

Safety Plan Lane Assistance

**Document Version: 1.0**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 11/24/2017 | 1.0 | Chris Ferone | First draft of document. |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# 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 define roles and outline the steps needed to achieve 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

**[Instructions:**

**REQUIRED**

**Discuss these key points about the system:**

**What is the item in question, and what does the item do?**

**What are its two main functions? How do they work?**

**Which subsystems are responsible for each function?**

**What are the boundaries of the item? What subsystems are inside the item? What elements or subsystems are outside of the item?**

The Lane Assistance System has two functions: **Lane departure warning** and **Lane keeping assistance.** When the driver drifts towards the edge of the lane, two things will happen:

1. the lane departure warning function will vibrate the steering wheel. In other words, the vehicle quickly moves the steering wheel back and forth to create a vibration.
2. the lane keeping assistance function will move the steering wheel so that the wheels turn towards the center of the lane

When the camera senses that the vehicle is leaving the lane, the camera sends a signal to the electronic power steering 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. That way the driver knows that the lane assistance system is active.

If the driver uses a turn signal, then the lane assistance system deactivates so that the vehicle can leave the lane. The driver can also turn off the system completely with a button on the dashboard.

The driver is still expected to have both hands on the steering wheel at all times. The electronic power steering subsystem has a sensor to detect how much the driver is already turning. The lane keeping assistance function will merely add the extra torque required to get the car back towards center. The extra torque is applied directly to the steering wheel via a motor.

The following diagram shows the boundaries between each system:



# Goals and Measures

## Goals

The goals of this project are to identify hazards within the lane assistance system, evaluate the risk of those hazards, and use system engineering to lower the 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 Auditor | 3 months prior to main assessment |
| Perform functional safety assessment | Safety Assessor | Conclusion of functional safety activities |

# Safety Culture

Safety is paramount. Safety cannot be ignored in order to meet deadlines or lower costs. Therefore, the following steps are being taken to ensure everyone within the company prioritizes safety:

1. Managers shall be responsible for ensuring that all design decisions, test plans, validation results, and other safety-related documentation clearly indicate their authorities to ensure accountability. Requirements tracking software shall be use to ensure traceability from requirements to design to testing and validation.
2. Each year one person within the company will be recognized for exceptional work promoting and prioritizing safety. This person will be awarded a one-time $1000 bonus.
3. Anyone who reports unsafe designs practices, or deficiencies in safety procedures is immune from any disciplinary action.
4. Any employees who willfully disregard safety plans, best practices, etc. will be subject to disciplinary action, including but not limited to suspension, demotion, and termination.
5. Those who design systems shall not be solely responsible for testing and validation nor hazard analysis.
6. Each engineer shall have clearly defined roles. A single person cannot manage all aspects of functional safety.

# Safety Lifecycle Tailoring

Because the OEM is supplying a functioning lane assistance system, only 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 clearly define and delineate the roles and responsibilities between the OEM and supplier.

In this project, the OEM is supplying a functioning lane assistance system. My company needs to analyze and modify the various sub-systems from a functional safety viewpoint.

# Confirmation Measures

The main purpose of confirmation measures is to ensure that the functional safety project conforms to ISO 26262 and does indeed make the vehicle safer.

The confirmation review is an audit conducted by an independent person to verify that the project is in compliance with ISO26262.

The functional safety audit confirms that actual implementation of the project confirms to the safety plan.

The functional safety assessment confirms that the plans, designs and developed products actually achieve functional safety.