

Safety Plan Lane Assistance

**Document Version: 1.1**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 21/06/2017 | 1.0 | EB | Initial version |
| 13/04/2019 | 1.1 | Ahmed Belal | Fill the document missing data |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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 safety plan is covered in part2 of ISO 26262 (Management of functional safety).

It gives an introduction about the system under analysis while defining the parts needs to be included in the safety activities from the V model. It also defines the resources needed to finish the safety activities and the role of the different entities and their exact deliveries. Finally, it defines the procedures needed to make sure that the system follows the ISO 26262 standards and that it does increase the safety of the implemented system.

Safety plan covers many subsections:

* Introduction: Covered in this section. Contains an overview of the system and the documents to be included.
* Item definition: Defines which particular vehicle system will be under analysis.
* Goals and measures: Discuss the goals of the project and which activities will be included.
* Safety life cycle tailoring: Discuss which part of the V model will be included in the safety project. We may be reusing the system from another one, or we made small parts of modifications, so the safety documents will only focus on the modified implemented subsystem.
* Resources required in the project: Define the resources needed for the project and the role of each team member.
* Supporting processes management: Discusses the systems engineering management, the methods used and the confidence level of the tools used.
* Development Interface Agreement (DIA): Discusses the deliveries needed, and the agreement between both OEM, and tier-1 supplier, or between tier-1 supplier, and tier-2 supplier.
* Project Schedule plan: The calendar of what tasks will be completed.
* Confirmation measures: Reports what will be done to prove that functional safety is achieved and that the functional safety activities increase the safety level of the implemented system.

## The scope of the Project

**[Instructions: Nothing to do here. This is for your information.]**

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

**[Instructions: Nothing to do here. This is for your information.]**

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 section defnes the particular vehicle system under analysis.

This project focuses on lane assistant system of the car. It has two main functionalities: lane departure warning, and lane keeping assistance.

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.

In the lane keeping assistance, The system will move the steering wheel back towards the lane center. This steering input will not occur if the driver owns steering, accelerating, or using turn signal.

In the lane keeping warning, the system will vibrate the steering wheel.

Lane Departure Warning Systems and Lane Keeping Systems rely on visible lane markings. They typically cannot decipher faded, missing, or incorrect lane markings. Markings covered in snow or old lane markings left visible can hinder the ability of the system

**What are the boundaries of the item? What subsystems are inside the item? What elements or subsystems are outside of the item?**

**OPTIONAL**

**Optionally, include information about these points as well. These were not included in the lectures, but you might be able to find this information online:**

* **Operational and Environmental Constraints. This could especially be limited to camera performance; lane lines are difficult to detect in snow, fog, etc**
* **Legal requirements in your country for lane assistance technology**
* **National and International Standards Related to the Item**
* **Records of previously known safety-related incidents or behavioral shortfalls**

**]**

# Goals and Measures

## Goals

Make sure that the lane keeping assistance feature is implemented safely, will not lead to injury or harm to humans and provide a safety case that has evidence that the implemented E/E system is safe to be used.

The possible risks have to be identified, and actions have to be taken in the implemented system to lower the risk to reasonable levels.

## Measures

|  |  |  |
| --- | --- | --- |
| Measures and Activities | Responsibility | Timeline |
| Follow safety processes | All Team Members | Constantly |
| Create and sustain a safety culture | Safety Manager | 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

The organization should motivate the achievements of functional safety.

The organization penalizes the act of not following the safety guidelines.

The rules of each team member are defined accurately.

All the decisions are well documented, and they can be traced back to their makers, and their editors by dates.

Audits for low-risk components are done by other team members other than the implementation team. An external audit does audits for high-risk components.

DIA defines the interactions with external companies and accurately identifies the rules of each one of the parties.

# Safety Lifecycle Tailoring

The following sections will be involved from the V model of ISO 26262:

* Concept phase
* Product Development at the System Level
* Product Development at the Software Level

# Roles

**[Instructions:**

**This section is here for your reference. You do not need to do anything here. It is provided to help with filling out the development interface agreement section.**

**]**

|  |  |
| --- | --- |
| 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

**[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?**

DIA is the full agreement between all the organizations involved in the safety activities in the project, and it contains the following sections:

* Record of the appointment of customer and supplier safety managers.
* Joint tailoring of the safety life cycle.
* Activities and processes to be performed by the supplier.
* Information and work products to be exchanged.
* Parties or persons responsible for each activity in the design and the production   
   phases.
* Any supporting processes or tools to ensure compatibility between customer and   
   supplier technologies.

The responsibilities of the OEM are:

* Identify the system description, and the High-Level Requirements (HLRs)
* Identify the definitions for the items involved in the project
* Define the safety activities that need to be involved in the system
* Do audits or hire a third party to do the audit during and after the   
   implementation of the system

The responsibilities of EB as a tier-1 supplier are:

* Identify the hazards that may occur in the system
* Define the Low-Level Requirements of the system
* Design the system on the component level
* Develop the system on both the system and software level
* Integration between the sub-components of the developed systems
* Make sure that all the activities follow the ISO 26262 standard

# Confirmation Measures

The main purpose of confirmation measures is to ensure that the people who developed the product and who reviewed it are independent parties and it checks the following:

* Make sure that processes comply with the functional safety standard
* Make sure that the project execution is following the safety plan
* Make sure that the design improves the safety

Ordinary reviews should be done after finishing a document. It can be a peer review, or it can be another team within the same company.

Safety audits ensure that the design and production implementation conform to the safety plan and ISO 26262 standard and this type of audit have to be independent of the team developing the project.

Safety assessment ensures that functional safety is achieved. This type of audit has to be independent of the team developing the project.

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.