Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.1

Document history

Date	Version	Editor	Description
21/06/2017	1.0	Udacity, EB	Initial version
13/04/2019	1.1	Ahmed Belal	Finalize the document

Table of Contents

Introduction

Purpose of the Safety Plan

This document gives an introduction about the lane assistence system, defines the resources needed to finish the project safety activities, and the role of the different entities, their exact deliveries. Finally, it defines the procedures needed to make sure that the system follows the ISO 26262 standards and that it does increase the safety of the implemented system.

The 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

Overview

The lane assistant system is a driver assistence system that helps the driver to keep the vehicle in the lane on highways or highways-like roads.

Main Functions

lane assistant system has two main functions:

- Lane keeping assistence function
- Lane departure warning function

If the driver unintentionally approches the lane boundries without turning turn signal on.
The system will assume that the driver has become distracted and did not mean to leave the lane.
Lane keeping assistence function: will apply opposite torque on the steering wheel to return the car back towards the lane center, the driver can override this torque.
Lane departure warning function: will provide visual warning on the instrument panel cluster (IPC), vibration on the steering wheel

Sub systems

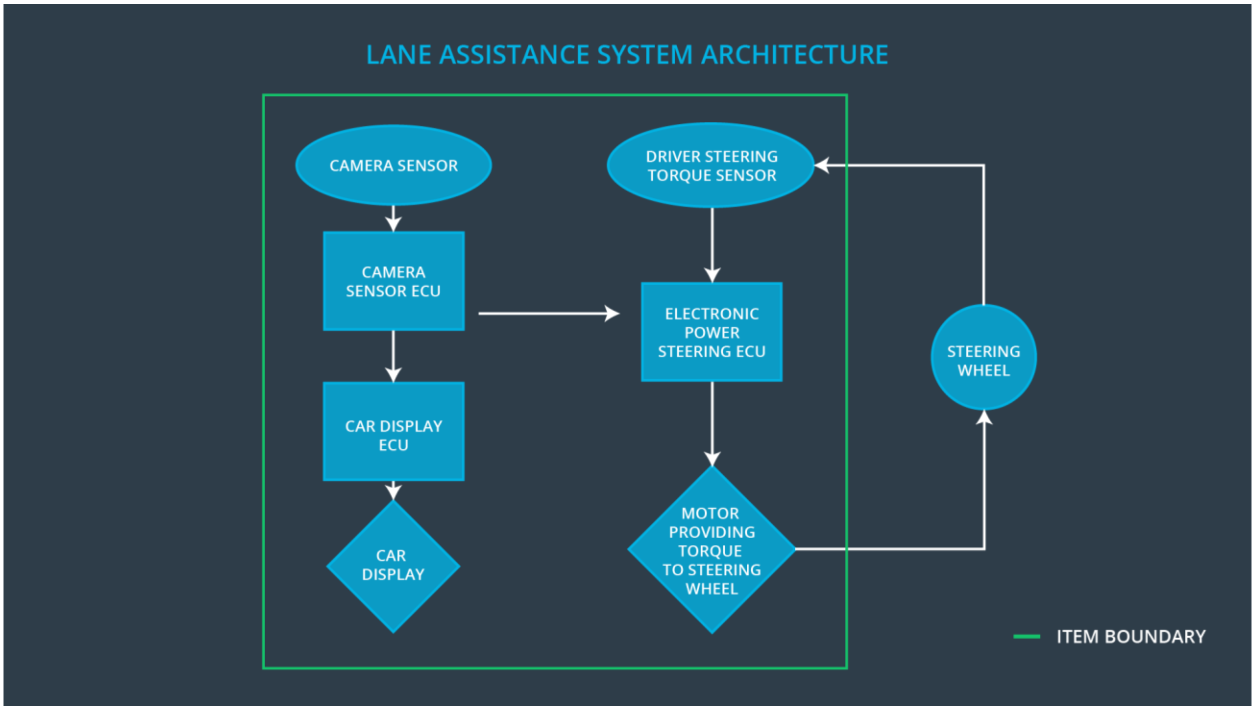
Lane assistence uses the following sub systems:

- **Forward Looking Camera (FLC)**: to identify the lane line and track lane and road boundries
- **Electronic Power Steering (EPS):** to apply opposite steering torque that helps on returning the vehicle to the center of road
- **Steering Wheel Vibration (SWV):** to apply vibration to the steering wheel
- **Instrument Panel Cluster (IPS):** to display warning messages to driver

Operational and environmental constrains

- Forward looking camera is working correctly, lane lines marking are visible
- Lane width: vehicle width + 1m to 4.6m
- Lane curvature: > 130m
- Speed range: 40mph to 120mph

Data Flow Diagram (DFD)


LANE ASSISTANCE SYSTEM ARCHITECTURE
CAMERA SENSOR
DRIVER STEERING TORQUE SENSOR
CAMERA SENSOR ECU
ELECTRONIC POWER STEERING ECU
STEERING WHEEL
CAR DISPLAY ECU
CAR DISPLAY
MOTOR PROVIDING TORQUE TO STEERING WHEEL
ITEM BOUNDARY

Goals and Measures

Goals

Make sure that the lane keeping assistance feature is implemented safely, will not lead to injury or harm to humans and provide a safety case that has evidence that the implemented E/E system is safe to be used.
The possible risks have to be identified, and actions have to be taken in the implemented system to lower the risk to reasonable 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

The organization should motivate the achievements of functional safety.
The organization penalizes the act of not following the safety guidelines.
The rules of each team member are defined accurately.
All the decisions are well documented, and they can be traced back to their makers, and their editors by dates.
Audits for low-risk components are done by other team members other than the implementation team. An external audit does audits for high-risk components.
DIA defines the interactions with external companies and accurately identifies the rules of each one of the parties.

Safety Lifecycle Tailoring

The following sections will be involved from the V model of ISO 26262:

- Concept phase
- Product Development at the System Level
- Product Development at the Software Level

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

DIA is the full agreement between all the organizations involved in the safety activities in the project, and it contains the following sections:

- Record of the appointment of customer and supplier safety managers.
- Joint tailoring of the safety life cycle.
- Activities and processes to be performed by the supplier.
- Information and work products to be exchanged.
- Parties or persons responsible for each activity in the design and the production phases.
- Any supporting processes or tools to ensure compatibility between customer and supplier technologies.

Responsibilities of the OEM:

- Identify the system description, and the High-Level Requirements (HLRs)
- Identify the definitions for the items involved in the project
- Define the safety activities that need to be involved in the system
- Do audits or hire a third party to do the audit during and after the implementation of the system
-

Responsibilities of EB as a tier-1 supplier:

- Identify the hazards that may occur in the system
- Define the Low-Level Requirements of the system
- Design the system on the component level
- Develop the system on both the system and software level
- Integration between the sub-components of the developed systems
- Make sure that all the activities follow the ISO 26262 standard

Confirmation Measures

The main purpose of confirmation measures is to ensure that the people who developed the product and who reviewed it are independent parties and it checks the following:

- Make sure that processes comply with the functional safety standard
- Make sure that the project execution is following the safety plan
- Make sure that the design improves the safety

Confirmation review: ensures that the project complies with ISO 26262. As the product is designed and developed, an independent person would review the work to make sure ISO 26262 is being followed.

Functional safety audits: Checking to make sure that the actual implementation of the project conforms to the safety plan is called a functional safety audit.

Functional safety assessment: Confirming that plans, designs and developed products actually achieve functional safety

---

A safety plan could have other sections that we are not including here. For example, a safety plan would probably contain a complete project schedule.

There might also be a "Supporting Process Management" section that would cover "Part 8: Supporting Processes" of the ISO 26262 functional safety standard. This would include descriptions of how the company handles requirements management, change management, configuration management, documentation management, and software tool usage and confidence.

Similarly, a confirmation measures section would go into more detail about how each confirmation will be carried out.