B. John Garrick Institute for the Risk Sciences

UCLA ENGINEERING

UCLA

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

Center for Reliability Engineering
The B. John Garrick Institute for the Risk Sciences
UCLA

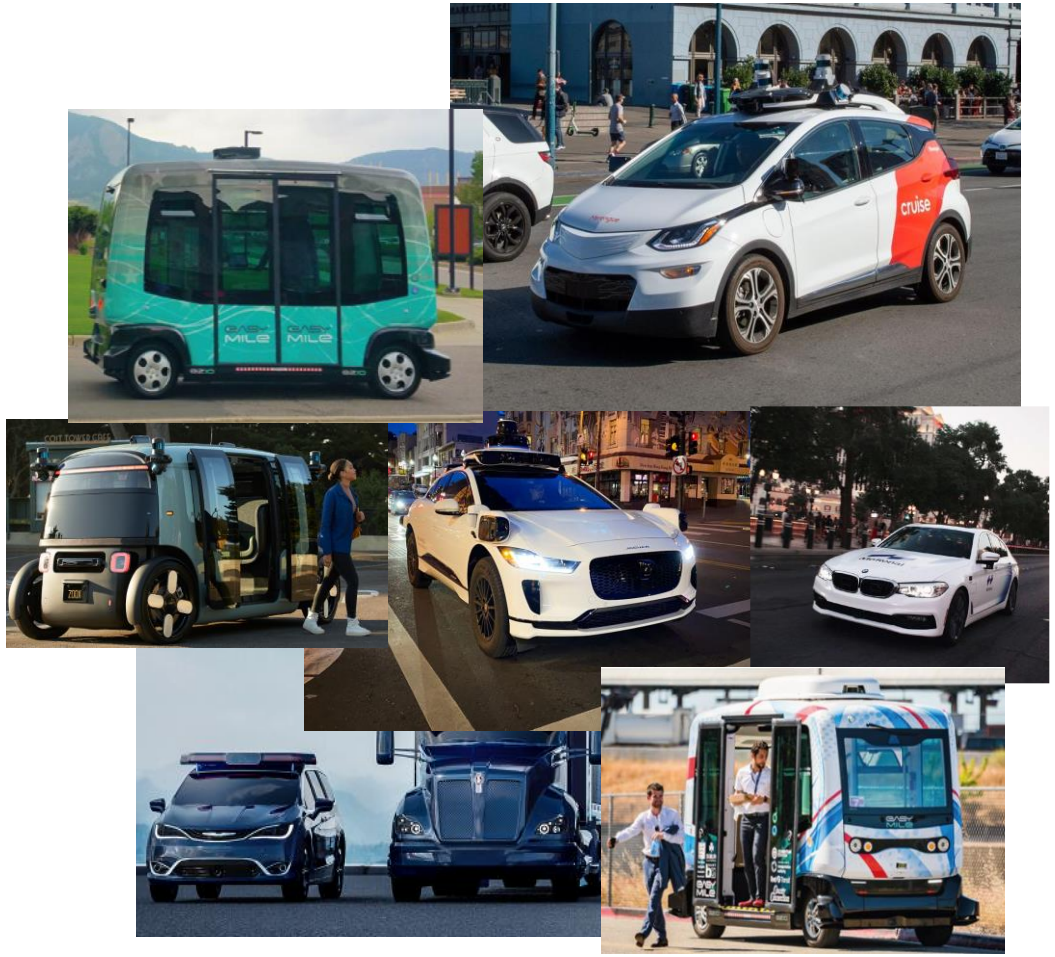
Camila Correa-Jullian*, John McCullough, Marilia Ramos, Ali Mosleh, Jiaqi Ma

2023 European Conference on Safety and Reliability 3rd – 7th September 2023, Southampton, UK

UCLA

Research Context

- Waymo, Cruise & Zoox are some companies involved in Mobility as a Service (MaaS) in the US.
- **Near-medium future**: Fleet operator's role 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.
- **Operational Safety aspects of Maintenance & Inspection activities are usually overlooked.**
- 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.



[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".

[4] 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 modelling.

UCLA

Research Context

- Waymo, Cruise & Zoox are some companies involved in Mobility as a Service (MaaS) in the US.
- **Near-medium future**: Fleet operator's role 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.
- **Operational Safety aspects of Maintenance & Inspection activities are usually overlooked.**
- 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.

Funded by the National Highway Traffic Safety Administration (NHTSA).

- In collaboration with Transportation Research Center (TRC) & ToXcel.
- Recommendations on fleet operators' risk mitigation activities.

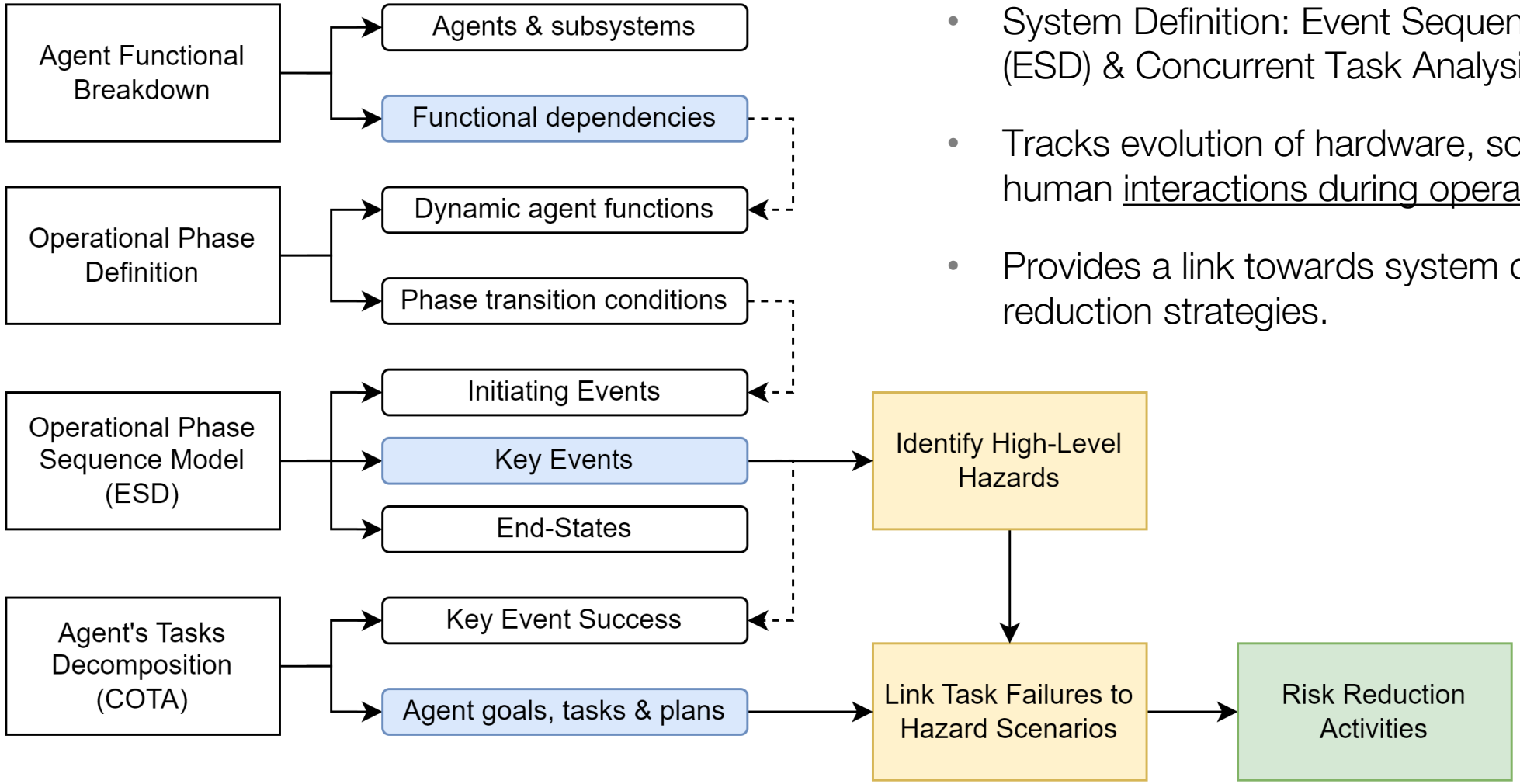
Structured approach to design inspection and maintenance operations – define tasks, responsibilities and resources required.

[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".

[4] 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 modelling.

UCLA

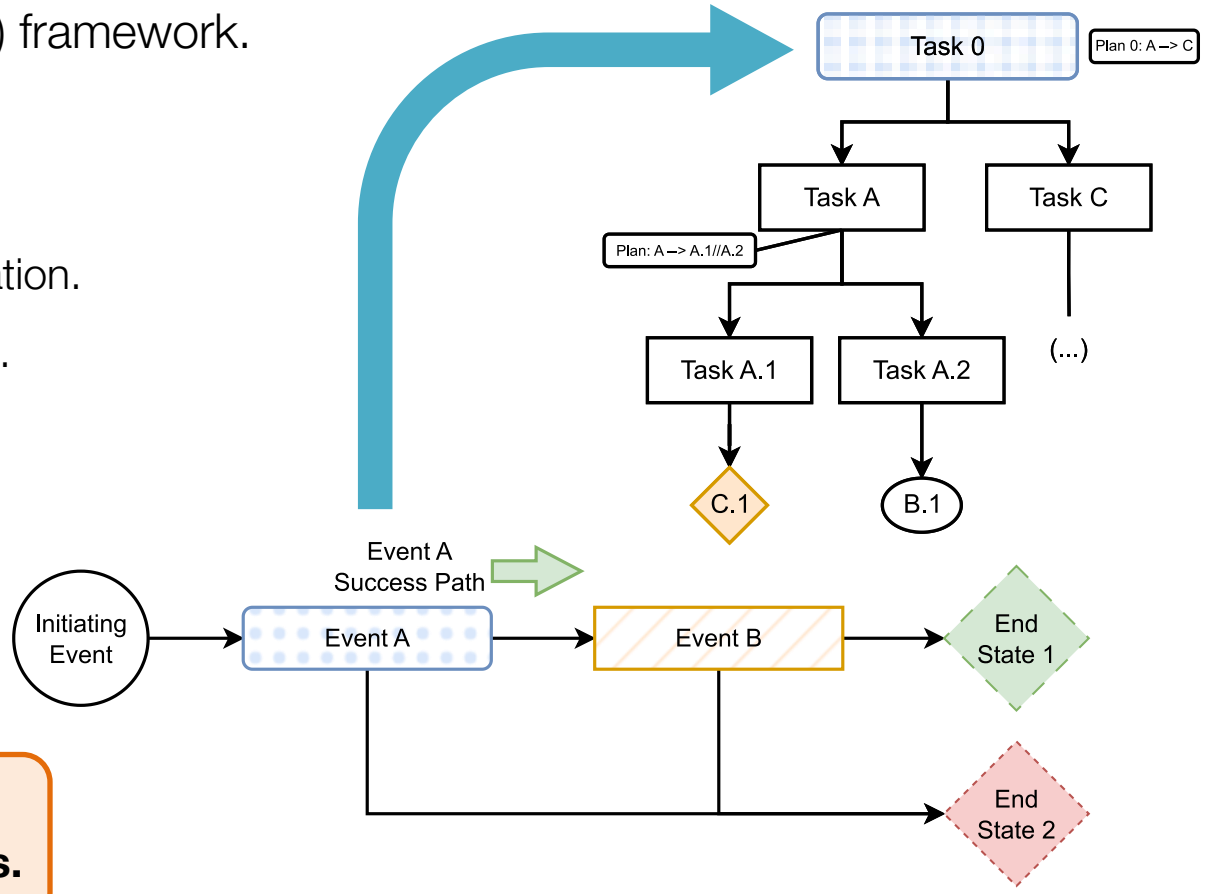
Modeling Approach



- System Definition: Event Sequence Diagrams (ESD) & Concurrent Task Analysis (CoTA)
- Tracks evolution of hardware, software, and human interactions during operation.
- Provides a link towards system design and risk reduction strategies.

Task Decomposition by **Information, Decision, and Action** Cognitive Model

- Human-System Interaction in Autonomy (H-SIA) framework.
- Task decomposition rules follow IDA:
  - Information reception and preprocessing.
  - Diagnosis, decision making and solution formulation.
  - Action execution process implementing the plan.
- Identify resources needed to perform tasks:
  - Information is transmission and presentation.
  - Agent's previous knowledge.
  - Mechanisms needed to perform the actions.



Task failures linked to errors in I-D-A stages due to absence or failures of elements **supporting the agents.**

[5] Ramos, M. A., Thieme, C. A., Utne, I. B., & Mosleh, A. (2020b). A generic approach to analysing failures in human – System interaction in autonomy.

Fleet Operations: Modeling Dynamic Phases

UCLA

ADS Vehicle

- DDT, mobility service, self-diagnostics, communication.

Fleet Operations Center

- Dispatching, passenger support, safety, post-incident procedures.

Maintenance Operations Center

- Inspection and maintenance, reporting to external parties.

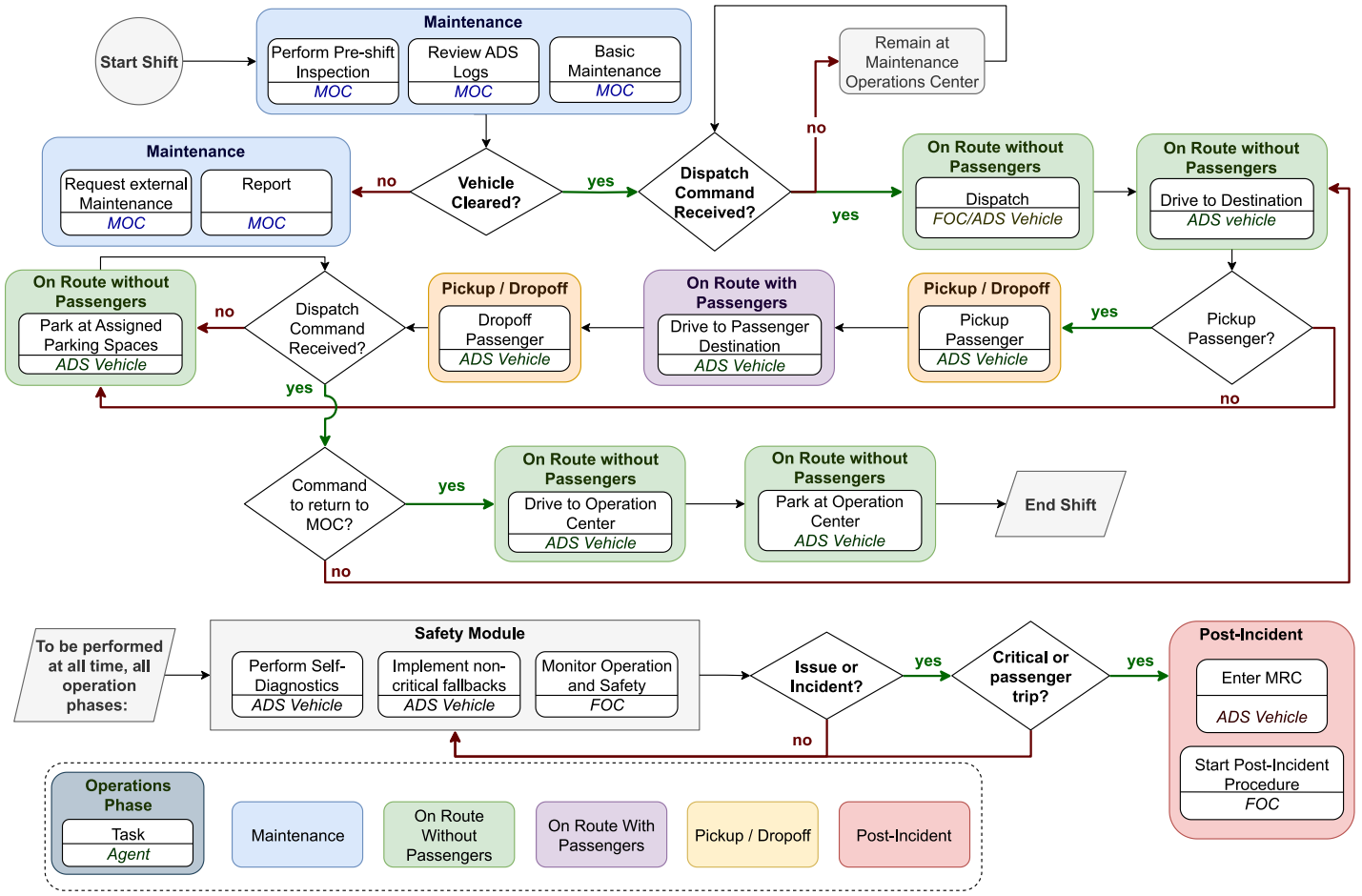
Inspection / Maintenance

On Route Without Passengers

On Route With Passengers

Pickup / Dropoff

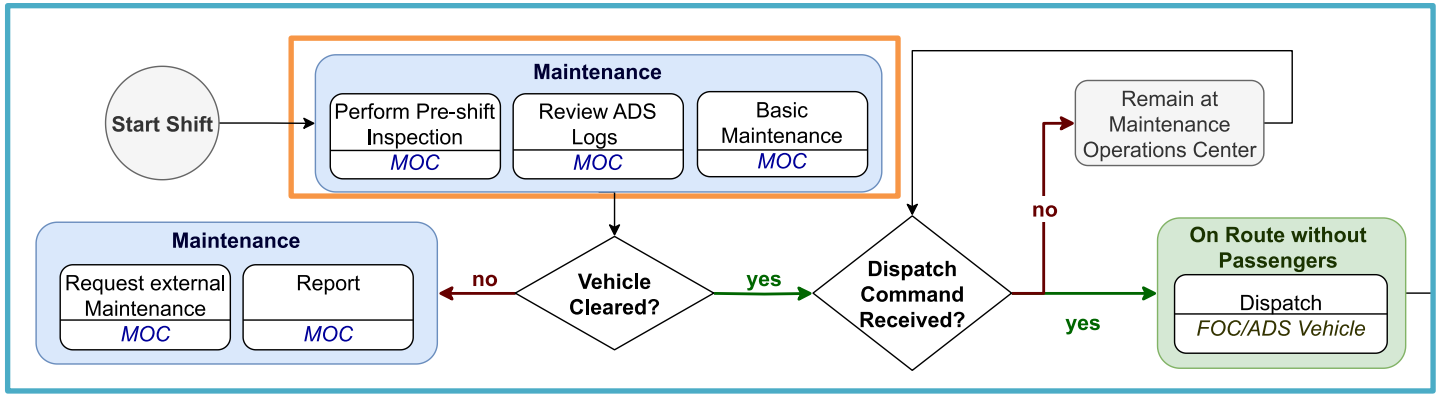
Post-Incident



Fleet Operations: Inspection & Maintenance

Inspection / Maintenance

- Performed by Maintenance Operation Center



Pre-shift Inspection

- Use of safety checklists
- Review of ADS diagnostic logs
- Frequency specified by ADS developer
- Anomalies are reported for further investigation

Low-complexity maintenance

- MOC only performs low-complexity maintenance procedures
- Complex repairs are coordinated with ADS developer

Service Maintenance

- Use of safety checklists to check for long-term degradation
- Frequency specified by ADS developer

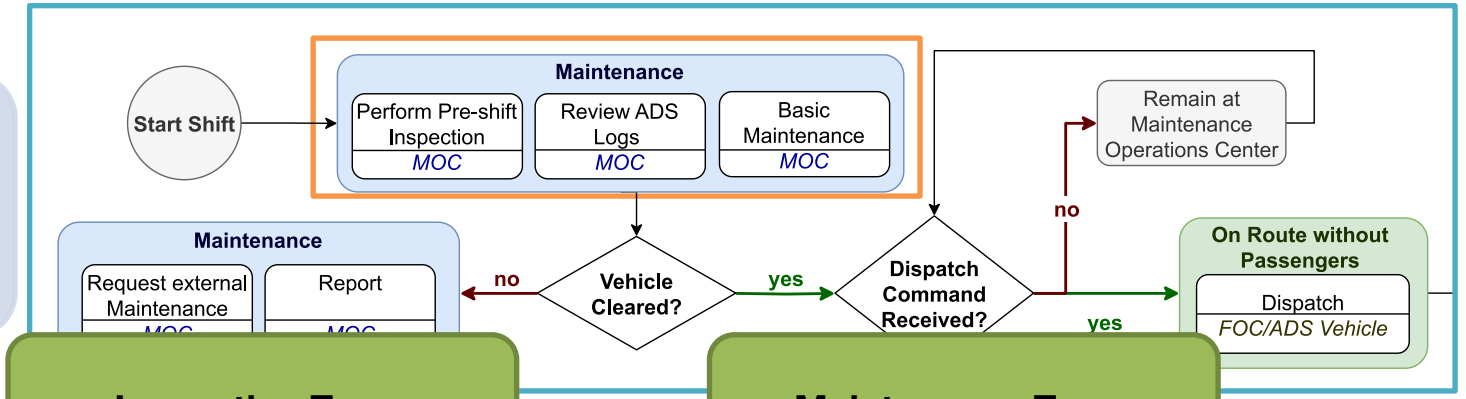
System Updates

- System software updates, instrument calibration and related activities are coordinated with ADS developer

Fleet Operations: Inspection & Maintenance

Inspection / Maintenance

- Performed by Maintenance Operation Center



Coordinator Team

Pre-shift Inspection

- Use of safety checklists
- Review of ADS diagnostic logs
- Frequency specified by ADS developer
- Anomalies are reported for further investigation

Low-complexity maintenance

- MOC only performs low-complexity maintenance procedures
- Complex repairs are coordinated with ADS developer

Inspection Team

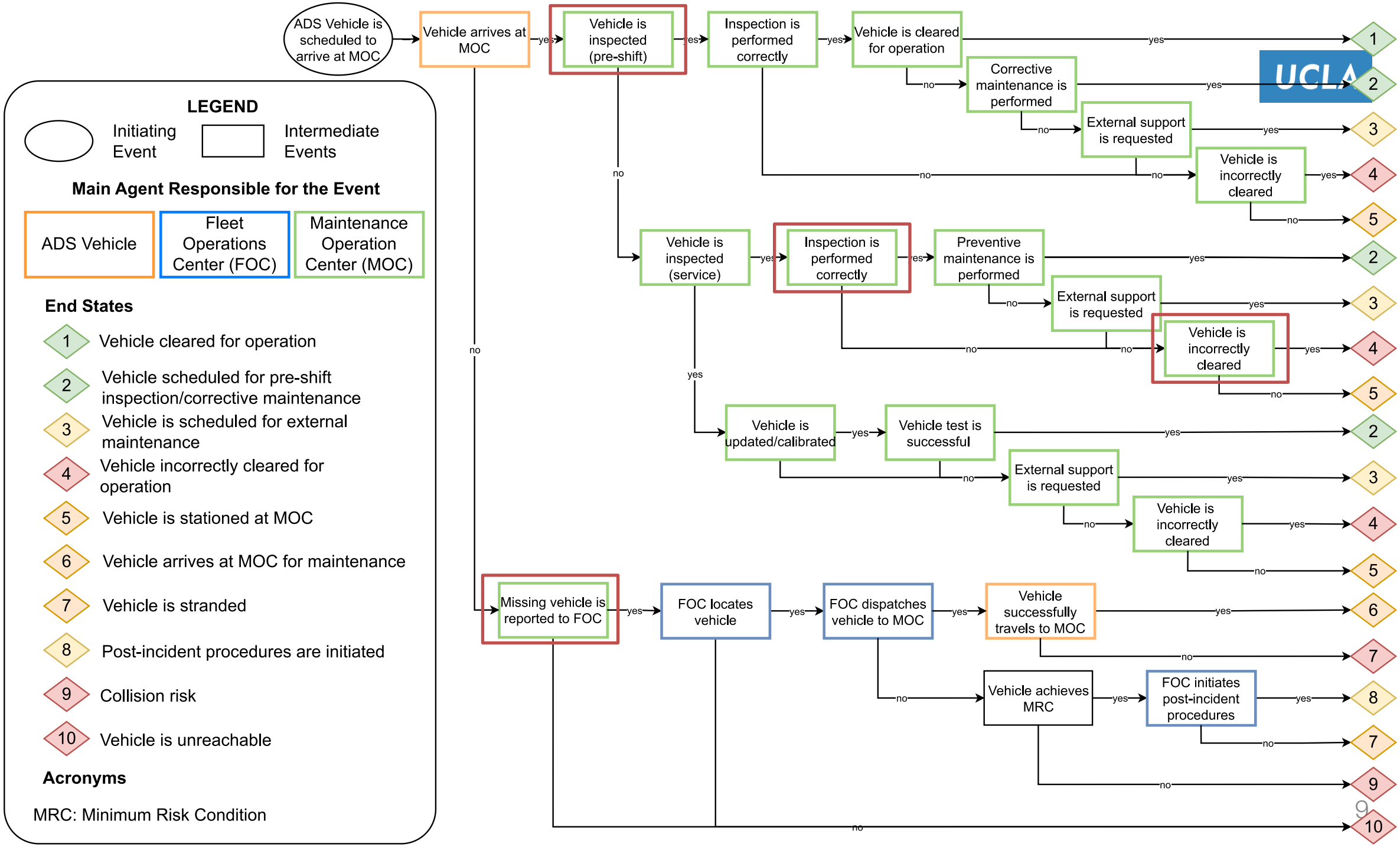
Maintenance Team

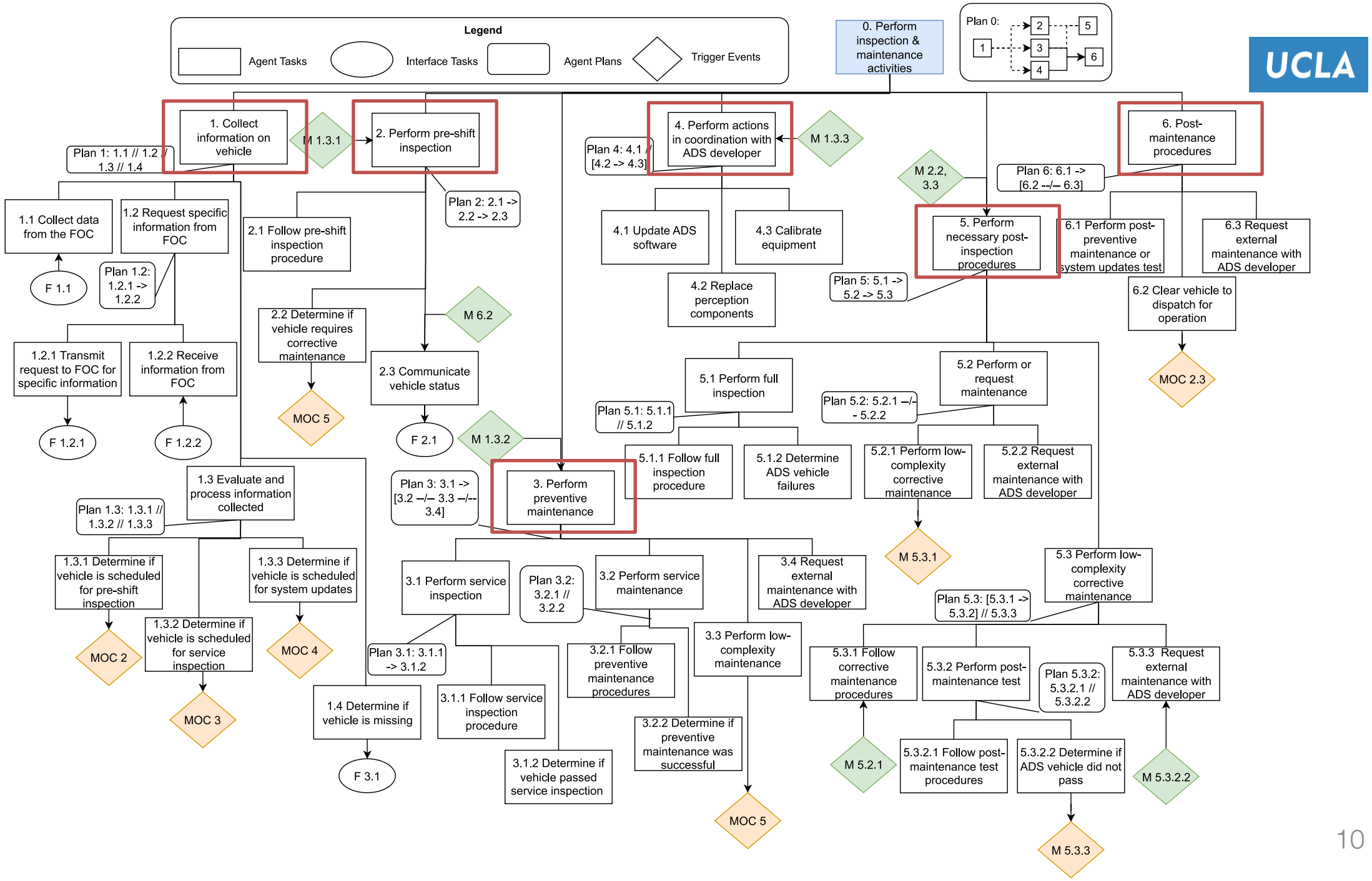
Service Maintenance

- Use of safety checklists to check for long-term degradation
- Frequency specified by ADS developer

System Updates

- System software updates, instrument calibration and related activities are coordinated with ADS developer


ADS Vehicle is scheduled to arrive at MOC
Vehicle arrives at MOC
Vehicle is inspected (pre-shift)
Inspection is performed correctly
Vehicle is cleared for operation
Corrective maintenance is performed
External support is requested
Vehicle is incorrectly cleared
Vehicle is inspected (service)
Inspection is performed correctly
Preventive maintenance is performed
External support is requested
Vehicle is incorrectly cleared
Vehicle is updated/calibrated
Vehicle test is successful
External support is requested
Vehicle is incorrectly cleared
Missing vehicle is reported to FOC
FOC locates vehicle
FOC dispatches vehicle to MOC
Vehicle successfully travels to MOC
Vehicle achieves MRC
FOC initiates post-incident procedures
yes
no
1
2
3
4
5
6
7
8
9
10
LEGEND
Initiating Event
Intermediate Events
Main Agent Responsible for the Event
ADS Vehicle
Fleet Operations Center (FOC)
Maintenance Operation Center (MOC)
End States
1 Vehicle cleared for operation
2 Vehicle scheduled for pre-shift inspection/corrective maintenance
3 Vehicle is scheduled for external maintenance
4 Vehicle incorrectly cleared for operation
5 Vehicle is stationed at MOC
6 Vehicle arrives at MOC for maintenance
7 Vehicle is stranded
8 Post-incident procedures are initiated
9 Collision risk
10 Vehicle is unreachable
Acronyms
MRC: Minimum Risk Condition


Legend
Agent Tasks
Interface Tasks
Agent Plans
Trigger Events
0. Perform inspection & maintenance activities
Plan 0:
1. Collect information on vehicle
M 1.3.1
2. Perform pre-shift inspection
Plan 1: 1.1 // 1.2 // 1.3 // 1.4
Plan 2: 2.1 -> 2.2 -> 2.3
4. Perform actions in coordination with ADS developer
M 1.3.3
Plan 4: 4.1 // [4.2 -> 4.3]
M 2.2, 3.3
6. Post-maintenance procedures
Plan 6: 6.1 -> [6.2 --/-- 6.3]
1.1 Collect data from the FOC
1.2 Request specific information from FOC
F 1.1
Plan 1.2: 1.2.1 -> 1.2.2
2.1 Follow pre-shift inspection procedure
4.1 Update ADS software
4.3 Calibrate equipment
4.2 Replace perception components
5. Perform necessary post-inspection procedures
6.1 Perform post-preventive maintenance or system updates test
6.3 Request external maintenance with ADS developer
Plan 5: 5.1 -> 5.2 -> 5.3
6.2 Clear vehicle to dispatch for operation
MOC 2.3
1.2.1 Transmit request to FOC for specific information
1.2.2 Receive information from FOC
F 1.2.1
F 1.2.2
2.2 Determine if vehicle requires corrective maintenance
M 6.2
MOC 5
2.3 Communicate vehicle status
F 2.1
M 1.3.2
5.1 Perform full inspection
5.2 Perform or request maintenance
Plan 5.1: 5.1.1 // 5.1.2
Plan 5.2: 5.2.1 --/-- 5.2.2
5.1.1 Follow full inspection procedure
5.1.2 Determine ADS vehicle failures
5.2.1 Perform low-complexity corrective maintenance
5.2.2 Request external maintenance with ADS developer
1.3 Evaluate and process information collected
Plan 3: 3.1 -> [3.2 --/-- 3.3 --/-- 3.4]
3. Perform preventive maintenance
Plan 1.3: 1.3.1 // 1.3.2 // 1.3.3
M 5.3.1
5.3 Perform low-complexity corrective maintenance
1.3.1 Determine if vehicle is scheduled for pre-shift inspection
1.3.3 Determine if vehicle is scheduled for system updates
3.1 Perform service inspection
Plan 3.2: 3.2.1 // 3.2.2
3.2 Perform service maintenance
3.4 Request external maintenance with ADS developer
Plan 5.3: [5.3.1 -> 5.3.2] // 5.3.3
MOC 2
1.3.2 Determine if vehicle is scheduled for service inspection
MOC 4
Plan 3.1: 3.1.1 -> 3.1.2
3.2.1 Follow preventive maintenance procedures
3.3 Perform low-complexity maintenance
5.3.1 Follow corrective maintenance procedures
5.3.2 Perform post-maintenance test
Plan 5.3.2: 5.3.2.1 // 5.3.2.2
5.3.3 Request external maintenance with ADS developer
MOC 3
1.4 Determine if vehicle is missing
3.1.1 Follow service inspection procedure
3.2.2 Determine if preventive maintenance was successful
M 5.2.1
5.3.2.1 Follow post-maintenance test procedures
5.3.2.2 Determine if ADS vehicle did not pass
M 5.3.2.2
F 3.1
3.1.2 Determine if vehicle passed service inspection
MOC 5
M 5.3.3

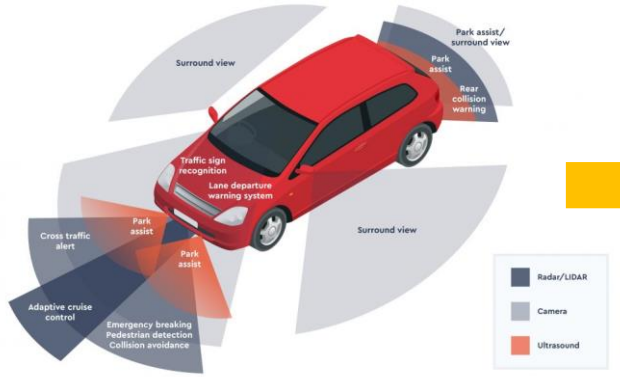
Placing Crew's Tasks in Perspective: ADS-vehicle failures during operation

UCLA

Crew's Key Event Failures:

- Report a missing vehicle.
- Inspect the vehicle (pre-shift/service).
- Perform the inspection correctly.
- Follow vehicle clearance procedures.
- Perform corrective maintenance.
- Perform preventive maintenance.
- Schedule external maintenance.
- Correctly perform system updates.

Task	Task Description	High-level risk contributors
1	Data Collection & Processing.	ADS sensor hardware, ADS software
2	Perform Dynamic Driving Tasks (DDT).	ADS software, ADS vehicle control.
3	DDT Fallback Monitoring.	ADS software
4	DDT Fallback Planning & Implementation.	ADS software, vehicle control
5	Communication Management (FOC, Passengers)	ADS connectivity, ADS sensor hardware
6	Real-time Diagnostics	ADS sensor hardware, ADS diagnostic software



Placing Crew's Tasks in Perspective: ADS-vehicle failures during operation

UCLA

Crew's Key Event Failures:

- Report a missing vehicle.
- Inspect the vehicle (pre-shift/service).
- Perform the inspection correctly.
- Follow vehicle clearance procedures.
- Perform corrective maintenance.
- Perform preventive maintenance.
- Schedule external maintenance.
- Correctly perform system updates.

Task	Task Description	High-level risk contributors
1	Data Collection & Processing.	ADS sensor hardware, ADS software
2	Perform Dynamic Driving Tasks (DDT).	ADS software, ADS vehicle control.
3	DDT Fallback Monitoring.	ADS software
4	DDT Fallback Planning & Implementation.	ADS software, vehicle control
5	Communication Management (FOC, Passengers)	ADS connectivity, ADS sensor hardware
6	Real-time Diagnostics	ADS sensor hardware, ADS diagnostic software

Risk Contributors

Failure Modes

Agent Responsible

Agent's Responsibility

Agent Responsibilities & Resources Required

UCLA

Coordinator Crew	Inspection Crew	Maintenance Crew
•Follow the provided activity schedule. •Manage arriving ADS vehicles. •Report if any vehicle has not arrived on schedule. •Collect relevant information about the vehicle. •Instruct MOC crew of procedures and updates from the ADS developers.	• Follow the established procedure to perform pre-shift and service inspection activities. • Interpret diagnostic logs and report anomalous system behavior. • Follow vehicle clearance procedures or transfer it to the maintenance crew.	• Follow the established procedure to perform low-complexity maintenance actions. • Follow the established procedure to perform system updates or instrumentation calibration. • Request external maintenance support to the ADS developer.

- Derive requirements to perform tasks:

Training | Tools | Procedures | Workplace adequacy

UCLA

Key Findings

- Reliability limitations addressed by MOC crew & ADS developer guidelines.
  - Frequency & quality of inspections and preventive maintenance activities.
  - Account for varying detectability of multiple failures.

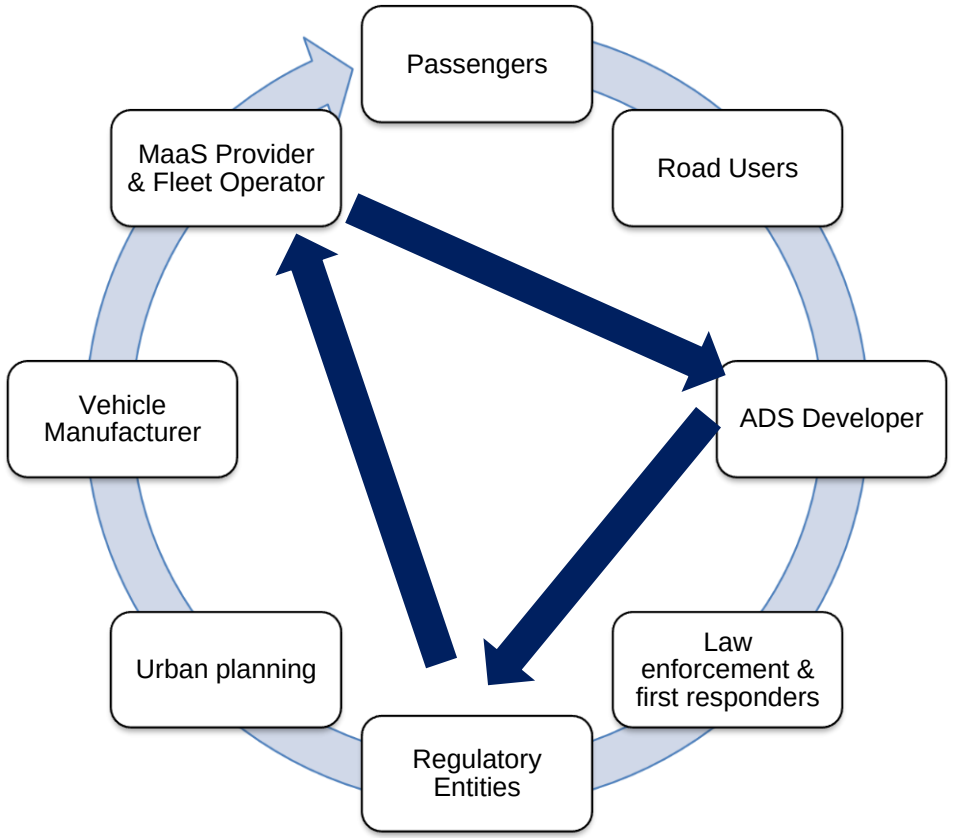
- The approach presented based on CoTA can be helpful to ensure all safety responsibilities address the identified safety hazards.
  - Can be used to assess if the necessary and sufficient tools are available for the agents to perform each I-D-A step associated with their tasks.
  - Highlights the dependencies between different agent's tasks for the success of overall system goals.

Human and organizational factors play a key role in automated system operations.

There is a need to study the complex interactions and emerging behaviors in ADS operation from an operational safety perspective (not only functional safety)

A limited knowledge of the fleet operators on the ADS would imply the need for a more active participation of the ADS developer.

Next Steps



Current stage:

- [Article under review] Development of comprehensive hazard identification methodology for complex socio-technical systems.
- [Under NHTSA review] The final report includes safety-related recommendations and the result from stakeholder validation activities.
  - 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.

Next steps:

- Extend analysis to on-board drivers interacting with vehicles equipped with high-level automated capabilities.
- Cognitive modeling of team interactions between ADS vehicles, remote operators, and on-board drivers.
- Conduct driving simulator & control room experiments to support & inform the team model.

B. John Garrick Institute for the Risk Sciences

UCLA ENGINEERING

UCLA

Thank you!

Center for Reliability Engineering
The B. John Garrick Institute for the Risk Sciences
UCLA

Camila Correa-Jullian*, John McCullough, Marilia Ramos, Ali Mosleh, Jiaqi Ma

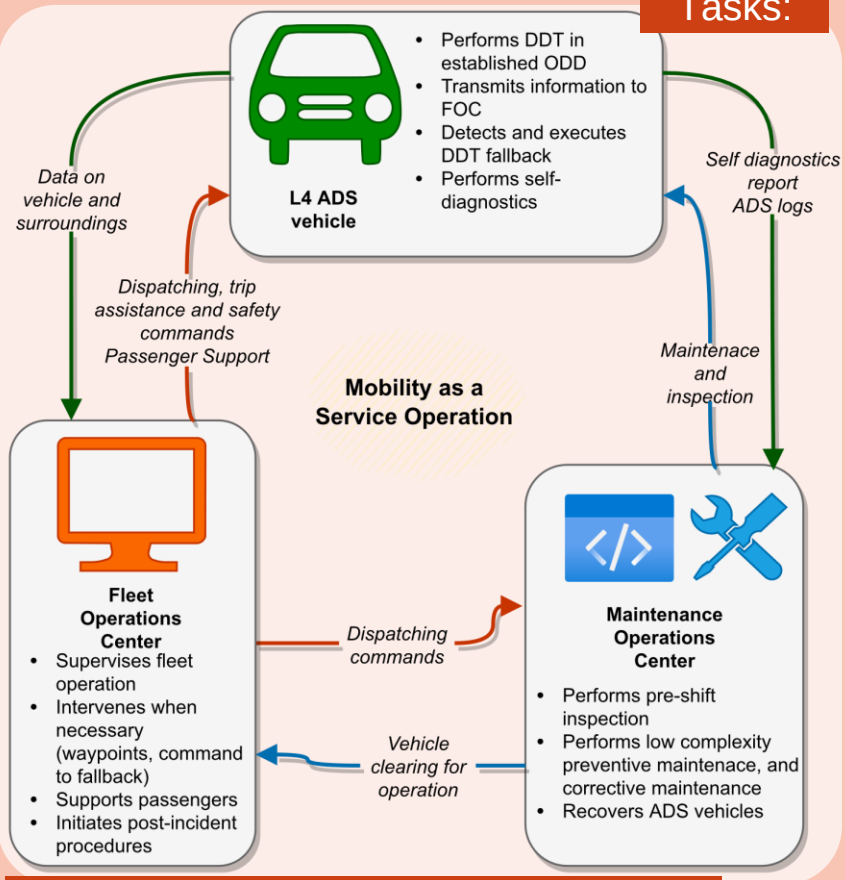
*ccorreaj@ucla.edu

2023 European Conference on Safety and Reliability 3rd – 7th September 2023, Southampton, UK

Overview of Operational Safety Concepts for Level 4 ADS Fleets

UCLA

Objective: Identify safety risks associated with **Level 4 ADS Mobility as a Service (MaaS) operations** and the responsibilities and activities (i.e., policies, procedures, and strategies) of the **fleet operator** to mitigate such risks.



2 "Reference" Fleet & Operational Phases Definition

3 Safety Risk Analysis of Reference Fleet

***What** may happen?*
***Who** is responsible?*
***How** can it happen?*
***Why** can it happen?*

4 Identification of Operational Safety Responsibilities

5 Review of Relevant Best Practices

***How** can it be **avoided** or how can its consequences be **mitigated**?*

Current stage:

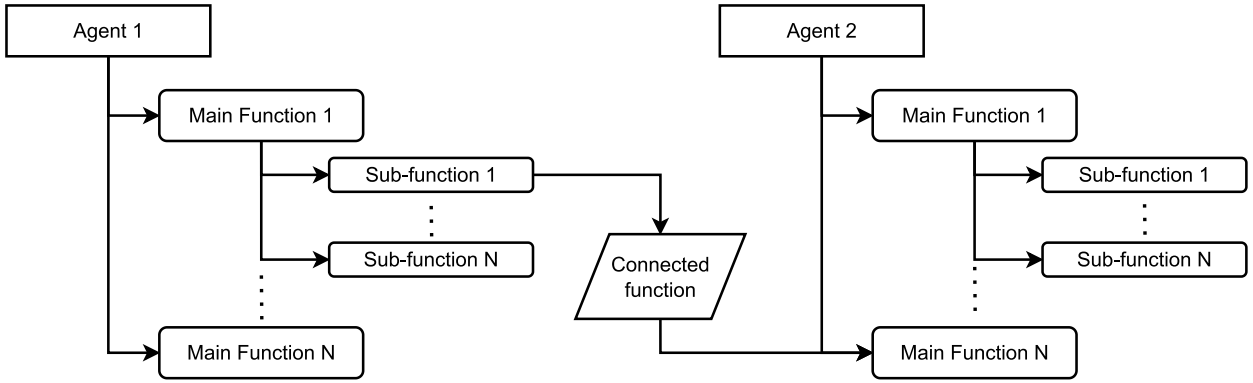
6 Development and assessment of risk mitigation activities for fleet operators

Principle Focus:

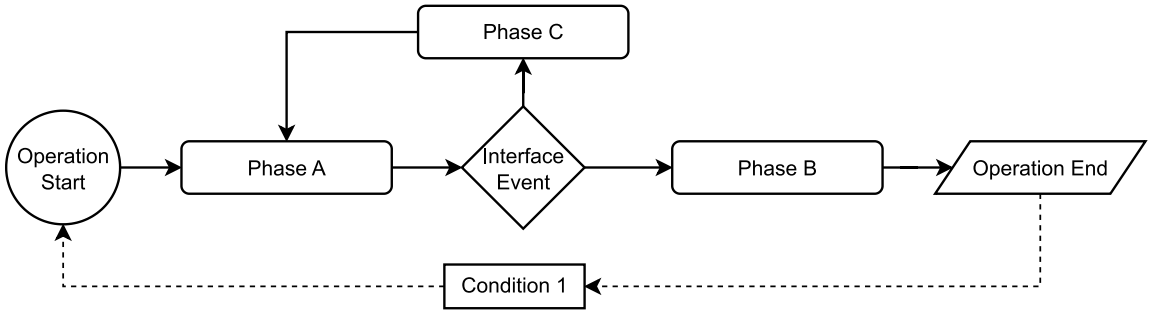
- Operator training & workplace adequacy.
- Incident management and investigation.
- Pre-shift inspection & maintenance activities.

System & Agent Definition

- **Agent Functional Breakdown**
  - Define relevant agents.
  - Breakdown functions.
  - Identify dependencies.
- **Operational Phase Definition**
  - Application-specific.
  - Functions can vary depending on stages or pre-existing conditions.
  - Define agent's objectives.
  - Define phase transition conditions.



Agent Functional Breakdown

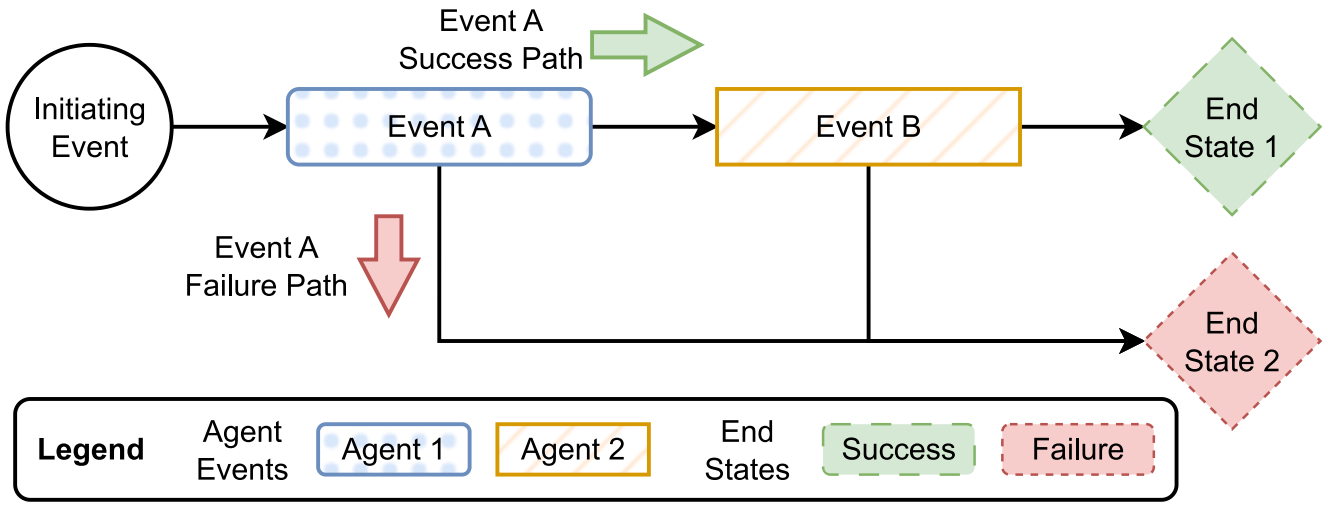


Operational Phase Definition

UCLA

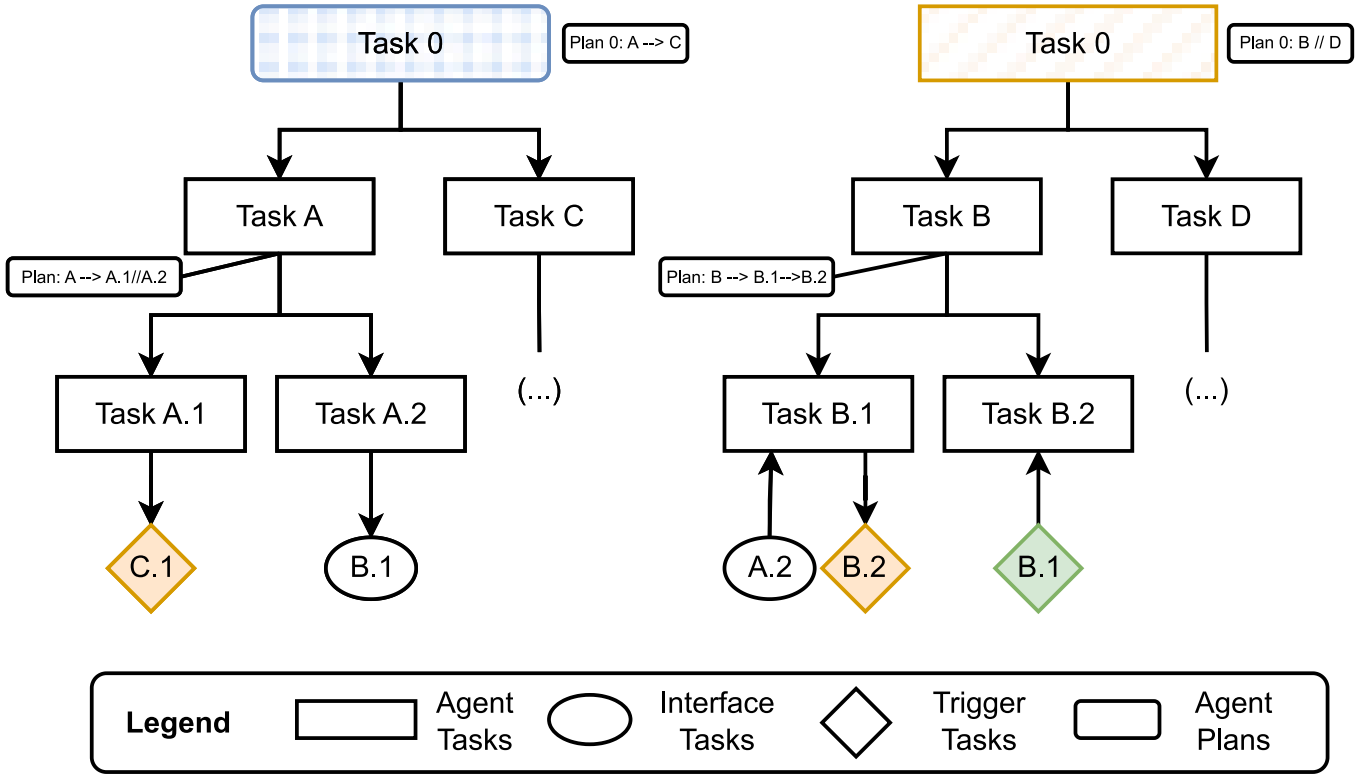
Operational Phase Modeling through Event Sequence Diagrams

- Sequence of pivotal events stemming from a common **initiating events** and leading to multiple **end-states**.
- Quantification of outcome's frequency based on event probabilities and initiating event's frequency.
- Each event is associated with a major agent function success/failure or to external events.



Modeling Agents through Concurrent Task Analysis

- Human-System Interaction in Autonomy (H-SIA) framework.
- Success of each ESD event explained through goals, tasks, and plans.
- Task decomposition relies on Information, Decision, and Action (IDA) cognitive phases.
- Task categories: sequential, parallel, trigger, and interface.



[5] Ramos, M. A., Thieme, C. A., Utne, I. B., & Mosleh, A. (2020b). A generic approach to analysing failures in human – System interaction in autonomy.