

Safety Plan Lane Assistance

**Document Version: 1.0**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 15.06.2018 | 1.0 | Malgorzata Plonka | Initial 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

This document defines an overall framework for the Lane Assistance item.

As part of the Advanced Driver Assistance System (ADAS), the lane assistance item may introduce a new risk in a vehicle. The safety plan is responsible for detection of the risk and reducing it to the acceptance levels.

## 

## 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 of this safety plan is the lane assistance system. The item has following main functions:

* **Lane departure warning function.** In case the vehicle left a lane without signalizing it, system assumes that it happens by mistake and starts to vibrate a steering wheel to warn a driver.
* **Lane keeping assistance function.** In case the vehicle does not drive near of lane center, the system will move the steering wheel so that the vehicle turns back towards the center of the lane.

Following subsystem cover functionality of the item:

* Camera subsystem
* Electronic Power Steering subsystem
* Car Display subsystem

How it works together?

When the camera sensor detects that the vehicle is leaving the lane, the camera sends a signal to the electronic power steering (EPS) system asking to turn and vibrate the steering wheel. The camera sensor will also request that a warning light turn on in the car display dashboard. This is how lane departure warning functions works. This function involves camera, electronic powers steering and car display subsystems.

When the camera sensor detects the driver does not drives towards center of a lane (with some tolerance) the electronic power steering (EPS) system is integrated in the steering wheel that start to move steering wheel to bring a vehicle back to lane center. This how Lane keeping function works. This function involves camera, electronic powers steering subsystems.

Below the composition of subsystems and a diagram showing the interaction between them.

* Camera subsystem containing two components:
  + Camera sensor
  + Camera sensor ECU (Electronic Control Unit)
* Electronic Power Steering subsystem containing three components
  + Electronic Power Steering ECU.
  + Driver Steering Torque Sensor.
  + Motor Proving Torque to Steering Wheel.
* Car Display subsystem containing two components:
  + Car Display ECU
  + Car Display



# Goals and Measures

## Goals

The goal of the projects is to achieve safety level of Lane Assistance system according to ISO 26262. To do this we are going to:

* Identify risk and hazardous situations
* Evaluate the risks of the hazardous situations
* finally apply systems engineering in order to lower these risk

## 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

* High priority

In our company, safety has the highest priority among the competing constraints like productivity and cost. Each new employee in our engineering department is assigned to have a training about ISO 26262 .

* Accountability

There is a special tem responsible for safety functionality. There is a manager leading working with a team that document all the development activities and decisions in order to ensure the accountability. The documents are managed in the way that all these activities are traceable.

* Rewards

Our Company motivates and supports the achievement of functional safety.

* Penalties

We penalize shortcuts that jeopardize safety or quality of our product. After the first attempt, the safety manager will send a warning notice. After the second attempt the employee will be reallocated or dismissed.

* Independence

We build our development, design, testing, and audit team independently.

Well defined processes. All processes are clearly defined and the documents are placed in a certain folder in our company network. Only team members with its appropriate role has a write access.

* Resources

We work together with our human resource team to plan, manage and find new talented engineers with the appropriate skills. In case of shortage

* 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

* 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

The purpose of a development interface agreement (DIA) is to ensure that all parties: OEM and Tier-1 are developing safe vehicles in compliance with ISO 26262.

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

Our company having Tier-1 role is going to analyze and modify various sub-systems according to functional safety requirements.

# Confirmation Measures

The main purpose of confirmation measures is to:

* ensure that a functional safety project conforms to ISO 26262, and
* ensure that the project really does make the vehicle safer

*Confirmation review*

ensure the projects comply 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*

make sure the actual implementation of the project conforms

to the safety plan.

*Functional safety assessment*

confirms that the plan, design and developed product actually achieve functional safety.