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
01/08/2018	1.0	Anil Kumar	First version

Table of Contents

Introduction

Purpose of the Safety Plan

Safety plan provides details of how functional safety ensured during development and production of the Product

It also defines clear roles and responsibilities between different parties involved.

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

Lane Assistance System: System Provide assistance to the driver to keep the vehicle in lane to improve the safe highway driving.

This system has two functions:

1. **Lane departure Warning:** If a driver departs a lane without using a turn signal, the system assumes that the driver has become distracted and did not mean to leave the lane. The system will vibrate the steering
2. **Lane Keep Assist:** If a driver departs a lane without using a turn signal, the system assumes that the driver has become distracted and did not mean to leave the lane. The move the steering wheel back towards the lane center

Sub Systems:

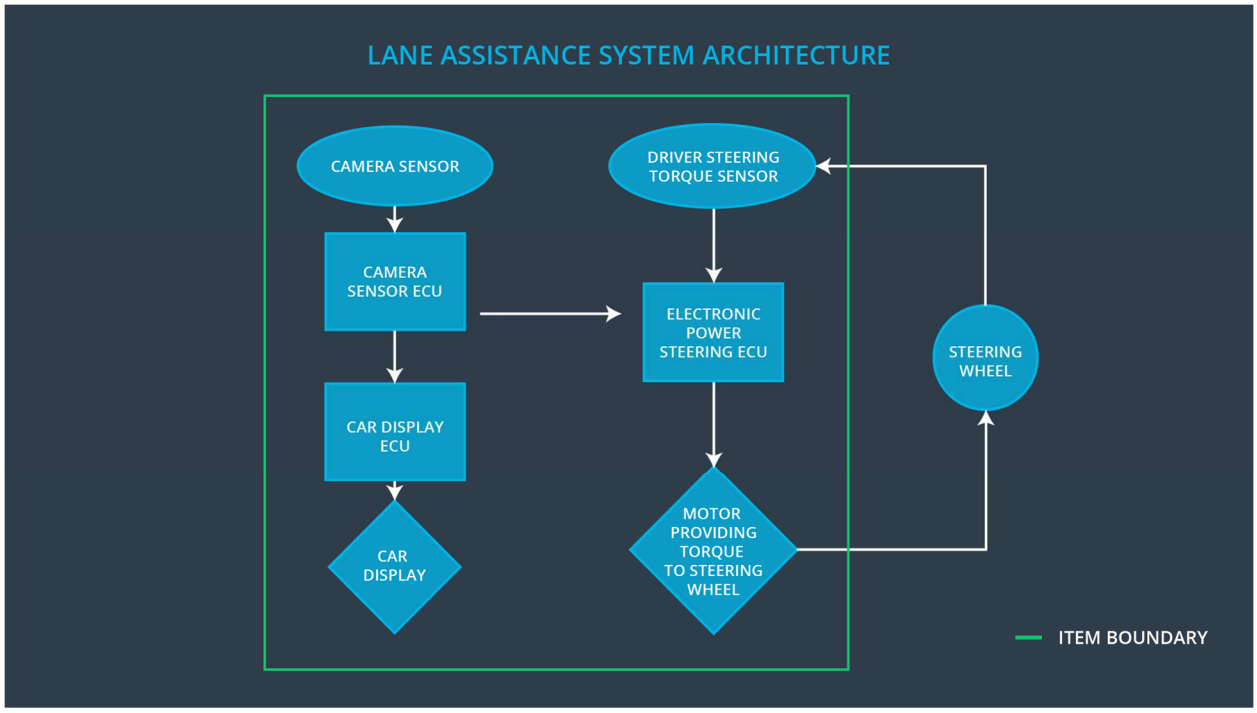
1. Camera Sensor ECU: Capture the Lane markings video frames through camera sensor and its responsibilities are:
    - Finds the Lane line in the video frames and track these Lane lines
    - Listens to the CAN BUS to keep track the status of Turn signal from Body control module
    - Send command to the Electronic Power Steering ECU in case of unsafe lane change detected to inform the driver by vibrating the steering wheel and to bringing back the vehicle towards lane center
    - Send command to Car Display ECU to display warning in the car dashboard

2. Electronic Power Steering ECU: Responsible for controlling the Steering wheel through motor providing torque to steering wheel and it responsible for vibrating steering wheel in case Lane departure warning received from Camera Sensor ECU and adds extra steering torque to the driver move back the vehicle towards lane center

3. Car Display ECU: Displays information and warning on the dashboard. In this system it displays car position with respect to the center of the lane and it displays warning to alert the driver in case of unintended lane departure detected

4. Steering wheel : Subsystem provides the yaw rate to the wheels based on its steering angle for that it listens to the Electronic Power Steering ECU

Below diagram describes architecture of the system the item boundary (green line) separates subsystems inside and outside of the item



Goals and Measures

Goals

1. Find the possible hazards
2. Analyze the risks and define the safety goals
3. Find the solution to minimize the risk to acceptable level

Measures

Measures and Activities	Responsibility	Timeline
Follow safety processes	All Team Members	Constantly
Create and sustain a safety culture	Safety Manager	Constantly
Coordinate and document the planned safety activities	Safety Manager	Constantly
Allocate resources with adequate	Project Manager	Within 2 weeks of start of project

functional safety competency		
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 of 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

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

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.

OEM responsible for:

- Providing functional safety goals or functional safety requirements to the Tier 1 supplier
- Define process and tools to be used

- Perform Safety Audits and assessment

Tier-1 supplier responsible for:

- Modifying the subsystems design, which required safety features to support safety requirements
- Develop/modify the subsystems according to the design to ensure risks are minimized to acceptable level
- Validate and test against safety requirement

Confirmation Measures

Confirmation measures serve two purposes:

- that a functional safety project conforms to ISO 26262, and
- That the project really does make the vehicle safer.

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.
.