

Safety Plan Lane Assistance

**Document Version: 1.0**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 8/9/2018 | 1.0 | Ajinkya Bhave | Safety Plan for Lane Assistance Item |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

[Document history](#_Toc524515730)

[Table of Contents](#_Toc524515731)

[Introduction](#_Toc524515732)

[Purpose of the Safety Plan](#_Toc524515733)

[Scope of the Project](#_Toc524515734)

[Deliverables of the Project](#_Toc524515735)

[Item Definition](#_Toc524515736)

[Goals and Measures](#_Toc524515737)

[Goals](#_Toc524515738)

[Measures](#_Toc524515739)

[Safety Culture](#_Toc524515740)

[Safety Lifecycle Tailoring](#_Toc524515741)

[Roles](#_Toc524515742)

[Development Interface Agreement](#_Toc524515743)

[Confirmation Measures](#_Toc524515744)

# Introduction

## Purpose of the Safety Plan

A safety plan provides an overall framework for a functional safety project. It also defines the responsibilities of the various actors involved in the project. The output of the design, implementation, and production phases are checked against the safety plan to ensure compliance.

## 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 to be analysed is the Lane Assistance (LA) system. This system alerts the driver when the vehicle is accidentally leaving the lane and attempts to steer the vehicle back to the centre of the lane.

This item has two functions:

1. Lane Departure Warning (LDW)
2. Lane Keeping Assistance (LKA)

The LDW function shall apply an oscillating steering torque to provide the driver a haptic feedback. The LKA function shall apply the steering torque when active in order to stay in ego lane.

The camera subsystem, the electronic power steering (EPS) subsystem, and the steering subsystem are responsible for the functions of the LA system.

The architecture and boundary of the item is shown in the figure below. The steering wheel is not included in the item.



# Goals and Measures

## Goals

The major goal is to follow the ISO 26262 framework to analyse the lane assistance system to: identify hazards, evaluate the risk in each hazardous situation, and prevent accidents from occurring by lowering the risk to reasonable levels methodically**.**

## 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

In my company, the following characteristics describe the safety culture followed and how it is maintained:

1. Safety has the highest priority among competing constraints like cost and productivity.
2. Processes are in place that ensure accountability such that design decisions are documented and traceable back to the people and teams who made the decisions.
3. The company motivates and supports the achievement of functional safety.
4. The company penalizes shortcuts that jeopardize safety or quality.
5. Teams who design and develop a product are independent from the teams who audit the work.
6. Company design and management processes are clearly defined and accessible.
7. Each project has the necessary resources including people with appropriate skills.
8. Intellectual diversity is sought after, valued and integrated into processes.
9. Communication channels encourage disclosure of problems without fear of being called out.

# 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

Please answer the following questions:

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

A Development Interface Agreement (DIA) 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.

The OEM is responsible for defining the functional and safety requirements, and system architecture at the item level. My company will be responsible for the technical safety requirements at the component level, including detailed software requirements, and the component-level software architecture. In summary, the OEM will be responsible for the product development at the item level while my company will be responsible for the software product development at the component level. I am assuming hardware is out of scope for this document.

# Confirmation Measures

1. What is the main purpose of confirmation measures?

Confirmation measures serve two purposes:

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

1. What is a confirmation review?

A review that 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.

1. What is a functional safety audit?

An audit that checks to make sure that the actual implementation of the project conforms to the safety plan.

1. What is a functional safety assessment?

An assessment confirming that plans, designs and developed products actually achieve functional safety.

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.