

Safety Plan Lane Assistance

**Document Version: 1.0**

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



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 3/1/18 | 0.1 | Ken Overholt | Initial draft |
| 3/3/18 | 0.2 | Ken Overholt | Candidate for final release |
| 3/8/18 | 1.0 | Ken Overholt | Final Release |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

Table of Contents

[Document history 2](#_Toc508301353)

[Table of Contents 2](#_Toc508301354)

[Introduction 3](#_Toc508301355)

[Purpose of the Safety Plan 3](#_Toc508301356)

[Scope of the Project 3](#_Toc508301357)

[Deliverables of the Project 3](#_Toc508301358)

[Item Definition 3](#_Toc508301359)

[Goals and Measures 5](#_Toc508301360)

[Goals 5](#_Toc508301361)

[Measures 5](#_Toc508301362)

[Safety Culture 6](#_Toc508301363)

[Safety Lifecycle Tailoring 6](#_Toc508301364)

[Roles 6](#_Toc508301365)

[Development Interface Agreement 7](#_Toc508301366)

[Confirmation Measures 7](#_Toc508301367)

# Introduction

## Purpose of the Safety Plan

The purpose is to provide an overall framework for the Lane Assistance item and to assign roles and responsibilities for functional safety for this item.

## 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 lane assistance item alerts the driver that the vehicle has accidentally departed its lane and attempts to steer the vehicle back towards the center of the lane. It has two main functions:

1. Lane departure warning
2. Lane keeping assistance

The lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback.

The lane keeping assistance function shall apply the steering torque, when active, in order to stay in the ego lane.

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

**A close up of a sign

Description generated with high confidence**

# Goals and Measures

## Goals

The goal of the project is to reduce risk for the lane-keeping assistance feature 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 | 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 Assessor | 3 months prior to main assessment |
| Perform functional safety assessment | Safety Assessor | Conclusion of functional safety activities |

# Safety Culture

Safety has the highest priority among competing constraints like cost and productivity. Processes ensure accountability such that design decisions are traceable back to the people and teams who made the decisions. The organization motivates and supports the achievement of functional safety through rewards. The organization penalizes shortcuts that jeopardize safety or quality. The teams who design and develop a product are independent from the teams who audit the work. The company design and management processes are clearly defined. Projects have the necessary resources including people with appropriate skills. Intellectual diversity is sought after, valued, and integrated into processes. Communication channels encourage disclosure of problems.

# Safety Lifecycle Tailoring

For the lane assistance project, the following safety lifecycle phases are in scope:

1. The Concept phase which includes the item definition, initiation of the safety lifecycle, hazard analysis and risk assessment, and the functional safety concept.

1. Product Development at the System Level
2. Product Development at the Software Level

The following phases are out of scope:

1. Product Development at the Hardware Level
2. 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

1. The purpose of the Development Interface Agreement is to delineate the design and production responsibilities between the OEM and Tier 1 supplier.
2. The OEM is supplying a functioning lane assistance system. The Tier 1 company needs to analyze and modify the various sub-systems from a functional safety viewpoint.

# Confirmation Measures

Confirmation measures serve two purposes:

1. Confirm that a functional safety project conforms to ISO 26262
2. Confirm that the project really does make the vehicle safer

The confirmation review ensures that the project complies with ISO 26262. As the product is designed and developed, an independent person will review the work to make sure ISO 26262 is being followed.

The functional safety audit checks to make sure that the actual implementation of the project conforms to the safety plan.

The functional safety assessment confirms that plans, designs, and developed products achieve functional safety.