

Safety Plan Lane Assistance

**Document Version: 1.0**

**Version 1.0, Released on 2018-05-18**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 2018-05-18 | 1.0 | Navin Rawther | First Draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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 defines the steps that are to be taken to achieve functional safety. It defines the goals and measures and roles and responsibilities to ensure that important safety design steps are not missed.

## 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

The Goal of this Safety Plan is to reduce risks to reasonable levels by identifying hazards that could lead to accidents, evaluating the risks associated with each hazard and using systems engineering to lower risks to acceptable levels.

## 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

Safety is the highest priority for our company among other constraints such as cost and productivity. We have incorporated the following to ensure this:

* **Accountability** in processes such that design decisions are traceable back to the people and teams who made the decisions
* **Rewards** that motivates and supports the achievement of functional safety
* **Penalties** that penalizes shortcuts that jeopardize safety or quality
* **Independence** betweenteams who design and develop a product and the teams who audit the work
* **Well defined processes** for design and management
* **Resources** in projects by including people with appropriate skills
* **Diversity** integrated into processes as they are highly valued
* **Communication** channels to encourage disclosure of problems

# 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

The Development Interface Agreement (DIA) defines the roles and responsibilities between the OEM and the Tier-1 company involved in developing the lane assistance system.

The OEM is responsible for providing a functional lane assistance system. The Tier-1 company is responsible for analyzing and modifying the sub-systems of the lane assistance system from a functional safety viewpoint. The Tier-1 company will be responsible for finding and fixing the safety problems in the lane assistance system.

# Confirmation Measures

The confirmation measures ensures:

* that the functional safety project conforms to ISO 26262, and
* that the project does make the vehicle safer.

The confirmation review ensures that the project compiles 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.

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

The functional safety assessment is the process of confirming that plans, designs and developed products actually achieve functional safety.