

Safety Plan Lane Assistance

**Document Version: [V1.1]**



# 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 |
| 23-01-2019 | V1.1 | Liping S | Draft the safety plan |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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?]**

Safety plan provides an framework to manage the safety the of the system. It gives an overview of the project and documentation; define the target system for analysis; discuss the goals and measures of the project; define the required resources and supported management methods; gives the project schedule and reports what will be done to prove that functional safety has been achieve.

## 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 item in question is a simplified version of a Lane Assistance System. The item provides lane departure warning and lane keeping assistance.

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

The Lane Assistance System will have two functions:

Lane departure warning

Lane keeping assistance

When the driver drifts towards the edge of the lane, two things will happen:

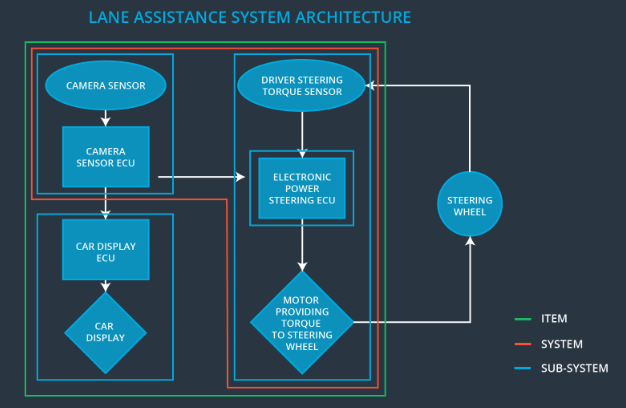
the **lane departure warning function** will vibrate the steering wheel

the **lane keeping assistance function** will move the steering wheel so that the wheels turn towards the center of the lane

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

There are three subsystems: Camera system, Electronic Power Steering system and Car Display system. The architecture and interaction between subsystems are shown on the attached diagram.

The camera system detects lane departures and tells the steering wheel how hard to turn. The driver receives a warning on the vehicle display and also receives a warning via a steering wheel vibrating. Simultaneously, the wheel adds extra steering torque to help the driver move back towards the center of the lane.



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

As shown on the above diagram, the green line defines the boundaries of the item. Inside the item, there are three subsystems: Camera system, Electronic Power Steering system and Car Display system. Elements like steering wheel and turn signal buttons are outside the item. Other subsystems in ADAS system like Adaptive Cruise Control, Automatic Parking, Blind Spot Monitoring, Tire Pressure Monitoring, Pedestrian Protection are also at outside.

**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 is to assure functional safety of the proposed system. By analyzing the lane assistance functions with ISO26262, the team can guide to identify hazards, evaluate the risk, and prevent accidents from occurring by lowering risk to reasonable levels via systems engineering.

## 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 | 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**

**]**

Ccharacteristics of 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 defines the roles and responsibilities between companies involved in developing a product. It 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.**

**]**

OEM:

Appoint safety manager

Supply hardware for prototyping and production

Define hardware safety lifecycle

Provide developing interfaces and hardware specifications and user guide.

Provide test data

The company:

Appoint safety manager

Supply system specifications

Define the system and subsystems, their functionalities and interfaces

Define system safety lifecycle

Provide functional safety analysis on the systems level and software level

Provide system verification and design documentation

# Confirmation Measures

**[Instructions:**

**Please answer the following questions:**

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

Confirmation measures serve two purpose:

. that a functional safety project conformas to ISO26262, and

. that 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.

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.