

Safety Plan Lane Assistance

**Document Version: [v1.0]**

**Template Version 1.1, Released on 2019-01-30**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 1/28/2019 | 1.0 | Dylan Brandtner | Initial version |
| 1/30/2019 | 1.1 | Dylan Brandtner | Updates from review |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

[Document history](#_Toc536185493)

[Table of Contents](#_Toc536185494)

[Introduction](#_Toc536185495)

[Purpose of the Safety Plan](#_Toc536185496)

[Scope of the Project](#_Toc536185497)

[Deliverables of the Project](#_Toc536185498)

[Item Definition](#_Toc536185499)

[Goals and Measures](#_Toc536185500)

[Goals](#_Toc536185501)

[Measures](#_Toc536185502)

[Safety Culture](#_Toc536185503)

[Safety Lifecycle Tailoring](#_Toc536185504)

[Roles](#_Toc536185505)

[Development Interface Agreement](#_Toc536185506)

[Confirmation Measures](#_Toc536185507)

# Introduction

## Purpose of the Safety Plan

**[Instructions: Answer what is the purpose of a safety plan?]**

The purpose of this safety plan is to outline the steps we plan to take to ensure the lane assistance system is functionally safe and assign roles and responsibilities to accomplish this.

## 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

**[Instructions:**

**REQUIRED**

**Discuss these key points about the system:**

**What is the item in question, and what does the item do?**

The Lane Assistance item is an ADAS system that alerts the user if it is drifting outside of its lane without using a turn signal and assists the driver in steering back into their lane.

**What are its two main functions? How do they work?**

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
* the **lane keeping assistance function** will move the steering wheel so that the wheels turn towards the center of the lane

**Which subsystems are responsible for each function?**

The camera, the electronic power steering, and car display subsystems are responsible for the above functions.

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

The boundaries of this system are described in the image below. 

**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

**[Instructions:**

**Describe the major goal of this project; what are we trying to accomplish by analyzing the lane assistance functions with ISO 26262?]**

The goal of analyzing the lane assistance functions with ISO 26262 is to reduce risk to acceptable levels and create a product that is functionally safe.

## Measures

**[Instructions:**

**Fill in who will be responsible for each measure or activity. Hint: The lesson on Safety Management Roles and Responsibilities.**

**The options are:**

**All Team Members**

**Safety Manager**

**Project Manager**

**Safety Auditor**

**Safety Assessor**

**]**

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

**[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**

**]**

We maintain a good safety culture by ensuring the following:

* Safety is the highest priority
* Team members are accountable for decisions impacting safety, and rewards and penalties are given when appropriate
* Development and safety auditing are kept independent to avoid bias
* Safety processes are well defined
* Projects have the necessary safety resources
* Intellectual diversity and communication is sought after and valued

# Safety Lifecycle Tailoring

**[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**

**]**

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

**[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?**

The development interface agreement serves to:

* Clarify the responsibilities of the different parties involved in a functional safety project
* Describe the work products that each company will provide
* Help avoid disputes between companies
* Clarify who will be responsible for any safety issues in post-production

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.**

We (Tier 1) are responsible for the functional safety of the camera, the electronic power steering, and car display subsystems as they relate to the lane assistance system.

OEM is responsible for overall item functional safety management, auditing, and assessing.

**]**

# Confirmation Measures

**[Instructions:**

**Please answer the following questions:**

1. **What is the main purpose of confirmation measures?**

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

1. **What is a confirmation review?**

A confirmation review ensures that the project complies with ISO 26262.

1. **What is a functional safety audit?**

A function safety audit ensures that the actual implementation of the project conforms to the safety plan

1. **What is a functional safety assessment?**

A functional safety assessment confirms 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.