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
11/5/2017	1.0	Nicholas Moellers	First Submission

Table of Contents

[Instructions: We have provided a table of contents. If the table of contents is not showing up correctly in your word processor of choice, please update it. The table of contents should show each section of the document and page numbers or links. Most word processors can do this for you. In Google Docs, you can use headings for each section and then go to Insert > Table of Contents. Microsoft Word has similar capabilities]

Introduction

Purpose of the Safety Plan

This document is meant to provide a plan which will ensure that risks for this autonomous vehicle feature are within the acceptable boundaries for our society. The responsibilities of all team members will be documented, as will the function of the critical components which will ensure vehicle and passenger safety.

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

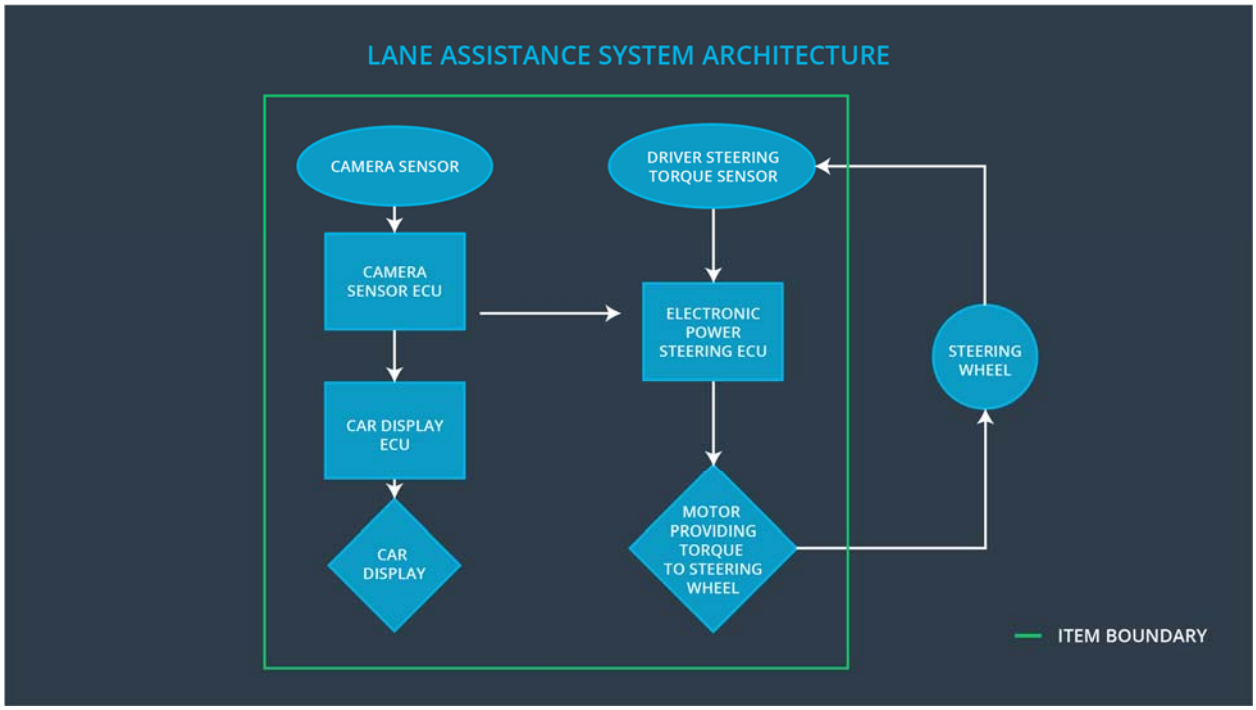
The item in question is a lane assistance feature, designed to keep the car driving in the ego lane.

The two main functions of the lane assistance feature are lane departure warning and lane keeping assistance:

1. Lane departure warning notifies the driver that the car is drifting out of the lane by imparting a vibration to the steering wheel and displaying a warning on the in car display.
2. Lane keeping assistance will apply a torque to the steering wheel to return the car back to the center of the lane.

The main subsystems involved in this feature are the camera sensor subsystem, the car display subsystem, and the electronic power steering subsystem. The camera sensor will take video of the lane and the camera sensor eco will process that the sensor data to determine the distance from the center of the lane and will transfer that information to both the car display and electronic power steering subsystems. The car display subsystem will display a warning if the car is leaving the lane. The electronic power steering subsystem will vibrate the wheel if the car is leaving the lane and apply a mild torque to the steering wheel to return the car to the ego lane. The feature will deactivate if the drive has signaled a lane change or if the drive is relying on the feature for fully autonomous driving.

All other subsystems are outside the scope of this safety plan, namely the steering wheel:



OPTIONAL

Optionally, include information about these points as well. These were not included in the lectures, but you might be able to find this information online:

- **Operational and Environmental Constraints. This could especially be limited to camera performance; lane lines are difficult to detect in snow, fog, etc**
- **Legal requirements in your country for lane assistance technology**
- **National and International Standards Related to the Item**
- **Records of previously known safety-related incidents or behavioral shortfalls**

]

Goals and Measures

Goals

The goal of this project is to ensure that the lane assistance function is delivered in line with society's expectation of safety.

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 Auditor	3 months prior to main assessment
Perform functional safety assessment	Safety Assessor	Conclusion of functional safety activities

Safety Culture

At our company, safety is always the highest priority. By rewarding activities that promote safety

and penalizing unsafe practices, we ensure that we deliver a safe product. Such activities are well documented in our safety process handbook, which our employees must review monthly. We have internal safety teams and contract out external safety assessors to ensure we are unbiased in our safety assessment.

Safety Lifecycle Tailoring

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 developer interface agreement defines the responsibilities between companies involved in developing a product. It is necessary to ensure that work was done according to the agreement and ultimately, in compliance with ISO 26262.

The OEM will be supplying a functioning lane assistance system. Our company will analyze and modify the various sub-systems from a functional safety viewpoint.

Confirmation measures exist to confirm that the safety project conforms to ISO 26262 and that it really does make the vehicle safer.

The confirmation review will ensure that the project complies with ISO 26262. This will be done by an independent person to ensure independence.

The functional safety audit will ensure that the implementation actually does conform to the safety plan.

The functional safety assessment will confirm that the designs and products actually do achieve functional safety.
