RESEARCH REPORT

Institute of Transportation Studies | UNIVERSITY OF CALIFORNIA

Risk Assessment for Remote Operation of Level 4 Automated Driving Systems

Jiaqi Ma, Associate Professor, UCLA Mobility Lab, UCLA
Camila Correa Jullian, PhD Student, UCLA Mobility Lab/Risk Institute, UCLA
Marilia Ramos, Assistant Researcher, UCLA Mobility Lab/Risk Institute, UCLA
Xin Xia, Assistant Project Scientist, UCLA Mobility Lab, UCLA

May 2024

California Resilient and Innovative Mobility Initiative

Report No.: UC-ITS-RIMI-5K | DOI: 10.7922/G23N21QC

Technical Report Documentation Page

1. Report No. UC-ITS-RIMI-5K	**2. Government Accession No.** N/A	**3. Recipient's Catalog No.** N/A
4. Title and Subtitle Risk Assessment for Remotely Operation of Level 4 Automated Driving Systems in Mobility as a Service Transport		**5. Report Date** May 2024 **6. Performing Organization Code** UCLA
7. Author(s) Jiaqi Ma, Associate Professor, UCLA Mobility Lab, UCLA; Camila Correa Jullian, PhD Student, UCLA Mobility Lab/Risk Institute, UCLA; Marilia Ramos, Assistant Researcher, UCLA Mobility Lab/Risk Institute, UCLA. Xin Xia, Assistant Project Scientist, UCLA Mobility Lab, UCLA		**8. Performing Organization Report No.** N/A
9. Performing Organization Name and Address Institute of Transportation Studies, UCLA 3320 Public Affairs Building Los Angeles, CA 90095-1656		**10. Work Unit No.** N/A **11. Contract or Grant No.** UC-ITS-RIMI-5K
12. Sponsoring Agency Name and Address The University of California Institute of Transportation Studies www.ucits.org		**13. Type of Report and Period Covered** Final Report (07/2022 – 06/2023) **14. Sponsoring Agency Code** UC ITS

15. Supplementary Notes
DOI:10.7922/G23N21QC

16. Abstract

The recent technological advances in Automated Driving Systems (ADS) have fueled interest in the use and impact of vehicle fleets involved in driverless passenger transport services. This research identifies key safety risks associated Level 4 ADS-equipped vehicle operation for fleets employed for Mobility as a Service (MaaS) applications. The study goes beyond assessing the functional safety of the ADS-equipped vehicles to explore the role of fleet operators in ensuring the operational safety of the vehicle fleets through remote driving assistance functions. This work identifies key responsibilities of the fleet operators in implementing risk reduction measures related to organizational management of change, training remote supervisors, ensuring suitable working conditions, enforcing vehicle connectivity and dispatching requirements, and coordinating incident mitigation procedures, training, tools, and work conditions. The study employs a hazard identification methodology that combines traditional and innovative methods to analyze risks involving human, software, and hardware systems. The study identified twenty hazard scenarios arising from system failures, human errors, and unsafe interactions during different operational phases. These are ranked based on their impact on safety and resource intensity, enabling fleet operators to make better decisions regarding resource allocation. By implementing these actions, fleet operators can prevent and mitigate safety hazards in the operation of ADS-equipped fleets though remote monitoring and driving assistance functions. The hazards and risk mitigation activities identified in this report may also improve the operational safety of passenger vehicles equipped with ADS technology as they become more widely deployed in future large-scale commercial operations.

17. Key Words Level 4 driving automation, risk assessment, hazard analysis, fleet management, automated vehicle control, remote control, traffic safety, computer models		**18. Distribution Statement** No restrictions.	
19. Security Classification (of this report) Unclassified	**20. Security Classification (of this page)** Unclassified	**21. No. of Pages** 78	**22. Price** N/A

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

The UC Institute of Transportation Studies

The University of California Institute of Transportation Studies (UC ITS) is a network of faculty, research and administrative staff, and students dedicated to advancing the state of the art in transportation engineering, planning, and policy for the people of California. Established by the Legislature in 1947, ITS has branches at UC Berkeley, UC Davis, UC Irvine, and UCLA.

The California Resilient and Innovative Mobility Initiative

The California Resilient and Innovative Mobility Initiative (RIMI) serves as a living laboratory – bringing together university experts from across the four UC ITS campuses, policymakers, public agencies, industry stakeholders, and community leaders – to inform the state transportation system's immediate COVID-19 response and recovery needs, while establishing a long-term vision and pathway for directing innovative mobility to develop sustainable and resilient transportation in California. RIMI is organized around three core research pillars: Carbon Neutral Transportation, Emerging Transportation Technology, and Public Transit and Shared Mobility. Equity and high-road jobs serve as cross-cutting themes that are integrated across the three pillars.

Acknowledgments

This study was made possible with funding received by the Resilient and Innovative Mobility Initiative from the State of California through a one-time General Fund allocation included in the 2021 State Budget Act. The authors would like to thank the State of California for its support of university-based research, and especially for the funding received for this project. The authors would also like to thank our collaborators at the UCLA Mobility Lab (Letian Gao and Xu Han) and the UCLA Risk Institute (Ali Mosleh).

Disclaimer

The contents of this report reflect the views of the authors, who are responsible for the facts and the accuracy of the information presented herein. This document is disseminated under the sponsorship of the State of California in the interest of information exchange. The State of California assumes no liability for the contents or use thereof. Nor does the content necessarily reflect the official views or policies of the State of California. This report does not constitute a standard, specification, or regulation.

Institute of Transportation Studies | UNIVERSITY OF CALIFORNIA

Risk Assessment for Remote Operation of Level 4 Automated Driving Systems

Jiaqi Ma, Associate Professor, UCLA Mobility Lab, UCLA
Camila Correa Jullian, PhD Student, UCLA Mobility Lab/Risk Institute, UCLA
Marilia Ramos, Assistant Researcher, UCLA Mobility Lab/Risk Institute, UCLA
Xin Xia, Assistant Project Scientist, UCLA Mobility Lab, UCLA

May 2024

California Resilient and Innovative Mobility Initiative

Report No.: UC-ITS-RIMI-5K | DOI: 10.7922/G23N21QC

Table of Contents

Table of Contents

List of Tables

List of Figures

Abbreviations

ADS	Automated Driving System
BNs	Bayesian Networks
CoTA	Concurrent Task Analysis
DDTs	Dynamic Driving Tasks
ESD	Event Sequence Diagrams
FTs	Fault Trees
FOC	Fleet Operations Center
MaaS	Mobility as a Service
MOC	Maintenance Operations Center
ODD	Operational Design Domain

Executive Summary

Executive Summary

Technological advances in Automated Driving Systems (ADS) have resulted in greater interest in their potential use in transport operations, both as individually owned vehicles and in fleets employed for passenger transport in Mobility as a Service (MaaS) contexts. MaaS can combine various transportation options (such as public transport, car-sharing and van pools, and taxis) into a single comprehensive on-demand mobility service. Successfully integrating ADS into MaaS will require careful attention to safety concerns on the roadway. This report presents a qualitative risk assessment of fleets employing advanced ADS vehicles for MaaS operations.

Amid the currently evolving technical, commercial, and regulatory environment, recent ADS testing and small-scale deployment incident reports suggest that a more focused approach to operational safety is required, for instance, to avoid traffic disruptions, or to determine appropriate incident management procedures (National Highway Traffic Safety Administration, 2022). Operational safety encompasses activities beyond the functional safety of the ADS-equipped vehicles and includes tasks such as service monitoring, dispatching, maintenance and repair, incident response, staffing and training, and passenger support. Operational safety issues may become an important element in deploying vehicles that do not have a trained safety driver on board, raising questions about how manufacturers, ADS developers and fleet operators may provide adequate safety assurance prior to widespread commercialization and deployment.

This research identifies key safety risks associated with remote monitoring and supervision of Level 4 ADS-equipped vehicle operations. Level 4 vehicles are designed to be capable of performing all driving tasks within a defined set of operational conditions defined in their Operational Design Domain (e.g., weather, road geometries) and are responsible for achieving a safe stop in the event of emergencies. Our analysis focuses on the use of automated vehicle fleets for passenger transport in MaaS, as these represent an important short- to medium-term application of the technology. However, the results presented in this report are also applicable to future applications for individually owned vehicles equipped with automated driving functions, particularly with regard to remote assistance during emergency situations. For this risk analysis we modeled a generic fleet and its operations consisting of light-duty passenger vehicles equipped with Level 4 ADS capabilities, owned, and managed by a fleet operator, with vehicles designed and manufactured by an ADS developer. The fleet operator is responsible for implementing risk mitigation strategies to ensure operational safety according to the specifications of the ADS developers. The functions of the fleet operator are divided among three decision-making systems or entities: the ADS-equipped vehicles, a Fleet Operations Center overseeing vehicle operations, and a Maintenance Operations Center responsible for inspection and maintenance activities. The ADS developer establishes the protocols for driverless operation based on the system's capabilities. For instance, Level 4 vehicles may be restricted to operating within a specified area (geofencing) or under certain speed limits. The fleet operator is responsible for ensuring these restrictions are observed as well as implementing additional constraints if necessary to ensure passenger safety.

To address the complex risks involving human, software, and hardware systems in an ADS fleet, we developed a hazard identification methodology which combines traditional and innovative hazard identification methods used in risk assessment, including Event Sequence Diagrams, Fault Trees, Concurrent Task Analysis, and System-Theoretic Process Analysis. The application of the methodology resulted in identifying 20 high-level hazard scenarios arising from system failures, human errors, and unsafe interactions encountered by all three entities during different operational phases. The high-level hazards are defined at sub-system level (instead of a more detailed component-level), focusing on how functions or tasks incorrectly performed can lead to safety-related consequences. The hazard identification process highlights the key role of reliable and secure communication channels between ADS-equipped vehicles and the remote operators tasked to supervise its functions. Likewise, while the ADS vehicle is expected to function independently within the operating conditions established by manufacturers—including environmental, geographical and time of day constraints, and traffic and roadway characteristics—hazards arising from system malfunctions or rare edge situations underscore the relevance of a adopting a layered approach to safety, where remote operation assistance may play an important role in emergency situations.

Furthermore, the hazard analysis identifies operational safety responsibilities for the fleet operator. These responsibilities are translated into risk mitigation actions, which include specific activities that fleet operators can undertake to prevent and mitigate safety hazards and their consequences. These risk mitigation activities, covering various aspects such as procedures, training, tools, work process and workplace design, are recommended to guide fleet operators in allocating resources. Over sixty activities relevant to remote ADS support operations were derived and ranked based on their potential impact on safety and resources required for implementation.

With the potential future introduction of large-scale Level 4 ADS fleet operations for Mobility as a System transport, it will be crucial to determine the activities, procedures, and requirements necessary to ensure operational safety, as is defining the roles of those entities responsible for achieving and maintaining safety. The main findings regarding key risk mitigation activities for ADS fleets, identified through a safety risk analysis, can be summarized as follows:

- Top priority risk mitigation activities for fleet operators include organizational management of change, training remote supervisors to monitor and intervene in vehicle operations, providing suitable working conditions for employees, enforcing vehicle connectivity and dispatching requirements, and coordinating internal incident mitigation activities.

- Without onboard trained safety drivers, remote fleet supervisors will play a crucial role in ensuring passenger and vehicle safety. Their top tasks include monitoring the vehicle's operation and intervening when required to ensure safety. To do this, fleet operators—in coordination with the ADS developers—must ensure remote operators have access to the necessary tools and training.

- The design of the overall system and human-system interface tools should consider human and physical time constraints, allowing remote operators sufficient time to perform monitoring and

expected driving and passenger assistance tasks efficiently under emergency situations (Mutzenich et al., 2021).

- Fleet operators may consider further restricting vehicle operations beyond the operational limits set by the ADS developers to always ensure reliable wireless communication with passengers. We suggest developing a Fleet Operational Design Domain to specify the conditions under which ADS vehicles can safely operate as part of MaaS transport.
- The extent of knowledge and information exchange between fleet operators and ADS developers is currently uncertain. This raises questions whether fleet operators' have sufficient knowledge about ADS software and hardware specifications, requirements, and maintenance procedures to ensure operational safety and regulatory compliance and whether ADS developers need to take a more active role in educating fleet operators.

Contents

Introduction

Automated Driving Systems (ADS) are expected to play an important role in the transportation environment, both as individually owned vehicles and fleets employed for passenger services within Mobility as a Service (MaaS) contexts. Successfully integrating ADS into MaaS will require careful attention to safety concerns on the roadway. This report presents the results of a qualitative risk assessment conducted for Level 4 ADS vehicle fleets. While extensive research has focused on improving the functional safety of ADS-equipped vehicles, their efficient and safe deployment as part of MaaS services will depend on several external factors, including the reliability of wireless connectivity, fleet management, and interaction with other vehicles on the road.

Currently, vehicle automation capabilities are categorized into six levels by the Society of Automotive Engineers (SAE), ranging from Level 0 to Level 5, based on the combination of driving support and automated driving features (SAE International, 2021). Level 4 ADS vehicles are capable of performing all driving functions under specific conditions outlined in their manufacturer's Operational Design Domain (ODD), without external commands or the intervention of a safety driver (National Highway Traffic Safety Administration, 2017; Thorn et al., 2018). In the event the vehicle exceeds its ODD (e.g., weather conditions, road geography restrictions), the ADS is expected to implement fallback strategies and achieve a safe stop, referred to as Minimal Risk Condition (MRC) without external assistance. At the present stage of ADS development, the short-term goals of companies involved in the industry is to deploy Level 4 ADS vehicles on a commercial scale, either for personal use or integrated into fleets.

The L4 ADS vehicles would be programmed to pick up travelers at specific locations and deliver them to their destinations along a designated route but would be restricted to specific geographic boundaries by geofencing or prevented from operating under certain conditions, such as severe weather. In the event of a violation of these protocols, an accident, or other situations requiring the vehicle to be shut down, human operators at a Fleet Operations Center would be required to initiate procedures to move the vehicle to a safe location or summon emergency services.

The main safety-related tasks Level 4 ADS vehicles must perform to ensure the safety of the passengers and surrounding road users are: (1) complying with the ODD limitations through self-diagnostic systems, (2) safely performing all the real-time operational and tactical functions required to operate a vehicle in on-road traffic (known as Dynamic Driving Tasks or DDT) under real-time conditions including monitoring the driving environment, detecting road features and other vehicles and road users, and environmental conditions, and (3) implementing fallback strategies in response to unexpected events, such as bringing the vehicle to a safe stopping position after a system failure or other event when the trip cannot be continued to reduce the risk of a collision (known as a Minimal Risk Condition or MRC). While most research efforts have focused on assessing the functional safety and system reliability of ADS vehicles based on testing or computer simulations (AVSC00006202103, 2021; Khastgir et al., 2021; Sohrabi et al., 2021), there is no clear approach to

establishing the operational safety responsibilities of the key agents involved in Level 4 ADS deployment, such as fleet operators, ADS developers, vehicle manufacturers, and regulatory entities.

Without trained on-board backup safety drivers, remote fleet supervisors may need to actively participate in ensuring passenger and vehicle safety by monitoring driving tasks and intervening indirectly when required. The remote operator functions include tasks referred to as remote driving assistance function, e.g., directing the disabled vehicle to a waypoint, issuing commands to the vehicle to reach a safe stopping location, or participating in post-incident management procedures. Note that direct vehicle control (i.e., throttle, brake, steer control) is exclusively the task of the ADS, the remote supervisor can only provide commands to assist the ADS. The role of remote fleet supervisors may vary from providing service assistance, to actively performing safety tasks in the case of passenger transport for MaaS. Determining the fleet operators' safety responsibilities when managing ADS fleets requires an in-depth assessment of the hazards arising from large-scale fleet operations. Likewise, many of these safety responsibilities may be transferable to the context of remote driver support for individually owned vehicles equipped with ADS technology. Comprehensive hazard identification and modeling are crucial steps to developing qualitative and quantitative risk assessments to develop preventive safety barriers and risk mitigation measures.

This report presents the results of our hazard identification process focused on the remote operation of ADS fleets employed for MaaS, using a model of a generic fleet using Level 4 ADS-equipped vehicles. While these vehicles are expected to perform all their driving tasks independently within their Operational Design Domain, remote operators may play a key role in providing system safety redundancy. However, these safety expectations require dedicated efforts from the fleet operators, ADS developers, and vehicle manufacturers to ensure potential hazards are correctly prevented or mitigated. Therefore, we derived a set of recommended risk mitigation activities for fleet operators based on the identified hazards.

This document is organized as follows. Section 2 presents the characteristics of the modeled fleet. Section 3 discusses the methods employed to determine critical potential hazards. Section 4 discusses the fleet operator's operational safety responsibilities and potential risk mitigation measures addressing the identified hazards.

Section 2: Developing the Model Fleet

The model fleet represents the anticipated configuration of ADS systems in the short- to medium-term fleet operations. Extensive research was conducted by examining relevant publications from authoritative sources such as NHTSA, AVSC, and SAE International (Automated Vehicle Safety Consortium AVSC, 2019; Blanco et al., 2020; Chaka et al., 2021; SAE International, 2021; Thorn et al., 2018). This review was supplemented with Voluntary Safe Self-Assessments (VSSAs) published by various ADS manufacturers and developers involved in Level 4 ADS operations, with a particular emphasis on MaaS operations. These VSSASs align with NHTSA's 2017 Voluntary Guidance, which outlines twelve priority safety design elements, serving as a valuable resource for testing and developing ADS (National Highway Traffic Safety Administration, 2017).

The model fleet's operational profile encompasses expected fleet usage, vehicle ownership, passenger interactions, Operational Design Domain restrictions, and functions related to remote fleet operations. The specified configuration and capabilities of the vehicles in the model fleet include vehicle segments, ADS capabilities, inspection, and maintenance activities, as well as testing and validation procedures.

Model Fleet Description

The model fleet is composed of standard passenger vehicles equipped with Level 4 ADS capabilities. These ADS-equipped vehicles are managed by a fleet operator who has procured them from an external ADS developer or vehicle manufacturer. Since the fleet provides on-demand passenger transport services, the primary responsibility of the fleet manager is to ensure the proper and safe functioning of the fleet, following the technical requirements set by the ADS developer and additional considerations to ensure passenger safety. The vehicles in the fleet do not have on-board safety drivers; instead, they rely on remote operators who monitor the vehicle's condition. The features of the model fleet were chosen to provide sufficient information for conducting the risk assessment and to accurately reflect the key attributes of the proposed fleet. Table 1 outlines the fleet’s operational profile and vehicle configuration.

Alternative Fleets

The lessons learned from this study could also be applied to individually owned Level 4 ADS-equipped vehicles, and purpose-built driverless vehicles. In particular, remote fleet operations such as service or driving assistance, could play an important role in vehicles designed exclusively for driverless passenger transport. These purpose-built vehicles may vary significantly from current passenger vehicles. For instance, these vehicles might not contain on-board driving mechanisms (steering wheel, throttle, and brake pedals), and might rely on interactive displays to communicate with passengers.

Table 1: Characteristics of model fleet.

Operational Profile	
Usage	24/7 ride-hailing services, consisting of a medium-scale fleet of 100–300 vehicles in multiple depots.
Vehicle Ownership	The fleet operators own the ADS-equipped vehicles.
Passenger interaction	Passengers hail rides through mobile applications (on cell phones), have access to on-board visual and audio information of vehicle status (battery, trip, etc.), emergency stopping and live rider support mechanisms (e.g., contact with a remote service operator).
ODD restrictions	Vehicles operate in urban and rural areas, limited by the geometry and quality of roads (well-maintained and signaled asphalt and concrete). Can operate on highways, parking structures, signaled intersections, and merge lanes. Areas of operation limited to specific areas by geofencing techniques and to light to moderate environmental conditions (light wind, rain, fog, snow allowed, heavy conditions of standing water, icy or snowy roads are out of scope). Speeds in the range of 35-65 mph.
Remote fleet operations	Fleet management center responsible for continuous monitoring, passenger communication and support, post-crash procedures, and supervisory operations in emergency situations. Safety operators can transmit commands to the ADS to achieve a Minimal Risk Condition to ensure passenger/vehicle safety while awaiting post-incident procedures. The safety operator does not directly control the vehicle (remote driving is not considered).
Vehicle configuration and capabilities	
Vehicle segment	Electric or hybrid light-duty passenger vehicles and SUVs sourced from multiple manufacturers.
ADS capabilities	Object and Event Detection and Response (OEDR) based on real-time perception data from a single vehicle (retrieved from the vehicle's sensors) and built-in behavior profiles; the self-diagnostic system can detect the need for corrective action and achieve a safe condition (MRC) with no human intervention; redundant safety-critical systems, dedicated cybersecurity units. Operation is supported by a local traffic rule onboard database and onboard High-Definition maps. The detection of abnormal events such as accidents, emergency vehicles, construction zones, and closed roads relies on single-vehicle perception data.
Inspection and maintenance	Pre-ride inspection checklists and regular maintenance activities, sufficient for the fleet operator to maintain the operation of the fleet as intended and inform the ADS developer. Fleet operator engages with the ADS developer to implement maintenance crew training program.
Testing and validation procedures	Feedback and communication from ADS manufacturer sufficient for the fleet operator to maintain the operation of the fleet as intended and inform the ADS manufacturer of faults or emergencies experienced by the fleet.

Section 3: Identifying Safety Hazards in Remote Fleet Operations

To identify the complex hazards associated with Level 4 ADS operations, we employed a combination of traditional hazard identification and modeling tools to identify and model multiple system hazards (Kramer et al., 2020). These tools s include fault tree analysis (FTA), event trees analysis (ETA), event sequence diagrams (ESDs), failure mode and effect analysis (FMEA), hazard and operability studies (HAZOP), and, more recently, Bayesian networks (BNs). These traditional hazard identification and modeling approaches, employed in both research and industry, have provided a basis for many industry standards (International Organization for Standardization, 2018a). In addition to these well-established methods, recent advancements have introduced novel techniques such as Concurrent Task Analysis (CoTA) and System-Theoretic Process Analysis (STPA) (Ramos et al., 2020b; Yang et al., 2020). These methods focus on identifying and modeling interactions in complex systems between subsystems, evolving feedback loops, and emergent properties. Emergent properties refer to the functions or characteristics of a system that arise from interactions between its components and the operational environment (Ferreira et al., 2013; Johnson, 2006). This methodology consists of three stages: system modeling, scenario modeling, and hazard identification (Figure 1, Table 3).

I. **System modeling:** Describe the main agents participating in the system's operation. An agent is a human, software, or machine subsystem with decision-making power over its own state and that of the system's entire operation. Agents can be composed of multiple elements, each expected to perform specific functions. This stage consists of:
    - **Step 1**: Describing the functions that each participating agent is responsible for performing.
    - **Step 2**: Defining the different operational phases and the agents' functions during each phase. The different agents and the various operating phases for the ADS-vehicle fleet are described below in the section entitled Stage 1: Modelling the System.

II. **Scenario modeling**: Build a representation of the system's operational phases to identify key events that may present hazards. This stage consists of:
    - **Step 3:** Modeling the operational phases through an Event Sequence Diagram (ESD).
    - **Step 4:** Modeling agents' normal tasks through Concurrent Task Analysis (CoTA).
    - **Step 5:** Modeling the results of encountering hazardous events that could result in a failure to safely to complete the trip through Fault Trees (FTs).
    - **Step 6:** Modeling agents' potential responses to the possible hazardous conditions with System Theoretic Process Analysis (STPA).

III. **Hazard identification**: Systematically identify and characterize potential hazards using the multiple techniques. This stage consists of:
    - **Step 7:** Utilizing each technique to answer the following questions: a) What hazards could occur in each operational phase? b) What entity is causing or contributing to the hazard? c)

How do these hazards develop? d) Why do they develop? e) What are the potential consequences of these hazards?

Each of the modelling tools used in Steps 3 through 6 are described in greater detail below. Additional details about the methodology can be found in (Correa-Jullian et al., 2024b).

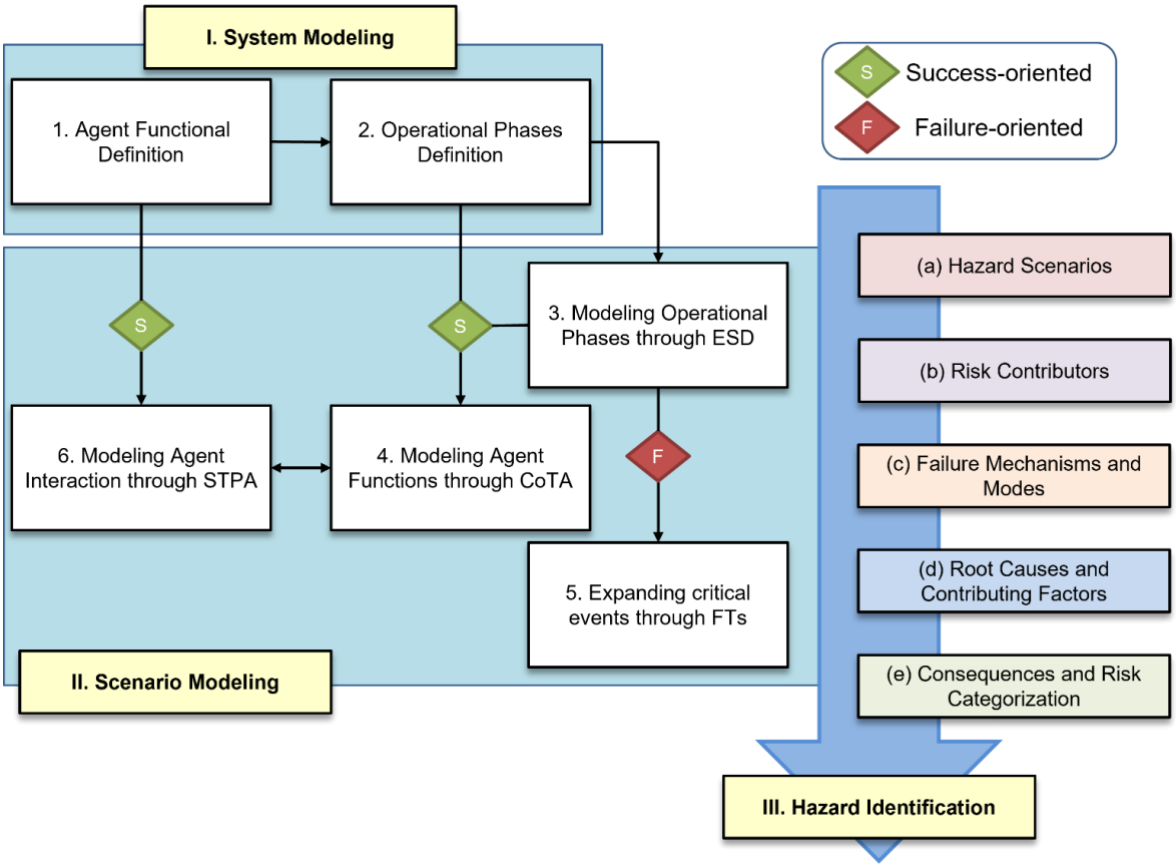

Figure 1: Overview of hazard identification methodology.

Stage I: Modeling the System

The analysis presented in this section is based on a model fleet of regular passenger vehicles with Level 4 ADS capabilities and no safety driver onboard. This analysis focuses on interactions between remote operators and the ADS-equipped vehicles.

Agent Functions

The model fleet system is composed of three distinct agents, each with their own set of functions (refer to Table 2). Each vehicle's operation is directly managed by the onboard ADS software, which continuously monitors the vehicle's surroundings in real time through on-board sensors. Individuals working in the Fleet Operations Center oversee and supervise the operation of the ADS vehicles, while those staffing the

Maintenance Center handle vehicle inspections, maintenance, and storage. Details about the ADS vehicle and the remote operators are provided in the following sections. Further information is available in Correa-Jullian *et al.* (2022a).

ADS Vehicle

Throughout its operation, each ADS vehicle performs automated driving tasks in accordance with Level 4 capabilities (SAE International, 2021). This includes engaging in normal driving activities or taking actions in response to a dangerous situation, a vehicle malfunction, or if it is exceeding its operating parameters. If the vehicle encounters a hazardous situation, or a passenger requests an emergency or unscheduled stop, the vehicle must either perform corrective actions to enable it to complete the trip or stop the vehicle at a safe location to discharge the passenger or until help can arrive, also known as performing a DDT-fallback (Ramos et al., 2023).

The responsibility for identifying the need for and executing these actions lies with the ADS vehicle. However, in the event of a system failure, a remote safety operator in the Fleet Operations Center can provide support and issue appropriate commands to the vehicle. As part of MaaS, the ADS-equipped vehicle would perform tasks such as picking-up and dropping-off assigned passengers, facilitating communication between the passenger and the remote operators, receiving commands from the Fleet Operations Center, and making emergency stops at a passenger's request. If an unoccupied vehicle experiences a non-critical safety issue the vehicle can navigate itself to a safe location where it can be retrieved and scheduled for maintenance and repairs.

Fleet Operations Center Remote Operators

Trained operators in the Fleet Operations Center oversee the ADS fleet operations. Their responsibilities include managing passenger requests, sending dispatch commands to the ADS vehicle, and communicating with passengers. These functions may be performed by two different types of remote operators, safety operators and service operators, each addressing vehicle and passenger related issues during operation.

While the ADS vehicle can make driving decisions independently, the remote operators have the ability to send commands to override actions initiated by the vehicle. These dispatch commands may be used based on factors like vehicle status, location, and occupancy. Further, remote operators can guide the vehicle through challenging situations by directing the vehicle to take an alternate route or directing it to a safe stopping place (Minimal Risk Condition).

In the event of an accident, the Fleet Operations Center staff is responsible for initiating post-incident management procedures, which involve contacting and dispatching first responders and vehicle recovery teams to the incident location. Additionally, the Fleet Operations Center plays a crucial role in reporting any abnormal vehicle behavior to the Maintenance Operations Center to initiate any required inspection and maintenance activities.

Table 2: Agent Responsibilities for ADS operations.

ADS Vehicle	Fleet Operations Center remote operators	Maintenance Operations Center crew
Use real-time sensor data to plan and perform Dynamic Driving Tasks.	Supervise vehicle operation and intervene when required (safety operator).	Follow ADS developers' maintenance requirements to prevent vehicle failures.
Transmit passenger communication requests to the Fleet Operations Center.	Manage passenger requests and contact first responders (service operator).	Perform pre-shift inspection prior to clearing vehicles for operation.
Transmit information about vehicle status, location, and alerts. Receive re-routing, waypoints, or fallbacks commands from remote operators.	Initiate post-incident procedures after vehicle is in a safely stopped condition (Minimal Risk Condition).	Perform corrective and preventive maintenance procedures prescribed by the ADS developers.
Detect that vehicle has deviated from its operating parameters, or suffered a failure, or that an incident has occurred.	Detect when actions must be taken due to the vehicle deviating from its operating parameters, or a vehicle failure or incident has occurred.	Manage and recover stranded vehicles.
Determine and undertake proper corrective actions.	Determine and undertake proper corrective actions.	Satisfy local regulations and reporting duties for post-incident procedures.

Vehicle Operations

The safety risk analysis of the model fleet considered various vehicle operating phases, as shown in Figure 2. Note that an *operational shift* denotes the continuous operation of an ADS vehicle within a defined period of time. The operational phases considered in the analysis were as follows:

- Inspection, maintenance, and system updates
- On-route to destination without passenger
- On-route to destination with passenger
- Passenger pick-up and drop-off
- Post-incident management

This report primarily focuses on the role of remote fleet operators, specifically during the on-route phase, passenger interaction phase, and post-incident management phase. A brief description of each operational phase is provided below, with further details available in (Correa-Jullian et al., 2022b).

a) On-route to destination without passengers: Once the ADS vehicle receives a dispatch command, it executes all necessary driving tasks to reach the passenger pickup point. If the ADS diagnostic module detects a non-critical system failure on route, the vehicle may automatically achieve a Minimal Risk Condition or redirect itself back to the Maintenance Operations Center, if possible. In other cases, the ADS is responsible for taking steps necessary to minimize any potential risk and achieve a Minimal Risk Condition, either automatedly or with assistance from the remote operator. If the vehicle becomes stranded, the maintenance staff is responsible for recovering it.

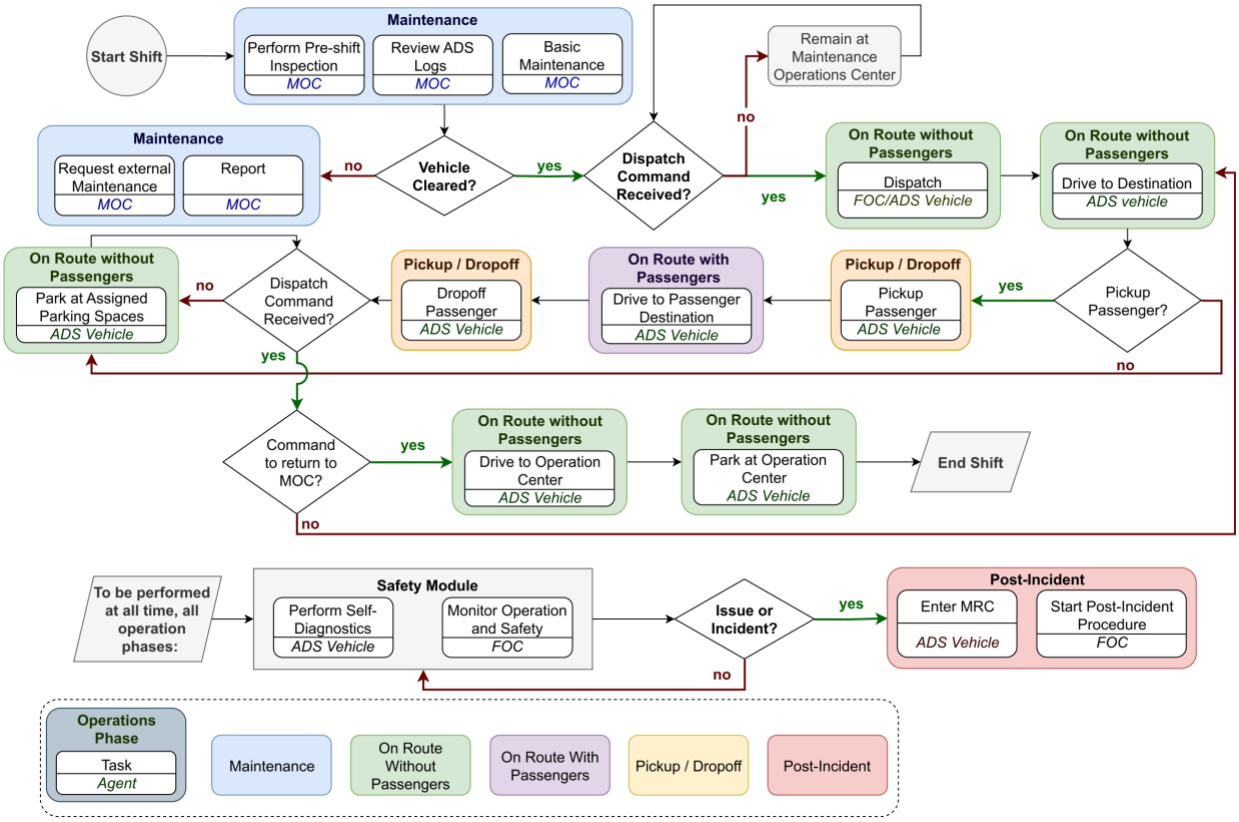

Figure 2: Simplified diagram of operational phases.

b) On-route to destination with passengers: This phase occurs between passenger pick-up and drop-off and involves interactions among the passenger, the ADS vehicle, and the remote operator. Passengers may ask to communicate with the remote operator or request an emergency stop. When the ADS receives the passenger emergency stop request it comes to a safe stop and automatically alerts the remote operator. Depending on the circumstances, the remote operator may allow the vehicle to continue after confirming with the passenger, direct the vehicle to a safe location, or initiate post-incident procedures.

c) Passenger pick-up and drop-off: When the ADS vehicle approaches the designated pick-up or drop-off location, it stops where passengers can safely board or exit the vehicle. Passengers are expected to follow safety instructions and confirm trip details through the vehicle's displays (e.g., drop-off location) before the ADS initiates the trip. Note that vehicles must be equipped with sensors that can verify passengers have for example, closed the vehicle's doors, and fastened seat belts. Similarly, during drop-offs, passengers must confirm the trip's completion to enable the ADS to accept new trip assignments.

d) Post-incident management: If the vehicle is involved in a traffic accident it is required to reach a safe stop (Minimal Risk Condition), and the remote operators must initiate post-incident procedures. At a minimum, these procedures include (1) automatically disabling the ADS, activating hazard lights (if not already on), unlocking doors, and disconnecting the main battery; (2) maintaining continuous communication between passengers and the remote operator, if possible; (3) contacting first responders and/or law enforcement to assist affected passengers or other road users. Vehicle operations are expected to comply with local legislation or regulatory requirements for severe incidents involving passengers or other road users.

Stage II: Scenario Modeling

We identified potential hazards for all the operational phases described in the previous section. For the present analysis, four Event Sequence Diagrams were developed to represent the operational phases, containing over 100 events related to the agent's performance and 41 distinct outcomes. Following this, 16 Concurrent Task Analysis models were developed based on the Event Sequence Diagrams, identifying over 200 tasks for the ADS vehicles, remote operators, and maintenance staff. Then, we selected 13 events to explore further through Fault Trees, decomposing the top failures into over 120 events. Finally, we developed a System Theoretic Process Analysis model that summarized 38 control actions and 35 distinct feedback responses. An example showcasing the use of Event Sequence Diagrams, and Fault Trees is presented in the following section (Correa-Jullian et al., 2022b, 2024b).

Scenario Modeling Tools

Event Sequence Diagrams

Event Sequence Diagrams are traditional hazard analysis methods based on breaking down potential hazards into a sequence of pivotal events stemming from a common initiating event and leading to different possible outcomes. Event Sequence Diagrams may be combined with Fault Tree Analysis, Bayesian Networks, and Concurrent Task Analysis to represent interactions between hardware and software failures (Thieme et al., 2020a, 2020b) and human errors (Ramos et al., 2019). In this study we developed an Event Sequence Diagram for each operational phase for the model fleet.

Concurrent Task Analysis

Concurrent Task Analysis (CoTA) is a deductive method which analyzes how system user's complete tasks to achieve their goals. It is used to analyze a system's expected behavior and performance based on breaking down system-level goals into sub-goals. These sub-goals are hierarchically organized through plans, indicating the order in which certain tasks must be performed to achieve the system-level goals. The breakdown of goals into subgoals follows an extension of the cognitive Information, Decision, and Action model (IDA) to human and automated systems (Chang & Mosleh, 2007; Ramos et al., 2020a, 2020b). In our study we developed a Concurrent Task Analysis for each agent involved in each operational phase, building on the Event Sequence Diagrams representing each phase (Ramos et al., 2020a).

Fault Trees

Fault Tree Analysis (FTA) is a traditional deductive method of hazard analysis based on how basic events, such as a failure in one system component, can lead to system-wide failures. The developed Fault Trees complement the Event Sequence Diagram for each operational phase analyzed.

System-Theoretic Process Analysis

System-Theoretic Process Analysis (STPA) is a deductive model that recognizes that hazards may develop from uncontrolled and unsafe interactions between system components. It is based on the STAMP (System Theoretic Accident Model and Processes) model, and systems and control theory (Leveson & Thomas, 2018). The method consists of four main steps: (1) Defining the system, subsystems, and system boundaries; deriving the potential, system-level hazards, and system-level constraints; (2) developing the hierarchical control structure diagram; (3) identifying unsafe control actions that may breach the system-level constraints; and (4) identifying the corresponding losses resulting from the unsafe control actions. We developed a system-level diagram based on the identified functions of the model fleet.

Table 3: Overview of hazard identification and modeling tools employed.

Modeling Tool	Advantages	Analysis Application
Event Sequence Diagram	(1) Can model dynamic causal relationships between initiating event, intermediate events, and possible outcomes. (2) Delivers an explicit method to quantify event frequencies. (3) They are frequently applied to depict software, hardware, procedures, and human-system interactions.	Developed to represent operational phases. Binary event outcomes (yes/no) lead to success or failure outcomes. Used to identify hazard scenarios (a), risk contributors (b), and consequences (e).

Modeling Tool	Advantages	Analysis Application
Concurrent Task Analysis (CoTA)	(1) Can model interactions between tasks performed by different agents for achieving a common goal and subgoals. (2) Allows modeling of sequential and parallel tasks for a single agent or between agents.	Developed to describe the tasks involved in the successful completion of a system goal. Used to identify additional hazards and identify potential failures and their causes (c). Developed for failure events, identification, failure propagation analysis, and procedures development.
Fault Tree (FT)	(1) Can identify causes and critical combinations of events leading to undesirable events. (2) Provides an explicit method to quantify failure probabilities based on Boolean algebra. (3) Can be used for reliability analysis at system/component-level or functional requirements.	Developed to describe a sequence of events leading to a system failure. Used to categorize of basic failure events by their possible root causes (human errors, hardware or software malfunctions, or process design errors) (d).
System-Theoretic Process Analysis (STPA)	(1) Can model interactions between components leading to system failures. (2) Analysis extends to non-failure events by analyzing system as a control structure. (3) Frequently applied for concept design analysis and environment-system interactions.	Developed to describe the interactions and feedback loops between different subsystems. Used to identify additional hazards and identify failure modes and mechanisms (c).

Scenario Example: On-Route Without Passengers

To simplify the analysis of the dynamic interactions between the ADS vehicles, the remote operators, and other external factors during the "on-route to destination without passengers" operational phase the model adopts the following assumption: The Event Sequence Diagram comprises the entire trip, regardless of whether multiple events may occur during the same trip. The diagram presented in Figure 3 illustrates a simplified Event Sequence Diagram. This diagram begins with the initiating event denominated "**The vehicle is on-route to destination**" and may result in various end states and outcomes described in Table 4.

In this simplified Event Sequence Diagram, key actions of the subsystems regarding information gathering, situation assessment and decision-making, and executing a response have been merged into a single event. The subdivision of these tasks follow an extension of the cognitive Information, Decision, and Action model (Chang & Mosleh, 2007) to human and autonomous systems (Ramos et al., 2020a, 2020b). This division of tasks is fundamental to identify different failures by the ADS and the human operators, as well as emergent failures and/or failures arising from unsafe interactions between these agents. For deeper analysis, the events "**ADS**

performs DDT-fallback correctly" and **"FOC sends correct DDT-fallback command"** should be further developed, for instance, through Fault Trees and Bayesian Networks. To model the operation of the ADS vehicle, the following assumptions have been made:

(1) A successful trip may be interrupted if the vehicle violates its operating parameters, wrongly executes a driving task, or because of an unavoidable external event. It should be noted that although these events can occur simultaneously, the presented Event Sequence Diagram only assumes one of these events occurs per trip.

(2) The ADS is the first line of response when an event interrupts a trip as it is designed to detect hazards in real-time and determine whether a response is required. The ADS must then plan and execute the necessary corrective action which for this operational stage may mean returning to normal driving operations, proceeding under limited driving conditions, or stopping at a safe location.

(3) The second line of response is the remote operator. The operator may intervene after the ADS vehicle has either failed to detect a problem or has failed to respond properly, in which case, if there is sufficient time for the operator to intervene, they will transmit the correct set of instructions. If the ADS vehicle receives and adopts the correct commands, it may be allowed to proceed with the trip or be instructed to stop at a safe location or to return to the Maintenance Operations Center. If the vehicle is directed to a safe stopping location, the remote operator is also responsible for initiating the required post-incident procedures.

(4) The proper post-incident procedures will depend on whether the vehicle is at risk of colliding with other road users; is capable of safely continuing its trip or can be remotely driven back to the Maintenance Operations Center, or must be recovered by the maintenance crew.

Table 4: Possible end states for "On-route without passengers" phase.

End State	Severity	Outcome
Trip is completed	None	The ADS successfully completed the designated trip. If any challenging situation arose, the ADS was able to overcome it automatically or through the intervention of the remote operator.
Post-incident procedures are initiated	Medium	The remote operator successfully initiated the post-incident procedures after the vehicle reached a safe location (Minimal Risk Condition). The specific response depends on the perceived severity of the incident and local regulations.
Vehicle is stranded	Medium	The remote operator has failed to initiate post-incident procedures to recover the vehicle after it reaches a safe location (Minimal Risk Condition).

End State	Severity	Outcome
Vehicle arrives at Maintenance Operations Center for maintenance	Low	The vehicle successfully undertakes corrective action initiated by the ADS or assisted by the remote operator after a non-critical system failure was detected.
Collision Risk	High	The vehicle is at risk of colliding with other road users or other objects because the ADS and the remote operator have failed to detect a problem and direct the vehicle to a safe stopping location.

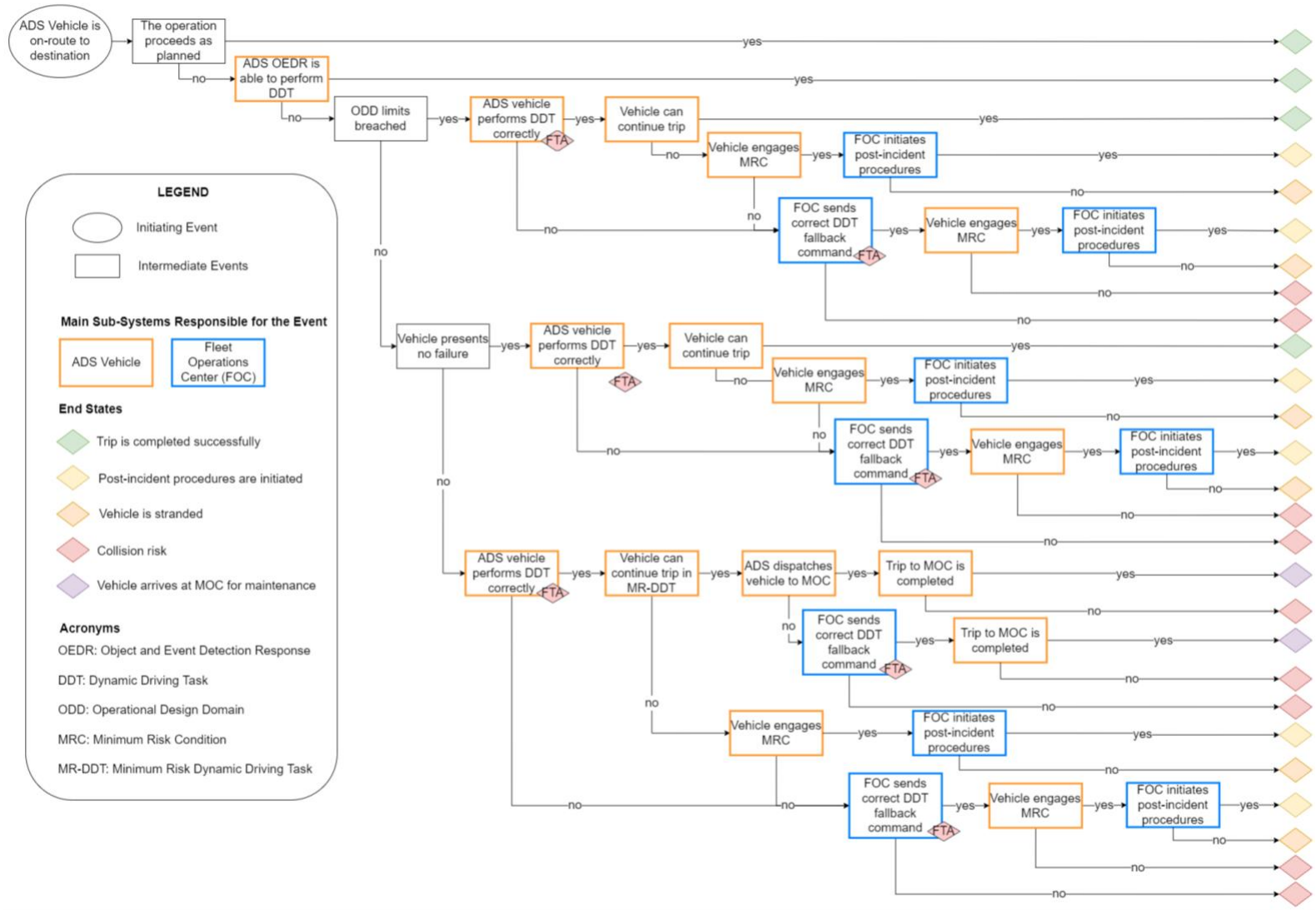

Figure 3: Event Sequence Diagram for "on-route without passenger" operational phase.

The key sub-events identified in this phase are described in Table 5. Each key event has a yes/no outcome and identifies which subsystem is primarily responsible for the outcome. Two key subevents are critical to the safe response of the ADS vehicle when faced with challenging situations: (1) the ADS independently takes appropriate corrective action or (2) a remote operator sends the ADS vehicle a command to take specific corrective action. These events are particularly relevant given the complex interactions between the subsystems involved that lead to successful or failed outcomes.

Table 5: Sub-events for "On-route without passengers" phase.

Intermediate Event	Success (Yes)	Failure (No)	Responsible Agent
The operation proceeds as planned.	The vehicle can perform normal driving functions and complete the trip in a safe manner.	Nominal operation is interrupted due to the vehicle not responding as expected. Possible causes: vehicle fails to detect objects that can affect the safe operation and respond appropriately, operating limits are exceeded, vehicle failures.	ADS
The vehicle successfully responds to a challenging situation.	The ADS can plan and execute an adequate response.	The ADS does not plan or execute an adequate response.	ADS
The vehicle exceeds its operating parameters.	The incident causes the ADS to operate outside its defined operating parameters (environmental conditions, traffic scenarios).	The incident does not cause the ADS to operate outside its defined parameters.	ADS
The vehicle does not suffer a failure.	The ADS functions are not compromised.	The ADS self-diagnostic module identifies a system failure. *	ADS
The vehicle successfully performs a fallback action.	The ADS detects that corrective action is required. The ADS can plan and execute the required actions.	The ADS does not detect that corrective action is required or fails to plan or execute the required actions.	ADS
The vehicle continues the trip.	The ADS can return to normal operating paraments through the actions implemented.	The ADS is not able to return to normal operating parameters through the actions implemented.	ADS

Intermediate Event	Success (Yes)	Failure (No)	Responsible Agent
The vehicle safely stops and engages an MRC.	The ADS vehicle can reach a safe place to stop.	The ADS does not reach a safe place to stop.	ADS
The Fleet Operations Center initiates post-incident procedures	The remote operator detects that post-incident procedures are required and initiates them.	The Fleet Operations Center operator does not detect that post-incident procedures are required. The vehicle is stranded.	FOC
Fleet Operations Center sends correct fallback instructions to the vehicle.	The remote operator detects that the vehicle is unable to respond properly and identifies the correct procedure and sends appropriate command to the vehicle.	The remote operator fails to detect that the vehicle requires instructions or fails to identify the correct procedure or send appropriate commands to the vehicle. **	FOC
The vehicle can take corrective action and safely continue trip under limited operational conditions.	The ADS self-diagnostic module determines that the system failure is not critical, and vehicle can continue the trip under limited conditions.	The ADS self-diagnostic module determines that the system failure is critical, and the vehicle cannot continue the trip.	ADS
The ADS dispatches the vehicle to Maintenance Operations Center	The ADS automatically reroutes the vehicle to the Maintenance Operations Center under safe conditions.	The ADS fails to reroute the vehicle to the Maintenance Operations Center under safe conditions.	ADS
The vehicle completes the trip to Maintenance Operations Center.	The ADS can drive the vehicle to the Maintenance Operations Center.	The ADS is not able to drive to the Maintenance Operations Center.	ADS

Note: *The effectiveness of the self-diagnostic module is incorporated through Fault Trees; ** The reliability of the wireless communication channels is incorporated through Fault Trees.

As mentioned, Fault Trees are a useful tool to model hardware, software, and human-related failures and errors. Figure 4 presents a simplified Fault Tree developing the subevent corresponding to the detection and planning phases. Here, the top event is "**FOC operator fails to detect and plan DDT-fallback required.**" In this case,

the top event may occur based on two sub-events referring to communication errors between the remote operator and the ADS vehicle. On the one hand, this may occur when the self-diagnostic module fails to detect that the Fleet Operations Center-ADS vehicle communication channels have failed. The latter may be further due to vehicle hardware or software failures in the vehicle's communication channels, or limited connectivity in the area. On the other hand, the remote operator may fail to act upon the information transmitted by the ADS vehicle if:

a) the remote operator fails to correctly monitor and assess the vehicle's state, fails to detect the need for corrective action, or does not following the established procedure to plan and communicate an adequate response.

b) the ADS vehicle fails to transmit the correct information because it does not detect that the ADS data recording mechanisms have experienced an undetected failure or if the ADS does not transmit information required for determining the vehicle's status. This is associated with flaws in the ADS software design and/or implementation and can be caused by the maintenance crew failing to follow system updates and maintenance procedures.

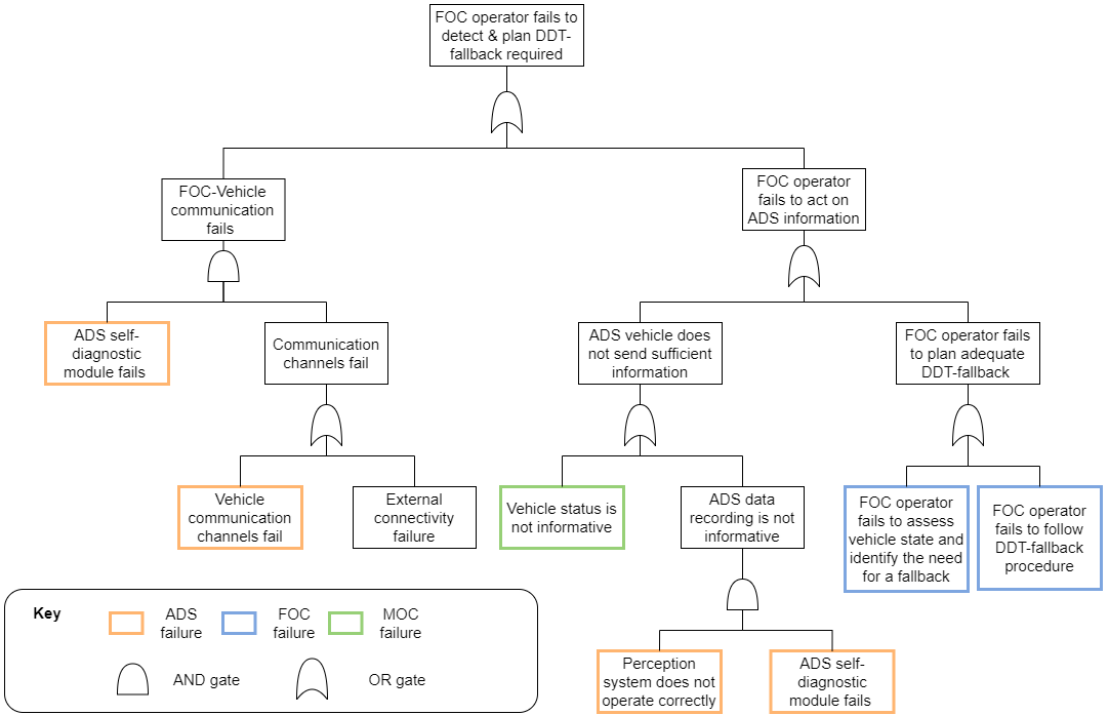

Figure 4: Example of high-level Fault Tree developed for "On-route without passenger" Event Sequence Diagram.

Table 6 presents a summary of the categories of basic events, the type of failure these represent, and which agent is responsible for their occurrence. These basic events are not completely developed to component-level failures, instead these represent function-level failures. Note that the underlying cause of many ADS vehicle

hardware and/or software failures may stem from less than adequate execution of pre-shift inspection or corrective maintenance procedures. Although not directly related to remote operations, these procedures are of key importance to support the fleets' operation, in particular, hardware failures that the ADS self-diagnostic system is not able to monitor without additional and failure-specific sensor systems (e.g., broken windshield or braking lights). Moreover, the ADS vehicle may not be capable of detecting every failure (e.g., malfunctioning lights). It is expected that the ADS developer establishes which components or subsystems require more frequent inspection to avoid unexpected operational failures, which may be crucial for both fleet operations and privately-owned vehicles.

Table 6: Basic Events for Fleet Operations Center fallback detection failure Fault Tree.

Basic Event	Failure Type	Responsible Agent
Self-diagnostic module fails	Software	ADS
Vehicle communication channels fail	Software/Hardware	ADS
External connectivity failure	External	-
Vehicle status is not informative	Maintenance/Design	MOC
Perception system does not operate correctly	Software/Hardware	ADS
Fleet Operations Center operator fails to assess vehicle state and identify the need for corrective action	Human	FOC
Fleet Operations Center operator fails to follow corrective procedure	Human	FOC

Stage III: Identifying Hazards

This section presents the main results of the third stage of the hazard identification process. The consolidation process is summarized in the following steps:

- The list of hazards is derived from event failures identified in the Event Sequence Diagram which are associated with an agent. For example, the hazard associated with the event "**The ADS vehicle detects a DDT-fallback is required**" is "**The ADS vehicle fails to detect a DDT-fallback is required**."
- Each hazard is associated with multiple failure modes (i.e., how the failure may occur) that are identified by connecting each event with specific Concurrent Task Analysis tasks and System-Theoretic Process Analysis actions. If applicable, each event is also associated with a fault tree. For example, "**The ADS vehicle fails to detect a DDT-fallback is required**" may be caused by failures at software or hardware level.

- Each failure is associated with a single risk contributor described in Table 7. Each risk contributor corresponds to a function of an agent that, when not implemented correctly, contributes to the development of the hazard scenario. This division of agent functions is valuable to determine hazard prevention and mitigation responsibilities. Elements related to inspection and maintenance operations are not considered in this analysis. More information about risks related to maintenance activities can be found in (Correa-Jullian et al., 2023, 2024a).
- Each hazard can potentially lead to various consequences, expressed through the Event Sequence Diagram end states. These consequences are assessed through the qualitative risk scale presented in the next section (Table 8).

Table 7: Risk contributor involved in remote operations breakdown and description.

Subsystem	Risk Contributor	Description
ADS	ADS vehicle	Refers to specific hardware of the vehicle, e.g., motion control.
	ADS hardware	Refers to specific vehicle hardware supporting ADS functions, e.g., instrumentation.
	ADS software	Refers to the ADS and other software-controlled processes of the vehicle.
	ADS communication	Refers to the communication channels' functionality, including hardware and software.
Fleet Operations Center (FOC)	Fleet Operations Center safety operator	Refers to remote operators located at the Fleet Operations Center's control center, focused on functional safety aspects. Monitoring the vehicle's safety and intervening to ensure the vehicle's safety are the responsibilities of the safety operator.
	Fleet Operations Center service operator	Refers to remote operators located at the Fleet Operations Center's control center, focused on mobility service aspects. Communications with passengers, first responders, and law enforcement are responsibility of the service operator.
	Fleet Operations Center communication	Refers to the functionality of the communication channels, including both hardware and software.

Qualitative Risk Assessment Scale

We categorized the safety hazards identified in our analysis using a multi-dimensional qualitative risk scale. This scale combines three factors drawn from the ISO 26262 ASIL risk assessment methodology: relative frequency, controllability, and severity (International Organization for Standardization, 2018b). In this scale, a

high-risk level is assigned to hazards that exhibit a high relative frequency, low controllability, and high severity.

We adopted a conservative approach to characterize the consequences represented by the possible outcomes. This approach favors the overestimation of errors as opposed to underestimation, thereby accounting for potential uncertainties. Given the scope of the analysis, we did not conduct a detailed breakdown of the consequences under different conditions at this stage. For example, the analysis did not examine how different travel speeds might impact the level of hazards in the event of a collision. The structure of each scale used in the analysis is described in Appendix B.

The risk level was categorized on a scale of 1-5, as shown in Table 8.

- Level 1: Very Low-level risks. The operation proceeds as expected or operational failures do not lead to imminent risks.
- Level 2: Low-level risks. The vehicle operation is interrupted but preventive and mitigative actions are available; or failures of preventive or mitigative actions do not lead to immediate consequences.
- Level 3: Medium-level risk. The vehicle's operation is interrupted and mitigative actions are available; or failures of mitigative actions do not lead to immediate consequences.
- Level 4: High-level risk. An incident has occurred, or the vehicle's operation is interrupted. Mitigative actions have failed or have not been performed, leading to immediate consequences.
- Level 5: Very high-level risk. Efforts to prevent an incident have failed. The vehicle is at risk of collision, passengers or other road users are endangered, and mitigative actions have failed or have not been performed and lead to immediate consequences.

Table 8: Resulting risk matrix.

Controllability	Exposure/ Severity	No incident*	Traffic disruption	Danger to property	Danger to life
High	Very Low	1	1	1	2
	Low	1	2	2	3
	Medium	1	2	3	3
	High	1	2	3	4
Medium	Very Low	1	2	2	3
	Low	2	3	3	4
	Medium	2	3	4	4
	High	3	4	4	5
Low	Very Low	1	2	3	3
	Low	2	3	4	4
	Medium	2	4	4	5
	High	3	4	5	5
Very Low	Very Low	2	3	3	4

Controllability	Exposure/ Severity	No incident*	Traffic disruption	Danger to property	Danger to life
	Low	3	4	4	5
	Medium	3	4	5	5
	High	4	5	5	5

* Severity Level 1: No incidents correspond to scenarios in which operation leads to any traffic, property, or injury related consequence, e.g., a passenger trip has successfully been completed. Organizational errors and failure to follow procedures are also categorized at this level as these do not produce any immediate consequences, e.g., the ADS vehicle has been incorrectly cleared for operation after failing a pre-shift inspection test. For more information, please refer to Appendix B.

Selected Results

This process resulted in identifying a total of 43 high-level hazards associated with 912 failure modes, which permitted us to trace multiple failure modes and agent interactions. Table 9 presents a selection of 20 hazard scenarios highlighting the fleet operator's remote operation functions. These hazard scenarios are mapped to the most relevant risk contributor among the Fleet Operations Center remote operations.

Table 9: List of safety hazards identified per Fleet Operations Center risk contributor.

ID	Agent	Hazard Scenario (Agent Fails to:)	Safety operator	Service operator	Communication	Highest Risk Level (R)
Operational Phase: On-route without Passengers						
1.1.3	ADS	perform DDT-fallback correctly	x		x	5
1.1.5	ADS	successfully travel to Maintenance Operations Center	x			5
1.1.6	ADS	request post-incident management procedures	x			3
1.2.1	FOC	detect DDT-fallback is required	x		x	5
1.2.2	FOC	send correct DDT-fallback command	x		x	5
1.2.3	FOC	dispatch vehicle to Maintenance Operations Center	x		x	5
1.2.4	FOC	initiate post-incident procedures	x		x	3
Operational Phase: On-route with Passengers						
2.1.2	ADS	perform DDT-fallback correctly	x		x	5
2.1.3	ADS	request post-incident management procedures	x			5

ID	Agent	Hazard Scenario (Agent Fails to:)	Safety operator	Service operator	Communication	Highest Risk Level (R)
2.2.1	FOC	detect DDT-fallback is required	x	x	x	5
2.2.2	FOC	send correct DDT-fallback command	x	x	x	5
2.2.3	FOC	initiate post-incident procedures	x	x	x	4
2.2.4	FOC	communicate with passenger	x	x	x	5
Operational Phase: Post-Incident Procedures						
5.2.1	FOC	confirm other road users are involved	x		x	4
5.2.2	FOC	contact first responders	x	x		4
5.2.3	FOC	report incident to Maintenance Operations Center	x	x	x	4
5.2.4	FOC	communicate with passenger	x	x	x	4
5.2.5	FOC	dispatch secondary vehicle for passengers	x	x	x	4
5.2.6	FOC	send correct DDT-fallback command	x		x	4
5.3.1	MOC	dispatch recovery team	x		x	4

For example: #2.2.1 "**FOC does not detect a DDT-fallback is required**" is characterized by the failure modes outlined in Table 10. These failure modes may also be triggered by prior events. Examples of corresponding prior failure modes are listed in Table 11. Based on the task decomposition performed, to determine the need for corrective action, the remote operator must assess whether the vehicle has exceeded its operating parameters. This evaluation requires the operator to be trained on the specifics outlined within the vehicle's Operational Design Domain and equipped with tools to assess the vehicle's real-time location and surroundings. Similarly, the operator is responsible for evaluating whether the vehicle has adequately responded in cases of on-board failure, collisions, external requests for a stop (e.g., by law enforcement or first responders), or incorrect execution of a response plan. The task of intervening in the vehicle's operation when necessary is expected to be performed concurrently with continuous monitoring of the vehicle, exchanging information with the vehicle as needed, and assessing whether the vehicle needs to be dispatched elsewhere.

Table 10: Example hazard scenario #2.2.1 main failure modes and agent responsibilities.

Risk Contributor	Failure Mode *Fails to/Fails to provide:*	Agent Responsible	Agent Responsibility
Safety operator	Evaluate if the operating parameters are exceeded	FOC safety operator	Follow established operating procedure
	Determine if there is an ADS vehicle failure		
	Determine if a collision has occurred		
	Determine if a passenger has requested an emergency stop		
	Determine if external party asked for a stop		
	Evaluate state of passengers and vehicle		
Fleet Operations Center communication	Receive request from ADS vehicle	FOC safety operator	Report anomalies during operation
	Receive outcome of DDT-fallback implementation		

Table 11: Example hazard scenario #2.2.1 prior failure modes and agent responsibilities.

Risk Contributor	Failure Mode *Fails to/Fails to provide:*	Agent Responsible	Agent Responsibility
ADS communication	Request a corrective action plan from Fleet Operations Center	ADS software	Verify functionality of ADS communication (diagnostics)
	Respond to request for information		
	Maintain stable communication with Fleet Operations Center		
	Transmit to Fleet Operations Center prescribed information.		
	Alert the Fleet Operations Center (safety operator) that corrective action is required		
	Request maintenance scheduling		
	Transmit communication from vehicle to Fleet Operations Center		
	Transmit communication from passenger to Fleet Operations Center		
ADS software	Transmit outcome of self-diagnostic tests	ADS software	Verify functionality of ADS software (diagnostics)

Risk Contributor	Failure Mode *Fails to/Fails to provide:*	Agent Responsible	Agent Responsibility
	Detect a vehicle communication channel failure		
	Processed perception data for remote operator supervision		Verify functionality of ADS software (e.g., perception, planning, control functions)
	Determine if a passenger has requested an emergency stop		Verify functionality of ADS software (passenger interaction)
	Determine if external party requested a stop		
	Recorded diagnostic logs for remote operator supervision	ADS software	Review state of ADS software (diagnostics)
	Detect that transmitted vehicle status is incorrect or incomplete		
	Use updated/correct High-Density maps		Review state of ADS software (built-in knowledge)
	Enforce updated/correct operating limits		
	Detect an external connectivity failure	Safety operator	Follow established operating procedure (DDT-fallback required)
Safety operator	Monitor ADS vehicle operations	Safety operator	Follow established operating procedure
	Evaluate ADS vehicle safety		
	Determine if more information is needed		
	Evaluate information from vehicle's ADS		
	Respond to ADS request		
Service operator	Receive requests from passengers	Service operator	Follow established operating procedure
	Alert of passenger emergency stop request		
	Communicate with passengers		
	Alert the Fleet Operations Center (safety operator) that corrective action is required, or request secondary vehicle.		
FOC communication	Transmit request for specific information to the vehicle's ADS	Safety operator	Report communication channel anomalies

Risk Contributor	Failure Mode *Fails to/Fails to provide:*	Agent Responsible	Agent Responsibility
	Confirm operational guidelines update		Follow established operating procedure

*This table is read as: The [Risk Contributor] presents the failure mode [Fails to/Fails to provide]. The [Agent Responsible] is expected to perform [Agent Responsibility] to avoid the hazard scenario and is affected by [Related Hazard] scenario.

The breakdown of these tasks emphasizes the significance of reliable and secure communication channels (such as video, sensors, and alarms) between the Fleet Operations Center safety operators and the ADS vehicle. This crucial aspect is further underscored by feedback loops between the vehicle and the safety operator that, if disrupted, may result in a hazard scenario (e.g., faulty sensor data transmitted from the ADS prevents the safety operator from identifying an issue with the vehicle). For example, the quality and completeness of the information recorded by the vehicle plays a vital role in providing the remote operator with the necessary tools to determine whether some corrective action needs to be taken, which depends not only on the reliability of the communication network but also on the design of the Fleet Operations Center's human-system interface. While communication failures can occur unexpectedly during the vehicle's operation, they may be a result of imperfect inspection and maintenance procedures or inadequate frequency of maintenance activities.

Moreover, if the ADS self-diagnostic module fails to identify on-board failures, the remote operator's ability to detect potential threats to the vehicle's operation could be significantly reduced. Factors such as training, shift hours, and other variables can also impact the operator's situational awareness. Additionally, pre-defined corrective procedures may not be suitable for specific hazardous situations that may arise. This is particularly critical during the initial phase of fleet operations when information on potential risks is limited or when vehicles encounter changing road conditions (e.g., construction zones, faulty/reprogrammed traffic signals). These procedures become critical, especially when addressing hardware failures that the ADS self-diagnostic system cannot monitor without additional dedicated sensor systems (e.g., broken windshield or malfunctioning braking lights). Furthermore, the ADS vehicle may not be capable of detecting every failure that impacts its performance. The ADS vehicle manufacturer and fleet operator should establish which components or subsystems require more frequent inspections to prevent unexpected operational failures.

This process is repeated until a comprehensive list of contributing failure modes, as presented in Table 10 and Table 11, is obtained for each derived hazard scenario. This enables tracing contributing failures modes and risk contributors across multiple hazards occurring during the same or distinct operational phases. Consequently, linking the contributing failure modes to specific risk contributors can be used to derive a list of operational safety responsibilities for each agent involved. Appendix C provides a summary of the contributing failure modes involved in remote operation of the ADS vehicle.

The hazards identified highlight the significant role of reliable and secure communication channels between the ADS-equipped vehicle and the remote operators tasked to supervise its functions. Likewise, while the ADS is expected to operate independently within the conditions established by its operating parameters, hazards arising from system malfunctions or rare hazards underscore the need for a layered-safety approach, where remote operation assistance may play an important role in emergency situations.

Section 4: Development of Risk Mitigation Measures

The methodology used to determine the safety responsibilities of the fleet operator is illustrated in Figure 5. The findings from Section 3 define the hazard scenarios by identifying various contributing failure modes. Further, each contributing failure mode is associated with a primary risk contributor and an agent responsible for preventing or reducing malfunctions, errors, or failures associated with the risk contributors. In many cases, the risk contributor and responsible agent align with the same functional sub-agent. This correlation occurs when the hazard scenarios stem from operational errors in the agents' performance.

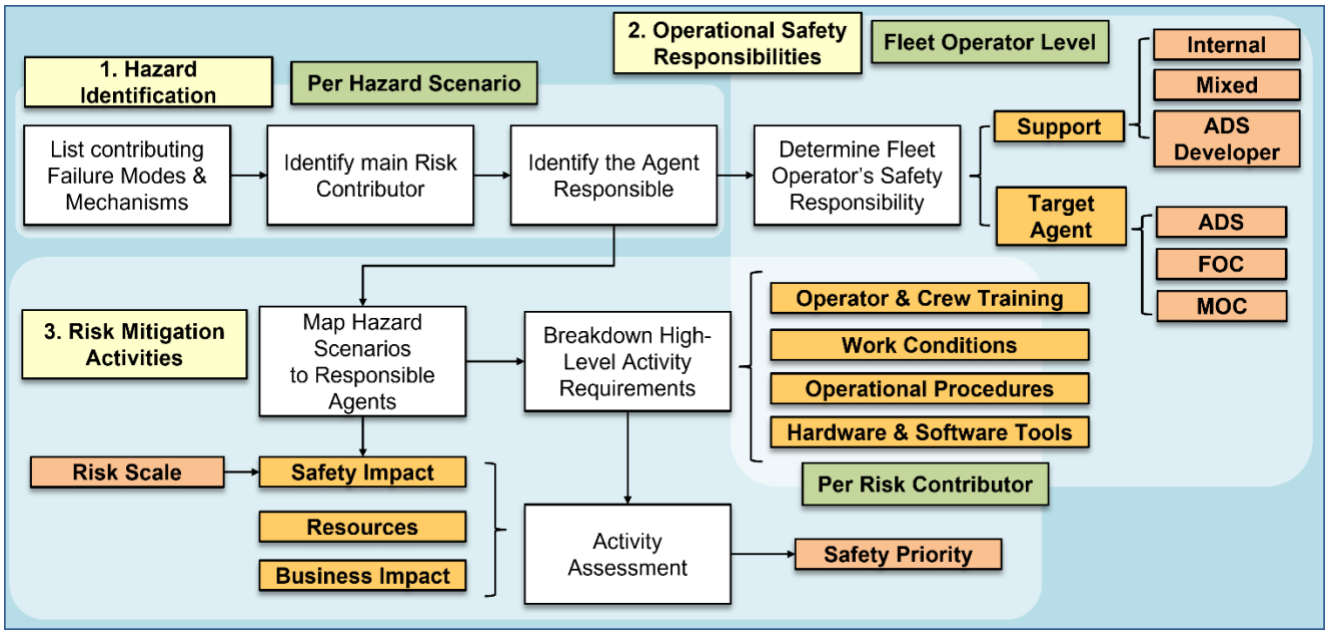

Figure 5: Derivation and assessment of risk mitigation activities.

Once the responsible agent has been identified, the next step involves determining the fleet operator's responsibilities in supporting their tasks. The fleet operator's role is to comply with the operational requirements specified by the ADS developer, develop and implement operational procedures, and provide training and/or appropriate tools for each agent to effectively perform their tasks. To further clarify the division of responsibilities, each high-level activity is assessed to determine if the fleet operator can develop them internally or if input from the ADS developer is necessary. For example, certain inspection and maintenance requirements are expected to be established by the ADS developer. In addition, some operational procedures or tools may require input from the ADS developer, depending on the fleet operator's access to the system's hardware and software components.

The risk mitigation activities are derived by further cataloguing the fleet operator's safety responsibilities, focusing on the elements required for the fleet operator's designated agent to perform the safety responsibilities. The functional breakdown of the high-level activity requirements considers the types of activities presented in Table 12. The risk mitigation activities are categorized according to the kind of support required: procedures, training, tools, and working conditions. This methodology guarantees that the risk mitigation activities cover all the identified safety responsibilities. Additionally, all safety hazard scenarios are cross-referenced through the safety responsibilities with the risk mitigation activities.

Table 12: Risk mitigation activity types considered.

Activity type	Description
Operational Procedures	Operational guidelines developed to support the activities of the human operators and crew, as well as to define the operational conditions of the ADS vehicle. These procedures include regulating the content, frequency, and requirements for communications, activities, and interactions between the agents and external entities.
Operator & Crew Training	Specific training activities focused on the tasks the remote operators and maintenance crew are expected to perform. This includes familiarization with the operational procedures, required Human-System Interface functions, emergency procedures and workplace safety guidelines.
Hardware & Software Tools	Hardware and software tools necessary for the agents to perform expected tasks. These include necessary communication devices, reliable connectivity conditions, passenger interaction devices, and tolls to support maintenance activities.
Work Conditions	General policies and equipment that are designed to improve multiple aspects of workplace adequacy as well as human operator and crew performance.

Qualitative Risk Mitigation Activity Assessment Scale

We developed a qualitative scale that categorizes the identified risk mitigation activities. Each activity is assigned a business impact category based on the potential safety impact and the estimated resources (cost, time, frequency) required by fleet operator to implement them. The structure of this scale is described in the following sections. More details are provided in Appendix D.

Business Impact

Each risk mitigation activity is characterized by the three category-based scales (cost, time, frequency) and the safety impact (derived from the risk scale). A combination of these scales is consolidated into a *business impact* indicating the priority of activity implementation. The business impact is categorized into four priority classes presented in Table 13 (1-4 from highest to lowest). This is represented by the following expression:

$$B_R = S_I \times R_C \times R_T \times R_F,$$

where R_S is the safety impact rank (1-5 scale, see Table D.1), R_C is the implementation cost level (1-3 scale, see Table D.3), R_T is the implementation time level (1-3 scale, see Table D.4) and R_F is the frequency of implementation (1-3 scale, see Table D.5). The values of B_R are then organized into the categories as shown in Table 14.

Table 13: Business impact scale levels.

Business impact	B_R Rank	B_R Rank range
Very high	1	[1, 4]
High	2	[5, 8]
Moderate	3	[9, 24]
Low	4	>24

For instance, a "high" business impact ($B_R = 1$) relates to low-effort activities with high safety impact. These activities would require a comparatively low implementation cost (Cost: Low), time (Time: Low), and frequency (Frequency: Once) that prevent or mitigate high-risk hazard scenarios. The business impact is represented by a four-dimensional matrix presented in Table 14. This table combines multiple lower-dimension matrices according to the activities' safety impact, cost, frequency, and time dimension.

Table 14: Consolidated business impact matrix.

Safety impact	Cost	Frequency	Time		
			High	*Medium*	*Low*
Very high	High	Once	3	2	1
		Periodic	3	3	2
		Constant	4	3	3
	Medium	Once	2	1	1
		Periodic	3	2	1
		Constant	3	3	2
	Low	Once	1	1	1
		Periodic	2	1	1
		Constant	3	2	1
High	High	Once	3	3	2
		Periodic	4	3	3
		Constant	4	4	3
	Medium	Once	3	2	1
		Periodic	3	3	2
		Constant	4	3	3

Safety impact	Cost	Frequency	Time		
			High	*Medium*	*Low*
	Low	Once	2	1	1
		Periodic	3	2	1
		Constant	3	3	2
Moderate	High	Once	4	3	3
		Periodic	4	4	3
		Constant	4	4	4
	Medium	Once	3	3	2
		Periodic	4	3	3
		Constant	4	4	3
	Low	Once	3	2	1
		Periodic	3	3	2
		Constant	4	3	3
Low	High	Once	4	3	3
		Periodic	4	4	3
		Constant	4	4	4
	Medium	Once	3	3	2
		Periodic	4	3	3
		Constant	4	4	3
	Low	Once	3	2	1
		Periodic	3	3	2
		Constant	4	3	3
Very Low	High	Once	4	3	3
		Periodic	4	4	3
		Constant	4	4	4
	Medium	Once	3	3	2
		Periodic	4	3	3
		Constant	4	4	3
	Low	Once	3	2	1
		Periodic	3	3	2
		Constant	4	3	3

Safety Priority Rank

Some activities with high safety impact may require a higher implementation cost or time or must be implemented periodically or constantly. This business impact scale would then rank these activities with a low priority, regardless of the safety impact. Hence, a modification is introduced: any risk mitigation activity with a

"Very high" or "High" safety impact is prioritized with a Safety Priority Rank 1; overriding the business impact scale for those activities but retaining the rank for lower safety impact activities. This is represented by the following expression, resulting in the categories presented in Table 15.

$$S_R = \{1 \quad if \ \leq 2\ B_R \quad if\ S_I > 2$$

Table 15: Safety priority scale levels.

Safety priority	S_R Rank	S_R Rank range
Top	1	1
Very high	2	[2, 4]
High	3	[5, 8]
Moderate	4	[9, 24]
Low	5	>24

High-Level Safety Responsibilities

This section summarizes the high-level fleet operator's safety responsibilities regarding the remote operators' tasks. These are summarized in Table 16, Table 17, and Table 18 depending on the support required to be implemented by the fleet operator.

Table 16: High-level safety responsibilities for the fleet operator to develop internally.

Fleet operator role	High-level activity	Agent
Develop	Adequate Human-System Interface (alarm systems, traffic monitoring) for FOC remote operators	Safety operator
Develop	Staffing policies (workload, shifts Procedural)	General (FOC)
Implement	Operation procedures (Maintenance operations)	Safety operator
Implement	Operation procedures (Passenger requests)	Service operator
Provide	Training and adequate tools (DDT-fallback, Monitoring, Dispatching, Connectivity, Incident management)	Safety operator
Provide	Training and adequate tools (Passenger requests, Incident management, Connectivity)	Service operator

Table 17: High-level safety responsibilities to coordinate with ADS developer.

Fleet operator role	High-level activity	Target agent
Develop	Adequate Human-System Interface (intervention mechanisms) for remote operators	Service operator
Implement	Operation procedures (Incident management)	Service operator
Implement	Operation procedures (Incident management DDT-fallback, Monitoring, Dispatching, Procedural)	Safety operator

Table 18: High-level safety responsibilities to adapt from the ADS Developer.

Fleet operator role	High-level activity	Target agent
Comply	Fleet is updated and operating in adequate conditions (DDT: object and event detection)	ADS vehicle (software)
Develop	Adequate Human-System Interface (intervention mechanisms) for remote operators (Procedural)	Safety operator
Implement	ADS ODD limitations based on MaaS and connectivity requirements (ADS Developer)	ADS software

Risk Mitigation Activities

The methodology for deriving risk mitigation activities resulted in a list of 140 activities, each evaluated based on their potential safety impact and the resources required for implementation (cost, time, frequency). These activities encompass various aspects of Level 4 ADS fleet operations for MaaS and can be condensed into 63 distinct activities specifically related to remote vehicle fleet operations. These activities cover areas such as operator and crew training, development of operational procedures, software and hardware tools, and factors related to the adequacy of the workplace.

Table 19 lists the top priority safety activities identified. The remote operators are responsible for carrying out these key activities which include those related to organizational management of change, training remote supervisors to monitor and intervene in vehicle operations, providing adequate working conditions for operators, enforcing the vehicle to operate within stable wireless connectivity areas, dispatching requirements, and coordinating internal incident mitigation activities. Providing adequate working conditions involves considering human factors principles to support operators and crew members in performing their tasks. These factors may be related to environmental conditions (lighting, noise, ventilation, ergonomic workstation design), floor layouts (location and orientation of equipment), and compliance with safety regulations specific to the

workplace. Adequate Human-System Interface and alarm design is also crucial for workplace adequacy, ensuring that it supports operators in their tasks by considering task complexity, time restrictions, and interactions with other agents.

Note that resource-intensive risk mitigation activities may be ranked as having a "Low" business impact due to the resources required for implementation. However, this ranking does not diminish their significance in terms of safety. To address this, a safety impact rule is introduced to emphasize the activities with the greatest safety impact. Therefore, the activities presented in Table 19 with a "Low" business impact are essential for safety and service operators in mitigating high-risk hazard scenarios, despite requiring a significant level of resources to implement, such as providing and maintaining an adequate Human-System Interface. The complete list of risk mitigation activities identified related to ADS fleet operations are detailed in Appendix D.3.

Table 19: Top safety priority risk mitigation activities.

Agent	Activity type	Activity purpose	Business impact
Safety Operator	Work conditions	Determine and implement adequate length of shifts	Very High
Safety Operator	Work conditions	Provide adequate working conditions	Very high
Service Operator	Tools	Provide in-vehicle passenger communication devices	Very high
ADS Vehicle	Tools	Provide communication devices between agents (Fleet Operations Center, Maintenance Operations Center)	Very high
Service Operator	Work conditions	Determine adequate length of shifts	Very high
Safety Operator	Procedures	Establish information sharing procedures between fleet operator's agents	Very high
Service Operator	Procedures	Establish information sharing procedures between fleet operator's agents	Very high
Service Operator	Procedures	Establish passenger data privacy policies	Very high
Safety Operator	Training	Maintain operational procedures updated	Very high
Service Operator	Training	Maintain operational procedures updated	Very high
ADS Vehicle	Procedures	Enforce data transmission and storage policies	High
ADS Vehicle	Tools	Provide navigation and High-Definition map support	High
Service Operator	Procedures	Manage requests from other agents (Fleet Operations Center, Maintenance Operations Center)	High
ADS Vehicle	Procedures	Enforce vehicle connectivity requirements	High

Agent	Activity type	Activity purpose	Business impact
ADS Vehicle	Procedures	Determine goals and strategies for hazard mitigation.	Medium
ADS Vehicle	Procedures	Observe defined operating parameters and local road restrictions	Medium
ADS Vehicle	Procedures	Monitor self-diagnostic capabilities (vehicle hardware, software)	Medium
ADS Vehicle	Procedures	Receive and implement hazard response commands	Medium
ADS Vehicle	Procedures	Interact with first responders/law enforcement	Medium
Safety Operator	Training	Use Human-System Interface to monitor and intervene the vehicle's operation	Medium
Safety Operator	Tools	Provide adequate Human-System Interface design to support agent tasks	Low
Service Operator	Tools	Provide adequate Human-System Interface design to support agent tasks	Low
Safety Operator	Work conditions	Provide and maintain functioning Human-System Interface	Low
Service Operator	Work conditions	Provide and maintain functioning Human-System Interface	Low

Section 5: Main Findings and Conclusions

With the potential future introduction of large-scale Level 4 ADS fleet operations for Mobility as a System transport, it will be crucial to determine the activities, procedures, and requirements necessary to ensure operational safety, as is defining the roles of those entities responsible for achieving and maintaining safety. The main findings regarding key risk mitigation activities for ADS fleets, identified through a safety risk analysis, can be summarized as follows:

- Top priority risk mitigation activities for fleet operators include managing change, training remote supervisors to monitor and intervene in vehicle operations, providing suitable working conditions for employees, enforcing vehicle connectivity and dispatching requirements, and coordinating internal incident mitigation activities.
- Without onboard trained safety drivers, remote fleet supervisors will play a crucial role in ensuring passenger and vehicle safety. Their top tasks include monitoring the vehicle's operation and intervening when required to ensure safety. Potential responsibilities include using indirect control methods such as directing a disabled vehicle to a waypoint or issuing commands to the vehicle directing it to a safe location until assistance can arrive.
- The design of the overall system and human-system interface tools should consider human and physical time constraints, allowing remote operators sufficient time to perform monitoring, and expected driving and passenger assistance tasks efficiently under emergency situations (Mutzenich et al., 2021).
- Fleet operators may consider further restricting vehicle operations beyond the operational limits set by the ADS developers to ensure reliable communication with passengers at all times. We suggest developing a Fleet Operational Design Domain to specify the conditions under which ADS vehicles can safely operate as part of MaaS transport.
- The extent of knowledge and information exchange between fleet operators and ADS developers is currently uncertain. This raises questions whether fleet operators' have sufficient knowledge about ADS software and hardware specifications, requirements, and maintenance procedures to ensure operational safety and regulatory compliance and whether ADS developers need to take a more active role in educating fleet operators.

It should be noted that several of the identified hazards and risk mitigation measures are also applicable in the case of consumer-level passenger vehicles equipped with limited ADS capabilities. In these situations, remote operators may play a less active role in operational safety, but nevertheless provide support to passengers during operations or in the event of an emergency.

References

Automated Vehicle Safety Consortium AVSC. (2019). *AVSC00001201911: AVSC Best Practice for In-Vehicle Fallback Test Driver Selection, Training, and Oversight Procedures for Automated Vehicles Under Test*. https://www.sae.org/standards/content/avsc00001201911/

AVSC00006202103. (2021). *AVSC Best Practice for Metrics and Methods for Assessing Safety Performance of Automated Driving Systems (ADS)*.

Blanco, M., Chaka, M., Stowe, L., Gabler, H. C., Weinstein, K., Gibbons, R. B., Neurauter, L., McNeil, J., Fitzgerald, K. E., Tatem, W., & Fitchett, V. (2020). *FMVSS Considerations for Vehicles With Automated Driving Systems: Volume 1* (V. T. T. Institute (ed.)). https://rosap.ntl.bts.gov/view/dot/54287

Chaka, M., Blanco, M., Stowe, L., McNeil, J., Kefauver, K., Fitchett, V. L., Fitzgerald, K. E., Trimble, T. E., Kizyma, D., Neurauter, L., Hardy, W. N., Anderson, G. T., Schultz, J., Thorn, E., Harper, C., Weinstein, K., Institute, V. T. T., & Administration, N. H. T. S. (2021). *FMVSS Considerations for Vehicles With Automated Driving Systems: Volume 2*. *1*(April), 630p. https://rosap.ntl.bts.gov/view/dot/54442%0Ahttps://trid.trb.org/view/1768673

Chang, Y. H. J., & Mosleh, A. (2007). Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents. Part 4: IDAC causal model of operator problem-solving response. *Reliability Engineering & System Safety*, *92*(8), 1061–1075. https://doi.org/10.1016/j.ress.2006.05.011

Correa-Jullian, C., McCullough, J., Ramos, M., Ma, J., Lopez Droguett, E., & Mosleh, A. (2022a). Modeling Fleet Operations of Autonomous Driving Systems in Mobility as a Service for Safety Risk Analysis. In M. C. Leva, E. Patelli, L. Podofillini, & S. Wilson (Eds.), *32nd European Safety and Reliability Conference (ESREL 2022)*. Research Publishing Services. https://doi.org/10.3850/978-981-18-5183-4_J03-06-566-cd

Correa-Jullian, C., McCullough, J., Ramos, M., Ma, J., Lopez Droguett, E., & Mosleh, A. (2022b). Safety Hazard Identification for Autonomous Driving Systems Fleet Operations in Mobility as a Service. *Probabilistic Safety Assessment and Management, PSAM 2022*.

Correa-Jullian, C., McCullough, J., Ramos, M., Mosleh, A., & Ma, J. (2023). Safety Hazard Identification of Inspection and Maintenance Operations for Automated Driving Systems in Mobility as a Service. *Proceeding of the 33rd European Safety and Reliability Conference*, 281–288. https://doi.org/10.3850/978-981-18-8071-1_P326-cd

Correa-Jullian, C., Ramos, M. A., Mosleh, A., & Ma, J. (2024a). An STPA-Based Analysis of Automated Driving Systems Fleet Maintenance Activities. *2024 Annual Reliability and Maintainability Symposium (RAMS)*, 1–6. https://doi.org/10.1109/RAMS51492.2024.10457750

Correa-Jullian, C., Ramos, M., Mosleh, A., & Ma, J. (2024b). Operational safety hazard identification methodology for automated driving systems fleets. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*. https://doi.org/10.1177/1748006X241233863

De Gelder, E., Elrofai, H., Saberi, A. K., Paardekooper, J.-P. P., Op den Camp, O., & de Schutter, B. (2021). Risk

Quantification for Automated Driving Systems in Real-World Driving Scenarios. *IEEE Access*, *9*, 168953–168970. https://doi.org/10.1109/ACCESS.2021.3136585

Ferreira, S., Faezipour, M., & Corley, H. W. (2013). Defining and addressing the risk of undesirable emergent properties. *SysCon 2013 - 7th Annual IEEE International Systems Conference, Proceedings*, 836–840. https://doi.org/10.1109/SYSCON.2013.6549981

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

International Organization for Standardization. (2018b). *ISO 26262:2018, Road vehicles — Functional safety*. https://www.iso.org/standard/68383.html

Johnson, C. W. (2006). What are emergent properties and how do they affect the engineering of complex systems? *Reliability Engineering and System Safety*, *91*(12), 1475–1481. https://doi.org/10.1016/j.ress.2006.01.008

Khastgir, S., Birrell, S., Dhadyalla, G., Sivencrona, H., & Jennings, P. (2017). Towards increased reliability by objectification of Hazard Analysis and Risk Assessment (HARA) of automated automotive systems. *Safety Science*, *99*, 166–177. https://doi.org/10.1016/j.ssci.2017.03.024

Khastgir, S., Brewerton, S., Thomas, J., & Jennings, P. (2021). Systems Approach to Creating Test Scenarios for Automated Driving Systems. *Reliability Engineering and System Safety*, *215*, 107610. https://doi.org/10.1016/j.ress.2021.107610

Kramer, B., Neurohr, C., Büker, M., Böde, E., Fränzle, M., & Damm, W. (2020). Identification and Quantification of Hazardous Scenarios for Automated Driving. In *Lecture Notes in Computer Science: Vol. 12297 LNCS* (pp. 163–178). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-030-58920-2_11

Leveson, N., & Thomas, J. (2018). *STPA Handbook*. https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

Mutzenich, C., Durant, S., Helman, S., & Dalton, P. (2021). Updating our understanding of situation awareness in relation to remote operators of autonomous vehicles. *Cognitive Research: Principles and Implications*, *6*(1), 9. https://doi.org/10.1186/s41235-021-00271-8

National Highway Traffic Safety Administration. (2017). Automated Driving System 2.0: A Vision for Safety. In *U.S. Department of Transportation*. https://www.nhtsa.gov/vehicle-manufacturers/automated-driving-systems

National Highway Traffic Safety Administration. (2022). Summary Report: Standing General Order on Crash Reporting for Automated Driving Systems. *U.S. Department of Transportation Summary Report DOT HS 813 324*, *June*, 1–9. www.nhtsa.gov/sites/nhtsa.gov/files/2022-06/ADS-SGO-Report-June-2022.pdf

National Research Council (US) Committee on Risk Assessment of Hazardous Air Pollutants. (1994). *Science and Judgment in Risk Assessment*. Washington (DC): National Academies Press (US); https://www.ncbi.nlm.nih.gov/books/NBK208270/

Ramos, M. A., Correa Jullian, C., McCullough, J., Ma, J., & Mosleh, A. (2023). Automated Driving Systems

Operating as Mobility as a Service: Operational Risks and SAE J3016 Standard. *2023 Annual Reliability and Maintainability Symposium (RAMS)*, 1–6. https://doi.org/10.1109/RAMS51473.2023.10088244

Ramos, M. A., Thieme, C. A., Utne, I. B., & Mosleh, A. (2020a). Human-system concurrent task analysis for maritime autonomous surface ship operation and safety. *Reliability Engineering and System Safety*, *195*, 106697. https://doi.org/10.1016/j.ress.2019.106697

Ramos, M. A., Thieme, C. A., Utne, I. B., & Mosleh, A. (2020b). A generic approach to analysing failures in human – System interaction in autonomy. *Safety Science*, *129*, 104808. https://doi.org/10.1016/j.ssci.2020.104808

Ramos, M. A., Utne, I. B., & Mosleh, A. (2019). Collision avoidance on maritime autonomous surface ships: Operators' tasks and human failure events. *Safety Science*, *116*, 33–44. https://doi.org/10.1016/j.ssci.2019.02.038

SAE International. (2021). *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*. SAE Standard J3016_202104.

Sohrabi, S., Khodadadi, A., Mousavi, S. M., Dadashova, B., & Lord, D. (2021). Quantifying the automated vehicle safety performance: A scoping review of the literature, evaluation of methods, and directions for future research. *Accident Analysis and Prevention*, *152*(January), 106003. https://doi.org/10.1016/j.aap.2021.106003

Thieme, C. A., Mosleh, A., Utne, I. B., & Hegde, J. (2020a). Incorporating software failure in risk analysis – Part 1: Software functional failure mode classification. *Reliability Engineering and System Safety*, *197*, 106803. https://doi.org/10.1016/j.ress.2020.106803

Thieme, C. A., Mosleh, A., Utne, I. B., & Hegde, J. (2020b). Incorporating software failure in risk analysis––Part 2: Risk modeling process and case study. *Reliability Engineering and System Safety*, *198*, 106804. https://doi.org/10.1016/j.ress.2020.106804

Thorn, E., Kimmel, S., & Chaka, M. (2018). A Framework for Automated Driving System Testable Cases and Scenarios. In *DOT HS 812 623* (Issue September). www.ntis.gov.

Yang, X., Utne, I. B., Sandøy, S. S., Ramos, M. A., & Rokseth, B. (2020). A systems-theoretic approach to hazard identification of marine systems with dynamic autonomy. *Ocean Engineering*, *217*, 107930. https://doi.org/10.1016/J.OCEANENG.2020.107930

Appendix A: List of Reviewed ADS Developers/Operators Resources for Model Fleet Development

- Apple (Apple, 2019)
- Argo AI (ArgoAI, 2021)
- Aurora (Aurora, 2021, 2022)
- Easy Mile (EasyMile, 2020)
- Ford (Ford, 2021)
- General Motors (General Motors, 2018)
- Local Motors (Local Motors, 2019)
- Lyft (Lyft, 2020)
- Motional (Motional, 2021)
- Nauto (Nauto, 2021)
- Navya (Navya, 2019)
- Nvidia (NVIDIA, 2021)
- Optimus Ride (Optimus Ride, 2019)
- Pony AI (Pony.ai, 2020)
- Toyota (Toyota, 2020)
- Waymo (Waymo, 2021)
- WeRide (WeRide, 2020)
- Zoox (Zoox, 2018, 2021)

Appendix B: Qualitative Risk Scale

A qualitative risk scale is proposed to categorize the identified safety hazards. Each safety hazard is assigned a risk category based on its potential consequences, represented by the end states of the Event Sequence Diagrams developed for each operational phase. Given the scope of the analysis, a detailed breakdown of the consequences under different conditions is not performed at this point (e.g., different speeds may result in different hazard levels in case of a collision).

The proposed multi-dimensional qualitative risk scale is composed of a combination of "relative frequency," "controllability," and "severity" inspired by the ISO 26262 ASIL risk assessment methodology (International Organization for Standardization, 2018b). For this work, a high relative frequency, low controllability, and high severity would result in a high risk. A conservative approach is used to characterize the consequences represented by the Event Sequence Diagram end states. Conservative risk assessments are generally adopted when the analysis contains significant uncertainties (National Research Council (US) Committee on Risk Assessment of Hazardous Air Pollutants., 1994). There are two main sources of uncertainties in this analysis. The first arises from the project's scope; the specific conditions in which the risk scenarios take place are not defined (e.g., weather conditions, vehicles' speed, surrounding traffic information). The second main source of uncertainties refers to the lack of probabilistic or frequency data for complete risk quantification, including hardware, software, and human failures for ADS Level 4 operating as MaaS. This approach is a specific strategy employed to address uncertainty and variability for estimating risk that favors one type of error (overestimation) over its converse (underestimation). For instance, any incidental scenario in which a passenger or other road user is involved is categorized as high severity (Level 4). Despite the potential overestimation of risks, the proposed scale is satisfactory for describing and categorizing the safety hazards in a hierarchical approach.

The structure of each of these scales is described in the following sections.

B.1 Severity scale

The severity is classified on a scale from 1 to 4. The consequences include traffic disruption, property damage-only (PDO), and risk of fatality and injury (to passengers and/or other road users). The following definitions are adopted (Table B.1):

- Level 1 corresponds to scenarios in which the operation does not lead to any traffic, property, or injury related consequence, e.g., a passenger trip has been successfully completed. Organizational errors and failure to follow procedures are also included at this level as these do not produce any immediate consequences.
- Level 2 corresponds to scenarios in which the interruption of an ADS vehicle's operation causes traffic disruptions and any incidents that may occur are so minor as to not result in property damage or injury.

It should be noted that some conditions may lead to more or less severe consequences. For instance, multiple vehicles entering Minimal Risk Condition (MRC) close to hospitals or evacuation routes cause a traffic disruption that may pose a danger to lives, as well as vehicles entering MRC in areas that reduce the road visibility to other road users.

- Level 3 corresponds to scenarios in which the ADS vehicle's operation has been interrupted or has been involved in an incident. No aggravating factors are present, i.e., no passengers or other road users have been exposed to harm.
- Level 4 corresponds to scenarios in which the ADS vehicle's operation has been interrupted or has been involved in an incident. This level also covers scenarios where the vehicle is not responsive to remote commands. One or more aggravating factors are present, i.e., passengers or other road users have been exposed to harm.

A conservative approach is taken toward the presence of potential hazards for passengers on board and other road users in the vicinity of the ADS vehicle. As a result, most of the post-incident scenarios are classified as level 4 (fatality and injury) instead of level 3 (PDO), regardless of the severity of the incident itself.

Table B. 1: Description of qualitative severity scale.

Consequence	Description	Level	Examples
No incident	The operation occurs as expected. No operational errors that lead to immediate hazards.	1	The vehicle safely completes a trip to the intended destination with no incidents.
Traffic disruption	The vehicle's operation is interrupted, e.g., a crash does not occur or if it does occur, it is so minor as to not result in property damage and injury. The vehicle achieves Minimal Risk Condition and needs to be retrieved by the maintenance crew or operates	2	The ADS vehicle is dispatched to the Maintenance Operations Center in MR-DDT condition.
			The vehicle engages Minimal Risk Condition and post-incident procedures are initiated. No other road users are involved.
			The vehicle engages Minimal Risk Condition and post-incident procedures are not initiated. No other road users are involved.

Consequence	Description	Level	Examples
	under MR-DDT conditions.		
Property damage-only (PDO)	The vehicle is involved in an incident where no passengers or road users are injured.	3	Incident without passengers onboard and no other road users are injured. Post-incident procedures are followed.
			Incident without passengers onboard and no other road users are involved. Post-incident procedures are not followed.
Fatality and Injury	The vehicle is (1) involved in an incident involving injuries or fatalities to vehicle occupants and/or other road users, or (2) unresponsive to remote commands with passengers onboard and/or affecting other road users.	4	Communication between vehicles and Fleet Operations Center is limited or interrupted. Vehicle and/or passengers are in an unknown state.
			The vehicle is unreachable or unresponsive to remote commands and fails to autonomously implement DDT-fallback actions when required.
			Incidents with or without passengers onboard and/or other road users are involved. Post-incident procedures are followed.
			Incidents with or without passengers onboard and/or other road users are involved. Post-incident procedures are not followed.
			The Fleet Operations Center is unaware other road users are involved in the incident and does not contact first responders or does not provide them with correct information.

B.2 Controllability scale

According to the Automotive Safety Integrity Level in the ISO 26262 functional safety standard, controllability represents the level of the ability of the driver to avoid harm. However, several challenges have been identified in applying the controllability scale, particularly in the context of automated vehicle operation (De Gelder et al., 2021; Khastgir et al., 2017). However, in a MaaS context with Level 4 ADS and no safety driver onboard, the term can be adapted to represent the ability of the participating agents (the ADS vehicle, remote operators, and maintenance crew members) to avoid harm. This provides a structured approach to categorize scenarios based on how successful these agents are in performing predefined tasks and procedures. If the three agents act as expected, they have a higher ability to prevent and mitigate harm, i.e., the operation is designed such

that harm can be avoided in most circumstances. Thus, a higher level of controllability is achieved when the ADS vehicle, the remote operators, and the maintenance crew act according to the operational requirements. The agents' actions are categorized as either:

- Prevention actions: Actions available to avoid an incident occurring, e.g., a vehicle detects a failure and safely enters Minimal Risk Condition (with or without assistance from the Fleet Operations Center).
- Mitigation actions: Actions available to mitigate harm after an incident has occurred, e.g., after a vehicle enters Minimal Risk Condition, the Fleet Operations Center operator initiates post-incident procedures.

The controllability is assessed through four levels (Table B.2):

- High (1): High controllability refers to scenarios in which all the participating agents act as expected. This includes scenarios in which the vehicle is rerouted to the Maintenance Operations Center due to non-safety critical failures.
- Medium (2): Medium controllability refers to scenarios in which one of the agents does not act as expected. However, other agents may perform additional preventive or mitigative actions. For instance, the Maintenance Operations Center fails to detect a vehicle failure during an inspection. However, the ADS and the Fleet Operations Center may detect failure during operation, and the vehicle can perform corrective actions before causing an incident.
- Low (3): Low controllability refers to scenarios in which two or more participating agents do not behave as expected. This level refers to scenarios where agents fail to prevent harm, although mitigation actions may still be performed, e.g., the remote operator follows the post-incident procedures to recover the vehicle.
- Very low (4): Very low controllability refers to scenarios in which an incident has occurred, and no preventive or mitigative actions are available for the agents to prevent or mitigate consequences. This includes failures to implement safety-related measures during post-incident procedures (e.g., contacting first responders).

Table B. 2: Description of qualitative controllability scale.

Controllability	Description	Level	Examples
High	All agents behave as expected.	1	The vehicle safely completes a trip to the intended destination with no incidents.
			The ADS vehicle is dispatched to the Maintenance Operations Center in MR-DDT condition.
Medium	An agent does not behave as expected and both preventive and mitigative	2	The ADS system may engage Minimal Risk Condition if the self-diagnostic module detects a system failure, and the remote operator may engage MR-DDT or Minimal Risk Condition if abnormal vehicle behavior is detected.

Controllability	Description	Level	Examples
	actions may be available.		The vehicle engages Minimal Risk Condition and post-incident procedures are available to mitigate risks.
Low	Two or more agents do not behave as expected and no preventive actions are available. Mitigation actions may still be available.	3	The vehicle engages Minimal Risk Condition, but post-incident procedures are not initiated. Mitigation actions are still available, as the remote operator may initiate post-incident procedures after communicating with passengers and/or first responders.
			Fleet Operations Center remote operator fails to dispatch a secondary vehicle for passengers to continue the trip after a vehicle failure. Mitigation actions are still available (e.g., the remote operator may dispatch a secondary vehicle after communicating with passengers).
Very Low	Two or more agents do not behave as expected and no preventive or mitigative actions are available.	4	The vehicle is unreachable or unresponsive to remote commands and fails to autonomously implement DDT-fallback actions when required.
			Communication between vehicles and Fleet Operations Center is limited or interrupted. Vehicle and/or passengers are in unknown state.
			The vehicle engages Minimal Risk Condition and post-incident procedures are not followed.
			Fleet Operations Center is unaware other road users are involved in the incident and does not contact first responders or does not provide them with correct information.

B.3 Relative Frequency scale

As little operational experience has been documented in sufficient depth to retrieve quantitative measures of likelihood or frequency data to characterize the scenarios, the proposed scale is based on the expected relative frequency of the end state with respect to the initiating event corresponding to each Event Sequence Diagram and the events leading to it.

The relative frequency is estimated through:

$$f_{rel} = f_{es} \times f_{ie} \, ,$$

where f_{es} represents the relative frequency of an end-state with respect to the other possible end states stemming from the same initiating event, and f_{ie} represents the relative frequency of the initiating event (IE) with respect to a period of ADS vehicle operation.

The relative frequency of an end state is estimated considering the probability of the event that may lead to them. For instance, a successful end state such as “trip successfully completed” is expected to be more frequent than the state concerning an incident and post-incident failures: the path from the IE to the successful end state involves the “success” path of the events, which is expected to have a higher probability than the “failure paths” (e.g., it is expected that the vehicle has a higher probability of functioning as expected than of presenting a critical failure while in operation).

The initiating event relative frequency is categorized as follows:

- High (3): End states derived from initiating events with expected high relative frequency considering the entire fleet operation. These correspond to a) ADS vehicle is on-route to destination without passengers, b) ADS Vehicle is on-route to destination with passengers, c) ADS vehicle is scheduled for passenger pick-up, and d) ADS vehicle is scheduled for passenger drop-off.
- Medium (2): End states derived from initiating events with expected medium relative frequency considering the entire fleet operation. These correspond to e) ADS vehicle is scheduled to arrive at the Maintenance Operations Center, f) ADS Vehicle is scheduled for pre-shift inspection, and g) ADS vehicle is scheduled for service maintenance.
- Low (1): End states derived from initiating events with expected low relative frequency considering the entire fleet operation. These correspond to h) post-incident procedures are initiated.

The end-state relative frequency is categorized as follows:

- High (3): End states which are expected to regularly occur during the operational phase. This refers to successful end states indicating a trip has been completed or that inspection and maintenance activities have successfully reflected the state of the vehicle.
- Medium (2): End states which may occur during the operational phase. This refers to end states resulting from low-severity vehicle failures and from less than adequate inspection/maintenance procedures.
- Low (1): End states which are not expected to occur during the operational phase. This refers to end states resulting from critical vehicle failures and from failures to follow operational procedures during vehicle post-incident management.

This scale is based on modeling assumptions which may overestimate the risk of low-likelihood events. In particular, the likelihood of the end states resulting from the post-incident procedures operational phase is potentially several orders of magnitude smaller than end states resulting from the on-route operational phases, which is not captured in the proposed scale ranging between 1-3.

The resulting relative frequency f_{rel} is then categorized into four levels (Table B.3). The description of each relative frequency category is presented in Table B.4. In the event there is data available to quantify both the initiating event frequency and the probability of failure of the Event Sequence Diagram events, a new relative frequency scale would need to be developed to adequately reflect each scenarios’ risk.

Table B. 3: Relative frequency matrix

Initiating Event/End-State Relative Frequency	High	Medium	Low
High	1	1	3
Medium	1	2	3
Low	3	3	4

Table B. 4: Description of qualitative relative frequency scale.

Consequence	Level	Examples
High	1	The vehicle safely completes a passenger trip to the intended destination with no incidents. This corresponds to a high relative frequency of the initiating event and end state.
Medium	2	The maintenance crew performs less than adequate inspection or maintenance activities. This corresponds to a medium relative frequency of the initiating event and end state.
Low	3	Incidents with or without passengers onboard and/or other road users are involved. Post-incident procedures are followed. This corresponds to a high relative frequency of the initiating event and a low relative frequency of the end state.
		The vehicle is unreachable or unresponsive to remote commands and fails to autonomously implement DDT-fallback actions when required. This corresponds to a medium relative frequency of the initiating event and a low relative frequency of the end state.
Very Low	4	Incidents with or without passengers onboard and/or other road users are involved. Post-incident procedures are not followed. This corresponds to a low relative frequency of the initiating event and end state.
		Fleet Operations Center operators are unaware other road users are involved in the incident and do not contact first responders or do not provide them with correct information. This corresponds to a low relative frequency of the initiating event and end state.

Appendix C: Contributing Failure Modes

C.1. Fleet Operations Center Remote Operators

Table C. 1: Contributing failure modes to Fleet Operations Center-related risk contributors.

Risk Contributor	Failure Mode *Fails to/Fails to provide:*
Fleet Operations Center Safety Operator	Acknowledge that ADS vehicle entered Minimal Risk Condition or requested post-incident procedures
	Assess if the ADS vehicle requires maintenance
	Attempt to communicate with missing vehicle
	Collect and transmit information on incident to Maintenance Operations Center
	Comply to "not cleared" status and incorrectly transmits a dispatch command
	Confirm maintenance scheduling request
	Confirm operational procedure update
	Deliver incident report
	Deliver requested information
	Detect vehicle is stranded
	Determine if a collision has occurred
	Determine if a passenger has requested an emergency stop
	Determine if a recovery team should be dispatched
	Determine if a secondary vehicle should be dispatched
	Determine if DDT can continue
	Determine if external party asked for a stop
	Determine if first responders should be alerted
	Determine if more information is needed

Risk Contributor	Failure Mode *Fails to/Fails to provide:*
	Determine if MR-DDT is achievable
	Determine if Stopped Stable Condition is achievable
	Determine if passengers or other road users were involved
	Determine if there is an ADS vehicle failure
	Determine if vehicle can perform MR-DDT
	Determine if vehicle should go into Minimal Risk Condition
	Dispatch a secondary vehicle to complete trip
	Dispatch the ADS vehicle for operation
	Dispatch vehicle to Maintenance Operations Center in MR-DDT
	Evaluate ADS vehicle safety
	Evaluate condition of missing vehicle
	Evaluate if the ODD is breached
	Evaluate information from ADS
	Evaluate state of passengers and vehicle
	Evaluate state of vehicle
	Evaluate the need and initiate post-incident procedures
	Follow DDT-fallback procedure
	Follow DDT-fallback requirements
	Follow emergency procedures
	Implement vehicle recovery procedure
	Inform DDT-fallback is required
	Inform vehicle status

Risk Contributor	Failure Mode *Fails to/Fails to provide:*
	Initiate post-incident procedures
	Monitor ADS vehicle operations
	Provide requested information
	Receive request for information
	Receive that ADS vehicle is missing
	Remote vehicle dispatch command
	Request maintenance activities schedule verification
	Request vehicle recovery
	Respond to ADS request
	Schedule vehicle for maintenance
	Transmit ADS fallback plan
	Transmit dispatch commands
Fleet Operations Center Service Operator	Alert DDT-fallback is required
	Alert first responders
	Communicate with passengers
	Inform passenger status
	Passenger emergency stop request
	Request secondary passenger vehicle
	Respond to passenger contact request
	Transmit Fleet Operations Center service operator contact request to passengers
	Receive requests from passengers
	Communicate with vehicle

Risk Contributor	Failure Mode *Fails to/Fails to provide:*
Fleet Operations Center Communication	Connect Fleet Operations Center safety operator to vehicle (DDT-fallback plans and waypoints)
	Receive from the Maintenance Operations Center if the vehicle is cleared
	Receive outcome of DDT-fallback implementation
	Receive request from ADS
	Transmit prescribed information to Maintenance Operations Center
	Transmit request to ADS for specific information

C.2. ADS-Equipped Vehicle

Table C. 2: Contributing failure modes to ADS vehicle-related risk contributors.

Risk Contributor	Failure Mode *Fails to/Fails to provide:*
ADS communication	Alert DDT-fallback is required
	Alert Fleet Operations Center
	Connect Fleet Operations Center Service Operator to passenger
	Establish and maintain communication with Fleet Operations Center
	Make general request
	Receive DDT-fallback strategy from Fleet Operations Center
	Receive remote commands
	Request plan for DDT-fallback strategy from Fleet Operations Center
	Request to adapt local path plan to waypoints provided by Fleet Operations Center
	Respond to request for information
	Transmit communication from Fleet Operations Center Service Operator to vehicle
	Transmit communication from passenger to vehicle
	Transmit communication from vehicle to Fleet Operations Center Control Center

Risk Contributor	Failure Mode *Fails to/Fails to provide:*
	Transmit communication from vehicle to Fleet Operations Center Service Operator
	Transmit information due to external connectivity failure
	Transmit information due to vehicle communication channel failure
	Transmit passenger contact request to Fleet Operations Center
	Transmit to Fleet Operations Center prescribed information
ADS hardware	Collect correct perception and localization data
ADS software	Adapt local path plan to DDT constraints (local traffic laws, ODD specifications)
	Adapt local path plan to provided waypoints
	Adapt local path to DDT plan
	Adequate DDT plan (OEDR)
	Alert battery charging is required
	Apply tactical maneuver
	Command DDT-fallback (emergency stop request)
	Detect a system failure (diagnostic module failure)
	Detected context (perception data) for DDT planning
	Determine if a collision has occurred
	Determine if a passenger has requested an emergency stop
	Determine if DDT can continue
	Determine if external party requested a stop
	Determine if MR-DDT is achievable
	Determine local road rules
	Determine optimal trajectory
	Determine if Stopped Stable Condition is achievable
	Determine if there is an ADS vehicle failure
	Determine if vehicle should go into Minimal Risk Condition

Risk Contributor	Failure Mode *Fails to/Fails to provide:*
	Early warning of safety-critical failures
	Enforce up to date/correct ODD limits (not available)
	Evaluate if the ODD is breached
	Evaluate outcome of implementation of DDT-fallback plan
	Execute optimal planned trajectory
	Implement correct DDT-fallback strategies
	Informative vehicle status
	Process and combine data
	Processed sensor data (perception) for Fleet Operations Center operator supervision.
	Receive internal dispatch command
	Receive remote dispatch command
	Recorded diagnostic logs for Fleet Operations Center operator supervision.
	Request kinematic action
	Request to adapt global path plan to waypoints provided by Fleet Operations Center
	Request vehicle commands (hazard lights, turn signals, etc.)
	Transmit outcome of self-diagnosis tests
	Use up to date/correct HD maps (not available)
ADS vehicle	Achieve Minimal Risk Condition
	Achieve Stopped Stable Condition
	Drive to Maintenance Operations Center in MR-DDT
	Correct vehicle control command
	Implement kinematic action
	Implement remote commands
	Implement signal action
	Perform DDT vehicle motion and maneuver execution to return to ODD

Appendix D: Risk Mitigation Activity Assessment

A qualitative scale is proposed to categorize the identified risk mitigation activities. Each activity is assigned a business impact category based on the potential safety impact, the estimated resources (cost, time) required and how frequently the fleet operator implements these. The structure of each of these scales is described in the following sections.

D.1 Safety Impact

The safety impact scale is derived from the qualitative risk scale discussed in Section 3. The safety impact of each activity is represented by a relative risk level, calculated as a combination of the risk level of the hazards prevented or mitigated by these activities and the relative importance of the activity for each target agent. This is represented by the following expression:

$$f_{RR} = R_{ave} \times I_{rel},$$

where R_{ave} is the average maximum risk of the hazard scenarios prevented or mitigated by these activities and I_{rel} is a value between [0,1] representing the ratio of the number of hazard scenarios impacted by each activity normalized by the total number of scenarios the target agent participates in. This allows the comparison of each activity independently of the hazard scenarios identified. Table D.1 presents the safety impact levels and corresponding average risk threshold. Table D.2 provides an example of the use of the safety impact scale with some identified risk mitigation activities.

Table D. 1: Safety impact level descriptions.

Safety Impact Level	Safety Impact Value	Average Risk Level
Very Low	5	Level <1
Low	4	Level 1<2
Moderate	3	Level 2<3
High	2	Level 3<4
Very high	1	> Level 4

Table D. 2: Example of safety impact scale.

Target Agent	Activity Type	Activity Purpose	# Hazards Involved	%Relative Importance	Average Risk Level	Relative Risk Level	Safety Impact
Fleet Operations Center Safety Operator	Procedures	Record operation logs to support accident investigation	15	0.50	4.33	2.17	Moderate
ADS Vehicle	Tools	Communication devices between agents (Fleet Operations Center, Maintenance Operations Center)	29	0.94	4.56	4.26	Very high
Fleet Operations Center Service Operator	Tools	In-vehicle passenger communication devices	11	1.00	4.33	4.33	Very high

D.2 Resources: Cost, Time & Frequency

Three category-based scales are developed to assess the resources required to implement the identified risk mitigation activities. Table D.3 and Table D.4 provide the qualitative measure of the cost and time required to implement the activities, respectively. Table D.5 provides a qualitative measure of how frequently the activities need to be implemented.

Table D. 3: Category-based risk mitigation activity assessment scale: implementation cost.

Cost Level	Level Description	Activity Type	Activity Example
High (3)	Activities of high complexity or requiring highly specialized personnel to develop or	Work conditions	Provide and maintain functioning Human-System Interface.
		Tools	Provide adequate Human-System Interface design to support agent tasks.
		Training	Follow incident management procedures and emergency response.

Cost Level	Level Description	Activity Type	Activity Example
	maintain elements in the system.	Procedures	Interact with first responders/law enforcement.
Moderate (2)	Activities that require the participation of multiple parties (i.e., fleet operator, ADS developer, first responders, law enforcement) to be developed and implemented.	Work conditions	Determine adequate length of shifts, provide adequate working conditions.
		Tools	Provide vehicle operation intervention mechanisms, passenger interaction cues (audio, video), low-complexity inspection and maintenance tools.
		Training	Coordinate team responses with other agents, select and transmit adequate DDT-fallback strategies, recognize DDT-fallback goals, and evaluate outcomes.
		Procedures	Establish responsibilities during post-incident procedures, implement specified inspection and maintenance contents and performance metrics, enforce ODD, connectivity and local restrictions, coordinate external maintenance activities with ADS developer.
Low (1)	Activities that can be developed internally by the fleet operator or can be explicitly implemented into the workflow.	Work conditions	Provide emergency procedure handbooks/guidelines.
		Tools	Provide in-vehicle passenger and between agents (Fleet Operations Center, Maintenance Operations Center) communication devices.
		Procedures	Provide shift take-over procedures, coordinate internal maintenance activities, record operation logs to support maintenance activities and accident investigation and operational procedure updates.
		Training	Enforce vehicle inspection and maintenance safety checklist, maintain operational procedures updated.

Table D. 4: Category-based risk mitigation activity assessment scale: implementation time.

Time Level	Level Description	Activity Type	Activity Example
High (3)	Activities that require extensive time to be designed and validated by specialized personnel.	Tools	Provide adequate Human-System Interface design to support agent tasks.
		Procedures	Establish responsibilities during post-incident procedures.
		Training	Follow incident management procedures and emergency response, recognize ODD conditions and system failures, select, and transmit adequate DDT-fallback strategies.
Moderate (2)	Activities that may require modifications or multiple iterations based on the fleet operator's experience. This includes the coordination of multiple teams to perform their tasks.	Procedures	Provide shift take-over procedures, coordinate internal maintenance activities, manage requests from other agents, interact with passengers and third parties.
		Work conditions	Provide and maintain functioning Human-System Interface, provide emergency procedure handbooks/guidelines.
		Training	Enforce vehicle inspection and maintenance safety checklist, recognize DDT-fallback goals, and evaluate outcomes, coordinate team responses with other agents, recognize Human-System Interface and connectivity failures.
		Tools	Provide vehicle operation intervention mechanisms and vehicle performance tests (at hardware, software, vehicle level).
Low (1)	Activities that may receive key input from external entities or directly obtained from external parties. The fleet operator implements these.	Procedures	Record operation logs to support maintenance activities and accident investigation and operational procedure updates, implement specified inspection and maintenance contents and performance metrics, establish information sharing procedures between fleet operator's agents.
		Tools	Provide in-vehicle passenger and between agents (Fleet Operations Center, Maintenance Operations Center) communication devices, provide low-complexity inspection and maintenance tools.
		Training	Maintain operational procedures updated.

Time Level	Level Description	Activity Type	Activity Example
		Work conditions	Determine adequate length of shifts, provide adequate working conditions.

Table D. 5: Category-based risk mitigation activity assessment scale: implementation frequency.

Frequency Level	Level Description	Activity Type	Activity Example
Constant (3)	Activities that are required to be constantly updated, available, or accessible to the fleet operator's agents.	Work conditions	Provide emergency procedure handbooks/guidelines and maintain functioning Human-System Interface.
		Tools	Provide in-vehicle passenger and between agents (Fleet Operations Center, Maintenance Operations Center) communication devices.
Periodic (2)	Activities that are expected to be revised on a periodic basis, based upon the input of the ADS developer, other third parties, and internal coordination experience.	Training	All training procedures are expected to be implemented periodically as defined by the fleet operator and ADS developer.
		Procedures	Interact with first responders/law enforcement, establish responsibilities during post-incident procedures, implement specified inspection and maintenance contents and performance metrics, enforce operating parameters, connectivity, and local restrictions.
		Tools	Provide vehicle operation intervention mechanisms and vehicle performance tests (at hardware, software, vehicle level).
Once (1)	Activities that are expected to not require modifications after implementation.	Procedures	Record operation logs to support maintenance activities and accident investigation and operational procedure updates, provide shift take-over procedures, establish information sharing procedures between fleet operator's agents, coordinate external maintenance activities with ADS developer.
		Work conditions	Determine adequate length of shifts, provide adequate working conditions.

D.3. List of Risk Mitigation Activities

The following tables provide the complete list of risk mitigation activities organized by the type of activity. Each activity is assessed through the safety priority and business impact priority scales discussed above.

Table D. 6: List of risk mitigation activities by type: operational procedures.

Rank Scale	Safety Priority Rank	Business Priority Rank
Activity Type/Target Agent*	**Procedures/ADS Vehicle**	
Enforce vehicle connectivity requirements	Top	High
Interact with first responders/law enforcement	Top	Medium
Enforce data transmission and storage policies	Top	High
Enforce ODD and local road restrictions	Top	Medium
Ensure self-diagnostic capabilities are available (vehicle hardware, software)	Top	Medium
Follow specified DDT-fallback goals and strategies	Top	Medium
Ensure DDT-fallback commands are received and implemented as specified	Top	Medium
Select routes within established ODD	Medium	Medium
Ensure dispatch commands are received and implemented as specified	Medium	Medium
Interact with passengers (pickup, start/end trip, drop-off)	Low	Low
Activity Type/Target Agent*	**Procedures/Fleet Operations Center Safety Operator**	
Establish information sharing procedures between fleet operator's agents	Top	Very high
Record operation logs to support accident investigation	Very high	Very high
Record operation logs to support maintenance procedures	Very high	Very high
Record operational procedure updates	High	High

Rank Scale	Safety Priority Rank	Business Priority Rank
Provide shift take-over procedures	High	High
Enforce vehicle dispatching requirements	High	High
Enforce vehicle physical recovery requirements	High	High
Manage requests from other agents (Fleet Operations Center, Maintenance Operations Center)	Medium	Medium
Locate and manage vehicles exhibiting abnormal behavior	Medium	Medium
Establish remote operator intervention criteria	Medium	Medium
Determine DDT-fallback goals and strategies	Low	Low
Establish responsibilities during post-incident procedures	Low	Low
Activity Type/Target Agent*	**Procedures/Fleet Operations Center Service Operator**	
Manage requests from other agents (Fleet Operations Center, Maintenance Operations Center)	Top	High
Establish information sharing procedures between fleet operator's agents	Top	Very high
Establish passenger data privacy policies	Top	Very high
Record operation logs to support accident investigation	Very high	Very high
Request secondary vehicle dispatch for passengers	Very high	Very high
Provide shift take-over procedures	High	High
Request intervention from Safety Operator	Medium	Medium
Establish responsibilities during post-incident procedures	Low	Low

*This table reads as: the fleet operator should provide operational procedures for the (*target agent*) that include how to (*activity).*

Table D. 7: List of risk mitigation activities by type: software and hardware tools.

Rank Scale	Safety Priority Rank	Business Priority Rank
Activity Type/Target Agent*	**Software and hardware tools/ADS Vehicle**	
Provide navigation and HD map support	Top	High
Provide communication devices between agents (Fleet Operations Center, Maintenance Operations Center)	Top	Very high
Provide passenger interaction cues (audio, video)	Medium	Medium
Activity Type/Target Agent*	**Software and hardware tools/Fleet Operations Center Safety Operator**	
Provide adequate Fleet Operations Center, Maintenance Operations Center Human-System Interface design to support agent tasks	Top	Low
Provide communication devices between agents (Fleet Operations Center, Maintenance Operations Center)	Medium	Medium
Provide vehicle operation intervention mechanisms	Medium	Medium
Activity Type/Target Agent*	**Software and hardware tools/Fleet Operations Center Service Operator**	
Provide adequate Human-System Interface design to support agent tasks	Top	Low
Provide in-vehicle passenger communication devices	Top	Very high

*This table reads as: the fleet operator should (*activity)* for the (*target agent*) to have adequate software and hardware tools to perform their tasks.

Table D. 8: List of risk mitigation activities by type: operator and crew training.

Rank Scale	Safety Priority Rank	Business Priority Rank
Activity Type/Target Agent*	**Operator and crew training/Fleet Operations Center Safety Operator**	

Rank Scale	Safety Priority Rank	Business Priority Rank
Enforce management of change policies	Top	Very high
Use Human-System Interface to monitor and intervene the vehicle's operation	Top	Medium
Enforce vehicle clearance requirements	Medium	Medium
Recognize Human-System Interface and connectivity failures	Medium	Medium
Coordinate team responses with other agents (Fleet Operations Center, Maintenance Operations Center)	Medium	Medium
Recognize DDT-fallback goals and evaluate outcomes	Medium	Medium
Recognize Human-System Interface information and alarms	Medium	Medium
Recognize operational conditions and system failures	Low	Low
Transmit adequate corrective actions	Low	Low
Select adequate corrective strategies	Low	Low
Follow incident management procedures and emergency response	Low	Low
Activity Type/Target Agent*	**Operator and crew training/Fleet Operations Center Service Operator**	
Enforce management of change policies	Top	Very high
Coordinate team responses with other agents (Fleet Operations Center, Maintenance Operations Center)	Medium	Medium
Recognize Human-System Interface and connectivity failures	Medium	Medium
Manage passenger communication (requests, interactions)	Medium	Medium
Interact with first responders/law enforcement during incident management	Low	Low

Rank Scale	Safety Priority Rank	Business Priority Rank
Follow incident management procedures and emergency response	Low	Low

*This table reads as: the fleet operator should provide a training program to the (*target agent*) that includes how to (*activity).*

Table D. 9: List of risk mitigation activities by type: work conditions.

Rank Scale	Safety Priority Rank	Business Priority Rank
Activity Type/Target Agent*	Work Conditions/Fleet Operations Center Safety Operator – Fleet Operations Center Service Operator	
Provide adequate working conditions	Top	Very high
Provide and maintain functioning Human-System Interface	Top	Low
Determine adequate length of shifts	Top	Very high
Provide emergency procedure handbooks/guidelines	Medium	Medium

*This table reads as: the fleet operator should provide adequate work conditions to the (*target agent*), including (*activity).*