

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 |
| 5/16/2018 | 1.0 | Shivam Jaiswal | First Attempt |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

**[Instructions: We have provided a table of contents. If the table of contents is not showing up correctly in your word processor of choice, please update it. The table of contents should show each section of the document and page numbers or links. Most word processors can do this for you. In** [**Google Docs**](https://support.google.com/docs/answer/116338?co=GENIE.Platform%3DDesktop&hl=en)**, you can use headings for each section and then go to Insert > Table of Contents.** [**Microsoft Word**](https://support.microsoft.com/en-us/help/285059/how-to-create-a-table-of-contents-by-marking-text-in-word) **has similar capabilities]**

[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

**[Instructions: Answer what is the purpose of a safety plan?]**

A Safety plan provides an overall framework for a functional safety project. The purpose of this safety plan is to provide an overall framework for the Lane Assistance item, and to assign roles and responsibilities functional safety items.

## 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?**

The name of item under consideration in this functional safety module is **Lane Assistance System.** The Lane Assistance item alerts the driver that the vehicle has accidentally departed its lane, and attempts to steer the vehicle back towards the center of the lane.

**What are its two main functions? How do they work?**

A **Lane Assistance System** has two main function:

* **Lane Departure Warning:** Lane Departure Warning is functionality that vibrates the steering wheel when the driver drifts away from center. Thus Lane Departure Warning helps driver to take appropriate action immediately. The lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback.
* **Lane Keeping Assistance:** Lane Keeping Assistance is functionality that turns the steering wheel back towards the center of the lane if driver starts to drift away from center. The lane keeping assistance function shall apply the steering torque when active in order to stay in ego lane.

**Which subsystems are responsible for each function?**

The item boundary was drawn to include three sub-systems:

* **Camera system:** The Camera System is composed of two components:

1. **Camera Sensor**
2. **Camera Sensor ECU (Electronic Control Unit)**

The camera system helps in lane keeping assistance.

* **Electronic Power Steering system:** The Electronic Power Steering system is composed of three components:

1. **Driver Steering Torque Sensor**
2. **Electronic Power Steering ECU**
3. **Motor Providing Torque to Steering Wheel**

The electronic power steering system helps in both lane keeping assistance aswell as lane departure warning.

* **Car Display system:** The Car Display systemis composed of two components

1. **Car Display ECU**
2. **Car Display**

The car display system helps to display lane departure warning.

**What are the boundaries of the item? What subsystems are inside the item? What elements or subsystems are outside of the item?**

**Lane Assistance System Boundary:**

****

The item boundary was drawn to include three sub-systems:

* Camera system
* Electronic Power Steering system
* Car Display system

**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

**[Instructions:**

**Describe the major goal of this project; what are we trying to accomplish by analyzing the lane assistance functions with ISO 26262?]**

The major goal of this project:

* Identify high risk situations in Lane Assistance system
* Lower risk to reasonable which is acceptable by society.

## 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

**[Instructions:**

**Describe the characteristics of your company's safety culture. How do these characteristics help maintain your safety culture. Hint: See the lesson about Safety Culture**

**]**

Below are the characteristics of company’s 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

**[Instructions:**

**Describe which phases of the safety lifecycle are in scope and which are out of scope for this particular project. Hint: See the** [**Intro section**](#_sh22j99mm02k) **of this document**

**]**

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?**

* 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 DIA also specifies what evidence and work products each party will provide to prove that work was done according to the agreement.
* The ultimate goal is to ensure that all parties are developing safe vehicles in compliance with ISO 26262.

1. **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.**

**]**

Major Roles and Responsibilities in Functional Safety for Lane Assistance System would be:

**Project Manager**

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

**Safety Manager**

* 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

**Safety Engineer**

* Product development
* Integration
* Testing at the hardware, software and system levels

**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

**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

**Test Manager**

* Plans testing activities
* Coordinates testing to show that the vehicle system works correctly



# Confirmation Measures

**[Instructions:**

**Please answer the following questions:**

1. **What is the main purpose of confirmation measures?**

Confirmation measures serve two purposes:

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

1. **What is a 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. The people who carry out confirmation measures need to be independent from the people who actually developed the project.

1. **What is a 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.

1. **What is a 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.