Safety Hazard Identification for Autonomous Driving Systems Fleet Operations in Mobility as a Service

Camila Correa-Jullian[a,b], John McCullough[a,b], Marilia Ramos[b], Jiaqi Ma[b,c], Enrique Lopez Droguett[b,c], Ali Mosleh[b]

[a] Dept. of Mechanical and Aerospace Engineering, University of California Los Angeles (UCLA), USA. E-mail: *ccorreaj@ucla.edu*, *jmccull@ucla.edu*

[b] B. John Garrick Institute for the Risk Sciences, University of California Los Angeles (UCLA), USA. E-mail: *marilia.ramos@ucla.edu, mosleh@ucla.edu*

[c] Dept. of Civil and Environmental Engineering, Univ. of California Los Angeles (UCLA), USA. E-mail: *jiaqima@ucla.edu*, *eald@ucla.edu*

Abstract: The safe and reliable operation of Automated Driving Systems (ADS) in the context of Mobility as a Service (MaaS) depends on a multitude of factors external to the vehicle's functionality and performance. In particular, it is expected that Level 4 ADS operations are supported by the actions of remote operators, specifically during the initial stages of deployment. In the future, fleet operators are expected to work with one or multiple ADS developers as technology providers to transform their fleets. Therefore, fleet management of ADS vehicles involved in MaaS will play an important role in ensuring traffic safety. In this work, we consider the role of fleet operators as separate entities than ADS developers. Fleet operator functions comprise a fleet operations center (FOC), where the ADS vehicle is monitored and supervised, and a maintenance operations center (MOC), focused on vehicle inspection, maintenance, and storage. Based on a L4 ADS MaaS system breakdown and identification of critical operational stages, we identify operational hazards through Event Sequence Diagram (ESD) and Fault Tree Analysis (FTA). The analysis highlights the role of the FOC and MOC in ensuring the correct operation of the vehicle and acting as a safety barrier for preventing or mitigating incidents.

Keywords: autonomous driving systems, remote operation, safety assessment, mobility as a service, hazard identification

1. INTRODUCTION

The concept of Mobility as a Service (MaaS) is expected to become key to the transportation scenario in the future decades. MaaS is frequently referred to as a new on-demand mobility paradigm where a common travel management platform integrates planning, booking, and paying activities for transport [1], [2]. This includes traditional transport means (bus, metro, taxi, etc.), as well as schemes based on ridesharing (car-sharing, bike-sharing, etc.). Autonomous Driving Systems (ADS) are expected to have a significant role in the MaaS context. However, the efficient and safe deployment of ADS as MaaS depends on a multitude of factors, including appropriate road infrastructure, wireless connectivity, users profile, and interaction with other road agents. Hence, the operation of these systems can be assessed through various criteria related to traffic safety, accessibility, and energy efficiency, among others.

Currently, vehicle automation capabilities are categorized by SAE under six levels, from Level 0 to Level 5, depending on the combination of driving support and automated driving features [3]. While many commercially available vehicles present various driving assisting tools, such as breaking assistance and proximity alarms, they still require the driver to perform the Dynamic Driving Tasks (DDT). In contrast, Level 5 (L5) ADS vehicles are planned as fully autonomous vehicles whose operation does not require human intervention nor is restricted to specific areas or conditions. At the current stage of development, shorter-time goals include the deployment of Level 4 (L4) vehicles at a commercial scale for either personal use or integrated through MaaS. Various companies are developing, testing, or operating these vehicles in the U.S., such as Waymo, Lyft, and Motional. By definition, L4 ADS are capable of performing all driving functions (DDT) under certain conditions and locations specified in their Operational Design Domain (ODD) [4], [5]. The ODDs restrict the vehicle's operation to known scenarios defined by the ADS technology developer, under which it can fully and independently operate without external commands nor the intervention of a safety driver. The ODD

includes the physical infrastructure the vehicle is expected to encounter, the interaction with multiple objects and other road users, and the operational constraints under which the vehicle was tested. The latter includes the geographic zones, connectivity, and environmental conditions. The ADS vehicle is generally expected to perform functions based on a multi-sensorial perception module, built-in traffic laws and HD maps, as well as object and event detection and response (OEDR) software. Thus, the ADS is expected to execute all DDT within the ODD.

The main safety-related tasks L4 ADS vehicles must perform are: (1) enforce the ODD through self-diagnostic systems, (2) perform safety-adequate DDTs relying on real-time conditions, and (3) achieve a Minimal Risk Condition (MRC) when required. The vehicle may breach the ODD during operation by wrongly executing OEDR, experiencing a safety-critical failure, or due to worsening environmental conditions. If the vehicle is not able to perform regular DDT under these conditions or is involved in an accident, the ADS is expected to implement a DDT fallback strategy to achieve MRC. This context-specific, fail-operational condition should be adopted by the vehicle to ensure safety of the passengers and surrounding road users. However, the implications of ODD requirements, fallback strategies, and MRC mechanisms on MaaS operational safety are still unclear[6]. Most research efforts regarding ADS vehicles have focused on demonstrating functional safety, system reliability, or the potential to increase traffic safety [7], [8]. In this context, scenario-based simulation and drive testing have become essential tools to demonstrate safety amid the evolving regulatory environment [9]. To date, there is no clear approach to define the operational safety responsibilities of the key agents involved in L4 ADS deployed for MaaS, such as the fleet operators, the ADS developers, vehicle manufacturers, and regulatory entities. Particularly, if the fleet operators (i.e., the mobility service provider) is an independent entity that purchases the vehicles from the ADS developer. Without onboard safety drivers, remote fleet supervisors may need to play an active role in ensuring passenger and vehicle safety, including monitoring tasks and, when necessary, intervening through indirect control (e.g., waypoints or command for achieving MRC). One of the challenges to conducting safety analysis is the limited operational data available, proprietary data sharing restrictions, and little knowledge of L4 ADS planned operational conditions. Therefore, the first step in understanding the fleet operator's role in L4 ADS MaaS safety is to model the interactions between the ADS vehicle, the passenger, and the remote fleet operators, and determine the extent of human participation in ensuring operational safety.

This work explores ADS MaaS operational scenarios through event sequence diagrams (ESD) to support hazard identification and modeling. Given the different operational designs proposed for ADS MaaS, a representative fleet – "reference fleet" - is used for building the scenarios. The remainder of this paper is organized as follows. Section 2 discusses the reference fleet characteristics, and the system breakdown and the operation phases identified in the MaaS operation. Section 3 presents the ESDs modeling and discussions regarding ADS operations on-route without passengers and an example of supporting Fault Trees. Finally, conclusions and future work directions are presented in Section 4.

2. ADS SYSTEM DEFINITION

2.1. Fleet Definition

The generic fleet consists of light-duty passenger vehicles with L4 ADS capabilities operating without the presence of a safety driver. The role of the ADS fleet is to perform MaaS functionalities for passengers in urban environments (i.e., ride-hailing through a mobile application). This fleet is managed by a *fleet operator* who has procured the vehicles from an *ADS vehicle manufacturer*. The main role of the fleet operator is to ensure the correct and safe operation of the fleet based on the technical requirements of the ADS manufacturer and comply with additional MaaS operational requirements. The fleet operator may establish or operate within a more restrictive ODD than the ADS developers determine to comply with connectivity and passenger communication needs [5], [10].

2.2. ADS Functional System Breakdown

The fleet operator's functions are divided into two separate entities. The fleet operations center (FOC) monitors and supervises the ADS vehicle's operation, while the maintenance operations center (MOC) is where the vehicles are inspected, maintained, and stored. In this work, the fleet operator is responsible

for crewing and training both centers, in accordance with the specifications determined by the ADS manufacturer. However, these roles may differ depending on the business relationship between the ADS developer and the fleer operator. The ADS MaaS operations can thus be broken down into three subsystems: the ADS vehicle, the FOC, and the MOC. The tasks of each subsystem are described below.

ADS vehicle: Each ADS vehicle is expected to perform autonomous driving tasks coherent with the definition of L4 throughout its operation. Additionally, MaaS-specific functionalities include key aspects of passenger-vehicle interaction, such as picking-up and dropping-off passengers assigned to it, enabling the communication between the passenger and the FOC operators, and receiving commands from the FOC. Note that the direct vehicle control is handled exclusively by the ADS software, which requires real-time monitoring data of the vehicle's surroundings. A critical functionality is the inclusion of an emergency stop request, in which the passenger can trigger the vehicle to enter a stopped stable condition (SSC). Depending on the context, whether the ODD is breached, a safety-critical failure, an incident, or an emergency stop request has occurred, the vehicle is expected to perform the DDT fallback actions necessary to return to the ODD, achieve an SSC or an MRC. Furthermore, in case a vehicle with no passengers onboard presents a non-safety-critical failure, the ADS can fallback to a Minimal Risk DDT (MR-DDT) condition. Under MR-DDT, the vehicle should drive with limited DDT (e.g., lower speed, void highways, etc.) to the MOC and be scheduled for maintenance and repairs.

Fleet operations center (FOC): The FOC is a physical space crewed by trained operators supervising various aspects of the MaaS operation. Depending on the fleet operator's organizational structure, these functions may be further divided into a control center (focused on functional safety aspects) and the service operator (focused on mobility service aspects). The main role of the FOC operators is to support the operations of the ADS vehicle. This includes monitoring the vehicles' overall operation, addressing the passengers' requests, sending commands to the vehicle, and managing the communication with the passenger. The commands sent by the FOC operators may dispatch the vehicle to different locations or directly assign waypoints to the vehicle's trajectory if the ADS cannot perform DDT fallback strategies when required autonomously. In the event of an incident, the FOC operators are responsible for initiating post-incident procedures. Depending on the event's severity, this may include contacting first responders and law enforcement, dispatching vehicle recovery teams or a secondary vehicle for the passenger, and recording and reporting the incident for investigation, as expected to be required by local regulations.

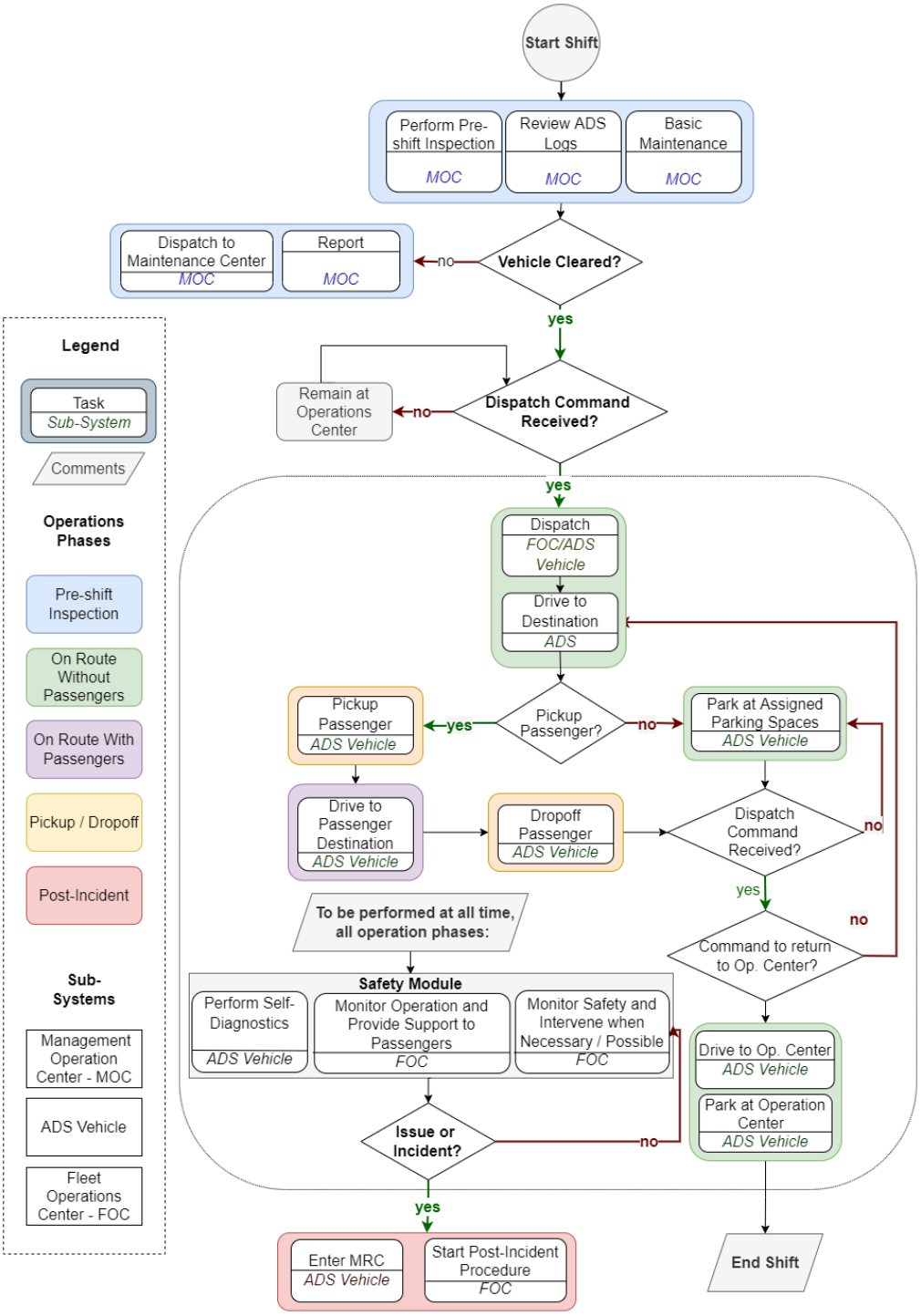
Maintenance operations center (MOC): The MOC refers to physical locations managed by the fleet operator where a trained crew performs multiple activities to ensure the correct and safe operation of the ADS vehicles. This entity may be further divided into external operations and maintenance centers. It is expected that the ADS vehicle manufacturer establishes minimum functional requirements that the fleet operator must enforce to minimize risks. The fleet operator's responsibility may be limited to performing low-complexity system inspections, maintenance, and general upkeep. In contrast, the ADS vehicle manufacturer should perform system updates, sensor calibration, and more complex maintenance activities. Hence, the fleet operator should ensure that remote operators and maintenance crews undergo appropriate training and should implement system upgrades or correcting system-level unexpected ADS behaviors. Further, the MOC is also expected to satisfy local regulations and reporting duties regarding post-incident procedures and investigations.

2.3. ADS Operation Phases

For the safety risk analysis of the reference fleet, a generic operational profile has been developed based on expected interactions between the sub-systems, i.e., the ADS vehicle, the FOC and MOC, organized in the operation phases presented in Figure 1 and described below. An *operational shift* denotes the continuous operation of an ADS vehicle within a delimited time period.

Pre-shift inspection and maintenance: An ADS vehicle may only be dispatched to perform passenger trips once it has passed a pre-inspection process and has been cleared for operation. The content and frequency of this procedure are expected to be determined by the ADS vehicle manufacturer and carried out by the fleet operator's MOC maintenance crew. This process must generally include performing a

Figure 1: Operation phases of ADS MaaS



checklist of all safety-critical subsystems and functions of the ADS vehicle, including reviewing the ADS onboard diagnostic logs and the inspection of the vehicle's general state (e.g., verifying tire pressure, windshield integrity, battery levels). If needed, low-complexity maintenance actions can be performed to ensure the vehicle's correct operation (e.g., adjusting tire pressure, charging the battery). It is expected that the ADS vehicle manufacturer, in coordination with the fleet operator, defines which low-complexity maintenance actions can be performed at the MOC and which actions require external maintenance requests. If the vehicle's condition is adequate, the MOC can clear the vehicle for operation. If any abnormal vehicle behavior is identified during the inspection process, the MOC is expected to report to the ADS vehicle manufacturer, submit a request for external maintenance, and may trigger a fleet-wide revision, system update or calibration, if required. Once the vehicle is cleared

for operation, it can be dispatched by either an FOC operator or automatically scheduled for a passenger pick-up by the ADS.

On-route to destination without passengers: When the ADS receives a dispatch command, the vehicle must perform all the required DDTs to arrive at the target destination. This phase includes the vehicle receiving the dispatch command, driving to the indicated location, attaining an SSC to perform passenger pickup interactions, and parking at designated areas between assigned trips. A vehicle currently operating might be dispatched to the MOC for low-complexity maintenance or battery charging after a passenger trip has ended. This setting is general, independent of the number and/or location of MOCs employed by the fleet operator in the area of operation (including maintenance centers and charging stations). It should be noted that the FOC cannot remotely drive the vehicle but can provide rerouting options via specifying waypoints or setting a target area of operation, or through specific dispatch commands (i.e., travel to a charging station, return to the MOC, etc.). If the ADS diagnostic module detects a system failure that does not compromise the vehicle's safety-critical systems, the vehicle may automatically perform MR-DDT fallback strategies and be rerouted to the MOC. Otherwise, if the vehicle presents a safety-critical failure, the ADS is expected to perform the fallback DDT and achieve an MRC (either automatically or assisted by the FOC operator). The vehicle must be recovered physically by a team dispatched from the FOC if it has been stranded at MRC for exceeding its ODD, depleting the battery, or any safety-critical systems have been compromised.

Passenger pickup & drop-off: This phase describes the interaction between the ADS vehicle and the passenger when boarding and leaving the vehicle. When the ADS vehicle is approaching the designated pickup location, it is expected to perform all the necessary DDT to achieve an SSC. Once the SSC is achieved, the passengers can safely board the vehicle. It is assumed that passenger assignment and authentication are mature in the mobility industry and function as planned. In addition, it is expected that the passenger must follow the required safety instructions (close doors, put on seat belt, etc.) and confirm the trip details (i.e., dropoff location) before the ADS can initiate the trip. Similarly, when dropping off passengers, the ADS is expected to achieve an SSC in the close vicinity of the dropoff location requested by the passenger considering the active ODD restrictions. The passenger must then exit the vehicle and confirm the trip has ended, enabling the ADS to accept any incoming trip assignments. Note that the only communication channels available when the passenger is not in the vehicle are through the ride-hailing mobile application. While in the vehicle, the passenger can access audio cues, visual displays, and direct communication with an FOC operator.

On-route to destination with passengers: This phase is defined between the passenger pickup and dropoff, as described in the previous stage. Additional to the functions described for the on-route without passenger, this phase must also consider the interactions between the passenger, the ADS vehicle, and the remote FOC operator. As previously mentioned, during the trip, the passenger has access to visual displays communicating the state of the trip, estimated time to destination, and other optional information regarding the vehicle. Further, passengers may request to communicate with the FOC operator to resolve any concerns they may have. The most critical interaction arises from the ability of the passengers to request an emergency stop. This request needs to be detected by the ADS, triggering fallback DDTs to achieve an SSC, and initiating communication with the FOC operator. Multiple actions of the FOC operator may be possible at this stage, including allowing the vehicle to continue the trip after passenger confirmation, triggering the vehicle into achieving MRC, contacting first responders, and initiating post-incident procedures.

Post-incident management: The post-incident procedures must be initiated by the FOC in the event the vehicle has been prompted to achieve an MRC. This may be caused by multiple reasons, including system failures, ODD breaches, external incidents, worsening environmental conditions, etc. At a minimum, it is expected that these procedures include (1) automatically disabling the ADS, turning on hazard lights (if not already on), unlocking doors, and disconnecting the main battery; (2) continuous passenger-FOC operator communication, if possible; (3) the FOC operator must contact first responders and/or law enforcement to aid the passengers or other road users affected; (4) the FOC operator is expected to request and dispatch a vehicle recovery team or a second ADS vehicle to either transport

the vehicle to the MOC, and/or provide alternative transportation for the passengers if they are able/wish to continue the trip. Local legislation or regulatory requirements are expected to exist within the post-incident management procedures in the case of severe incidents (i.e., those involving passengers or other road users). After an incident has occurred and the immediate priorities have been addressed, it is expected that the vehicle will be inspected in-depth at the MOC to determine the potential causes of the incident. The vehicles' onboard data collection capabilities must suffice to recreate incident events for analysis and may trigger fleet-wide revisions by both the fleet operator and the ADS vehicle manufacturer.

3. EVENT SEQUENCE DIAGRAMS & FAULT TREES

A general risk assessment framework is presented in Figure 2. Hazard identification and modeling is a key step in developing qualitative and quantitative risk assessments. A series of traditional approaches have been consistently employed in research and industry, evolving from system decomposition methods to focusing on the interaction between critical subcomponents and activities. System reliability assessments have frequently relied on traditional tools such as fault tree analysis (FTA), event trees analysis (ETA), failure mode and effect analysis (FMEA), hazard and operability studies (HAZOP), and, more recently, Bayesian networks (BNs) to identify and model multiple system hazards [11]. Modern techniques such as concurrent task analysis (CoTA) and system-theoretic process analysis (STPA) aim to identify and model interactions between subsystems and emerging behaviors [12], [13]. ETA is an inductive hazard analysis method based on the functional decomposition of events. It provides a systematic method of recording the accident sequences between the initiating events and subsequent events that can result in hazards exposure. Events can be ordered by chronological or causal order, and the sequence is characterized by the probability of occurrence of each event. Event Sequence Diagrams (ESDs) can be defined as generalized event trees (ETs), allowing them to better represent dynamic systems [14]. ESDs depict a sequence of pivotal events stemming from a common initiating event and leading to different end-states. ESDs may be combined with FTA, BBN and CoTA to represent interactions between hardware and software failures [15], [16], as well as human errors [17]. The quantification of ETs and ESDs allows estimating each outcome's frequency based on the initiating event's frequency and the intermediary events' probabilities [18].

Figure 2: General Risk Assessment Outline.

The current work adopts ESDs and FTs as initial methods for mapping out the undesired events that may occur in each operation phase. This application aims to identify the sequences of events that highlight remote FOC operators' critical role as key safety barriers. Section 3.1 presents an example regarding the On-Route Without Passenger phase.

3.1. ESD: On-route without passenger

The model of the interactions between the ADS, the FOC, and other external factors during the operational phase on-route without passengers adopts the following assumptions. To simplify the analysis of these dynamic interactions, the ESD comprises the entirety of a trip, independently of whether multiple events may occur during the same trip. This ESD begins with the initiating event denominated "The vehicle is on-route to destination" and may diverge into the end states described in **Table 0**. The diagram presented in Figure 3 illustrates a simplified ESD. The key sub-events identified in this phase are described in **Table 2**. Each event is described in terms of the binary yes/no outcome, as well as which subsystem is mainly responsible for the outcome. These are:

- ADS: The ADS is the main responsible for subevents that depend on the vehicle's expected functionality or are triggered by a hardware, software, or procedure failure.

- MOC: The MOC is the main responsible for subevents referring to ADS vehicle failures which are expected to be prevented by the correct development of the pre-shift inspection processes.
- FOC: The FOC is the main responsible for subevents that depend on an expected interaction between the FOC remote operator and the passenger or the ADS vehicle itself.

In this simplified ESD, key actions of the subsystems regarding information gathering, situation assessment and decision-making, and action execution have been merged into a single event. The subdivision of these tasks follow an extension of the cognitive model IDA [19] (Information, Decision, and Action) to human and autonomous systems [12], [18]. This division of tasks is fundamental to identify different failure modes of the ADS and the human operators, as well as emergent failures and/or failures arising from unsafe interactions between these elements. For deeper analysis, the events "**ADS performs DDT-fallback correctly"** and **"FOC sends correct DDT fallback command** should be further developed, for instance, through FTs and BNs. To model the operation of the ADS vehicle, the following assumptions have been made:

(1) A successful trip may be interrupted by the vehicle breaching the ODD, presenting a failure, by wrongly executed DDTs, or an unavoidable external event. It should be noted that although these events can occur simultaneously, the presented ESD only considers that one of these events occurs per trip.
(2) The ADS is the first safety barrier when an event has interrupted a trip under nominal conditions. Based on real-time perception and localization data, the ADS is expected to detect that fallback DDTs are required. The ADS must then plan and execute the DDT fallback which, for this operational stage, may lead to returning to nominal DDT, entering MR-DDT, or achieving MRC. This depends on whether the ADS can assess that it can safely continue the trip based on the detected failures, ODD breaches, or other challenging scenarios. If the vehicle cannot continue the trip, it must perform DDT fallback actions leading to an MRC.
(3) The second safety barrier is the remote FOC operator. The need for the FOC operator to intervene may occur after the ADS has either not detected that DDT fallbacks were necessary or has wrongly executed the selected fallback strategy. In this case, if there is sufficient time for the operator to intervene, they are expected to plan and transmit the correct DDT fallback strategy. Implementing the selected fallback strategy depends on the ADS vehicle receiving and adopting the remote commands. In this case, the possible actions are triggering the vehicle to enter an MRC or dispatching it to the MOC in MR-DDT mode. In case the vehicle enters an MRC, the FOC operator is also responsible for initiating the post-incident procedures, depending on the severity of the incident.
(4) The severity of the end-state consequences will depend on whether the vehicle is at risk of collision with objects or other road users due to unattended ADS malfunctioning and the non-timely intervention of the remote FOC operator; has entered into MRC and post-incident procedures have been initiated; is left stranded in MRC; or has successfully completed the trip in MR-DDT back to the MOC.

Table 1: On-route without passengers ESD possible end states.

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 FOC operator.
Post-incident procedures are initiated	Medium	The FOC operator successfully initiated the post-incident procedures given that the vehicle has entered MRC. The specific response depends on the perceived severity of the incident and the local regulations in place.
Vehicle is stranded	Medium	The FOC operator has failed to initiate post-incident procedures to recover the vehicle once it has entered MRC.
Vehicle arrives at MOC for maintenance	Low	The vehicle successfully implemented MR-DDT fallback (automatically dispatched by the ADS or assisted by the FOC operator) given a non-critical system failure was detected.
Collision Risk	High	The vehicle is at risk of colliding with other road users or other objects given that the ADS and the FOC operator have failed to detect and implement MRC when required.

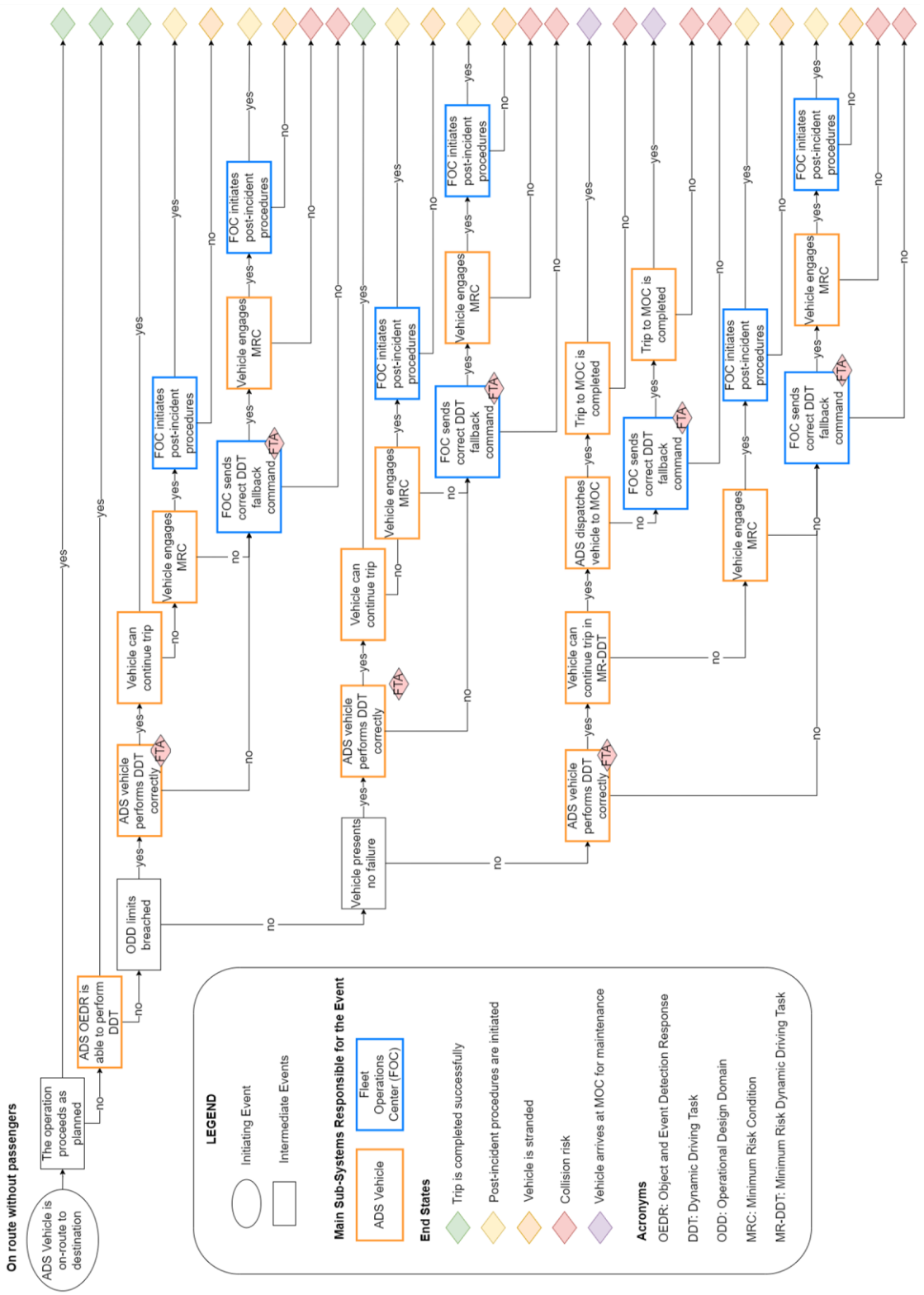
Two key subevents are identified as critical to the safe response of the ADS vehicle when faced with challenging situations. These refer to (1) **ADS performs DDT-fallback correctly** and (2) **FOC sends correct DDT fallback command.** These events are particularly relevant given the complex interactions between the subsystems involved that lead to successful or failed outcomes, considering that these can be further subdivided into identifying-planning-execution phases based on the IDA model.

Table 2: Event description for on-route without passengers ESD.

Event	Yes	No	Main Role
The operation proceeds as planned	The vehicle is able to perform DDT and complete the trip in a safe manner.	Nominal operation is interrupted due to the vehicle not responding as expected. Possible causes: wrong execution of OEDR, ODD limits are breached, vehicle failures.	ADS/ External
ADS OEDR is able to perform DDT	The vehicle encounters a challenging situation and the OEDR module is able to plan or execute an adequate response.	The vehicle encounters a challenging situation and the OEDR module does not plan or execute an adequate response.	ADS/MOC
ODD limits are breached	The incident causes the ADS to operate outside ODD (environmental conditions, traffic scenarios).	The incident does not cause the ADS to operate outside the ODD.	ADS
Vehicle presents no failure	The ADS functions are not compromised.	The ADS self-diagnostic module identifies a system failure.*	ADS/MOC
ADS performs DDT-fallback correctly	The ADS detects that a fallback strategy is required. The ADS is able to plan and execute DDT fallback actions.	The ADS does not detect that a fallback strategy are required. The ADS fails to plan or execute adequately the DDT fallback actions.	ADS/MOC
Vehicle can continue trip	The ADS is able to return to the ODD through the DDT-fallback actions implemented.	The ADS is not able to return to the ODD through the DDT-fallback actions implemented.	ADS
Vehicle engages MRC	The ADS achieves an MRC through the implementation of DDT fallback strategies.	The ADS does not achieve an MRC through the implementation of the DDT fallback strategies.	ADS
FOC initiates post-incident procedures	The FOC operator detects that post-incident procedures are required and initiates them.	The FOC operator does not detect that post-incident procedures are required. Vehicle is stranded.	FOC
FOC sends correct DDT fallback command	The FOC operator detects that the ADS requires DDT fallback strategies. The FOC operator plans and sends the DDT fallback strategy command to the ADS	The FOC operator does not detect that the ADS requires DDT fallback strategies. The FOC operator fails to adequately plan or send the DDT fallback strategy command to the ADS**	FOC
Vehicle can continue trip in MR-DDT	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
ADS dispatches vehicle to MOC	The ADS automatically reroutes the vehicle to the MOC under MR-DDT.	The ADS fails to reroute the vehicle under MR-DDT.	ADS
Trip to MOC is completed	The ADS is able to drive the vehicle to the MOC.	The ADS is not able to implement MR-DDT OEDR actions to drive to the MOC.	ADS

Note: *The effectivity of the self-diagnostic module is incorporated through FT; ** The reliability of the wireless communication channels is incorporated through FT.

Figure 3: ESD for on-route without passenger operational phase.



As mentioned, FTs and BNs are useful tools to model hardware, software, and human-related failures and errors. Figure 4 presents a simplified FT describing (2), 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 FOC operator and the ADS vehicle. On the one hand, this may occur when the self-diagnostic module fails to detect that the FOC-Vehicle communication channels have failed. The latter may be further due to vehicle hardware or software failures of the vehicle's communication channels, or limited connectivity in the area. On the other hand, the remote FOC operator may fail to act upon the information transmitted by the ADS vehicle if:

a) the FOC operator fails to plan the adequate DDT-fallback. This may occur if the operator fails to correctly monitor and assess the vehicle's state, failing to detect the need for the fallback, or by not following the established DDT-fallback procedure to plan and communicate an adequate fallback strategy.
b) the ADS vehicle fails to transmit the correct information. This may occur if the ADS data recording mechanisms are not informative (i.e., an undetected failure in the perception module) or if the ADS does not transmit information required for determining the vehicle's status. This is associated with shortcomings in the ADS software design and/or implementation and can be caused by the MOC maintenance crew failing to follow system updates and maintenance procedures.

Table 3 presents a summary of the undeveloped basic events, the type of failure these represent, and which subsystem is the main responsible for their occurrence. Note that the underlying cause of many hardware and/or software failures of the ADS vehicle may stem from less than adequate execution of pre-shift inspection or corrective maintenance procedures at the MOC. These procedures are of key importance, particularly when discussing 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). Therefore, the pre-shift inspection frequency should be determined either through statistical analysis or condition-based maintenance to ensure the timely detection of vehicle failures. It is expected that the ADS vehicle manufacturer and the fleet operator establish which components or subsystems require a more frequent inspection to avoid unexpected operational failures.

Figure 4: Example of high-level FT developed for on-route without passenger ESD.

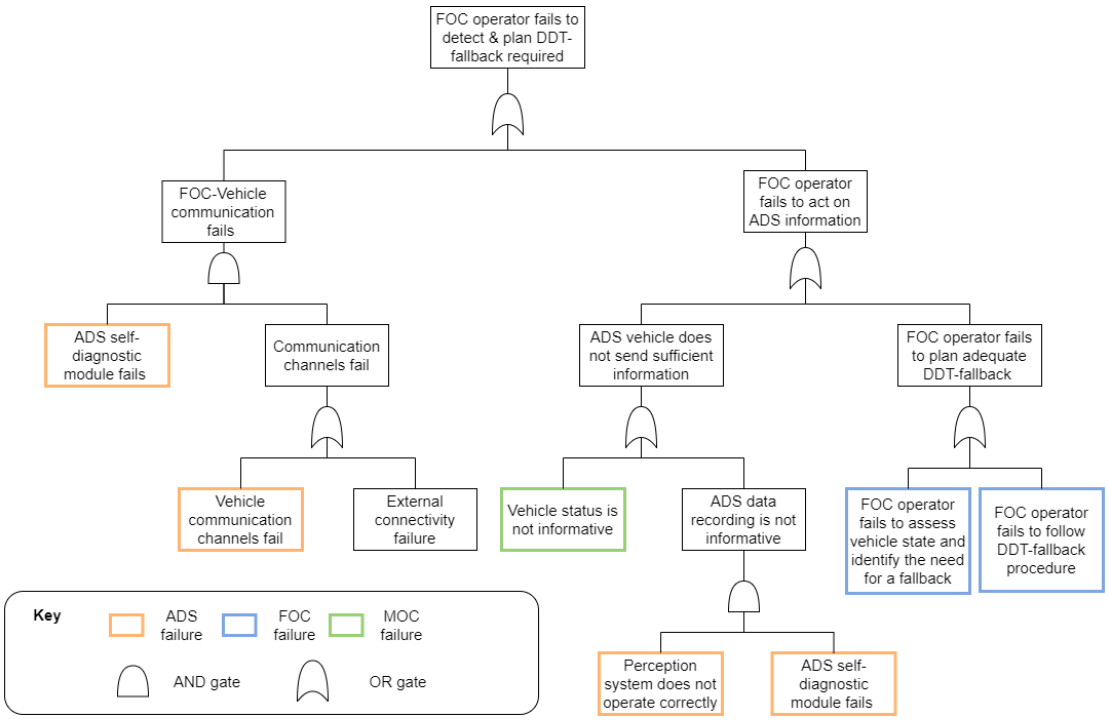


Table 3: Undeveloped Events for FOC fallback detection failure FT.

Undeveloped Event	Failure Type	Main Role
Self-diagnostic module fails	Software	ADS
Vehicle communication channels fail	Software/Hardware	ADS/MOC
External connectivity failure	External	-
Vehicle status is not informative	Maintenance/Design	MOC
Perception system does not operate correctly	Software/Hardware	ADS/MOC
FOC operator fails to assess vehicle state and identify the need for a fallback	Human	FOC
FOC operator fails to follow DDT-fallback procedure	Human	FOC

The limited ability of static models to characterize dynamic hazard events is one of the most relevant shortcomings of traditional hazard identification methods, such as ESDs and FTs. This is particularly relevant when analyzing complex systems that are expected to exhibit intricate subsystem interactions, evolving feedback loops, and emerging properties. Further, even in autonomous systems, human interactions and emerging behavior play a key role in system operations [20]. Human reliability analysis methods are thus a valuable tool to assess the causes of their errors and aid the development of adequate mitigation measures. Despite known limitations, traditional static methods still play an important role in hazard identification and modeling steps and aid the safety assessment while analyzing system designs. These methods are widely used in industry, and many standards have been developed based on these [21]. Further work is needed to collect relevant data to quantify the likelihood and consequences of the failures described.

4. CONCLUSION

In the advent of the expansion of L4 ADS vehicle operations, most research efforts have focused on determining the functional safety of these complex systems. However, as these automated vehicles will become more frequent in MaaS, operational safety must also be addressed. This work explores how L4 ADS fleets may operate as MaaS, focusing on the interactions between the ADS and the remote fleet operator. A functional breakdown of these operations is presented, along with a generic operational profile. Based on identifying distinct operation phases, ESD are employed to model potential hazard scenarios which may be encountered. An example is presented for the case of an ADS vehicle driving towards a destination with no passengers on board. After identifying key sub-events of this phase, methods to quantify these are discussed and an example FT is presented for the top failure of the FOC operator not detecting and planning a required DDT fallback. Based on the events and subevents defined in this work, the high-level FTs developed highlight the importance of considering the active roles the FOC and MOC play in ensuring operational safety.

The discussion and results presented in this paper are part of a larger project aiming at identifying ADS L4 operating as MaaS fleet operators' safety responsibilities and risk mitigation activities. The authors are conducting further work to develop the ESDs and accompanying FTs, as well as CoTA and STPA.

References

[1] Y. Z. Wong, D. A. Hensher, and C. Mulley, "Mobility as a service (MaaS): Charting a future context," *Transp. Res. Part A Policy Pract.*, vol. 131, pp. 5–19, Jan. 2020.

[2] A. Polydoropoulou, I. Pagoni, and A. Tsirimpa, "Ready for Mobility as a Service? Insights from stakeholders and end-users," *Travel Behav. Soc.*, vol. 21, no. November 2018, pp. 295–306, Oct. 2020.

[3] SAE J3206, "Taxonomy and Definition of Safety Principles for Automated Driving System (ADS)," vol. 4970, 2021.

[4] National Highway Traffic Safety Administration, "Automated Driving System 2.0: A Vision for Safety," 2017.

[5] E. Thorn, S. Kimmel, and M. Chaka, "A Framework for Automated Driving System Testable

Cases and Scenarios," 2018.
[6] C. W. Lee, N. Nayeer, D. E. Garcia, A. Agrawal, and B. Liu, "Identifying the Operational Design Domain for an Automated Driving System through Assessed Risk," in *2020 IEEE Intelligent Vehicles Symposium (IV)*, 2020, no. Iv, pp. 1317–1322.
[7] AVSC00006202103, "AVSC Best Practice for Metrics and Methods for Assessing Safety Performance of Automated Driving Systems (ADS)," 2021.
[8] S. Sohrabi, A. Khodadadi, S. M. Mousavi, B. Dadashova, and D. Lord, "Quantifying the automated vehicle safety performance: A scoping review of the literature, evaluation of methods, and directions for future research," *Accid. Anal. Prev.*, vol. 152, no. January, p. 106003, Mar. 2021.
[9] S. Khastgir, S. Brewerton, J. Thomas, and P. Jennings, "Systems Approach to Creating Test Scenarios for Automated Driving Systems," *Reliab. Eng. Syst. Saf.*, vol. 215, p. 107610, Nov. 2021.
[10] M. Chaka *et al.*, "FMVSS Considerations for Vehicles With Automated Driving Systems: Volume 2," vol. 1, no. April, p. 630p, 2021.
[11] B. Kramer, C. Neurohr, M. Büker, E. Böde, M. Fränzle, and W. Damm, "Identification and Quantification of Hazardous Scenarios for Automated Driving," in *Lecture Notes in Computer Science*, vol. 12297 LNCS, Springer Science and Business Media Deutschland GmbH, 2020, pp. 163–178.
[12] M. A. Ramos, C. A. Thieme, I. B. Utne, and A. Mosleh, "A generic approach to analysing failures in human – System interaction in autonomy," *Saf. Sci.*, vol. 129, Sep. 2020.
[13] X. Yang, I. B. Utne, S. S. Sandøy, M. A. Ramos, and B. Rokseth, "A systems-theoretic approach to hazard identification of marine systems with dynamic autonomy," *Ocean Eng.*, vol. 217, p. 107930, Dec. 2020.
[14] S. Swaminathan and C. Smidts, "The Event Sequence Diagram framework for dynamic Probabilistic Risk Assessment," *Reliab. Eng. Syst. Saf.*, vol. 63, no. 1, pp. 73–90, Jan. 1999.
[15] C. A. Thieme, A. Mosleh, I. B. Utne, and J. Hegde, "Incorporating software failure in risk analysis – Part 1: Software functional failure mode classification," *Reliab. Eng. Syst. Saf.*, vol. 197, p. 106803, May 2020.
[16] C. A. Thieme, A. Mosleh, I. B. Utne, and J. Hegde, "Incorporating software failure in risk analysis—Part 2: Risk modeling process and case study," *Reliab. Eng. Syst. Saf.*, vol. 198, p. 106804, Jun. 2020.
[17] M. Abilio Ramos, I. B. Utne, and A. Mosleh, "Collision avoidance on maritime autonomous surface ships: Operators' tasks and human failure events," *Saf. Sci.*, vol. 116, pp. 33–44, Jul. 2019.
[18] M. A. Ramos, C. A. Thieme, I. B. Utne, and A. Mosleh, "Human-system concurrent task analysis for maritime autonomous surface ship operation and safety," *Reliab. Eng. Syst. Saf.*, vol. 195, p. 106697, Mar. 2020.
[19] Y. H. J. Chang and A. Mosleh, "Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents. Part 4: IDAC causal model of operator problem-solving response," *Reliab. Eng. Syst. Saf.*, vol. 92, no. 8, pp. 1061–1075, Aug. 2007.
[20] M. A. Ramos and A. Mosleh, "Human Role in Failure of Autonomous Systems: A Human Reliability Perspective," *Proc. - Annu. Reliab. Maintainab. Symp.*, vol. 2021-May, 2021.
[21] International Organization for Standardization, "ISO 26262:2018, Road vehicles — Functional safety." 2018.