

Safety Plan Lane Assistance

**Document Version: [Version]**

**Template Version 1.0, Released on 2017-06-21**



# Document history

**[Instructions: Fill in the date, version and description fields. You can fill out the Editor field with your name if you want to do so. Keep track of your editing as if this were a real world project.**

**For example, if this were your first draft or first submission, you might say version 1.0. If this is a second submission attempt, then you'd add a second line with a new date and version 2.0]**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 01.04.2018 | 1.0 | Siddarth Kothiwale | First Try |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# 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

Safety Plan first defines the broad scope for functional safety and steps needed and also roles and responsibilities of the people involved so that functional safety can be achieved

## 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 system under consideration is the lane assistance system

The item will alert the driver if the vehicle leaves the lane by vibrating the steering and then helps the driver in bringing the car back to the center.

When the driver drifts towards the edge of the lane, two things will happen:

1. the lane departure warning function will vibrate the steering wheel
2. the lane keeping assistance function will move the steering wheel so that the wheels turn towards the center of the lane

The subsystem responsible for each functions are:

1. Camera system
2. Electronic Power Steering system
3. Car Display system

The boundaries of the item are shown in figure below:

Answer:

**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:**

# Goals and Measures

## Goals

The goal of this project is functional safety. We are trying to bring down the risks involved in the driver assistance system to acceptable level.

## 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

The Charecteristics of safety culture are:

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

# Safety Lifecycle Tailoring

Safety Lifecycle Tailoring aims at using as many pre-existing steps in the safety lifecycle as possible and concentrating only on the parts impacted by the changes.

The following phases are in scope:

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

# 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

A DIA (development interface agreement) 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 Tier-1 supplier will analyze and modify the subsystem in the roles of Functional safety engineer and functional safety manager.

SafetyManager: The roles include writing the safety plan and monitoring

Safety Engineer: Architectural design and implementation

# Confirmation Measures

Confirmation measures serve two purposes:

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

# 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.

# Function 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

Answer: 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.