Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 2.0

Document history

Date	Version	Editor	Description
01/01/2019	1.0	Chris Sketch	Initial Documentation
01/05/2019	2.0	Chris Sketch	Add table for subsystems

Table of Contents

Introduction

Purpose of the Safety Plan

The purpose of a safety plan is to outline the steps we will take in order to achieve functional safety. The safety plan will define the parts of the safety lifecycle impacted by new development, the roles and responsiblities of team members, the steps the company takes to promote safety culture, and the confirmation measures that will be used to determine that the plan makes the vehicle safer.

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

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 warns the driver when unintentionally leaving the lane, and assists the driver is staying within the lane.

The first function of the lane assistance item is lane departure warning. Lane departure warning warns the driver when unintentionally leaving the lane by providing haptic feedback by applying an oscillating torque to the steering wheel.

The second function of the lane assistance item is lane keeping assistance. When active, lane keeping assistance will automatically assist the driver in staying in their lane by applying a steering torque in order to stay in the vehicles current lane.

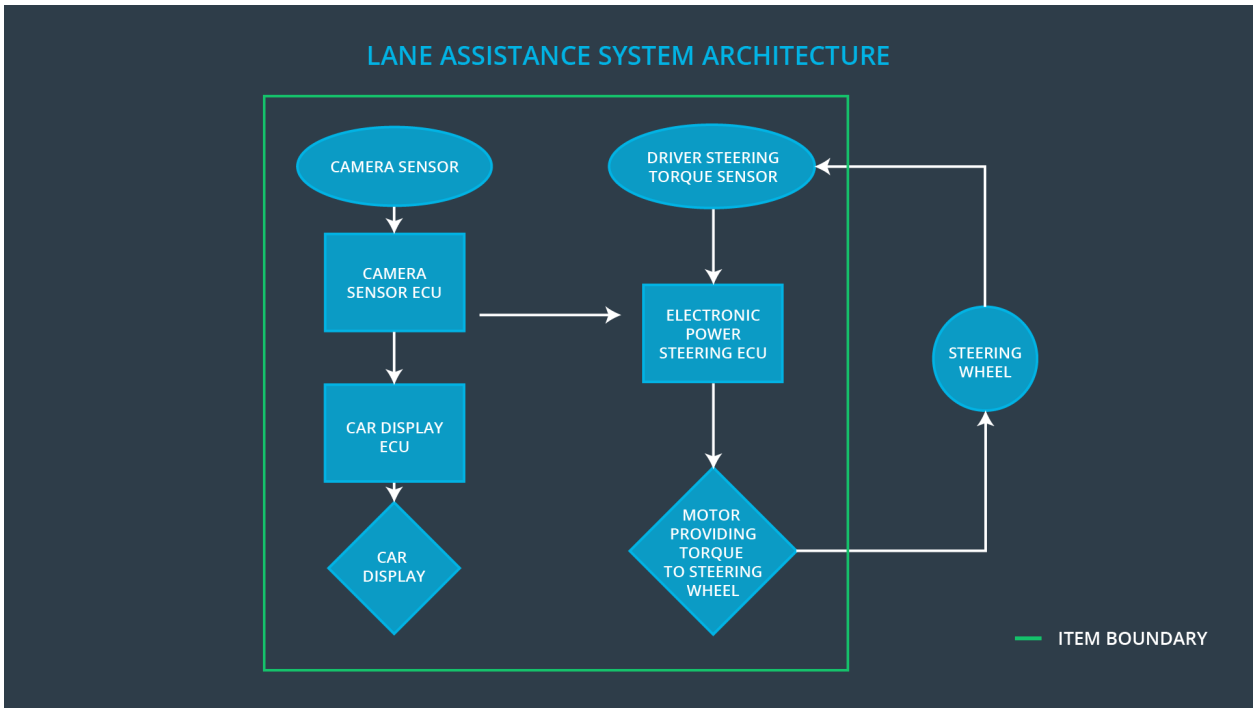

Figure 1.1: Lane assistance item boundary

The item boundary is drawn in the Figure 1.1.
The lane assistance item contains three subsystems: the camera subsystem, the electronic power steering subsystem, and the car display subsystem. The three subsystems are each involved in lane departure warning and lane keeping assistance.

Subsystem Name	Purpose	Components	Interface
Camera subsystem	responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake	The camera subsystem contains a camera sensor and a camera sensor ECU.	he camera subsystem sends requests to the electronic power steering subsystem and the car display subsystem.
Electronic power steering subsystem	Responsible for measuring the torque provided by the driver and then adding an appropriate amount of	The electronic power steering subsystem contains a driver steering torque sensor, an electronic power steering	The electronic power steering subsystem receives requests from the camera subsystem. The electronic power steering

	torque based on a lane assistance system torque request.	ECU, and a motor providing torque to the steering wheel.	subsystem receives requests from and sends requests to the steering system.
Car display subsystem	Responsible for displaying a warning light indicating the vehicle is departing its current lane when the camera subsystem requests it.	The car display subsystem contains a car display ECU and a car display.	The car display subsystem receives requests from the camera subsystem.

Goals and Measures

Goals

The purpose of this project is to achieve functional safety for the lane keeping item.

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 Assesor	Conclusion of functional safety activities

Safety Culture

Our company's number one priority is safety. All assessments and audits will be performed by an independent assessor and auditor. All documentation is tied to the person responsible for performing the task using up-to-date safety requirements software. Our company has well defined processes in place in order to assign qualified personnel to the project. Our company will be in close communication in order to detect problems as early as possible and achieve functional safety.

Safety Lifecycle Tailoring

The safety plan will cover the concept phase, product development at the system level, and product development at the software level. Product development at the hardware level, production, and operation are outside the scope of this safety plan.

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

1. The puuropse of a development interface agreement is to clarify the responsibilities of the different parties involved in a functional safety project, to describe the work products that each company will provide, to help avoid disputes between companies, and to clarify who will be responsible for any safety issues in post-production.

2. The OEM will be responsible for ensuring that the subsystems perform their intended tasks as specified in the safety plan. The tier 1 supplier (us?) will be responsible for modifying the subsystems so that they achieve functional safety. An independent auditor

and assesor will be responsible for determining whether the system meets functional safety. After accepting the assessment, the OEM will be responsible for all safety related issues in post-production.

Confirmation Measures

1. The purpose of confirmation measures are to ensure that a functional safety project conforms to ISO-26262 and that the project makes the vehicle safer
2. A confirmation review is an independent assessment of whether the project complies with ISO-26262.
3. A functional safety audit is a task performed to check whether the actual implementation of the project conforms to its associated safety plan.
4. A functional safety assessment is a task that confirms that the product achieves functional safety