

Safety Plan Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 16 May 2018 | 1.0 | Rajagopala Rao Srinadhuni | Overview of the functional safety plan to be followed for Lane Assistance |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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 Safety Plan shall provide an overview to the functional safety plan, guiding us on how to plan a safe system. To implement functional safety in a vehicle, we must clearly set what must be accomplished. We shall define roles and outline how to achieve each of them. The vehicle system under analysis shall also be described in this document. Additionally, the document shall talk about the Safety Culture followed, and how the plan actually achieves a safe system.

## 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

This set of documents shall focus on a Lane Assistance System, which works to monitor a car’s position on the road. It checks whether a lane change is intentional and gives a warning and/or control signals to correct changes that are not. The system implemented in our case, follows a sensory warning system, which gives it the name Haptic Lane Feedback System. The following points discuss the main functionalities of the Lane Assist System:

* Lane Departure Warning: Is a warning given when lane change occurs unintentionally, or as defined by the system. Checks are placed on systems such as *turn indictors* or *sensors*, upon whose behavior warnings are issued, in the form of steering vibration (here) or an audible signal
* Lane Keeping Assistance: The vehicle provides assistance, when an unintentional lane change warning is received, to stay in the current lane. This is done by moving the steering gently towards the center of the lane

The following components constitute the Lane Departure Warning functionality:

* Sensors: A variety of sensors may be used to check whether a lane change is unintentional. Cameras are the most widely used sensor, followed by lasers or infra-red or even something as simple as turn indicators
* Warning system: Constitutes a system to warn the driver that an unintentional lane change is being performed. Usually an auditory signal such as a beep or a steering vibration is produced. Our system produces a steering vibration to warn the driver

The Lane Keeping Assistance functionality is comprised of the following sub-system(s):

* Power Steering / Steering Assist: When the Lane Departure System issues a warning, the steering system is activated to produce a reverse torque that slowly corrects the incorrect drift created

Coordinating between the two systems, is a third component, the electronic control unit, described as follows:

* Electronic Control Unit(ECU): Is the brain of the system. Coordinates between sensors and steering assist system, deciding which signal to issue a warning and act upon and which signals to treat as Keep Lane signals

Lastly we shall talk about the system boundaries, where we describe how the Lane Assistance System fits with other functionalities and systems present in the vehicle:

* Camera: The system connects to a camera as sensor to detect when the vehicle moves out of its lane while driving.
* Lane change indicator lamps: When the camera detects a change in lane, it sends a command to the ECU which then check whether the lane change indicators are being used
* ECU: Compares sensor data and issues warning if lane change seems unintentional. Otherwise the system stays latent
* Steering assist: When a lane change warning is issued, the system activates to generate an opposing torque and differ the accidental lane change

The Steering assist and ECU can be seen as components present as part of the Lane Assist System itself. The Camera and lane change indictors work as components outside the system and give their input to the Lane Assist System.

We now have a basic definition of the Item in consideration for this document, to proceed with further definition of the Safety Plan.

# Goals and Measures

## Goals

ISO 26262 is the standard for establishing functional safety standards. We aim to set a standard for the safety guidelines defined for lane assistance functions, analyzed through ISO 26262 processes. This way we can understand the system we are working with so that

* We understand the working and are able to identify all possible hazards
* Analyze the possible hazards and calculate the risk they produce
* Use this analysis as a basis for introducing checks in our system, when designing the system and implementing the same, so that we take care of vulnerabilities

The ultimate goal is thus to produce a system that is functionally safe, having checks or warnings for hazards that are deemed risky (subject to quantifiers). The ISO standard provides us with a means to establish the same in defined, definite structure.

## 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 Auditor | 3 months prior to main assessment |
| Perform functional safety assessment | Safety Assessor | Conclusion of functional safety activities |

# Safety Culture

*Characteristics of safety culture: high priorty(more like golden rule), accountability, rewards, penalties, independence, well defined processes(like ISO 26262), resources, diversity*

**[Instructions:**

**Describe the characteristics of your company's safety culture. How do these characteristics help maintain your safety culture. Hint: See the lesson about Safety Culture**

**]**

**Safety is the highest priority. All design decisions are …**

**The design team and audit team are …**

**The functional safety team has members from …**

Safety of a system is ensured not only by checking the technical aspects but by also maintaining a consistent safety culture at the organizational level. Safety is not a constraint but a necessity in all planning processes. The following points talk about the safety culture followed

* Safety takes highest priority: No other perspective such as cost or profit or a deadline can take precedence over safety. This means that whenever faced with a choice, safety is the only answer
* Traceability: All steps taken as part of Functional Safety procedure must be well documented, so that each step can be checked against and traced back to its creator. This not only provides a strong, structured base for our purpose but also enforces accountability in the system
* Independence: The audit team is an independent team, separate from the team designing the safety plan

# Safety Lifecycle Tailoring

*Mention parts of the V model that you shall follow -> Again mention phases in scope and objects out of scope*

**[Instructions:**

**Describe which phases of the safety lifecycle are in scope and which are out of scope for this particular project. Hint: See the** [**Intro section**](#_sh22j99mm02k) **of this document**

**]**

# 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

*Defines an agreement between the OEM and Tier 1 Org.*

*Major Sections: -> Refer to Fernando’s slide 12 in Wednesday’s class*

**[Instructions:**

**Assume in this project that you work for the tier-1 organization as described in the above roles table. You are taking on the role of both the functional safety manager and functional safety engineer.**

**Please answer the following questions:**

1. **What is the purpose of a development interface agreement?**
2. **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.**

**]**

# Confirmation Measures

*Points that serve purposes:*

*That a functional safety project conforms to ISO 26262*

*The project does really make the vehicle safer*

**[Instructions:**

**Please answer the following questions:**

1. **What is the main purpose of confirmation measures?**
2. **What is a confirmation review?**
3. **What is a functional safety audit?**
4. **What is 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.