Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.0
Released on 2018-06-13

Document history

Date	Version	Editor	Description
06-Jun-2018	0.1	Nikhil Patel	Initial Draft
13-Jun-2018	1.0	Nikhil Patel	First Attempt

Table of Contents

Contents

Introduction

Purpose of the Safety Plan

Design a Vehicle involves different systems and subsystem like electrical & electronics, hydraulic, mechanical, chemical sub systems, and each of this subsystem is produced from different vendors thus to achieve safety so as to have a safe system, and minimized risk associated with each sub system. To achieve this goal, Safety plan defines the steps to be followed and explains the roles and responsibility of resources involved in the project. Among others this includes to define the system under consideration and to set up a goal for the project. Determine the steps that will be taken to ensure safety and appoint roles and personnel involved in the project. The project timeline sets deadlines and milestones to successfully implement the project in time

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:

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

Here we have a safety plan which investigates about “Lane Assistance System” which is a part of “Advance Driver Assistance System” (ADAS). This system will alert the driver whenever the potentially dangerous situation like when the vehicle drift towards edge of the lane and then driver need to take control of steering wheel so that car turns towards the center of the center, thus preventing accident from happening.

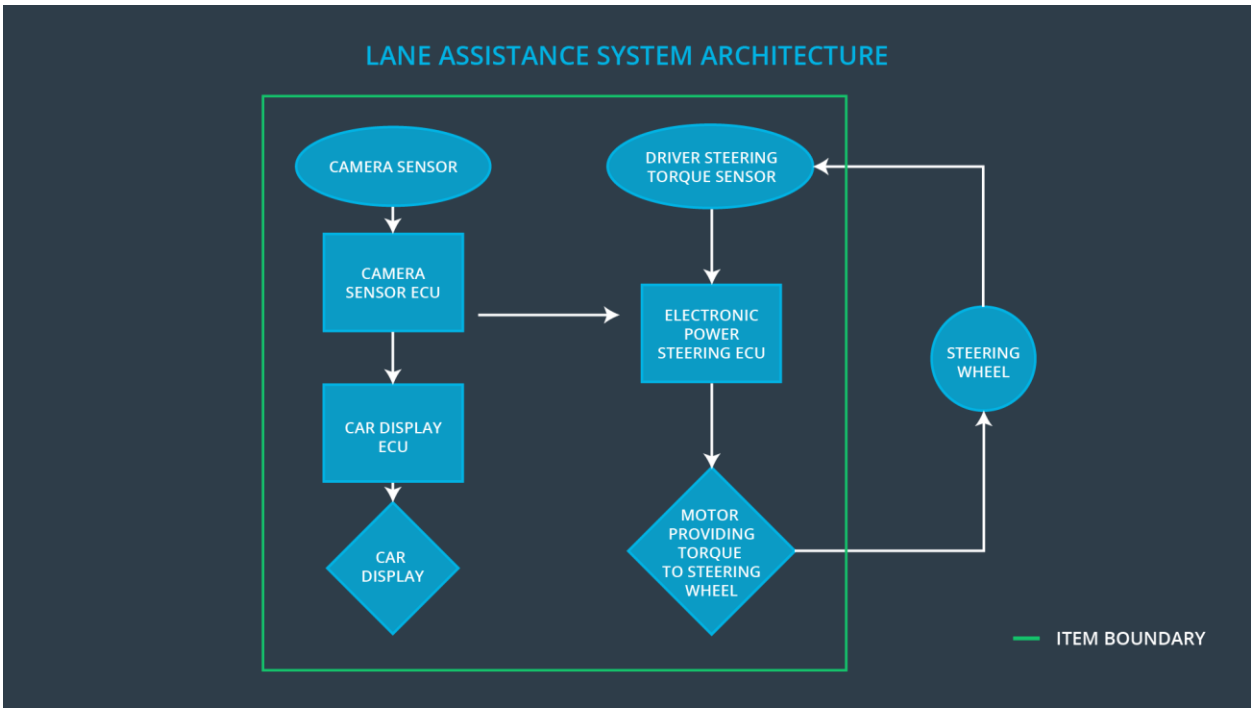
This task is achieved by the following functions.

- **Lane departure warning:** While sensing the current position of the car relative to the lane position, if the vehicle is more leaned towards the edge then the steering wheel need to vibrate, this will help the driver to take the corrective action. Camera detects the lane departure which sends the signal to the power steering system which will turn apply torque to vibrate the steering wheel.

- **Lane keeping assistance:** When the driver changes the lane without any proper signals then the 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. Like above one, this one is also detected by the camera subsystem and sends the signals to the power steering system which apply the torque for some duration.

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

Subsystem Responsibilities:

1. Cameras: - This subsystem identify relative position of the car with respect to the lane and sending the signals to the power steering subsystem and car display subsystem
2. 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).

3. Car display subsystem: - Will take input from camera subsystem and warning light will be displayed accordingly.

Goals and Measures

Goals

Analyze the lane departure warning function and lane keeping assistance system for identifying all the possible defects and the resulting hazard situation in order to achieve safe and reliable “Lane Assistance function” with ISO 26262. Also this would ensure that risk is within the 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

Since the cost and productivty are important for a successful system and market integration, safety is our number one priority. Designing functional safety is following defined processes and assures that design decisions are traceable back to the people and teams who made the decisions. Development and auditing teams are indepent and have to involve people of different of intellectual backgrounds. It is crucial that communication between those teams is based on full disclosure of problems. All necessary resources including people with appropriate skills are assigned to this functional safety project.

- **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

When dealing with a new implementation and not modification, the entire safety lifecycle including all the phases mentioned in chapter **Scope of the Project** have to be too followed and documented. Hardware components and respective product development, as well as the final production and operations phase are part of another team's functional safety analysis and hence not part of this 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

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.

Here are major sections of a DIA:

- Appointment of customer and supplier safety managers
- Joint tailoring of the safety lifecycle

- Activities and processes to be performed by the customer; activities and processes to be performed by the supplier
- Information and work products to be exchanged
- Parties or persons responsible for each activity in design and production
- Any supporting processes or tools to ensure compatibility between customer and supplier technologies

Confirmation Measures

Confirmation Measures Definitions

- 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.

- Functional safety audit

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

- Functional safety assessment

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