



Elektrobit



UDACITY

Safety Plan Lane Assistance

Document Version: 1.0



Document history

Date	Version	Editor	Description
20/5/2018	0.1	Ujjwal Saxena	Initial draft
21/5/2018	0.2	Ujjwal Saxena	Updated Goals and Measures
22/5/2018	1.0	Ujjwal Saxena	Finalized document

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

This document acts as a framework for the functional safety plan for Lane Assistance System. This defines the steps needed to be taken to ensure a functionally safe system (viz. Lane Assistance system) and it also allocates roles and responsibilities to the relevant personnel.

Scope of the Project

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

1. Concept phase
2. Product Development at the System Level
3. Product Development at the Software Level

We will discuss these three in further detail.

The following phases are out of scope:

1. Product Development at the Hardware Level
2. Production and Operation

Deliverables of the Project

Following are the deliverables of the project.

1. Safety Plan
2. Hazard Analysis and Risk Assessment
3. Functional Safety Concept
4. Technical Safety Concept
5. Software Safety Requirements and Architecture

Item Definition

Lane Assistance System helps the vehicle to stay in the center of the lane. It also warns the driver by means of vibration in the steering wheel if the car moves to the edge of the lane or moves out of the lane.

Lane assistance system does the following two tasks.

1. **Lane Keeping Assistance:**

This helps in keeping the vehicle in the ego lane. Ego lane is the lane in which vehicle is currently driving. So if a car is not in the ego lane, this functionality moves the steering wheel by applying steering torque to bring the vehicle back to the center of the lane.

2. **Lane Departure warning**

Lane departure warns the driver whenever the car moves out of the ego lane. The lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback. When the vehicle drifts away from the lane, this vibrates the steering wheel to warn the driver.

Subsystems of Lane Assistance System:

1. Camera Subsystem
2. Car Display subsystem
3. Electronic Power Steering subsystem

Lane Assistance System consists **Camera subsystem**, **Car Display subsystem** and the **Electronic Power Steering subsystem** within its boundaries. **Steering wheel subsystem** lies outside of the boundary.

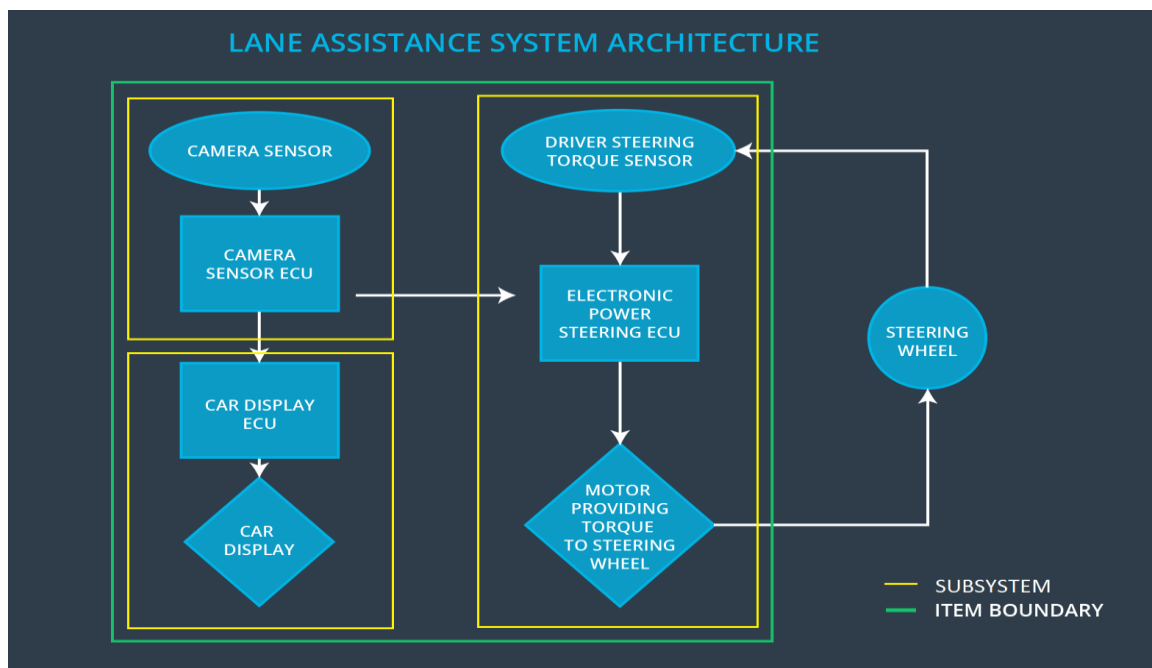


Figure 1 Lane Assistance system Architecture

Goals and Measures

Goals

The primary goal of safety plan is to determine all possible risks of the lane assistance system. Additionally, to conform to ISO 26262 Standards and ensuring the safe and reliable working of the lane assistance system. Based on the outcome of risk analysis, we can classify safety levels and devise plans to mitigate risks and avoid potential hazards. Risks determined here are ones which are reasonable and under the acceptance limits of the society.

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 safety lifecycle	Safety Manager	Within 4 weeks of start of project
Plan 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

Safety culture are the characteristics an organization exhibits in order to implement the well-defined and well managed safety processes within itself. Some of the characteristics of a good safety culture of an organization are:

- **High priority**
Safety has the highest priority among competing constraints like cost and productivity within an organization.
- **Accountability**
All design decisions and development activities are documented to ensure accountability and are traceable back to the people and teams who made those decisions.
- **Rewards**
The organization motivates and supports the achievement of functional safety by rewarding such employees who adhere to such standards.
- **Penalties**
The organization penalizes employees using shortcuts that jeopardize safety or quality. It also penalizes the processes which overlook the defined safety measures.
- **Independence**
Teams who design and develop a product are independent from the teams who audit the work. This is necessary so as not to keep any bias towards a certain procedure.
- **Well defined processes**
Organization design and management processes are clearly defined and accessible to employees.
- **Resources**
Projects should 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 Lane Assistance Project, the following safety lifecycle phases are in scope:

1. Concept phase
2. Product Development at the System Level
3. 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

Development interface agreement (DIA) is a mutually agreed agreement between multiple parties that sets forth the expectations from each one. Here the parties in question are the OEM, Tier 1 Suppliers and the Tier 2 Suppliers. DIA ensures that all parties are developing safe vehicles in compliance with ISO 26262.

The responsibilities of the OEM are to define the functionality of the lane assistance system and to conduct the activities in scope of project manager, safety manager and safety engineer in item level.

Confirmation Measures

The main purpose of confirmation measures is:

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

Confirmation review is a measurement process to ensure compliance of project with ISO 26262 standards throughout product design and development stages. An independent review process makes sure ISO 26262 is being followed.

Functional safety audit checks ensure that the actual implementation of the project conforms to the safety plan. Functional safety assessment confirms that plans, designs and developed products actually achieve functional safety.
