

Safety Plan Lane Assistance

**Document Version: [Version]**

**Template Version 1.0, Released on 2018-06-23**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 2018-06-23 | 1.0 |  | Initial Draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# Table of Contents

[Document history 2](#_Toc517299135)

[Table of Contents 2](#_Toc517299136)

[Introduction 3](#_Toc517299137)

[Purpose of the Safety Plan 3](#_Toc517299138)

[Scope of the Project 3](#_Toc517299139)

[Deliverables of the Project 3](#_Toc517299140)

[Item Definition 4](#_Toc517299141)

[Goals and Measures 5](#_Toc517299142)

[Goals 5](#_Toc517299143)

[Measures 5](#_Toc517299144)

[Safety Culture 6](#_Toc517299145)

[Safety Lifecycle Tailoring 6](#_Toc517299146)

[Roles 6](#_Toc517299147)

[Development Interface Agreement 7](#_Toc517299148)

[Confirmation Measures 7](#_Toc517299149)

# Introduction

## Purpose of the Safety Plan

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

## 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

**[Instructions:**

**REQUIRED**

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

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

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

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

**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

**[Instructions:**

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

## 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

Below are the characteristics of our safety culture:

* **High priority**: safety has been given the highest priority among competing constraints like cost and productivity
* **Accountability**: processes which we follow ensures accountability such that design decisions are traceable back to the people and teams who made the decisions
* **Rewards**: we motivates and supports the achievement of functional safety
* **Penalties**: we penalizes shortcuts that jeopardize safety or quality
* **Independence**: teams who design and develop a product are independent from the teams who audit the work
* **Well defined processes**: our design and management processes are clearly defined
* **Resources**: here we have projects which have necessary resources including people with appropriate skills
* **Diversity**: intellectual diversity is sought after, valued and integrated into processes
* **Communication**: we have various communication channels to encourage disclosure of problems

# 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**

**]**

# 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

**Purpose**:  To define the roles and responsibilities between OEM involved in developing the system and to ensure that all parties are developing safe vehicles in compliance with ISO 26262

In this project, the OEM is supplying a functioning lane assistance system. We as functional safety engineer sharing social responsibility need to analyze and modify the various sub-systems from a functional safety viewpoint.

# Confirmation Measures

Confirmation measures serve two purposes:

1. Functional safety project conforms to ISO 26262, and
2. The project really does make the vehicle safer.

The people who carry out confirmation measures need to be independent from the people who actually developed the project.

There are various different ways to carry out confirmation measures listed below:

##### **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.

##### **Functional 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.