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
2018-03-18	1.0	Felipe A. L. Reis	First submission.

Table of Contents

Introduction

Purpose of the Safety Plan

This safety plan provides an overall framework for the Lane Assistant System' functional safety project. This document follow instructions of ISO 26262 standard.

ISO 26262, titled "Road vehicles - Functional safety" is a standard for functional safety for electronic and electrical systems in production of automobiles [1].

In addition, this document contains safe procedures to follow under software and hardware development, deployment and delivery, from functional system perspective.

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

This project defines a Lane Assistance System, responsible to automatically keep the car inside the lane if it moving out the lane. This assistant helps the driver to keep the vehicle centered inside a lane.

Lane Assistance System is part of a group of functionalities defined as ADAS (Advanced Driver Assistance System), which has the objective to help the driver to keep safety, with basically two major functions:

- Alert the driver in dangerous situations;
- Take control of the vehicle to prevent accidents [2].

Lane Assistance System Functionality

This functionality has two functions:

- *Lane departure warning function* → responsible to vibrate the steering wheel to alert the driver of a warning. In formal description, this functionality “shall apply an oscillating steering torque to provide the driver a haptic feedback”;
- *Lane keeping assistance function* → responsible to automatically move the wheel to keep the car centered in the lane. In formal description, this functionality “shall apply the steering torque when active in order to stay in ego lane”.

The functionality works with a camera sensor that identifies if the vehicle is leaving the lane and sends a signal to the electronic power steering wheel to vibrate and adjust the vehicle direction, keeping the car inside the lane. If the driver wants to change lane, is expected to turn on the turn signal (that deactivates the system) or to manually deactivate the system with a button on the dashboard.

Item Architecture

The Lane Assistance System Architecture is defined in Image 1. As shown in Image 1, the Item boundary contains three subsystems:

- Camera system *(Camera Sensor ECU);*
- Car Display System *(Car Display ECU);*
- Electronic Power Steering System *(Electronic Power Steering ECU).*

Outside Item boundary is some system like wheel, throttle and other components of the vehicle.

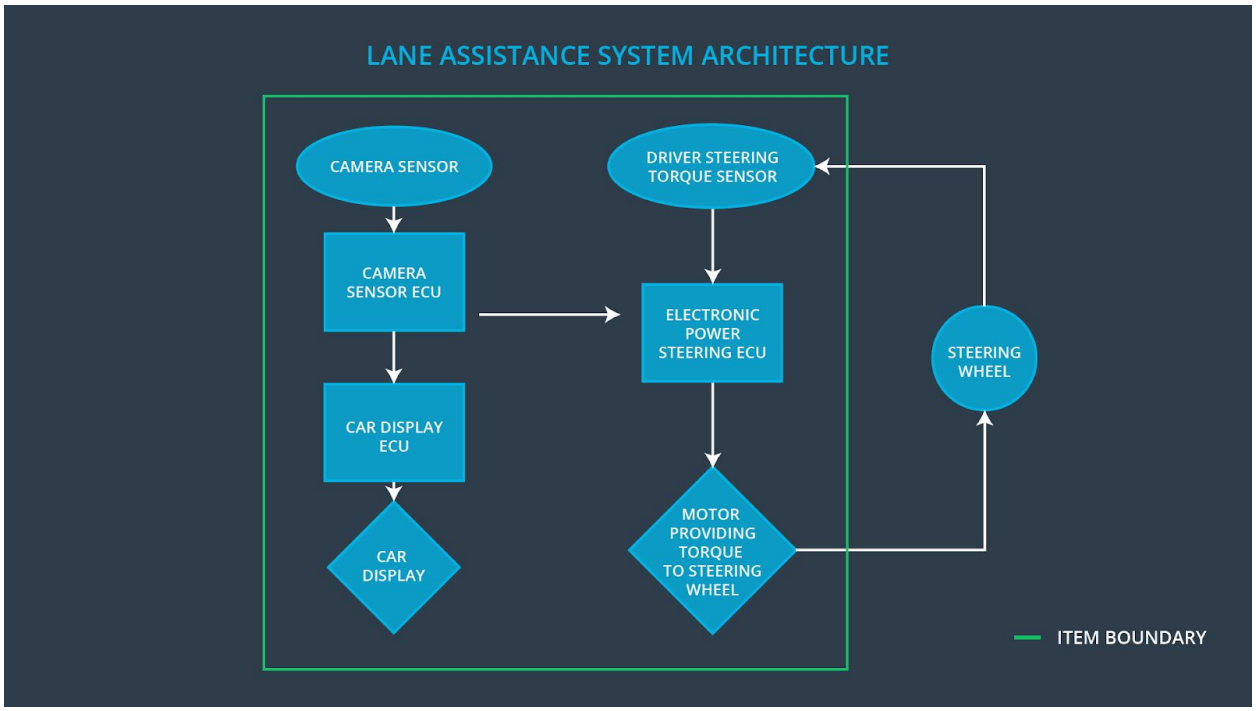

Image 1. Lane Assistance System Architecture - Item Level

Camera Subsystem

Camera subsystem is responsible to identify if the vehicle is leaving the lane. This subsystem also communicates with Electronic Power Steering subsystem to correct the car moviment and to the Car Display subsystem to provide a feedback to the driver.

Electronic Power Steering Subsystem

Electronic Power Steering subsystem is responsible to apply an extra torque to keep the car centered in the lane. After receive an alert of Camera subsystem, this subsystem also identifies the torque applied by the driver on the steering wheel and add an extra torque to correct the trajectory. The torque is applied to the steering wheel using a motor. As an extra

Car Display Subsystem

After receive a signal from the Camera Subsystem, this subsystem turn on a light in the car dashboard to indicate that the system is already on.

Goals and Measures

Goals

The goal of this document is provide a hazard analysis and risk assessment to predict and identify possible problems that can cause accidents and lead to an injury. The major objective is to reduce the risk to acceptable levels, tolerated by society. The risks are analysed following ISO 26262 directives, using a serie of concepts that can help to reduce possible problems.

Analyzing the Lane Assistance System with ISO 26262, it is expected to identify possible risks, make an analysis of that and apply methods to decrease them to the lower value possible.

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

Here are some characteristics that help our company to create a good safety culture:

- *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 [3].

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

This section contains the roles for functional safety and it correspondent organizations.

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 [4]

Confirmation Measures

The two main purposes of confirmation measures are:

1. that a functional safety project conforms to ISO 26262, and
2. that the project really does make the vehicle safer [5].

Confirmation measures contains some of definitions, that helps to understand the concept. The concepts are defined below.

- 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 audit → 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 is called a functional safety assessment [5].

References

1. ISO 26262. **Wikipedia**. Available in https://en.wikipedia.org/wiki/ISO_26262. Accessed in 2018-03-18.
2. Functional Safety - ADAS - Advanced Driver Assistance System. **Udacity**. Available in https://classroom.udacity.com/nanodegrees/nd013/parts/6047fe34-d93c-4f50-8336-b70ef10cb4b2/modules/6dc3d743-2b0f-4ae6-97b7-e2ff866f17ef/lessons/1117330b-7b93-4621-8ef0-882d6ad15983/concepts/6a2ef718-3cd8-466d-83e2-0b25f04a5d66 Accessed in 2018-03-18.
3. Functional Safety - Safety Culture. **Udacity**. Available in https://classroom.udacity.com/nanodegrees/nd013/parts/6047fe34-d93c-4f50-8336-b70ef10cb4b2/modules/6dc3d743-2b0f-4ae6-97b7-e2ff866f17ef/lessons/46dcd53a-2a28-4a58-8df0-09b22e5ccdfe/concepts/8524bbfb-1539-4883-bc91-c0510c9e2fbb. Accessed in 2018-03-18.
4. Functional Safety - Development Interface Agreement. **Udacity**. Available in https://classroom.udacity.com/nanodegrees/nd013/parts/6047fe34-d93c-4f50-8336-b70ef10cb4b2/modules/6dc3d743-2b0f-4ae6-97b7-e2ff866f17ef/lessons/46dcd53a-2a28-4a58-8df0-09b22e5ccdfe/concepts/ab68ef33-0cd5-4a70-966f-85bf6179a45a. Accessed in 2018-03-22.
5. Functional Safety - Confirmation Measures. **Udacity**. Available in https://classroom.udacity.com/nanodegrees/nd013/parts/6047fe34-d93c-4f50-8336-b70ef10cb4b2/modules/6dc3d743-2b0f-4ae6-97b7-e2ff866f17ef/lessons/46dcd53a-2a28-4a58-8df0-09b22e5ccdfe/concepts/5b84bcda-50a1-45e0-99ff-f78647d4c626. Accessed in 2018-03-22.