

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 |
| 3/13/2018 | 1 | Scott Schnelle | First draft of Safety Plan |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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 define a framework for safely implementing a Lane Assistance system on a vehicle. It includes the scope of the project, creates deliverables, defines what each item should do, develops goals and measures, and defines roles and responsibility for the systems functional safety.

## 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 for this safety plan is a Lane Assistance System. The two main functions of this system are:

* **Lane Departure Warning:** When the vehicle drifts out of the desired lane, the vehicle provides haptic feedback by vibrating the steering wheel to alert the driver.
* **Lane Keeping Assistance:** When the vehicle begins to drift out of the desired lane, the vehicle provides a control input, either braking inside wheels or providing steering torque, to keep the vehicle in its desired lane.

The system uses the following subsystems and components to implement these functions:

* Cameras
  + Camera Sensor
  + Camera ECU
* Electronic Power Steering (EPS)
  + Driver Steering Torque Sensor
  + EPS ECU
  + Motor to provide corrective torque
* Car Display
  + Car Display
  + Car Display ECU

The following diagram shows how the subsystems are connected:



The camera senses the vehicles position within the lane and if it is departing its desired lane. If it is, it sends a signal to the electronic power steering unit to vibrate the wheel and provide corrective torque. The camera ECU also sends a signal to the car display to visually alert the driver with a warning light. The system should be able to differentiate between if the vehicle is drifting out of its lane or if the driver is attempting a lane change, with or without the turn signal on. The system can be turned on/off by a button on the steering wheel.

The driver is expected to have both hands on the steering wheel at all times. The EPS system should be able to detect the driver’s presence via torque input.

The Lane Assistance system does not include the following:

* Adaptive Cruise Control
* Blind Spot Monitoring
* Traffic Jam Assist

# Goals and Measures

## Goals

The goals of this project are:

* Identify potential risk and hazardous situation that could arise with any malfunction in the Lane Assistance system
* Evaluate these risk
* Reduce these risk to acceptable 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

To implement a culture of safety, the following characteristics needs to be observed:

* 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

This section defines the roles and responsibilities between parties involved in the Lane Assistance project to ensure its development in compliance with ISO 26262.

* **Functional Safety Manager - Item Level**: Pre-audits, plans the development phase for the Lane Assistance item.
* **Functional Safety Engineer - Item Level**: Develop prototypes, integrate subsystems combining them into the Lane Assistance item from a functional safety viewpoint.
* **Project Manager - Item Level**: Allocates the resources needed for the item.
* **Functional Safety Manager - Component Level (Scott Schnelle)**: Pre-audits, plan the development for the components of the Lane Assistance item.
* **Functional Safety Engineer - Component Level (Scott Schnelle)**: Develop prototypes and integrate components conforming the Lane Assistance item.
* **Functional Safety Auditor**: Make sure the project conforms to the safety plan.
* **Functional Safety Assessor**: Judges where the project has increased safety.

# Confirmation Measures

The purposes of the confirmation measures are to:

* Ensure the Lane Assistance project conforms to ISO 26262.
* Ensure the Lane Assistance project really does make the vehicle safer.

The Confirmation review ensure the projects comply 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. A Functional safety audit make sure the actual implementation of the project conforms to the safety plan. A Functional safety assessment confirms that the plan, design and developed product achieve functional safety.