Functional Safety Analysis of Automated Vehicle Lane Centering Control Systems

John Brewer and Wassim Najm
Volpe National Transportation Systems Center

July 22, 2015

2015 Automated Vehicles Symposium

Project Purpose

- Goal

  Ensure the safe operation and functional safety of reliable automated lane centering control systems at all NHTSA automation levels

- Objectives

  1. Conduct comprehensive hazard analysis
  2. Provide research findings supportive of functional safety concepts and requirements , including
     - diagnostic needs
     - identify performance parameters
     - functional safety test scenarios
     - driver-vehicle interface requirements
  3. Provide research findings supportive of improving driver awareness and training

- Focus
  - Light vehicles
  - Steering and/or braking lateral controls
  - Shared lateral and longitudinal control systems

Research Approach and Tasks

System Description and Understanding

Hazard Analysis

Diagnostic and Prognostic Needs

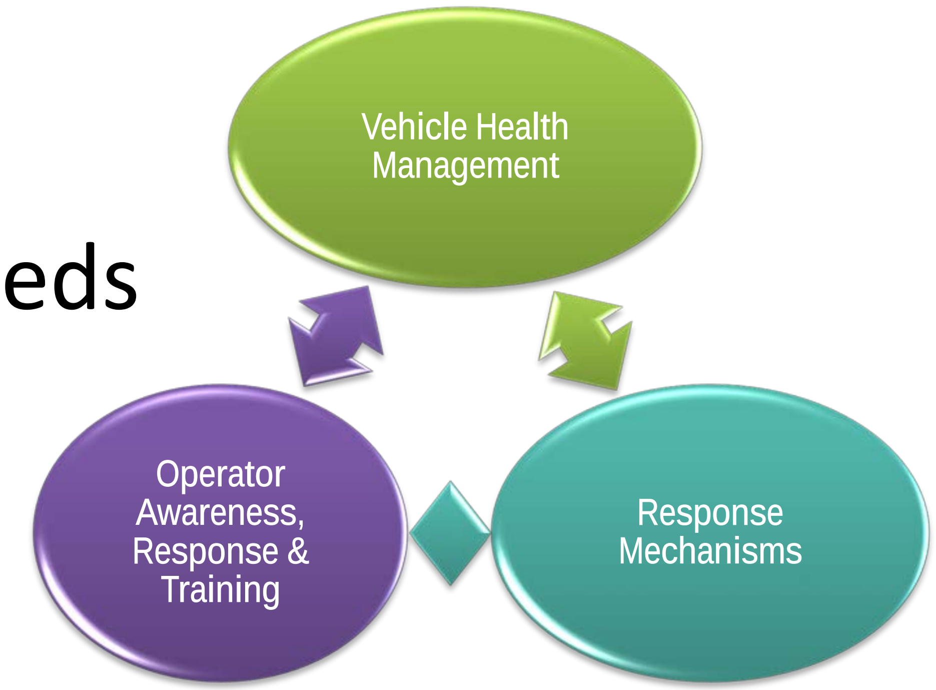
Functional Safety Requirements

Performance Parameters

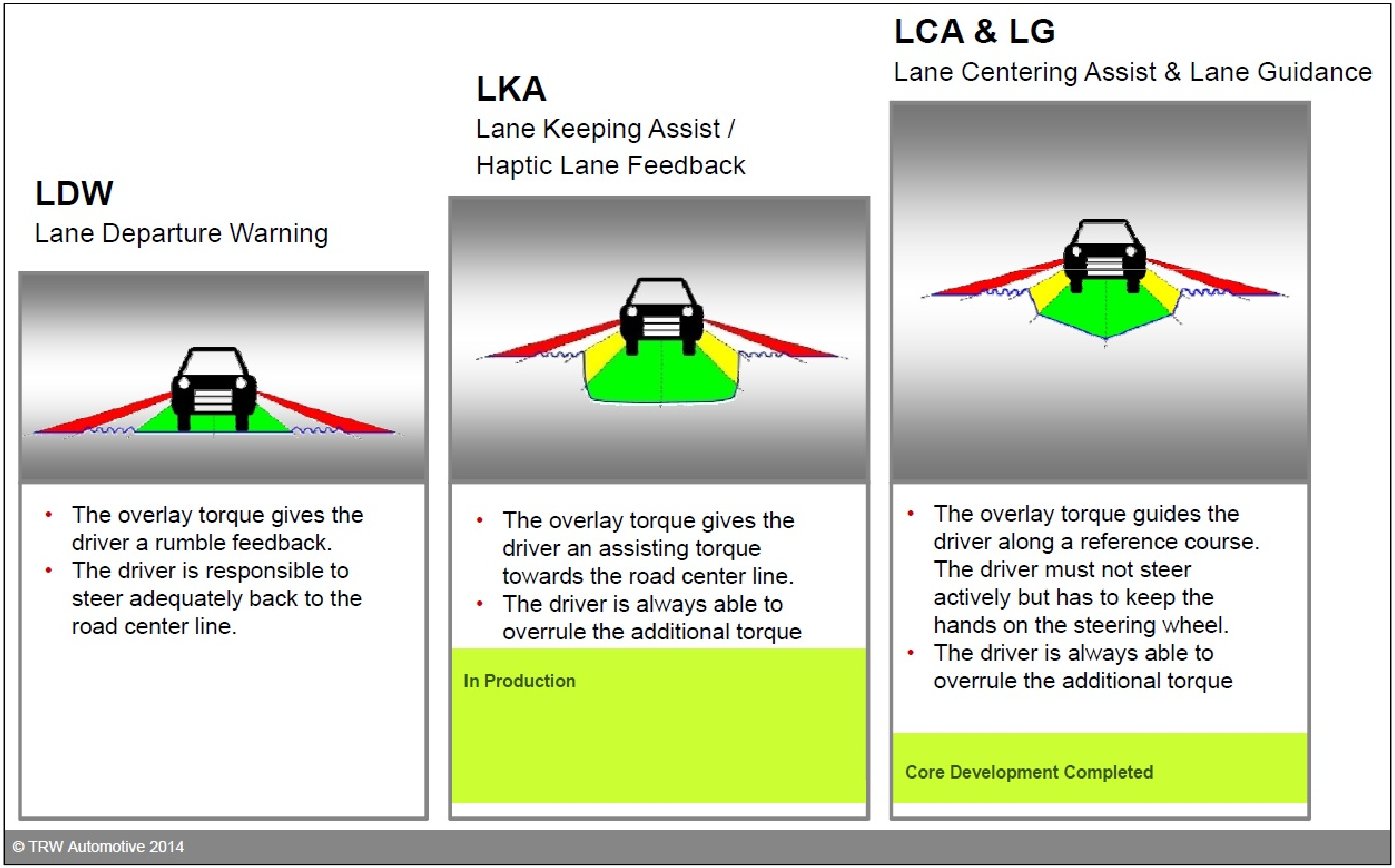
Driver-Vehicle Interface Needs

Driver Awareness and Training Needs

Functional Safety Test Scenarios



TRW Automotive Depiction of Lateral Assist Technologies (used with permission)



Terminology and Nomenclature

- Lateral Control ("Lane Centering")
  - An essential function of vehicle automation when integrated with longitudinal vehicle control systems such as adaptive cruise control
  - Largely implemented through shared braking and/or steering control services with longitudinal control systems
- Automated Lane Centering vs. Automated Lane Keeping
  - ALC provides continuous control across the lane width
  - ALK provides control inputs only near lane boundaries
- Industry often refers to these features as "assist"
  - e.g., "Lane Keep Assist" or "Lane Center Assist"
  - Emphasizes that current implementations are convenience features rather than safety systems

Subject Matter Expert Interviews

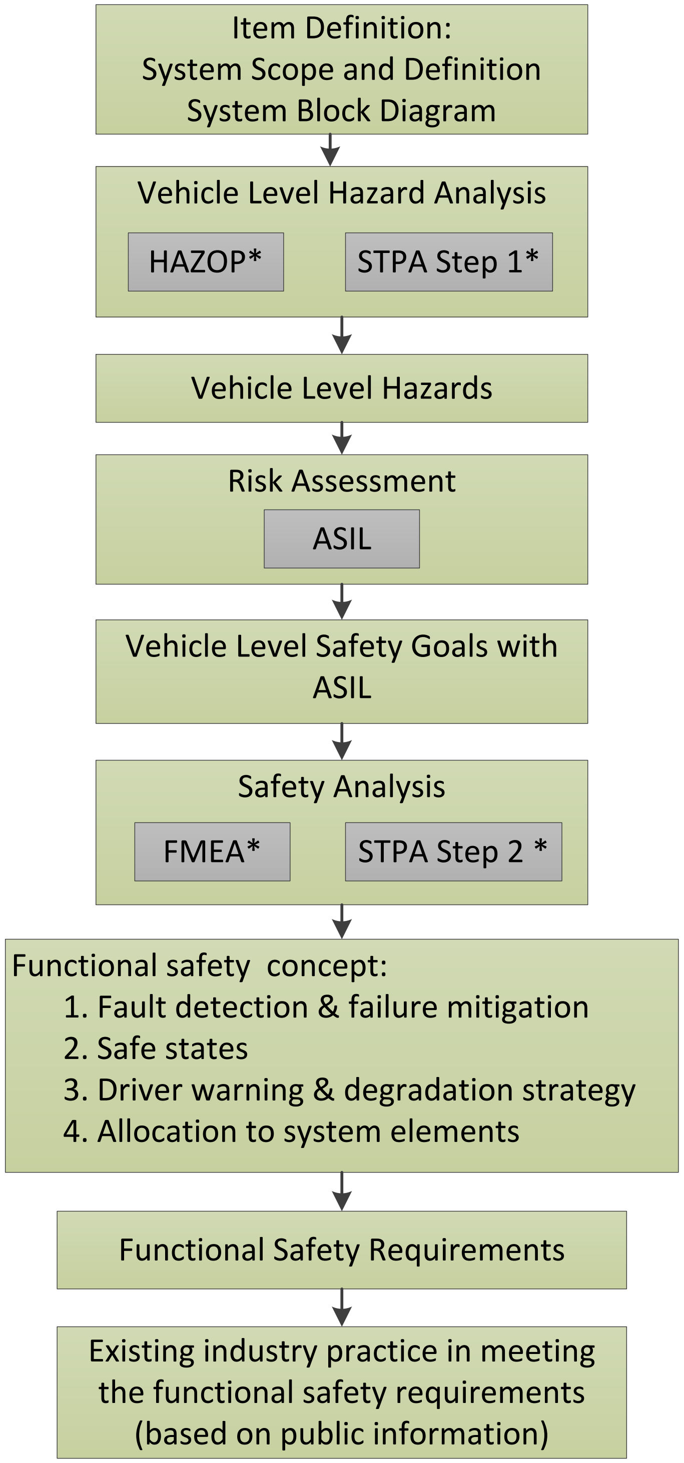
The SMEs included representatives from:

- The University of Minnesota
- The University of California, Berkeley
- ESG Automotive (ESG)
- The U.S. Army Tank Automotive Research, Development and Engineering Center (TARDEC)
- Ford Motor Company (Ford)
- TRW Automotive (TRW)
- Google, Inc.

Subject Matter Expert Insights

- Lateral control is more commonly implemented through steering rather than torque vectoring and brake vectoring.
- Current ALK/ALC Limitations:
  - Vehicle (roadway illumination, quality of sensor data, etc.)
  - Performance envelope (vehicle speed, curvature, etc.)
  - Infrastructure (road markings, etc.)
  - Environment (weather, lighting, etc.)
  - Other (roadway hazards, traffic diverted away from lanes, etc.)
- OEMs classify current lateral assist technologies as Level 1 or 2
- Driver notification and monitoring driver engagement are significant challenges for Level 3
- Driver-Vehicle Interface (DVI)/Human-Machine Interface (HMI) approaches have not been standardized.
- Industry considers overall automated system safety in addition to functional safety

Analytical Process



*ISO 26262 does not require specific methods for hazard and safety analyses. Other comparable hazard and safety analysis methods may be used.

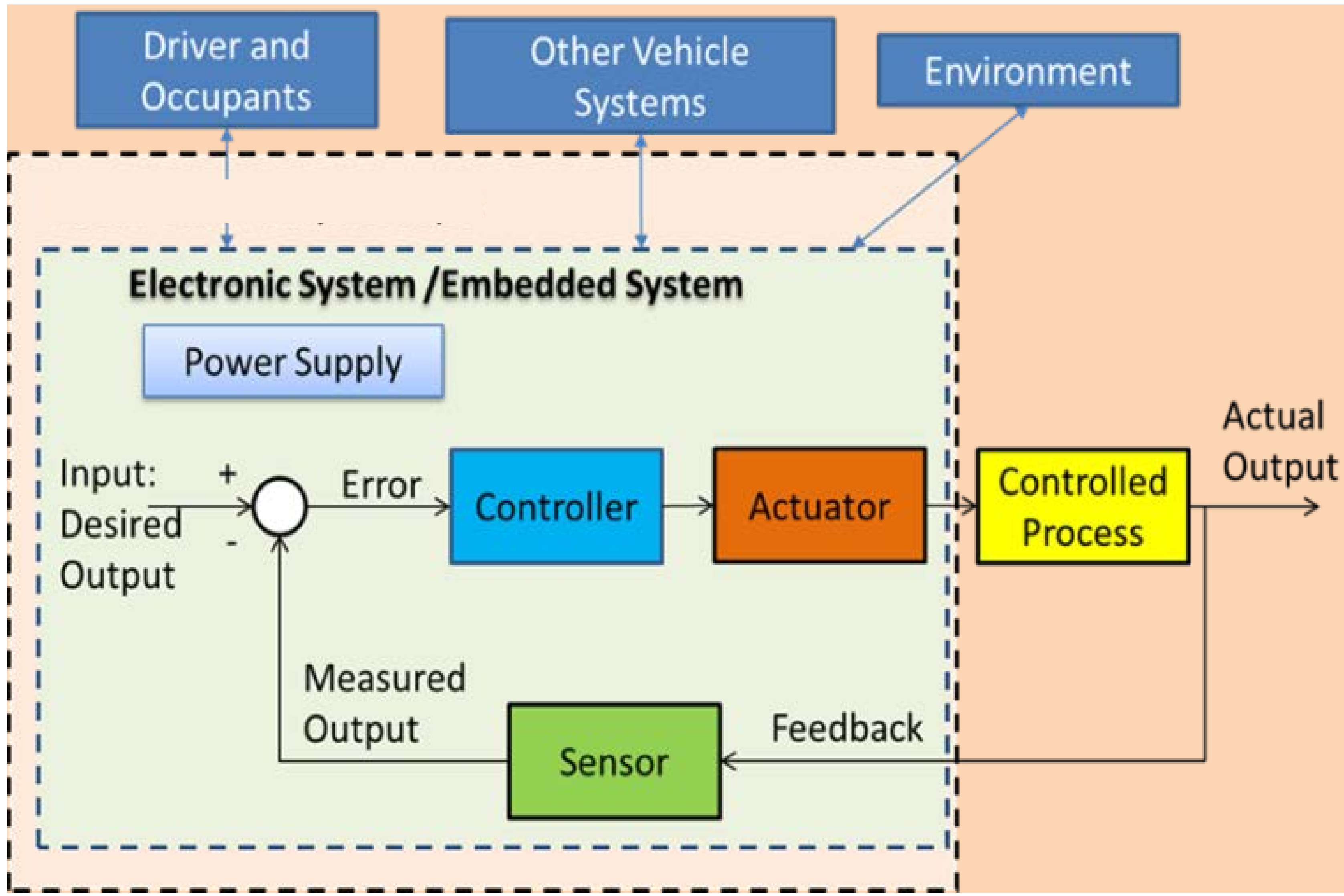
Hazard Analysis and Risk Assessment

Identify potential vehicle-level hazards and causal factors associated with the failure of lane centering technologies and component braking services

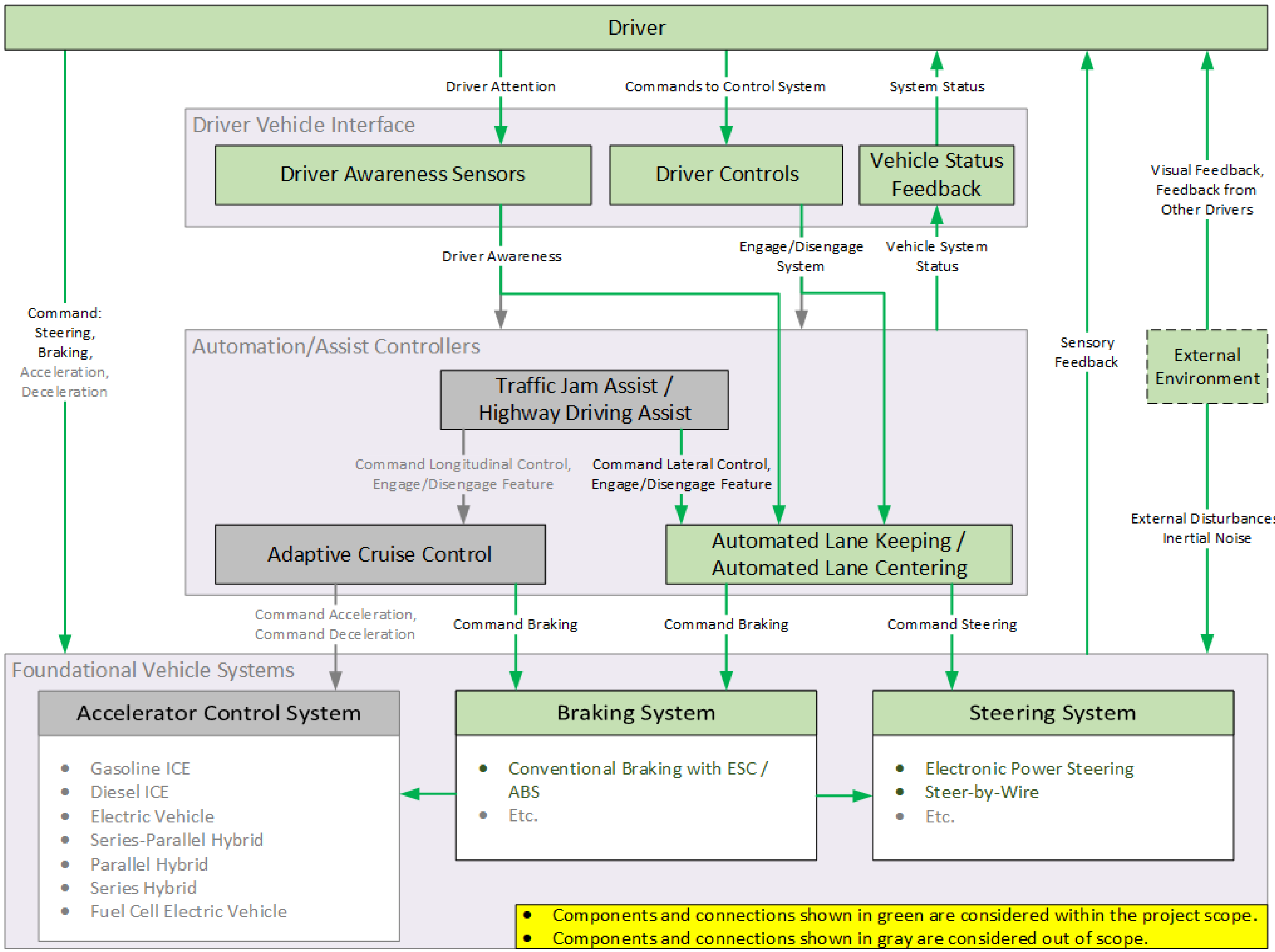
1. Query crash data, recalls, and owners complaints
2. Conduct comprehensive hazard analysis to identify hazards, unsafe control actions, and causal factors
   - System Theoretic Process Analysis (STPA)
   - HazOp plus Safety Analysis (e.g., FMEA)
3. Perform risk assessment to classify hazards according to severity, exposure, and controllability
   - Consider exposure and vehicle use cases in various driving scenarios (i.e., normal-driving, driving-conflict, and crash-imminent situations) and environmental conditions.

Hazard Analysis with STPA Method

System Description
↓
System-Level Losses
↓
Hazards
↓
Unsafe Control Actions
↓
Causal Factors



Analytical Scope of Automated Lane Centering/Automated Lane Keeping Systems



Foundational Analysis Across NHTSA Automation Levels

Foundational System	Level 1	Level 2	Level 3	Level 4
Steering (Electric Power Steering [EPS], Steer-by-Wire [SbW])				
Braking (ESC, ABS)				
Acceleration Control (ICE, EV, HEV)				

ALC/ALK

ACC

Vehicle Dynamics Integrated Module [VDIM]

Proposed Hazard Analyses

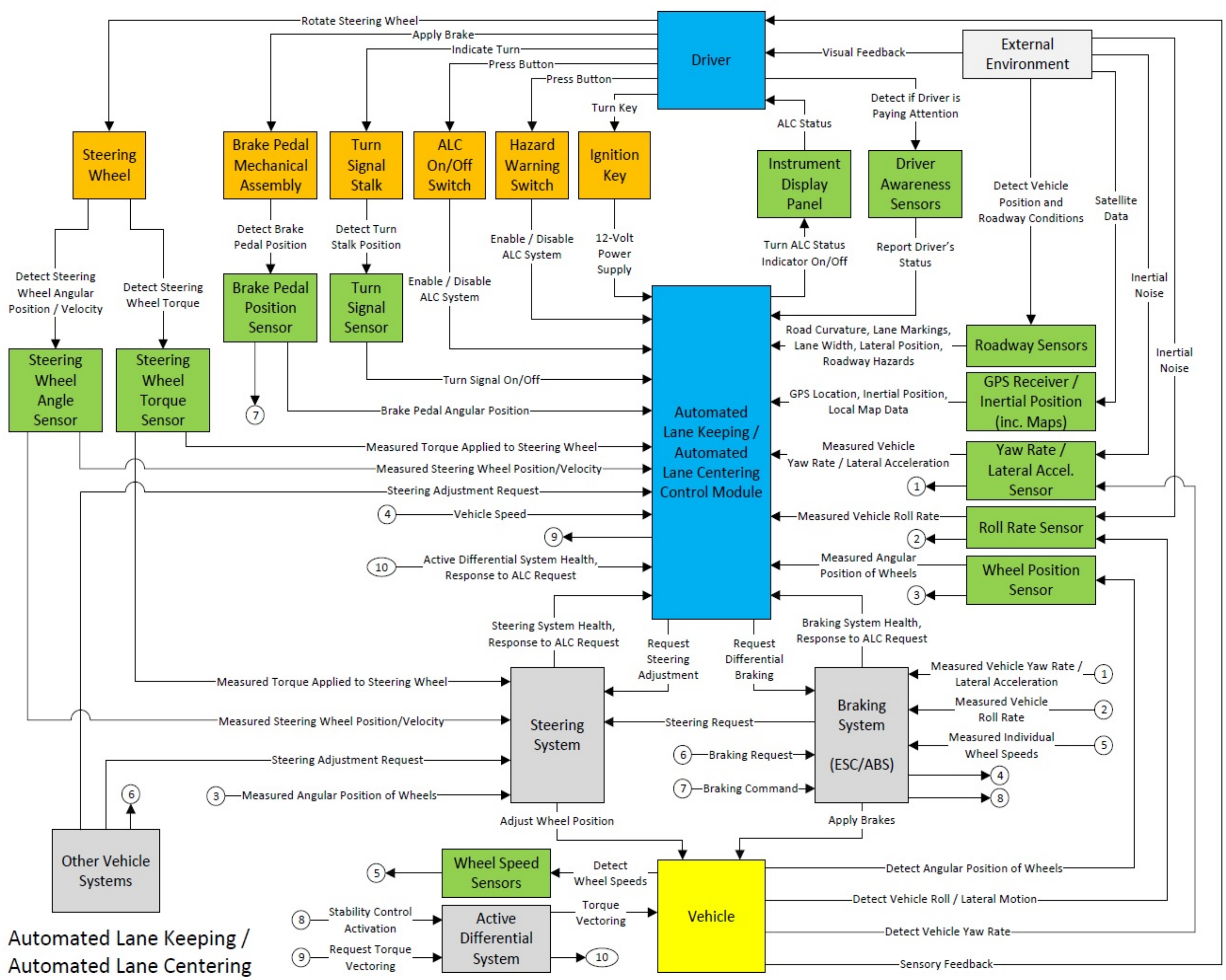
- One analysis of ALK/ALC system with steering and braking as "black boxes"
  - Will not consider specifics of sensors.
  - Will focus on the critical sensor information for the ALK/ALC control module.
- Steering
  - Two steering system analyses (Electric Power Steering, Steer-by-Wire).
  - ALK/ALC interface is via steering requests from "Other Vehicle Systems"
- Braking
  - One braking system analysis (Conventional braking with ESC/ABS).
  - ALK/ALC interface is via braking requests from "Other Vehicle Systems".

Relationship Between Lateral Control and NHTSA Automation Levels*

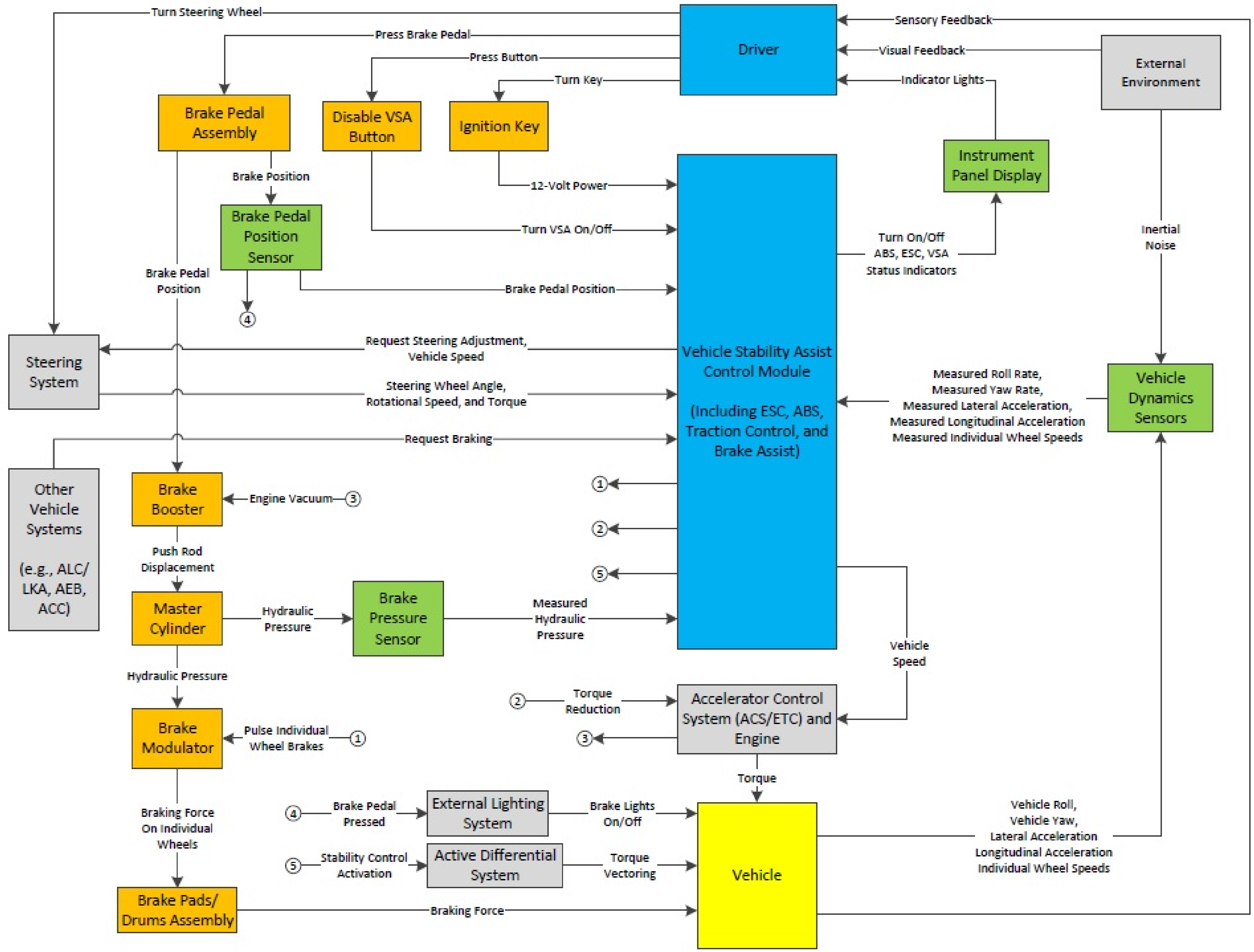
- At Level 1, ALK/ALC is a stand-alone feature
- At Level 2, ALK/ALC may be combined with another feature (e.g., Adaptive Cruise Control [ACC]) to provide some automation
- At Level 3 or 4, both lateral and longitudinal control need to be integrated into "path planning" and hazard recognition/avoidance
  - Complete Level 3 / 4 functionality is out of scope for this project
  - Analyses of foundational systems are still relevant for Levels 3 and 4.

*For this poster, "Level" refers to *NHTSA Automation Level* rather than the SAE definition

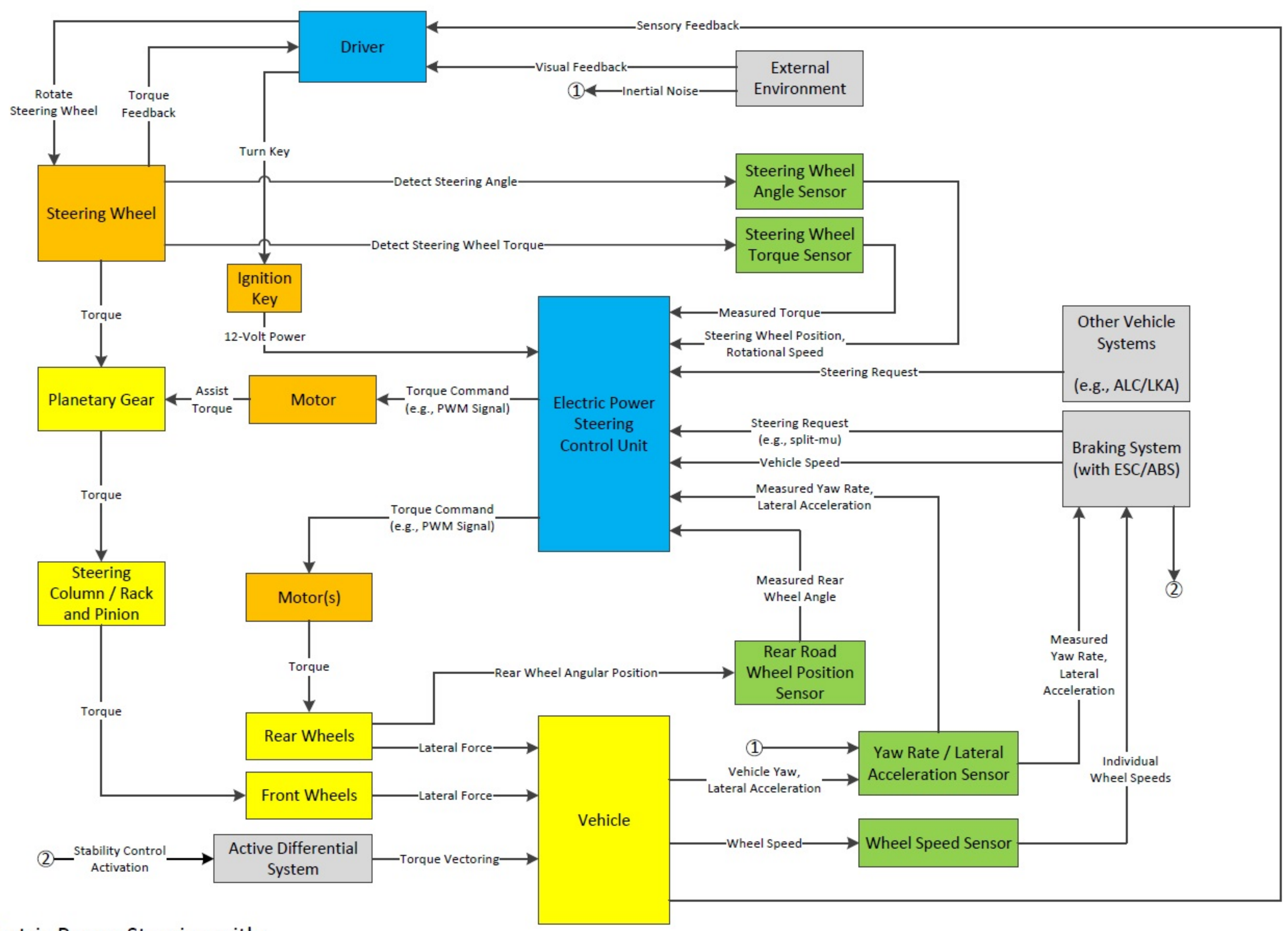
Control Structure Diagram for a Lane Keep Assist/Lane Centering Assist System



Control Structure Diagram for a Conventional Hydraulic Brake System with Electronic Stability Control



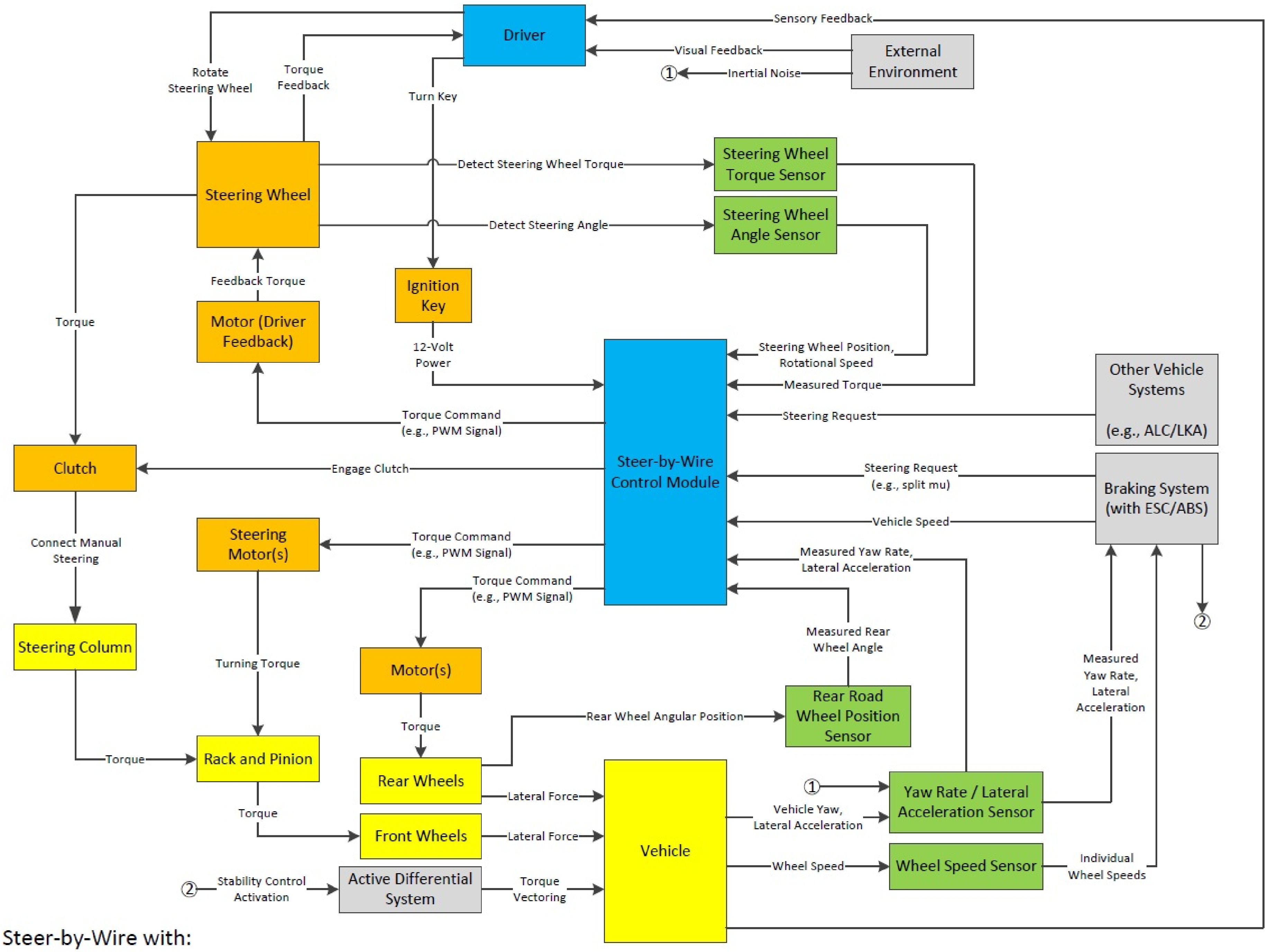
Control Structure Diagram for an Electric Power Steering System



Electric Power Steering with:

- Active Steering
- Active Feedback
- All-Wheel Steering

Control Structure Diagram for a Steer-by-Wire System



Steer-by-Wire with:

- All-Wheel Steering