Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.0

Document history

Date	Version	Editor	Description
02/08/2018	0.1	Pablo	Purpose of Safety Plan; Safety Culture
02/26/2018	0.2	Pablo	Goals and Measures: Measures; DIA-1; Confirmation Mesures
04/14/2018	1.0	Pablo	Completed

Table of Contents

Introduction

Purpose of the Safety Plan

The purpose of this safety plan is to define roles and responsibilities, and outline the steps we will take to achieve functional safety of a lane assistance system of a car.

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 System alerts the driver when the vehicle accidentaly leaves its lane, and corrects the steering towards the center of the vehicle ego lane.

The two main functions of the lane assistant system are:

- Lane departure warning.
- Lane keeping assistance.

When the driver drifts towards the edge of the lane:

the **lane departure warning** function shall apply an oscillating steering 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 subsystems responsible for each function are:

Camera system
Electronic Power Steering system
Car Display system

Figure 1 shows the boundaries of the item, as well as the subsystems inside and outside the item.

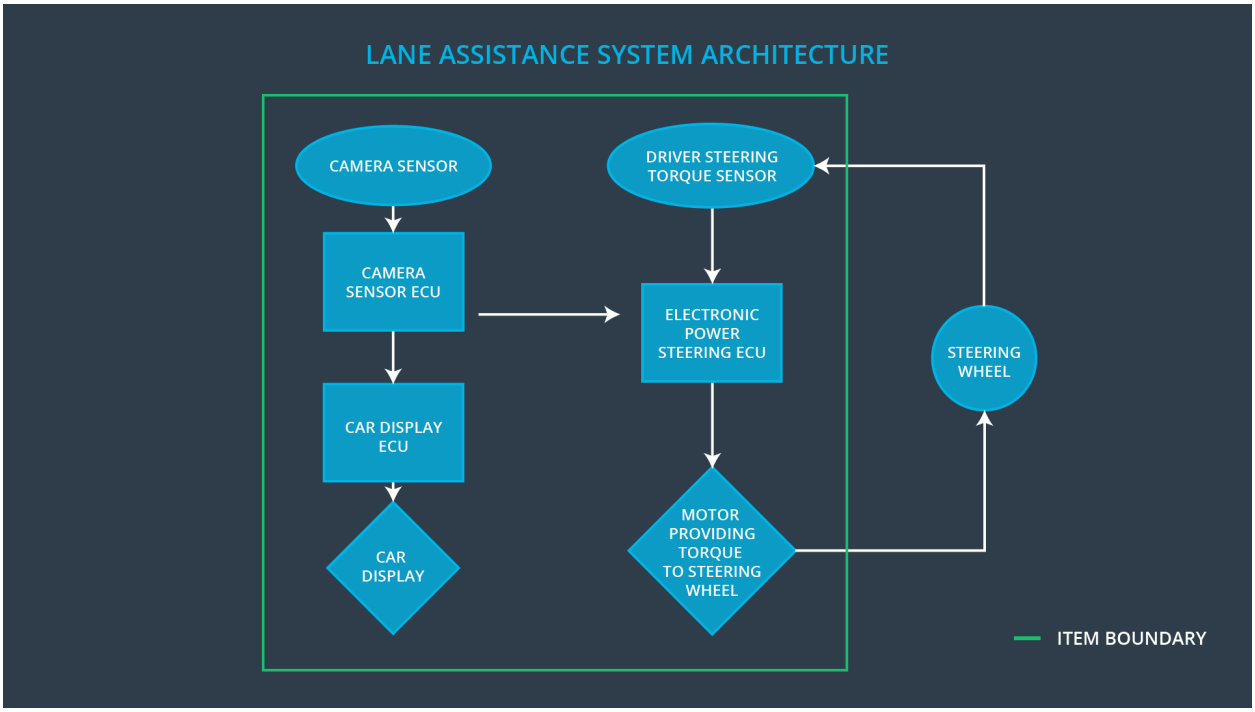

Figure 1: Lane Assistance System Architecture

Goals and Measures

Goals

The major goal of this project is to reduce the risk of the Lane Assistance System item to acceptable levels.

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

Our company safety culture has the following main characteristics:

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.

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

The purpose of this development interface agreement (DIA) is to define the roles and responsibilities between companies involved in developing the lane assistance system. In addition, the DIA 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 involved in this project are developing safe vehicles in compliance with ISO 26262.

The following table reflects the responsibilities of our company (Tier-1) versus the responsibilities of the OEM in this project.

Role	Responsible
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

A description of each role is provided.

Functional Safety Manager

Planning, coordinating and documenting of the development phase of the safety lifecycle
Tailors the safety lifecycle
Maintains the safety plan
Monitors progress against the safety plan
Performs pre-audits before the safety auditor

Functional Safety Engineer

Product development
Integration
Testing at the hardware, software and system levels

Project Manager

Overall project management
Acquires and allocates resources needed for the functional safety activities
Appoints safety manager or might act as safety manager

Safety Auditor

Ensures that the design and production implementation conform to the safety plan and ISO 26262.
Must be independent from the team developing the project

Safety Assessor

Independent judgement as to whether functional safety is being achieved via a functional safety assessment
Must be independent from the team developing the project

Confirmation Measures

The main purpose of confirmation measures is to assure that the functional safety project conforms to ISO 26262, its execution is following the safety plan, and the design of the lane assistance system does indeed improve the safety of the vehicle.
Some important definitions are:

- **Confirmation review**: Ensures that the project complies with ISO 26262. This work must be done by an independent person.
- **Functional safety audit:** Its goal is to make sure that the actual implementation of the project conforms to the safety plan.
- **Functional safety assessment:** Its objective is to confirm that plans, designs and developed lane assistance system actually achieve functional safety.