Elektrobit

UDACITY

# Safety Plan Lane Assistance

**Document Version:** 1.1

Template Version 1.0, Released on 2017-06-21

# Document history

| Date | Version | Editor | Description |
|---|---|---|---|
| 3/24/18 | 1.0 | Yury Astashonok | First revision |
| 4/3/18 | 1.1 | Yury Astashonok | Updated Goals and Measures |
| | | | |
| | | | |
| | | | |

# Table of Contents

# Introduction

## Purpose of the Safety Plan

The purpose of this safety plan is to provide an overall framework for the Lane Assistance item, and to assign goals and responsibilities for the functional safety for this 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 Lane Assistance item helps the driver to avoid moving out of the current lane unintentionally. It alerts the driver when the vehicle steers out of the lane with an oscillating steering torque and applies counter-steering to direct the vehicle towards lane center.

Lane Assistance item performs two main functions:

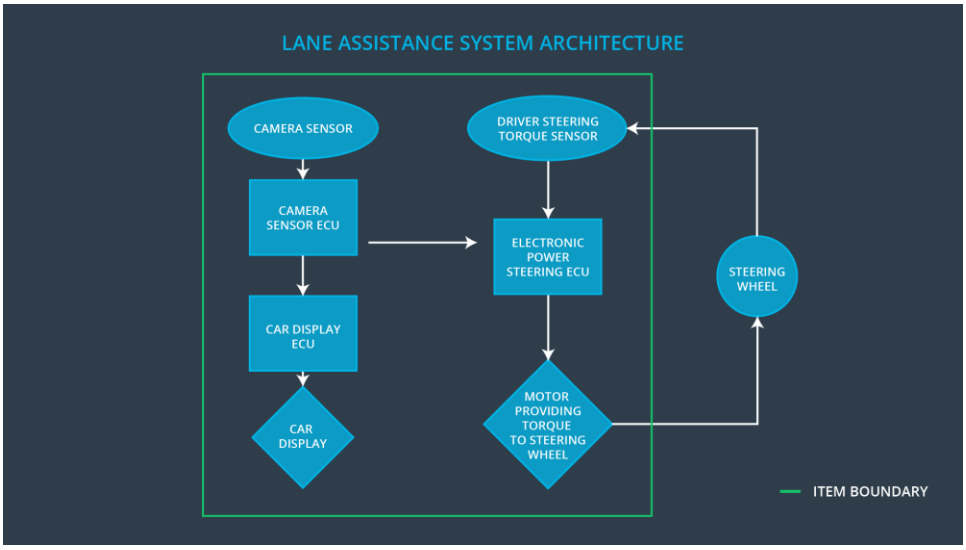
1. Lane departure warning.
2. Lane keeping assistance.

The lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback.

The lane keeping assistance function shall apply the steering torque when active in order to stay in ego lane.

Lane Assistance item contains the following three subsystems:

1. Camera system;
2. Electronic Power Steering system;
3. Car Display system.




# Goals and Measures

## Goals

The major goal of the project is to avoid accidents caused by Lane Assistance item malfunction by reducing risk to acceptable level. This is achieved by ensuring that the Lane Assistance functionality meets ISO 26262 safety standard. In order to meet the goal the following activities are identified:

1. Provide hazard analysis and risk assessment;
2. Identify functional safety requirements;
3. Derive technical safety requirements;
4. Define software requirements;

## 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 | Safety Manager | 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

Safety is an important part of our culture, and we strive to maintain high safety standards by implementing the following key characteristics:

1. Safety is the highest priority. We do not compromise safety for the sake of cost or productivity;
2. Every design and management process is clearly defined with an owner who is fully accountable for process safety when making design decisions;
3. Safety audits are performed regularly by auditors independent from developers. We praise individuals for achieving functional safety;
4. We ensure projects have enough resources and teams are staffed with experts having necessary skills; We value intellectual diversity and encourage leaders to seek for it;
5. Efficient communication is important for making informed decisions; we ask teams to open and maintain communication channels with all stakeholders.

# Safety Lifecycle Tailoring

Lane Assistance project extends an existing Advanced Driver Assistance System with new features, Lane Departure Warning and Lane Keeping Assistant. New functionality impacts only certain project phases, therefore not all of the phases of the safety lifecycle are in the scope for this project. Particularly, the following safety lifecycle phases are in scope for the project:

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

Keeping certain phases out of the scope of the project allows to focus only on the new parts of the product.

# 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

The purpose of Development Interface Agreement is to define roles and responsibilities of each party of the development process. All involved parties need to agree on the conent of the DIA before the project begins.

Activities and processes to be performed by the OEM:

1. Develop item prototype
2. Integrate components provided by the Tier-1 supplier into the item
3. Perform regular functional safety audits on the item level

Activities and processes to be performed by the Tier-1 supplier:

1. Tailor the safety lifecycle on the component level
2. Plan the development phase on the component level
3. Develop components prototype
4. Allocate resources on the component level

# Confirmation Measures

The main purpose of confirmation measures is to ensure that the project

1. conforms to ISO 26262 standard;
2. increases vehicle safety.

Three primary confirmation measures will be used:

1. Confirmation review;
2. Functional safety audit;
3. Functional safety assessment.

Confirmation review ensures that the project complies with ISO 26262.

Functional safety audit is performed to make sure that the implementation of the project conforms the safety plan described in this document.

Functional safety assessment plans, designs and developed products achieve functional safety.