

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 |
| 29th April, 2018 | 1.0 | Microsoft word | Initial version of safety plan document |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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

A safety plan is a document that provides an overall framework for a functional safety project. Different parts of safety plan document include

1. Safety culture
2. Safety lifecycle
3. Safety management roles and responsibilities
4. Development interface agreements
5. Confirmation measures.

## 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

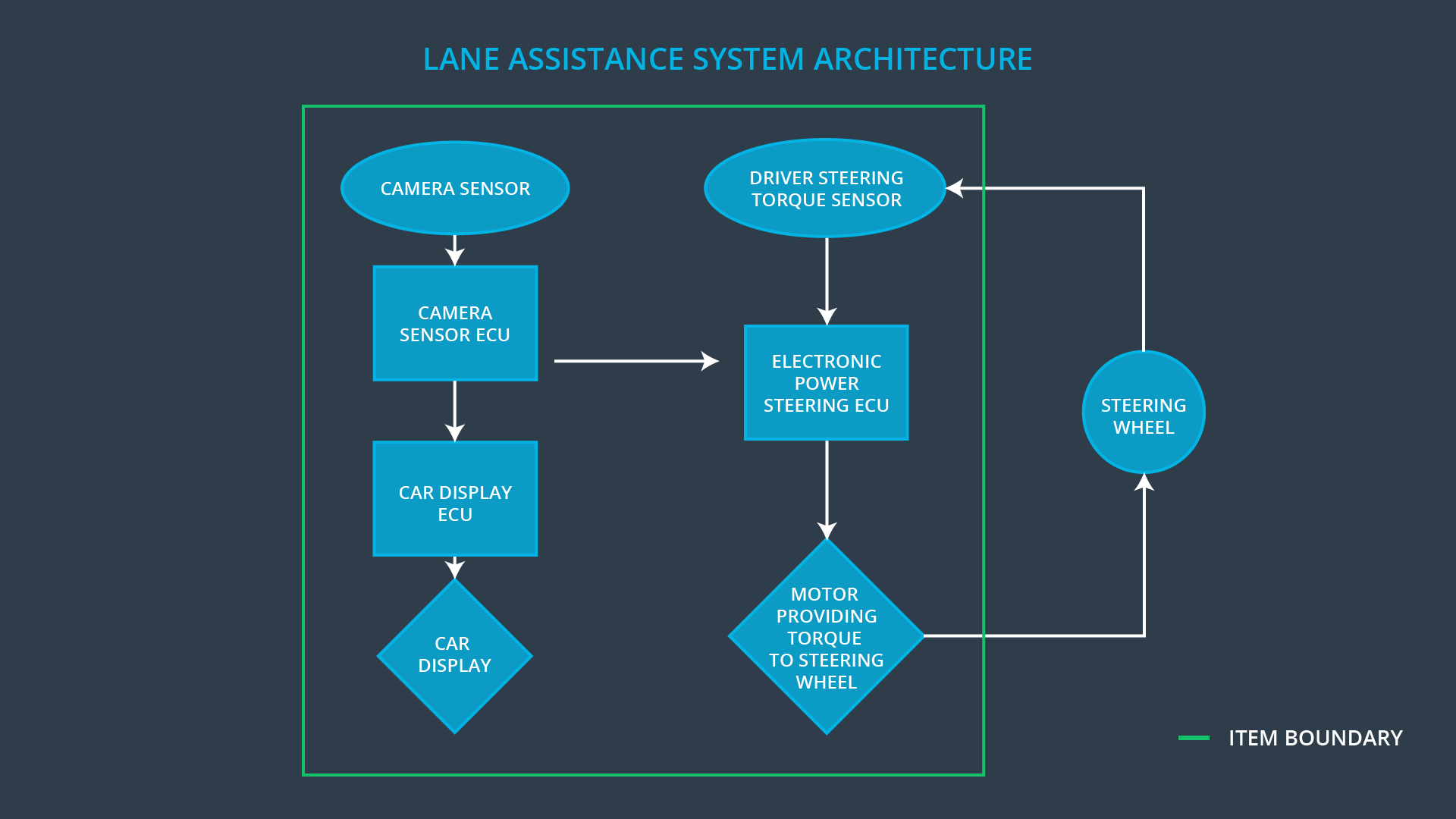
Hazard Analysis and Risk Assessment

Functional Safety Concept

Technical Safety Concept

Software Safety Requirements and Architecture

# Item Definition



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

ADAS advanced driver assistance system often called ADAS systems, are to help driver in the driving process.

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

ADAS systems has two functions:

1. Alert the driver to potentially dangerous situations.
2. Take the vehicle control to prevent from accidents.

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

1. Lane Departure Warning Function: Whenever a driver steers off the lane, the lane departure warning function will signal this to the driver by causing vibration of the steering wheel. Lane departures are detected by a camera subsystem will cause the power steering subsystem to generate a torque to vibrate the steering wheel.
2. Lane keeping assistance function- Whenever a driver is steering off the lane, the lane keeping assistance function will help the car get back on the lane by applying some amount of torque for a duration of time.

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

1. Lane Departure warning function - Camera subsystem, Power steering subsystem and Driver display subsystem
2. Lane keeping assistance function – Camera subsystem, Power steering subsystem, Display subsystem.

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

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

1. Camera system
2. Electronic power steering system
3. 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

To analyze the Lane departure warning function and lane keeping assistance function for possible defects and resulting hazards, come up with a plan to minimize the risk to acceptable levels.

## Measures

|  |  |  |
| --- | --- | --- |
| Measures and Activities | Responsibility | Timeline |
| Follow safety processes | Safety engineer | 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 manger | 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

Here are some characteristics of a good 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

The Lane Assistance Project is a modification to an existing automotive system and only requires the following phases:

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

|  |  |
| --- | --- |
| 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

**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.

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 and Tier 1 supplier take on a customer: supplier relationship. The OEM will provide requirements for what a vehicle system needs to do. Then the Tier 1 supplier develops and produces the system for the OEM. The OEM may provide a preliminary product design and then the tier 1 supplier will finish the details. In this case, the OEM will provide our company with the requirements for the lane keeping system and our company will develop and produce the system for the OEM and analyze and modify the various systems from a functional safety.

# Confirmation Measures

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

Confirmation measures serve two purposes.

* That a functional safety project conforms to ISO 26262, 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.