

Safety Plan Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 05/21/2018 | 1.0 | Swapnil More | First Draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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 document the functional safety framework of a Lane Assistance System and outline that the system follows ISO 26262 standards

## 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 document is a Level 2 Lane Assistance System. The system is part of the Advanced Driver Assistance package. It has two main functions:

**Lane Departure Warning:** If a driver departs a lane without using a turn signal, the system assumes that the driver has become distracted and did not mean to leave the lane. The system will then alert the driver using audio, visual and/or haptic feedback. (i.e. steering vibration, warning alarm or a flashing dashboard warning

**Lane Keeping Assistance:** If the drifting driver is doesn’t stabilize the vehicle before it leaves the lane, the system applies a steering torque to keep the vehicle in the current lane.

The Camera subsystem and Display subsystem analyze the Lane Departure Warning function whereas the Lane Keep Assistance is performed by the Electronic Power Steering subsystem.

**Lane Assistance Subsystem Components (Figure 1):**

* Camera Subsystem:
  + Camera Sensor
  + Camera Sensor ECU
* Display Subsystem:
  + Car Display ECU
  + Car Display
* Electronic Power Steering Subsystem:
  + Driver Steering Torque Sensor
  + Electronic Power Steering ECU
  + Motor providing torque to the steering wheel

The steering wheel itself is not part of the system.

**Lane Assistance Functionality (Figure 2):**

When the camera sensor detects a lane departure, the camera sensor ECU sends a signal to the Car Display ECU to broadcast a warning display. Based on whether, the lane assist in on/off, lane assist system is active, the car display flashes an appropriate message on the dashboard screen. Simultaneously, the Camera ECU calculates the steering wheel torque required to stabilize the vehicle and broadcasts the torque message to the electronic power steering ECU. Bases on the status of Lane Assistance System and the driver steering wheel input, the EPS ECU activates the steering wheel motor to generate appropriate torque. As a safety measure, in case the EPS ECU fails, it requests the display ECU to show a malfunction warning.



Figure : Lane Assistance Subsystems



Figure : Lane Assistance Functionality

# Goals and Measures

## Goals

The goals of the project are:

* Identify hazards in the Lane Assistance system that could cause physical injury or damage to a person’s health
* Evaluate the risk of the hazardous situations so that we know how much we need to lower the risk
* Use systems engineering to lower risks to reasonable levels and prevent accidents

## 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 | All Team Members | 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 Assesor | Conclusion of functional safety activities |

# Safety Culture

In order to ensure a good safety culture, the following characteristics must be observed:

* **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

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

This sections defines the roles and responsibilities between the parties involved in the Lane Assistance Project (i.e. OEM, Tier-1 Supplier and/or External Supplier) to ensure its development in compliance with ISO 26262:

* **Functional Safety Manager – Item Level:** Entire Lane Assist System
  + Planning, coordinating and documenting of the development phase of the safety lifecycle
  + Tailors the safety lifecycle
  + Maintains the safety plan
  + Monitors progress against the safety plan
  + Performs pre-audits before the safety auditor
* **Functional Safety Engineer – Item Level:** Entire Lane Assist System
  + Product development
  + Integration
  + Testing at the hardware, software and system levels
* **Project Manager – Item Level:** Entire Lane Assist System
  + Overall project management
  + Acquires and allocates resources needed for the functional safety activities
  + Appoints safety manager or might act as safety manager
* **Functional Safety Manager – Component Level (Swapnil More):** Particular Lane Assist Component
  + Planning, coordinating and documenting of the development phase of the safety lifecycle
  + Tailors the safety lifecycle
  + Maintains the safety plan
  + Monitors progress against the safety plan
  + Performs pre-audits before the safety auditor
* **Functional Safety Engineer – Component Level:**  Particular Lane Assist Component
  + Product development
  + Integration
  + Testing at the hardware, software and system levels
* **Functional Safety Auditor:** Internal or External
  + Ensures that the design and production implementation conform to the safety plan and ISO 26262.
  + Must be independent from the team developing the project
* **Functional Safety Assessor:** Internal or External
  + Independent judgement as to whether functional safety is being achieved via a functional safety assessment
  + Must be independent from the team developing the project

# Confirmation Measures

Confirmation measures serve two purposes:

* that a functional safety project conforms to ISO 26262, and
* that the project really does make the vehicle safer

**Confirmation Measures Definitions**

***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***

Checking to make sure that the actual implementation of the project conforms to the safety plan is called a functional safety audit.

***Functional safety assessment***

Confirming that plans, designs and developed products actually achieve functional safety is called 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.