

Safety Plan Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 5/21/18 | 1.0 | Yue | First attempt |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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 purpose of this safety plan is to provide a comprehensive framework for the Lane Assistance item, and to define roles for this item to be under analysis.

## 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 Lane Assistance system attempts to keep the vehicle in the canter of the lane and alerts the driver when the vehicle has departed the lane.

The Lane Assistance system will have to functions:

1. Lane departure warning
2. Lane keeping assistance

The lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback.

The lane keeping assistance function shall apply the steering torque when active in order to stay in ego lane.

The Camera system, the Electronic Power Steering system and the Car Display system are all responsible for both of the functions.



# Goals and Measures

## Goals

Ensure the Lane Assistance system safety.

Analyze various electronic and electrical system malfunctions to prevent accident.

## Measures

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

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

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 purpose of the development interface agreement is to assign responsibilities to OEM and Tier-1.

Functional Safety Manager- Item Level

* Planning, coordinating and documenting of the development phase of the safety lifecycle
* Tailors the safety lifecycle
* Maintains the safety plan
* Monitors progress against the safety plan
* Performs pre-audits before the safety auditor

Functional Safety Engineer- Item Level

* Item development
* Integration
* Testing at the hardware, software and item levels

Project Manager - Item Level

* Item management
* Acquires and allocates resources needed for the functional safety activities
* Appoints safety manager or might act as safety manager

Functional Safety Manager- Component Level

* Planning, coordinating and documenting of the development phase of the safety lifecycle
* Tailors the safety lifecycle
* Maintains the safety plan
* Monitors progress against the safety plan
* Performs pre-audits before the safety auditor

Functional Safety Engineer- Component Level

* Component development
* Integration
* Testing at the hardware, software and component levels

Functional Safety Auditor

* Ensures that the design and production implementation conform to the safety plan and ISO 26262.
* Must be independent from the team developing the project

Functional Safety Assessor

* Independent judgement as to whether functional safety is being achieved via a functional safety assessment
* Must be independent from the team developing the project

# Confirmation Measures

Confirmation measures serve two purposes:

* A functional safety project conforms to ISO 26262
* The project really does make the vehicle safer.

The Confirmation Measures has three parts:

* 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.