



Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21



Document history

Date	Version	Editor	Description
2/8/2019	1.0	Akshat Yadav	Initial revision

Table of Contents

1 Introduction.....	3
1.1 Purpose of the Safety Plan.....	3
1.2 Scope of the Project.....	3
1.3 Deliverables of the Project.....	3
2 Item Definition.....	3
3 Goals and Measures.....	5
3.1 Goals.....	5
3.2 Measures.....	5
4 Safety Culture.....	6
5 Safety Lifecycle Tailoring.....	6
6 Roles.....	7
7 Development Interface Agreement.....	7
8 Confirmation Measures.....	8

1 Introduction

1.1 Purpose of the Safety Plan

This document outlines the steps required to achieve functional safety for a Lane Assistance item. It also defines the roles and responsibilities of the team.

1.2 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

1.3 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

2 Item Definition

The item considered in this plan is a simplified version of a Lane Assistance System, which detects the deviation of vehicle from its current lane and assists the driver to maintain the vehicle inside the lane.

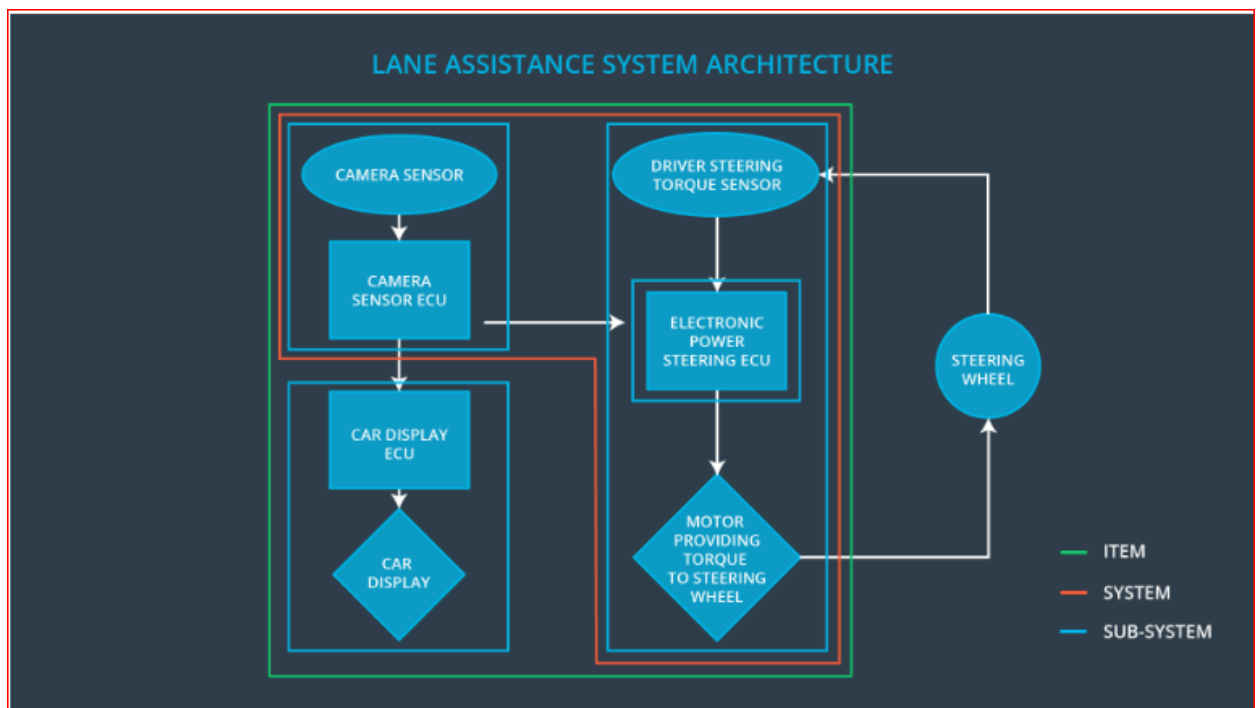
The two main functions of the item are as follows:

- **Lane departure warning function:** The lane departure warning system uses the camera to detect lane departure and apply an oscillating steering torque to provide the driver a haptic feedback.
- **Lane keeping assistance function:** The lane keeping assistance functionality automatically assist the driver in maintaining the lane by applying steering torque and turning the steering wheel towards the center of the lane.

Lane Assistance system architecture:

The functionality of the item is implemented by the following subsystem:

- **Camera Subsystem:** There are two components to this subsystem.
 - Camera Sensor: Senses if the vehicle is leaving the lane.
 - Camera Sensor ECU: Sends signal to the electronics power steering to turn and vibrate the steering and also to the car display ECU to indicate the activity.
- **Electronic Power Steering subsystem:** This subsystem is composed by three components:
 - Driver Steering Torque Sensor: Senses the torque applied by the driver.
 - Electronic Power Steering ECU: Detects how much the driver is already turning and commands the steering motor the extra torque required to get the car back towards center.
 - Motor Providing Torque to Steering Wheel.
- **Car Display subsystem:** This subsystem is composed by two components:
 - Car Display ECU: Send signal to display a warning light on the display board.
 - Car Display



The camera system detects lane departures and tells the steering wheel how hard to turn. The driver receives a warning on the vehicle display and also receives a warning via a steering wheel vibrating. Simultaneously, the wheel adds extra steering torque to help the driver move back towards the center of the lane.

The figure defines the boundaries of the item and the subsystems.

3 Goals and Measures

3.1 Goals

The goals of the project are as follows:

- Identify risk and hazardous situations in the Lane Assistance system components malfunction that may cause physical injury or damage to a person's health.
- Evaluate the risks of the hazardous situations.
- Lowering high risk level situations to reasonable levels acceptable by current society measures

3.2 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-	Safety	3 months prior to main

assessment prior to audit by external functional safety assessor	Manager	assessment
Perform functional safety assessment	Safety Assessor	Conclusion of functional safety activities

4 Safety Culture

In order to ensure a safety culture 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

5 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

6 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

7 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 (OEM):** Pre-audits, coordinate and document the item level planned safety activities including: concept phase, and product development at the system and software level.
- **Functional Safety Engineer - Item Level (OEM):** Develop prototypes, integrate subsystems combining them into the Lane Assistance item from a functional safety viewpoint.
- **Project Manager - Item Level (OEM):** Allocation of Item level resources with adequate functional safety competency, and appointment of external Functional Safety Auditor and Assessor. Lane assistance system functional safety plan, and confirmation measures acceptance.
- **Functional Safety Manager - Component Level (Tier-1):** Pre-audits, plan the development for the components of the Lane Assistance item.
- **Functional Safety Engineer - Component Level (Tier-1):** 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:** Perform functional safety assessment at conclusion of functional safety activities and judge whether the project has increased safety.

8 Confirmation Measures

The confirmation measures ensure the following purpose:

- The Lane Assistance project conforms to ISO 26262.
- The Lane Assistance project really does make the vehicle safer.

Confirmation review ensures that 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.

Functional safety audit make sure the actual implementation of the project conforms to the safety plan.

Functional safety assessment confirms that the plan, design and developed product actually achieve functional safety.