Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P326-cd

Safety hazard identification of inspection and maintenance operations for Automated Driving Systems in Mobility as a Service

Camila Correa-Jullian[1,2], John McCullough[1], Marilia Ramos[2], Ali Mosleh[2], Jiaqi Ma[2,3]

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

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

[3] *Dept. of Civil and Environmental Engineering, University of California, Los Angeles, USA. E-mail: jiaqima@ucla.edu*

Cooperative decision-making between humans and automated agents operating at various levels of autonomy (LoA) is an increasing trend observed across multiple industries and research areas. Assessing emerging properties and unintended behaviors in complex engineering systems is key to developing policies to prevent and mitigate risks during operation stages. An aspect often overlooked in analyses of autonomous system operation is developing and enforcing adequate inspection and maintenance policies. In this work, the Concurrent Task Analysis (CoTA) method is used to analyze the operation of a Level 4 Automated Driving System (L4 ADS) fleet employed for Mobility as a Service (MaaS). The method is employed to define tasks and responsibilities key to supporting the safe operation of the ADS vehicles based on a functional breakdown of the system, the development of operational scenarios, and the identification of safety hazards. The CoTA describes the interaction between distinct fleet operator agents (e.g., fleet monitoring and vehicle maintenance), identifies critical tasks, and traces cascading and latent failures between them. This paper presents the CoTA of the inspection and maintenance operational phases and discusses the safety implications on the fleet operator's safety responsibilities to ensure adequate operation of the ADS fleet.

Keywords: Concurrent task analysis, automated driving systems, safety assessments, mobility as a service, inspection and maintenance procedures.

1. Introduction

Autonomous Driving Systems (ADS) vehicles are poised to transform the transportation landscape in the future. The Society of Automotive Engineers (SAE) establishes six levels of vehicle automation. Level 5 represents a fully self-driving vehicle that operates without human intervention and is unrestricted in its operational range. Level 4 (L4) ADS, on the other hand, can perform all Dynamic Driving Tasks (DDT) within a designated Operational Design Domain (ODD) and may require human input under certain conditions (SAE International, 2021). Vehicles equipped with L4 ADS are becoming commercially available in the context of Mobility as a Service (MaaS). Companies such as Waymo and Cruise are some of the leading companies in the U.S. in terms of developing, testing, and deploying these vehicles.

Amid the currently evolving technical, commercial, and regulatory environment, using L4 ADS for MaaS raises questions about how developers and fleet operators may provide adequate safety assurance prior to widespread commercialization and deployment. Recent incident reports collected from testing and small-scale deployment imply that a more focused approach on operational safety is required, for instance, to avoid traffic disruptions, or to determine appropriate incident management procedures (National Highway Traffic Safety Administration, 2022). The latter may become an important element when scaling operations where passengers are on-board a vehicle with no safety driver.

In general, efforts in assessing the safety of ADS vehicles have focused either on aspects of functional safety and component-level reliability,

or high-level traffic safety impacts (Sohrabi et al., 2021). Scenario-based simulation and drive testing demonstrate system performance empirically (Khastgir et al., 2021; Zhao et al., 2020). However, ADS are complex systems composed of several sub-systems whose interaction may lead to unintended behaviors. Therefore, identifying and analyzing sub-systems' and emergent failures is crucial for preventing and mitigating operational risks. Further, the application of traditional risk assessment methods has been mostly limited to hazards originating from hardware or software malfunctions. Nevertheless, risk analyses must also include organizational safety and human-related issues, as they are crucial in ensuring ADS operational safety and gaining the public's trust (Lokshina et al., 2021; Ramos & Mosleh, 2021).

At a system level, operational safety aspects require further study; in particular, what are the supporting inspection and maintenance activities that need to be performed by the fleet operators to ensure the safe deployment of ADS vehicles. In the context of large-scale fleet operations, inspection and maintenance activities play a critical supporting role (Kumar et al., 2022). Indeed, the maintenance crew's adequate performance can be vital to preventing high-severity hazard scenarios that may arise from the failure of the ADS vehicles' elements. While errors of the maintenance crew may not necessarily lead to an immediate vehicle failure, they can increase the severity or likelihood of failures developed later. These latent failures' effect on the system's overall performance is difficult to trace and quantify. While the vehicles are expected to be equipped with online fault and failure detection mechanisms and context-aware fallback responses, fleet operators still require tools to maintain and manage the vehicles. Further, issues such as software updates, instrument calibration, and repairs may become defining elements in the relationship between fleet operators and the ADS developers.

The importance and complexity of inspection and maintenance activities calls for a structured approach to design the operation so that the fleet operator provides the maintenance crew with adequate resources to inspect, diagnose, and correct possible issues of the ADS vehicle before clearing it for operation. Approaches such as System-Theoretic Process Analysis (STPA) (Leveson & Thomas, 2018) and Concurrent Task Analysis (CoTA) (Ramos et al., 2020a, 2020b) provide a practical alternative to traditional hazard identification methodologies for complex systems. This work presents an application of the CoTA method to identify safety hazards and define responsibilities key to supporting the safe operation and maintenance of the L4 ADS fleets employed for MaaS. This constitutes a crucial step that can provide insight to develop more comprehensive procedures and guidelines to ensure operational safety.

2. Concurrent Task Analysis

CoTA is a method recently developed as part of the Human-System Interaction in Autonomy (H-SIA) framework to assess the safety of autonomous systems (Ramos et al., 2020a, 2020b). This method analyzes a system's expected behavior and performance based on the hierarchical decomposition of system-level goals. The CoTA method can be implemented as a valuable hazard identification methodology or used to identify operational responsibilities of multiple agents (a sub-system with agency within the system operation) to perform common high-level safety-related goals. CoTA models are constructed from scenario-based method Event Sequence Diagrams (ESDs) and may be combined with Fault Trees to provide qualitative and quantitative insights. The ESD pivotal events, which should be associated with one agent only, are translated into the tasks required for each event to be successful. Hence, CoTA models can be developed to express dependencies between the system's agents' tasks depending on the operational scenario, phase, or mode. Developing a CoTA diagram starts with defining the agents to be analyzed and the main task (Task 0) to be accomplished (Thieme et al., 2023). The main system-level goal is then decomposed or *redescribed* until the desired level of task granularity is achieved. The sub-goals of each group of tasks are organized through plans, indicating the order in which sub-goals must be achieved to support the completion of system-level goals. Depending on the necessary conditions for a sequence of events to be successful, tasks can be categorized as:

- Sequential tasks: Tasks performed in sequence.
- Parallel tasks: Tasks performed concurrently.

- Trigger tasks: Tasks that trigger the initiation of other tasks.
- Interface tasks: Tasks that provide input for different agents.

The re-description level adopted in CoTA follows an extension of the cognitive model IDA–Information, Decision, and Action–to human and autonomous systems (Chang & Mosleh, 2007; Ramos et al., 2020a, 2020b). Therefore, all tasks performed by either human or machine agents are decomposed into steps focusing on receiving information, deciding the adequate action to be performed, and performing the corresponding action. The subtasks are re-described until one of the following conditions are met (*stop-rules*) (Thieme et al., 2023):

- The sub-tasks are associated with only one of the IDA phases;
- The dependency of interface tasks is explicitly identified;
- The dependency of trigger tasks is explicitly identified.

This process can be employed to identify the resources needed to perform said actions, e.g., how the information is transmitted and presented to the agent, what previous knowledge the agent requires to decide the appropriate action, and what mechanisms are needed to perform the actions adequately.

3. Case Study: Level 4 ADS Fleets in MaaS

The focus of this study is the reference fleet defined in (Correa-Jullian et al., 2022a, 2022b). This fleet comprises light passenger vehicles equipped with SAE L4 ADS-coherent capabilities, i.e., high-automation vehicles performing DDTs under specific ODD conditions.

The operation of these vehicles is supported by a fleet operations center (FOC), with remote operators dedicated to performing safety (monitoring, limited intervening) and service-related tasks (communicating with passengers, contacting third parties). Vehicle inspection, maintenance, and management are handled by the maintenance operations center (MOC).

The tasks of these agents are organized into different operational phases, such as when the vehicle is on-route with or without passengers onboard, post-incident management, and inspection and maintenance activities.

3.1 *System modeling through ESD and CoTA*

CoTA diagrams are developed for each agent and operational phase. The main goals and tasks are redescribed for each operational phase as detailed in Section 2. For this analysis, we have combined the activities performed during inspection, corrective maintenance, preventive maintenance, and system updates. The difference between these maintenance-related activities resides in the type of actions and frequency at which they are performed, i.e., verifying the vehicle is fit for operation vs. updating or replacing major software or hardware components. A simplified ESD addressing these activities is presented in Figure 1. Corresponding end-states are described in Table 1.

The resulting CoTA diagram is shown in Figure 2. The primary agent of this phase is the MOC, whose main task (Task 0) is to perform the inspection and maintenance activities. The MOC's tasks are divided into three sub-agents: the inspection crew, maintenance crew, and coordinator crew (Table 4). These sub-agents, particularly the coordinators, will need to work alongside FOC remote operators to gather information about the vehicle and determine what kind of inspection and maintenance activities are required (Task 1). A vehicle arriving at the MOC may be scheduled for inspection prior to being cleared for a new operational shift (Task 2), or for corrective maintenance actions due to failure during operation (Task 5). The vehicle may also be scheduled for preventive actions such as service maintenance (Task 3, for elements not as frequently inspected) or any system software updates or instrument calibration (Task 4) as required by the schedule provided by the ADS developer. Depending on the outcome of these tasks (Tasks 2, 3, 4), further activities are performed at the MOC (Tasks 5, 6), or external maintenance support is requested from the ADS developer. Related tasks of the FOC are listed in Table 3.

To visualize the effect of the MOC crew's correct performance on the vehicle's safety, we analyze the ADS vehicle's subsystems critical to its operation. Table 2 provides a high-level description of the ADS vehicle's main tasks to be performed on-route when transporting passengers. These tasks are broadly categorized as collecting and processing real-time data (Task 1), performing DDT functions (Task 2), determining if a DDT-

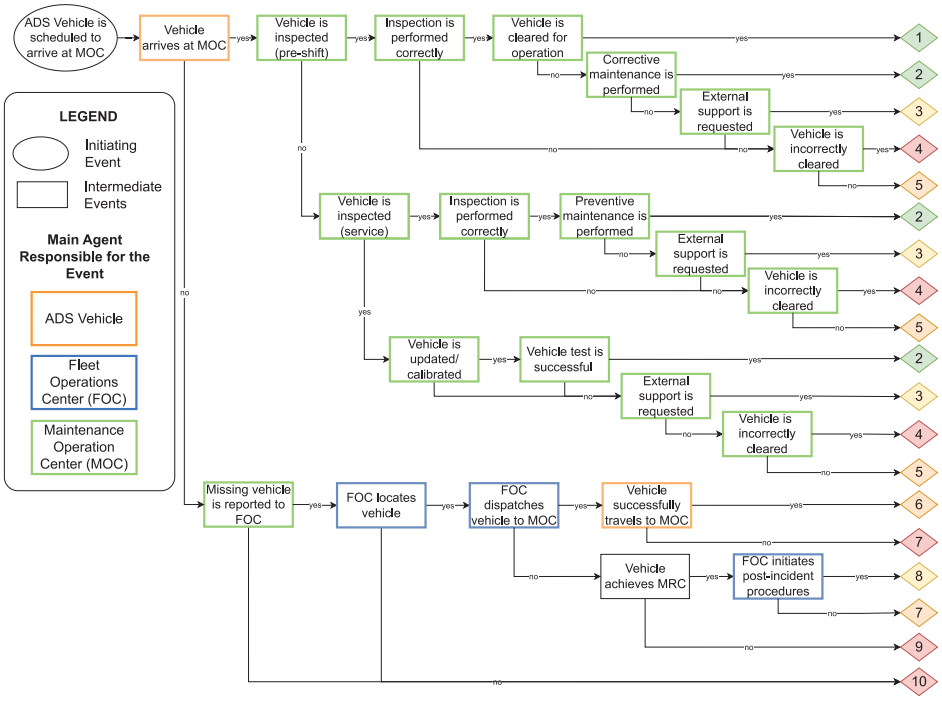

Figure 1: Simplified ESD for inspection and maintenance activities.

Table 1: ESD end-states for inspection and maintenance activities.

No.	End-State	No.	End-State
1	Vehicle cleared for operation	6	Vehicle arrives at MOC for maintenance
2	Vehicle scheduled for pre-shift inspection or for corrective maintenance	7	Vehicle is stranded
3	Vehicle is scheduled for external maintenance	8	Post-incident procedures are initiated
4	Vehicle incorrectly cleared for operation	9	Collision risk
5	Vehicle is stationed at MOC	10	Vehicle is unreachable

fallback plan is required based on context-specific triggers (Task 3) and implementing the selected fallback plan (Task 4). DDT fallback triggers include ODD breaches, a vehicle failure, a collision, an external party or passenger onboard requesting the vehicle to stop, or by encountering edge/corner cases. Vehicle connectivity (Task 5) and self-diagnostic modules (Task 6) support the vehicle's safe operation, acting as additional safety barriers.

These safety barriers rely on ADS sensor hardware, software, connectivity, and vehicle control elements. These are identified as potential risk contributors in Table 2, i.e., sensor hardware, data fusion software, vehicle control, built-in traffic and navigation assistance, DDT fallback strategies plans, and assessment tools. Failures during the operation of any of these elements would lead to multiple undesirable consequences, ranging from traffic disruptions and property damage to potential injuries of passengers and/or other road users. For instance, the ADS vehicle not detecting a DDT fallback is required may be caused by sensor hardware failures, errors in sensor fusion, object detection or trajectory prediction software, or a passenger stop request that may not have been recognized by the ADS software (Correa-Jullian et al., 2022a).

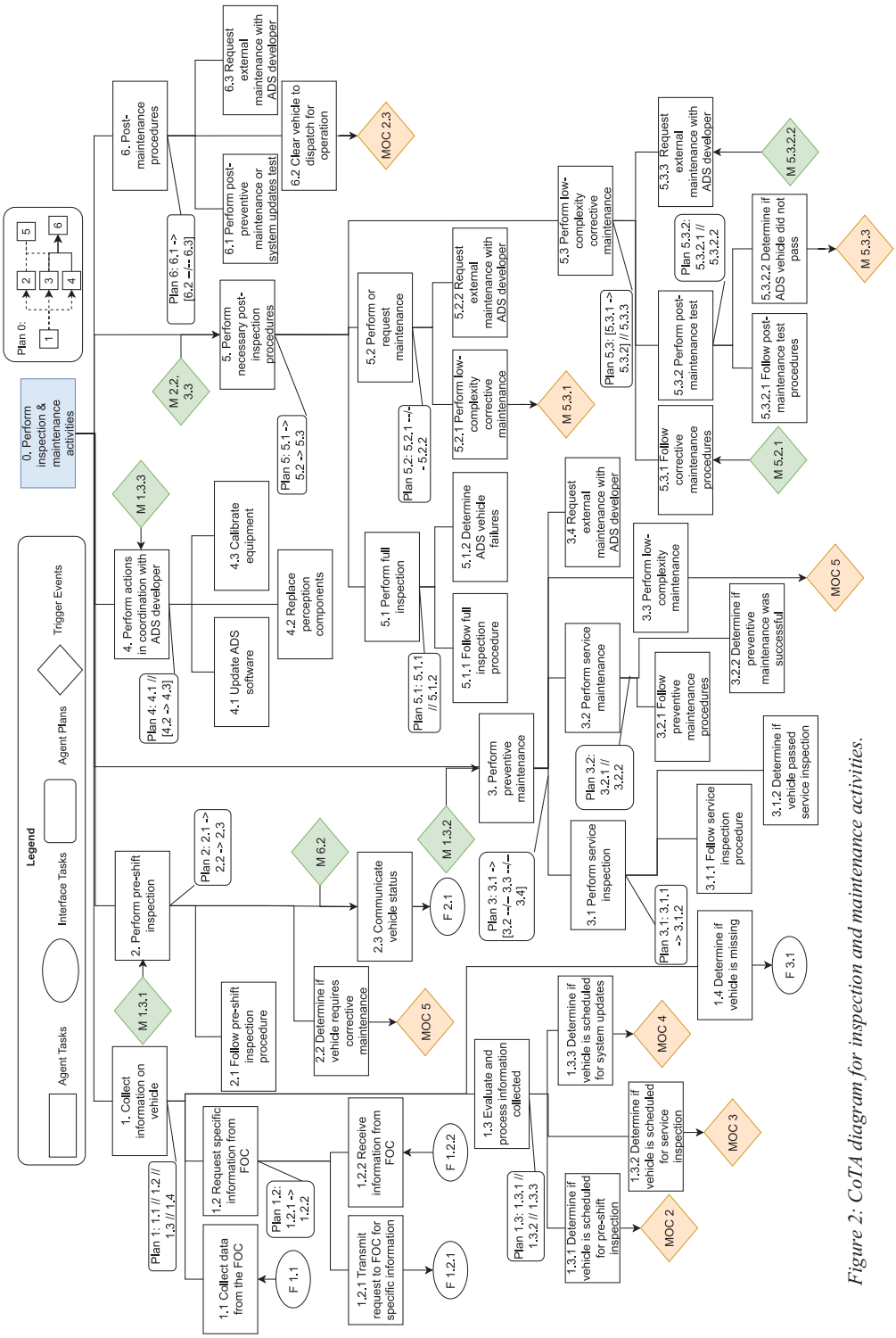

Figure 2: CoTA diagram for inspection and maintenance activities.

Table 4: MOC sub-tasks for inspection and corrective maintenance operational phases.

Task	Type	Description
1	Sequential	The MOC coordination team collects information on the vehicle to determine what inspection or maintenance activity is required: pre-shift inspection (Task 2), service inspection and maintenance (Task 3), or system updates (Task 4). If any vehicle expected at the MOC has not arrived and the FOC should be contacted for support.
2	Exclusive Sequential/ Trigger	The MOC inspection crew performs the inspection according to the specified procedure and determines if the vehicle is fit for operation. If the vehicle passes the pre-shift inspection, the MOC inspection crew informs the FOC that the vehicle has been cleared for operation.
3	Exclusive Sequential/ Trigger	The MOC inspection crew performs the service inspection according to the specified procedure and determines if the vehicle requires additional corrective actions (Task 5, performed by the MOC maintenance crew) or if external maintenance support is required.
4	Exclusive Sequential	The MOC maintenance crew performs maintenance actions in coordination with the ADS developer in the case the vehicle is scheduled for a system update.
5	Triggered/ Trigger	The MOC maintenance crew perform the necessary corrective maintenance actions or request external support from the ADS developer.
6	Sequential	The MOC maintenance crew verifies the system updates or preventive maintenance actions. If the vehicle passes the tests, the MOC maintenance crew should refer the vehicle to the MOC inspection crew for pre-shift inspection. If the vehicle does not pass the pre-shift inspection, the MOC should request external maintenance.

Table 3: FOC sub-tasks for inspection and corrective maintenance operational phases.

Task	Type	Description
1	Parallel	The FOC operator support inspection and maintenance activities. Tasks include transmitting recorded logs (1.1) and requested vehicle data (1.2.1, 1.2.2) to the MOC.
2	Parallel	The FOC operator is expected to receive information on which vehicles have been cleared for operation by the MOC inspection crew (2.1). The FOC operator should then dispatch the vehicle for operation.
3	Parallel/ Trigger	If the FOC operators receive a request from the MOC crew that a vehicle is missing (3.1), it is expected to locate, dispatch, or direct the vehicle to an MRC.

Table 2: ADS vehicle on-route high-level tasks and risk contributors.

Task	Task Description	High-level risk contributors
1	The ADS continuously collects and processes information about the vehicle's state and surroundings from its sensor suite.	ADS sensor hardware, ADS software
2	The ADS uses the processed information to perform Dynamic Driving Tasks (DDT), including trajectory planning and prediction, and object and event detection and response (OEDR).	ADS software, ADS vehicle control.
3	The ADS continuously performs real-time safety evaluation to determine if a DDT fallback plan is required.	ADS software
4	This task is triggered only if a DDT fallback is required. This includes determining, implementing, and evaluating the outcome of a DDT fallback plan. The ADS may request a fallback plan from the FOC if it cannot develop a fallback strategy.	ADS software, vehicle control
5	The ADS is expected to continuously receive and transmit requests to the FOC and maintain a reliable communication with passengers.	ADS connectivity, ADS sensor hardware
6	The ADS continuously monitors its subsystems to identify any faults, failures, or malfunctions. Diagnostic logs are transmitted to the FOC.	ADS sensor hardware, ADS diagnostic software

3.2 *Identification of operational safety hazards and responsibilities*

Each safety hazard is derived from the failure of an ESD event. Only ESD events associated with an agent are considered (as shown in Figure 1). Each high-level safety hazard relates to multiple failure modes identified through the CoTA. Focusing on the MOC's agents, the following safety hazards are found:

The MOC fails to:

(i) Report a missing vehicle.
(ii) Inspect the vehicle (pre-shift/service).
(iii) Perform the inspection correctly.
(iv) Follow vehicle clearance procedures.
(v) Perform corrective maintenance.
(vi) Perform preventive maintenance.
(vii) Schedule external maintenance.
(viii) Correctly perform system updates.

These safety hazards may lead to the end-state (4) "Vehicle incorrectly cleared for operation". This end-state qualitatively represents a higher severity than, for instance, the vehicle being stationed at the MOC (5). Further, this kind of latent operational failure may lead to the ADS vehicle failing to perform its tasks (Table 2).

From an operational safety perspective, the MOC's tasks focus on preventing an ADS vehicle operates with existing failures or develops a failure during operation. Given the safety hazards identified and the MOC's hierarchy of tasks, the following operational responsibilities are identified for each sub-agent:

MOC coordinators crew (Task 1):

- Follow the provided inspection and maintenance activity schedule.
- Manage arriving ADS vehicles and report if any vehicle has not arrived on schedule.
- Collect relevant information about the vehicle from the FOC's operation logs.
- Instruct MOC crew of inspection and maintenance procedures and updates from the ADS developers to the crew.

MOC inspection crew (Tasks 2-5):

- Follow the established procedure to perform pre-shift and service inspection activities (including safety checklists, diagnostic software tests).
- Interpret diagnostic logs and report anomalous system behavior.
- Follow vehicle clearance procedures or transfer it to the maintenance crew.

MOC maintenance crew (Tasks 3-4-6):

- Follow the established procedure to perform low-complexity corrective maintenance or preventive maintenance actions.
- Follow the established procedure to perform system updates or instrumentation calibration.
- Request external maintenance support to the ADS developer if task complexity exceeds established procedures.

An overarching responsibility of the MOC coordination crew is to adequately instruct the inspection and maintenance crew about the procedures they must follow. Note that the bulk of the MOC's activities, such as safety checklists and software tools, are expected to be provided by or developed in coordination with the ADS developer. If so, the fleet operator's role is to ensure inspection and maintenance activities are performed as intended by the ADS developer.

Effective hazard identification methodologies play a key role in defining what is safe enough, providing a robust basis for future risk quantification efforts. Identifying the safety hazards through a structured methodology is the first step to developing adequate safety barriers from a functional and procedure-based perspective. These barriers, in the form of operational procedures or system design, are needed to address human and organizational aspects still present in autonomous system operations. The approach presented based on CoTA can be helpful to ensure all safety responsibilities address the identified safety hazards. From these results, further work may be focused on deriving the requirements (e.g., tools, training, etc.) each agent requires to perform their safety-related tasks.

4. Conclusions

Hazard identification methodologies usually focus on functional safety aspects for many complex systems. However, when analyzing the safety hazards of a system's operation, other essential aspects may become relevant, such as addressing the system's evolution during operation. In the case of ADS fleets, this implies the need to analyze the subsystems or agents that support the vehicle's operation rather than the

vehicle software and hardware only. This work focuses on the inspection and maintenance activities of an L4 ADS fleet for MaaS, tracing latent operational errors that can lead to high-risk hazards. These latent failures or errors can be traced by the CoTA, where tasks and responsibilities are hierarchically linked. The use and development of the CoTA model allows redescribing each task to a level of granularity from where specific safety responsibilities may be derived. The analysis provides essential insights into operational safety concerns related to the large-scale deployment of ADS vehicles.

Acknowledgement

This research is partly supported by the U.S. Department of Transportation National Highway Traffic Safety Administration. The work presented in this paper remains the sole responsibility of the authors.

References

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. *32nd European Safety and Reliability Conference (ESREL 2022).* 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. Presented at Probabilistic Safety Assessment and Management (PSAM 16). *Presented at Probabilistic Safety Assessment and Management (PSAM 16)*.

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

Kumar, G., James, A. T., Choudhary, K., Sahai, R., & Song, W. K. (2022). Investigation and analysis of implementation challenges for autonomous vehicles in developing countries using hybrid structural modeling. *Technological Forecasting and Social Change*, *185*, 122080. https://doi.org/10.1016/J.TECHFORE.2022.122080

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

National Highway Traffic Safety Administration. (2022). Summary Report: Standing General Order on Crash Reporting for Level 2 Advanced Driver Assistance Systems. *U.S. Department of Transportation Summary Report DOT HS 813 324*, *June*, 1–9. https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-06/ADAS-L2-SGO-Report-June-2022.pdf

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

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., Ramos, M. A., Holte, E. A., Johnsen, S. O., Myklebust, T., & Smogeli, Ø. (2023). *New Design Solutions and Procedures for Ensuring Meaningful Human Control and Interaction with Autonomy: Automated Ferries in Profile*. 213–242. https://doi.org/10.1007/978-3-031-24740-8_11

Zhao, X., Salako, K., Strigini, L., Robu, V., & Flynn, D. (2020). Assessing safety-critical systems from operational testing: A study on autonomous vehicles. *Information and Software Technology*, *128*, 106393. https://doi.org/10.1016/j.infsof.2020.106393