Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.0
Released on 2018-05-22

Document history

Date	Version	Editor	Description
14-May-2018	0.1	Jyothikumar	Initial Draft
22-May-2018	1.0	Jyothikumar	First Attempt

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

Vehicles have many different subsystems like electrical & electronics, hydraulic, mechanical, chemical sub systems. Every system is produced by different vendors. To achieve safe system, risk associated with each sub system has to be minimized. To achieve this goal, Safety plan defines the steps to be followed and explains the roles and responsibility of resources involved in the project.

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

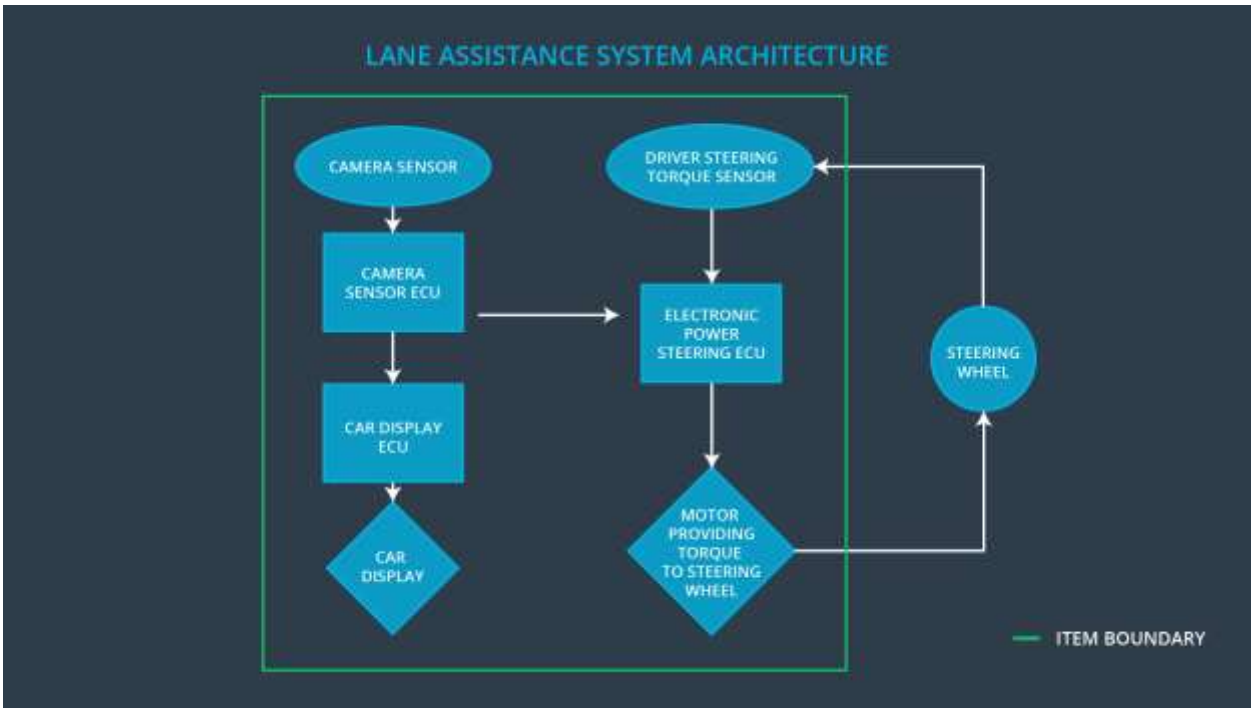
The safety plan investigates about “Lane Assistance System” which is a part of “Advance Driver Assistance System” (ADAS). This will alert the driver if the vehicle drift towards edge of the lane and take control of steering wheel so that car turn towards the center of the center.

This item is achieved by the following functions.

- **Lane departure warning:** This will sense current position of car in the lane. If it drives towards the edge, the steering wheel will be vibrated. This will help the driver to take the corrective action.
- **Lane keeping assistance:** If the driver changes the lane without proper signal, Lane departure warning will alert the driver. In case, driver is not responded to the alert, “Lane keeping Assistance” system take control of steering wheel in order to stay on the lane.

The above functions perform automatically. Apart from vibrating the steering wheel, warning light will be displayed in the car dashboard.

Architecture of Lane Assistance System:



The Lane Assistance system has *THREE* subsystems.

- **Camera subsystem**
  It composed of 2 components.
  - Camera sensor
  - Camera ECU

- **Electronic power steering subsystem**
  It composed of 3 components.
  - Driver steering torque sensor
  - Electronic power steering ECU
  - Motor providing torque to steering wheel
- **Car Display subsystem**
  It composed of 2 components.
  - Car Display
  - Car Display ECU

The camera subsystem is responsible for finding the car position on the lane and sending alert signal to Electronic power steering subsystem and Car display subsystem. Electronic power steering subsystem is responsible for vibrating the steering wheel (Lane departure warning) and detects how much the driver is already turning the vehicle and add required torque to get the car back towards the center (Lane Keeping Assistance). Car display subsystem will take input from camera subsystem and warning light will be displayed accordingly.

Goals and Measures

Goals

The main goal of the project is to achieve safe and reliable “Lane Assistance function” with ISO 26262. This can be done by identifying hazard situation and evaluating risk in our system. Reducing the risk by acceptable level by performing system engineering.

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	Project Manager	3 months prior to main assessment
Perform functional safety assessment	Safety Assessor	Conclusion of functional safety activities

Safety Culture

In our organization, Safety culture is straightly followed to ensure functional safety of our product. It includes the 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

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 Development Interface Agreement (DIA) is to define the roles and responsibilities between OEM and Tier-1 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. The ultimate goal is to ensure that all parties are developing safe vehicles in compliance with ISO 26262

In this project, OEM is supplying functioning lane assistance system. Tier-1 will analyze and modify only the subsystem from a functional safety standpoint.

OEM is responsible for overall vehicle safety where they conduct safety activities in item level. Our company is responsible for conducting the activities in scope of safety manager and safety engineer of the component level. 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

The main purpose of confirmation measures is:

- To ensure that Lane Assistance project conforms to ISO 26262
- To ensure that Lane Assistance project really does make the vehicle safer.

The 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.
A Functional safety audit make sure the actual implementation of the project conforms to the safety plan.
A Functional safety assessment confirms that the plan, design and developed product 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.