Elektrobit

UDACITY

# Safety Plan Lane Assistance

**Document Version:** [Version]

**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 |
|---|---|---|---|
| 25/12/2018 | 1.0 | Ahmed Desoky | Safety plan for Lane Assistance project |
| | | | |
| | | | |
| | | | |
| | | | |

# 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

This documents defines the overall framework for a Lane Assistance item.

## 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

The item under safety analysis is a simpliflied version Lane Assistance system.
It consists of two main functionalities:

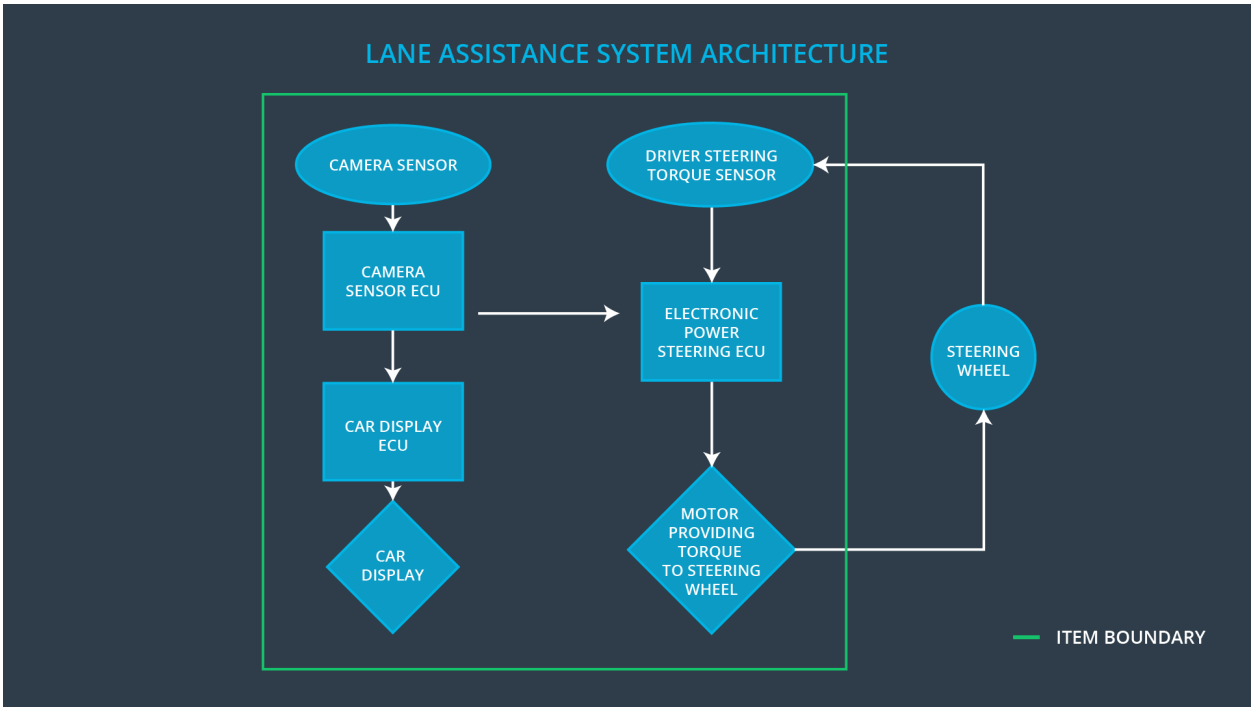
- Lane Departure Warning (LDW) : when the driver goes near to the edge of the lane without turning on the turn signal, the steering wheel vibrates to warn the driver
- Lane Keeping Assistance (LKA) : This feature applies a torque to the steeting wheel to have the car back the ego lane (the lane where the car is driving originally)

Our system functionalites are implemented using the follwing sub-systems:

- Camera sub-system: consists of two main components:

    - Camera sensro
    - Camera ECU
- Electronic power steering sub-system: consists of three compenents:
    - Driving steering torque sensor
    - Electronic power steering ECU
    - Motor providing torque to the steering wheel
- Car display sub-system: consists of two compenents:
    - Car display
    - Car display ECU

The following diagram shows the interaction between the different sub-systes:




When the camera sensor senses that the car is going to leave the lane or going to the edge of the the lane, the camera ECU sends a signal to the steering power sub-system to vibrate the steering wheel.
In the meantime, the camera ECU sends a singal to the car display sub-system to warn the driver using an indicator in the dashboard.
If the driver uses the turn signal, the lane assistance system deactivates so that the car can leave the lane normally.
The driver can turn off the sustem using the button in the dashboard.

The electronic steering power sensor detects how much the driver is turning.

The electronic steering power ECU will add extra torque to the steering wheel to get the car back the lane center.
This torque is applied via a motor in the electronic steering power sub-system.

The driver is still expected to have his/her both hands on the steering wheel all the time.

The Lane Assistance systems does not include the following functionalities:

- Adaptive Cruise Control
- Blind Spot Detection
- Closing Vehicle Warning
- Pedestrian Detection
- Rear Crash Warning
- Emeregency Braking

# Goals and Measures

## Goals

The goals of this project are:

- Identify risks and hazardous situations in the Lane Assistance system due to malfunctions
- Evaluation risks of the hazardous situations
- Lower the risks to acceptable levels

## 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

Our organization applies the following policies for ensuring and appying a safety culture within all our products and projects:

- High Priority: Safey has the highest priority among other values such as cost and productivity
- Accountabilty: Our organization is using software tools and processes that ease the traceability of decisions with their makers and teams.
- Rewards: Our organization rewards for following and fulfulling functional safety
- Penalties: Our organization penalizes for violations of functional safety rules
- Independency: Our organization makes sure the design and development teams are independent audits teams.
- Well-defined process: Each engineer working in our organization is introduced and trained to our process. We make sure that this process is well-defined to each individual.
- Resources: Our organization provides the necessary resources for each project either internally or externally.

# Safety Lifecycle Tailoring

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

# 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

This section defines the roles and responsiblities between the different parties involved in the Lane Assistance item to ensure compliance to the ISO 26262:

- **Functional Safety  Manager- Item Level:** Pre-audis, plans the development phase of Lane Assistance item
- **Functional Safety  Engineer- Item Level:** Develops prototypes, integrates sub-systems to the Lane Assistance item from functional safety perspective.
- **Project Manager - Item Level:** Allocates resources needed to the project
- **Functional Safety  Manager- Camera Component Level:** Pre-audis, plans the development phase of camera sub-system
- **Functional Safety  Engineer- Camera Component Level:**  Develops prototypes, integrates sub-systems to the camera sub-system from functional safety perspective.
- **Functional Safety  Manager- Steering Power Component Level:** Pre-audis, plans the development phase of steering power sub-system
- **Functional Safety  Engineer- Camera Component Level:**  Develops prototypes, integrates sub-systems to the steering power sub-system from functional safety perspective.
- **Functional Safety  Manager- Car Display Component Level:** Pre-audis, plans the development phase of car display sub-system
- **Functional Safety  Engineer- Car Display Component Level:**  Develops prototypes, integrates sub-systems to the car display sub-system from functional safety perspective.
- **Functional Safety Auditor:** Makes sure the project follows the safety plans
- **Functional Safety Assessor:** Makes the final judge whether the project increases safety or not.

# Confirmation Measures

The purpose of confirmation measures:

- Ensures that the Lane Assistance project is following the ISO26262.
- Ensures that the Lane Assistance project increases safety

As the project in under development, an independent person would review the designs and development to make sure that ISO 26262 is followed.
A functional safety audit makes sure that the actual implmentation is following the ISO 26262.
A function safety assessment will be done to judge the project if it is safe or not.

---

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.