

Safety Plan Lane Assistance

**Document Version: 1.0**

**Released on 2018-05-25**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 25-05-2018 | 1.0 | Srigandhan | First Submission |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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 safety plan gives an overview of how to achieve a safe system. To have a safe system, risk associated with each sub systems has to be minimized. In order to achieve this goal, Safety plan defines the steps to be followed and explains the roles and responsibility of resources involved in the 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 item of concern in this project is a *Lane assistance system*.

The two main function of this item are:

* **Lane departure warning function**
* **Lane keeping assistance function**

The item’s *lane departure warning function* vibrates the steering wheel in case the car moves to the edge of the lane and the l*ane keeping assistance function* moves the steering wheel so that the car turns back to the center of the lane.

The item functionalities are implemented by the following subsystem:

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

The following diagram shows the interaction between different subsystems.

****

A drift from the lane center is detected by the car’s *camera sensor* subsystem. The *electronic power steering ECU* subsystem takes inputs from the *camera sensor* subsystem and the *driver steering torque* subsystem and outputs to a *motor* providing torque to the steering wheel. In addition a *car display* subsystem provides visual feedback for the driver. All these subsystems are part of the item. The *steering wheel* itself is not part of the item and thus not part of this project.

# Goals and Measures

## Goals

The major goal of this project is to assure safe and reliable operation of the vehicle’s lane assistance function, according to ISO 26262. To achieve functional safety we are going to identify hazards, measure risks and finally apply systems engineering in order to lower risk to a reasonable level.

## Measures

|  |  |  |
| --- | --- | --- |
| Measures and Activities | Responsibility | Timeline |
| Follow safety processes | All Team Members | Constantly |
| Create and sustain a safety culture | Safety Manager | 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

Although cost and productivity are important for a successful system and market integration, safety is our number one priority. Meeting functional safety standards on a regular basis is going to be rewarded whereas not following essential safety requirements so as to avoid work done there or to reduce costs is never an option and will be penalized. Designing functional safety is following defined processes and assures that design decisions are traceable back to the people and teams who made the decisions. Development and auditing teams are independent and have to involve people of different intellectual backgrounds. It is crucial that communication between those teams is based on full disclosure of problems. All necessary resources including people with appropriate skills are assigned to this functional safety project.

# 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

The purpose of the development interface agreement (DIA) is to define the roles and responsibilities between OEM and tier-1 involved in developing this product. Both parties agree on the contents of the DIA before the project begins. The DIA specifies what evidence and work products each party will provide to prove that work was done according to the agreement.

The OEM provides a functioning lane assistance system. Tier-1 analyzes and modify various sub-systems according to functional safety requirements.

OEM is responsible for overall vehicle safety. Here we conduct safety activities in item level. Our company is responsible for conducting the activities in scope of safety manager and safety engineer of the component level. 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

*Confirmation measures* ensure that the applied processes comply with functional safety standards provided by ISO 26262 and project execution is following the safety plan, therefore verifying whether the design really improve safety.

On providing ***confirmation review****,* during design and development of the product, compliance with ISO 26262 is assured by an independent person.

A ***functional safety audit*** checks that the actual implementation of the project considers the safety plan.

Finally***functional safety assessment***confirms 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.