

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 |
| 23-May-2018 | 1.0 | Sharath Srinivasan | First Version with all the specific details |
| 25-May-18 | 1.1 | Sharath Srinivasan | Final 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 functional safety plan is to provide a framework for the safety aspects of the Lane Assistance system.
* The safety plan assigns functional safety roles and responsibilities for individual subsystem.
* Implementing a Safety plan involves using system engineering to lower the risk to a responsible level.
* This also helps in measuring risks and identifying Hazards.
* A safety plan helps us identify a new system level safety requirement that lets us allocate these requirements to higher level in order to pertain from potential failures in various electrical and electronic systems, framed by ISO 26262.

## 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

**Block Diagram:**



**The following question will be addressed in this section.**

* 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?

The Lane Assistance system attempts to determine when a driver had departed a lane unintentionally. The system monitors the vehicle’s position within a lane and also takes driver intention into account, especially the use of turn signals. The system attempts to alert the driver to steer the vehicle back into the original “ego” lane.

The Lane Assistance system has two primary roles:

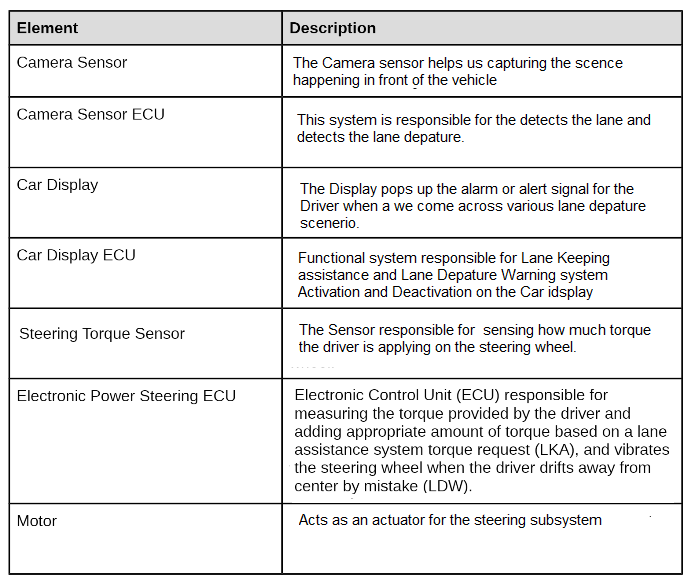
* **Lane Departure Warning**: This Provides an alerting signal to alarm the driver when a lane is departed unintentionally. In this case, the warning includes a display and a haptic signal provided by applying oscillating torque to the steering wheel.
* **Lane Keeping Assistance**: This Provides torque to the steering system, attempting to help the vehicle remain in the ego lane.

There are three subsystems involved in the Lane Assistance system, play a role in both the lane departure warning and lane keeping assistance roles.

.

* The Camera subsystem.
* The Electronic power steering subsystem.
* The Car display system.

|  |  |
| --- | --- |
| ID | Goal |
| Safety\_Goal\_01 | The Oscillating toque generation on the Lane Keeping Assistance system should alert the driver in a subtle . |
| Safety\_Goal\_02 | Lane Keeping will be time constrained and limited in order to avoid the misuse of the autonomous driving system. |
| Safety\_Goal\_03 | The Camera ECU should always check for the Lane |
| Safety\_Goal\_04 | Deactivate the Lane Keeping Assistance . |



# Goals and Measures

## Goals

* Vehicles are complex systems with both sociological and technical requirements.
* Safety includes not only analysis of individual software and hardware components, but also the interaction between systems and subsystems, as well as the safety culture of an organization.
* The Functional Safety Plan outlines roles and responsibilities of individual team members, as well as the overarching safety culture of the organization and the product safety lifecycle. ISO 26262 is the standard That has to be followed.
* Identify High risks and reduce the risk into reasonable levels by implementing system engineering.

## Measures

|  |  |  |
| --- | --- | --- |
| 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 Assessor | Conclusion of functional safety activities |

# 

# Safety Culture

* **Priority**
  + Safety has the highest priority, greater than other considerations like productivity and cost. The processes assure accountability such that decisions are traceable back to the people and teams who made the decisions.
* **Accountability**
  + The processes assure accountability such that decisions are traceable back to the people and teams who made the decisions.
* **Rewards and Penalties**
  + This organization rewards the achievement and motivation of functional safety.
  + While penalizing shortcuts and decisions that jeopardize quality and safety.

Teams which designs and develops products are independent of those who audit the work. All stakeholders adhere to a well-defined process.

This organization puts an emphasis on communication between team members and teams, encouraging early disclosure of potential problems. All projects and teams are allocated the necessary resources, including individuals with the appropriate skills, to successfully do their work. Intellectualdiversity is sought, valued, and integrated into processes.

# Safety Lifecycle Tailoring

The following safety lifecycle phases are in scope for this project:

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 Development Interface Agreement (DIA) defines the roles and responsibilities between companies developing a product. The essential aim of the DIA is the ensure that all teams contribute to the development of safe vehicles in accordance with ISO 26262. This is done by specifying evidence and work products provided by each vendor to prove work was completed according to the agreement.

The main reasons behind this:

* Liability
* Avoids Disputes

**Tier 1 vendor**

* Appointing these positions:
  + Functional Safety Manager
  + Functional Safety Engineer
* Joint tailoring of the safety lifecycle of the Lane Assistance subsystems
* Analysis of the Lane Assistance subsystems from a functional safety viewpoint
* Modification of the Lane Assistance subsystems from a functional safety viewpoint
* Providing tools and/or processes to ensure compatibility with OEM technologies
* Documentation of all above activities
* Completion and exchange of the following work products:
  + Hazard Analysis and Risk Assessment
  + Functional Safety Concept
  + Technical Safety Concept
  + Software Requirements and Architecture
  + Fully developed and tested subsystems

**OEM**

* Appointing these positions:
  + Item Level Functional Safety Manager
  + Item Level Functional Safety Engineer
  + Item Level Project Manager
  + Functional Safety Auditor
  + Functional Safety Assessor
* Joint tailoring of the safety lifecycle of the Lane Assistance system.
* Analysis of the Lane Assistance system as a whole from a functional safety viewpoint.
* Modification of the Lane Assistance system as a whole from a functional safety viewpoint.
* Providing tools and/or processes to ensure compatibility with Tier 1 vendor technologies.

# Confirmation Measures

* Confirmation measures ensure that:
* The project and processes are within the **ISO 26262.**
* The project really does improve safety and minimize to zero risk and failure.
* The executing confirmation measures must be independent from those who developed the project.
* A functional safety audit ensures the actual implementation of the project conforms to the safety plan.
* A functional safety assessment 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.