



# Safety Plan Lane Assistance

**Document Version: 1.0**

Template Version 1.0, Released on 2017-06-21



# Document history

Date	Version	Editor	Description
2018-03-03	1.0	Maximilian Wenger	Initial Version

## Table of Contents

Document history .....	2
Table of Contents.....	2
Introduction .....	3
Purpose of the Safety Plan .....	3
Scope of the Project .....	3
Deliverables of the Project.....	3
Item Definition .....	4
Goals and Measures .....	5
Goals.....	5
Measures .....	5
Safety Culture .....	6
Safety Lifecycle Tailoring .....	6
Roles .....	7
Development Interface Agreement.....	7
Confirmation Measures .....	7

# Introduction

## Purpose of the Safety Plan

The purpose of this safety plan is to ensure that the lane assistance functionality will be safe. It will outline all of the roles that are involved in ensuring this and all steps that will be taken to achieve functional safety of the finished product.

## 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:

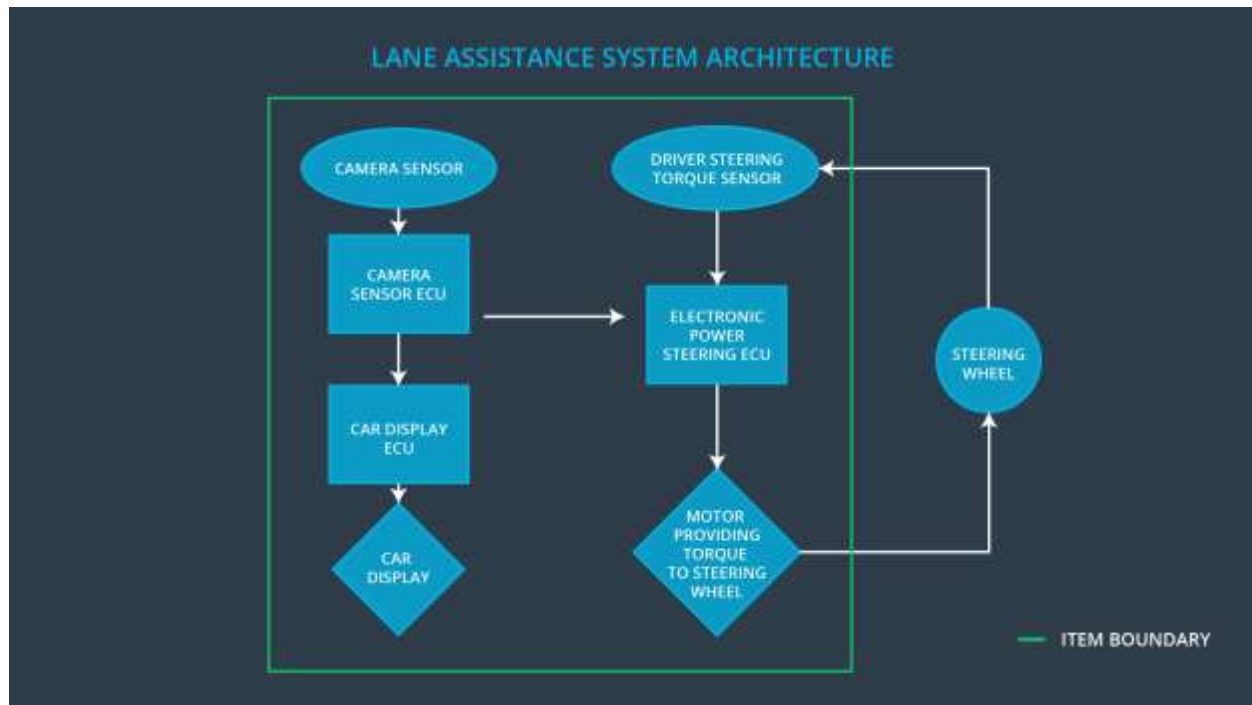
- Product Development at the Hardware Level
- Production and Operation

## 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 scope for this project is a lane keeping assistance system. The lane assistance item helps the driver to keep the vehicle in the lane it is currently in (ego lane) and not depart the lane by accident.

The item senses when the vehicle is about to leave the ego lane and vibrates the steering wheel to alert the driver, while also applying steering torque to return to the ego lane. Additionally, the item activates a warning light in the car display to communicate to the driver that it is active.

The system responsible for detecting the lane departure is a camera and its ECU. This system works in concert with a power steering system that contains a torque sensor for detecting the driver's input to the steering wheel and an actuator to apply force to the steering wheel itself. The power steering system is responsible for applying the torque holding the vehicle in the ego lane.

The car display system is responsible for showing a warning to the driver that the lane assistance item is active.

The boundaries of the item are defined as follows. The lane assistance item contains a display sub-system and a system for detecting and correcting lane departures. The system for detecting and correcting lane departures contains the camera subsystem and the power steering subsystem. The steering wheel is not part of the item.

# Goals and Measures

## Goals

The goal of this project is to ensure the functional safety of the lane assistance function. This will be achieved by following the ISO 26262 standard and the steps laid out in this document.

## 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 of our products is our company's highest priority. We assure that this priority is enforced by our implementation of the following measures:

- Traceability. All design decisions within our product development process are documented with a date and a responsible person.
- Independent Audits. There are yearly randomized audits of 10% of our projects, where project documentation is audited by people not associated with the project.
- Incentives. We reward associates that find potential safety issues and have implemented a web-based solution that is part of every project from the outset.
- Processes. All of our processes are versioned and available on our intranet. We encourage active participation of all associates in continually improving the processes via the integrated "discussion" functionality.

# Safety Lifecycle Tailoring

The lane assistance functionality was developed originally by the OEM. The task of this project is to assess and improve the functional safety of this initial product. Therefore, the safety lifecycle does only need to take into consideration the parts of the lane assistance function that are changed during the course of this project.

The phases of the safety lifecycle that are in scope for this project are:

- Concept phase
- Product development at the system level
- Product development at the software level

This project will disregard the following phases:

- 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

This development interface agreement delineates the roles and responsibilities of the OEM and Tier-1 during the development of the lane assistance function. It also defines which work products will be produced and exchanged between the parties.

The OEM agrees to provide the Tier-1 with a functioning lane assistance system.

The Tier-1 agrees to analyze the lane assistance system and its component parts with regard to their functional safety. The work product will be a the deliverables mentioned in the introduction. The responsible person at the Tier-1 is the author of this document.

## Confirmation Measures

The confirmation measures are put in place to ensure that the project conforms to the ISO 26262, follows the safety plan and actually makes the product safer.

The confirmation review ensures that the project follows the ISO 26262 process and is conducted by an independent party.

The functional safety audit is conducted by the safety auditor and ensures that the implementation of the project follows the safety plan.

The functional safety assessment is intended to confirm that all plans, designs and functions developed within the project actually achieve functional safety.