

Safety Plan Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 18-06-2018 | 1.0 | Shubham | Initial Draft |
| 19-06-2018 | 1.1 | Shubham | Final Version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

[Document history](#_1t3h5sf)

[Table of Contents](#_ktt3lgighckp)

[Introduction](#_zakt536q9xt3)

[Purpose of the Safety Plan](#_52ybytyytfvs)

[Scope of the Project](#_sh22j99mm02k)

[Deliverables of the Project](#_fzzlhwsfq6ys)

[Item Definition](#_t6m96u2v69wo)

[Goals and Measures](#_km1cu1hyl182)

[Goals](#_ww7fqc274i9y)

[Measures](#_v2rbrzjrkt9b)

[Safety Culture](#_b23s6orj91gm)

[Safety Lifecycle Tailoring](#_pqn9poe0nvtc)

[Roles](#_xlicd1ijavb7)

[Development Interface Agreement](#_swj0emygbhrm)

[Confirmation Measures](#_lllavvxrxrdy)

# Introduction

## Purpose of the Safety Plan

The purpose of the Safety plan is to provide an overall framework to ensure the functional safety work for the Lane Assistance item. The Safety Plan is developed in accordance with ISO26262 to document how management of functional safety is defined within this project.

## 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 aims to provide assistance to driver to keep its own lane and to avoid unintended lane departures.

This item has two main functions:

* **Lane Departure Warning (LDW)** - The LDW function shall apply an oscillating steering torque to provide haptic feedback to the driver to inform about a possible lane departure.
* **Lane Keeping Assistance (LKA).** The LKA function shall apply a steering torque, turning back into the ego lane to prevent a lane departure.

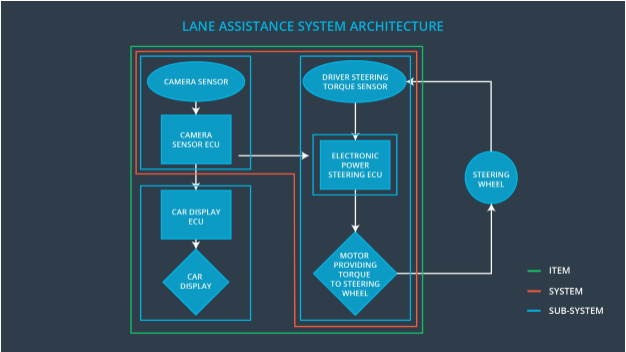
There are three main subsystems involved in this activity:

* Camera Subsystem
* Car display subsystem
* Electronic power steering Subsystem

In relation with LKA, Camera Control subsystem is responsible for the vision system (i.e. detecting a possible lane departure and deciding the control request for steering actuation), EPS is responsible for the motion system (i.e. the actual steering actuation) and Car dashboard control is responsible to inform the driver about a lane departure.

In relation with LDW, Camera Control responsible for the vision system as for LKA (here deciding the oscillation characteristics request), EPS is responsible for the haptic warning actuation and Car dashboard control responsible to inform the driver of lane departure. However, Car dashboard control is also responsible for informing the driver of function availability and providing the possibility to turn off the function.

The Lane assistance system architecture can be seen below, where the earlier mentioned subsystems are included and the item boundary is visible. Steering wheel actuation is outside of the item boundary which means that the new modifications doesn’t deal with steering wheel as it is not part of current project scope.



# Goals and Measures

## Goals

## The goal of this project is to reduce electrical and electronics risks and hazardous events to an acceptable level with the use of ISO26262 for the lane assistance item. Based on the outcome of risk analysis, we can classify safety levels and come up with plans to minimize these risks and avoid potential hazards.

## 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 | All team members | 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

Here are some characteristics of a good safety culture:

* **High priority**: safety has the highest priority among competing constraints like cost and productivity. Hence no compromise should be done while measuring safety.
* **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**: appropriate penalties should be imposed if someone doesn’t adhere to the safety guidelines.
* **Independence**: audit team and the development team should be independent, this will make sure that the audit was unbiased.
* **Well defined processes**: company design and management processes should be clearly defined
* **Resources**: allocated resources to the project should be suffice to complete each and every requirement and the resources should have required skill set.
* **Diversity**: intellectual diversity is sought after, valued and integrated into processes
* **Communication**: communication channels encourage disclosure of problems

# Safety Lifecycle Tailoring

For Lane Assistance project. Following phases of the safety lifecycle are in the scope, since the lane assistance item is not new but only needs modifications:

* Concept Phase
* Product development at the system level
* Product development at the software level

The phases that are out of the scope for this project are:

* 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

Development interface agreement(DIA) is a mutually agreed agreement between multiple parties that sets forth the expectations from each one. Other goals achieved via DIA are:

* clarify the responsibilities of the different parties involved in a functional safety project.
* describe which work product(s) each company shall provide - help avoid disputes between companies
* clarify who will be responsible for any safety related issues in post-production

The responsibilities of the OEM are to define the functionality of the lane assistance system and to conduct the activities in the scope of project manager, safety manager and safety engineer in item level.

# Confirmation Measures

The main purpose of confirmation measures is to verify that processes comply with the functional safety standard, i.e. ISO26262, that project execution is following safety plan and that the design really does improve safety.

##### 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 used to ensure that the implementation of the project adheres to the safety plan.

An independent external safety assessor shall make a functional safety assessment of the project, i.e. review the final work and confirm that plans, designs and developed products 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.