Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
10-17-18	1.0	Madhukar	Initial Draft

Table of Contents

Introduction

Purpose of the Safety Plan

This document has been prepared to properly defined the framework of “Lane Assistance System”.
In this doument project scope, deliverables, roles & responciblities of stakeholders has been detailed.

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

Lane Assistance System is a functionality of autonomous vehicle. While driving it assist the user in driving inside the lane and when it predicts its otherwise behavior, it warns the user.

Its major functionality:
1> Lane departure warning: To warn user in case vehicle is drifting away from the lane
2> Lane keeping assistance: Assist vehicle to ride inside the lane in auto drive mode

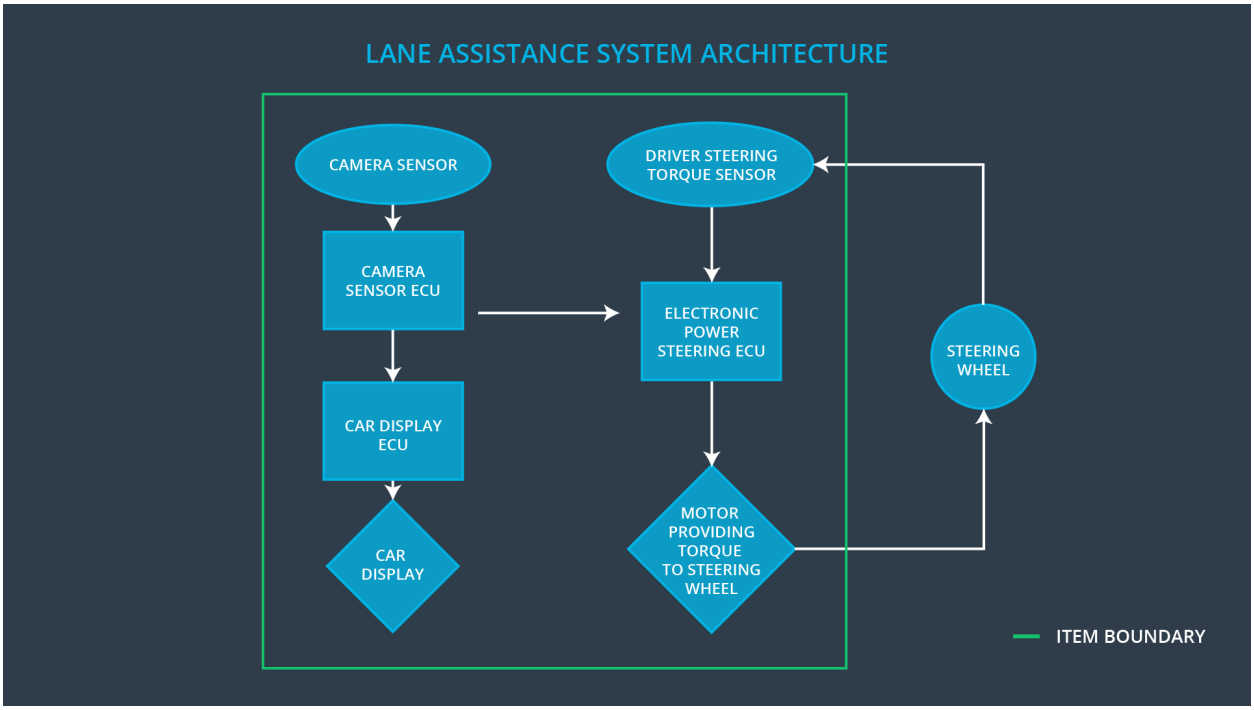
Following subsystems are used for Lane Assitance functionality:

> Camera Subsystem: It has following components
- Camera Sensor
- Camera Sensor ECU

> Electronic Power Steering Subsystem: It has following components
- Steering Torque Sensor
- Electronic Power Steering ECU
- Steering Wheel Motor

> Car Display Subsystem: It has following components
- Car Display
- Car Display ECU

Following diagram shows the interaction between above mentione subsystem:



During driving when camera predicts that the vehicle is departing from the lane, it sends signal to the Electronic Power Steering system through communication channel. Electronic Power steering system then provide additional torque needed to the steering to keep the vehicle in lane and also puts vibration in the steering to warn the user.

These functionality will be active when Auto Drive Mode will be active during driving. Also, when turn signal is ON, Lane Assistance System remain deactivated till the Turn indicator is active. Lane assistance can also be deactivated manually through activate-deactivate button.

Apart from providing the asistance in Lane driving, this system will also provide information on dashboard using some indicator whenever camera subsystem predicts that vehicle is leaving the lane.

Goals and Measures

Goals

This project goals are:

- Identify risk and hazardous situations in the Line Assistance system components malfunction causing injuries to a person.
- Evaluate the risks of the hazardous situations.
- Low to risk of the malfunctions to a reasonable levels acceptable by current 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	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 Manager	3 months prior to main assessment
Perform functional safety assessment	Safety Assessor	Conclusion of functional safety activities

Safety Culture

Our organization has a good safety culture having following characteristics:

- **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

Following phases of safety lifecycle are in the scope:

> Concept Phase
> System level Product development
> SW level product development

Following phases of safety lifecycle are out of scope:

> HW system development
> Production and development

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 ultimate goal is to ensure that all parties are developing safe vehicles in compliance with ISO 26262.
A DIA (development interface agreement) defines the roles and responsibilities between 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.

2. Being the Tier-1 Supplier we will be accountable for the lane assistance component and not the other parts of the vehicle. The Tier-1 Supplier will analyze and modify various sub-systems of the lane assistance component from a functional safety viewpoint.
The Tier-1 company will act and fix all bugs which apply to the lane assistance system. All other issues have to be investigated by the 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.

Confirmation review: It 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.

Functional Safety Audit: It is checking to make sure that the actual implementation of the project conforms to the safety plan.

Functional Safety Assesment: It 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.