Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
10.21.2018		Wanlin Yang	Lesson 15: Safety Plan
10.28.2018		Wanlin Yang	gandue

Table of Contents

Introduction

Purpose of the Safety Plan

The purpose of this safety plan is to provide an overall framework for the Lane Assistance item, and to assign roles and responsibilities for functional safety for this item.

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 lane assistance item alerts the driver that the vehicle has accidentally departed its lane, and attempts to steer the vehicle back toward the center of the lane.

The Lane Assistance System will have two functions:

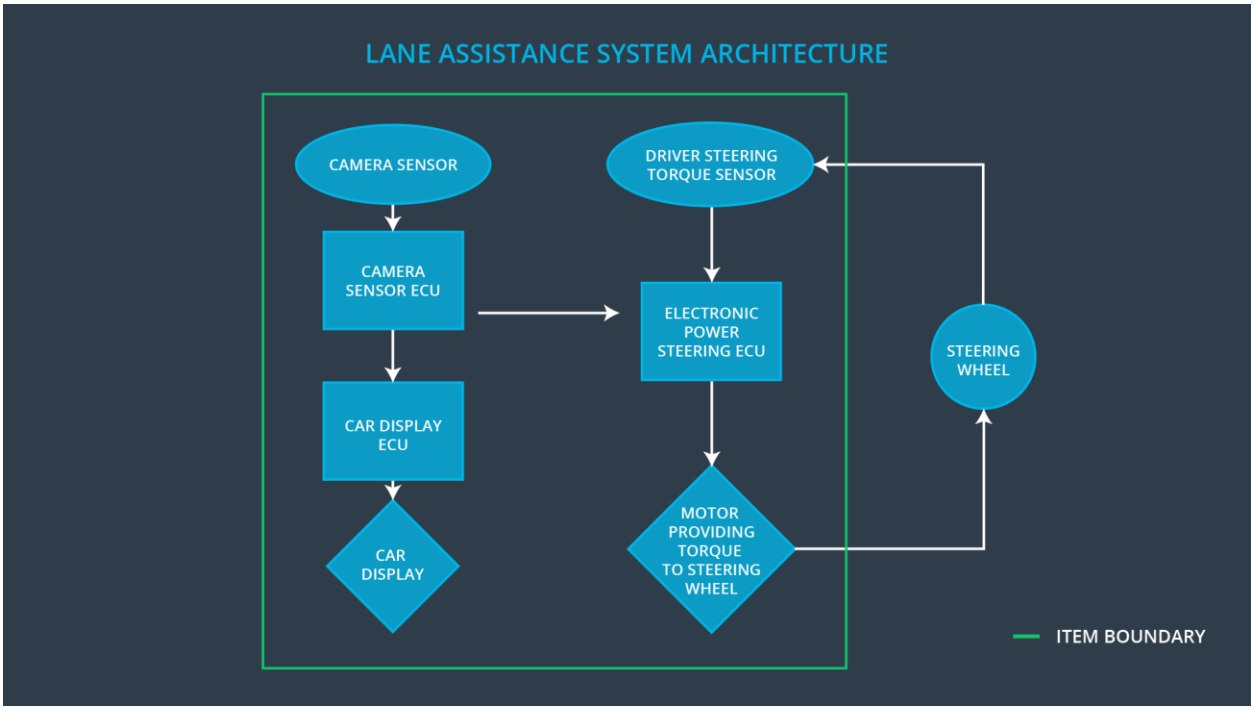
1. Lane departure warning
2. Lane keeping assistance

The lane departure warning function shall apply an oscillating torque to provide the driver a haptic feedback.
The lane keeping assistance function shall apply the steering torque when active in order to stay in ego lane.

The Lane Assistance System includes three sub-systems that responsible for each functions:

1. Camera system
2. Electronic power steering system
3. Car display system

The boundaries and subsystems are shown in the following figure.



Goals and Measures

Goals

The ultimate goal is to ensure that all parties are developing safe vehicles in compliance with ISO 26262. There are three main goals:

1. Identify risk and hazardous situations in the Line Assistance system components malfunction causing injuries to a person
2. Evaluate the risks of the hazardous situations.
3. Low to risk of the malfunctions to a reasonable levels acceptable by current sociatity.

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

A good safety culture includes:

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

With such good safety culture, everybody can follow the clear policies and strategies. This would be helpful during the development.

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

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

In this project, the OEM is supplying a functioning lane assistance system. Our company needs to analyze and modify the various sub-systems from a functional safety viewpoint.

Confirmation Measures

Confirmation Measures serve two purposes:

1. A functional safety project conforms to ISO 26262.
2. The project really does make the vehicle safer.

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 checking to make sure that the actual implementation of the project conforms to the safety plan.

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