The B. John Garrick Institute for the Risk Sciences
UCLA ENGINEERING

An STPA-based analysis of Automated Driving Systems fleet maintenance activities

Camila Correa-Julian, MSc*,

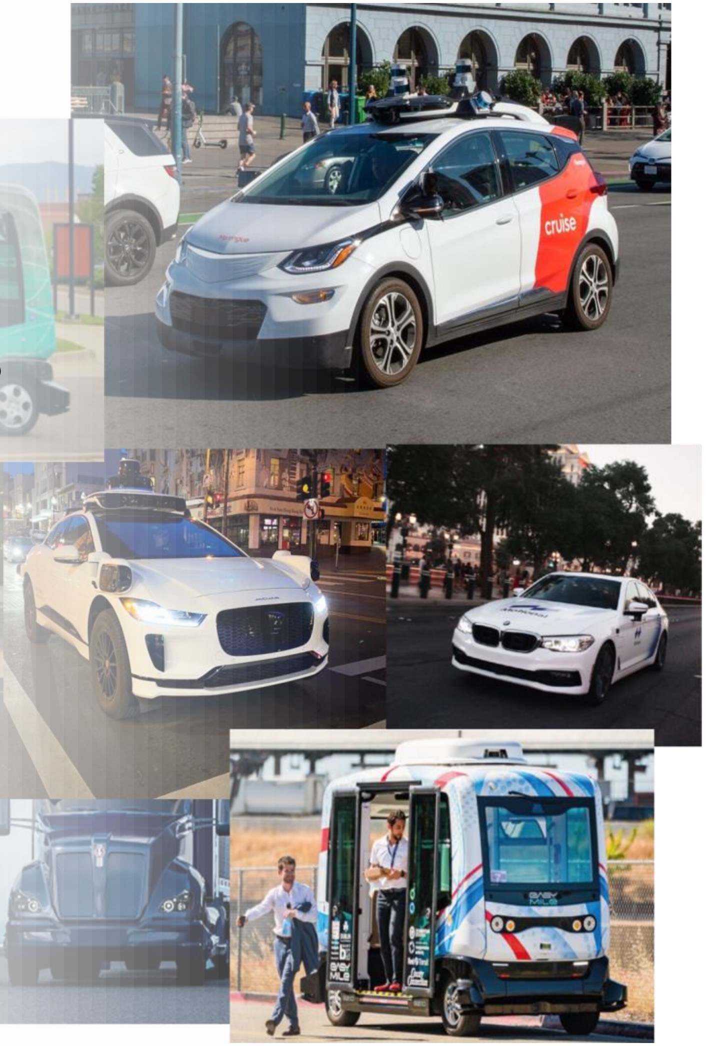
Marilia A. Ramos, PhD; Ali Mosleh, PhD; Jiaqi Ma, PhD.

The B. John Garrick Institute for the Risk Sciences, University of California Los Angeles

RAMS 2024

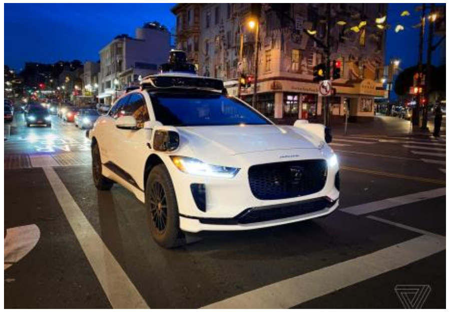
Overview and Outline

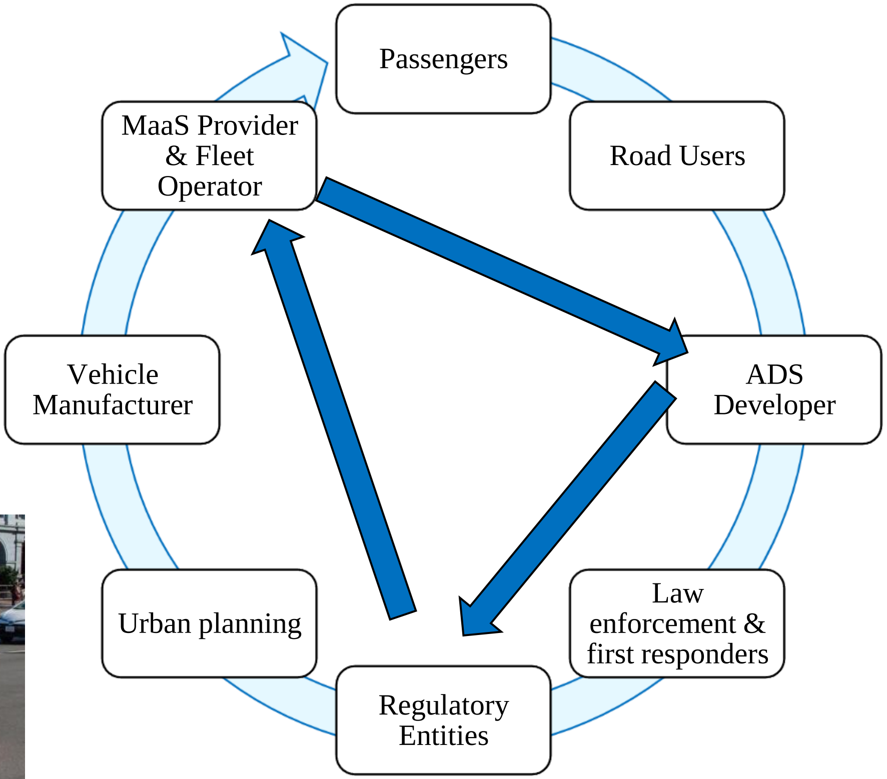
- Introduction: Automated Driving Systems in Mobility as a Service.
- Inspection and Maintenance Activities in Fleet Operations.
- Using System-Theoretic Process Analysis (STPA) for Fleet Operations.
- Safety Hazards & Operational Safety Responsibilities Identification.
- Summary & Conclusions



SAE Level 4 Autonomous Driving Systems (ADS) in Mobility as a Service (MaaS)

- Mobility as a Service (MaaS) integrates various forms of transport and transport-related services into a single, comprehensive, and on-demand mobility service [1,2].
- Waymo, Cruise & Zoox, are some companies involved in MaaS.





[1] Y. Z. Wong, D. A. Hensher, and C. Mulley, "Mobility as a service (MaaS): Charting a future context".
[2] A. Polydoropoulou, I. Pagoni, and A. Tsirimpa, "Ready for Mobility as a Service? Insights from stakeholders and end-users".

L4: SAE Level 4
ADS: Automated Driving System

Operational Safety: Maintenance & Inspection activities are usually overlooked

- Operational Safety goes beyond functional safety.
- Inspection and maintenance activities play a critical supporting role in large-scale fleet operations.
- Effects of latent failures on system safety – increase likelihood or severity of developing hazards.
- In ADS fleets: Software updates, instrument calibration & repairs can become a defining element in the partnership of ADS developers and fleet operators.

Operational Aspects

- Operational Design Domain (ODD)
- Dispatching & planning
- Health & status monitoring
- *Inspection, maintenance, & repair*
- Incident response, investigation, & reporting
- Crew staffing & training
- Passenger communication & safety

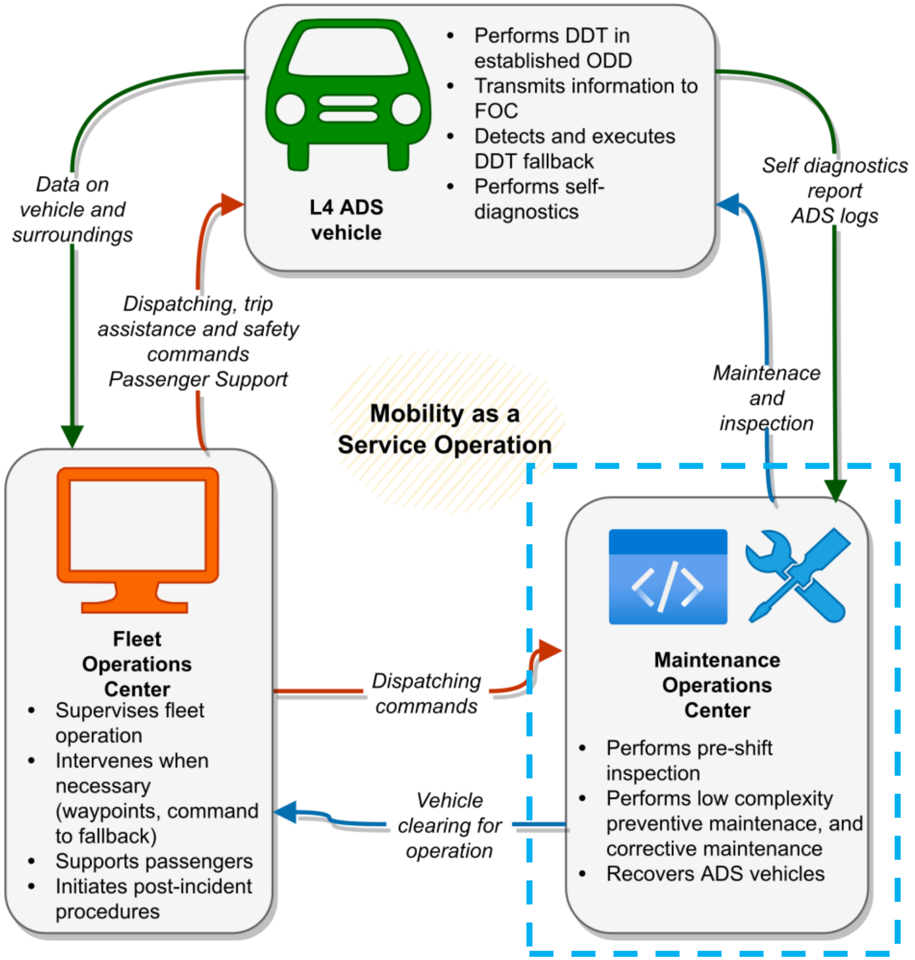
Structured approach to design inspection and maintenance operations – define tasks, responsibilities and resources required.

[3] G. Kumar, A. T. James, K. Choudhary, R. Sahai, and W. K. Song, "Investigation and analysis of implementation challenges for autonomous vehicles in developing countries using hybrid structural modeling,"

ADS: Automated Driving System DDT: Dynamic Driving Task ODD: Operational Design Domain

Agent and Operational Phase Breakdown

Inspection / Maintenance	• Performed by Maintenance Operation Center
On Route Without Passengers	• Performed by ADS Vehicle and Fleet Ops Center
On Route With Passengers	• Performed by ADS Vehicle and Fleet Ops Center
Pickup / Dropoff	• Performed by ADS Vehicle
Post-Incident	• Performed by ADS Vehicle and Fleet Ops Center



L4 ADS vehicle

- Performs DDT in established ODD
- Transmits information to FOC
- Detects and executes DDT fallback
- Performs self-diagnostics

Fleet Operations Center

- Supervises fleet operation
- Intervenes when necessary (waypoints, command to fallback)
- Supports passengers
- Initiates post-incident procedures

Maintenance Operations Center

- Performs pre-shift inspection
- Performs low complexity preventive maintenance, and corrective maintenance
- Recovers ADS vehicles

Mobility as a Service Operation

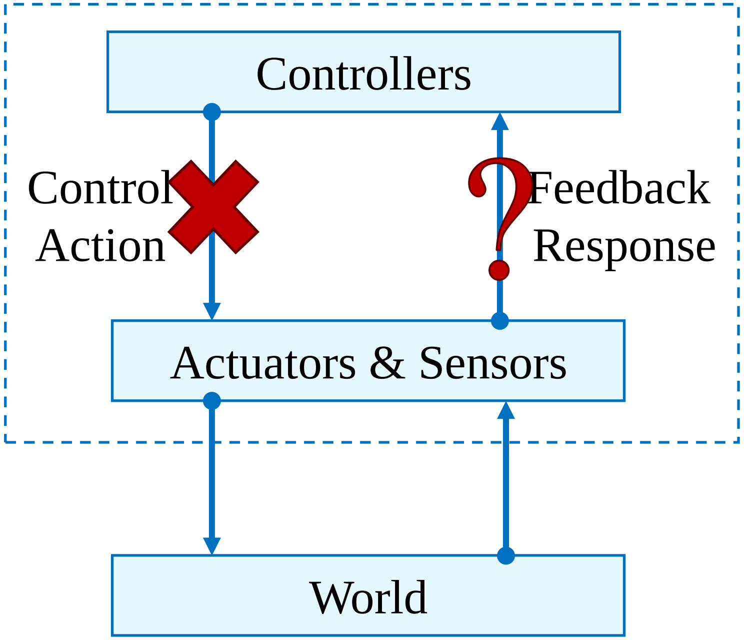
Data on vehicle and surroundings
Dispatching, trip assistance and safety commands
Passenger Support
Self diagnostics report
ADS logs
Maintenace and inspection
Dispatching commands
Vehicle clearing for operation

[4] Camila Correa-Jullian, John McCullough, Marilia Ramos, Jiaqi Ma, Enrique Lopez Droguett, and Ali Mosleh. “Modeling Fleet Operations of Autonomous Driving Systems in Mobility as a Service for Safety Risk Analysis” (ESREL 2022), “Safety Hazard Identification for Autonomous Driving Systems Fleet Operations in Mobility as a Service” (PSAM 16).

System-Theoretic Process Analysis (STPA)

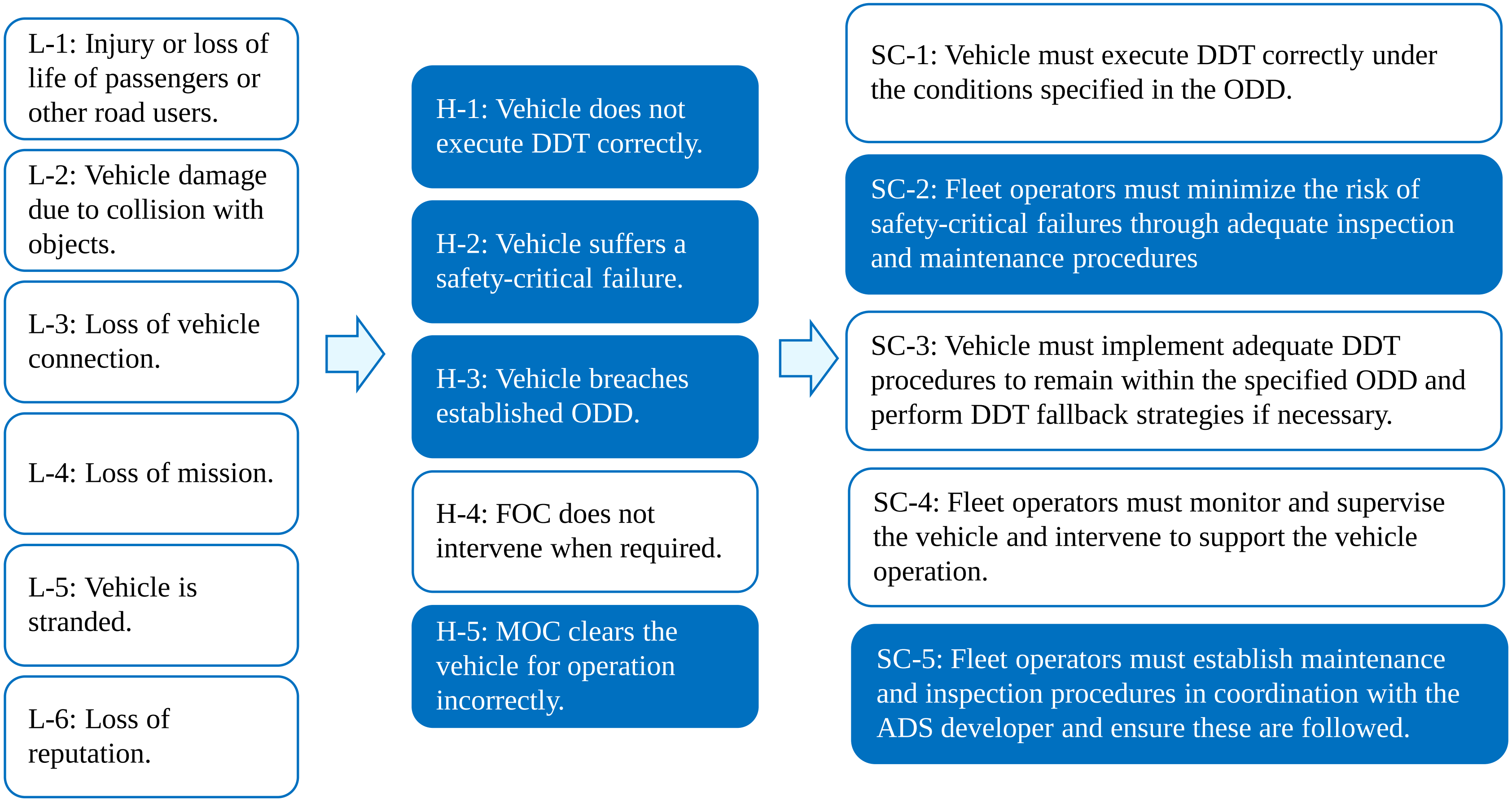
- Roots in systems & control theory and System Theoretic Accident Model and Processes (STAMP).
- Methodology:
  - ❑ Define the system, stakeholders, loss scenarios, system boundaries, system-level hazards, and system-level constraints.
  - ❑ Develop the hierarchical control structure diagram.
  - ❑ Identify UCAs that may breach the system-level constraints.
  - ❑ Identify the corresponding loss scenarios resulting from the UCA.

Method focused on analyzing Unsafe Control Actions (UCAs) and their effect on system-level safety.



[3] Leveson, N. and Thomas, J. (2018) STPA Handbook.

System Modeling: System-level Losses (L), Hazards (H) and Safety Constraints (SC)



L-1: Injury or loss of life of passengers or other road users.

L-2: Vehicle damage due to collision with objects.

L-3: Loss of vehicle connection.

L-4: Loss of mission.

L-5: Vehicle is stranded.

L-6: Loss of reputation.

H-1: Vehicle does not execute DDT correctly.

H-2: Vehicle suffers a safety-critical failure.

H-3: Vehicle breaches established ODD.

H-4: FOC does not intervene when required.

H-5: MOC clears the vehicle for operation incorrectly.

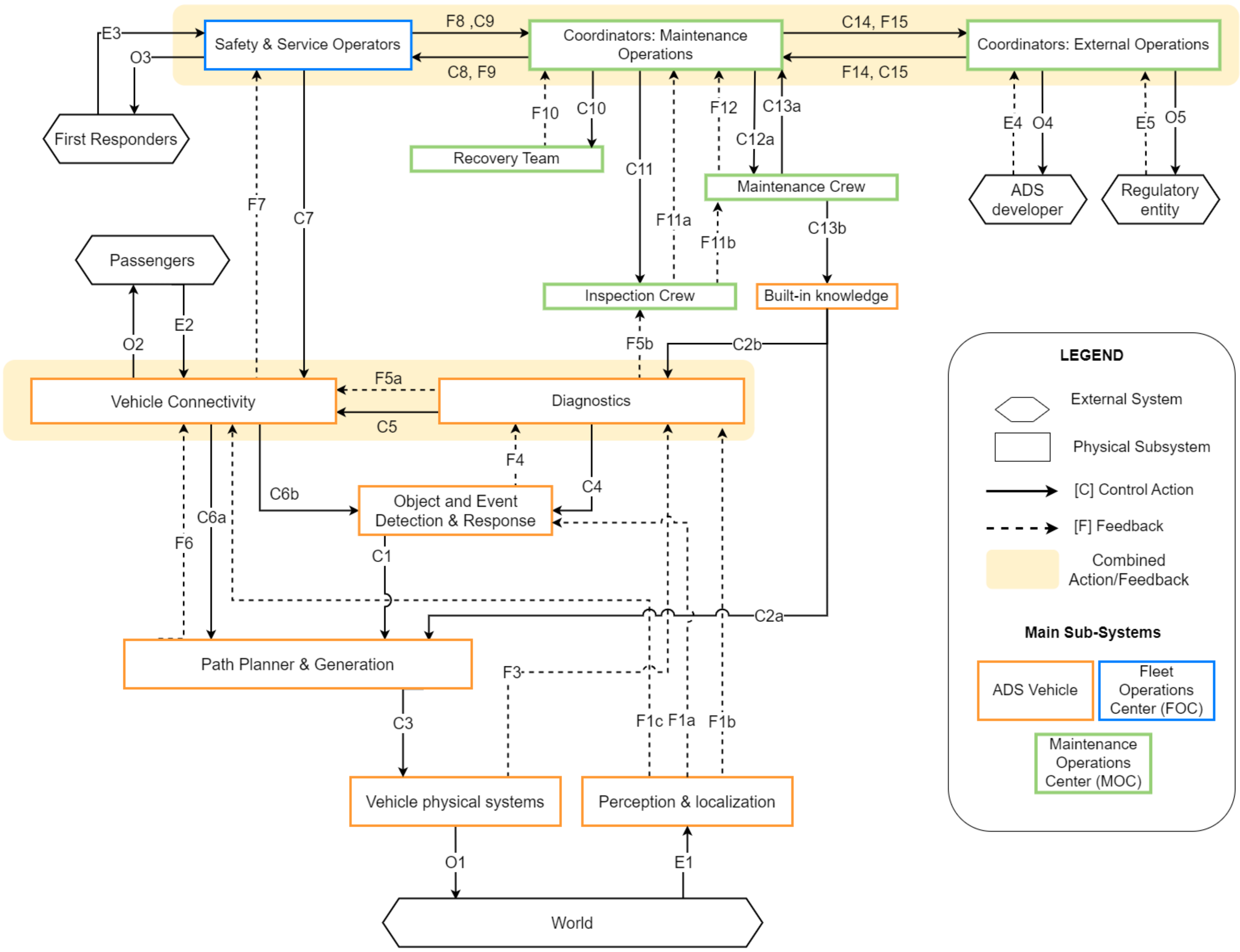
SC-1: Vehicle must execute DDT correctly under the conditions specified in the ODD.

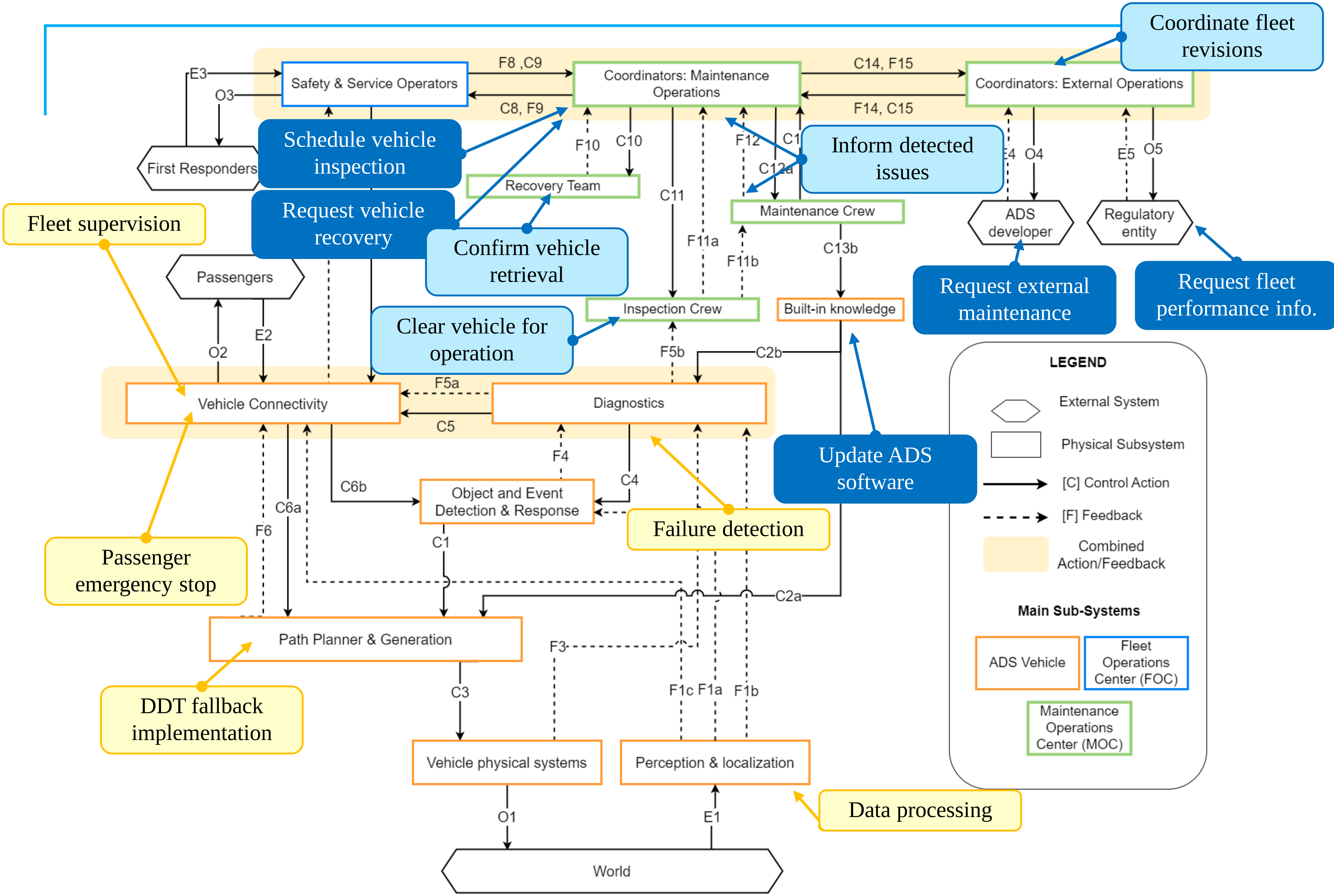
SC-2: Fleet operators must minimize the risk of safety-critical failures through adequate inspection and maintenance procedures

SC-3: Vehicle must implement adequate DDT procedures to remain within the specified ODD and perform DDT fallback strategies if necessary.

SC-4: Fleet operators must monitor and supervise the vehicle and intervene to support the vehicle operation.

SC-5: Fleet operators must establish maintenance and inspection procedures in coordination with the ADS developer and ensure these are followed.


E3
O3
Safety & Service Operators
F8 ,C9
C8, F9
Coordinators: Maintenance Operations
C14, F15
F14, C15
Coordinators: External Operations
First Responders
F10
C10
Recovery Team
C11
F12
C12a
C13a
Maintenance Crew
E4
O4
ADS developer
E5
O5
Regulatory entity
F7
C7
F11a
F11b
C13b
Passengers
E2
O2
Inspection Crew
Built-in knowledge
F5b
C2b
Vehicle Connectivity
F5a
C5
Diagnostics
F4
C4
C6b
Object and Event Detection & Response
C6a
F6
C1
C2a
Path Planner & Generation
F3
C3
F1c
F1a
F1b
Vehicle physical systems
Perception & localization
O1
E1
World
LEGEND
External System
Physical Subsystem
[C] Control Action
[F] Feedback
Combined Action/Feedback
Main Sub-Systems
ADS Vehicle
Fleet Operations Center (FOC)
Maintenance Operations Center (MOC)



Coordinate fleet revisions

Schedule vehicle inspection

Inform detected issues

Request vehicle recovery

Confirm vehicle retrieval

Fleet supervision

Request external maintenance

Request fleet performance info.

Clear vehicle for operation

Update ADS software

Failure detection

Passenger emergency stop

DDT fallback implementation

Data processing

Safety Hazards & Responsibilities

- High-level safety hazards characterized by over 75 different failure modes.
- The Maintenance Operations Center crew fail to:
  - ❑ Recover a missing vehicle.
  - ❑ Schedule inspection and maintenance activities.
  - ❑ Perform the inspection and maintenance correctly.
  - ❑ Follow vehicle clearance procedures.
  - ❑ Perform low-complexity maintenance.
  - ❑ Request external maintenance support.
  - ❑ Correctly implement operational procedure updates.
  - ❑ Report system anomalies to ADS developer.
  - ❑ Coordinate system updates with ADS developer.

To ensure operational safety human and organizational factors in procedure & system designed need to be addressed

Challenge to quantify effect of latent failures – but approach may provide good insight to design safety barriers.

Further discussion is needed on what will be required from the ADS developers – what information, training, or supervision will be provided to the fleet developers.

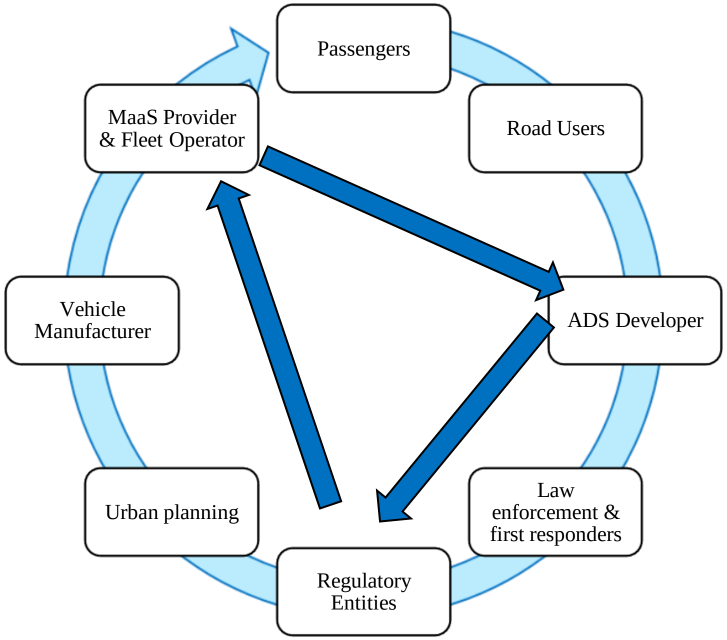
Summary & Conclusion

- Inspection & maintenance activities will play an important role in ADS fleet operations.
- Effective hazard identification methods are required to construct safe & robust system of systems.
- STPA provides focus to unintended consequences and emerging behaviors.
- Opportunities to leverage method to detect need for operational & maintenance procedures.

Next Steps and Future Work

Next steps:

- [*Under revision*] Development of comprehensive hazard identification methodology for complex socio-technical systems.
- The authors are conducting stakeholder validation activities in the context of Level 4 ADS Fleet Operations as Mobility as a Service.
- 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.



Expected impact:

- Model interactions between ADS-equipped vehicle and human operators to ensure operational safety.
- Inform of key responsibilities and risk mitigation activities of fleet operators.

The B. John Garrick Institute for the Risk Sciences
UCLA ENGINEERING

An STPA-based analysis of Automated Driving Systems fleet maintenance activities

Camila Correa-Julian, MSc*, ccorreaj@ucla.edu

Marilia A. Ramos, PhD; Ali Mosleh, PhD; Jiaqi Ma, PhD.

The B. John Garrick Institute for the Risk Sciences, University of California Los Angeles

RAMS 2024