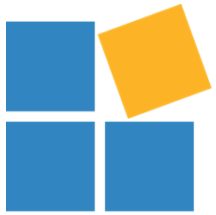


B. John Garrick Institute for the Risk Sciences

UCLA ENGINEERING

UCLA

Safety Hazard Identification for Autonomous Driving Systems Fleet Operations 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*, Jiaqi Ma, Enrique Lopez Droguett, Ali Mosleh

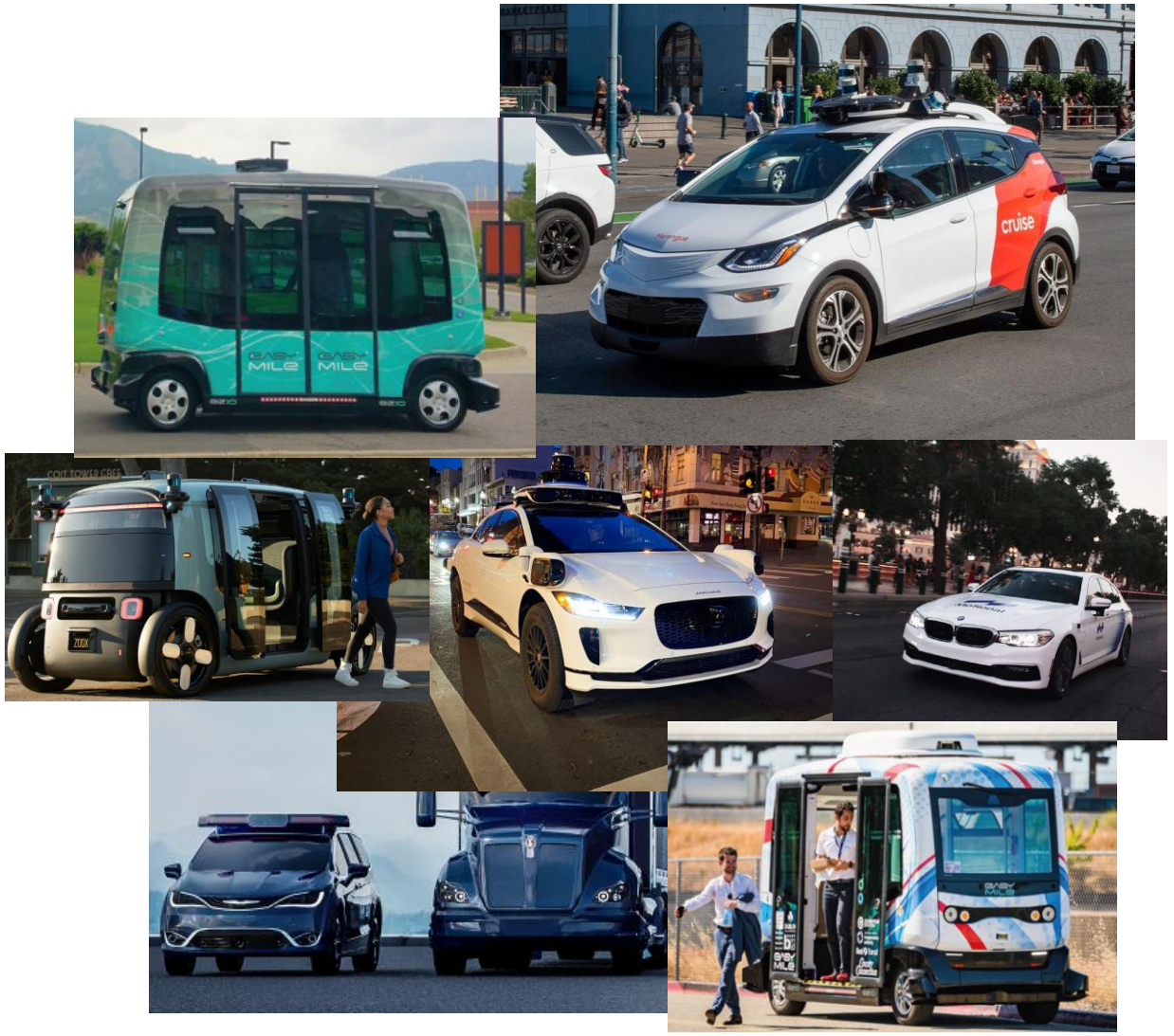
Probabilistic Safety Assessment and Management PSAM 16, June 26-July 1, 2022, Honolulu, Hawaii

UCLA

Research Context

"Automated Driving Systems (ADS) offer the potential to reduce crash-related deaths and injuries, improve access to transportation, reduce traffic congestion and emissions, and improve productivity and quality of life for millions of people."

--National Highway Traffic and Safety Administration (NHTSA, 2021)



- 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, Lyft, Uber, Motional, EasyMile, Navya 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".

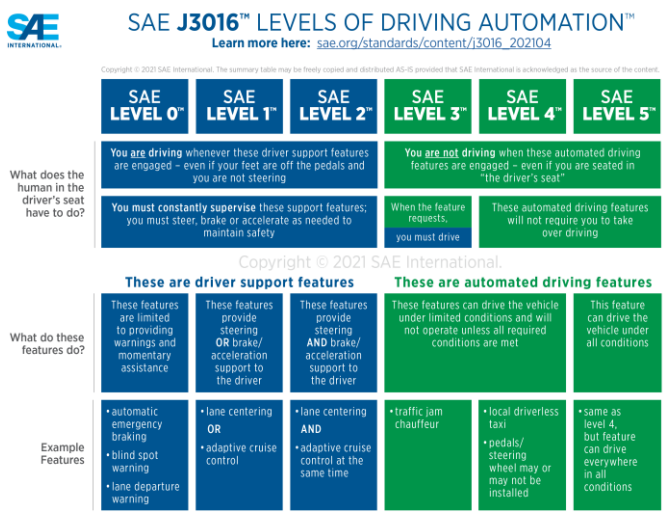
L4 ADS: High Driving Automation

UCLA

- SAE J3016: “The ***sustained*** and ***ODD***-specific performance by an ***ADS*** of the entire ***DDT*** and ***DDT fallback*** […] as well as achieving a ***minimal risk condition*** […]”

- Safety-related tasks:
  1. Enforce the ODD through self-diagnostic systems.
  2. Perform safety-adequate DDTs relying on real-time conditions.
  3. achieve a Minimal Risk Condition (MRC) when required.

- Key Terms:
  - Operational Design Domain (ODD)
  - Dynamic Driving Task (DDT)
  - Minimal Risk Condition (MRC)

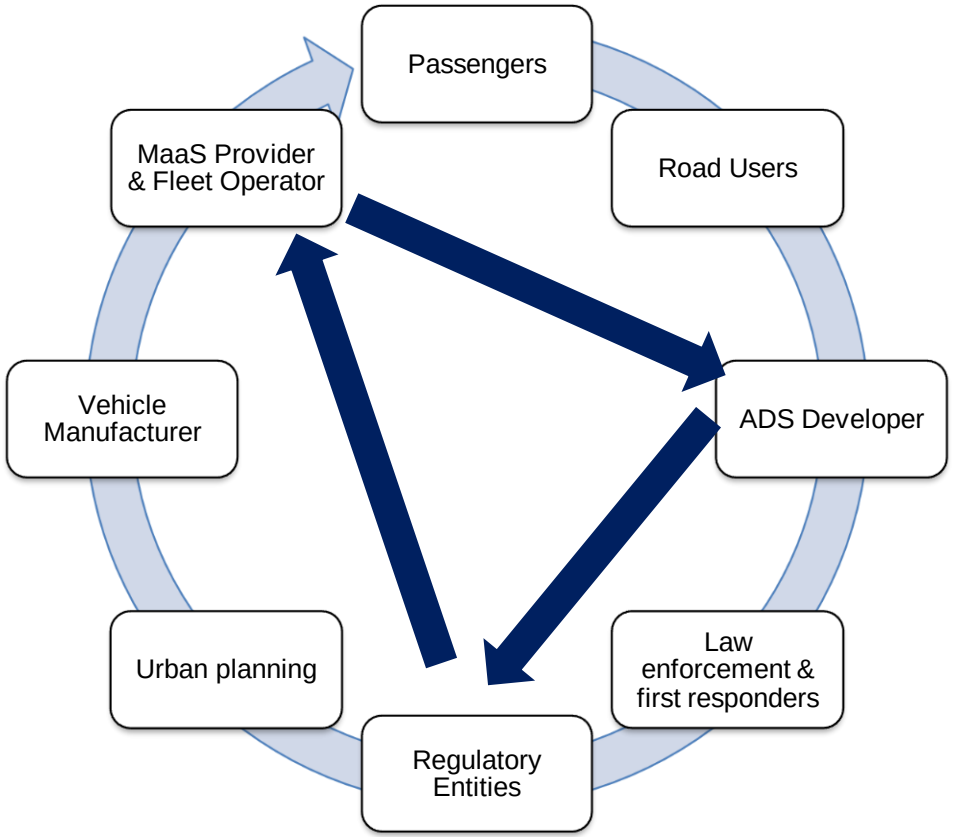


How does this translate into the Mobility as a Service context?

[3] SAE J3016_202104, Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, Available [online]: https://www.sae.org/standards/content/j3016_202104/

UCLA

Multiple actors involved in L4 ADS Fleet Operations for MaaS



- Road testing and commercial ride-hailing of L4 ADS with no safety driver are already legal in certain areas.
- Now: ADS developers build their own vehicles or closely work with vehicle manufacturers and service providers.
- Future: Fleet operators are expected to work with single or multiple ADS developers & vehicle manufacturers.
- **No clear path** for regulatory entities to address **who** is responsible for avoiding incidents.

[4] CPUC Issues First Driverless Autonomous Vehicle Passenger Service Deployment Permit. June 02, 2022.
https://www.cpuc.ca.gov/news-and-updates/all-news/cpuc-issues-first-driverless-autonomous-vehicle-passenger-service-deployment-permit

Goal: Identify safety risks associated with **L4 ADS MaaS operations** and the responsibilities of the **fleet operator** to mitigate such risks.

UCLA

Definition of “Reference Fleet”

Explore operational scenarios to support hazard identification

Model operational scenarios

- Limited operational data available
  - Model interactions between agents to determine what data requirements exist to quantify risk.
- Business relationship between ADS developer & fleet operator may vary
  - Fleet operator is independent agent.
  - Procured vehicles from an ADS developer and manufacturer.
- New definitions required
  - Stopped Stable Condition (SSC)
  - Minimal Risk DDT (MR-DDT)

Goal: Identify safety risks associated with **L4 ADS MaaS operations** and the responsibilities of the **fleet operator** to mitigate such risks.

Definition of "Reference Fleet"

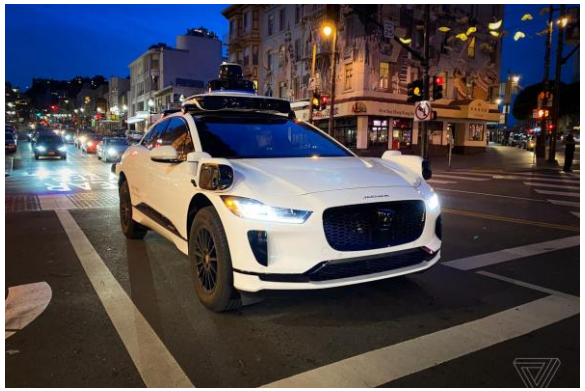
Explore operational scenarios to support hazard identification

Model operational scenarios

Assumptions:

- Light-duty passenger vehicles.
- No safety driver.
- Urban environments MaaS.
- Fleet operator must ensure the safe operation of the fleet.
- ADS developer specifies technical requirements for safe operation.
- The fleet operator may establish or operate within a more restrictive ODD.

Cruise vehicle based on Chevy Bolt model



Waymo vehicle based on Chrysler Pacifica Hybrid Minivan model

[5] E. Thorn, S. Kimmel, and M. Chaka, "A Framework for Automated Driving System Testable Cases and Scenarios," 2018.
[6] M. Chaka *et al.*, "FMVSS Considerations for Vehicles With Automated Driving Systems: Volume 2," vol. 1, no. April, p. 630p, 2021.

Reference Fleet System Breakdown

UCLA

ADS Vehicle

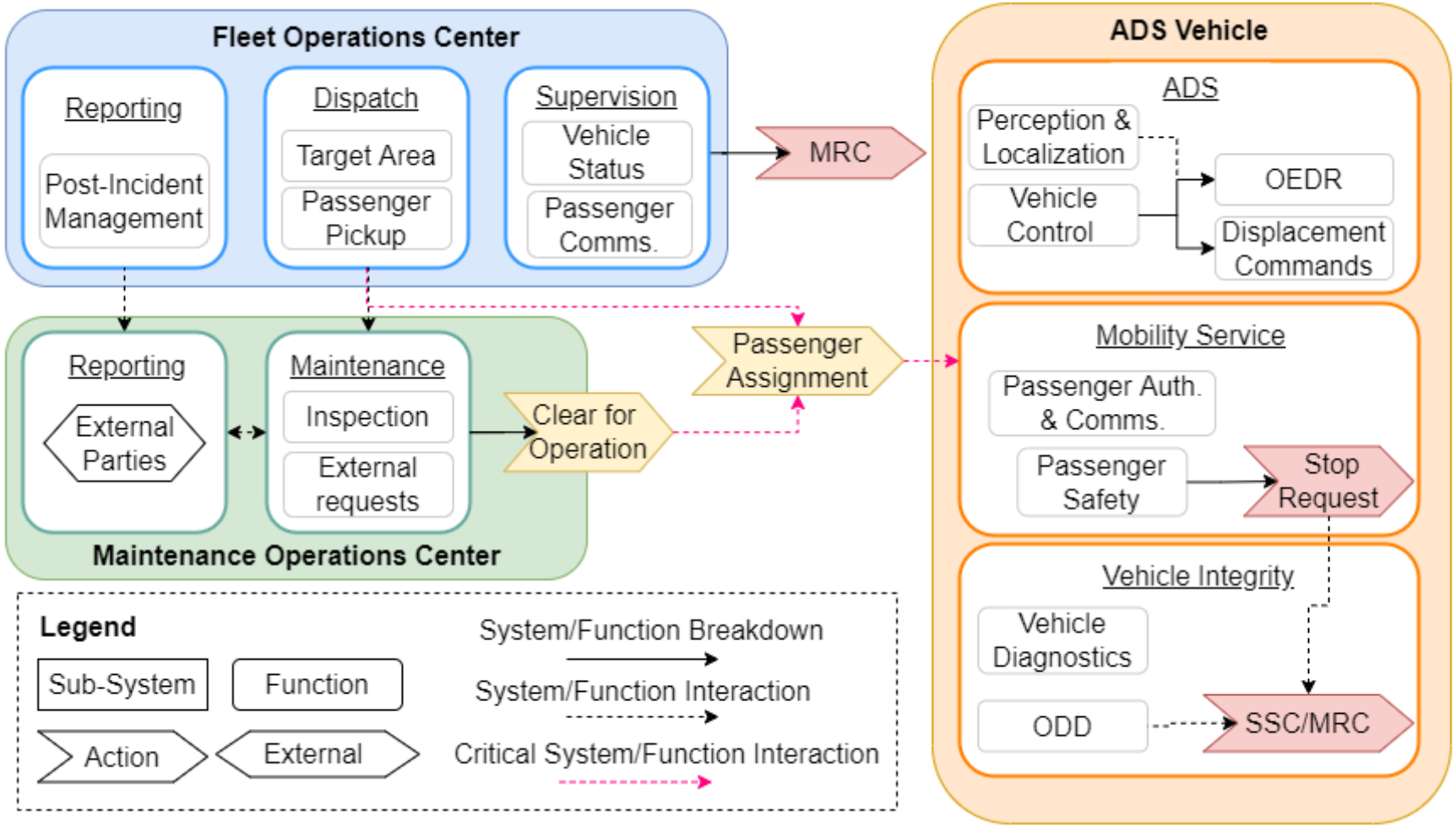
- DDT, mobility service, self-diagnostics, communication.

Fleet Operations Center

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

Maintenance Operations Center

- Inspection and maintenance, reporting to external parties.



Goal: Identify safety risks associated with **L4 ADS MaaS operations** and the responsibilities of the **fleet operator** to mitigate such risks.

UCLA

Definition of "Reference Fleet"

Explore operational scenarios to support hazard identification

Model operational scenarios

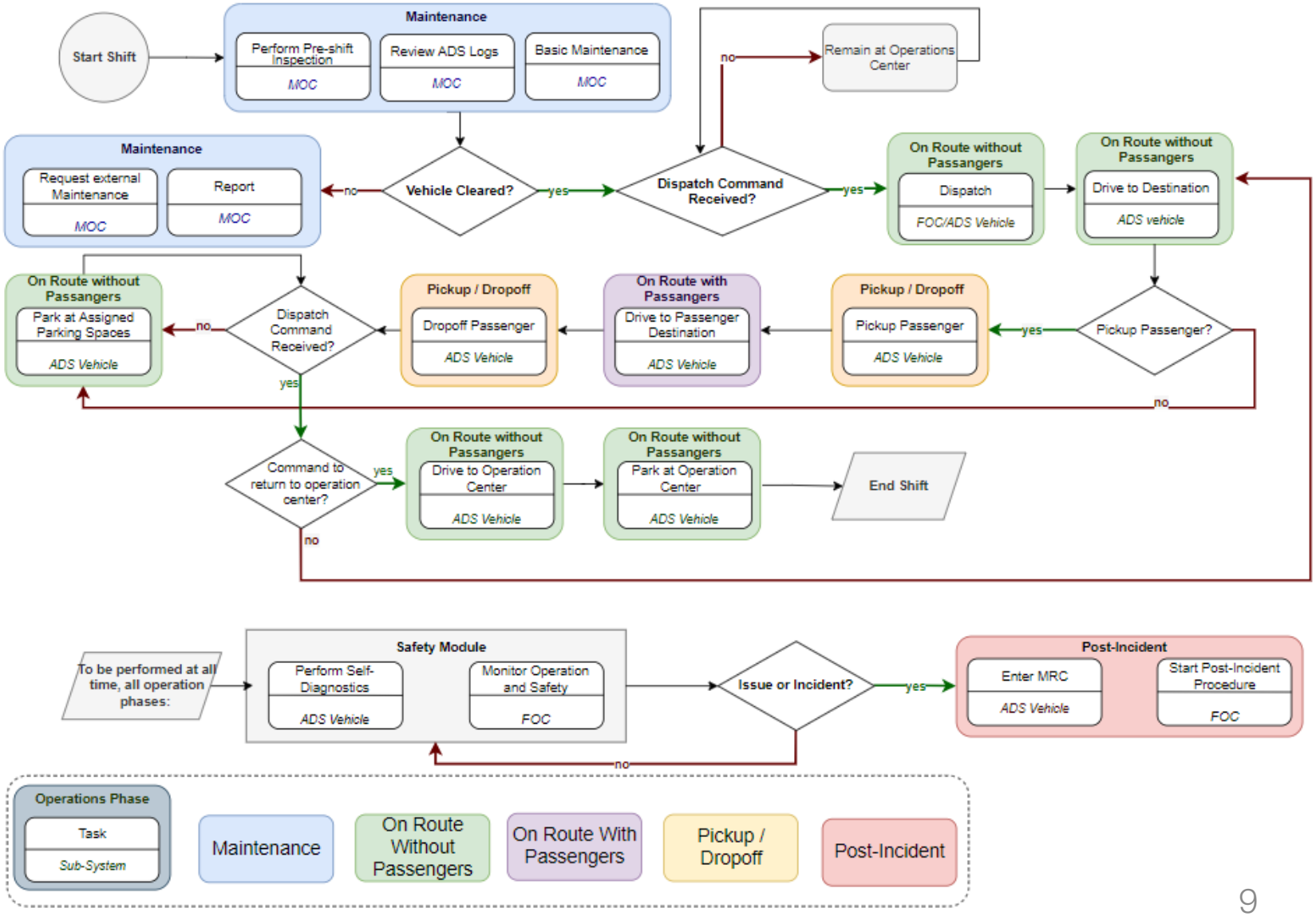
Assumptions:

- ADS vehicle operation characterized by a "shift" defined between inspections.
- Generic operational profile.
  - Inspection & Maintenance
  - On-Route with/without Passengers
  - Post-Incident Management
- Role of each agent is specified.
  - Fleet Operations Center (FOC)
  - Maintenance Operations Center (MOC)
  - ADS Vehicle

Definition of System Breakdown

UCLA

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



Goal: Identify safety risks associated with **L4 ADS MaaS operations** and the responsibilities of the **fleet operator** to mitigate such risks.

UCLA

Definition of "Reference Fleet"

Explore operational scenarios to support hazard identification

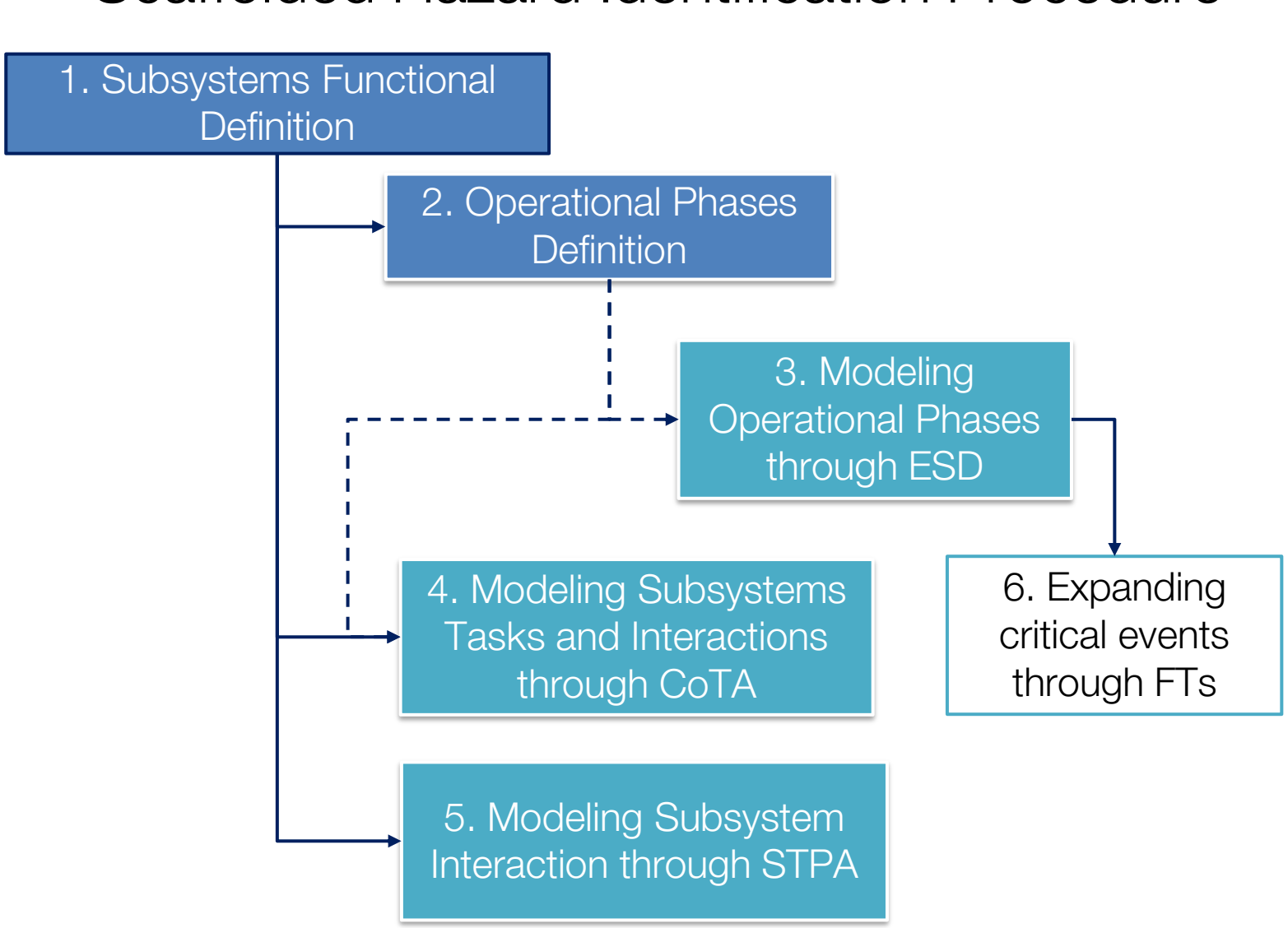
Model operational scenarios

Approach:

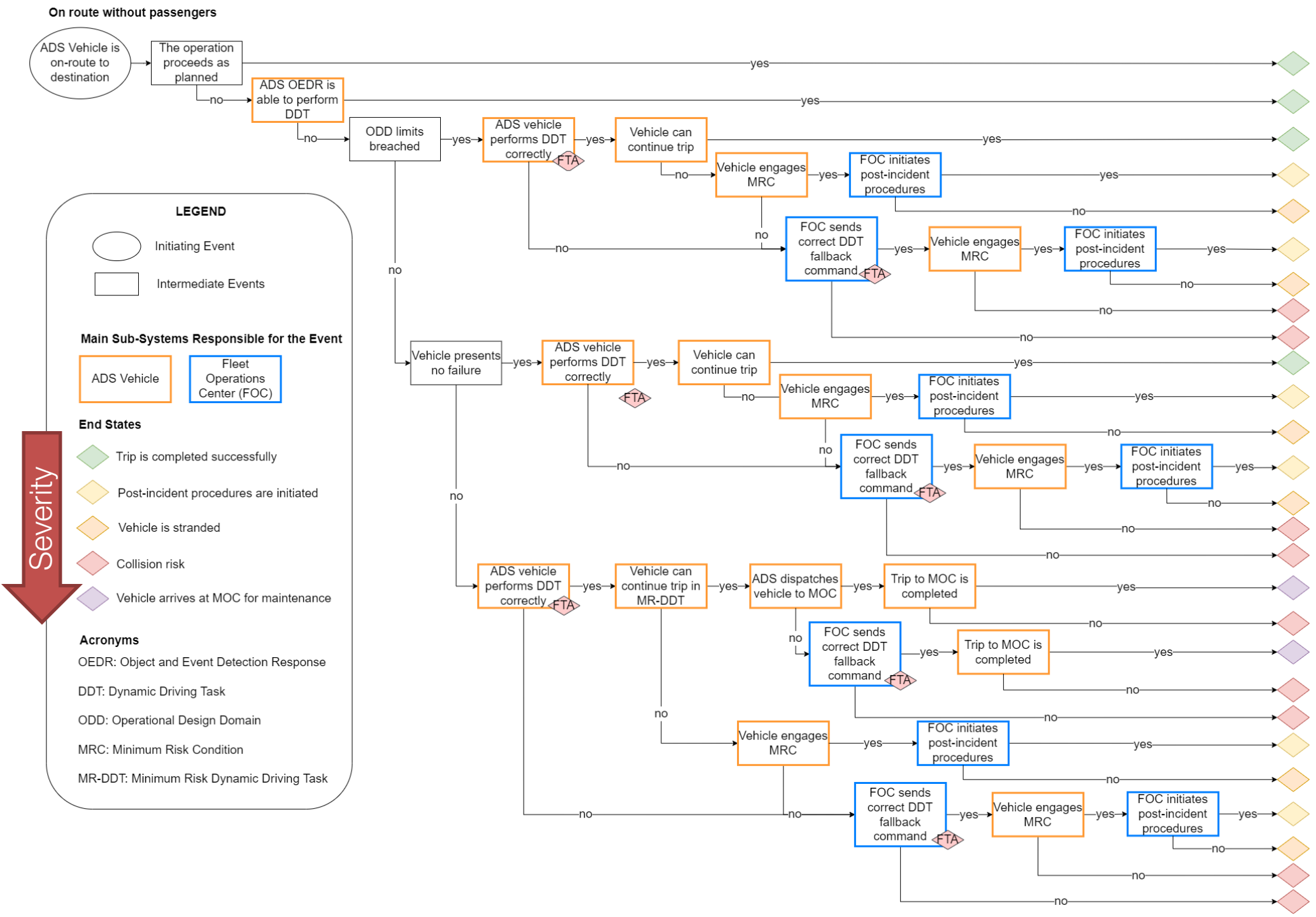
- Hazard identification & modeling key aspect of risk assessments.
- Traditional approaches (Fault Trees, Event Trees, FMEA, etc.)
- Complex interactions: System-Theoretic Process Analysis (STPA) & Concurrent Task Analysis (CoTA).

Combination of methods to achieve a Systematic & Scaffolded Hazard Identification Procedure

UCLA



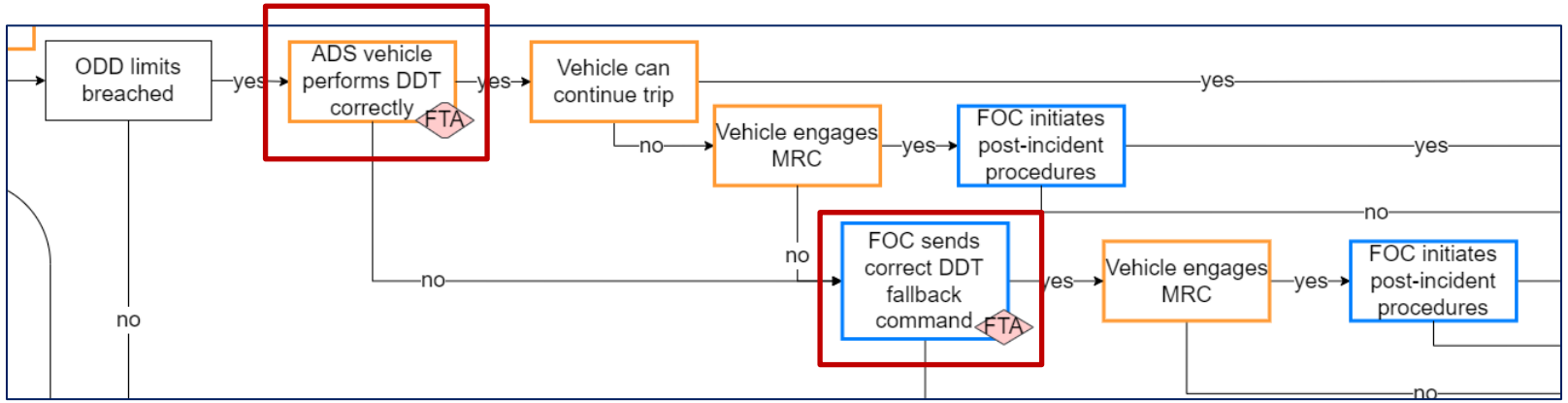
Risk Contributors	Who?
Hazard Scenarios by Operational Phase	What may happen?
Failure Mechanisms/Modes	How may it happen?
Root Causes/Performance Influencing Factors	Why may it happen?
Risk Classification (Consequence x Likelihood)	What are the Risks should it happen?



On-Route without Passengers:

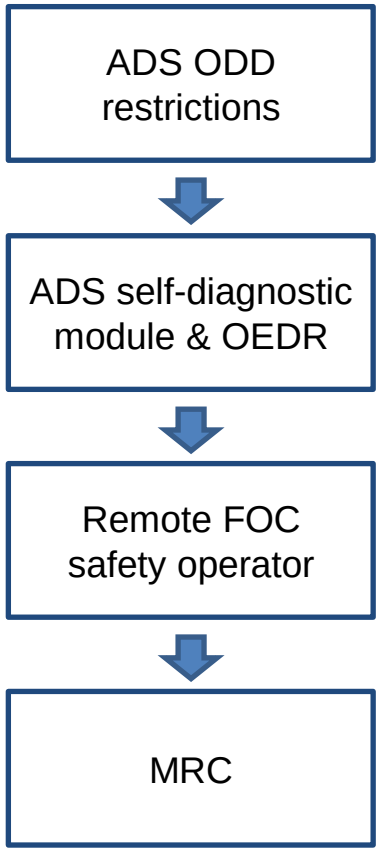
- Initiating Event: “ADS in on-route to destination”.
- Intermediate events are successes (yes) or failures (no).

Extension of Information, Decision, and Action (IDA) model to human and autonomous systems



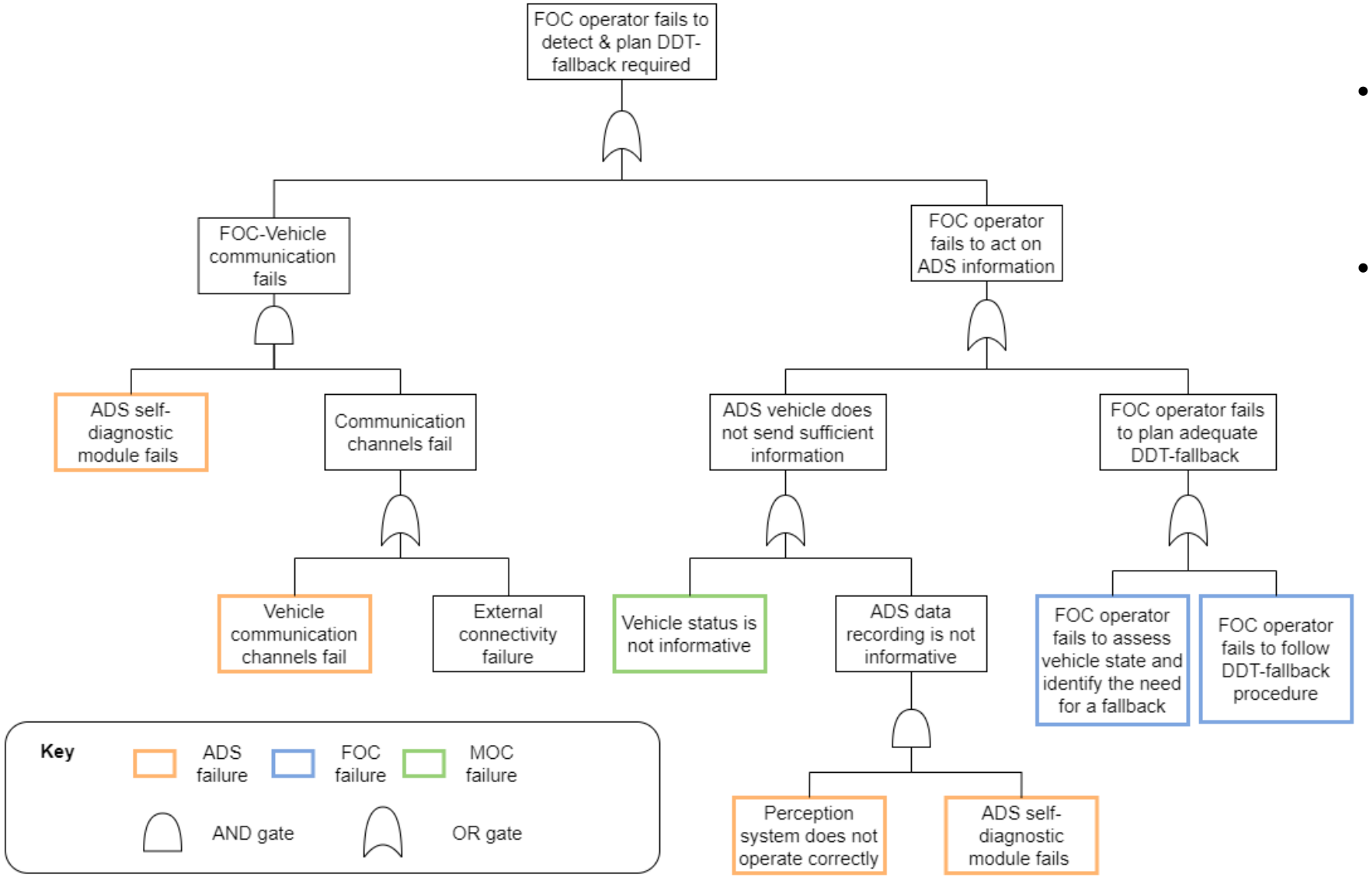
- Division of tasks to identify different failure modes of the ADS and the human operators.
- Account for emergent failures and/or failures arising from unsafe interactions between elements.
- Further analysis through FTs, CoTA, STPA, and BNs.

Safety Barriers Hierarchy



[7] 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.
[8] 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.

Expansion of Key Events: Why?



- High-level expansion of key events to identify the main subsystem responsible.
- Basic Events:
  1. Software-related malfunction.
  2. Hardware-related malfunction.
  3. MOC-related error.
  4. FOC-related error.
  5. External events.
  6. Procedure design error.

Key Findings

- Communication errors play an important role.
  - Supports a more restrictive ODD when considering passenger communications.
  - Self-diagnostic module reliability limitations must be accounted for.
- FOC operator may fail to act based on incomplete or imperfect information available.
  - Failure to monitor & supervise ADS.
  - Failure to intervene when required.
  - Failure to follow adequate DDT fallback.
- Reliability limitations addressed by MOC crew & ADS developer guidelines.
  - Less than adequate inspection or maintenance procedures.
  - Frequency of pre-shift and service inspections.
  - Account for varying detectability of multiple failures.

Static models have a limited capacity to characterize dynamic hazard events.

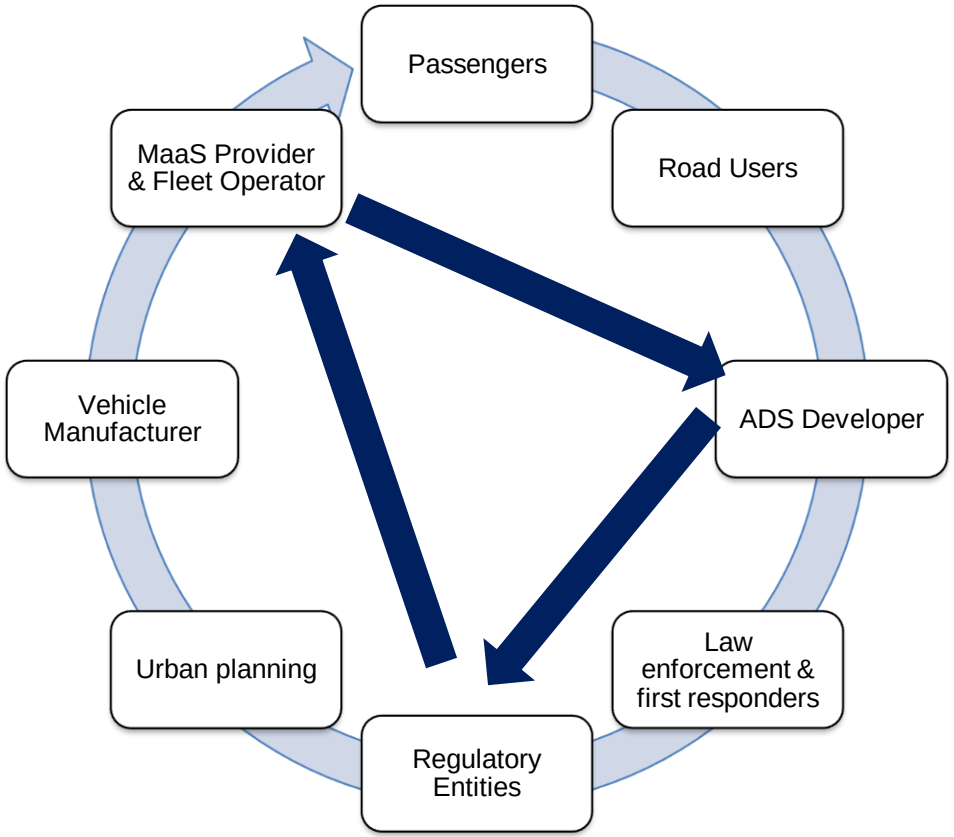
Traditional models still are valuable tools to identify and model hazards to aid risk and safety assessments.

Even in autonomous systems, human interactions and emerging behavior play a key role in system operations.

[9] 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.

UCLA

Summary & Next Steps



1. Explores L4 ADS fleets operation as MaaS, focusing on the interactions between the ADS and the remote fleet operator.
2. Presents an ADS functional breakdown and a generic operational profile.
3. ESDs and FTs are employed to model potential hazard scenarios.
4. An example is presented for the case of an ADS vehicle driving towards a destination with no passengers on board.

Next steps:

- The authors are conducting further work to develop the ESDs and accompanying FTs and include CoTA and STPA methods.

Impact:

1. Model interactions between ADS vehicle and human operators to ensure operational safety.
2. Identify key responsibilities and risk mitigation activities of fleet operators.

B. John Garrick Institute for the Risk Sciences

UCLA ENGINEERING

UCLA

Thank you!

Camila Correa-Jullian, ccorreaj@ucla.edu;

John McCullough, jmccull@ucla.edu;

Marilia Ramos*, marilia.ramos@ucla.edu;

Jiaqi Ma, jiaqima@ucla.edu;

Enrique Lopez Droguett, eald@ucla.edu;

Ali Mosleh, mosleh@ucla.edu

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

Probabilistic Safety Assessment and Management PSAM 16, June 26-July 1, 2022, Honolulu, Hawaii