

Safety Plan Lane Assistance

**Document Version: [Version]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 20/May/2018 | 1.0 | Arpit Srivastava | Safety Plan |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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 sets up a gudeline for lane assistance. The safety plan in addition to being a guideline is also a reference for roles and responsibilities.**

## Scope of the Project

**[Instructions: Nothing to do here. This is for your information.]**

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

**[Instructions: Nothing to do here. This is for your information.]**

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 item being discussed is the lane assistance item.

Main functions include:

* **Lane departure warning function**: This handles those cases where the vehicle enroaches the edge of the drivable portion. A warning in the form of vibration is triggered to warn the driver.
* **Lane keeping assistance function**: The lane keeping assistance function serves as a corrective measure which corrects the steering wheel towards the opposite side to help the car get back into the lane center and drive safely.

The implementation is as follows:

* **Camera sensors**:
  + Camera sensor
  + Camera sensor ECU (Electronic Control Unit)
* **Electronic Power Steering subsystem**:
  + Driver Steering Torque Sensor.
  + Electronic Power Steering ECU.
  + Motor Proving Torque to Steering Wheel.
* **Car Display subsystem**:
  + Car Display ECU
  + Car Display

The above information is visualised as follows:



The chain of triggers works as follows:

* The camera detects lane departure, and triggers a signal to the electronic power steering system to turn and vibrate the steering wheel.
* A warning light also turns on in the car Thus, the driver knows that the lane assistance system is active.
* Additionally, If there’s a turn signal, the lane assistance system deactivates to allow turning.
* The driver being aware of the departure from lane, may turn off the system, to take over and perform corrective measures.
* The system will assist the driver in that case by adjusting to the corrective measure taken by the driver.

# Goals and Measures

## Goals

1. Identify risk and hazardous situations in the Line Assistance system components malfunction causing injuries to a person.
2. Evaluate the risks of the hazardous situations.
3. Low to risk of the malfunctions to a reasonable levels acceptable by current sociatity.

## 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 | All Team Members | 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

Here are the characteristics of prevalent safety culture:

Here are some characteristics of a good 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

**[Instructions:**

**This section is here for your reference. You do not need to do anything here. It is provided to help with filling out the development interface agreement section.**

**]**

|  |  |
| --- | --- |
| 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

**[Instructions:**

**Assume in this project that you work for the tier-1 organization as described in the above roles table. You are taking on the role of both the functional safety manager and functional safety engineer.**

**Please answer the following questions:**

1. **What is the purpose of a development interface agreement?**
2. **What will be the responsibilities of your company versus the responsibilities of the OEM? Hint: In this project, the OEM is supplying a functioning lane assistance system. Your company needs to analyze and modify the various sub-systems from a functional safety viewpoint.**

**]**

The purpose of DIA is to clearly assign roles and responsibilities of the portfolio’s and ensure that ISO 26262 is rigourously implemented.

The responsibilities are as follows:

### **ROLE**

### **JOB DESCRIPTION**

Safety Auditor makes sure that the project conforms to the safety plan

Test Manager planning and overseeing testing activities

Safety Manager pre-audits, plans the development phase

Safety Assessor judges whether the project has increased safety

Project Manager allocates resources as needed

Safety Engineer develops prototypes, integrates sub systems into larger systems

# Confirmation Measures

**[Instructions:**

**Please answer the following questions:**

1. **What is the main purpose of confirmation measures?**
2. **What is a confirmation review?**
3. **What is a functional safety audit?**
4. **What is a functional safety assessment?**

**]**

### **Confirmation Measures Purpose**

Confirmation measures serve two purposes:

* that a functional safety project conforms to ISO 26262, and
* that 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.

### **Confirmation Measures Definitions**

### 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.