

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 |
| 04/01/2018 | 1.0 | Oyama | First Attempt |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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?]**

We the purpose of the safety plan is to provide an overall framework for the Lane Assistance item, and to assign roles and responsibilities for functional safety for this item.

## 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?**

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

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

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

**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**

**]**

The lane assistance item alerts the driver that the vehicle has accidentally departed its lane and attempts to steer the vehicle back toward the center of the lane.

The Lane Assistance System will have two functions:

1. Lane departure warning
2. Lane Keeping Assistance

The lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback.

The lane keeping assistance function shall apply the steering torque when active to stay in ego lane.

The camera subsystem, the electronic power steering subsystem, and the car display system are each responsible for each of the functions.



1. Camera system is responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake.
2. Electronic Power Steering system is responsible for the torque provided by the driver and then adding an appropriate amount of torque based on a lane assistance system torque request.
3. Car Display system is responsible for the alert to the driver when the vehicle leaves the lane by mistake.

# 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 ISO 26262 functional safety standard covers electronic and electrical malfunctions in passenger vehicle systems. The standard provides a framework for reducing risks that could harm people's health. In ISO26262 functional safety, these are the four main steps involved in functional safety according to the standard:

(1) Requirements engineering Define what the system is going to do

(2) Designing or modifying a system architecture Design what the system will look like

(3) Test the system to make sure it behaves as expected

(4) Integrate the system into larger systems

By analyzing the lane assistance functions with ISO 26262, we can get the details for each step above, make a plan to reduce risks, and after this step, we can move forward to the right side of the V model, which involves implementing the plans and designs through software and hardware engineering. Implementations also need to be tested to make sure that they follow the design specifications from the left side of the V.

## 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**

**]**

**Good 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

**[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?**
2. **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.**

**]**

What Goes into a DIA (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.

The DIA 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.

Here are major sections of a DIA:

Appointment of customer and supplier safety managers

Joint tailoring of the safety lifecycle

Activities and processes to be performed by the customer; activities and processes to be performed by the supplier

Information and work products to be exchanged

Parties or persons responsible for each activity in design and production

Any supporting processes or tools to ensure compatibility between customer and supplier technologies

Quiz Roles and Responsibilities

Do you remember the different roles and responsibilities in functional safety? (Hint: go back to the previous lesson page if you have trouble remembering)

# 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?**

**]**

Confirmation Measures Purpose

Confirmation measures serve two purposes:

that a functional safety project conforms to ISO 26262, and

that the project really does make the vehicle safer.

The people who carry out confirmation measures need to be independent from the people who actually developed the project.

Confirmation Measures Definitions

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.

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.

Functional safety assessment

Confirming that plans, designs and developed products actually achieve functional safety is called a functional safety assessment.

You will not be required to write out a full confirmation measure section in the final project's safety plan; but you will need to show that you understand the purpose of the confirmation measures.

Levels of Independence

The person who developed a document, plan, design or product should not be the same person who carries out a confirmation measure; confirmation measures require independence.

ISO 26262 requires different levels of independence depending on what part of the functional safety lifecycle is under review.

For example, the department or company who develops a Hazard Analysis and Risk Assessment (HARA) needs to be completely separate from the department or company who makes sure the HARA was carried out according to ISO 26262. That’s because HARA is the critical first step in identifying high risk situations.

On the other hand, a person who develops a system that is rated low risk can be on the same team as the person who reviews the system for ISO 26262 compliance.

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.