Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
18-06-2018	1.0	Vikas Bijalwan	Document for safety plan

Table of Contents

Introduction

Purpose of the Safety Plan

A safety plan provides an overall framework for a functional safety project. In this document it serves as a functional safety plan for Lane Assistance System. It also includes the assignment of roles and responsibilities for the item's functional safety.

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 we are considering here is a simplified version of Lane Assistance System.

The main functions of the item are:

Lane departure warning
Lane keeping assistance

The item considers 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 (lane departure warning) and also move the steering wheel back towards the lane center (lane keeping assistance).

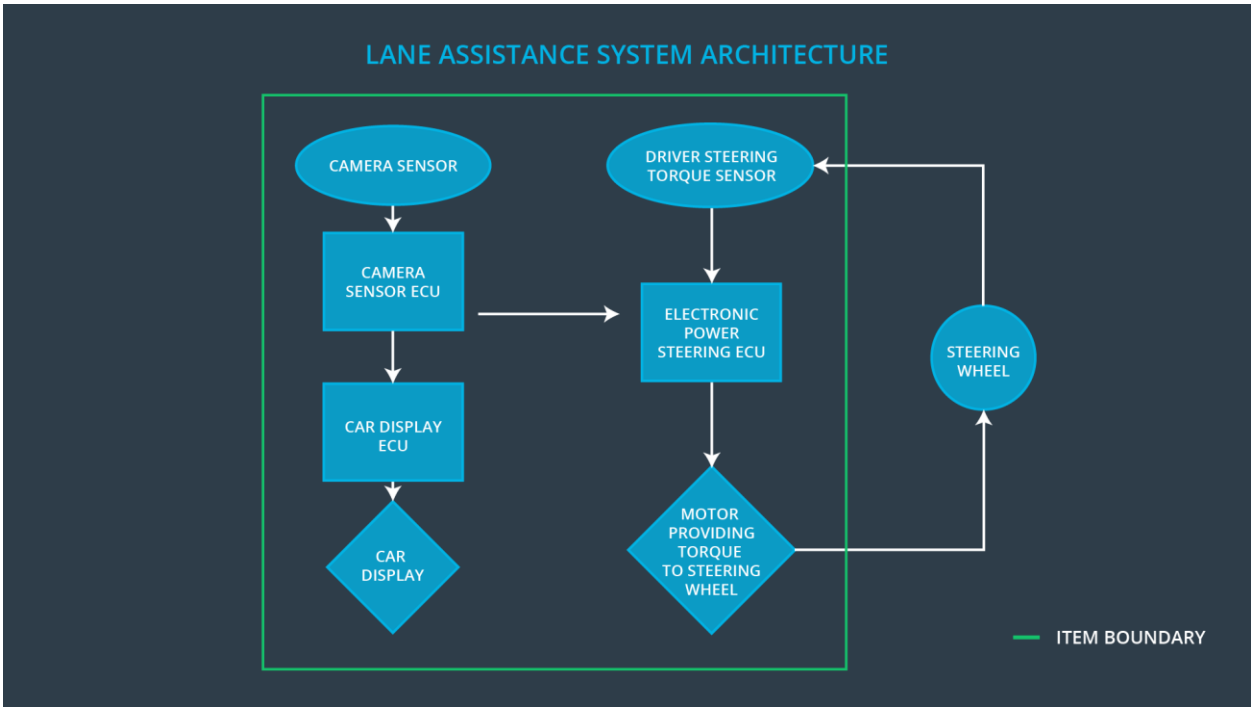
The item functionalities are implemented by the following subsystem:

- A Camera subsystem is composed by two components:
  - Camera sensor
  - Camera sensor ECU (Electronic Control Unit)

- An Electronic Power Steering subsystem is composed by three components:
  - Driver Steering Torque Sensor.
  - Electronic Power Steering ECU.
  - Motor Proving Torque to Steering Wheel.

- A Car Display subsystem is composed by two components:
  - Car Display ECU
  - Car Display

Below is the architectural diagram showing the interaction between different subsystems in a Lane Assistance System:



The drift from the lane's center is detected by the car's camera sensor subsystem. The ECU (electronic control unit) subsystem takes input form the camera sensor subsystem and the driver steering torque subsystem and feeds the output to the motor providing torque to the steering wheel along with the car display subsystem providing the visual feedback for the driver. All these subsystems are part of the item except the steering wheel and thus is not considered as a part of this project.

The Line Assistance System does not include the following functionalities:

- Adaptive Cruise Control
- Automatic Parking
- Blind Spot Monitoring
- Tire Pressure Monitoring
- Pedestrian Protection

Goals and Measures

Goals

The major goal of the project is to assure safe and reliable operation of the E/E/PS components of the vehicle's lane assistance function, according to ISO 26262.
To achieve functional safety, we:

- Identify risk and hazardous situations in the Line Assistance system components malfunction causing injuries to a person.
- Evaluate the risks of the hazardous situations.
- Low the risk of malfunctions to a reasonable levels acceptable by current 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	Safety Manager	3 months prior to main assessment

external functional safety assessor		
Perform functional safety assessment	Safety Manager	Conclusion of functional safety activities

Safety Culture

Although cost and productivity are important for successful system but safety should be given priority. In order to ensure a safety culture, the following characteristics needs to be observed:

- 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

This section defines the roles and responsibilities between parties involved in the Lane Assistance project to ensure its development in compliance with ISO 26262.

- **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 from a functional safety viewpoint**.**
- **Project Manager - Item Level**: Allocates the resources needed for the item.
- **Functional Safety Manager - Component Level (Darien Martinez)**: Pre-audits, plan the development for the components of the Lane Assistance item.

- **Functional Safety Engineer - Component Level (Darien Martinez)**: 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

The purpose of the confirmation measures is:

- Ensure that the project conforms to ISO 26262 and
- Ensure that the project really does make the vehicle safer.

The Confirmation review ensure the projects comply 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.
A Functional safety audit make sure the actual implementation of the project conforms to the safety plan.

A Functional safety assessment confirms that the plan, design and developed product 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.