Elektrobit

UDACITY

# Safety Plan Lane Assistance

**Document Version:** [1.0]

# Document history

| Date | Version | Editor | Description |
|---|---|---|---|
| 2019.06.28 | 1.0 | Yuan.J | Initial Version |
| | | | |
| | | | |
| | | | |
| | | | |

# Table of Contents

# Introduction

## Purpose of the Safety Plan

The purpose of the Safety Plan is to provide the overall framework for the lane Assistance Item, to manage and guide the execution of the safety activities of the project including dates, milestones, tasks, deliverables, responsibilities and resources. It assigns roles and responsibilities for 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 alert the driver that the vehicle has accidentally departed its lane and attempts to steer the vehicle back toward the center of the lane.

The Lane Assistance System will have two functions:

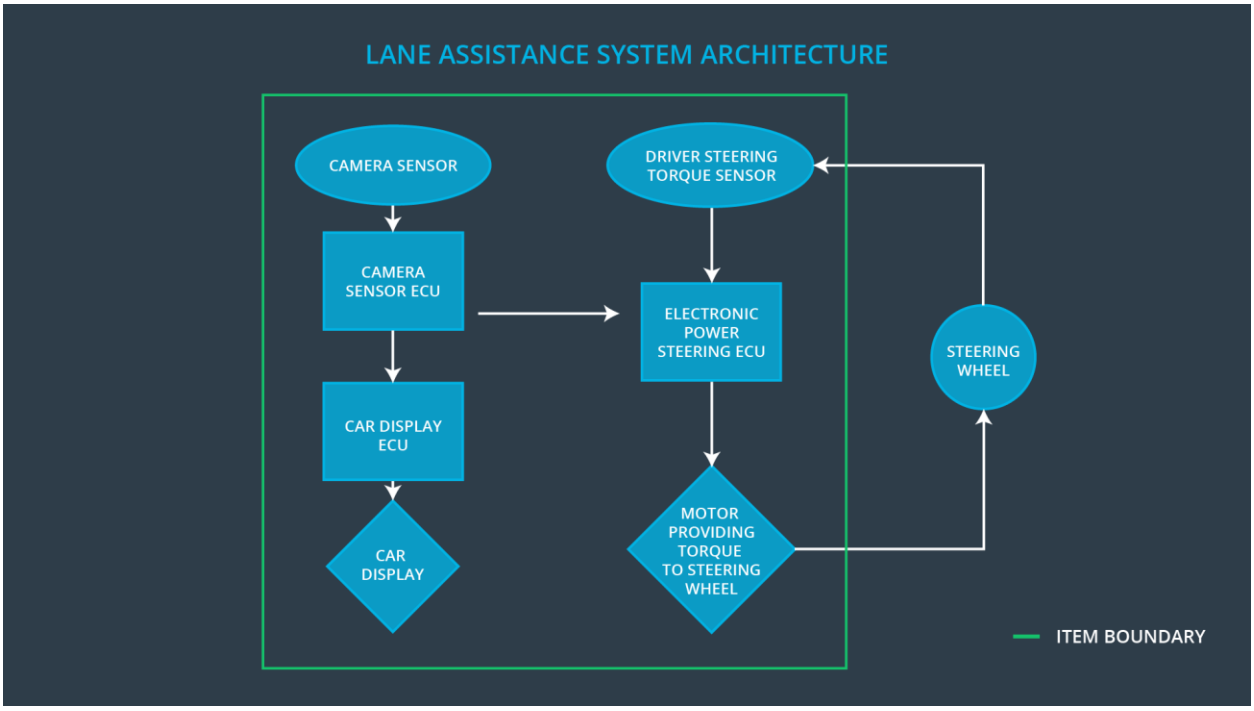
1. Lane departure warning
2. Lane keeping assistance

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.

Inside the item lane assistance system are the following subsystems:

- Camera subsystem,
- Electronic power steering subsystem
- Car display system.

The boundaries of the item are shown as below.



# Goals and Measures

## Goals

The main goal of the Lane Assistance Functional Safety Plan is to identify risk hazardous situations in the project and reduce risk of hazardous failures 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 | 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

The Safety Culture of our company includes the following aspects

- **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 functional safety initial plan, the ISO 26262 standard have been tailored to include the following safety lifecycle phases 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

We welcome our selected Tier-1 supplier to help us tailor the ISO 26262 standard further tos build safe vehicles

# 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 purpose of a DIA is shown below.

- Avoid disputes during the planning and development of a product.
- Resolve the issues of liability. It
- Makes clear who should fix safety issues as well.

Responsibility of OEM

- Appointment of customer safety managers in item level
- Joint tailoring of the safety lifecycle
- Activities and processes to be performed by the customer;
- Information and work products to be exchanged with supplier
- Parties or persons responsible for each activity in design and production
- Any supporting processes or tools to ensure compatibility with supplier technologies

Responsibility of our company as the safety manager (Tier1)

- Appointment of supplier safety managers in component level
- Joint tailoring of the safety lifecycle
- Activities and processes to be performed by the supplier
- Information and work products to be exchanged with customer
- Parties or persons responsible for each activity in design and production
- Any supporting processes or tools to ensure compatibility with customer technologies

# 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.

**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 actually achieve functional safety is called a functional safety assessment.