Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
22/05/2018	1.0	Sanchit Agrawal	First Submission

Table of Contents

Introduction

Purpose of the Safety Plan

The document provides overall role and responsibilities of the Lane Assistance item’s functional safety and its framework.

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 item identified in this project is a Lane assistance system.
Two main functions are:

1. **Lane Departure Warning Function:**

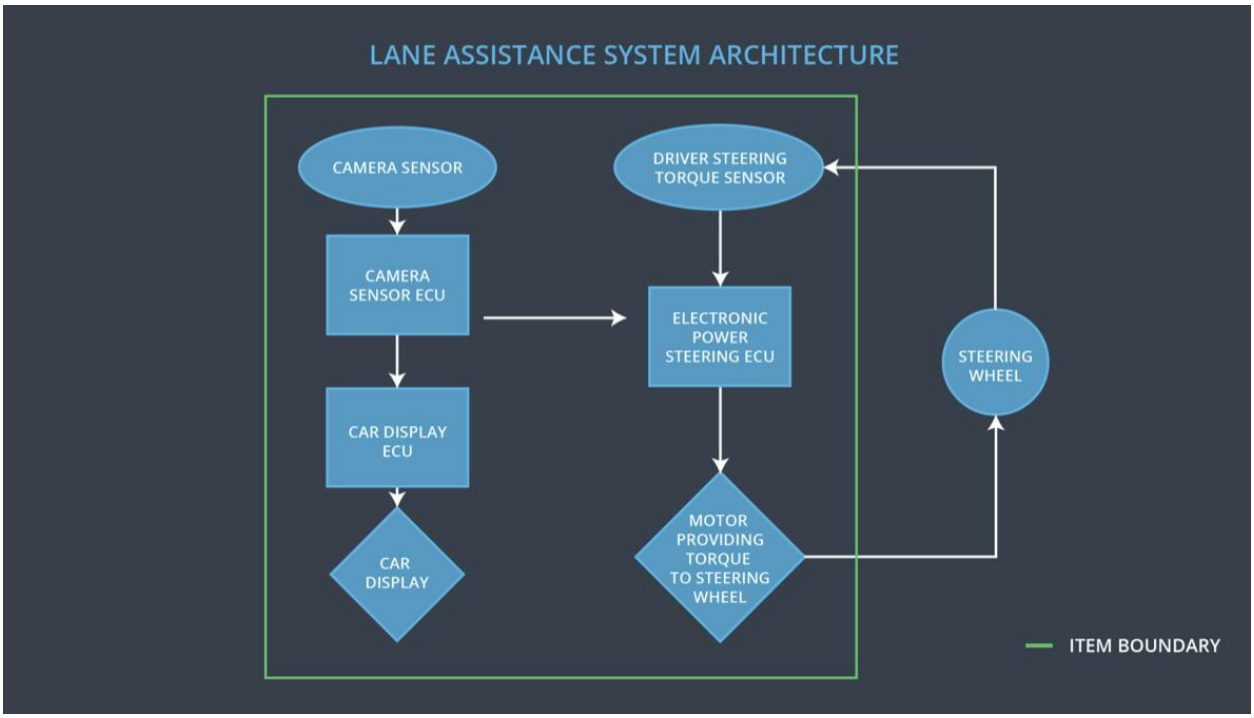
It is a function which vibrates the steering wheel if car move towards the edge of the lane.

2. **Lane keeping assistance function:**

It is responsible for keeping the car towards the center of the lane.
The responsible subsystem are:

- **Camera subsystem**: This has two components:
  - Camera sensor
  - Camera sensor ECU (Electronic Control Unit)
- **Electronic Power Steering subsystem**: This has three components:
  - Driver Steering Torque Sensor.
  - Electronic Power Steering ECU.
  - Motor Proving Torque to Steering Wheel.
- **Car Display subsystem**: This has two components:
  - Car Display ECU
  - Car Display

The below diagram describe the flow between different subsystems:



Goals and Measures

Goals

This project goals are:

- Identify risk and hazard situations in the system that could cause injuries to the person.
- Evaluate the risks of the hazardous situations.
- Identify the minimal cost for the risk that is acceptable by the society.

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	All Team Members	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 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.

Roles and responsibilities are:

- **Functional Safety Manager - Item Level**: Pre-audits, plans the development phase for the Lane Assistance item.
- **Functional Safety Engineer - Item Level**: Develop prototypes, integrate subsystems combining them into the Lane Assistance item.
- **Project Manager - Item Level**: Allocates the resources needed for the item.
- **Functional Safety Manager - Component Level(Sanchit Agrawal)**: Pre-audits, plan the development for the components of the Lane Assistance item.
- **Functional Safety Engineer - Component Level(Sanchit Agrawal)**: Develop prototypes and integrate components conforming the Lane Assistance item.
- **Functional Safety Auditor**: Make sure the project conforms to the safety plan.
- **Functional Safety Assessor**: Judges where the project has increased safety.

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 Measures Definitions

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.

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.