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 |
|---|---|---|---|
| 06/21/19 | 1.0 | Adam Gotlib | First draft |
| 06/23/19 | 1.1 | Adam Gotlib | Removed template-specific parts of the document |
| | | | |
| | | | |
| | | | |

# Table of Contents

# Introduction

## Purpose of the Safety Plan

The Safety Plan provides groundwork and context for the entire safety case. It shows which vehicle system will be under consideration and defines roles, responsibilites, and processes required to implement appropriate functional safety measures.

## 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

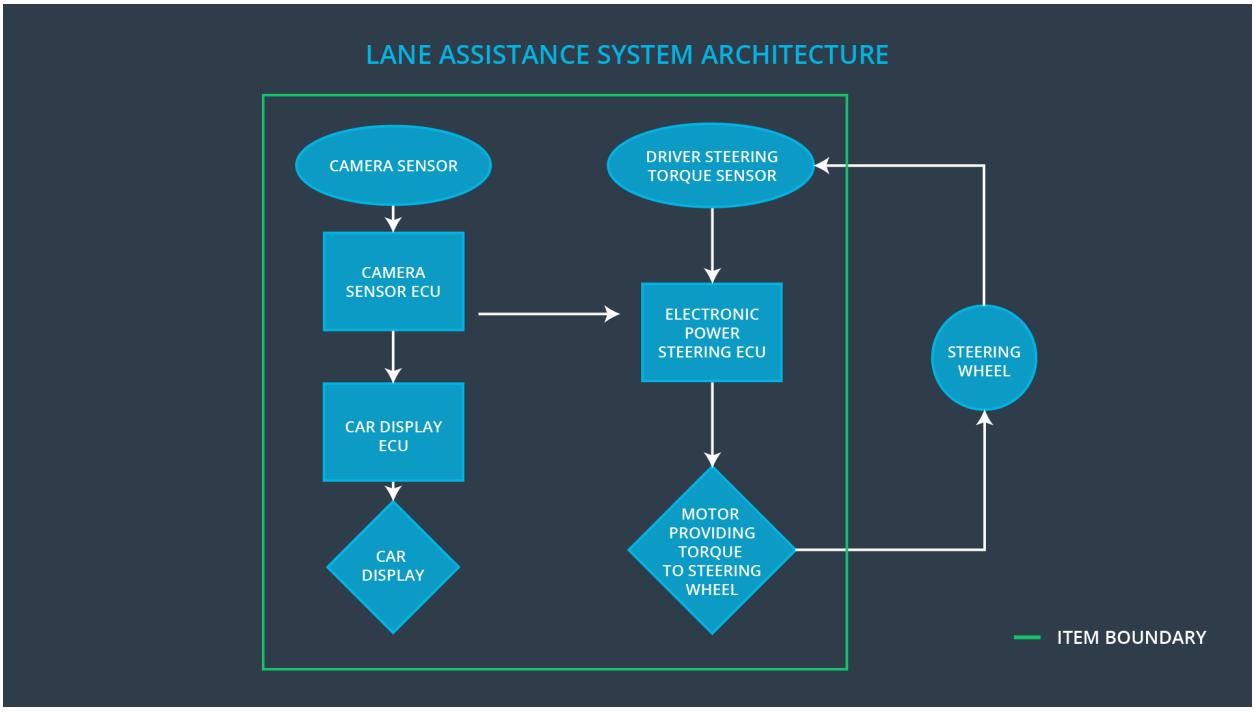
# Item Definition

The item in question is a **Lane Assistance (LA)** system whose purpose is to prevent a distracted driver from unintentionally leaving their current lane.

The two main functions of the LA system are **Lane Departure Warning (LDW)** function and **Lane Keeping Assistance (LKA)** function. Both of the functions activate when an unintentional lane departure is detected.

The LDW provides the driver with a haptic feedback in the form of oscillating torque applied to the steering wheel in order to direct the driver's attention back on the road.

At the same time, LKA applies an additional torque to the steering wheel in order to move the vehicle closer to the center of the lane.



The above diagram provides an overview of the LA system architecture. Here, three subsystems can be distinguished:

- **Camera** subsystem, which detects lane departure using specialized computer vision techniques. Additionally, state of the turn signals is used to asses intentionality of the maneuver;
- **Electronic Power Steering (EPS)** subsystem, which measures the torque provided by the driver and then adds an appropriate amount of torque if an unintentional lane departure is detected;
- **Car Display** subsystem, which notifies the driver of functioning of the system.

  The three aforementioned subsystem form entirety of the system. Note the actual steering wheel is not part of the system, but only the actuator that applies torque to it.

# Goals and Measures

## Goals

The goal of this project is to identify and mitigate main hazards associated with possible malfunctioning of electronic and electric elements of the LA system. The item at hand has direct impact on the driving task, which is why safety is a critical part of the design. By working within framework of the widely recognized ISO 26262 standard, we can thus ensure high quality of functional safety management.

## 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 Assesor | Conclusion of functional safety activities |

# Safety Culture

The company's safety culture can be desctibed by the following characteristics:

- **High priority**: safety takes precedence over other project constraints;
- **Accountability**: every decision can be traced back to people who made it; this way the blur of responsibilities related to safety can be avoided;
- **Rewards** and **Penalties**: a solid incentive system is formed to encourage achievement of functional safety;
- **Independence**: to reduce bias and make sure the development teams' interests (which e.g. may involve finishing the project within prescribed timeframe) are not in conflict with fuctional safety;
- **Well defined processes:** to make it clear for everyone involved what steps are required to achieve functional safety; also to be able to verify how the processes have been conducted afterwards;
- **Diversity**: to reduce bias and include important insight from different experts at the company;
- **Communication**: to make sure no critical information relating to functional safety gets stuck on the way.

# Safety Lifecycle Tailoring

The following phases of the safety lifecycle are in scope of this particular project:

- Concept phase
- Product Development at the System Level
- Product Development at the Software Level

# 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 a development interface agreement is to delineate responsibilities in a customer–supplier relationship and ensure all parties are developing save vehicles in compliance with ISO 26262.

Responsibilities of my company:

- Planning, coordinatinfg, and documenting of the development phase of the safety lifecycle;
- Product development, integration and testing on software level;

Responsibilities of the OEM:

- Planning, coordinatinfg, and documenting of the development phase of the safety lifecycle;
- Ensuring that the design and production implementation conform to the safety plan and ISO 26262;
- Performance of functional safety assesment to judge whether functional safety is being achieved.

# Confirmation Measures

The purpose of the confirmation measures can be divided into three parts, which are:

- validating that processes comply with the ISO 26262 standard;
- validating that the project does improve overall safety;
- verifying that the project execution is following the safety plan.

**Confirmation review** involves an independend person reviewing work as the product is being designed and developed, to make sure ISO 26262 is being followed.

A **functional sefety audid** serves the purpose of verification that the actual implementation of the project is going according to the safety plan.

A **functional safety assesment** serves the purpose of balidation that the project does achieve good level of functional safety.

]

A safety plan could have other sections that we are not including here. For example, a safety plan would probably contain a complete project schedule.

There might also be a "Supporting Process Management" section that would cover "Part 8: Supporting Processes" of the ISO 26262 functional safety standard. This would include descriptions of how the company handles requirements management, change management, configuration management, documentation management, and software tool usage and confidence.

Similarly, a confirmation measures section would go into more detail about how each confirmation will be carried out.