Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
10.12.2017	1.0	Raz Nissim	First draft

Table of Contents

Introduction

Purpose of the Safety Plan

The safety plan documents the process and the requirements for achieving functional safety in the creation of advanced driver assistance systems (ADAS). The plan defines the roles and responsibilities of team members, creating accountability for safety performance. Development interfaces are detailed in order to define responsibilities across different functions working on the project.

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 Advanced Driver Assistance System is an electromechanical system which provides two functions:

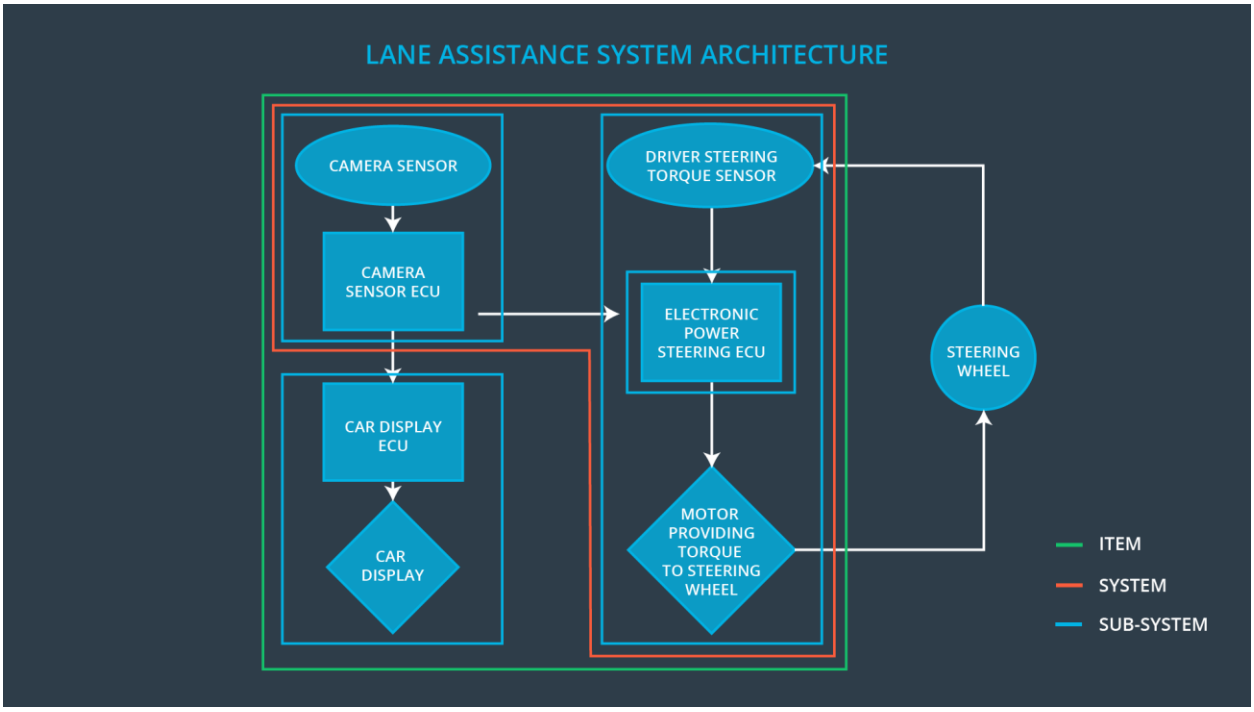
1. Lane departure warning: The system will provide haptic feedback through the vibrations in the wheel when the system detects unintentional departure from current lane.
2. Lane keeping assistance: The system will actuate vehicle controls to assist the driver in positioning the vehicle into the center of the current lane.

The system will only provide warnings and limited assistance to the driver. Limitations on the usability of the system will also be described based on the operating environment and scenarios for the vehicle.

Achieving this functionality will be done using computer vision algorithms on camera images. These images will be used to detect lane lines on the road. The camera control unit will calculate desired torque requirements and issue requests to the electronic power steering ECU. It will also issue lane departure warning requests to the electronic power steering ECU where the steering wheel should be vibrated to warn the driver. The camera control unit will communicate with the car display ECU to indicate its state (ON/OFF/FAULT) on car display.

The electronic power steering system shall receive torque requests from the camera ECU and actuate the power steering motor to achieve the desired response. The power steering motor shall also detect driver steering input and ensure that the ADAS system is only functional when the driver is in control of the vehicle.

The overall hardware system architecture is given below. The scope of the system is shown in the orange box and is made up of two sub-systems shown in blue boxes:



Goals and Measures

Goals

The goal of this project is to understand and implement the requirements of ISO 26262 for the lane departure and lane keeping feature as a use case. This includes identifying and quantifying the risks. The system will then be engineered per the standards of ISO 26262, with the safety requirements in mind. Risk identified as unreasonable, shall be dealt with and mitigated.

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

For our company, safety is the highest priority. Every employee has responsibility for safety, from the engineer to the CEO. We have a zero-tolerance approach to shortcuts which jeopardize the safety of our products. Our design and engineering teams work separately from our safety auditors, and every single employee undergoes safety standards training. Employees are encouraged to report potential problems instead of covering them up.

Safety Lifecycle Tailoring

This project focuses on the design and product development stages, since no new hardware is required. This will include a hazard analysis and risk assessment, as well as a functional safety concept. After product development, we will validate the system ensuring it upholds the safety requirements.

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 is to thoroughly define the responsibilities and roles of all parties tasked with the creation of the product. All parties must agree on its contents before development begins. As a tier-1 supplier, our responsibility is to ensure the project conforms to ISO 26262 standards as detailed in the safety plan, as well as to develop prototypes and subsystem integration.

Confirmation Measures

The main purpose of conformation measures is to ensure ISO 26262 standards are met, and that the product really increases a vehicle’s safety. During development, we’ll review progress making sure ISO 26262 is followed. Finally, confirming that the design and implementation achieve functional safety will be done in our functional safety assessment.

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.