

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 |
| 7/16/2018 | 1.0 | Deepak Zambre | Initial Draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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

Herein we outline plan / processes to minimize risk via system engineering that may arise due to probable hazards in Advanced Lane Assistance System.

## 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

Advanced Lane Assist is composed to two primary functions:

* Lane Departure Warning  
  If a driver drives beyond current lane without turn indicator ‘on’ then he / she is alarmed / warned via steering wheel vibration.
* Lane Keeping Assist  
  When Lane Departure Warning is issued, this system will try to steer vehicle back to center of current lane.

Following diagram outlines the sub-systems that are part of Advanced Lane Assist System:

A close up of a sign

Description generated with high confidence

Camera Sensor ECU uses images captured using camera sensor to detect lanes and determine if vehicle is drifting over a lane line. If the car drifts over a lane edge without a turn indicator ‘on’, it sends a message to Electronic Power Steering ECU and Car Display ECU. Car Display ECU displays a visual warning to driver about ‘Lane drift’ and engagement of ‘Lane Assist’. Electronic Power Steering ECU provides a mechanical feedback to driver about lane drift by steering vibration. It also applies required torque to steering wheel to move vehicle back to center of current lane. Lane Assist warning and steering torque is disabled once the vehicle is within the lane boundaries. During this process if the driver applies more torque to drift away from current lane then ‘Lane Assist’ is disabled. Lane Assist is not enabled if lane detection is not possible due to inclement weather, bad road conditions, etc.

# Goals and Measures

## Goals

* Identify hazards that may arise in Lane Assist System
* Evaluate the risk attached to each hazard by analyzing its failure nature and probability
* Minimize the risk of failures to acceptable limits of current 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

Here are some characteristics of a good safety culture that will be observed in the company:

* 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

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 goal is to ensure that all parties are developing safe vehicles in compliance with ISO 26262.

OEM is responsible for:

* Ensuring vehicle is safe after integration of various systems (including Lane Assist System) and following functional safety plan for such

Tier-1 supplier is responsible for:

* Lane Assist System development and following functional safety plan for such
* Any bugs / issues for Lane Assist System

# 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.

**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.

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.