Elektrobit

UDACITY

# Safety Plan Lane Assistance

**Document Version: [1.0]**

**Template Version 1.0, Released on 2017-06-21**

## Document history

| Date | Version | Editor | Description |
|---|---|---|---|
| 12/11/2018 | 1.0 | MElSobky | Initial Version |
| | | | |
| | | | |
| | | | |
| | | | |

# Table of Contents

# Introduction

## Purpose of the Safety Plan

A safety plan provides an overall framework for a functional safety project and to provide an overall framework for the lane assistance item and to assign role and responsabilities for functional safty 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

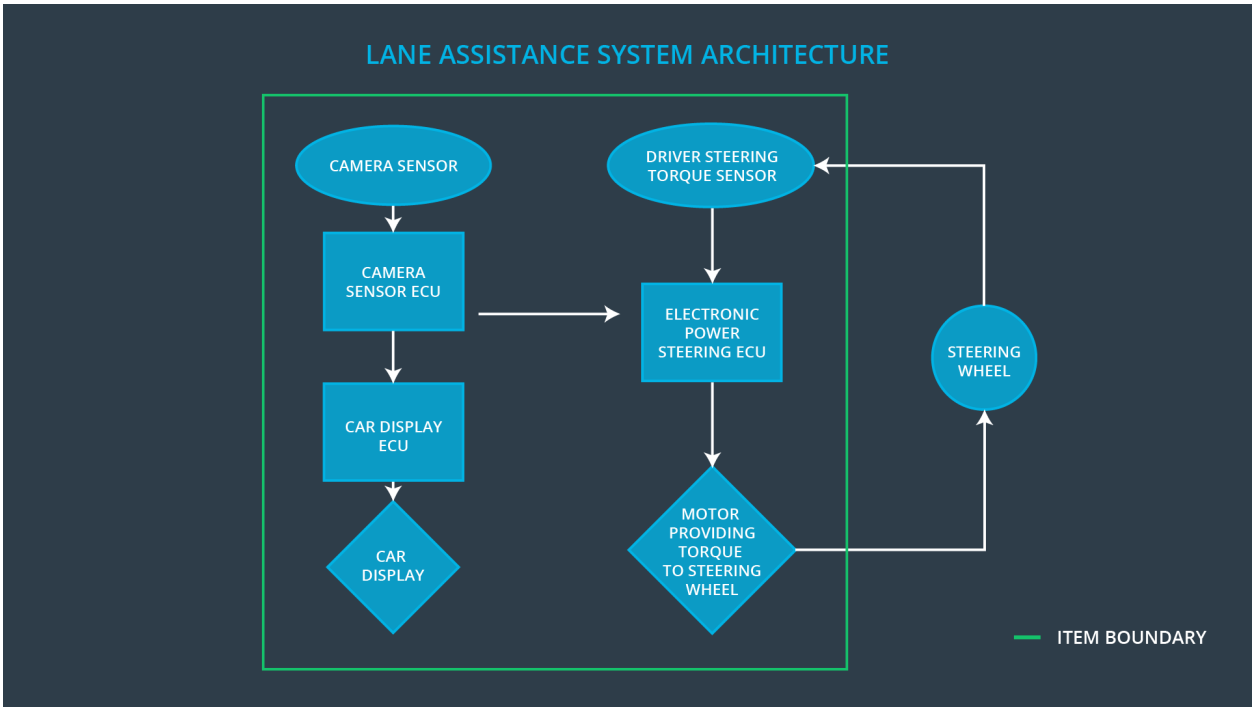
The lane assistance system item alerts the driver that the vehicle has accidentally departed it's lane, and attempts to steer the vehicle back toward the center of the lane.

The Lane Assistance System will have two 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

The Camera sub-system , Electronic Power Steering sub-system, Car Display sub-system are all responsible for each of the functions.



# Goals and Measures

## Goals

The major goal of this project is to assure safe and reliable operation of the EPS components of the lane assistance functions according to ISO 26262 by identfying hazards, measruring risks and applying system engineering to lower the risk to a reasonable level.

## Measures

| Measures and Activities | Responsibility | Timeline |
|---|---|---|
| Follow safety processes | everybody | Constantly |
| Create and sustain a safety culture | everybody | 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

We give safety the highest priority among competing constraints like cost and productivity. That's why our processes ensures accountability such that design decisions are traceable back to the people and teams who made the decisions.The organization motivates and supports the achievement of functional safety and penalizes shortcuts that jeopardize safety or quality. Also teams who design and develop a product are independent from the teams who audit the work.

Our design and management processes are clearly defined and projects have necessary resources including people with appropriate skills taking into account intellectual diversity that is valued and integrated into the processes. We encourage disclosure of problems through our .communication channels

# Safety Lifecycle Tailoring

When dealing with a new implementation the entire safety lifecycle including all the phases mentiond in chapter Scope of the Project have to be to followed and documented. Hardware components and respective product development, as well as the final production and operations phase are not part of this project.

# 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 defines the roles and responsibilities between OEM and Tier-1. The DIA also specifies what evidence and work products OEM and Tier-1 will provide to prove that work was done according to the agreement.

The OEM is supplying a functioning lane assistance system. Tier-1 will analyze and modify the LDW and LKA from a functional safety viewpoint.

The following are major sections of a DIA:

- Appointment of customer and supplier safety managers
- Joint tailoring of the safety lifecycle
- Activities and processes to be performed by the customer; activities and processes to be performed by the supplier
- Information and work products to be exchanged
- Parties or persons responsible for each activity in design and production

- Any supporting processes or tools to ensure compatibility between customer and supplier technologies

# Confirmation Measures

Confirmation measures serve two purposes:

- that a functional safety project conforms to ISO 26262
- 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 is* 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 is* Confirming that plans, designs and developed products actually achieve functional safety is called a functional safety assessment.