

Safety Plan Lane Assistance

**Document Version: 1.0**

**2019-03-12**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 2019-03-12 | 1.0 | Sergey Morozov | Completed all document sections |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# Table of Contents

[**Document history**](#_3dy6vkm) **2**

[**Table of Contents**](#_ih3zmjgtg18m) **3**

[**Introduction**](#_2s8eyo1) **4**

[Purpose of the Safety Plan](#_17dp8vu) 4

[Scope of the Project](#_3rdcrjn) 4

[Deliverables of the Project](#_26in1rg) 4

[**Item Definition**](#_6ld7ca20i6la) **5**

[**Goals and Measures**](#_35nkun2) **7**

[Goals](#_1ksv4uv) 7

[Measures](#_44sinio) 7

[**Safety Culture**](#_d8qmunglpit0) **8**

[**Safety Lifecycle Tailoring**](#_z337ya) **9**

[**Roles**](#_oyhnivu0agpn) **10**

[**Development Interface Agreement**](#_imgk4udqs29n) **11**

[**Confirmation Measures**](#_j50cwdcgpnbe) **12**

# Introduction

## Purpose of the Safety Plan

The safety plan gives an overview of how to achieve a safe system. It specifies what system is under consideration, the goal of the project, what steps will be taken to ensure safety, the roles and personnel involved in the project, and the project timeline.

## 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 in question is a Lane Assistance System which is a kind of an Advanced Driver Assistance Systems (ADAS). The main functions of an ADAS are to (1) alert the driver to potentially dangerous situations and (2) take control over the vehicle to prevent accidents from occurring. In case of a lane assistance system, the (1) and (2) functions can be restated as

1. Lane Departure Warning function and
2. Lane Keeping Assistance function.

The Lane Departure Warning function shall apply an oscillating steering torque to provide haptic feedback for the driver.

The Lane Keeping Assistance function shall apply the steering torque when active in order to stay in ego lane. (Ego lane refers to the lane in which the vehicle currently drives.)

The Lane Assistance System contains three sub-systems:

* Camera sub-system,
* Electronic Power Steering sub-system, and
* Car Display sub-system.

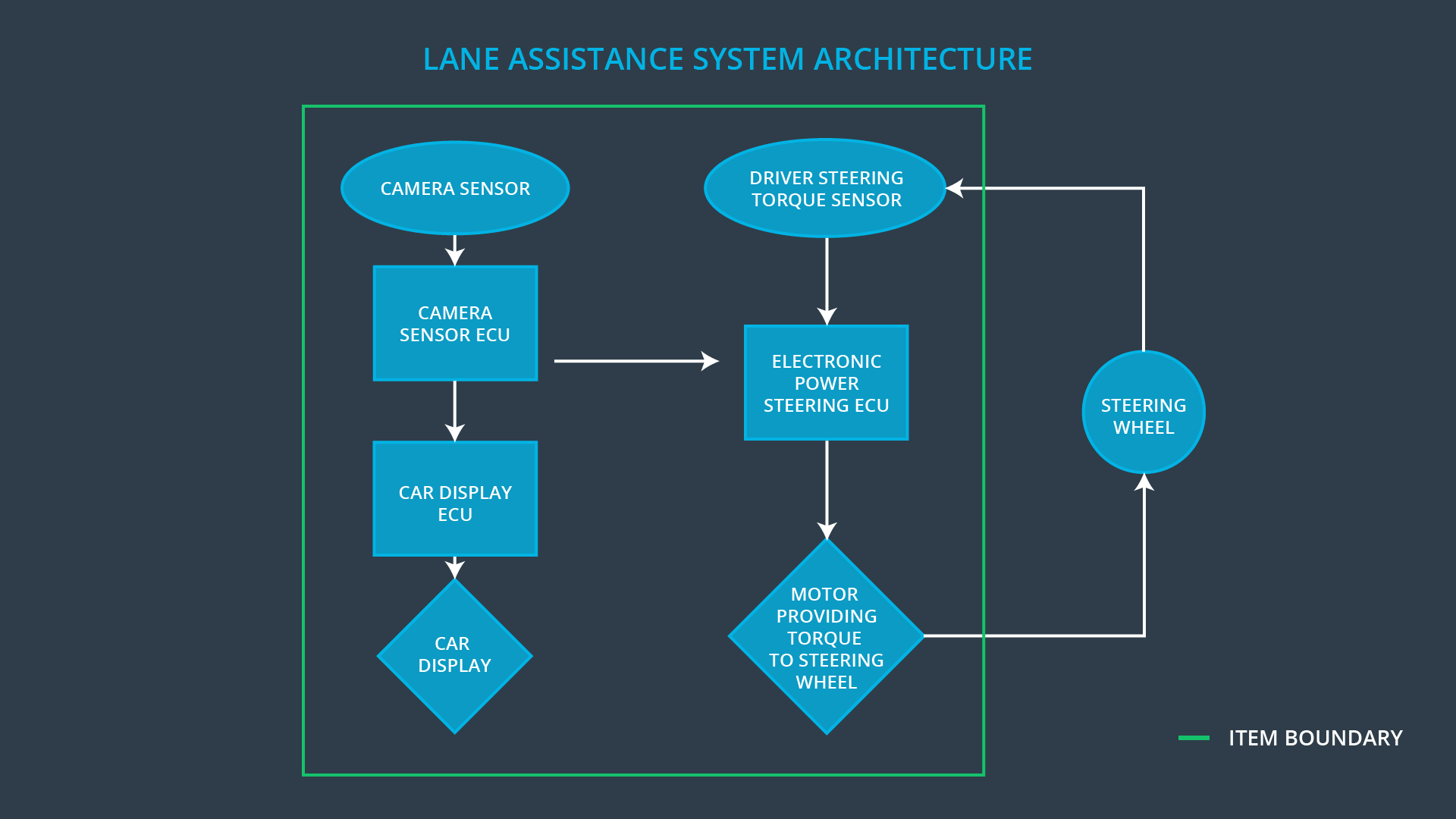
Camera sub-system is responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake.

Electronic Power Steering sub-system is responsible for measuring the torque provided by the driver and then adding an appropriate amount of torque based on a lane assistance system torque request.

Car Display sub-system is responsible for providing visual notifications to the driver.

The Camera and Electronic Power Steering sub-systems are involved in providing the Lane Keeping Assistance function while the Camera and Car Display sub-systems are involved in providing the Lane Departure Warning function.

The Item (Lane Assistance System), its sub-systems, and their components are represented on the following diagram.



The Car Display sub-system is composed of the following components: Car Display Electronic Control Unit (ECU) and Car Display itself. The Camera sub-system is composed of Camera Sensor and Camera Sensor ECU. The Electronic Power Steering sub-system is composed of Driver Steering Torque Sensor, Electronic Power Steering ECU, and Motor Providing Torque to Steering Wheel.

Notice that the Steering Wheel itself is not the part of the Item definition.

# Goals and Measures

## Goals

The goal of this functional safety case is to reduce risks connected to the Lane Assistance System to levels acceptable by society and current legislation in major auto markets. The goal is achieved by following the ISO 26262 standard guidelines.

## 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 the start of the project |
| Tailor the safety lifecycle | Safety Manager | Within 4 weeks of the start of the project |
| Plan the safety activities of the safety lifecycle | Safety Manager | Within 4 weeks of the start of the 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 the main assessment |
| Perform functional safety assessment | Safety Assessor | The conclusion of functional safety activities |

# Safety Culture

To maintain a good safety culture the guiding principles from the list below must be followed:

* 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 of 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

All phases of safety lifecycle mentioned in [Scope of the Project](#_3rdcrjn) section need to be considered since the Lane Assistance System is a new product, not a modification of an existing one. The safety lifecycle phases are restarted here again.

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 of 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. DIA helps avoid disputes between companies. It clarifies who will be responsible for any safety issues in post-production. The ultimate goal is to ensure that all parties are developing safe vehicles in compliance with ISO 26262.

The OEM is responsible for supplying a functioning lane assistance system. The Tier-1 supplier is responsible for analyzing and modifying various sub-systems from a functional safety viewpoint.

The responsibilities for specific roles are presented below.

* Functional Safety Manager - Item Level: maintains the Safety Plan for the Item, plans, coordinates, and documents the development phase of the safety lifecycle on the Item level, performs pre-audits of the overall system before the Safety Auditor.
* Functional Safety Engineer - Item Level: integrates sub-systems combining them into the Item and performs tests at a system level.
* Project Manager - Item Level: appoints safety manager, acquires and allocates resources needed for the functional safety activities.
* Functional Safety Manager - Component Level: plans, coordinates, and documents of the development phase of the safety lifecycle on the sub-systems level, monitors progress against the Safety Plan and performs pre-audits of the sub-systems before the Safety Auditor.
* Functional Safety Engineer - Component Level: develops sub-systems and tests them at hardware and software levels.
* Functional Safety Auditor: ensures that the design and production implementation conform to the Safety Plan and ISO 26262.
* Functional Safety Assessor: judges as to whether functional safety is being achieved via a functional safety assessment.

# 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.

The people who carry out confirmation measures need to be independent of the people who actually developed the project.

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.

Checking to make sure that the actual implementation of the project conforms to the safety plan is called a functional safety audit.

Confirming that plans, designs, and developed products actually achieve functional safety is called a functional safety assessment.