Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.0

Document history

Date	Version	Editor	Description
2017-09-05	1.0	Yifei Li	First Submission
2017-09-25	1.1	Yifei Li	Added responsibilities clarification between OEM and Tier 1

Table of Contents

Introduction

Purpose of the Safety Plan

The purpose of safety plan is to define roles and outline the steps and resources to achieve functional safety including describing vehicle system that will be under analysis, the goals of the project and the activities that will be included; it also explains the safety culture expected, tools used in order to schedule, manage and measure 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:

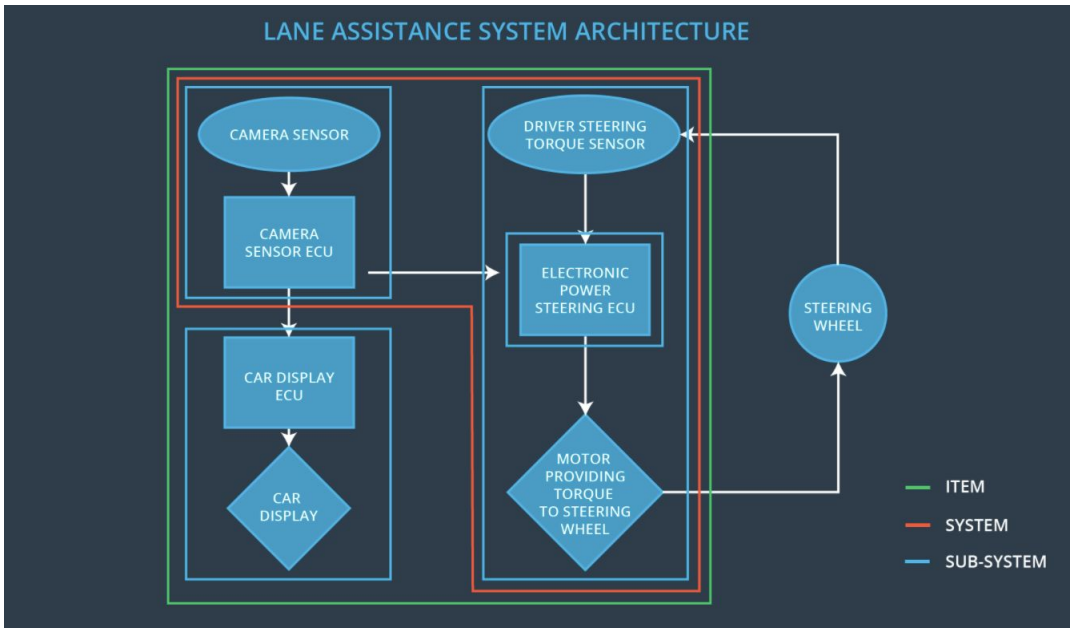
- Safety Plan
- Hazard Analysis and Risk Assessment
- Functional Safety Concept
- Technical Safety Concept
- Software Safety Requirements and Architecture

Item Definition

- A lane assistance item or system alerts the driver of unintentional lane departure and helps to driver to keep inside the lane. A lane assistance item generally has two functions:
    1. lane departure warning
    2. lane keeping assistance

    If a driver departs a lane without using a turn signal, the system assumes that the driver has become distracted and did not mean to leave the lane. The system will vibrate the steering (lane departure warning) and also move the steering wheel back towards the lane center (lane keeping assistance).

- Lane assistance item or Lane assistance system can be divided into three sub-systems:
    1. Camera system
       responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake
    2. Electronic Power Steering system
       responsible for measuring the torque provided by the driver and then adding an appropriate amount of torque based on a lane assistance system torque request
    3. Car Display system
       Responsible for displaying warning messages when the vehicle leaves the lane by mistake
- Camera system and Car Display system are responsible for lane departure warning function
- Camera system and Electronic Power Steering system are responsible for lane keeping assistance
- Below diagram explains the lane assistance system architecture. Steering wheel is outside of the lane assistance system. Inside the lane assistance system, camera system is combined by camera sensor and camera sensor ECU; Car display system is combined by car display and car display ECU; Electronic power steering system is combined with motor, driver steering torque sensor and electronic power steering ECU.



Goals and Measures

Goals

The goal of this safety plan is to ensure that all parties developing safe vehicles are in compliance with ISO 26262 and the final Vehicle Lane Assistance System does make the vehicle safer.

Measures

Measures and Activities	Responsibility	Timeline
Follow safety processes	All Team Members	Constantly
Create and sustain a safety culture	Safety Manager	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

Safety has the highest priority among other competing constraints like cost and productivity. Each person is held accountable for the products/parts he or she is designing and developing, and we will take great effort to motivates and supports those who achieved great results of functional safety, on the contrary, those jeopardize safety or quality will be penalized. We value each person's opinion and we seek, value and integrate intellectual diversity into the processes and we provide necessary resources including people with appropriate skills to achieve the goals. We seem independence, we will have work audited by other teams that are independent from teams who design and develop a product. At last, we promotes good communication, we believe in building good communication channels can encourage resolution and disclosure or problems.

Safety Lifecycle Tailoring

Since hardware, production and operation of the Lane Assistance System is not changed, we will tailor safety lifecycle as such that only Product Concept Phase, Product Development at the System Level and Product Development at the Software Level will be discussed and addressed.

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 Development Interface Agreement (DIA) defines the roles and responsibilities between companies involved in developing a product. All involved parties need to agree on the contents of the DIA before the project begins. The DIA also specifies what evidence and work products each party will provide to prove that work was done according to the agreement. The ultimate goal is to ensure that all parties are developing safety vehicles in compliance with ISO 26262.

OEM is responsible for defining requirements of the system including the sub-systems. Tier 1 supplier is responsible for the development and actual production of the system. OEM should be liable for any undefined and/or mis-defined requirements that result to functional safety issues. Tier-1 supplier is liable for any product design and/or production issues that do not meet OEM's requirements and/or safety goals.

Integration of the sub-system into a working lane assistance system would be OEM's responsibility while tier 1 supplier is responsible for development of the sub-system and any issues associated with it.

Confirmation Measures

The purpose of confirmation measures is to:

1. Ensure a functional safety project confirms to ISO 26262
2. Ensure that the project really does make the vehicle safer

Confirmation review is to ensure that the project complies with ISO 26262. As the project is designed and developed, an independent person would review the work to make sure ISO 26262 is followed.

Functional safety audit is to check and make sure that the actual implementation of the project conforms to the safety plan.

Functional safety assessment is to confirm that plans, designs and developed products actually achieve functional safety.