Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
20/06/2016	1.0	Aditya	

Table of Contents

Introduction

Purpose of the Safety Plan

The Safety plan defines and outlines the steps to achieve functional safety. It also includes the assignment of roles and responsibilities for 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 safety plan is a simplified version of Lane Assistance system. This Advanced Driver Assistance System alerts the driver of a potential dangerous situation and take control over the vehicle to prevent accidents from occurring.

The Lane Assistance system has two main functions –

- Lane departure warning: When the driver drifts out towards the edge of the lane, this function applies an oscillating steering torque to provide the driver a haptic feedback.

- Lane keeping assistance: This function will apply a steering torque when active in order to stay in the lane.

Both this functions are automatic and a warning light shall be displayed on the cars dashboard when any of the above functions is active.

The above functionalities are implemented by following subsystems:

- Camera subsystem having a camera sensor and an Electronic Control Unit (ECU).
- Electronic Power Steering consisting a Driver Steering Torque Sensor, Electronic Power Steering ECU and a Motor providing torque to the Steering Wheel.
- Car Display System having Car Display and its ECU.

The following figure (Fig 1) show interactions between above system.

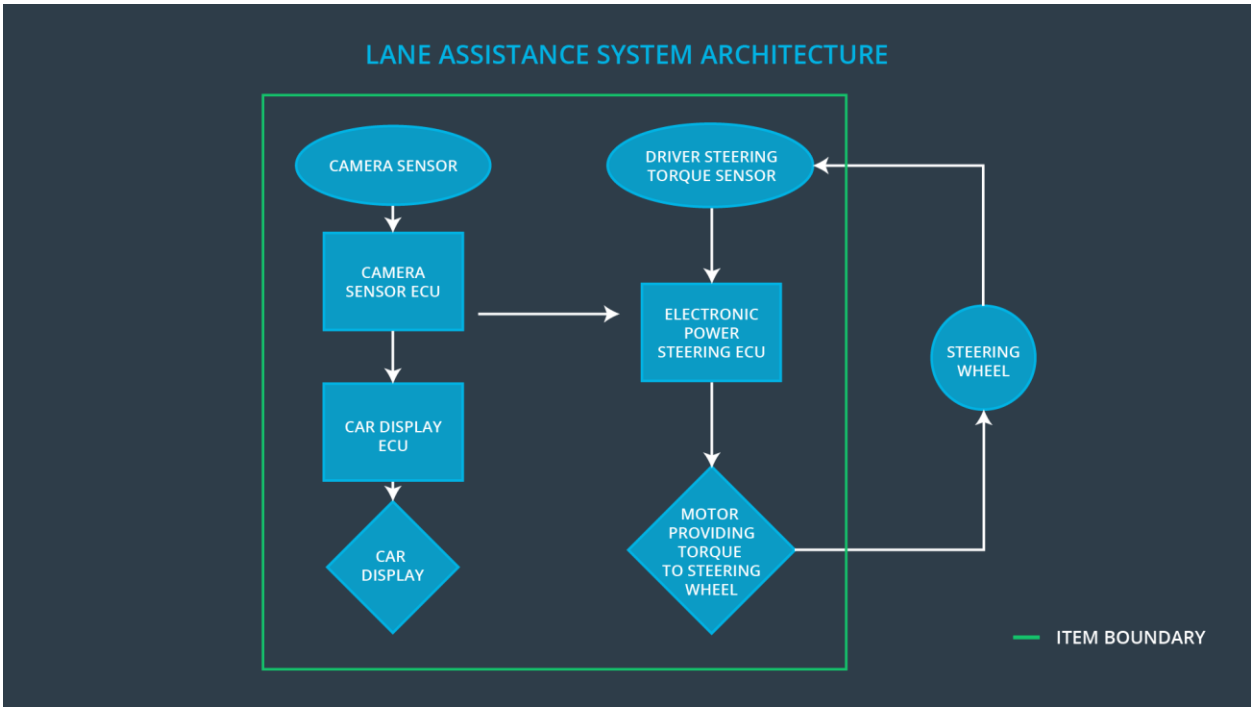

Fig 1

The camera subsystem is responsible for monitoring the cars position in the lane and activates the functions i.e. turn and vibrate the steering wheel. It also turns on the warning light on the display to inform the driver that the lane assistance system is active.
If the driver uses a turn signal, them the lane assistance system deactivates so that the vehicle can change the lane. The driver can also turn off the system with a button the dashboard.

Goals and Measures

Goals

The project goals are as follows-

- Identify risk and hazardous situations in the Lane Assistance System.
- Evaluate the risk of hazardous situations.
- Lower the risk of the malfunctions to reasonable levels acceptable 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	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

To ensure safety culture following characteristics need to observed:

- 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

The Lane Assistance Project is a modification to an existing system and require only the following phases:

In scope phases:

- Concept Phase
- Product Development at System Level
- Product Development at Software Level

Out of scope phases:

- Product Development at 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

A DIA (development interface agreement) defines the roles and responsibilities between companies involved in developing a product. The ultimate goal is to ensure that all parties are developing safe vehicles in compliance with ISO 26262.

Here are major steps 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 ensure two purposes that a functional safety project conforms to ISO 26262, and that the project really does make the vehicle safer. Therefore, a confirmation review, functional safety audit and functional safety assessment will be conducted.
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 is conducted to make sure that the actual implementation of the project conforms to the safety plan.

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.