Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
23-May-2018	1.0	Nishant Katariya	Initial Draft

Table of Contents

Introduction

Purpose of the Safety Plan

Purpose of this safety plan is to provide the overall framework for safety related to Lane Assistance system. It also defines roles and responsibilities for functional safety of this item.

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 Item under focus of this project is Lane assistance system. The Lane Assistance System have two functionalities:

1. Lane departure warning
2. Lane keeping assistance

When the driver drifts towards the edge of the lane, two things will happen:

- the lane departure warning function will vibrate the steering wheel as a warning
- the lane keeping assistance function will move the steering wheel so that the wheels turn towards the center of the lane, it is kind of an action.

A more formal requirement of lane departure warning system is as follow “The lane departure warning function shall apply an oscillating torque to steering wheel to provide driver haptic feedback”. Putting simply the vehicle quickly rotate the steering wheel back and forth which creates vibration.

The **lane keeping assistance functionality** will automatically **assist** the driver to keep the lane; the steering wheel turns towards the center of the lane If a driver departs a lane without using a turn signal. Putting it formally “The Lane keeping assistance system apply the steering torque to stay in the ego lane”. Ego lane is the lane in which our vehicle is currently driving.

Fig 1.1 shows the Lane Assistance System Architecture at whole, all the subsystems and their boundaries on high level.

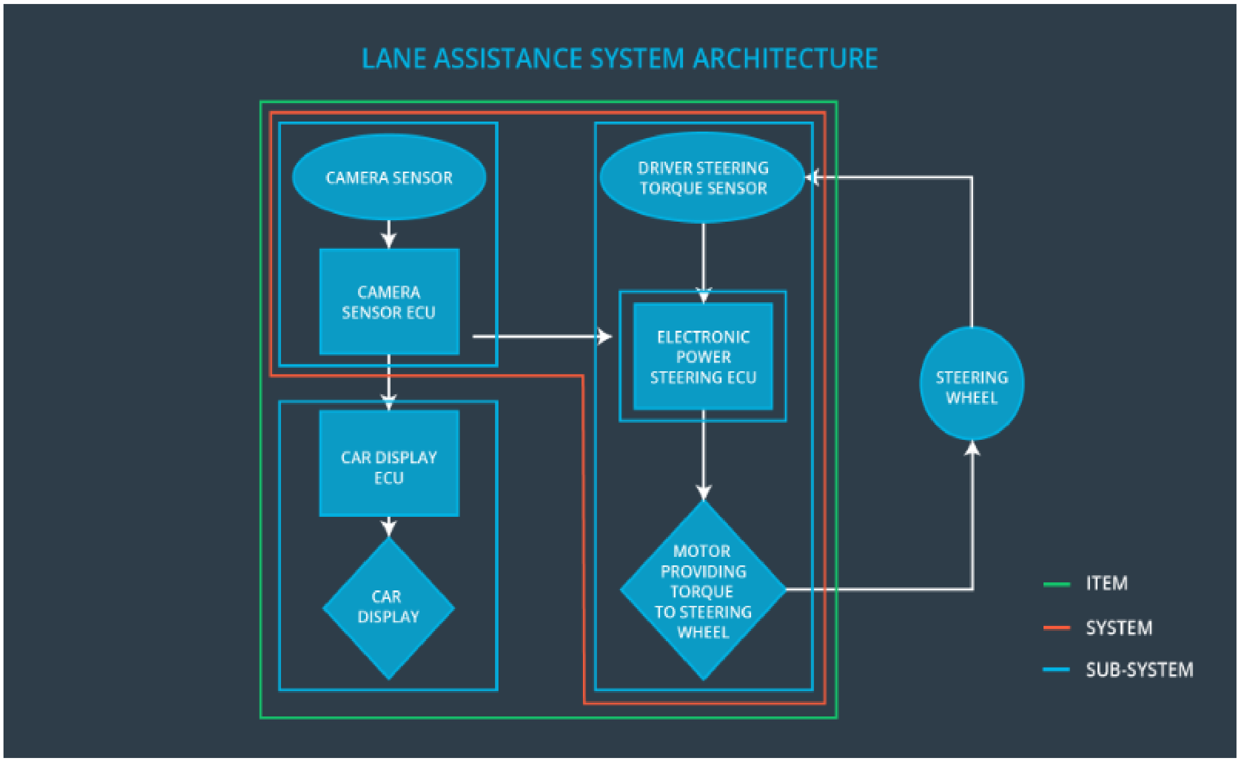
LANE ASSISTANCE SYSTEM ARCHITECTURE
CAMERA SENSOR
CAMERA SENSOR ECU
CAR DISPLAY ECU
CAR DISPLAY
DRIVER STEERING TORQUE SENSOR
ELECTRONIC POWER STEERING ECU
MOTOR PROVIDING TORQUE TO STEERING WHEEL
STEERING WHEEL
ITEM
SYSTEM
SUB-SYSTEM

Fig 1.1

Camera sensor perceives the vehicle leaving the lane, it sends the signal to the Electronic power steering system request to turn/vibrate the steering wheel.
ECU (Electronic Control Unit) is a microcomputer that contains software and hardware specific to vehicle’s functionality.

The camera ECU have the hardware and software required for detecting lanes using computer vision techniques like machine learning or image processing.

camera sub system detects lane departures and request the steering wheel how hard to turn. The driver receives a warning on the vehicle display and also receives an alert via a steering wheel vibrating. Simultaneously, the wheel adds extra steering torque to help the driver move back towards the center of the lane.

As shown in fig 1.1 all the subsystems and systems are part of the Item except steering wheel which does not fall into the boundary of the item.

Goals and Measures

Goals

The overall goal of this project is to assure safe operation of E/E components of Lane Assistance function as per the ISO 26262. Goals can be divided in 3 steps as follows:

1. Identify risk and hazards in the Lane Assistance System
2. Evaluate the risk of hazards
3. Lower risk using systems 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	Safety Manager	3 months prior to main assessment
Perform functional safety assessment	Safety Assessor	Conclusion of functional safety activities

Safety Culture

It is important that technology malfunction is not the only one source of vehicle accidents. Social and organization factors play a very important role to ensure safety, we at our company follows a safety culture described in below points:

High Priority	Safety is at the highest priority among other constrains like cost and productivity
Accountability	Ensuring accountability such that designs are traceable back to the team who made decisions.
Rewards	Organization promotes safety by providing with rewards.
Penalties	Organization penalizes the unsafe shortcuts
Independence	Responsibilities of the team are independent from other teams
Communication	disclosure of problems is encouraged through different communication channels

Safety Lifecycle Tailoring

We are dealing with the new system and not the modification to existing system, so all the phases of the safety lifecycle mentioned under scope of the project will be considered.

The following phases 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 the DIA (Development Interface Agreement) is to clearly define activities, process to be done by different organization to avoid conflicts and assure liability.
DIA also defines the work product and evidences to prove work was done as per the agreement. The ultimate goal is to make sure all the parties are developing product as per ISO 26262.

OEM will supply the functioning lane assistance system, as a tier-1 company our company will analyze and modify the various sub-systems from a functional safety viewpoint.

Following are major sections of a DIA:

- Appointment of supplier and customer safety managers
- Parties or persons responsible for each activity in design and production

- Activities and processes to be performed by the customer; activities and processes to be performed by the supplier
- Joint tailoring of the safety lifecycle
- Information and work products to be exchanged
- Any supporting processes or tools to ensure compatibility between customer and supplier technologies

Confirmation Measures

Confirmation measures serve following purposes:

- A functional safety project confronts to ISO 26262
- Project really does make the vehicle safer

Confirmation review
It ensures the project complies with standard ISO 26262 and independent team/person review that the ISO 26262 standard has been followed.

Functional safety audit
It is the check to make sure that final implementation of project conforms to the safety plan

Functional safety assessment
It is process of confirming that safety plans, designs and final product actually achieved the 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.