

Safety Plan Lane Assistance

**Document Version: 1.0**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 5/22/2018 | 1.0 | Rahul Bhartari | First Version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

[Document history 1](#_Toc514833027)

[Table of Contents 2](#_Toc514833028)

[Introduction 3](#_Toc514833029)

[Purpose of the Safety Plan 3](#_Toc514833030)

[Scope of the Project 3](#_Toc514833031)

[Deliverables of the Project 3](#_Toc514833032)

[Item Definition 3](#_Toc514833033)

[Goals and Measures 5](#_Toc514833034)

[Goals 5](#_Toc514833035)

[Measures 5](#_Toc514833036)

[Safety Culture 6](#_Toc514833037)

[Safety Lifecycle Tailoring 6](#_Toc514833038)

[Roles 6](#_Toc514833039)

[Development Interface Agreement 6](#_Toc514833040)

[Confirmation Measures 7](#_Toc514833041)

# Introduction

## Purpose of the Safety Plan

Safety is one of the most important part of development of a complex system like a vehicle. It has to be integrated deep into the development process. This document covers the entire framework for embedding safety into development process, including the measures, roles and responsibilities in the process.

## 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 considered in this safety plan is Lane Assistance System.

Two main functions of this item are:

* **Lane departure warning**

When driver drifts the vehicle towards the edge of current lane without using turn signal, the system assumes that the driver has got distracted and steering wheel starts to vibrate to warn the driver. The system moves the steering wheel back and forth to vibrate the steering wheel.

* **Lane keeping assistance**

When driver drifts the vehicle towards the edge of current lane without using turn signal, this function turns the steering wheel to bring the vehicle to the center of the lane. Steering torque is applied on the steering wheel in order to turn it.

The functions of the item are implemented in the following subsystems:

* Camera subsystem
  + Camera Sensor
  + Camera Sensor ECU
* Car display subsystem
  + Car Display
  + Car Display ECU
* Electronic power steering subsystem
  + Driver Steering Torque Sensor
  + Electronic Power Steering ECU
  + Motor providing Torque to Steering Wheel

Following diagram shows the interconnected subsystems.



Camera subsystem detects when the vehicle is about to leave the lane. If driver does not use the turn signal, then the camera subsystem communicates with car display and electronic power steering subsystems. Car display subsystem shows the warning signal to the driver on the displayed dashboard. Electronic power steering subsystem uses driver steering torque sensor to detect how much torque is driver applying on the steering wheel and then the lane keeping assistance function will add the additional torque required and turn the steering to keep the vehicle in the center of the lane.

The entire lane assistance system can be switched on or off by the driver at will.

Lane assistance system does not provide the following functions:

* Automatic lane change
* Decipher missing or incorrect lanes or lanes covered in snow
* Automatic cruise control

# Goals and Measures

## Goals

The main goal of this project is to identify high risk situations that could arise in Lane assistance system and lower the risk to reasonable levels to ensure safe and reliable operation of E/E components of the system in accordance with ISO 26262 standard. To achieve functional safety, we are going to identify hazards, measure the risks and apply systems engineering to lower the risks to the reasonable level which is acceptable to the society.

## 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

Following are the characteristics implemented for a good safety culture:

* **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

When doing a new implementation, the entire safety lifecycle has to be considered and documented. For modification, only the parts impacted by the new functionality have to be documented.

For this project, product development at concept, system and software level are in scope. Product development at hardware level, production and operation level are out of scope for this project.

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

The ultimate goal is to ensure that all parties are developing safe vehicles in compliance with ISO 26262.

Here are major sections of a DIA:

* Appointment of customer and supplier safety managers
* Joint tailoring of the safety lifecycle
* Activities and processes to be performed by the customer and the supplier
* Information and work products to be exchanged
* Parties or persons responsible for each activity in design and production
* Any supporting processes or tools to ensure compatibility between customer and supplier technologies

# Confirmation Measures

The purpose of *Confirmation measures* is to ensures that a functional safety project conforms to ISO 26262 and that the project really does make the vehicle safer. The people who carry out confirmation measures need to be independent from the people who actually developed the project

*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* is the checking performed to make sure that the actual implementation of the project conforms to the safety plan.

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