Elektrobit

UDACITY

# Safety Plan Lane Assistance

**Document Version:** [Version]

Template Version 1.0, Released on 2017-06-21

# Document history

| Date | Version | Editor | Description |
|---|---|---|---|
| 01/10/2017 | 1.0 | Pedro Lizana | First version of document. |
| | | | |
| | | | |
| | | | |
| | | | |

# Table of Contents

# Introduction

## Purpose of the Safety Plan

The purpose of the safety plan is to provide an overall framework to asses the functional safety of the Lane Assistance item, as well as to assign safety management roles and responsibilities related to 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

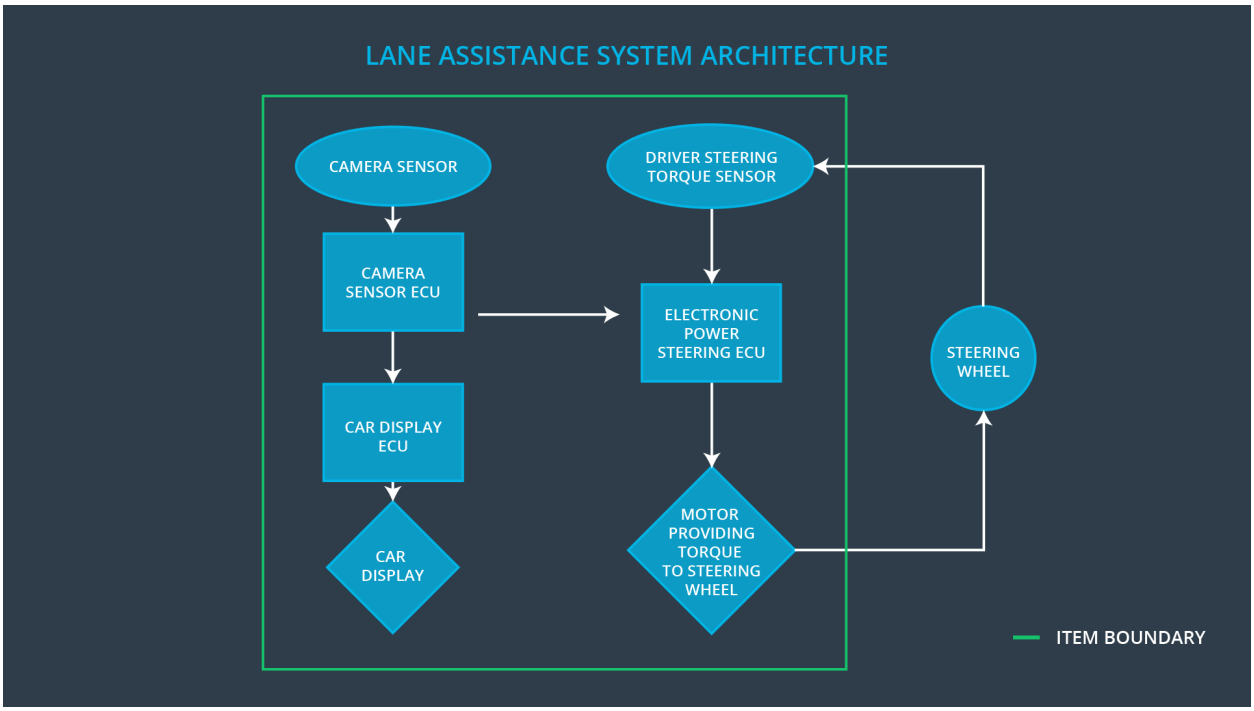
The Lane Assistance item warns the driver that it has departed its ego (current) lane activating the turn light signal, and tries to steer back the vehicle towards the center of the lane.

The Lane Assistance system will have two functions:

1. Lane departure warning (LDW): this function shall apply and oscillating steering torque to provide the driver a haptic feedback.
2. Lane keeping assistance (LKA): this function shall apply the steering torque when active in order to stay in ego (current) lane.

The camera subsystem, the electronic power steering subsystem, and the car display subsystem are all responsible for both functions.

The lane assistance system architecture including the item boundaries can be observed in the following diagram.



# Goals and Measures

## Goals

The goal of this project is to identify high risk situations and hence find ways to lower this risk to reasonable levels. For this we will comply with the ISO 26262 standard which only covers electronic and electrical malfunctions in passenger vehicle systems.

## 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

Our safety culture promotes the following characteristics:

- **Safety 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

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

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.

The DIA also specifies what evidence and work products each party will provide to prove that work was done according to the agreement. Hence it avoids disputes and solves liability issues.

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

As a Tier-1 supplier of cameras for lane assistance features, the responsibility of our company is to provide cameras that comply with functional safety standards. This means, cameras that are able to store and transfer pictures to the OEM lane assistance system with a sufficient enough resolution (acceptable picture quality) and frequency (acceptable failure rates).

# 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.

The people who carry out confirmation measures need to be independent from the people who actually developed the project.

A **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.

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

A **functional safety assessment** is confirming that plans, designs and developed products actually achieve functional safety is called a functional safety assessment.
.