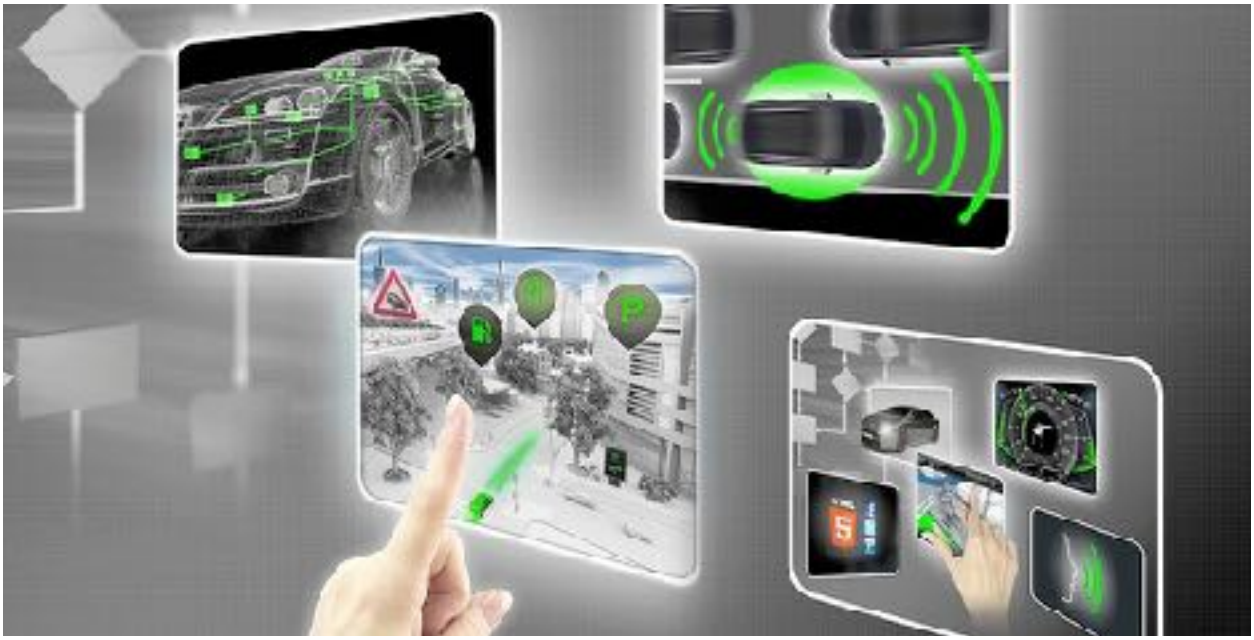
Elektrobit

UDACITY

# Safety Plan Lane Assistance

**Document Version: 1.0**

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



# Document history

| Date | Version | Editor | Description |
|---|---|---|---|
| 02-18-2018 | 0.1 | Michael Bachmann | Added purpose of the safety plan, measures, safety culture, safety lifecycle tailoring, DIA and confirmation measures. |
| 02-20-2018 | 0.2 | Michael Bachmann | Added Item Definition and Goal. Updated Safety Lifecycle Tailoring. |
| 03-06.2018 | 1.0 | Michael Bachmann | First attempt for submission |
| | | | |
| | | | |

# Table of Contents

# Introduction

## Purpose of the Safety Plan

Vehicles are complex systems with both sociological and technical requirements. Defining a safe vehicle requires more than a methodical analysis of hardware and software components. To achieve this goal, the Safety Plan defines and outlines the steps to achieve functional safety:

- The scope of the project
- Deliverables of the project
- The particular vehicle system that will be under analysis (Item Definition)
- Goals and measures
- Safety culture
- Safety lifecycle tailoring
- Roles
- Development interface agreement
- Confirmation 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

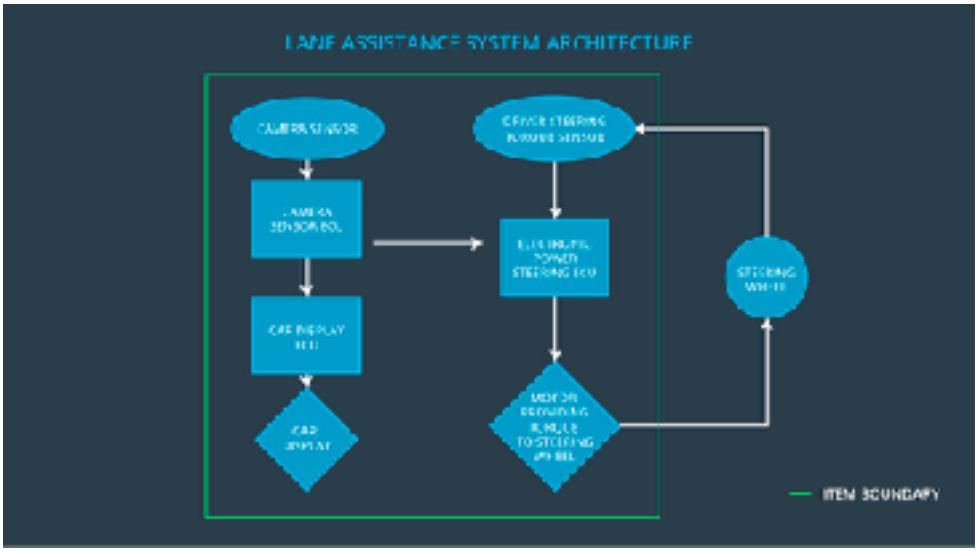
This safety plan covers the Lane Assistance System which is an Advanced Driver Assistance System (ADAS). The Lane Assistance System alert the driver to potentially dangerous situations and take control over the vehicle to prevent accidents from occurring. To do this the item has two main functions:

- Lane departure warning
- Lane keeping assistance

The lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback if the car drifts towards the edge of the ego lane.  The lane keeping assistance function shall apply the steering torque when active in order to stay in ego lane. Both functions will act automatically and additionally to the vibrating steering wheel a warning light shall be displayed on in the car display dashboard. The item consists of three subsystems with their own components:

- Camera subsystem consisting of 2 components:
  - Camera sensor
  - Camera sensor Electronic Control Unit (ECU)
- Electronic power steering subsystem consisting of 3 components
  - Driver Steering Torque Sensor
  - Electronic Power Steering ECU
  - Motor Providing Torque to Steering wheel
- Car display subsystem consisting of 2 components:
  - Car Display ECU
  - Car Display

The following diagram shows the interaction between the three subsystems:



The camera subsystem is responsible for detecting and monitoring the position of the car in the ego lane and informing the car display and electronic power steering subsystem if the car drifts towards the edge. The electronic power steering subsystem detects how much the driver is already turning the vehicle and add a extra torque required to get the car back towards the center. The car display subsystem is only responsible for displaying the warning if necessary.

The Lane Assistance Systems deactivates itself if the driver uses a turn signal. Another way to turn the system off is to use a button on the dashboard.

# Goals and Measures

## Goals

The project goals are:

- Identify risk and hazardous situations in the Line Assistance System components malfunction causing injuries to a person.
- Evaluate the risk of hazardous situations.
- Low the risk of the malfunctions to reasonable levels acceptable by current society.

## 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

To increase functional safety our organization provides a safety culture. This includes the following characteristics:

- High priority: Safety is highest priority
- Well defined processes: Clearly defined management processes and  company design
- Accountability: Decisions are documented and traceable
- Diversity: People with different skills and backgrounds work together
- Independence: The auditors and testers belong to a different organization unit than the product designers and developers
- Communication: Potential safety problems have to be reported immediately to the developers for further investigations

The above values are communicated through all management levels to help our employees to archive the functional safety and project goals together.

# Safety Lifecycle Tailoring

For this project the safety plan is tailored. The following 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 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

The Development Interface Agreement (DIA) helps to avoid disputes during planning and development of the lane assistance system as it defines the above roles and responsibilities between the involved companies. The OEM is responsible for the overall vehicle safety and all ISO 26262 required functional safety actions. The companies agreed that the above tailored safety lifecycle is enough to fulfill the ISO 26262 norms for the lane assistance system. Furthermore all useful information for which helps to achieve function safety and concerns the lane assistance component will be shared through the appointed Functional Safety Managers. The Tier-1 Supplier is accountable for the lane assistance component and not the other parts of the vehicle. Therefore the Tier-1 Supplier will analyze and modify various sub-systems of the lane assistance component from a functional safety viewpoint.
The Tier-1 company will act and fix all bugs which apply to the lane assistance system. All other issues have to be investigated by the OEM.

# Confirmation Measures

The confirmation measures ensures that the processes comply with the functional safety standard, project execution is following the safety plan and that the design improves functional safety. Therefore a confirmation review, functional safety audit and functional safety assessment will be executed.
The confirmation review ensures that the project complies to ISO 26262 and will be performed by a person which is independent from the design team. The functional safety audit checks that the actual implementation of the projects conforms to the safety plan. Lastly the functional safety assessment confirms that project plans, designs and development actually achieve 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.