

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 |
| 11.05.2018 | 1.0 | Sundeep Pundamale Selvaraj | First Draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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 the safety plan is to provide an overall framework for functional safety of the Lane Assistance Item and in addition describe the roles and responsibilities within the framework.

## **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 in question is the Lane Assistance System. The Lane Assistance System alerts the driver when the vehicle is moving out of the lane accidently and in addition it attempts to steer the vehicle back safely to the centre of the lane.

The Lane Assistance System has two functions:

1. Lane departure warning
2. Lane keeping assistance

The lane departure warning function applies an oscillating steering torque to provide the driver a haptic feedback and the lane keeping assistance function applies the steering torque when active in order to keep the car in the ego lane.

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



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 centre of the lane.

# **Goals and Measures**

## **Goals**

The major goal of this project is to design a Lane Assistance System which is functionally safe. Functional safety includes:

* Identifying hazards in a passenger vehicle’s electronic or electric system that could cause physical injury or damage to a person's health
* Evaluate the risk of the hazardous situation so that we know how much we need to lower the risk
* With the help of System Engineering, prevent accidents from occurring by lowering risk to reasonable levels

## **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**

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**

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**

The purpose of a development interface agreement is to define 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.

The major sections of DIA are:

* 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

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

# 

# **Confirmation Measures**

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

Confirmation measures serves two purposes:

* Functional safety of the project conforms to ISO 26262
* The project really does make the vehicle safer

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

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?**

A functional safety audit ensures the actual implementation of the project conforms to the safety plan is called a functional safety audit.

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

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.