Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

[Instructions: Fill in the date, version and description fields. You can fill out the Editor field with your name if you want to do so. Keep track of your editing as if this were a real world project.

For example, if this were your first draft or first submission, you might say version 1.0. If this is a second submission attempt, then you'd add a second line with a new date and version 2.0]

Date	Version	Editor	Description
27/11/2018	1.0	Sara Mostafa	First attempt.

Table of Contents

Introduction

Purpose of the Safety Plan

The purpose of this safety plan is to provide an overall framework for lane assistance item, and to assign role 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 accidentaly departed its lane, and accepts to steer the vehicle back to the center of the lane.

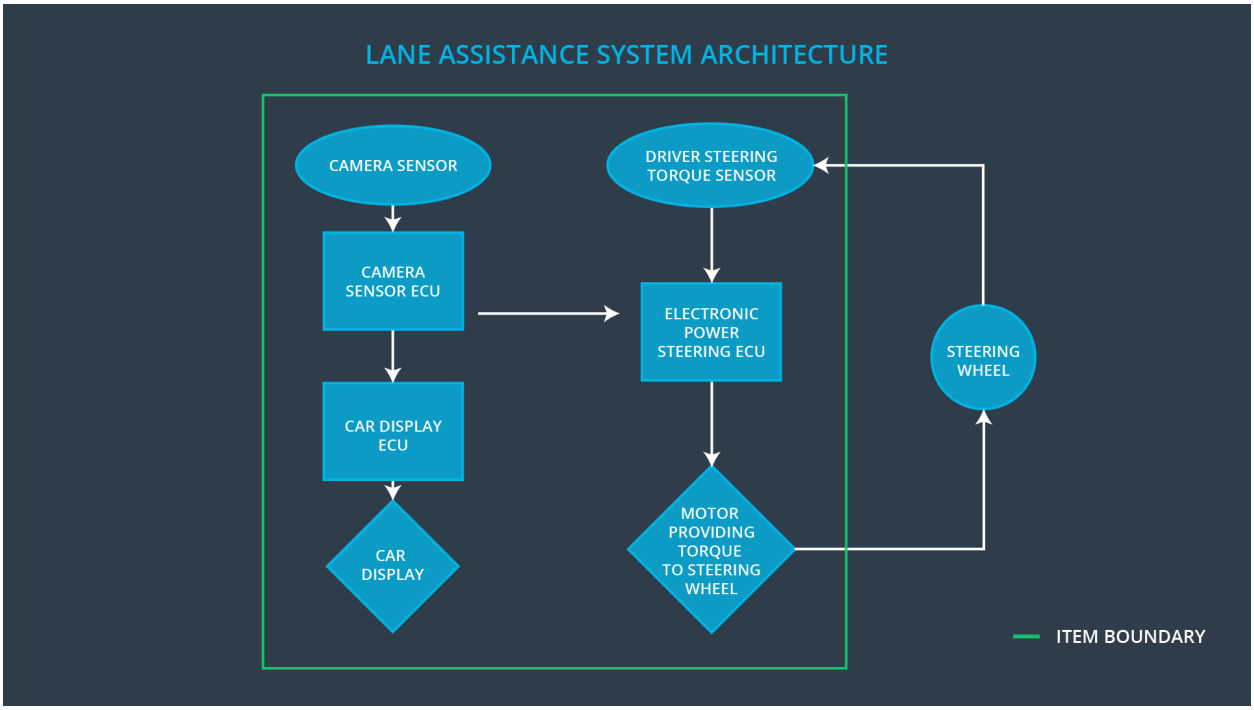
The lane assistance system has two functions:

1. Lane departure warning.
2. Lane keeping assistance.

The lane departure warning function shall apply an oscillating steering torque to provide the driver hopetic feedback.

The lane keeping assistance function shall apply the steering torque when active in order to stay in ego lane.

The camera subsystem, the elctronic power steering subsystem, and the car display system are all responsible for each functions.



Goals and Measures

Goals

The lane keeping assistance function shall be time limited and addational steering torque shall end after a given time interval so the driver cannot misuse the system for autonomous driving. The lane keeping assistance function should only work for a certain amount of time. Maybe the system brings the vehicle back to center one or two times and then stop assisting.

From the situational analysis and risk assessment discussed for the lane keeping assistance functionality, we determine ASIL B. So the safety goal for this case is ASIL B. The lane departure warning functionality, on the other hand, was determined to have ASIL A.

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

One of the high level changes is establishing a “Safety Culture” where safety is one of the highest priorities. This is contrary to the traditional priority list where schedules and cost are some of the highest priorities.
A poor safety culture dramatically elevates the risk of creating an unsafe product. If an organization cuts corners on safety, one should reasonably expect the result to be an unsafe outcome.

Safety Lifecycle Tailoring

When dealing with a new implementation and not modification, the entire safety lifecycle including all the phases mentiond in chapter Scope of the Project have to be to followed and documented. Hardware components and respective product development, as well as the final production and operations phase are part of another teams functional safety analysis and hence not part of this project.

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) 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 safe vehicles in compliance with ISO 26262.

Here are major sections of a DIA:

- Appointment of customer and supplier safety managers
- Joint tailoring of the safety lifecycle
- Activities and processes to be performed by the customer; activities and processes to be performed by the supplier
- Information and work products to be exchanged
- Parties or persons responsible for each activity in design and production
- Any supporting processes or tools to ensure compatibility between customer and supplier technologies

Confirmation Measures

Confirmation measures ensure that the applied processes comply with functional safety standards provided by ISO 26262 and that project execution is following the safety plan, therefore verifying if the design really does improve safety.

Functional saftey assessment confirms that plans, designs and developd products actually achieve functional safety.