Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
04 Sep 2017	1.0	Navneet Latawa	First submission

Table of Contents

Introduction

Purpose of the Safety Plan

The purpose of this safety plan is to prepare the safety plan for Lane Assistance Functional Safety project to be followed by the people involved in developing a product. It will highlight the people to be involved, processes they need to follow and what they need to do to comply with the safety standards.

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

LaneAssistance - As part of Lane Assistance project, we will discuss item **LaneAssistance** which will actually be part of a bigger system Advanced Driver Assistance System(ADAS) developed by OEM.

Two main functions of **LaneAssistance** will be :

- **Lane departure warning(LDW)**
  This module will generate a warning as soon as vehicle tries to go outside the current lane boundary. This system will be active only if driver has not activated the lane changing signal
- **Lane keeping assistance(LKA)**
  - This module will direct the car to stay in the lane. It will identify the lanes and control vehicle so that it stays in the lane.

There will be three sub-systems:

Camera System :
This sub-system will capture lane images and will identify lane boundaries.

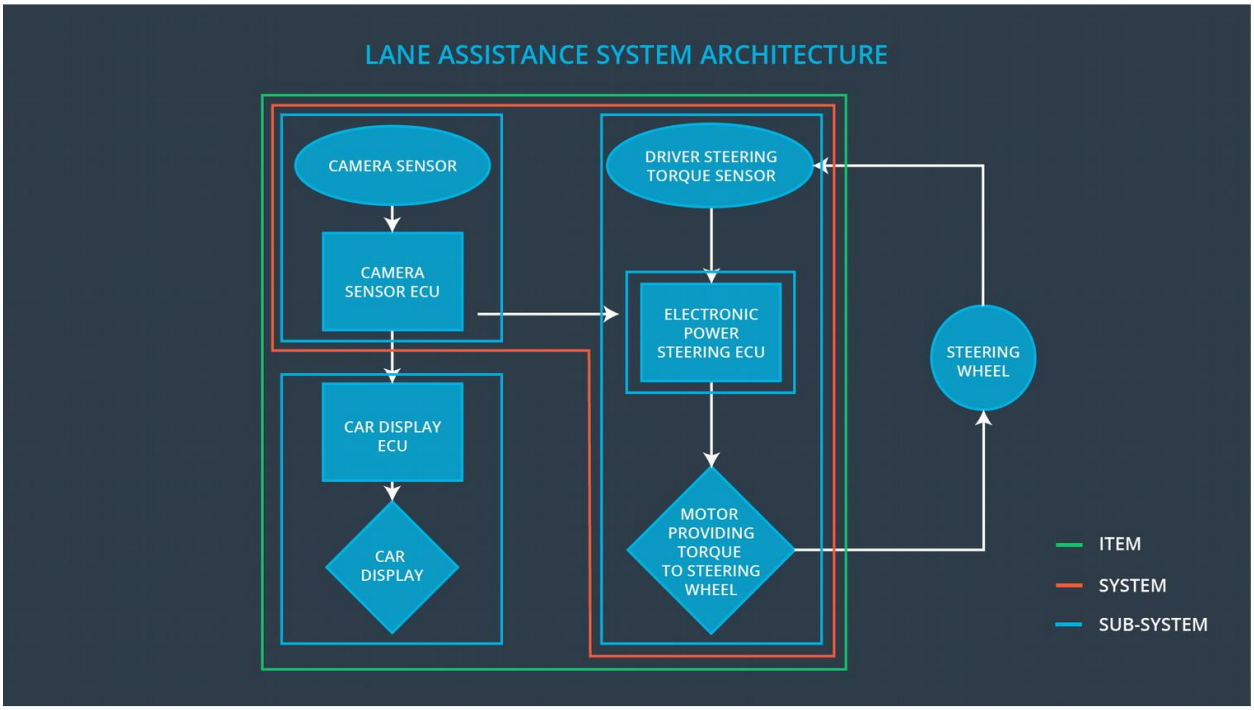
Electronic Power Steering system(EPS)
This system combines LDW, LKA torques with driver provided torque and send torque signal to the motor to provide LDW and LKA functionality.

Car Display System
It has display for LDW and LKA activation/deactivation and on/off switch for LDW and LKA functionality.

Main functionality of system

The system behaves in a way that as soon as car is about to leave the lane, LDW and LKA functionality is activated - warning signal is sent to the car display and appropriate torque is calculated to be sent to EPS ECU (Electronic control unit) to be sent to the motor. There are limits set for the torque so that it is not beyond the limits to avoid car becoming uncontrollable. LKA functionality is activated for only a fixed duration so that driver does not assume car to be fully autonomous.
As driver is also providing torque, EPS ECU determines how much extra torque is to be provided.
Driver also has the option to turn on\off Lane Assistance system using on\off switch on car display.
Lane Assistance functionality is deactivated when driver is using lane change signal.

.



Following modules are not part of this project

- Sensor modules to detect other cars' parameters – project will use existing\available sensor modules
- Vibration system hardware : project will use existing vibration generating hardware. Out system will only send signals to the vibration system to work
- Pre-trained machine learning module : this will be an existing pre-trained module to identify the road
- Cruise Control
- Blind spot monitoring
- Tire Pressure monitoring

Goals and Measures

Goals

The main goal of this LaneAssistance project is to prepare the Functional Safety documents so that product can be developed keeping in mind the necessary Safety standards and to ensure that all parties involved are in compliance with common standards ISO 26262. Preparing these documents will help identify the hazards and risks related to the product developed and processes to be followed to ensure Functional safety of the product.

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

Safety Culture

Safety is the keystone of our company and our success depends upon providing safe running vehicles to the people. Main highlights of our safety culture are:

High priority: safety will be given highest priority among competing constraints like cost and productivity

Accountability: people and team making design decision should be held accountable through traceability mechanism

Rewards: People and teams adhering to highest Safety standards should be appropriately rewarded

Penalties: Anyone violating or causing\making others to violate policies should be penalized

Independence: teams who design and develop a product should be independent from the teams who audit the work

Well defined processes: company design, development, safety and management processes should be clearly defined

Resources: projects should have necessary resources including people with appropriate skills

Diversity: Teams developing products should encourage intellectual diversity and it should be integrated into processes

Communication\Ombudsman : communication channels should be established to encourage disclosure of problems. Anonymous call system should be established to report any safety related incidents anyone comes across

Safety Lifecycle Tailoring

Safety manager will define the full safety lifecycle for developing a product. It will include all steps and policies to be followed to make sure that safety plan is adhered to.

After identification of whether the development is related to a new product or it is going to change an existing product, it will be Safety Manager's responsibility to decide which safety processes are to be followed.

For the lane assistance project, the safety lifecycle will be tailored to

- include following phases:
  - Concept phase
  - Product Development at the System Level
  - Product Development at the Software Level
- exclude the following phases:
  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

Purpose of a development interface agreement

Development interface agreement will be prepared to clarify the roles and responsibilities between companies involved in the development. It will include clear instructions about who is responsible for what aspects and what quality levels of the product delivery.

Development interface agreement will ensure that the involved parties are in compliance with ISO 26262.

Responsibilities

Tier-1 (Our Company)
Our company will be responsible for ensuring that the sub-systems we develop follow the safety standards. As Functional Safety Manager and Engineer roles are played by our company employees, they will be responsible for following :

Functional Safety Manager

- Prepares and maintains Safety plan for the subsystem
- Monitors progress against the safety plan
- Pre-audits - pre-audits will be done at pre-defined frequency

Functional Safety Engineer

- Prototypes will be developed for the sub-systems,
- Sub-systems will be integrated into large systems

OEM(Original Equipment Manufacturer)
OEM will be reponsible for the whole product\item. It will take sub-systems from the Tier-1 and Tier 2 suppliers and will integrate to build a product. OEM will be responsible for following roles:

Project Manager

- Overall project management for the whole project
- Acquires and allocates resources needed for the functional safety activities
- Appoints safety manager or might act as safety manager

Safety Manager

OEM Safety Manager keeps the whole product in mind while doing following activities

- Planning, coordinating and documenting of the development phase of the safety lifecycle

- Maintains the safety plan
- Monitors progress against the safety plan
- Performs pre-audits before the safety auditor

Safety Engineer

OEM Safety Engineer keeps the whole product in mind while doing following activities

- Product development
- Integration
- Testing at the hardware, software and system levels

OEM or External

Safety Auditor

- Ensures that the design and production implementation conform to the safety plan and ISO 26262
- Must be independent from the team developing the project

Safety Assessor

- Independent judgement as to whether functional safety is being achieved via a functional safety assessment
- Must be independent from the team developing the project

Confirmation Measures

The main purpose of Confirmation measures is that

- Functional Safety Project confirms to the ISO 26262
- project does make the vehicle safer
- project conforms to ehe safety plan

Confirmation review

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

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

Functional safety assessment

Functional safety assessment confirms that plans, designs and developed products actually achieve functional safety.