

Safety Plan Lane Assistance

**Document Version: 1.0**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 2019-01-16 | 1.0 |  | First draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

Table of Contents

[Document history 2](#_Toc535387383)

[Table of Contents 2](#_Toc535387384)

[Introduction 4](#_Toc535387385)

[Purpose of the Safety Plan 4](#_Toc535387386)

[Scope of the Project 4](#_Toc535387387)

[Deliverables of the Project 4](#_Toc535387388)

[Item Definition 5](#_Toc535387389)

[Goals and Measures 6](#_Toc535387390)

[Goals 6](#_Toc535387391)

[Measures 6](#_Toc535387392)

[Safety Culture 7](#_Toc535387393)

[Safety Lifecycle Tailoring 7](#_Toc535387394)

[Roles 7](#_Toc535387395)

[Development Interface Agreement 8](#_Toc535387396)

[Confirmation Measures 8](#_Toc535387397)

# Introduction

## Purpose of the Safety Plan

A safety plan documents how the functional safety is ensured by the company. Documenting the processes and steps of the development ensures the usage of best practices. It also contains documentation about what was changed in order to reduce the risk to acceptable 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 lane assistance system helps the driver to stay in a lane. It consists of a lane departure warning and a lane assistance.

The lane departure warning senses the lane with a camera and vibrates the steering wheel, if the car is going to leave the current lane without any turn signal active. If the driver does not have any turn signal on and drives over a lane boundary, the system considers this case as unwanted by the driver and warns him by vibrating the steering wheel.

The lane assistance tries to keep the car in the middle of the lane. If the car goes outside the middle of the lane, it applies torque to the steering wheel in order to steer the car back to the middle of the lane. If the driver seems to be inactive (not having its hands on the steering wheel) the system will turn inactive as well, because the driver must always have the control over the car. If the system turns inactive because of the driver being absence it indicates this by an acoustic signal.

The system consists of the camera sensor and the camera sensor ECU for sensing the lane boundaries.

The car display ECU and the car display are used to display the status of the lane assistance system.

The driver steering torque sensor and the electronic power steering ECU are used to detect whether the driver has its hand on the steering wheel or not.

The electronic power steering ECU and the motor providing torque to the steering wheel are used to vibrate in case of a lane departure or to apply torque to the steering wheel in order to keep the car in the middle of the lane.

All the above-mentioned subsystems are included in the safety plan, except for the steering wheel.

# Goals and Measures

## Goals

**[Instructions:**

**Describe the major goal of this project; what are we trying to accomplish by analyzing the lane assistance functions with ISO 26262?]**

## Measures

**[Instructions:**

**Fill in who will be responsible for each measure or activity. Hint: The lesson on Safety Management Roles and Responsibilities.**

**The options are:**

**All Team Members**

**Safety Manager**

**Project Manager**

**Safety Auditor**

**Safety Assessor**

**]**

|  |  |  |
| --- | --- | --- |
| Measures and Activities | Responsibility | Timeline |
| Follow safety processes |  | Constantly |
| Create and sustain a safety culture |  | Constantly |
| Coordinate and document the planned safety activities |  | Constantly |
| Allocate resources with adequate functional safety competency |  | Within 2 weeks of start of project |
| Tailor the safety lifecycle |  | Within 4 weeks of start of project |
| Plan the safety activities of the safety lifecycle |  | Within 4 weeks of start of project |
| Perform regular functional safety audits |  | Once every 2 months |
| Perform functional safety pre-assessment prior to audit by external functional safety assessor |  | 3 months prior to main assessment |
| Perform functional safety assessment |  | Conclusion of functional safety activities |

# Safety Culture

**[Instructions:**

**Describe the characteristics of your company's safety culture. How do these characteristics help maintain your safety culture. Hint: See the lesson about Safety Culture**

**]**

# Safety Lifecycle Tailoring

**[Instructions:**

**Describe which phases of the safety lifecycle are in scope and which are out of scope for this particular project. Hint: See the** [**Intro section**](#_sh22j99mm02k) **of this document**

**]**

# Roles

**[Instructions:**

**This section is here for your reference. You do not need to do anything here. It is provided to help with filling out the development interface agreement section.**

**]**

|  |  |
| --- | --- |
| 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

**[Instructions:**

**Assume in this project that you work for the tier-1 organization as described in the above roles table. You are taking on the role of both the functional safety manager and functional safety engineer.**

**Please answer the following questions:**

1. **What is the purpose of a development interface agreement?**
2. **What will be the responsibilities of your company versus the responsibilities of the OEM? Hint: In this project, the OEM is supplying a functioning lane assistance system. Your company needs to analyze and modify the various sub-systems from a functional safety viewpoint.**

**]**

# Confirmation Measures

**[Instructions:**

**Please answer the following questions:**

1. **What is the main purpose of confirmation measures?**
2. **What is a confirmation review?**
3. **What is a functional safety audit?**
4. **What is a functional safety assessment?**

**]**

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.