Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 2.0
Final Version 2.0, Released on 2019-05-29

Document history

Date	Version	Editor	Description
29-May-2019	1.0	Sandeep Patil	Initial Version
30-May-2019	2.0	Sandeep Patil	Updated details in the individual chapters

Table of Contents

Introduction

Purpose of the Safety Plan

The purpose of safety plan is to identify high risk involved in the Lane Assistance System and to lower them to reasonable levels. This is done by identifying hazards, measuring risks. These risks are further lowered using Systems Engineering.

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 (LAS) when enabled, continuously detects if the driver is unintendedly crossing lane. If the ego vehicle is crossing lane without the relevant direction indicator, the system shall give haptic feedback and provide counter torque to the steering wheel to bring back the ego vehicle in the lane.

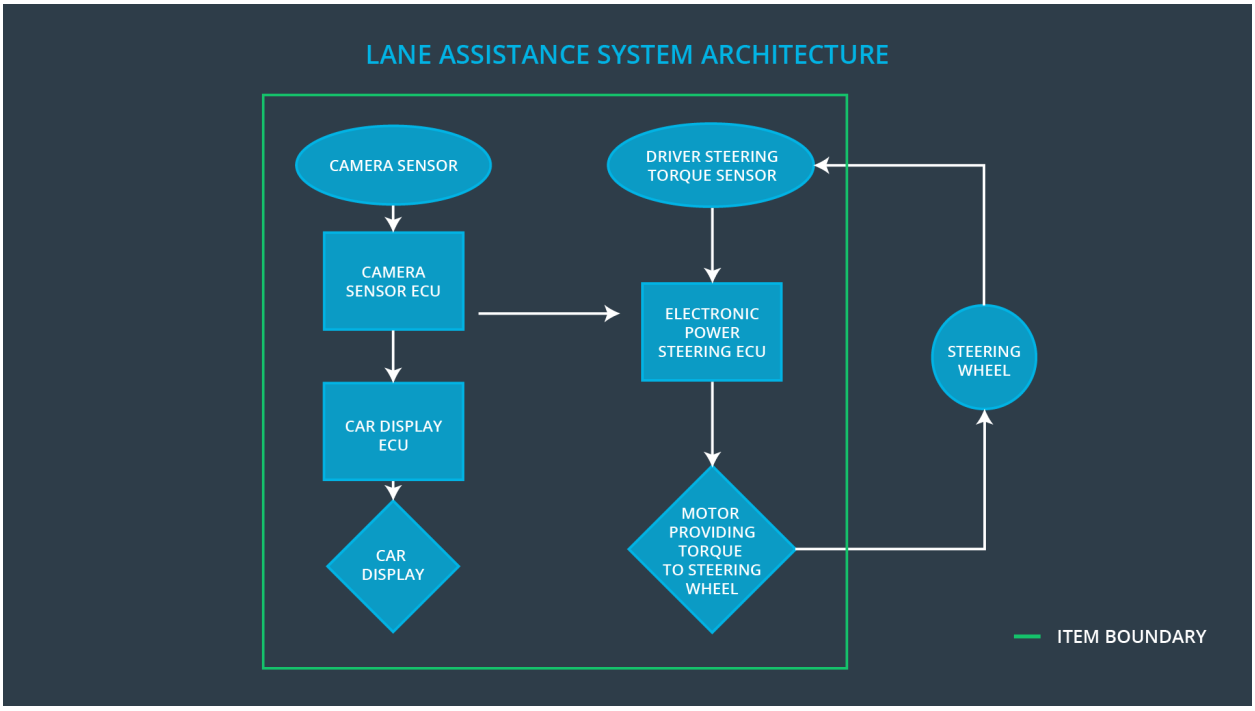
The two main functions of LAS are as follows.

1. Lane Departure Warning
   If the unintended lane departure is detected, the system vibrates the steering wheel to caution the driver about the behavior.

2. Lane Keeping Assistance
   The system provides counter torque to the steering wheel to bring back the ego vehicle into the lane

The LAS consists of 3 subsystems

1. **Camera (CAM)** subsystem which is responsible for detection of Lane Departure and deciding if it was intended or not. It generates torque request for counter steering and also sends haptic signal for steering wheel for vibration.
2. **Electronic Power Steering (EPS)** subsystem which is responsible for calculating final torque by combining the torque request coming from the CAM subsystem and the Driver and providing it to the steering wheel
3. **Car Display Unit (CDU)** subsystem which is responsible for delplaying status of the the LDW and LKS function activation



Goals and Measures

Goals

The major goal of this project is to identify and reduce risk to acceptable levels in the LAS which would cause injuries to a person.

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	All Team Members	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

In our company, we follow a good safety culture which have below characteristics.

- **High Priority**
  We give highest priority to the Safety among the competing constraints like cost and productivity

- **Accountability**
  All the process we follow are tailored to ensure accountability by making sure the forward and reverse traceability from the design decision to the people and teams who made them
- **Rewards**
  We motivate and support the achievements of functional safety
- **Penalties**
  The organization discourage and penalizes shortcuts that jeopardize safety or quality
- **Independence**
  We maintain independent team for design and develop of a product from the team who audit the work
- **Well defined processes**
  All the management and design processes are defined clearly as per the ASPICE Level 3 certification
- **Resources**
  Project is provided with necessary resource in terms of skilled employes and safety approved tools
- **Diversity**
  Intellectual diversity is sought after, valued and integrated into processes
- **Communications**
  Communication channels encourage disclosure of problems

Safety Lifecycle Tailoring

The safety lifecycle phases that are in the scope of the project are as follows

- Concept phase
- Product development at the system level
- Product development at the software level

The following phases are out of the scope of this project

- 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

This section defines the roles, responsibilities between OEM and us (XYZ company) in developing LAS and workproducts in compliance with ISO 26262.

Role	Responsibility
Functional Safety Manager	Item Level - Pre audit and plan the development phase at Item Level
Functional Safety Engineer	Item Level - Develops prototype, integrate subsystem into large system
Project Manager	Item Level - Allocates resources as needed
Functional Safety Manager	Component Level - Pre audit and plan development phase at component level for LAS
Functional Safety Engineer	Component Level - Develops prototype, integrate modules into components LAS
Functional Safety Auditor	External - Make sure the project conforms to the safety plan
Functional Safety Assessor	External - Judges if the project has increased safety

Confirmation Measures

The purpose of confirmation measure is to ensure that the project conforms to the Functional Safety standard ISO 26262 and also check if the project makes the vehicle really safer.

Confirmation review shall be performed to ensures that the project complies with ISO 26262. As the product is designed and developed, The review shall be done by an independent.

There shall be Functional safety audit to make sure that the actual implementation of the project conforms to the safety plan.

There shall be Functional safety assessment confirming 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.