

Safety Plan Lane Assistance

**Document Version: [1]**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 25-10-2018 | 1.0 | Archit Rastogi | Safety Plan for Lane Assistance Systems |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

[Document history](#t3h5sf1)

[Table of Contents](#ktt3lgighckp1)

[Introduction](#zakt536q9xt3)

[Purpose of the Safety Plan](#ybytyytfvs)

[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 safety plan provides an overall framework for the lane assistance system safety.

Safety plan discusses about the following:

* Item Definition
* Goals and Measures
* Safety Culture
* Safety Lifecycle Tailoring
* Safety Management Roles and Responsibilities
* Development Interface Agreements
* Confirmation Measures

## 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 system is a simplified version of a Lane Assistance System. The Lane Assistance System has 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.

The **lane keeping assistance functionality** will automatically **assist** the driver; the steering wheel turns towards the center of the lane.

The item functionalities are implemented by the following subsystem:

* **Camera subsystem**: This subsystem is composed by two components:
  + Camera sensor
  + Camera sensor ECU (Electronic Control Unit)
* **Electronic Power Steering subsystem**: This subsystem is composed by three components:
  + Driver Steering Torque Sensor.
  + Electronic Power Steering ECU.
  + Motor Proving Torque to Steering Wheel.
* **Car Display subsystem**: This subsystem is composed by two components:
  + Car Display ECU
  + Car Display

When the camera senses that the vehicle is leaving the lane, the camera sends a signal to the electronic power steering system asking to turn and vibrate the steering wheel.

The camera sensor will also request that a warning light turn on in the car display dashboard. That way the driver knows that the lane assistance system is active.

What if the driver wants to leave the lane? If the driver uses a turn signal, then the lane assistance system deactivates so that the vehicle can leave the lane. The driver can also turn off the system completely with a button on the dashboard.

The driver is still expected to have both hands on the steering wheel at all times. The electronic power steering subsystem has a sensor to detect how much the driver is already turning. The lane keeping assistance function will merely add the extra torque required to get the car back towards center. The extra torque is applied directly to the steering wheel via a motor.

****

# Goals and Measures

## Goals

1. **Identify hazards** in Lane assistance system that could cause physical injury or damage to a person's health
2. **Evaluate the risk** of the hazardous situation so that we know how much we need to lower the risk
3. Via **systems engineering**, prevent accidents from occurring by lowering risk to reasonable levels.

## Measures

|  |  |  |
| --- | --- | --- |
| Measures and Activities | Responsibility | Timeline |
| Follow safety processes | All members | Constantly |
| Create and sustain a safety culture | All Members | Constantly |
| Coordinate and document the planned safety activities | All 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 Assesor | Conclusion of functional safety activities |

# 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

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 OEM is supplying a functioning lane assistance system and is responsible for over vehicle functional safety. Tier-1 supplier needs to analyze and modify the various sub-systems from a functional safety viewpoint. All functional safety information will be shared through appointed Functional safety managers

# 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