

Safety Plan Lane Assistance

**Document Version:1.0 (2018-04-24)**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 2018/4/24 | 1.0 | Yifei Huang | Initial version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

[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

The purpose of this safety plan is to provide a guide line to make sure the advanced driver assistance system (ADAS) lane assistance feature functional safety.

## 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

The lane assistance system will provide 2 basic functions:

1. Lane keeping assistance function.
2. Lane departure warning function.

* Camera system
* Electronic Power Steering system
* Car Display system

you can see that the item boundary was drawn to include three sub-systems:

* Camera system
* Electronic Power Steering system
* Car Display system

Your job in functional safety is to further refine the system to take into account potential malfunctions. To ensure functional safety, you might end up adding additional subsystems or elements to the original system architecture provided to you.

In general, the **item definition** will mention which systems are part of the **item** as well as any other information known about the item such as:

* *Functional concept* of the product, which describes what the item is supposed to do; recall that functional safety engineering involves analyzing what happens when the system malfunctions, and the item does not do what it is supposed to do. So it is important to understand the product's purpose.
* *Operational and Environmental Constraints*
* *Legal Requirements*
* *National and International Standards Related to the Item*
* *Records of previously known safety-related incidents or behavioral short-falls*

These features requires

1. Camera sensor and camera sensor ECU, which will detect if the vehicle is off the lane center.
2. Car display and car display ECU, which will exhibit the information on the display
3. Electronic power steering ECU, which will provide torque to steering wheel.

(the steering wheel is more in the mechanical part, it’s functionality not in this safety plan discussion)

1. S driver steering torque sensor will provide feedback to the electronic power steering ECU.



**[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?**

The Lane Assistance System will have two functions:

1. Lane departure warning
2. Lane keeping assistance

When the driver drifts towards the edge of the lane, two things will happen:

* the **lane departure warning function** will vibrate the steering wheel
* the **lane keeping assistance function** will move the steering wheel so that the wheels turn towards the center of the lane

To state the **lane departure warning** engineering requirement more formally: "the lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback." In other words, the vehicle quickly moves the steering wheel back and forth to create a vibration. You can assume that the engineering requirement came from a product engineering team, and your job will be to add extra requirements to ensure functional safety.

The **lane keeping assistance functionality** will automatically **assist** the driver; the steering wheel turns towards the center of the lane. We will formally list the requirement as "the lane keeping assistance function shall apply the steering torque when active in order to stay in ego lane". Ego lane refers to the lane in which the vehicle currently drives.

**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**

**]**

# Goals and Measures

## Goals

### lane Keeping Assistance Safety Goals

What about the lane keeping assistance function? In this case, the hazardous situation involved the driver taking both hands off the wheel. Because the functionality was always on, the driver could misuse the lane keeping assistant as if it were meant for autonomous driving. What would the safety goal be for this second case?

Lane keeping goal:

The lane keeping assistance function shall be time limited and the additional steering torque shall end after a given time interval so that the driver cannot misuse the system for autonomous driving.

Lane departure warning function goal:

The oscillating steering torque from the lane departure warning function shall be limited.

**S3 x E3 x C3 = ASIL C**

**[Instructions:**

**Describe the major goal of this project; what are we trying to accomplish by analyzing the lane assistance functions with ISO 26262?]**

## 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 accessor** | 3 months prior to main assessment |
| Perform functional safety assessment | **Safety accessor** | Conclusion of functional safety activities |

# Safety Culture

S Company always put the functional safety at the highest priority on the products and projects.

Functional safety is the first consideration.

S company provide weekly functional safety meeting and share the best practice among different teams.

S company set Best Safety Team/ Member awards quarterly and rewards the member /team did best in the field.

S company provide SOP (standard [Standard operating procedure](https://en.wikipedia.org/wiki/Standard_operating_procedure)) guide line for each person on their major work.

Communication between different team on the functional safety are highly encouraged.

**Functional**

**[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**

**]**

# Safety Lifecycle Tailoring

The life cycle includes:

1. Concept phase
2. Product Development at the System Level
3. Product Development at the Software Level

**[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**

**]**

# 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

afety As

**[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.**

**]**

# 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?**

**]**

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.