Elektrobit

UDACITY

# Safety Plan Lane Assistance

**Document Version: 1.0**

# Document history

| Date | Version | Editor | Description |
|---|---|---|---|
| 20/5/2018 | 0.1 | Kapil Saini | Initial draft |
| 21/5/2018 | 0.1 | Kapil Saini | Updated Goals and Measures |
| 22/5/2018 | 1.0 | Kapil Saini | Finalized document |
| | | | |
| | | | |

# Table of Contents

# Introduction

## Purpose of the Safety Plan

This document acts as a framework for the functional safety plan for Lane Assistance System. This defines the steps needed to be taken to ensure a functionally safe system (viz. Lane Assistance system) and it also allocates roles and responsibilities to the relevant personnel.

## Scope of the Project

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

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

**Lane Assistance System** assists in keeping keep vehicle in middle of the lane and additionally warn the driver if he drifts towards the edge of lanes without the intent of switching lanes.

The two major functions performed by the lane assistance system are

- **Lane Keeping Assistance**:

  This helps in keeping the vehicle in ego the lane. Ego lane is the lane in which vehicle is currently driving. So if a car is not in the ego lane, this functionality moves the steering wheel by applying steering torque to bring the vehicle back to the center of the lane.

- **Lane Departure warning**

  Lane departure warns the driver whenever he steers off the lane. The lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback. When the vehicle drifts away from the lane by mistake, this vibrates the steering wheel to alert driver.

Subsystems responsible for the working of each function of Lane Assistance System:

- Camera Subsystem
- Car Display subsystem
- Electronic Power Steering subsystem

Lane Assistance System consists **Camera subsystem, Car Display subsystem** and the **Electronic Power Steering subsystem** within its boundaries. **Steering wheel subsystem** lies outside of the boundary (*refer: Figure 1 Lane Assistance System Architecture*)

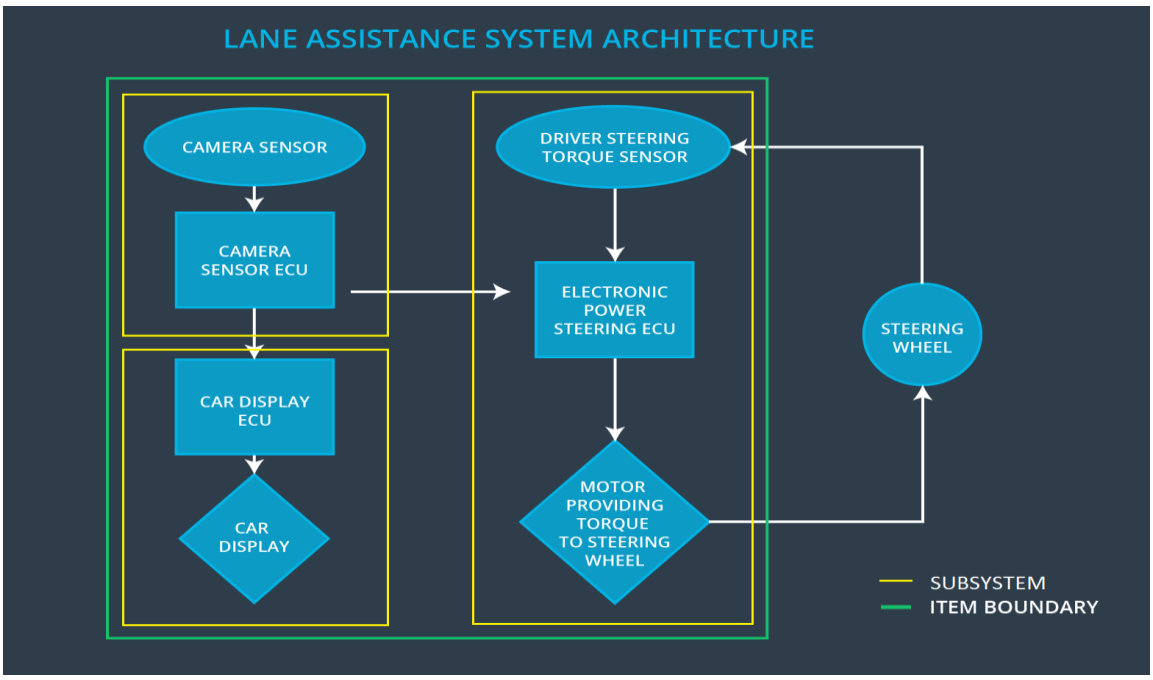


*Figure 1 Lane Assistance system Architecture*

# Goals and Measures

## Goals

The primary goal of safety plan is to determine all possible risks of the lane assistance system. Additionally, to conform to ISO 26262 Standards and ensuring the safe and reliable working of the lane assistance system. Based on the outcome of risk analysis, we can classify safety levels and devise plans to mitigate risks and avoid potential hazards.

## Measures

| 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 planned safety activities | All Team Members | Constantly |
| 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

Some of the characteristics of a good safety culture of an organization:

- **High priority**
  Safety has the highest priority among competing constraints like cost and productivity within an organization.

- **Accountability**
  All design decisions and development activities are documented to ensure accountability and are traceable back to the people and teams who made those decisions.

- **Rewards**
  The organization motivates and supports the achievement of functional safety by rewarding such employees who adhere to such standards.

- **Penalties**
  The organization penalizes employees using shortcuts that jeopardize safety or quality.

- **Independence**
  Teams who design and develop a product are independent from the teams who audit the work.

- **Well defined processes**
  Organization design and management processes are clearly defined and accessible to employees.

- **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.

# Safety Lifecycle Tailoring

For 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

# Roles

| 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

Development interface agreement (DIA) is a mutually agreed agreement between multiple parties that sets forth the expectations from each one. Here the parties in question are the OEM, Tier 1 Suppliers and the Tier 2 Suppliers. DIA ensures that all parties are developing safe vehicles in compliance with ISO 26262.

The responsibilities of the OEM are to define the functionality of the lane assistance system and to conduct the activities in scope of project manager, safety manager and safety engineer in item level.

# Confirmation Measures

The main purpose of confirmation measures is:

- To ensure that a functional safety project conforms to ISO 26262.
- To ensure that the project really does make the vehicle safer

Confirmation review is a measurement process to ensure compliance of project with ISO 26262 standards throughout product design and development stages. An independent review process makes sure ISO 26262 is being followed.

Functional safety audit checks ensure that the actual implementation of the project conforms to the safety plan. Functional safety assessment confirms that plans, designs and developed products actually achieve functional safety.