Elektrobit

UDACITY

# Safety Plan Lane Assistance

**Document Version:** [2.0]

Template Version 1.0, Released on 2017-06-21

# Document history

**[Instructions: Fill in the date, version and description fields. You can fill out the Editor field with your name if you want to do so. Keep track of your editing as if this were a real world project.**

**For example, if this were your first draft or first submission, you might say version 1.0. If this is a second submission attempt, then you'd add a second line with a new date and version 2.0]**

| Date | Version | Editor | Description |
|---|---|---|---|
| 08-05-2019 | 1.0 | Vaidehi Venkatesan | Initial draft of the safety plan |
| 08-07-2019 | 2.0 | Vaidehi Venkatesan | Final proof-read |
| | | | |
| | | | |
| | | | |

# Table of Contents

**[Instructions: We have provided a table of contents. If the table of contents is not showing up correctly in your word processor of choice, please update it. The table of contents should show each section of the document and page numbers or links. Most word processors can do this for you. In Google Docs, you can use headings for each section and then go to Insert > Table of Contents. Microsoft Word has similar capabilities]**

# Introduction

## Purpose of the Safety Plan

**[Instructions: Answer what is the purpose of a safety plan?]**

Designing a safe vehicle requires a safety plan as its first step. Vehicular systems are complex models with social and technological requirements. Safety Plan provides an overall framework for the functional safety of Lane Assistance System project. The key topics in a safety plan include:

1. **Define item** for which functional safety is designed for.
2. Describe how new **roles** / features are introduced in to the system to ensure safety and how existing product is being modified in order to accommodate the functional safety standard.
3. Describe how **safety lifecycle is tailored** to include selective parts of V Model in the functional safety project.
4. Enlists the different **resources** and their roles in the team.
5. Details **system engineering methods** required to support the process
6. Chalk out a **project schedule plan** of when tasks will be completed
7. List **confirmation measures** that will be used to prove that the functional safety has been achieved.

This document helps in

1. Safety assessment audits under ISO26262 to ensure decisions made in the lane assistance project achieves appropriate functional safety.
2. Serves as a reference document while modifying the lane assistance system. It also serves as a proof post-production for quality regulation bodies (e.g. Government) to check and ensure that the system available in-market was defined and tested with functional safety standards.

## Scope of the Project

**[Instructions: Nothing to do here. This is for your information.]**

For the lane assistance project, the following safety lifecycle phases are in scope:

Concept phase
Product Development at the System Level
Product Development at the Software Level

The following phases are out of scope:

- Product Development at the Hardware Level
- Production and Operation

## Deliverables of the Project

**[Instructions: Nothing to do here. This is for your information.]**

The deliverables of the project are:

- Safety Plan
- Hazard Analysis and Risk Assessment
- Functional Safety Concept
- Technical Safety Concept
- Software Safety Requirements and Architecture

# Item Definition

**[Instructions:**

**OPTIONAL**
**Optionally, include information about these points as well. These were not included in the lectures, but you might be able to find this information online:**

- **Operational and Environmental Constraints. This could especially be limited to camera performance; lane lines are difficult to detect in snow, fog, etc**
- **Legal requirements in your country for lane assistance technology**
- **National and International Standards Related to the Item**
- **Records of previously known safety-related incidents or behavioral shortfalls**

**]**
**Discuss these key points about the system:**

The item or system under consideration in the functional safety module is “Lane Assistance System”. The Lane Assistance Item alerts the driver that the vehicle has accidentally departed its lane and attempts to steer the vehicle back toward the center of the lane.

**What is the item in question, and what does the item do?**
This system will have two key functions:

1. Lane departure warning - to alert the driver when the vehicle departs from the lane.
2. Lane keeping assistance - to ensure the vehicle is in the lane during driving.

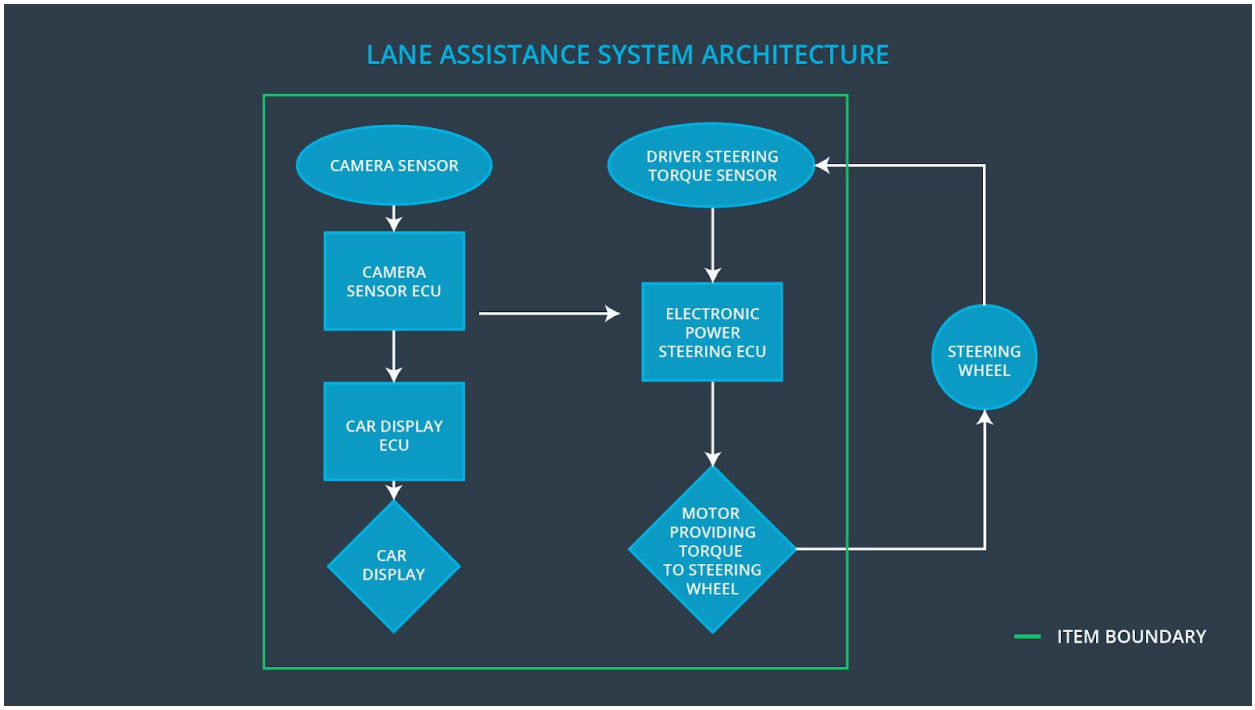
### What are its two main functions? How do they work?

When the driver drifts towards the edge of the lane, two things will happen:

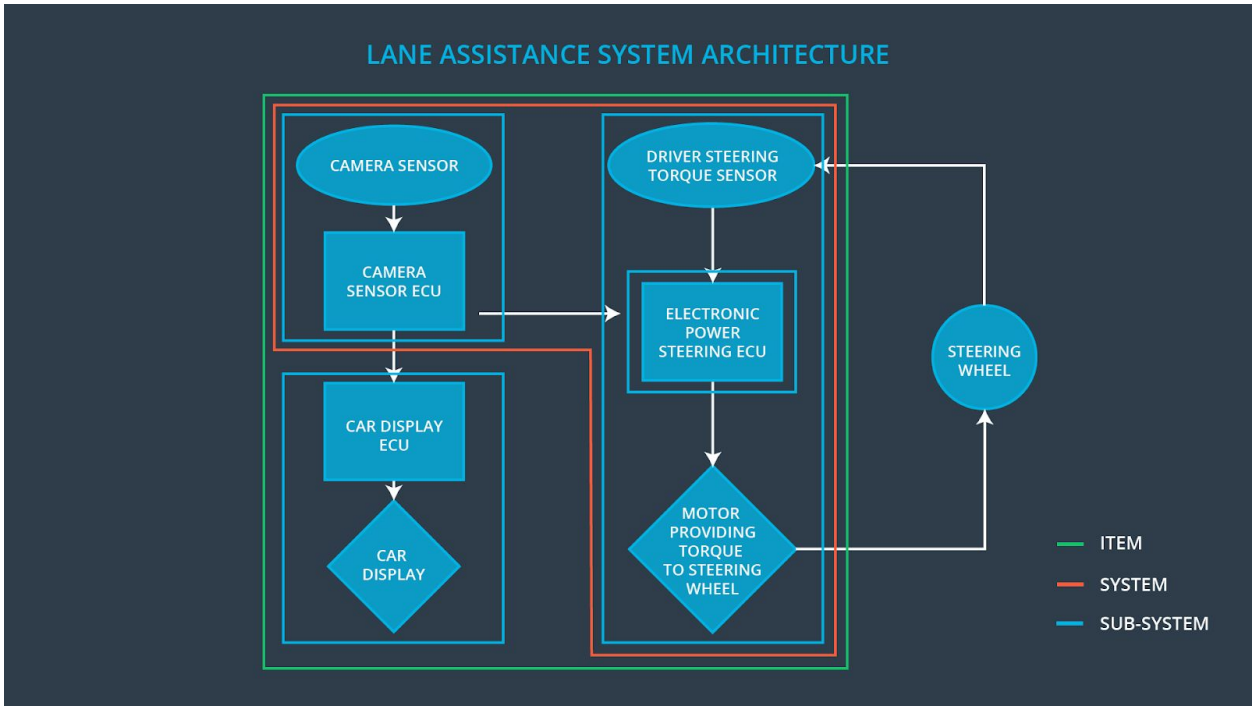
- Lane departure warning function will vibrate the steering wheel to alert the driver.
    - Formally, this engineering requirement given by the product engineering team can be described as: the lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback.
- Lane keeping assistance function will move the steering wheel so that the wheels turn towards the center of the lane
    - Formally, the lane keeping assistance function shall apply the steering torque when active in order to stay in the ego lane.

### What are the boundaries of the item? What subsystems are inside the item? What elements or subsystems are outside of the item?

The following figure shows the architecture of Lane Assistance Item.




At a sub-system level:




The item boundary indicated by the green line includes three subsystems indicated by blue bounding boxes:

| Subsystem | Responsibilities |
|---|---|
| 1. Camera System including camera sensor and ECU | Responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake |
| 2. Electronic Power Steering System including torque sensor, ECU and motor providing torque to the steering wheel | Responsible for measuring the torque provided by the driver and then adding an appropriate amount of torque based on a lane assistance system torque request |
| 3. Car Display System include ECU and display dashboard | Responsible for displaying warnings in the car dashboard in the event of lane departure |

Since functional safety design for ISO26262 involves only electronic and electrical systems only, the item definition does not include the motor control of the steering wheel.

### Which subsystems are responsible for each function?

**For lane departure warning,**

1. **Camera** system detects the departure from the lane

    a. It sends a signal to **electronic power steering** system (EPS) to turn and vibrate the steering wheel
    b. It also requests a warning light in **display dashboard**. This is to indicate that the lane assistance system is active.
2. EPS vibrates steering wheel.

On receiving a signal from the driver to turn off lane departure warning, (for the driver is trying to switch lanes and either switches on “turn” signal or switches off lane assistance button from the dashboard).

1. EPS system stops vibrating the wheel.

**For lane keeping assistance function,**

1. **Camera** system detects lane lines
2. **EPS** has a sensor to detect how much the driver is turning
    a. On noticing a substantial torque which can violate lane keeping, EPS notifies the motor to apply a counter torque to bring the vehicle back towards the center of the ego lane.

This project designs the functional safety for a simplified version of Lane Assistance System. Other factors related to safety plan of Lane Assistance Item are

## Operational and Environmental constraints

1. (Environmental) Lane markings (Source - Wikipedia):

    Lane Departure Warning Systems and Lane Keeping Systems rely on visible lane markings. They typically cannot decipher faded, missing, or incorrect lane markings. Markings covered in snow or old lane markings left visible can hinder the ability of the system.

2. (Operational) Automated control vs. Driver Assistance (Source - Wikipedia):

Lane Departure Warning Systems biggest limitation is that it is not in complete control of the vehicle. The system does not take into account other vehicles on the road and cannot “replace good driving habits”.

3. NHTSA Standards :

    As per NHTSA (National Highway Traffic Safety Administration - US Department of Transportation), it is the onus of technology team to identify the operational design domain(ODD) in which the ADS system is designed to function. These include factors like roadway types, speed range, lighting conditions, weather conditions, and other operational constraints. Environment factors also include sporadic events (e.g., emergency vehicles, construction zones) and weather patterns (tornado / tsunami / avalanche / hurricane / storm etc.)

    Lane Assistance Systems defined in this project  discuss about operational domain of

1. Roadway type - highway driving and country road driving
2. Speed range - Medium and high speeds
3. Lighting conditions - medium / poor lighting conditions
4. Weather conditions - Rainy weather pattern

## Legal Requirements

1. (Source Wikipedia): Lane Assistance Systems also face many legal limitations regarding autonomous driving. As stated previously, this system requires constant driver input. Vehicles with this technology are limited to assisting the driver, not driving the vehicle.
2. Hands-off detection modules have been made mandatory starting April 1, 2018 to ensure LKA systems are not misused by drivers.
3. An autoblog post discusses how EU has passed long-debated legislation that will make nine driver safety systems required fitment on new all cars from 2024.
4. This paper discusses the safety regulations and laws around lane assistance systems for the elderly and the accountability of vehicle / driver for accidents.

In this project, we will use a LKA safety module to ensure drivers donot misuse lane keep assistance function as an auto-pilot functionality.

## National and Internal Standards related to Lane Assistance Systems

1. ISO standards for Lane Assistance Systems
2. ISO standards for PADS (Partially Automated Driver Systems)
3. Different standards' terminology and manufacturing teriminology has been described in this AAA article.
4. A technical report on warnings and driver interface elements presents a survey of international standards on Lane Assistance Systems

## Records of previously known safety-related incidents or behavioral short-falls

1. Consumer report article showcases how lane assistance features helped in reducing accidents
2. This thesis discusses the limitations of study done on lane assistance systems in measuring their efficacy and safety

# Goals and Measures

## Goals

**[Instructions:**
**Describe the major goal of this project; what are we trying to accomplish by analyzing the lane assistance functions with ISO 26262?]**
**The main goal of this project is to reduce the risk of electrical and electronic components of lane assistance system to acceptable levels such that it is ISO26262 compliant. The safety cases built for this project will provide evidence that the lane assistance project has made the vehicle safer to use both sociologically and technically.**

## Measures

**[Instructions:**
**Fill in who will be responsible for each measure or activity. Hint: The lesson on Safety Management Roles and Responsibilities.**

**The options are:**
**All Team Members**
**Safety Manager**
**Project Manager**
**Safety Auditor**
**Safety Assessor**
**]**

| Measures and Activities | Responsibility | Timeline |
|---|---|---|
| Follow safety processes | All Team Members | Constantly |
| Create and sustain a safety culture | All Team Members | Constantly |
| Coordinate and document the | Safety | Constantly |

| | | |
|---|---|---|
| planned safety activities | Manager | |
| Allocate resources with adequate functional safety competency | Project Manager | Within 2 weeks of start of project |
| Tailor the safety lifecycle | Safety Manager | Within 4 weeks of start of project |
| Plan the safety activities of the safety lifecycle | Safety Manager | Within 4 weeks of start of project |
| Perform regular functional safety audits | Safety Auditor | Once every 2 months |
| Perform functional safety pre-assessment prior to audit by external functional safety assessor | Safety Manager | 3 months prior to main assessment |
| Perform functional safety assessment | Safety Assessor | Conclusion of functional safety activities |

# Safety Culture

**[Instructions:**
**Describe the characteristics of your company's safety culture. How do these characteristics help maintain your safety culture. Hint: See the lesson about Safety Culture**
**]**

**The following are characteristics of a good safety culture:**

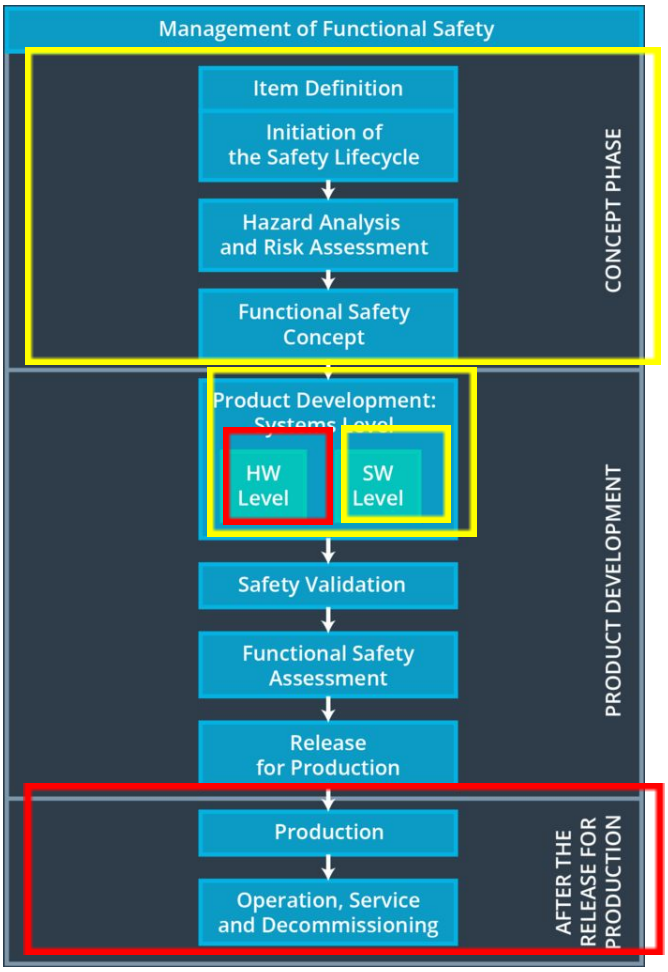
- **High priority**: safety has the highest priority among competing constraints like cost and productivity
- **Accountability**: processes ensure accountability such that design decisions are traceable back to the people and teams who made the decisions
- **Rewards**: the organization motivates and supports the achievement of functional safety
- **Penalties**: the organization penalizes shortcuts that jeopardize safety or quality
- **Independence**: teams who design and develop a product should be independent from the teams who audit the work
- **Well defined processes**: company design and management processes should be clearly defined

- **Resources**: projects have necessary resources including people with appropriate skills
- **Diversity**: intellectual diversity is sought after, valued and integrated into processes
- **Communication**: communication channels encourage disclosure of problems
- **Quality management:** ensure system designed is verified for quality at every step of development phase. This is not a part of ISO26262. However, a good safety culture includes quality management standards adherence (ISO 9001 or IATF 16949) as one of its characteristics.

# Safety Lifecycle Tailoring

**[Instructions:**
**Describe which phases of the safety lifecycle are in scope and which are out of scope for this particular project. Hint: See the Intro section of this document**
**]**

The sections highlighted in yellow bounding boxes will be in-scope for the lane assistance item. The boxes indicated in red are considered out of scope.



# Roles

**[Instructions:**
**This section is here for your reference. You do not need to do anything here. It is provided to help with filling out the development interface agreement section.**
**]**

| Role | Org |
|---|---|
| Functional Safety  Manager- Item Level | OEM |
| Functional Safety  Engineer- Item Level | OEM |
| Project Manager - Item Level | OEM |
| Functional Safety  Manager- Component Level | Tier-1 |
| Functional Safety  Engineer- Component Level | Tier-1 |
| Functional Safety Auditor | OEM or external |
| Functional Safety Assessor | OEM or external |

# Development Interface Agreement

**[Instructions:**
**Assume in this project that you work for the tier-1 organization as described in the above roles table. You are taking on the role of both the functional safety manager and functional safety engineer.**

**Please answer the following questions:**
**]**

1. **What is the purpose of a development interface agreement?**
   A Development Interface Agreement defines the roles and responsibilities during design and production between OEL and Tier-1 and Tier-1 and Tier-2 suppliers involved in developing a product. All involved parties need to agree on the contents of the DIA before the project begins.

   The DIA also specifies what evidence and work products each party will provide to prove that work was done according to the agreement. This agreement also helps in avoiding disputes between the collaborating companies by enlisting who is responsible for any safety-issues post production.

The goal is to ensure that all parties are developing safe vehicles in compliance with ISO 26262.

**2. What will be the responsibilities of your company versus the responsibilities of the OEM? Hint: In this project, the OEM is supplying a functioning lane assistance system. Your company needs to analyze and modify the various sub-systems from a functional safety viewpoint.**

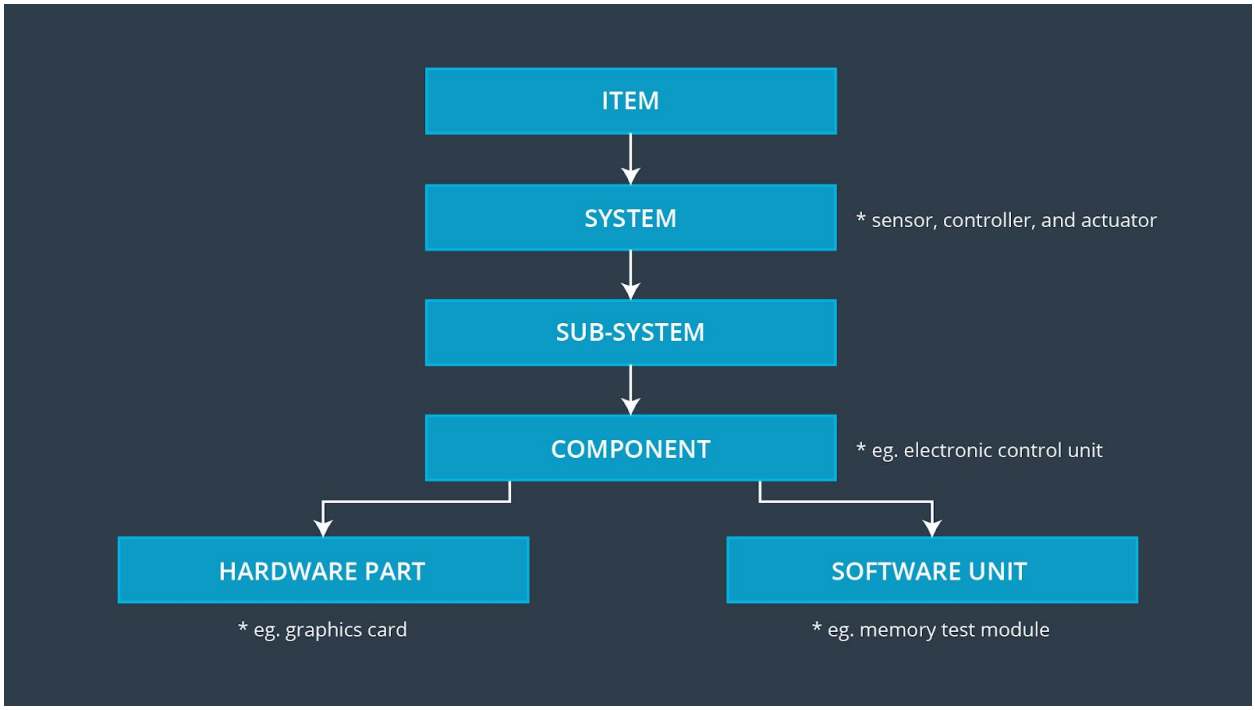
The OEM is providing an overall functionality of lane assistance system. The Tier-1 company involved will only be looking into the components that get affected by the functional safety requirements and design. **The prior exercises of understanding the scope of the project and safety lifecycle tailoring in the flattened V-Model helps in understanding how the OEM owns the larger responsibility of the entire functionality which is out-of-scope of this project while Tier-1 is in-scope phases of the V-Model.**

The subsystems involved in the item are:

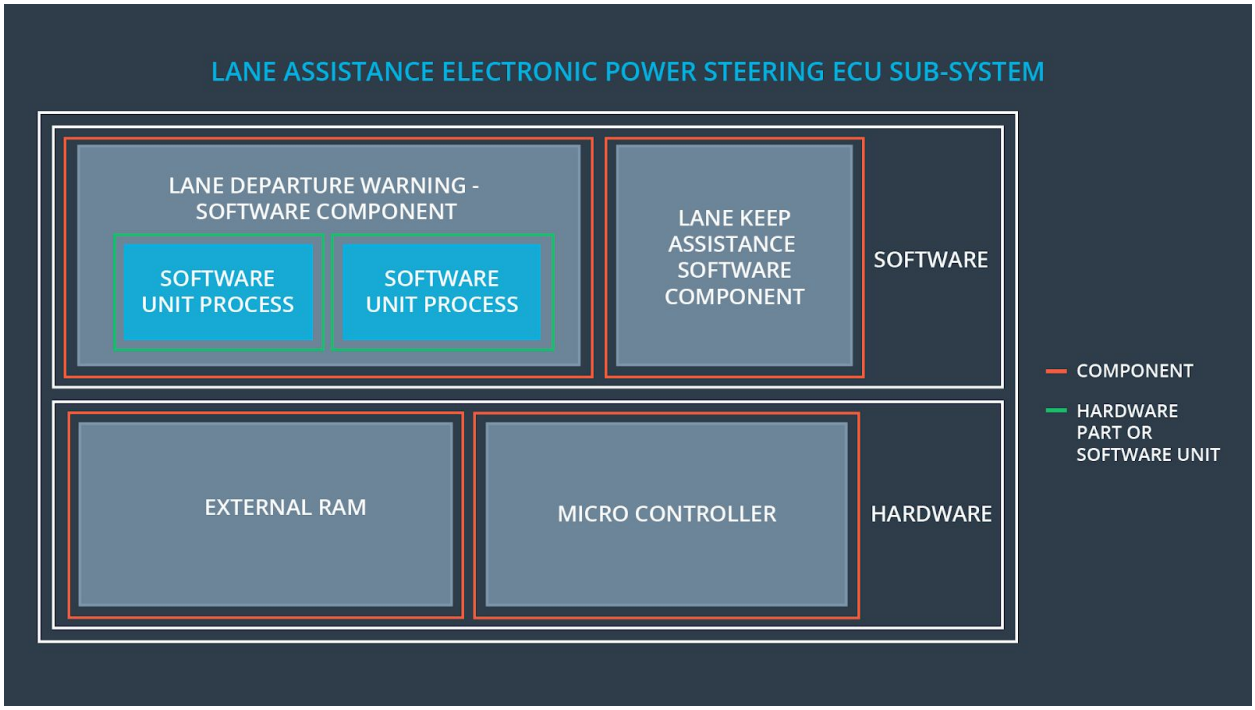
- Camera Subsystem
- Display Subsystem
- Electronic Power steering subsystem

As per the DIA and the safety management role definition, the roles in Tier-1 company are that **of "Functional Safety Manager – Component Level" and "Functional Safety Engineer – Component Level".**

In order to drill down to the Tier-1's responsibilities, it is important to understand the system hierarchy of the item we are interested in. The figure below shows the Full System Hierarchy.




From a safety lifecycle tailoring process, we can exclude the hardware part from consideration here. Looking at a drilled-down version of sub- system architecture, the following figure shows the Electronic Power Steering subsystem at a component level.



The red bounding boxes indicate the different components in the subsystem**. The relevant software components of interest are viz.**

- **Lane Departure Warning Component**
- **Lane Keep Assistance Software Component**

Tier-1 will be involved in the concept phase, product development at system level of subsystem and at the software component level.

# Confirmation Measures

1. **What is the main purpose of confirmation measures?**
   Confirmation measures serve two purposes:
   - that a functional safety project conforms to ISO 26262, and
   - that the project really does make the vehicle safer.

   It is important to ensure that the people who carry out the confirmation measures are independent from the people who actually developed the project
2. **What is a confirmation review?**
   Confirmation review ensures that the project complies with ISO 26262. As the product is designed and developed, an independent person would review the work to make sure ISO 26262 is being followed.
3. **What is a functional safety audit?**
   Functional Safety Audit is an official inspection to ensure that the actual implementation of the project conforms to the safety plan.
4. **What is a functional safety assessment?**
   Functional Safety Assessment assesses a functional safety project and confirms that the plans, designs and developed products actually achieve functional safety.

---

A safety plan could have other sections that we are not including here. For example, a safety plan would probably contain a complete project schedule.

There might also be a "Supporting Process Management" section that would cover "Part 8: Supporting Processes" of the ISO 26262 functional safety standard. This would include descriptions of how the company handles requirements management, change management, configuration management, documentation management, and software tool usage and confidence.

Similarly, a confirmation measures section would go into more detail about how each confirmation will be carried out.