Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
03/02/2019	1.0	Rangarajan Ramanujam	Initial draft of the Safety plan

Table of Contents

Introduction

Purpose of the Safety Plan

Vehicles are complex systems with both sociological and technical requirements. Hence it is imperative to methodically analyze the hardware and software requirements to develop a safe vehicle. This document defines the overall framework for a Lane assistance system. This document also specifies the roles and responsibilities of the item's functional safety.

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 considered in this plan is the simplified version of the Lane assistance system. Lane assistance system is one of the features which falls under the Advanced driver assistance system (ADAS). The lane assistance system alerts the driver of potentially dangerous driving scenarios and provide assistance pre-emptively to prevent accidents.

This item performs two basic functions:

- ***Lane Departure warning(LDW) function:*** When the driver drifts out towards the edge of the lane, the LDW system shall apply an oscillating steering torque to warn the driver by provision of tactile feedback.
- ***Lane keeping assistance(LKA) function:*** When the driver drifts out towards the edge of the lane, the LKA system shall apply a steering torque to guide the vehicle towards the center of the ego(current vehicle) lane.

In addition to the above mentioned functions, this item shall light up a warning light in the car dashboard to present visual confirmation of driver assistance provided.

The above behavior is functionally achieved through the following subsystems:

- **Camera subsystem** : This subsystem consists of 2 components
  - Camera Sensor
  - Camera Sensor Electronic Control Unit(ECU)
- **Electronic power steering subsystem**: This subsystem consists of 3 components
  - Driver Steering Torque Sensor
  - Electronic Power Steering ECU
  - Motor providing torque to steering wheel
- **Car display subsystem** : This subsystem consists of 2 components
  - Car Display ECU
  - Car Display

The following diagram depicts the architecture of the Lane assistance item:

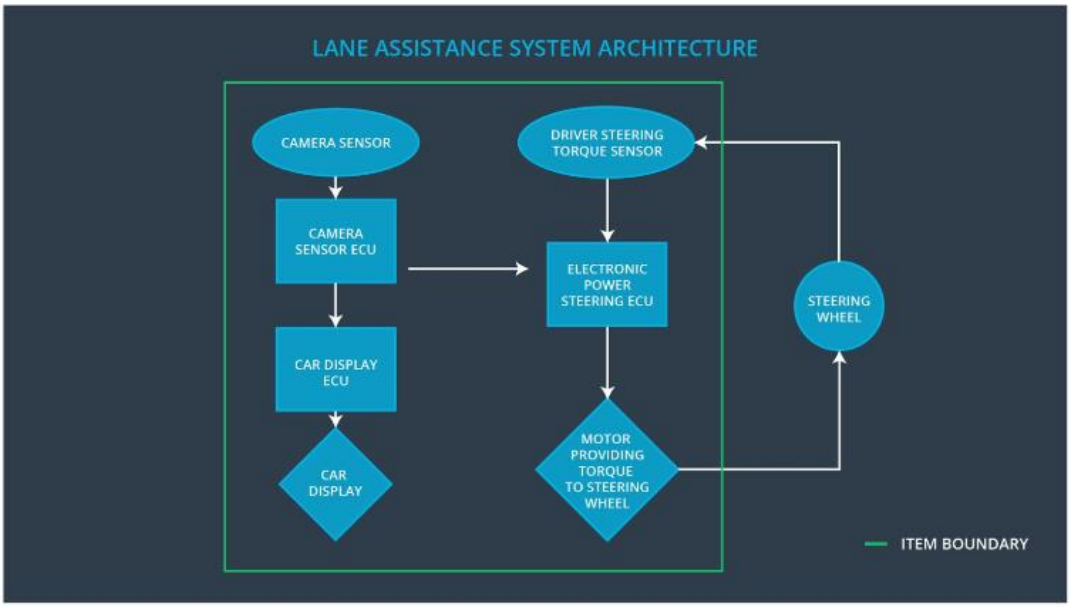

Fig 1: Lane Assistance System Architecture

The camera subsystem is responsible for detecting and monitoring the position of the car in the ego lane. The camera senses the vehicle leaving the lane and requests the steering ECU and the car display ECU's to react accordingly. The car display will show a warning light on the dashboard. This way the driver is notified through both visual and tactile feedback that the lane assistance system is active.

There are several conditions under which the behavior of this system is defined as under:

- The lane line detection can be difficult in extreme weather conditions such as snow, rain,etc. Under unreliable detecting conditions, the lane assistance system will not provide assistance.

- If the driver uses a turn signal, the lane assistance system deactivates so that vehicle can leave the lane. Driver shall be provided an option to turn off the system completely through a button on the dashboard
- If the Drivers hands or not on the wheel, the lane assistance system will not provide assistance. The steering system has the ability to detect whether driver's hands are ON/OFF.

The Lane assistance system does not include Autonomous driving functionality.

Goals and Measures

Goals

The Lane assistance system does not include Autonomous driving functionality.
The project goals are:

- Identify risky and hazardous situations in the Lane assistance system components which has the potential to cause injuries to a person
- Evaluate the corresponding risks of hazardous situations
- Lower risk of malfunctions to reasonable levels that are acaeptable by current society

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

Our organization has a rich safety culture enforced through the following characteristics:

- ***High priority***: Safety has the highest priority
- ***Well defined processes***: Clearly defined management processes and company design
- ***Accountability***: Quality process to ensure design decisions are documented and traceable
- ***Diversity***: People with different skills and backgrounds work together
- ***Communication***: Potential safety problems are reported immediately and solutions are clearly documented
- ***Rewards & Penalties***: Compromise of safety and quality are penalized. Management shall always motivate and support achievement of functional safety among competing constraints like cost and productivity.
- ***Independence***: Product designers, developers, auditors and testers belong to a different organization

The above values are communicated through all management levels to encourage proactive actions and engineer built in quality into system designs.

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 Development Interface Agreement (DIA) helps to avoid disputes during planning and development of the lane assistance system as it clearly defines the roles and responsibilities between the involved companies. This section defines the roles and responsibilities in the development of ISO 26262 compliance for the Lane assistance functionality.

- **Functional Safety Manager-Item Level** : Pre aduits, plans the development phase for the lane assistance item
- **Functional Safety Engineer-Item Level** : Develop prototypes, integrate subsystems combining them into the lane assistance item to achieve intended functionality
- **Project manager – Item Level** : Allocates the resources needed for the item
- **Functional Safety Manager – Component Level(Rangarajan Ramanujam)** : Pre aduits, plan the development for the components of the lane assistance item
- **Functional Safety Engineer – Component Level(Rangarajan Ramanujam)** : Develop prototypes and integrate components conforming to the lane assistance systems
- **Functional Safety Auditor** : Conformance to safety plan
- **Functional Safety Assessor** : Assessment of increased safety of item

The OEM is responsible for overall safety and all ISO 26262 required functional safety actions. The companies agree that the above tailored safety life cycle is adequate to confirm with ISO 26262 norms. Our company will act and fix all the bugs which apply only to the lane assistance system. All other issues have to be investigated by the OEM.

Confirmation Measures

The purpose of the confirmation measures are:

- Processes comply with the functional safety standard(ISO 26262)
- Project execution is following the safety plan
- Design improves functional safety.

The ***Confirmation Review*** will ensure project compliance to ISO 26262 and will be performed by a person independent of the design and development team.

Functional Safety Audit shall be executed to ensure implementation conforms to safety plan.

Functional Safety Assessment shall be executed to confirm that the plan, design and developed product improves functional safety of the item

---

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.