

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 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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 safety plan is identifying the various roles and resposibilities in the development process. It specifies how functional safety will be ensured throughtout the entire development project and in production.

## 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 this safety plan is the lane assistance system.

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

The two main functions are Lane Departure Warning Function and Lane Keeping Assistance Function. Lane Departure Warning Function vibrates the steering wheel when the driver drifts away from center by mistake. Lane Keeping Assistance Function turns the steering wheel back towards the center of the lane if the driver starts to drift away from center.

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

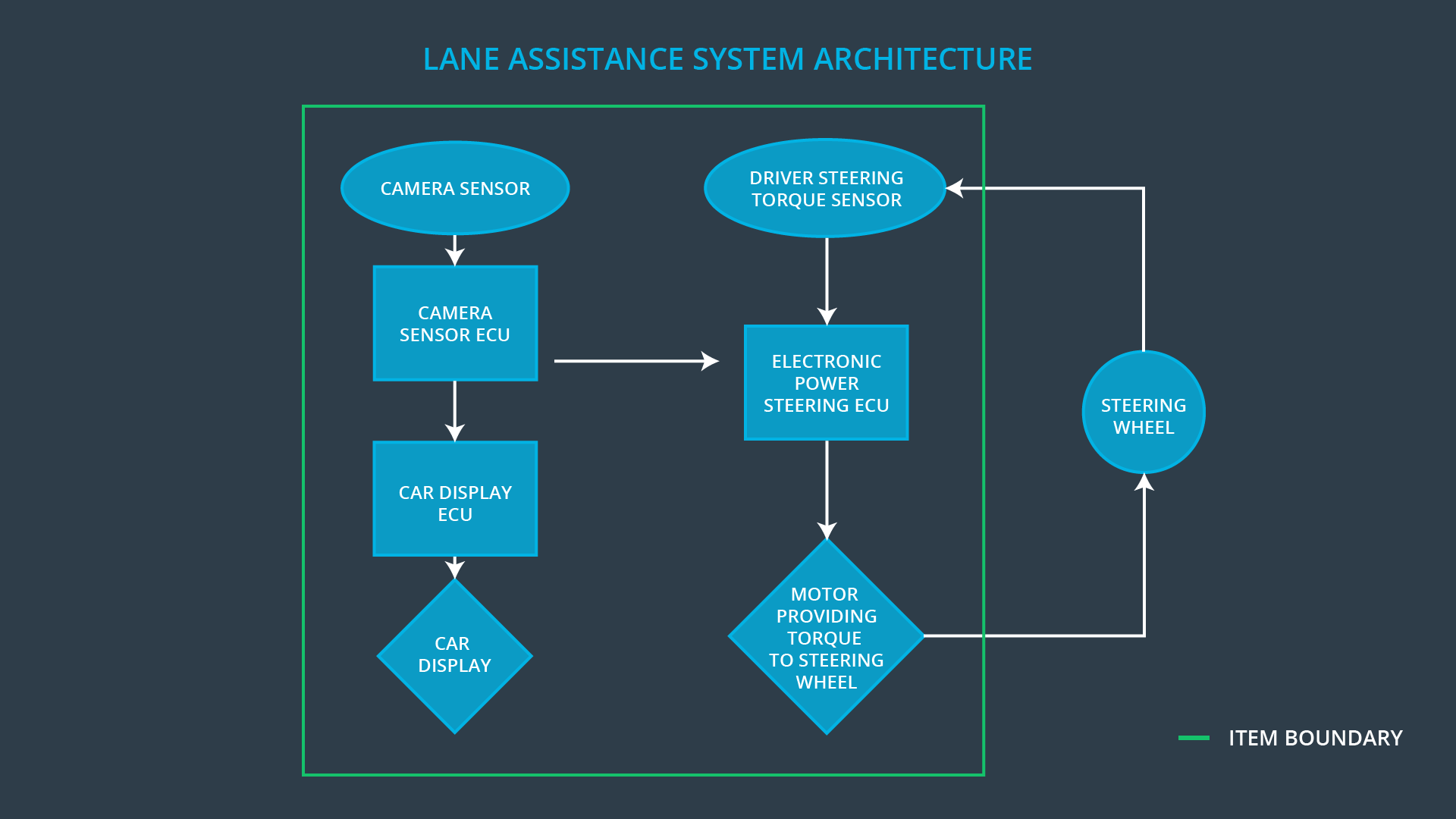
Camera subsystem is responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake.

Car Display subsystem is responsible for controlling the display to warn the drivers.

Electronic Power Steering subsystem is responsible for measuring the torque provided by the driver and then adding an appropriate amount of torque based on a lane assistance system torque request.

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

The boundaries of the item are as follows. The subsystems which are inside the item are: camera sensor, camera sensor ecu, car display, car display ecu, driver steering torque sensor, electronic power steering ecu, motor providing torque to steering wheel. The subsystem which is outside of the item is: steering wheel.

****

**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 of this project is to identify hazards in lane assistance system that could cause physical injury or damage to a person’s health, evalute the risk of hazardous situation so that we know how much we need to lower the risk via system engineering, prevent accidents from occurring by lowering risk to resonable levels. System engineering helps you figure out what your vehicle needs to do and what your vehicle design needs to look like on order to remain safe.

## 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 | 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 | Saafety 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**

**]**

In order to maintain a safety culture, some characteristics should be observed:

* 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?**

DIA serve several purposes:

1. Clarify the responsibilities of the different parties involved in a functional safety project

2. Describe the work products that each company will provide.

3. Help avoid disputes between companies.

4. Clarify who will be responsible for any safety issues in post-production.

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.**

**]**

|  |  |
| --- | --- |
| Role | resposibilities |
| Functional Safety Manager- Item Level | Pre audits, plan the development phase of lane assistance system |
| Functional Safety Engineer- Item Level | Develops prototypes, integrates sub systems into lane assistance system |
| Project Manager - Item Level | Allocates resources as needed |
| Functional Safety Manager- Component Level | Pre audits, plan the development phase of the component |
| Functional Safety Engineer- Component Level | Develops prototypes, integrates components |
| Functional Safety Auditor | Makes sure that the project conforms to the safety plan |
| Functional Safety Assessor | Judges whether the project has increased safety |

# 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?**

**]**

1. Confirmation measures serve two purposes:

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

2. 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.

3. Functional safety audit checks to make sure that the actual implementation of the project conforms to the safety plan.

4. Functional safety assessment confirms that plans, designs and developed products 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.