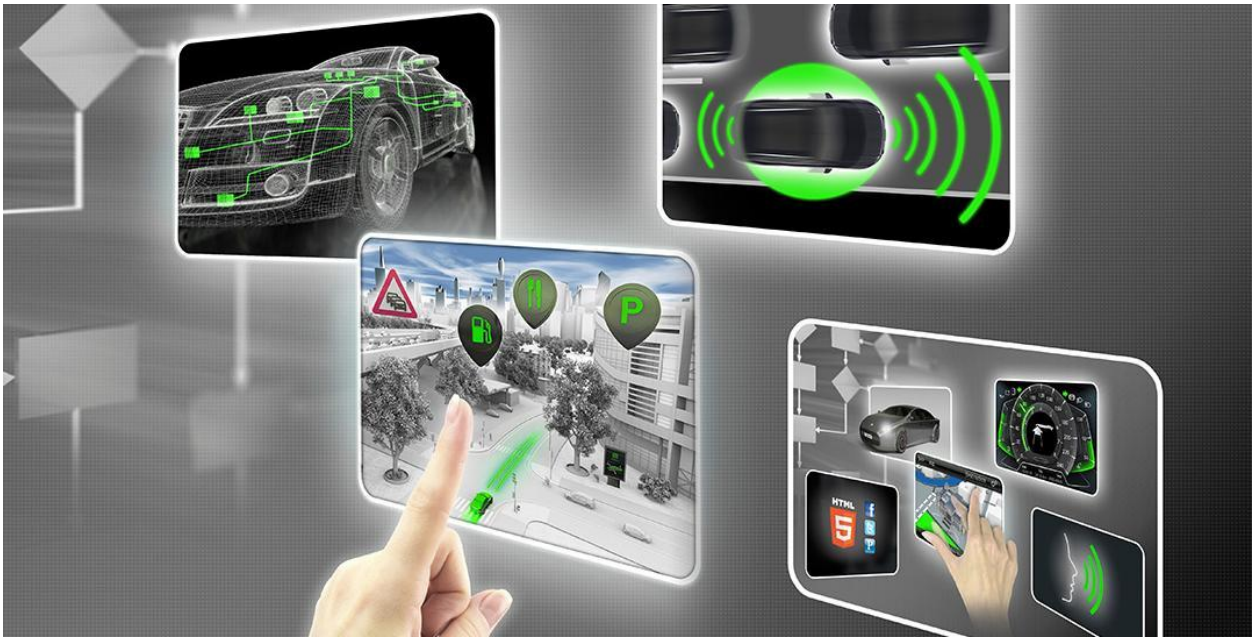


# Safety Plan Lane Assistance

**Document Version: 1.0**

# Document history

| Date | Version | Editor | Description |
|---|---|---|---|
| 13.08.2018 | 1.0 | Reuss | First version |
| | | | |
| | | | |
| | | | |
| | | | |

# Table of Contents


Document history

Table of Contents

Introduction
- Purpose of the Safety Plan
- Scope of the Project
- Deliverables of the Project

Item Definition

Goals and Measures
- Goals
- Measures

Safety Culture

Safety Lifecycle Tailoring

Roles

Development Interface Agreement

Confirmation Measures

# Introduction

## Purpose of the Safety Plan

The safety plan provides an overall framework for this functional safety relevant project with the following parts included:

- Define the scope of the project and deliverables of the project
- Give a clear item definition
- Define goals and measures
- Describe the safety culture
- Tailor the safety lifecycle of the project
- Define Roles & Responsibilites
- Specify the DIA

## 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

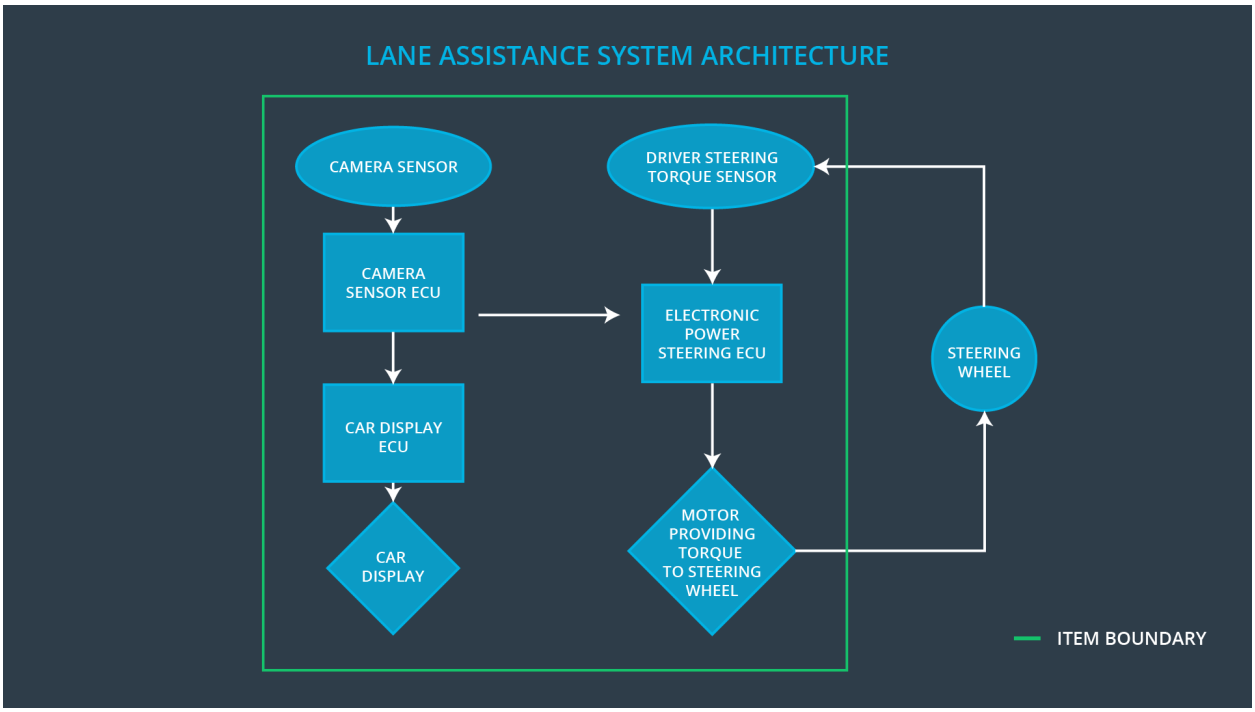
# Item Definition

This item in this project is a lane keeping assistance system. It assists the driver in not leaving the driving lane unintended.

The lane assistance system has two functions:

1. Lane departure warning
2. Lane keepings assistance

When the driver drifts towards the edge of the lane, the lane departure warning function will vibrate the steering wheel and the lane keeping assistance function will move the steering wheel, so that the car goes back to the center of the lane.




There are three subsystems inside the item:

- Camera subsystem, consisting out of camera ECU and camera sensor
- Electronic Power Steering subsystem, consisting out of steering ECU, steering torque sensor and steering motor
- Car Display subsystem, consisting out of car display ECU and car display.

The boundary of the item is between steering wheel and steering motor respectively between torque sensor and steering wheel. The steering wheel is outside of the item.

The camera subsystem is responsible for detecting lane lines and unintended lane departures.
The car display subsystem is responsible for warning the driver via a flashing symbol on the vehicle display
The electronic power steering subsystem is responsible for measuring the torque provided by the driver and adding additional torque to help drive the car back to the center of the lane, based on the measurements of the camera subsystem.

# Goals and Measures

## Goals

The major goal of this project is to reduce risks and avoid injury and harm to peoples.

## 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 Manager | Once every 2 months |
| Perform functional safety pre-assessment prior to audit by external functional safety assessor | Safety Auditor | 3 months prior to main assessment |
| Perform functional safety assessment | Safety Assessor | Conclusion of functional safety activities |

# Safety Culture

These are the characteristics of our 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

The purpose of a development interface agreement is ensure that all parties develop a safe vehicle according to ISO 26262.

It helps to avoid disputes, defines liability and clarifies who will be responsible for any safety issues in post-production. It defines as well what evidence and work products will be provided to prove that work was done according to the agreement.

The responsibility of the OEM is integration of the lane assistance system into the vehicle.
The responsibility of this project is: Developing, testing and verifying the systems including all subsystems in regards to the provided requirements by OEM.

# 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.

A confirmation review is a review, done by a project independent person, to ensure that the work products comply with the ISO 26262 standard.

A functional safety audit is checking to make sure that the actual implementation of the project conforms to the safety plan.

A functional safety assessment confirms 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.