

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 |
| 06/21/19 | 1.0 | Adam Gotlib | First 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 Safety Plan provides groundwork and context for the entire safety case. It shows which vehicle system will be under consideration and defines roles, responsibilites, and processes required to implement appropriate functional safety measures.

## 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 **Lane Assistance (LA)** system whose purpose is to prevent a distracted driver from unintentionally leaving their current lane.

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

The two main functions of the LA system are **Lane Departure Warning (LDW)** function and **Lane Keeping Assistance (LKA)** function. Both of the functions activate when an unintentional lane departure is detected.

The LDW provides the driver with a haptic feedback in the form of oscillating torque applied to the steering wheel in order to direct the driver’s attention back on the road.

At the same time, LKA applies an additional torque to the steering wheel in order to move the vehicle closer to the center of the lane.

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

****

The above diagram provides an overview of the LA system architecture. Here, three subsystems can be distinguished:

* **Camera** subsystem, which detects lane departure using specialized computer vision techniques. Additionally, state of the turn signals is used to asses intentionality of the maneuver;
* **Electronic Power Steering (EPS)** subsystem, which measures the torque provided by the driver and then adds an appropriate amount of torque if an unintentional lane departure is detected;
* **Car Display** subsystem, which notifies the driver of functioning of the system.

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

The three aforementioned subsystem form entirety of the system. Note the actual steering wheel is not part of the system, but only the actuator that applies torque to 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 of this project is to identify and mitigate main hazards associated with possible malfunctioning of electronic and electric elements of the LA system. The item at hand has direct impact on the driving task, which is why safety is a critical part of the design. By working within framework of the widely recognized ISO 26262 standard, we can thus ensure high quality of functional safety management.

## 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 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**

**]**

The company’s safety culture can be desctibed by the following characteristics:

* **High priority**: safety takes precedence over other project constraints;
* **Accountability**: every decision can be traced back to people who made it; this way the blur of responsibilities related to safety can be avoided;
* **Rewards** and **Penalties**: a solid incentive system is formed to encourage achievement of functional safety;
* **Independence**: to reduce bias and make sure the development teams’ interests (which e.g. may involve finishing the project within prescribed timeframe) are not in conflict with fuctional safety;
* **Well defined processes:** to make it clear for everyone involved what steps are required to achieve functional safety; also to be able to verify how the processes have been conducted afterwards;
* **Diversity**: to reduce bias and include important insight from different experts at the company;
* **Communication**: to make sure no critical information relating to functional safety gets stuck on the way.

# 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 phases of the safety lifecycle are in scope of this particular project:

* Concept phase
* Product Development at the System Level
* Product Development at the Software Level

# 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 a development interface agreement is to delineate responsibilities in a customer–supplier relationship and ensure all parties are developing save 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.**

Responsibilities of my company:

* Planning, coordinatinfg, and documenting of the development phase of the safety lifecycle;
* Product development, integration and testing on software level;

Responsibilities of the OEM:

* Planning, coordinatinfg, and documenting of the development phase of the safety lifecycle;
* Ensuring that the design and production implementation conform to the safety plan and ISO 26262;
* Performance of functional safety assesment to judge whether functional safety is being achieved.

**]**

# Confirmation Measures

**[Instructions:**

**Please answer the following questions:**

1. **What is the main purpose of confirmation measures?**The purpose of the confirmation measures can be divided into three parts, which are:

* validating that processes comply with the ISO 26262 standard;
* validating that the project does improve overall safety;
* verifying that the project execution is following the safety plan.

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

Confirmation review involves an independend person reviewing work as the product is being designed and developed, to make sure ISO 26262 is being followed.

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

Verification that the actual implementation of the project is going according to the safety plan.

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

Validation that the project does achieve good level of 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.