

Safety Plan Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 06/21/2018 | 1.0 | Shivam Chawla | Highlighted a safety plan |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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

A functional safety is critical to any functional safety project. This document provides a framework for Lane assistance item and it also deals with responsibilities of functional safety of an item.

## 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

**Item**: Here a little modified Lane Assistance Version is considered as item. An **Item** is just a high level system in the vehicle; in this case, the item is the lane assistance system.

**Functions:**

The Lane Assistance System will have two functions:

1. Lane departure warning
2. Lane keeping assistance

When the driver drifts towards the edge of the lane, two things will happen:

* the **lane departure warning function** will vibrate the steering wheel or more formally: "the lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback." In other words, the vehicle quickly moves the steering wheel back and forth to create a vibration.
* the **lane keeping assistance function** will move the steering wheel so that the wheels turn towards the center of the lane or it can be described as "the lane keeping assistance **function** shall apply the steering torque when active in order to stay in ego lane". Ego lane refers to the lane in which the vehicle currently drives.

**Sub Systems:**

As described in blue box in following diagram:



* **Camera subsyatem**
  + Camera Sensor
  + Camera Sensor ECU
* **Electronic Power Steering subsystem**
  + Driver Steering Torque sensor
  + Electronic Power Steering ECU
  + Motor Proving Torque to Steering Wheel
* **Car Display subsystem**
  + Car Display ECU
  + Car Display

**Boundaries:**

The Line Assistance System does not include the following functionalities:

* Tire Pressure Monitoring
* Pedestrian Protection
* Automatic Parking
* Blind Spot Monitoring
* Adaptive Cruise Control

# Goals and Measures

## Goals

Goals for this project are:

* Identification of risks and hazars associated with Lane Assistance System components.
* Evaluation of the risks involved
* Lowering the risks to reasonable levels acceptable by current functionality

## 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 Assessor | Conclusion of functional safety activities |

# Safety Culture

Here are some characteristics of 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

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

A DIA (development interface agreement) defines the roles and responsibilities between 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.

1. **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.**

**]**

**Company Responsibilities:**

**On Component level:**

* 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
* Product development
* Integration
* Testing at the hardware, software and system levels

**OEM Responsibilities:**

**All above responsibilities on Item level and below:**

* Overall project management
* Acquires and allocates resources needed for the functional safety activities
* Appoints safety manager or might act as safety manager
* Ensures that the design and production implementation conform to the safety plan and ISO 26262.
* Must be independent from the team developing the project

**OEM/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
* 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

The purpose of the confirmation measures are:

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

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.

Funtional 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.