NHTSA

NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION

Hazard Analysis of Concept Heavy Truck Platooning Systems

Alrik L. Svenson,
Research Engineer

SAE Government/Industry Meeting
Next Steps in Commercial Vehicle Safety
February 2, 2021

Research Objectives

- Explore how safety hazards can be assessed and how they vary based on different levels of implementation.
- Identify various strategies and types in truck platooning systems (current and future concepts).
- Develop an understanding of heavy truck platooning concepts.
- Perform hazard analyses on *generic* heavy truck platooning system concepts and identify cross-cutting and unique items.

Hazard Analysis of Concept Heavy Truck Platooning Systems

Project Team: Battelle, The Volvo Group, WABCO, and SAE International

Research Tasks:

- Market study to identify current and future concept systems
- Conduct hazard analysis and risk assessment
- Select representative, “generic,” platooning system concepts for functional safety analyses
- Safety of the Intended Functionality Analysis (SOTIF)
- Fault Tree Analysis (FTA) for selected hazards

Identifying Hazards

- **Hazard – an event that poses a danger to people, the system, or the environment. Caused by:**
  - Human error
  - Failure of hardware
  - Software issues
  - Limitations of the system design
- **Risk Assessment – to identify:**
  - **Severity**
    - Cost of the hazard, in terms of injuries or fatalities to users and the public
    - System repair costs or environmental damage
  - **Frequency**
    - Measures likelihood of occurrence, per unit of time or usage
  - **Controllability**
    - Ability of an operator to mitigate a hazardous situation

ISO 26262 Road Vehicles – Functional Safety standard

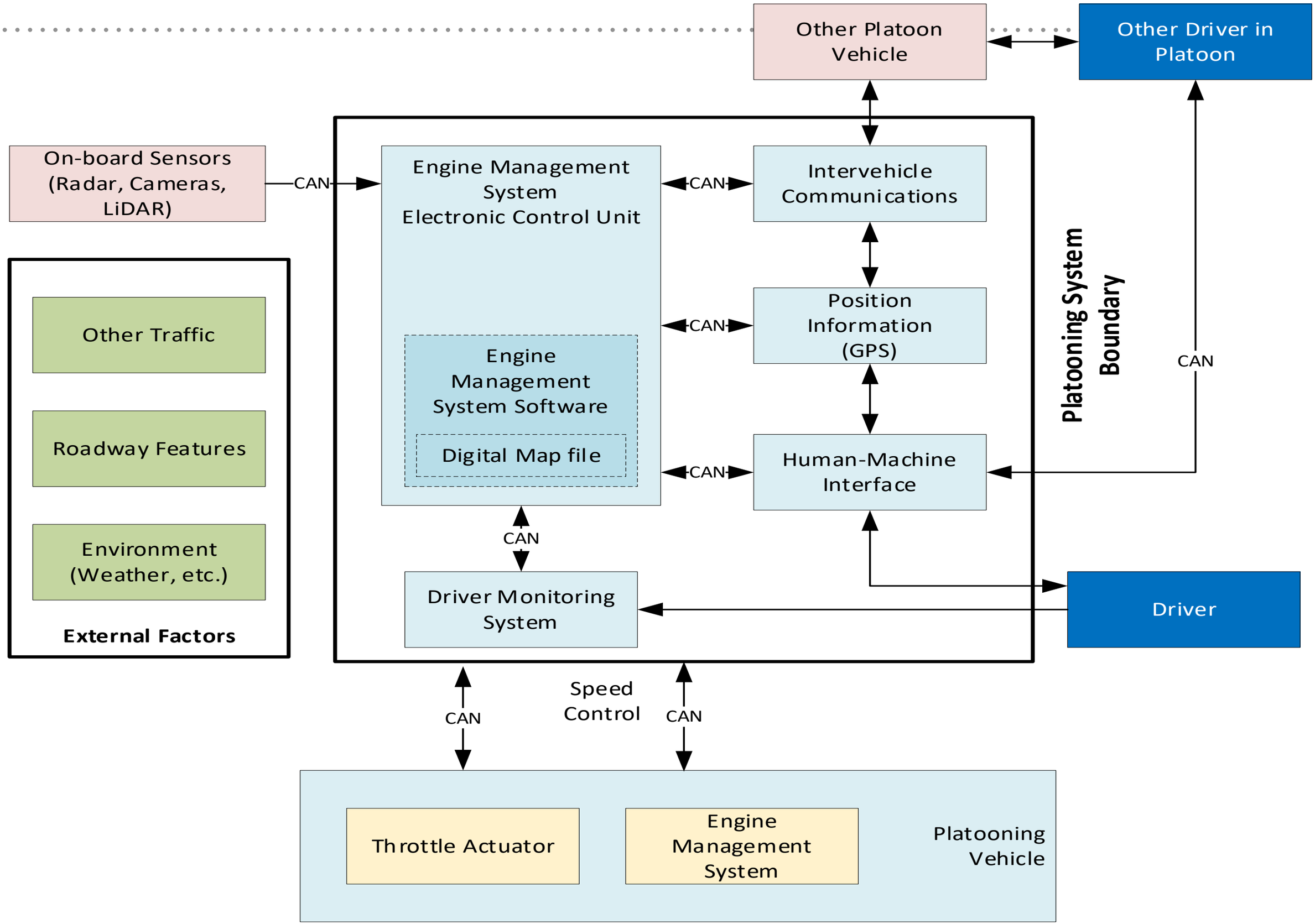
Platooning System Concepts

System	Truck Configura-tion	# of Vehicles in Platoon	Driver Present in Each Vehicle	Lead Vehicle Driver Responsibilities	Following Vehicle Driver Responsibilities
2VL1	Single tractor-semitrailer	2	Yes	Speed and steering control, and managing the platoon	Steering control only
3VL2	Single tractor-semitrailer	3	Yes	Speed and steering control, and managing the platoon	Neither steering nor speed control

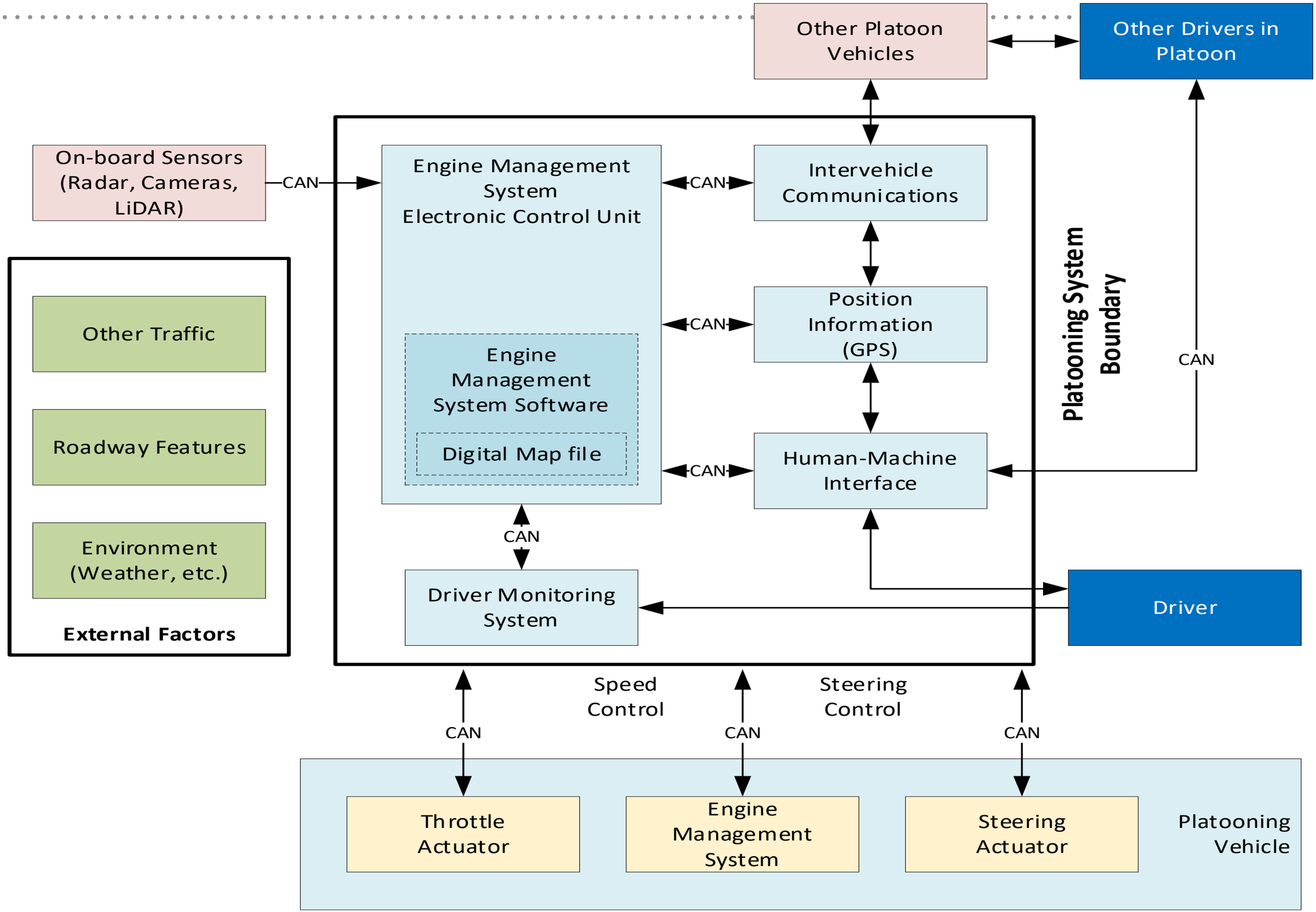
Operational Design Domain (ODD) and System Assumptions:

- Platoon is already in formation
- Operating on a freeway
- Platoon is cruising at a nominal steady-state speed
- No hazardous materials are being transported
- Inter-vehicle communications
- Environmental conditions, such as weather and traffic were included as appropriate

2VL1 Concept Platooning System



3VL2 Concept Platooning System



Determination of Hazards and Risks

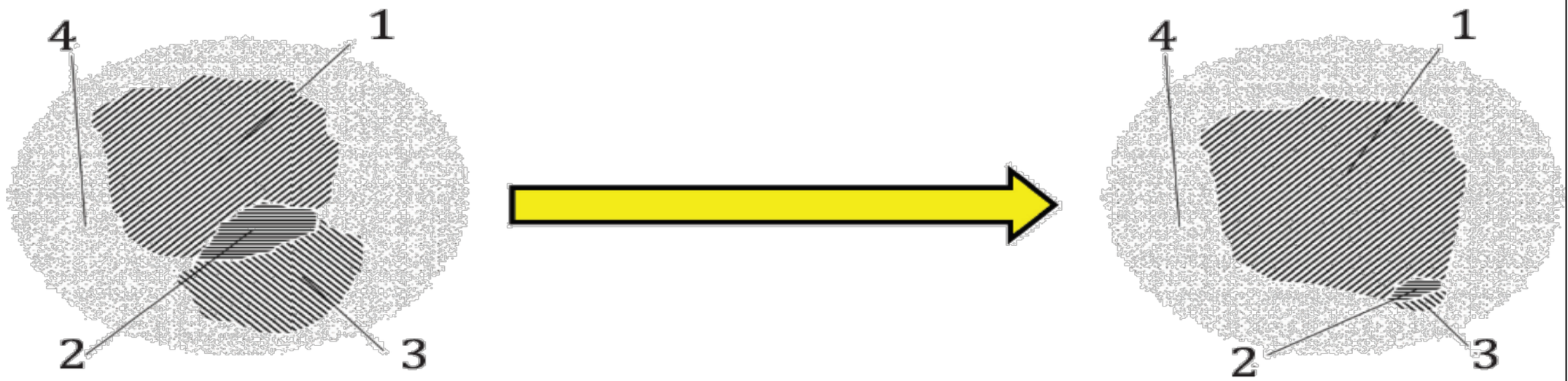
- **List of 57 hazards was identified**
  - Categorized by: equipment failures, operational environmental hazards and human factors.
  - Classified by: severity, probability of exposure, and controllability.
  - Assigned ASIL to each hazard.
  - Safety Mitigations were developed.
  - Risk Analysis was conducted using input from industry stakeholders.

Example Hazards

Hazard ID	Description	System Applicability
17	There is an unexpected stoppage in traffic.	2VL1 and 3VL2
18	There is unexpected road debris.	2VL1 and 3VL2
28	There is a difference in tire wear (e.g. traction, tread depth, grip, etc.) between the Lead and Following Vehicles.	2VL1 and 3VL2
33	There is a loss in steering control in the Lead Vehicle.	2VL1
34	There is a loss in steering control in the Following Vehicle.	3VL2
41	There is a cyber-attack on the Following Vehicle's communication subsystem.	2VL1 and 3VL2
53	A motorcycle performs a cut-in between two platooning vehicles.	2VL1 and 3VL2
57	The driver of the Lead Vehicle performs an evasive steering maneuver.	3VL2

Safety of the Intended Functionality Analysis

- Safety of the Intended Functionality (SOTIF) Analysis
- Performed using ISO 21448 Standard
- Purpose: Reducing the unknown unsafe scenarios is done iteratively as the SOTIF Process proceeds.



Example of an Initial Starting Point of Development

Goal for the Finished Development

Key

1 known safe scenarios (Area 1)

2 known unsafe scenarios (Area 2)

3 unknown unsafe scenarios (Area 3)

4 unknown safe scenarios (Area 4)

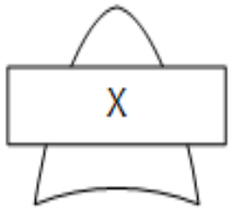
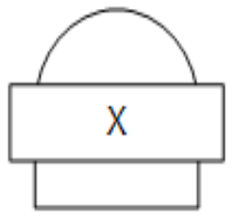
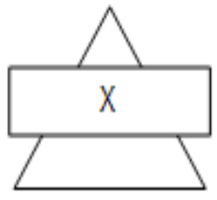
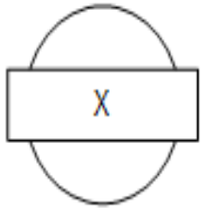
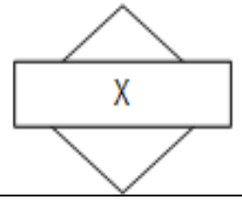
Source: ISO26262 Standard

Findings from the SOTIF Analysis

- Not having a functional system specification was challenging.
  - SOTIF completed with available information and estimated (or assumed) design details as an example of the process.
- Known unsafe conditions identified as a baseline for establishing list of example verification tasks.
  - In actual SOTIF, validation use case scenarios are developed to identify unknown unsafe scenarios.
  - Unexpected scenarios add to the list of known unsafe conditions.
  - Iterative process of SOTIF increases the safety and reliability of the platooning system.

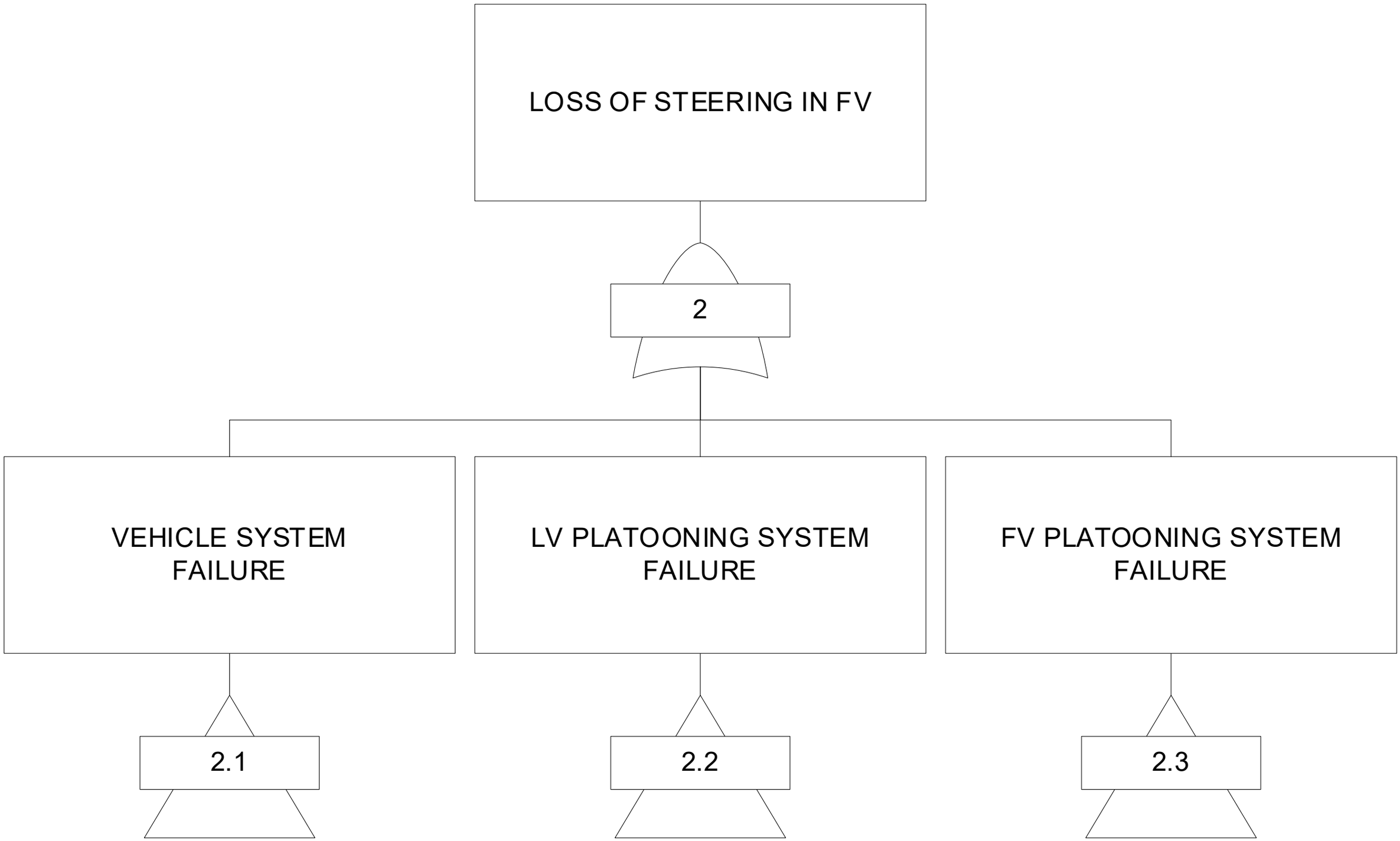
Fault Tree Analysis (FTA)

1. Identify undesired events
2. Understand the system
3. Construct the fault tree
4. Evaluate the fault tree
5. Control the hazard

Symbol	Symbol Description	Symbol Definition
	Or Gate	Illustrates the output occurs if at least a single event occurs.
	And Gate	Illustrates the output occurs if and only if all inputs occur.
	Transfer Gate	Illustrates a transfer continuation from a different part within the fault tree tha this was developed.
	Basic Event	Identifies a basic initiating System or Subsystem fault.
	Undeveloped Event	Identifies an event that does not need to be further developed or resolved.

Example Fault Tree Analysis

- **There is a loss of steering in the Following Vehicle (FV)**



Study Findings

- All but a few of the hazards described in the hazard analysis could be mitigated to an the lowest ASIL level during the risk assessment:
  - An unexpected stoppage in traffic.
  - Unexpected road debris.
  - Difference in tire wear (e.g., traction, tread depth, grip, etc.) between the LV and FV(s).
  - Loss in steering control in the LV.
  - Loss in steering control in the FV.
  - Cyber-attack on the FV's communication subsystem.
  - A motorcycle performs a cut-in between two platooning vehicles.
  - Driver of the LV performs an evasive steering maneuver.
- Remaining hazards were analyzed in SOTIF and FTA analyses to determine safety countermeasures.

Study Findings (Cont.)

- SOTIF analysis methodology is a useful analysis tool for truck platooning systems.
- The feedback loop inherent in the SOTIF analysis can help to increase the safety and reliability of a platooning system.
- Based on the FTA results, systems with a human-in-the-loop could benefit from safety mitigations such as training and operating procedures that are fully dependent upon the human complying.

Final Report Available at:

National Transportation Library

https://ntl.bts.gov/

Contact Information:

Alrik L. Svenson, NHTSA
Alrik.Svenson@dot.gov