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
05-11-2018	1.0	Rasmita Samantaray	Initial Release

Table of Contents

Document history

Table of Contents

Introduction
- Purpose of the Safety Plan
- Scope of the Project
- Deliverables of the Project

Item Definition

Goals and Measures
- Goals
- Measures

Safety Culture

Safety Lifecycle Tailoring

Roles

Development Interface Agreement

Confirmation Measures

Introduction

Purpose of the Safety Plan

The purpose of the plan is to provide an overall process used to achieve functional safety for the implementation of an Advanced Driver Assistance Systems (ADAS). This document describes a safety plan of the lane assistance, detect risk and reduce it to the acceptance levels.

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

This project covers the **Lane Assistance System** which is an Advanced Driver Assistance System (ADAS). It consists of two sub-systems:

1. **Lane Departure Warning**:
The system will provide feedback to driver when the system detects that the vehicle is unintentionally departing its current lane.

2. **Lane Keeping Assistance**: The other part of the overall system to steer the car back into the centre of the current lane.

The item boundary include three sub-systems as given in Figure 1:
• Camera system
• Electronic Power Steering system
• Car Display system

When the camera senses that the vehicle is leaving the lane, the camera sends a signal to the electronic power steering system requesting to turn and vibrate the steering wheel. Also the camera sensor detect the road lanes and request to turn on the warning light in the car display dashboard to indicate the driver that the lane assistance system is active. The electronic power steering subsystem has a sensor to detect how much the driver is already turning. The lane keeping assistance function adds the extra torque required to get the car back towards centre. The extra torque is applied directly to the steering wheel via a motor.

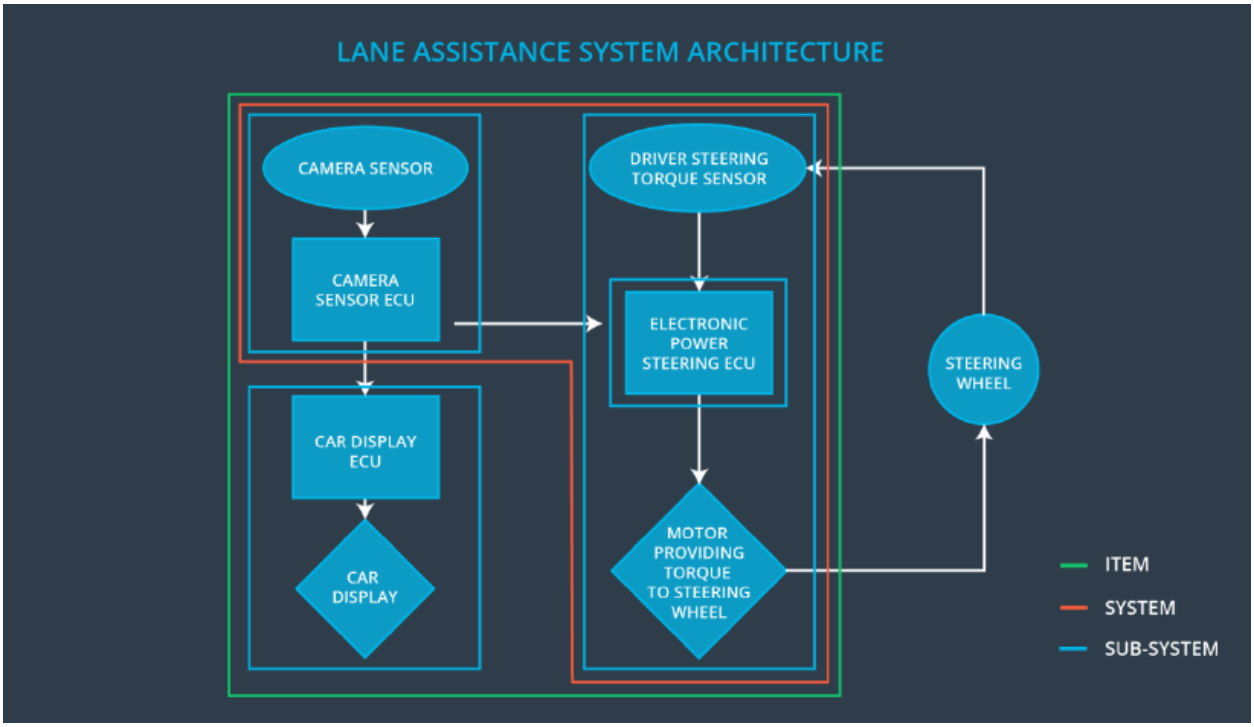

Figure 1: Lane Assistance System Architecture

The steering wheel is the element that is not included in this item because of its non-electric component.
This item has several constraints regarding the operation and environment situations, which are:

- In several conditions, such as in snow and foggy weather, the lane detection result of the camera is not very reliable.
- During in a construction zone, the lane markings may not be present. Depending on the country regulation the temporary lane colour can be less contrast so that it influences the lane detection.
- Driving at night without headlights on might provide improper illumination.

Goals and Measures

Goals

The goal of this project is to achieve functional safety of the ADAS item by analyzing the system functions with ISO 262626. This will allow identification of hazards and quantification of risk. Systems engineering will be used to minimize risk to a level such that it is acceptable to the public and does not further increase the level of risk pertaining the operating the vehicle. Through this process all unreasonable risk situations are mitigated for the ADAS.

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

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

R**esources**: projects have necessary resources including people with appropriate skills

D**iversity**: intellectual diversity is sought after, valued and integrated into processes

Communication: communication channels encourage disclosure of problems

Safety Lifecycle Tailoring

For tailoring the safety lifecycle, 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 purpose of a development interface agreement (DIA) is to ensure that all parties are developing safe vehicles in compliance with ISO 26262.

The responsibilities of the OEM are to define the functionality of the lane assistance system and to conduct the activities in scope of project manager, safete manager and safety engineer in item level. Our company is responsible for conducting the activities in scope of safety manager and safety engineer of the component level.

Confirmation Measures

The main purpose of confirmation measures is:

- To ensure that a functional safety project conforms to ISO 26262, and
- To ensure that the project really does make the vehicle safer

Confirmation review is a measurement process to ensure 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 checks to make sure that the actual implementation of the project conforms to the safety plan.

Functional safety assessment confirms 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.