

Safety Plan Lane Assistance

**Document Version: 1.0**

**Template Version 1.0, Released on 2017-06-21**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 08.01.2018 | 1.0 | Liang Zhang | First attempt |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

[Document history](#_Toc521357624)

[Table of Contents](#_Toc521357625)

[Introduction](#_Toc521357626)

[Purpose of the Safety Plan](#_Toc521357627)

[Scope of the Project](#_Toc521357628)

[Deliverables of the Project](#_Toc521357629)

[Item Definition](#_Toc521357630)

[Goals and Measures](#_Toc521357631)

[Goals](#_Toc521357632)

[Measures](#_Toc521357633)

[Safety Culture](#_Toc521357634)

[Safety Lifecycle Tailoring](#_Toc521357635)

[Roles](#_Toc521357636)

[Development Interface Agreement](#_Toc521357637)

[Confirmation Measures](#_Toc521357638)

# Introduction

## Purpose of the Safety Plan

The safety plan provides an overall framework for the **lane assistance** item, for example, the scope of the project and the lane assistance item. It also assigns roles and responsibilities for this project.

## 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 item we consider in this plan is a Lane Assistance System, which alerts the driver when the vehicle has accidently departed the lane and attempt to steer the vehicle back to the center of the lane.

The Lane Assistance System will have two functions:

* Lane departure warning: When the driver drifts towards the edge of the lane, this function will vibrate the steering wheel
* Lane keeping assistance: When the driver drifts towards the edge of the lane, this function will move the steering wheel so that the wheels turn towards the center of the lane

The item boundary is defined in the following system architecture diagram.



From the diagram below, it shows that the item includes three sub-systems:

* **Camera system**

This sub-system is composed of two components

* + camera sensor
  + camera sensor ECU
* **Electronic Power Steering system**

This sub-system is composed of two components

* + driver steering torque sensor
  + electronic power steering ECU
  + motor providing torque to steering wheel
* **Car Display system**

This sub-system is composed of two components

* car display
* car display ECU

To summarize the functionality, the **camera system** detects lane departures and tells the steering wheel how hard to turn. The driver receives a warning on the **vehicle display** and also receives a warning via a **steering wheel vibrating**. Simultaneously, the wheel adds extra **steering torque** to help the driver move back towards the center of the lane.



Note that **steering wheel** is out of the item.

# Goals and Measures

## Goals

The goal of this project:

* Identify hazard situations in the lane assistance item.
* Evaluate risk of each hazard situation.
* Derive requirements to lower the risks to the acceptable level by the society.

## Measures

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

The following characteristics of safety culture should be followed during the Lane Assistance project:

* **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

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 |
| Functional Safety Assessor | OEM |

# Development Interface Agreement

A DIA (development interface agreement) defines the *roles* and *responsibilities* between companies involved in the Lane Assistance project. The DIA also specifies *evidence* and *work products* each party will provide to prove that work was done according to the agreement. The ultimate goal of DIA is to ensure that all parties are developing safe vehicles in compliance with ISO 26262.

*For OEM*

* **Functional​ ​Safety​ ​Manager**​: pre-audits, plans the development phase for the Lane Assistance item.
* **Functional​ ​Safety​ ​Engineer**​​: develop prototypes, integrate subsystems combining them into the Lane Assistance item from a functional safety viewpoint.
* **Project​ ​Manager**​: allocates the resources needed for the item.
* **Functional​ ​Safety​ ​Auditor**​: make sure the project conforms to the safety plan.
* **Functional​ ​Safety​ ​Assessor**​: judges where the project has increased safety.

*For Tier One*

* **Functional​ ​Safety​ ​Manager​ ​(Liang Zhang)**:​ pre-audits, plan the development for the components of the Lane Assistance item.
* **Functional​ ​Safety​ ​Engineer​ ​(Liang Zhang)**:​ develop prototypes and integrate components conforming the Lane Assistance item.

# 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.

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

*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* is to make sure that the actual implementation of the project conforms to the safety plan is called a functional safety audit.

*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.