

Safety Plan Lane Assistance

**Document Version: 1.1**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 15.02.2018 | 1.0 | VIvanov | Draft version of document |
| 16.02.2018 | 1.1 | VIvanov | Item Definition update |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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

This document defines a safety plan of Lane Assistance project as a goal of safety achievement during project development. Document includes the goals of the project what activities will be included, defines roles on the team, who will develop the project and confirmation measures for proving achieved functional safety.

## 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 investigated in this plan is Lane Assistant project.

The Lane Assistance project has two functions:

* Lane Departure Warning
* Lane Keeping Assistance

**Lane Departure Warning** behavior: When the car departs a lane without using a turn signal the system will vibrate the steering wheel to warn the driver.

**Lane Keeping Assistance** behavior: When the car departs a lane without using a turn signal the system will move the steering wheel back towards the lane center.

The item consists following sub-systems and components:

1. **Camera Subsystem**
   1. Camera sensor.
   2. Camera sensor ECU (Electronic Control Unit).
2. **Electronic Power Steering Subsystem**
   1. Driver Steering Torque Sensor.
   2. Electronic Power Steering ECU.
   3. Motor Proving Torque to Steering Wheel.
3. **Car Display Subsystem**
   1. Car Display ECU.
   2. Car Display.

Lane Assistant project Architecture:



The Lane Assistant project does not include following functionalities:

* Adaptive Cruise Control
* Automatic Parking
* Blind Spot Monitoring
* Tire Pressure Monitoring
* Pedestrian Protection

# Goals and Measures

## Goals

The goals of project are:

* Identify risk and hazardous situations caused by the Line Assistance project components malfunction for persons in car and for other cars.
* Evaluate the risk level of the hazardous situations.
* Low to risks of the malfunctions to a reasonable level.

## 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

In order to ensure that safety culture is in a good shape following characteristics shall be tracked:

* **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, 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

# 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 section defines the roles and responsibilities between OEM and Tier-1 involved in in the Lane Assistance project development.

The OEM provides a functioning Lane Assistance System. Tier-1 is going to analyze and modify sub-systems, listed in **Item Definition** according to functional safety requirements.

* **OEM:**
  + **Functional Safety Manager - Item Level**: Pre-audits, plans the development phase for the Lane Assistance item.
  + **Functional Safety Engineer - Item Level**: Develop prototypes, integrate subsystems combining them into the Lane Assistance item from a functional safety viewpoint.
  + **Project Manager - Item Level**: Allocates the resources needed for the item.
* **Tier-1 (Camera Subsystem):**
  + **Functional Safety Manager - Component Level**: Pre-audits, plan the development for the components of the Lane Assistance item:
    - Camera Subsystem components
  + **Functional Safety Engineer - Component Level**: Develop prototypes and integrate components into the Lane Assistance item:
    - Camera Subsystem components
* **Tier-1 (Electronic Power Steering Subsystem):**
  + **Functional Safety Manager - Component Level**: Pre-audits, plan the development for the components of the Lane Assistance item:
    - Electronic Power Steering Subsystem components
  + **Functional Safety Engineer - Component Level**: Develop prototypes and integrate components into the Lane Assistance item:
    - Electronic Power Steering Subsystem components
* **Tier-1 (Car Display Subsystem):**
  + **Functional Safety Manager - Component Level**: Pre-audits, plan the development for the components of the Lane Assistance item:
    - Car Display Subsystem components
  + **Functional Safety Engineer - Component Level**: Develop prototypes and integrate components into the Lane Assistance item:
    - Car Display Subsystem components
* **OEM/External:**
  + **Functional Safety Auditor**: Make sure the project conforms to the safety plan.
  + **Functional Safety Assessor**: Judges where the project has increased safety

# Confirmation Measures

The confirmation measures have following purposes:

* That the Lane Assistance project conforms to ISO 26262.
* That the Lane Assistance 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*** checks to make sure that the actual implementation of the project conforms to the safety plan is called a functional safety audit.

***Functional safety assessment*** confirms that plans, designs and developed products actually achieve functional safety is called a functional safety assessment.