

Safety Plan Lane Assistance

**Document Version: v1.0**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 12/17/2017 | V1.0 | Joshua Schoenfield | First Submission |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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 an overall framework for achieving functional safety for the Lane Assistance item. The plan will also assign roles and responsibilities for achieving functional safety associated with that item

## 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 Item alerts a driver that the vehicle has accidentally departed or is accidentally departing its lane, and attempts to steer the vehicle back towards the center of the lane.

The Lane Assistance Item will have two functions:

1. Lane departure warning
2. Lane keeping assistance

When the driver drifts towards the edge of the lane, the lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback.

When the driver drifts towards the edge of the lane, the lane keeping assistance function shall apply the steering torque when active in order to stay in ego lane.

The camera subsystem, the electronic power steering subsystem and the car display system are responsible for each of the functions.

The boundary of this item is displayed in the following figure, indicating that the item contains elements from the camera subsystem, the power steering subsystem and the car display system, but that the steering wheel is outside of the item’s scope:



# Goals and Measures

## Goals

By analyzing the lane assistance functions with ISO 26262, we are able to work systematically towards reduction of risk associated with this item to an acceptable level. Furthermore, the documentation prescribed by the ISO 26262 standard ensures that the company and workers can readily demonstrate that best practices have been followed.throughout development, testing and production.

## 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

As a company dedicated to maintaining a good safety culture, we emphasize several points:

* Safety is a **High Priority**: Safety has the highest priority, even relative to interests such as cost and productivity
* Culture of **Accountability**: Design decisions affecting safety are traceable back to the peoople and teams who made those decisions because of processes that ensure accountability
* **Rewards**: The achievement of functional safety is motivated throughout the organization
* **Penalties**: Shortcuts that jeopardize safety or quality are penalized by the organization
* **Independence**: The persons and teams who audit safety are independent of the teams that develop and design a product
* **Well defined processes**:Both design and management processes are clearly defined
* Allocation of adequate **Resources**: All projects are given sufficient resources to achieve functional safety, including personnel
* Intellectural **Diversity**: A range of viewpoints is assembled and valued and integrated into processes
* **Communication**: Open communication about safety ensures that problems are disclosed

# Safety Lifecycle Tailoring

For this 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

A Development Interface agreement, or DIA, specifies the roles and responsibilities that different companies involved in developing a product are responsible for. Furthermore, it will lay out what work products and evidence that each party will provide to demonstrate that the agreement has been fulfilled. Such an agreement will help avoid disputes, allocate liability, and make clear who should fix various safety issues.

As a Tier-1 organization, we will be responsible for supplying and analyzing the various subsystems (Camera, Electronic Power steering and Car Display System) and components that comprise the complete Lane Assistance item. Throughout, a functional safety viewpoint should be applied to both the analysis and modifications of any subsystems. The OEM is supplying a safely functioning lane assistance system. As such, the project manager at the item level shall be a member of the OEM’s team. The safety manager and safety engineer at the item level shall also be a member of the OEM team. The component level safety manager and safety engineer shall be members of the Tier-1 supplier. The auditors and assessors shall come from an external team or an unrelated OEM team.

# Confirmation Measures

The main purpose of confirmation measures is to ensure that a functional safety project conforms to ISO 26262 and that the project has succeeded in actually making the vehicle safer.

A confirmation review consists of an independent person reviewing the work as the product is designed and developed to ensure that ISO 26262 is being followed. Such a review ensures that the project complies with the necessary standard.

A functional safety audit is a check to confirm that the actual implementation of the project conforms to the safety plan as previously designated.

A functional safety assessment confirms that the plans, designs and deveoped products have actually achieved 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.