

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 |
| 6 Nov 2017 | 1.0 | Calvin Low | Initial Version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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 goal of this document is to list down how functional safety will be achieved for the use of lane assistance system in the entire development project and production environment. This safety plan lists the techniques and measures applied as part of the development to ensure targeted ASIL is achieved.

## 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

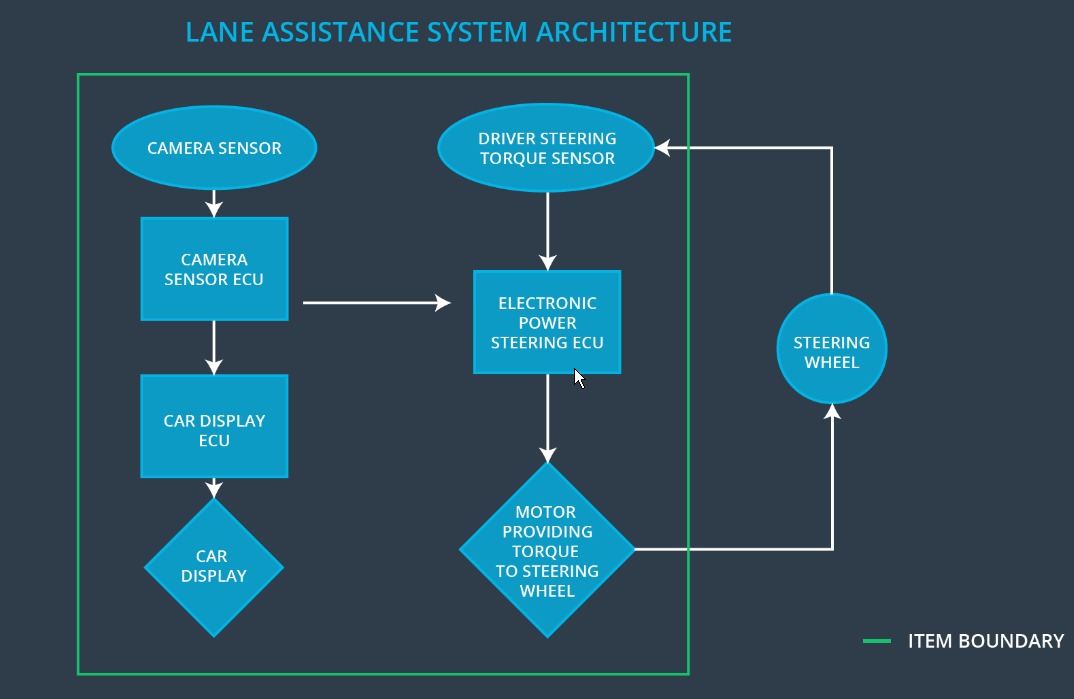
**[Instructions:**

**REQUIRED**

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

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

**Lane Assistance System Architecture**



Lane Assistance System (LAS) is a safety feature designed to alert driver in the event the vehicle moves from its lane unintentionally, and to assist the driver to navigate the car to stay on the current lane.

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

Two Main functions

1. Lane Departure Warning – This feature alerts the driver when the vehicle starts to deviate from the lane it is on and apply steering torque to provide the driver a feedback.
2. Lane keeping Assistance. This feature helps the car to stay near the center of lane.

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

|  |  |
| --- | --- |
| Subsystem | Function |
| Car Display Subsystem | Lane Departure Warning |
| Camera Sensor Subsystem | Lane Departure Warning / Lane keeping Assistance |
| Electronic Power Steering Subsystem | Lane keeping Assistance |
|  |  |
|  |  |

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

Looking at the architecture diagram, the LAS has the following subsystem

1. Car Display Subsystem
2. Camera Sensor Subsystem
3. Electronic Power Steering Subsystem

A camera sensor monitors the road and recognizes the lane structure. In the event a drift out of lane is detected, a signal is send to car display ECU to turn on the warning light and a signal is send to the Electronic Power Steering Subsystem to the steering wheel.

Subsystem out of the LAS

1. Automatic Parking system
2. Blind spot detector system
3. Pedestrian identifier 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 goals of the functional safety:

1. Identify the hazardous evens which might cause harm due to a electronic malfunction of Lane Assistance System.
2. Asses the risk associated with the identified hazards.
3. Lower the high level risk of hazardous environment to an acceptable risk level vis system 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 Assesor | 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**

**]**

**A good safety culture has the following characteristics:**

* **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?**

The development interface agreement (DIA) are a set of working agreement defining roles and responsibilities between companies involved in the product development. All parties would need to agree on the rules and content of the DIA before work can begin.

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 OEM is responsible for supplying a functional lane assistance system. As a tier-1 organization the following are the responsibilities:

* Provide functional safety requirements.
* Develop safety plan for hardware and software layer with OEM partner.
* Verify and validate the final product meets the functional safety requirement.

As a tier-1 organization the personals involved are:

* Tier-1 program manager who will communicate with OEM partners on product timeline, resource allocation and component selections.
* Tier-1 Safety manager develops safety plan and work with OEM safety manager during the project phase.

As a OEM organization the personals involved are:

* Project manager will manage the resource for the development of the lane assistance system based on the requirement provided by vendor. He/She will also need to communicate with the vendor program manager on product requirement and development schedule.
* Safety manager will work with tier-1’s safety manager to ensure requirements of the lane assistance system are meets as stated in the DIA.

# 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?**

**]**

The confirmation measure man purposes:

* Ensure the lane assistance system project meets ISO26262
* The lane assistance system makes the vehicle safer.

Confirmation Review – A third party safety auditor who is independent will review the work to ensure compliance with ISO26262 standards.

Functional Safety Audit – Ensure the implementation of the lane assistance system follows the requirement of safety plan.

Functional Safety Assessment – Ensure the plans, designs and product development actually achieve 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.