ Park Out Safety Goals: 1, 2, 3)
  - In these operating scenarios, the system would have sufficient confidence in the data provided by one sensor type to safely activate.
  - The driver should be notified when activating the system in an unsupported operating scenario.
- Issue all notifications through multiple channels (e.g., visual and audio). (Relevant Park Assist/ Park Out Safety Goals: 4)
- Disable active steering and provide trajectory guidance only. (Relevant Park Assist/ Park Out Safety Goals: 1, 4)
  - This safe state may depend on the availability of certain sensing technologies (e.g., front-facing camera).
  - Notify the driver of the limited operation.
- Disable the system. (Relevant Park Assist/Park Out Safety Goals: All)
  - Notify the driver that the park assist or park out system is not available.

Rear Brake Assist

Safety Goal, Rear Brake Assist–1

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to the RBA system causing insufficient vehicle propulsion. For example, insufficient vehicle propulsion could result from failures that prevent the RBA system from releasing the brake pressure when appropriate.

- Ensure that the system provides the correct level of propulsion through design and validation techniques in accordance with the QM[52] classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

[52] Note that safety goals assigned "QM" typically are not shown in the functional safety concept, as internal quality management processes rather than ISO 26262 concepts apply to these safety goals. However, in this study, these safety goals are shown for completeness.

- Prevent all faults that could cause the RBA system to maintain the brake pressure when the driver resumes accelerating. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the RBA system causing insufficient vehicle propulsion cannot be prevented, then detect and mitigate the fault.
- Ensure the validity and correctness of signals provided by the environmental sensors and other critical sensors for the RBA system.
- Acknowledge all faults communicated by other vehicle systems that may prevent the RBA system from releasing the brake pressure, including faults communicated by the powertrain system and braking system.
- If a failure that could lead to insufficient vehicle propulsion occurs, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.
- If a failure that could lead to insufficient vehicle propulsion occurs, warn the driver and communicate any necessary actions to the driver (e.g., manually disengage the system).

Safety Goal, Rear Brake Assist–2

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to the RBA system causing loss of vehicle propulsion. For example, a failure in the RBA system may cause the system to command zero propulsion torque at the wrong TTC threshold.

- Prevent the system from requesting unintended zero propulsion torque through design and validation techniques in accordance with the QM[53] classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could cause the RBA system to erroneously request zero propulsion torque. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.

[53] Note that safety goals assigned "QM" typically are not shown in the functional safety concept, as internal quality management processes rather than ISO 26262 concepts apply to these safety goals. However, in this study, these safety goals are shown for completeness.

- If a fault that leads to the RBA system erroneously requesting zero propulsion torque cannot be prevented, then detect and mitigate the fault.
- Ensure the validity and correctness of communication signals from other vehicle systems to the RBA system.
- If a failure that could lead to loss of vehicle propulsion occurs, transition into a safe state within the FTTI.
- If a failure that could lead to loss of vehicle propulsion occurs, warn the driver and communicate any necessary actions to the driver.

Safety Goal, Rear Brake Assist–3

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to the RBA system commanding excessive vehicle deceleration. For example, a failure in the RBA system may cause the system to apply the brakes when no object is in the bus's path.

- Prevent excessive vehicle deceleration or braking under all operating conditions through design and validation techniques in accordance with the ASIL A classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the RBA system commanding excessive vehicle deceleration or braking. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the RBA system commanding excessive vehicle deceleration or braking cannot be prevented, then detect and mitigate the fault.
- Prevent unintended activation of the RBA system, including activation of the RBA system when the transmission is not in the reverse position.
- Ensure the validity and correctness of signals provided by the environmental sensors and other critical sensors for the RBA system.
- Ensure the validity and correctness of communication signals from other vehicle systems to the RBA system.
- If a failure that could lead to excessive vehicle deceleration or braking occurs, transition into a safe state within the FTTI.

- If a failure that could lead to excessive vehicle deceleration or braking occurs, warn the driver and communicate any necessary actions to the driver (e.g., manually disengage the system).

Safety Goal, Rear Brake Assist–4

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to insufficient vehicle deceleration or braking by the RBA system. For example, a failure may cause the RBA system to command less braking than necessary to slow the bus when an object is detected.

- Ensure that the system provides the correct level of deceleration or braking through design and validation techniques in accordance with the QM[54] classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the RBA system commanding insufficient vehicle deceleration or braking. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the RBA system commanding insufficient vehicle deceleration or braking cannot be prevented, then detect and mitigate the fault.
- Ensure the validity and correctness of signals provided by the environmental sensors and other critical sensors for the RBA system.
- Acknowledge all faults communicated by other vehicle systems that may prevent the vehicle from achieving the intended decrease in speed, including faults communicated by the powertrain system or the braking system.
- If a failure that could lead to insufficient vehicle deceleration or braking occurs, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.

[54] Note that safety goals assigned "QM" typically are not shown in the functional safety concept, as internal quality management processes rather than ISO 26262 concepts apply to these safety goals. However, in this study, these safety goals are shown for completeness.

- If a failure that could lead to insufficient vehicle deceleration or braking occurs, warn the driver and communicate any necessary actions to the driver.

Safety Goal, Rear Brake Assist–5

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to loss of vehicle deceleration or braking by the RBA system. For example, a failure may prevent the RBA system from applying the brakes at the final TTC threshold.

- Prevent loss of vehicle deceleration or braking through design and validation techniques in accordance with the ASIL A classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could prevent the RBA system from applying the brakes at the final TCC threshold. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to loss of vehicle deceleration or braking cannot be prevented, then detect and mitigate the fault.
- Acknowledge all faults communicated by other vehicle systems that may prevent the vehicle from achieving the intended decrease in speed, including faults communicated by the braking system.
- If a failure that could lead to loss of vehicle deceleration or braking occurs, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.
- If a failure that could lead to loss of vehicle deceleration or braking occurs, warn the driver and communicate any necessary actions to the driver (e.g., apply the brakes).

Safety Goal, Rear Brake Assist–6

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to inadequate alerting of the driver. For example, a failure may prevent the RBA system from issuing a driver alert at the appropriate TTC thresholds.

- Ensure that the system issues driver alerts through design and validation techniques in accordance with the QM[55] classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could prevent the RBA system from issuing driver alerts at the appropriate TCC thresholds. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to inadequate alerting of the driver cannot be prevented, then detect and mitigate the fault.
- Ensure the validity and correctness of signals provided by the environmental sensors and other critical sensors for the RBA system.
- Acknowledge all faults communicated by other vehicle systems that may prevent the system from alerting the driver, including faults communicated by the instrument panel and head unit systems.
- If a failure that could lead to inadequate alerting of the driver occurs, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.

Safety Goal, Rear Brake Assist–7

These safety goals are intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to improper transition of control between the driver and the RBA system. For example, a failure may affect the RBA system status notification to the driver.

- Ensure that the system status is properly conveyed to the driver through design and validation techniques in accordance with the QM[56] classification.
- Ensure that the driver is capable of overriding the system through design and validation techniques in accordance with the ASIL A classification.

These safety goals are common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

---

[55] Note that safety goals assigned "QM" typically are not shown in the functional safety concept, as internal quality management processes rather than ISO 26262 concepts apply to these safety goals. However, in this study, these safety goals are shown for completeness.

[56] *Ibid.*

General Safety Strategy Considerations

Top-level considerations to help achieve these safety goals:

- Prevent all faults that could prevent RBA system override or displaying the RBA system status. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that could prevent RBA system override or displaying the RBA system status cannot be prevented, then detect and mitigate the fault.
- Acknowledge all faults communicated by other vehicle systems that may prevent RBA system override or displaying the RBA system status, including faults communicated by the braking system, instrument panel, and head unit systems.
- If a failure that could prevent RBA system override or displaying the RBA system status, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.
- If a failure that could prevent RBA system override or displaying the RBA system status, warn the driver and communicate any necessary actions to the driver.

Potential Safe States

For the RBA system, potential safe states include:

- Limit system operation to braking-only. (Relevant Rear Brake Assist Safety Goals: 6)
  - The driver should be notified of the limited operation.
- Limit system operation to operating scenarios that can be supported with only one sensor type. (Relevant Rear Brake Assist Safety Goals: 1, 2, 3, 4, 5)
  - In these operating scenarios, the system would have sufficient confidence in the data provided by one sensor type to safely activate.
  - The driver should be notified of the limited operation.
- Issue all notifications through multiple channels (e.g., visual and audio). (Relevant Rear Brake Assist Safety Goals: 7)
- Disable active braking and provide warnings via a brake jerk and the HMI. (Relevant Rear Brake Assist Safety Goals: 2, 4, 5, 6, 7)
  - The driver should be notified of the limited operation.
- Disable active braking and provide warnings via the HMI only. (Relevant Rear Brake Assist Safety Goals: All)
  - The driver should be notified of the limited operation.

Traffic Jam Assist

Safety Goal, Traffic Jam Assist–1

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to the TJA system commanding excessive vehicle propulsion. For example, excessive vehicle propulsion may occur from failures that cause the TJA system to command additional propulsion when the lead vehicle is stopped.

- Prevent excessive vehicle propulsion under all operating conditions through design and validation techniques in accordance with the C classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification below may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the TJA system commanding excessive vehicle propulsion. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the TJA system commanding excessive vehicle propulsion cannot be prevented, then detect and mitigate the fault.
- When the TJA system is active, prevent all faults that increase propulsion torque when additional propulsion is not requested by the driver, the TJA system, or higher priority safety systems.
- Prevent unintended activation of the TJA system.
- Ensure the validity and correctness of signals provided by the environmental sensors and other critical sensors for the TJA system.
- Ensure the validity and correctness of communication signals from other vehicle systems to the TJA system.
- If a failure that could lead to excessive vehicle propulsion occurs, transition into a safe state within the FTTI.
- If a failure that could lead to excessive vehicle propulsion occurs, warn the driver and communicate any necessary actions to the driver (e.g., manually disengage the system).
- Ensure that the acceleration resulting from failures[57] does not exceed TBD m/s^2. The allowable acceleration should be determined so that it does

[57] Establishing an acceptable acceleration rate for nominal system performance that ensures the safety of passengers and the driver would be part of the system design and would not be covered by ISO 26262.

not cause displacement of unsecured standing or seated passengers, or displacement of objects in a way that could cause harm to the passengers or driver.

Safety Goal, Traffic Jam Assist–2

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to insufficient vehicle propulsion by the TJA system. For example, insufficient vehicle propulsion could result from failures that cause the TJA system to receive less propulsion than requested.

- Ensure that the system provides the correct level of propulsion through design and validation techniques in accordance with the ASIL A classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the TJA system commanding insufficient vehicle propulsion. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the TJA system commanding insufficient vehicle propulsion cannot be prevented, then detect and mitigate the fault.
- Ensure the validity and correctness of signals provided by the environmental sensors and other critical sensors for the TJA system.
- Acknowledge all faults communicated by other vehicle systems that may prevent the vehicle from achieving the intended increase in speed, including faults communicated by the powertrain system.
- If a failure that could lead to insufficient vehicle propulsion occurs, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.
- If a failure that could lead to insufficient vehicle propulsion occurs, warn the driver and communicate any necessary actions to the driver.

Safety Goal, Traffic Jam Assist–3

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to the TJA system causing loss of vehicle propulsion. For example, loss of vehicle propulsion may result from failures that cause the stop-and-go system to shut off the engine while the vehicle is moving at higher speeds.

- Prevent the stop-and-go subsystem from shutting off the engine while the vehicle is in motion through design and validation techniques in accordance with the QM[58] classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the TJA system shutting off the engine while the vehicle is in motion. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the TJA system shutting off the engine while the vehicle is in motion cannot be prevented, then detect and mitigate the fault.
- Ensure the validity and correctness of signals provided by the environmental sensors and other critical sensors for the TJA system.
- Acknowledge all faults communicated by other vehicle systems that may cause propulsion loss, including the powertrain system.
- If a failure that could lead to loss of vehicle propulsion occurs, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.
- If a failure that could lead to loss of vehicle propulsion occurs, warn the driver and communicate any necessary actions to the driver (e.g., manually disengage the system).

Safety Goal, Traffic Jam Assist–4

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to the TJA system commanding vehicle movement in the wrong longitudinal direction. This safety goal is only applicable for TJA systems with the stop-and-go feature equipped on buses with electric powertrains. For example, a failure may cause an electric powertrain to incorrectly execute the TJA system commands in the reverse direction.

- Ensure that vehicle motion occurs in the intended longitudinal direction through design and validation techniques in accordance with the ASIL A classification.

[58] Note that safety goals assigned "QM" typically are not shown in the functional safety concept, as internal quality management processes rather than ISO 26262 concepts apply to these safety goals. However, in this study, these safety goals are shown for completeness.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Acknowledge all faults communicated by other vehicle systems that may cause the propulsion system to provide propulsion in the wrong direction, including the powertrain system.
- Prevent propulsion commands from the TJA system when the transmission is in a position other than drive.
- If a failure that could lead to vehicle movement in the wrong direction occurs, transition into a safe state within the FTTI.
- If a failure that could lead to vehicle movement in the wrong direction occurs, warn the driver and communicate any necessary actions to the driver (e.g., apply the brakes).

Safety Goal, Traffic Jam Assist–5

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to the TJA system commanding excessive vehicle deceleration or braking. For example, a failure may cause the TJA system to decelerate the vehicle more than necessary for the driving situation.

- Prevent excessive vehicle deceleration or braking under all operating conditions through design and validation techniques in accordance with the ASIL A classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the TJA system commanding excessive vehicle deceleration or braking. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the TJA system commanding excessive vehicle deceleration or braking cannot be prevented, then detect and mitigate the fault.
- Prevent unintended activation of the TJA system.

- Ensure the validity and correctness of signals provided by the environmental sensors and other critical sensors for the TJA system.
- Ensure the validity and correctness of communication signals from other vehicle systems to the TJA system.
- When the TJA system is active, prevent all faults that cause deceleration or braking when deceleration is not requested by either the driver, the TJA system, or higher priority safety systems.
- Ensure that the vehicle speed is zero before shutting off the engine.
- If a failure that could lead to excessive vehicle deceleration or braking occurs, transition into a safe state within the FTTI.
- If a failure that could lead to excessive vehicle deceleration or braking occurs, warn the driver and communicate any necessary actions to the driver (e.g., manually disengage the system).
- Ensure that deceleration resulting from failures[59] does not exceed TBD m/s^2. The allowable deceleration should be determined so that it does not cause displacement of unsecured standing or seated passengers, or the displacement of objects in a way that could cause harm to the passengers or driver.

Safety Goal, Traffic Jam Assist–6

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to insufficient vehicle deceleration or braking by the TJA system. For example, a failure may cause the TJA system to command less braking than necessary to sufficiently slow the bus as it approaches the lead vehicle.

- Ensure that the system provides the correct level of deceleration or braking through design and validation techniques in accordance with the QM[60] classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the TJA system commanding insufficient vehicle deceleration or braking. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.

[59] Establishing an acceptable deceleration rate for nominal system performance that ensures the safety of passengers and the driver would be part of the system design and would not be covered by ISO 26262.

  - If a fault that leads to the TJA system commanding insufficient vehicle deceleration or braking cannot be prevented, then detect and mitigate the fault.
- Ensure the validity and correctness of signals provided by the environmental sensors and other critical sensors for the TJA system.
- Acknowledge all faults communicated by other vehicle systems that may prevent the vehicle from achieving the intended decrease in speed, including faults communicated by the powertrain system or the braking system.
- If a failure that could lead to insufficient vehicle deceleration or braking occurs, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.

If a failure that could lead to insufficient vehicle deceleration or braking occurs, warn the driver and communicate any necessary actions to the driver (e.g., apply the brakes).

Safety Goal, Traffic Jam Assist–7

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could prevent the TJA system from stopping the vehicle at zero speed. For example, a failure in the stop-and-go subsystem may cause a delay in shutting off the engine when the bus is stopped.

- Prevent loss of deceleration or braking through design and validation techniques in accordance with the ASIL B classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the TJA system incorrectly stopping the engine or inadvertently restarting the engine when the vehicle is stopped. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the TJA system commanding insufficient vehicle deceleration or braking cannot be prevented, then detect and mitigate the fault.

[60] Note that safety goals assigned "QM" typically are not shown in the functional safety concept, as internal quality management processes rather than ISO 26262 concepts apply to these safety goals. However, in this study, these safety goals are shown for completeness.

- Acknowledge all faults communicated by other vehicle systems that may prevent the vehicle from properly stopping the engine, including faults communicated by the powertrain system and brake system.
- If a failure that could prevent the vehicle from stopping at zero speed occurs, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.
- If a failure that could prevent the vehicle from stopping at zero speed occurs, warn the driver and communicate any necessary actions to the driver (e.g., apply the brakes).

Safety Goal, Traffic Jam Assist–8

These safety goals are intended to establish a set of safety requirements that detect and mitigate potential failures that could cause the vehicle to roll away when the TJA system is active. For example, in system designs where the TJA system engages the parking brake during prolonged stops, a failure may allow the TJA system to disengage the parking brake before the service brake is re-engaged.

- Prevent vehicle rollaway under all operating conditions through design and validation techniques in accordance with the QM[61] classification.
- Prevent unintended vehicle motion under all operating conditions through design and validation techniques in accordance with the QM[62] classification.

These safety goals are common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

- Top-level considerations to help achieve these safety goals include:
- Prevent all faults that could lead to the TJA system allowing the vehicle to roll away. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the TJA system allowing the vehicle to roll away cannot be prevented, then detect and mitigate the fault.
- Acknowledge all faults communicated by other vehicle systems that may prevent the vehicle from remaining stopped, including faults communicated by the powertrain system and braking system.
- If a failure that could lead to the vehicle rolling away occurs, transition into a safe state within the FTTI.

[61] Note that safety goals assigned "QM" typically are not shown in the functional safety concept, as internal quality management processes rather than ISO 26262 concepts apply to these safety goals. However, in this study, these safety goals are shown for completeness.

[62] *Ibid.*

  - Ensure that sufficient power is provided to the system to allow transition into the safe state.
- If a failure that could lead to the vehicle rolling away occurs, warn the driver and communicate any necessary actions to the driver (e.g., apply the brakes).

Safety Goal, Traffic Jam Assist–9

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to the TJA system commanding excessive lateral motion. For example, excessive lateral motion may occur from failures that cause the TJA system to command sudden steering when the roadway is straight.

- Prevent excessive lateral motion/yaw through design and validation techniques in accordance with the ASIL B classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the TJA system commanding excessive lateral motion/yaw. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the TJA system commanding excessive lateral motion/yaw cannot be prevented, then detect and mitigate the fault.
- When the TJA system is active, prevent all faults that increase steering torque when additional steering is not requested by the driver, the TJA system, or higher priority safety systems.
- Prevent unintended activation of the TJA system.
- Ensure the validity and correctness of signals provided by the environmental sensors and other critical sensors for the TJA system.
- Ensure the validity and correctness of communication signals from other vehicle systems to the TJA system.
- If a failure that could lead to excessive lateral motion/yaw occurs, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.
- If a failure that could lead to excessive lateral motion/yaw occurs, warn the driver and communicate any necessary actions to the driver (e.g., manually disengage the system).

Safety Goal, Traffic Jam Assist–10

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to insufficient lateral motion by the TJA system. For example, insufficient lateral motion may occur from failures that cause the TJA system to command less steering than needed to follow the road curvature.

- Ensure that the system provides the correct level of lateral motion/yaw through design and validation techniques in accordance with the ASIL B classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the TJA system commanding insufficient lateral motion/yaw. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the TJA system commanding insufficient lateral motion/yaw cannot be prevented, then detect and mitigate the fault.
- Ensure the validity and correctness of signals provided by the environmental sensors and other critical sensors for the TJA system.
- Acknowledge all faults communicated by other vehicle systems that may prevent the vehicle from achieving the intended level of steering, including faults communicated by the steering system and braking system.
- If a failure that could lead to insufficient lateral motion/yaw occurs, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.
- If a failure that could lead to insufficient lateral motion/yaw occurs, warn the driver and communicate any necessary actions to the driver (e.g., resume steering).

Safety Goal, Traffic Jam Assist–11

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to the TJA system commanding vehicle movement in the wrong lateral direction. For example, a failure might cause the TJA system to issue a steering command in the opposite direction of the road curvature.

- Ensure that lateral motion/yaw is provided in the correct direction through design and validation techniques in accordance with the ASIL C classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to the TJA system commanding lateral motion/yaw in the wrong direction. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to the TJA system commanding lateral motion/yaw in the wrong direction cannot be prevented, then detect and mitigate the fault.
- Ensure the validity and correctness of signals provided by the environmental sensors and other critical sensors for the TJA system.
- If a failure that could lead to lateral motion/yaw in the wrong direction occurs, transition into a safe state within the FTTI.
- If a failure that could lead to lateral motion/yaw in the wrong direction occurs, warn the driver and communicate any necessary actions to the driver (e.g., manually disengage the system).

Safety Goal, Traffic Jam Assist–12

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could allow the TJA system to continue providing propulsion while the passenger door is open. For example, a failure may prevent the TJA system from recognizing that the passenger door was inadvertently opened.

- Prevent continued vehicle motion while the passenger door is open through design and validation techniques in accordance with the ASIL A classification.

This safety goal is specific to transit buses, since light vehicles do not have centrally-operated passenger doors.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could prevent the TJA system from determining the passenger door state.[63] Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.

[63] This assumes that the ACC system design includes measures to prevent vehicle motion when the doors are open during nominal (i.e., unfaulted) operation.

  - If a fault that could prevent the TJA system from determining the passenger door state cannot be prevented, then detect and mitigate the fault.
- Acknowledge all faults communicated by other vehicle systems that may prevent the TJA system from responding to an open passenger door, including faults communicated by the door control system.
- If a failure that could allow the bus to continue moving while the passenger door is open occurs, transition into a safe state within the FTTI.
- If a failure that could allow the bus to continue moving while the passenger door is open occurs, warn the driver and communicate any necessary actions to the driver (e.g., close the passenger door).
- Communication of the passenger door state from the door control system to the TJA system should be designed and validated in accordance with the specified ASIL.

Safety Goal, Traffic Jam Assist–13

This safety goal is intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to a lane or roadway departure while the TJA system is engaged. For example, a failure might prevent the TJA system from recognizing that the vehicle is approaching a lane boundary.

- Prevent a lane or roadway departure while the system is engaged through design and validation techniques in accordance with the ASIL C classification.

This safety goal is common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve this safety goal include:

- Prevent all faults that could lead to a lane or roadway departure while the TJA system is engaged. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that leads to a lane or roadway departure while the TJA system is engaged cannot be prevented, then detect and mitigate the fault.
- Ensure the validity and correctness of signals provided by the environmental sensors and other critical sensors for the TJA system.
- Acknowledge all faults communicated by other vehicle systems that may lead to a lane or roadway departure while the TJA system is engaged, including faults communicated by the steering system and braking system.
- If a failure occurs that could lead to a lane or roadway departure while the TJA system is engaged, transition into a safe state within the FTTI.

  - Ensure that sufficient power is provided to the system to allow transition into the safe state.
- If a failure occurs that could lead to a lane or roadway departure while the TJA system is engaged, warn the driver and communicate any necessary actions to the driver (e.g., resume steering).

Safety Goal, Traffic Jam Assist–14

These safety goals are intended to establish a set of safety requirements that detect and mitigate potential failures that could lead to improper transition of control between the driver and the TJA system. For example, a failure may affect the TJA system status notification to the driver.

- Ensure that the system status is properly conveyed to the driver through design and validation techniques in accordance with the ASIL A classification.
- Ensure that the driver is capable of overriding the system through design and validation techniques in accordance with the ASIL A classification.

These safety goals are common to both transit buses and light vehicles, although the ASIL classification specified may be different in light vehicles.

General Safety Strategy Considerations

Top-level considerations to help achieve these safety goals include:

- Prevent all faults that could prevent the TJA system from responding to the driver's request or displaying the TJA system status. Such faults and their root causes may be determined through a comprehensive safety analysis in accordance with ISO 26262.
  - If a fault that could prevent the TJA system from responding to the driver's request or displaying the TJA system status cannot be prevented, then detect and mitigate the fault.
- Acknowledge all faults communicated by other vehicle systems that may prevent the TJA system from responding to the driver's request or displaying the TJA system status, including faults communicated by the instrument panel and head unit systems.
- If a failure that could prevent the TJA system from responding to the driver's request or displaying the TJA system status occurs, transition into a safe state within the FTTI.
  - Ensure that sufficient power is provided to the system to allow transition into the safe state.

- If a failure that could prevent the TJA system from responding to the driver's request or displaying the TJA system status occurs, warn the driver and communicate any necessary actions to the driver.

Potential Safe States

For the TJA system, potential safe states could be achieved through driver takeover via a tiered system disengagement, such as:

- Limit system operation to longitudinal control only. (Relevant Traffic Jam Assist Safety Goals: 9, 10, 11, 13)
  - The driver should be notified of the limited operation.
- Limit system operation to lateral control only. (Relevant Traffic Jam Assist Safety Goals: 1, 2, 4, 5, 6)
  - The driver should be notified of the limited operation.
- Issue all notifications through multiple channels (e.g., visual and audio). (Relevant Traffic Jam Assist Safety Goals: 14)
- Disable the system and return control back to the driver. (Relevant Traffic Jam Assist Safety Goals: All)
  - The driver should be notified of system disengagement.
  - The system should command zero propulsion input.

APPENDIX H

Example Functional Safety Measures

Adaptive Cruise Control

- Safety Goal(s): "Prevent excessive vehicle propulsion under all vehicle operating conditions" and "prevent excessive vehicle deceleration or braking under all operating conditions."
  - Check the ACC system's critical calibration parameters every key cycle.
  - Verify the correctness of measured vehicle dynamics.
  - Verify the correctness of the vehicle acceleration profile.
  - Verify the correctness of the acceleration rate limit for the ACC system.
  - Verify the correctness of the vehicle deceleration profile.
  - Verify the correctness of the deceleration rate limit for the ACC system.
  - Ensure that the correct speed profile is selected at all times depending on the passenger and cargo status.
- Safety Goal(s): "Prevent continued vehicle motion while the passenger door is open."
  - Ensure that the ACC system controller detects right passenger door state at all times.
  - Ensure that the correct door state is communicated to the ACC controller at all times.
  - Detect loss of signal from the door control module to the ACC controller.
  - Detect intermittent connections between the door control system and ACC system.
  - Monitor the response time of the ACC controller to changes in the passenger door status. If the response time threshold is exceeded, alert the driver and/or transition to the appropriate safe state.
  - Monitor the timing of the passenger door status signal to the ACC controller. If the signal is delayed, alert the driver and/or transition to the appropriate safe state.

Automatic Emergency Braking

- Safety Goal(s): "Prevent excessive vehicle deceleration or braking under all operating conditions."
  - Ensure that the TTC thresholds are correct at every key cycle.

  - Ensure that the relevant vehicle state parameters are correct when communicated to the AEB system at all times.
  - Ensure that the relevant vehicle dynamics parameters are correct when communicated to the AEB system.
  - Ensure that the deceleration limits are correct are every key cycle.
  - Verify that the correct amount of additional braking is provided
  - Verify that the magnitude of the brake jerk is correct.

Docking

- Safety Goal(s): "Ensure that the vehicle stops at the driver-specified distance from the curb at a bus station/stop."
  - Check the correctness of the calibration parameters for sensor height every key cycle.
  - Validate the distance between the bus and the curb.
  - Verify the driver-specified distance from the curb.
  - Verify the bus alignment relative to the curb.
  - Verify the presence of any objects that may affect the ability of the docking system to steer the vehicle to the designated distance from the curb.
  - Ensure that system correctly issues the command to suspend the LK/LC system.
  - Verify the correctness of any requests to suspend the LK/LC system.
  - Detect intermittent communication with the LK/LC system when the docking system is active.

Full Park Assist/ Valet Parking

- Safety Goal(s): "Prevent excessive lateral motion/yaw."
  - Verify that the distance between the bus and the curb is correct.
  - Ensure that sensors can detect the correct location of the curb even in the event of a hardware failure.
- Safety Goal(s): "Prevent excessive lateral motion/yaw" and "prevent insufficient vehicle deceleration or braking under all vehicle operating conditions."
  - Ensure that sensors can detect the boundary of the parking spot even in the event of a hardware failure.

Lane Keeping/ Lane Centering/ Steering Assist

- Safety Goal(s): "Prevent excessive lateral motion/yaw."
  - Prevent all failures in the lane keeping/lane centering/steering assist system that does not allow it to respond to suspension requests from the docking system.
  - Verify that the system has correct lateral acceleration threshold every key cycle.

Object Detection and Collision Avoidance

No transit bus specific functional safety requirements were identified for this system.

Park Assist/ Park Out

- Safety Goal(s): "Prevent excessive lateral motion/yaw."
  - Verify that the distance between the bus and the curb is correct.
  - Ensure that sensors can detect the correct location of the curb even in the event of a hardware failure.

Rear Brake Assist

- Safety Goal(s): "Prevent excessive vehicle deceleration or braking under all operating conditions."
  - Ensure that the TTC thresholds are correct at every key cycle.
  - Ensure that the relevant vehicle state parameters are correct when communicated to the rear brake assist system at all times.
  - Ensure that the relevant vehicle dynamics parameters are correct when communicated to the rear brake assist system.
  - Ensure that the deceleration limits are correct are every key cycle.
  - Verify that the correct amount of additional braking is provided
  - Verify that the magnitude of the brake jerk is correct.

Traffic Jam Assist

- Safety Goal(s): "Prevent excessive vehicle propulsion under all vehicle operating conditions" and "prevent excessive vehicle deceleration or braking under all operating conditions."
  - Check the TJA system's critical calibration parameters every key cycle.
  - Verify the correctness of measured vehicle dynamics.
  - Verify the correctness of the vehicle acceleration profile.
  - Verify the correctness of the acceleration rate limit for the TJA system.
  - Verify the correctness of the vehicle deceleration profile.

  - Verify the correctness of the deceleration rate limit for the TJA system.
  - Ensure that the correct speed profile is selected at all times depending on the passenger and cargo status.
- Safety Goal(s): "Prevent continued vehicle motion while the passenger door is open."
  - Ensure that the TJA system controller detects right passenger door state at all times.
  - Ensure that the correct door state is communicated to the TJA controller at all times.
  - Detect loss of signal from the door control module to the TJA controller.
  - Detect intermittent connections between the door control system and TJA system.
  - Monitor the response time of the TJA controller to changes in the passenger door status. If the response time threshold is exceeded, alert the driver and/or transition to the appropriate safe state.
  - Monitor the timing of the passenger door status signal to the TJA controller. If the signal is delayed, alert the driver and/or transition to the appropriate safe state.
- Safety Goal(s): "Prevent excessive lateral motion/yaw."
  - Prevent all failures in the TJA system that does not allow it to respond to suspension requests from the docking system.
  - Verify that the system has correct lateral acceleration threshold every key cycle.

Acronyms/Abbreviations

ACC	Adaptive cruise control
AEB	automatic emergency braking
APTA	American Public Transportation Association
ASIL	Automotive Safety Integrity Level
E/E	Electrical and electronic
FMVSS	Federal Motor Vehicle Safety Standard
FTTI	Fault tolerant time interval
HARA	Hazard analysis and risk assessment
HAZOP	Hazard and Operability Analysis
HMI	Human-machine interface
ISO	International Organization for Standardization
OEM	Original equipment manufacturer
QM	Quality management
SAE	SAE International (formerly Society of Automotive Engineers)
SME	Subject matter expert
STPA	Systems-Theoretic Process Analysis
TJA	Traffic jam assist
TTC	Time-to-collision
UCA	Unsafe control action
VRU	Vulnerable road user

REFERENCES

[1] A. Nasser, J. Brewer, W. Najm, and J. Cregger, *Transit Bus Automation Project: Transferability of Automation Technologies Final Report*. Washington, DC: Federal Transit Administration, 2018.

[2] SAE International, *Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems (SAE J3016)*. Warrendale, PA: SAE International, 2018.

[3] International Organization for Standardization, *ISO 26262: Road Vehicles—Functional Safety*. Geneva: 2018.

[4] Department of Defense, *Department of Defense Standard Practice: System Safety (MIL-STD-882E)*, 2012.

[5] International Electrotechnical Commission, *IEC 61882: Hazard and Operability Studies (HAZOP Studies) – Application Guide*, 2001-05, Edition 1.0.

[6] N. Leveson, *Engineering a Safer World*, Cambridge: MIT Press, 2012.

[7] American Public Transit Association, *Standard Bus Procurement Guidelines*, Washington, DC, 2013.

[8] R. Schubert and M. Obst, "The Role of Multisensor Environmental Perception for Automated Driving," in *Automated Driving: Safer and More Efficient Future Driving*. Switzerland: Springer International Publishing, 2017, pp. 161-182.

[9] SAE International, *Considerations for ISO 26262 ASIL Hazard Classification (SAE J2980)*. Warrendale, PA: 2015.

[10] J. Brewer, C. Becker, L. Yount, and J. Pollard, "Functional Safety Assessment of a Generic Automated Lane Centering (ALC) System and Related Foundational Vehicle Systems." Washington, DC: National Highway Traffic Safety Administration, 2018.

[11] Volpe National Transportation Systems Center, *Transit Bus Automation: Technology Packages and Use Cases*. Washington, DC: Federal Transit Administration, 2018.

[12] J. Becker, M. Helmle, and O. Pink, "System Architecture and Safety Requirements for Automated Driving," in *Automated Driving: Safer and More Efficient Future Driving*. Geneva: Springer International Publishing, 2017, pp. 265-283.

[13] R. Vincelli and T. Yasumasu, "Mastering Functional SAfety and ISO-26262." Orange County, CA: Renesas Electronics America, Inc., 2012.

[14] C. N. Abernethy, H. H. Jacobs, G. R. Plank, J. H. Stoklosa, and E. D. Sussman, "Maximum Deceleration and Jerk Levels that Allow Retention of Unrestrained, Seated Transit Passengers." *Evaluation*, 1(10), 1980.

[15] J. H. J. Allum, "Organization of Stabilizing Reflex Responses in Tibialis Anterior Muscles Following Ankle Felxion Perturbations of Standing Man." *Brain Research*, 264(2), pp. 297-301, 1983.

[16] C. F. Hirshfeld, "Disturbing Effects of Horizontal Acceleration." *Electric Railway Presidents' Conference Committee*, 1932.

[17] L. L. Hoberock, "A Survey of Longitudinal Acceleration Comfort Studies in Ground Transportation Vehicles." *Journal of Dynamic Systems, Measurement, and Control*, 99(2), pp. 76-84, 1977.

[18] B. E. Maki, "A System Identification Approach to Balance Testing." *Progress in Brain Research*, 76, pp. 297-306, 1988.

[19] J. P. Powell and R. Palacin, "Passenger Stability within Moving Railway Vehicles: Limits on Maximum Longitudinal Acceleration." *Urban Rail Transit*, 1(2), pp. 95-103, 2015.

[20] M. Simoneau and P. Corbeil, "The Effect of Time to Peak Ankle Torque on Balance Stability Boundary: Experimental Validation of a Biomechanical Model." *Experimental Brain Research*, 165(2), pp. 217-228, 2005.

[21] National Association of City Transportation Officials, "Vehicle Widths and Buffers," 2019, https://nacto.org/publication/transit-street-design-guide/transit-lanes-transitways/lane-design-controls/vehicle-widths-buffers/. Accessed 27 December 2019.

[22] National HIghway Traffic Safety Administration, Federal Motor Vehicle Standard No. 105– Hydraulic and Electric Brake Systems. Washington, DC, 49 CFR Ch.V 157.105, 2011.

[23] National HIghway Traffic Safety Administration, Federal Motor Vehicle Standard No. 121–Air Brake Systems. Washington, DC, 49 CFR 517.121.

[24] International Organization for Standardization, *Pas 21448: Road Vehicles—Safety of the Intended Functionality*. Geneva: 2019.

[25] National HIghway Traffic Safety Administration, "Rollover | Safercar," 2019, https://www.safercar.gov/Vehicle-Shoppers/Rollover. Accessed 15 July 2019.

[26] A. Constant and E. Lagarde, "Protecting Vulnerable Road Users from Injury." *PLoS Medicine*, 7(3), 30 March 2010.

U.S. Department of Transportation

Federal Transit Administration

U.S. Department of Transportation
Federal Transit Administration
East Building
1200 New Jersey Avenue, SE
Washington, DC 20590
https://www.transit.dot.gov/about/research-innovation