Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.0

Document history

Date	Version	Editor	Description
10.09.2017	1.0	Sergei Dmitriev	Initial version

Abbreviation List

N	Abbreviation	Definition
1.	DIA	Development Interface Agreement
2.	LDW	Lane Departure Warning
3.	LKA	Lane Keeping Assistance
4.	OEM	Original Equipment Manufacturer

Table of Contents

Introduction

Purpose of the Safety Plan

The Safety Plan defines roles, participating in functional safety processes, their responsibilities, scope and deliverables of the project, item under safety analysis. This plan also maintains the DIA and confirmation measures.

Scope of the Project

For the lane assistance project, the following safety lifecycle phases are in scope:

1. Concept phase
2. Product Development at the System Level
3. Product Development at the Software Level

The following phases are out of scope:

1. Product Development at the Hardware Level
2. 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

This functional safety project considers the Lane Assistance System, which includes the following sub-systems:

- Camera System
- Electronic Power Steering System
- Car Display System

The boundary of the item is shown in **Figure 1**.

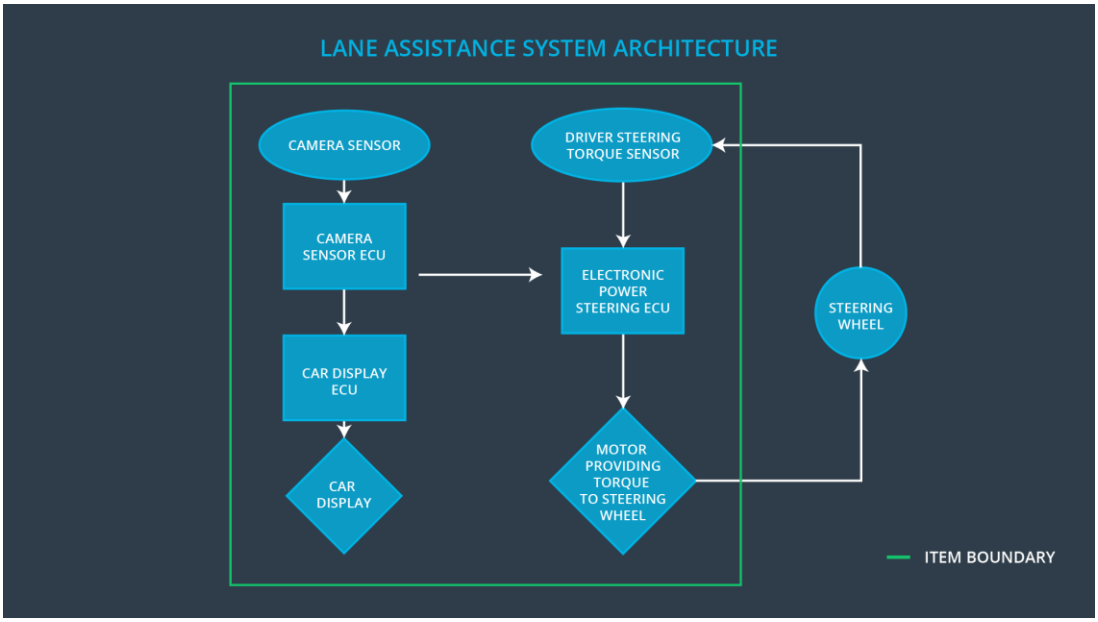

Figure 1

The Lane Assistance System has two functions:

- The LDW
- The LKA

These functions will be activated by a signal from the Camera System when a driver departs a lane without using a turn signal. In this case, the LDW function will vibrate the steering wheel and the LKA will turn the steering wheel back towards the lane center. The Camera System will also send a signal to the Car Display System to turn on a warning light.
If the driver uses a turn signal, then the lane assistance system deactivates so that the vehicle can leave the lane. The driver can also turn off the system completely with a button on the dashboard.

Goals and Measures

Goals

The goal of this project is to identify, evaluate and reduce unreasonable risks of using functionality of the lane assistance system.

Measures

Measures and Activities	Responsibility	Timeline
Follow safety processes	Safety auditor	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

The safety culture in the company provided by the following elements:

- High priority of the safety among things like cost and productivity
- Accountability of people who are involved in safety process
- Independence of team which is responsible for safety analysis
- Well defined processes of safety analysis

Safety Lifecycle Tailoring

The following parts of V model are included in this project:

- 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 the DIA is to specify the roles and responsibilities among companies involved in the Lane Assistance System project.

N	Organization	Responsibilities
1.	OEM	• Manage the whole functional safety project • Plan, coordinate, develop the Lane Assistance System on item level • Provide information support to Tier 1 organization
2.	Tier 1	• Plan, coordinate, develop the Lane Assistance System on sub-system (component) level • Provide all contractual deliverables to OEM organization • Fix software safety issues on sub-system (component) level

Confirmation Measures

The main purposes of the Confirmation Measures are the following:

- The functional safety project conforms to ISO 26262
- The functional safety project improves safety of a vehicle

Meeting the first purpose is checked during a Confirmation review, which makes sure the project followed ISO 26262. For checking of the second purpose achievement, Functional safety assessment procedure is used for confirmation that all functional safety goals are achieved.
In addition, Functional safety audit is also a part of the Confirmation measures, which makes sure that the actual implementation of the project conforms to the safety plan.