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 |
|---|---|---|---|
| 10/04/2017 | 1.0 | Ibis Prevedello | First draft |
| 10/18/2017 | 1.1 | Ibis Prevedello | Correction of responsibility |

# Table of Contents

# Introduction

## Purpose of the Safety Plan

This safety plan intends to document and show in a detailed way how the Lane Assistance was designed and tested. Besides, it will also assign roles, responsibilities and show how the best practices were followed to achieve a better quality and minimize risks as much as possible.

## 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 is important to alert the driver when its non-intentionally leaving a lane by vibrating the steering wheel and/or with sound and visual alarms. Besides, the Lane Assistance also works with the Adaptive Cruise Control to maintain the car inside a line actuating on the steering wheel.

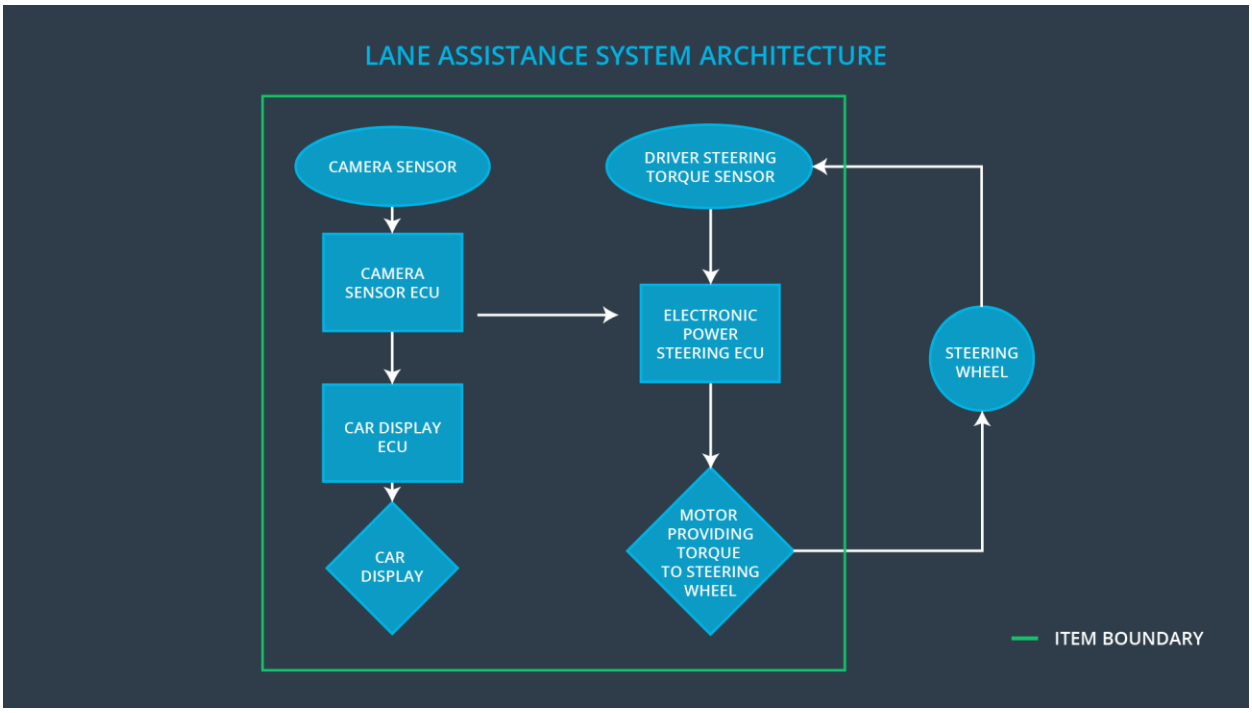


*Figure 1 - Lane assistance system architecture*

The two main functions of this system are the “lane departure warning” and the “lane keeping assistance”.

The lane departure warning is active when the car starts deviating from the lane without to signal a left or right turn. It alerts the driver by vibrating the steering wheel, a sound effect and a visual effect on the panel.

The lane keeping assistance actively makes the car to stay on the middle of the center lane by applying a counter-steering force on the steering wheel, if the driver doesn’t proactively correct the vehicle’s course after the alerts from the lane departure warning.

For the lane departure warning, the subsystem used is the camera and the alert displays (panel, sound and steering wheel vibration). For the lane keeping assistance, it uses also the camera and the steering wheel.

The boundaries of the lane assistance include the camera sensor, camera sensor ECU, car display ECU, car display, driver steering torque sensor, electronic power steering ECU and motor providing torque to steering wheel. For the element that are outside of the system is the steering wheel.

# Goals and Measures

## Goals

The goal of this document is to define the lane assistance safety plan in accordance with the ISO 26262.

## Measures

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

Here are some 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

# Safety Lifecycle Tailoring

The safety lifecycle phases that are in scope of this project are concept phase, product development at the system level and product development at the software level.

On the other hand, product development at the hardware level and production and operation are out of scope.

# 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

A DIA (development interface agreement) defines the roles and responsibilities between companies involved in developing a product. All involved parties need to agree on the contents of the DIA before the project begins. It also specifies what evidence and work products each party will provide to prove that work was done according to the agreement. Finally, it ensures that all parties are developing safe vehicles in compliance with ISO 26262.

The responsibility of our company is to analyze and modify the various sub-systems from a functional safety viewpoint that meets the requirements needed by the OEM for the functioning lane assistance system.

# Confirmation Measures

There are two main purpose of confirmation measures, that a functional safety project conforms to ISO 26262, and that the project really does make the vehicle safer.

**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.

**Functional safety audit**

Checking to make sure that the actual implementation of the project conforms to the safety plan is called a functional safety audit.

**Functional safety assessment**

Confirming that plans, designs and developed products achieve functional safety is called a functional safety assessment.