

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 |
| 17/05/18 | 1.0 | Trijeet | Initial Draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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?]**

The purpose of the safety is to provide an overview of how safe the system is and what measures shall be taken to ensure its safeness. It identifies the responsibilities of personnel that are involved in the functional safety of the lane assistance system, including the steps that are to be performed to adhere to the safety precautions.

## 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

**[Instructions:**

**REQUIRED**

**Discuss these key points about the system:**

**What is the item in question, and what does the item do?**

The lane assistance system is the primary target of this project. The system must have a feedback procedure that warns the driver as and when the car drifts away from the drivable portion of the lane, i.e. towards edges. Ideally the car should drive keeping to the center of the lane. Hence the feedback should assist the driver to keep to the center of the lane or otherwise drive back to the center of the lane whenever the car goes off-center.

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

The lane assistance system must have at least the following two functions:

1. **Lane Departure Warning** whenever the car drifts off-center of the lane. This warning may then be translated into a steering torque so as to drive the car back to the lane's center.
2. **Lane Keeping Assistance** to help the car stay on the center of the track as the lane turns. Similar to the above, the assistance function then may be translated to steering torque for the car so that the car turns proportionately to the turn of the lane, thereby preventing over-turning or under-turning.

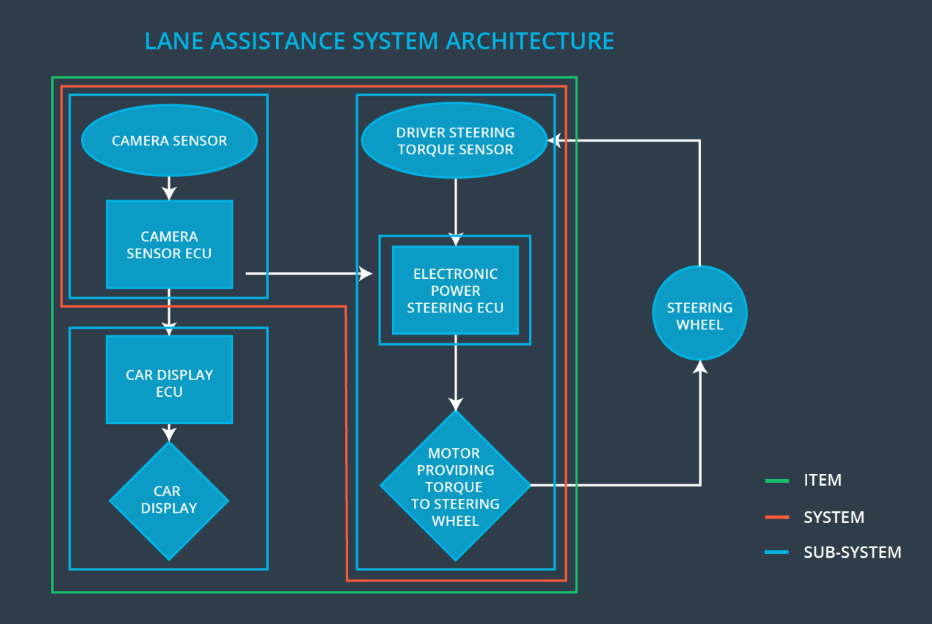
**Which subsystems are responsible for each function?**

The above functions are dependent on the following subsystems:

1. **Camera sensor**, that senses the lane environment and the car’s drift from the lane’s center.
2. **Electronic power steering ECU**, that takes input from the camera subsystem and calculates the amount of torque required on the steering wheel. The torque is actuated by a motor attached to the steering wheel.
3. **Display ECU**, that provides continuous visual feedback to the driver.

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

The following diagram describes the boundary and the subsystems inside and outside of it:



**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 goal in this project is to make sure that the operations of the Lane Departure Warning and Lane Keeping Assistance functionalities operate safely and reliably. This includes identification of potential risks that exists and possible hazards that might occur during operation and finally come up with a plan that minimizes the risks to some reasonably acceptable level.

## Measures

**[Instructions:**

**Fill in who will be responsible for each measure or activity. Hint: The lesson on Safety Management Roles and Responsibilities.**

**The options are:**

**All Team Members**

**Safety Manager**

**Project Manager**

**Safety Auditor**

**Safety Assessor**

**]**

|  |  |  |
| --- | --- | --- |
| Measures and Activities | Responsibility | Timeline |
| Follow safety processes | All Team Members | Constantly |
| Create and sustain a safety culture | Safety Manager | 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**

**]**

* **Priority**: We ensure that safety is considered with the highest priority and not just cost and productivity.
* **Accountability**: We ensure that all design decisions are tractable to the respective teams who made the decisions.
* **Rewards**: We encourage employees to notify instances of incorrect process during the development.
* **Penalties**: While meeting functional safety should be mandatory, any negligence in this regard is severely penalized. It may also lead to termination of the employee.
* **Independence**: To prevent any bias, the design & development teams are always kept independent of the audit team.
* **Well defined process**: All design and development processes are well defined and documented.
* **Resources**: We have all necessary resources including employees with appropriate skills who are allocated to this project.
* **Diversity**: Intellectual diversity is always valued in our company.
* **Communication & Disclosure**: Communication between the teams are encouraged with full 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**

**]**

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?**

The purpose of the DIA (Development Interface Agreement) is to make sure that each individual or party involved in the development process ultimately delivers a safe product 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.**

The responsibility of OEM is to provide with a working lane assistance system and supervise the activities in the scope of project manager, safety manager and safety engineer at the item level. Our company will conduct the activities in the scope of safety manager and safety engineer at the component level.

**]**

# Confirmation Measures

**[Instructions:**

**Please answer the following questions:**

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

The purpose of the confirmation measure is to make sure that the processes adhere to the functional safety standards laid down in ISO 26262. It also ensures whether that the project is being executed following the safety plans.

1. **What is a confirmation review?**

An independent person provides the confirmation review to confirm that the design and development is in complies to ISO26262.

1. **What is a functional safety audit?**

Functional safety audit verifies that the project implementation adheres to the safety plans.

1. **What is a functional safety assessment?**

Functional safety assessment analyzes whether the plans, designs and developed products have achieved functional safety or not.

**]**

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.