

Safety Plan Lane Assistance

**Document Version: [2.0]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 03/11/2018 | 1.0 | Atul Kumar | Draft version |
| 24/112018 | 2.0 | Atul Kumar | Version 2.0 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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

Provide the document for the audit purpose for different stack holders. In multivendor development, safety plan provides overall framework for functional safety of the lane assistance pertaining to the potential malfunctions of the electric and electronic system based on ISO26262 standard or tailed one.

## 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 Item is a simplified version of an Advanced Driver Assistance System

As known as ADAS that warns the driver of unintended steering drifts and assists the driver in steering back to the center of the current lane. The item will have two functions

1. Lane departure warning
2. Lane keeping assistance

Use case: when driver drifts towards the edge of the lane system will perform two things

1. The lane departure warning function shall apply an oscillating steering torque to

provide the driver a haptic feedback (vibration).

2. The lane keeping assistance function shall apply the steering torque when active in

order to stay in ego (current active) lane.

The item boundary includes three sub-systems as shown in Figure:

1.Camera system

2.Electronic Power Steering system

3.Car Display system

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. When 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 canter. The extra torque is applied directly to the steering wheel via a motor. As shown in below figure, the Lane Assistance Item does not include the following systems normally found in a fully implemented ADAS system:

1.Adaptive Cruise Control

2.Automatic Parking

3.Blind Spot Monitoring

4.Tire Pressure Monitoring

5.Pedestrian Protection



# Goals and Measures

## Goals

The goals of the Lane Assistance Functional Safety Plan for the project are:

1. Identify risk hazardous situations in a lane assistance electronic or electric system

malfunction that may cause physical injury or damage to a person’s health.

2.Evaluate the risk level of the hazardous situation

3.Via systems engineering, lowering high risk level situations to reasonable levels to

prevent accidents from occurring.

## 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 Manger | 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

We believe and will behave in the following manner to achieve the highest safety record in the industry:

1. High priority: safety has the highest priority among competing constraints like cost and

Productivity.

2.Accountability: processes ensure accountability such that design decisions are

traceable back to the people and teams who made the decisions.

3. Rewards: the organization motivates and supports the achievement of functional safety.

4. Penalties: the organization penalizes shortcuts that jeopardize safety or quality.

5. Independence: teams who design and develop a product should be independent from

the teams who audit the work.

6. Well defined processes: company design and management processes should be

clearly defined.

7. Resources: projects have necessary resources including people with appropriate skills.

8.Diversity: intellectual diversity is sought after, valued and integrated into processes.

9.Communication: communication channels encourage disclosure of problems.

# Safety Lifecycle Tailoring

For the lane assistance project functional safety initial plan, the ISO 26262 standard have been

tailored to include the following safety lifecycle phases in scope:

1. Concept phase

2. Product Development at the System Level

3 Product Development at the Software Level

The following phases are out of scope:

1 Product Development at the Hardware Level

2 Production and Operation [Start of production]

We welcome our selected Tier-1 supplier to help us tailor the ISO 26262 standard further to

# 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

All the stakeholders involved in the Lane Assistance project agree to and in the following operating

principals to ensure that we are developing safe vehicles in compliance with ISO 26262

standard, tailored:

1. OEM Project Manager: Item Level resources allocation with adequate functional safety

competency, and appointment of external Functional Safety Auditor and Assessor. Lane

assistance system functional safety plan, and confirmation measures acceptance.

2. Tier-1 Project Manager: Component Level resources allocation with adequate

functional safety competency.

3. Appointed OEM Functional Safety Manager/Engineer (John Chen): Coordinate and

document the item level planned safety activities including: concept phase, and product

development at the system and software level. Perform functional safety preassessment

prior to audit by external functional safety assessor three months prior to

main assessment.

4.Tier-1 Safety Manager: Joint tailoring of the safety lifecycle.

5. All OEM, Tier-1 and their selected suppliers team members: Follow safety processes

and Create and sustain a safety culture as identified in section 4 of this plan.

6.Appointed Tier-1 Safety Manager/Engineer: Coordinate and document the component

level planned safety activities including: concept phase, and product development at the

component and sub-system software level in compliance with the item level planned and

safety activities as developed by OEM Functional Safety Manager/Engineer.

7. Appointed Safety Auditor: Plan the safety activities of the safety lifecycle once every

two months.

8. Appointed Safety Assessor: Perform functional safety assessment at conclusion of

functional safety activities.

# Confirmation Measures

It serves two main things

1.The Lane Assistance safety project can align with ISO26262 or tailored version.

2. The lane Assistance safety project makes the vehicle safer/reduce risk.

The confirmation review would ensure that the safety project is ISO26262 compliance/tailed version by an independent appointed safety auditor. The functional safety Audit would ensure that the actual implementation of the project meet the safety plan by an independent appointed auditor. The functional safety assessment will ensure that plans, design and developed products actually meet functional safety independent appointed achieve functional safety by an independent appointed safety accessor.