Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 2.0

Document history

Date	Version	Editor	Description
12/3/17	1.0	Vatche Donikian	Initial attempt at Safety Plan
12/18/17	2.0	Vatche Donikian	Second submission

Table of Contents

[Instructions: We have provided a table of contents. If the table of contents is not showing up correctly in your word processor of choice, please update it. The table of contents should show each section of the document and page numbers or links. Most word processors can do this for you. In Google Docs, you can use headings for each section and then go to Insert > Table of Contents. Microsoft Word has similar capabilities]

Introduction

Purpose of the Safety Plan

The purpose of this safety plan is to ensure that the Lane Assistance system functions at the safest level possible and to ensure that if a malfunction occurs, the consequences are minimized.

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

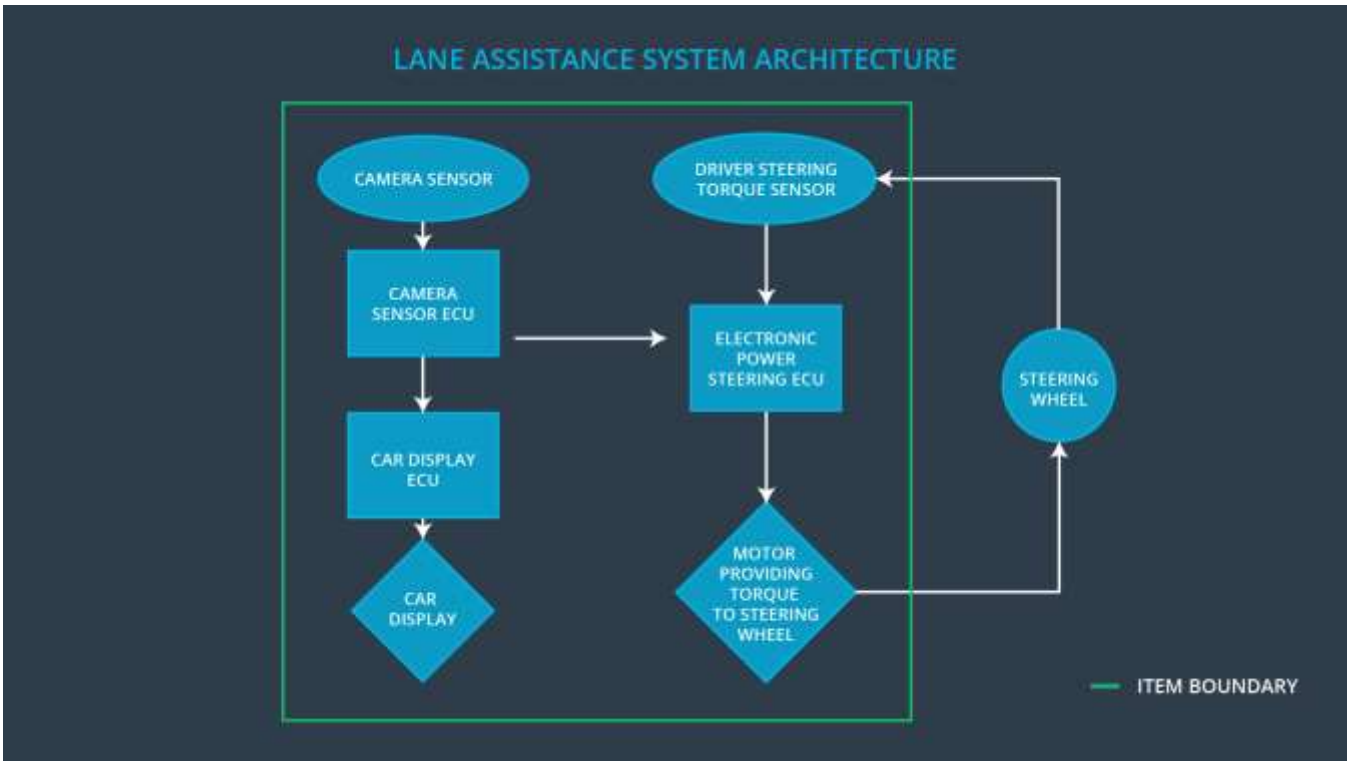
Deliverables of the Project

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 of concern is the Lane Assistance, which helps notify the driver and correct steering for instances when the vehicle is leaving the current lane without using a turn signal. The two main functions are the Lane Departure Warning (LDW) and the Lane-Keep Assistance (LKA). LDW warns the driver if the vehicle is leaving the lane without the turn signal by vibrating the steering wheel and flashing a light on the dash. If the steering is not corrected, the LKA function provides torque to the steering wheel to correct the vehicle back into the lane. The subsystems used are the Camera subsystem, the Display subsystem, and the Electronic Power Steering (EPS) subsystem. The boundary of the item includes the camera sensor and ECU, the car display and ECU, the driver steering torque sensor, EPS ECU, and the motor that provides torque to the steering wheel. The physical steering wheel itself is outside the boundary of the item. The diagram below shows the system architecture.



Goals and Measures

Goals

The goal of this functional safety analysis is to study the Lane Assistance item under the scope of ISO 26262 to make sure that hazardous risks associated with the item are specified, categorized, and minimized.

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 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 safety culture at the company is strong. First off, safety is priority above everything and anything else. This means that even if there is a higher cost, it is necessary to get more testing done to make sure the product is as safe as possible. Just as this safety plan, everything is well documented in order to trace back where a safety issue was first introduced in the V model process of an electrical system. Also, shortcuts are penalized, and abiding by the safety measures result in rewards for the employees. These characteristics make sure that the most careful attention is given to the safety requirements of systems in order to minimize malfunctions, injuries, and hazards.

Safety Lifecycle Tailoring

The lane assistance system already exists, so not all phases are in scope for this assessment. The concept phase and the product development at both the system level and software level all are in scope. The product development at the hardware level and the production and operation of the item are out of scope.

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

The purpose of a development interface agreement is to avoid disputes between OEM, Tier 1, and Tier 2 companies that all work on different components of an item. The DIA specifies what each company is responsible for providing and ensures that all companies must abide by ISO 26262.

The OEM company is responsible for testing the functional safety of the lane assistance system at the item level, and then providing my company with a working lane assistance system. My company is responsible for looking at each of the components that make up the item, analyzing the risks associated with each component, and making modifications to the subsystems in ways that make the safety of the system higher. As safety manager and engineer, I will be responsible for integrating the subsystems into the larger item, and pre-auditing the system before it is sent back to the OEM supplier for auditing and assessment.

Confirmation Measures

The main purposes of confirmation measures are to ensure that the functional safety project follows the ISO 26262 guidelines and that the design does indeed make the vehicle safer. The confirmation review makes sure that the project complies with ISO 26262. The functional safety audit is where the project is checked to make sure that the implementation follows the safety plan. The functional safety assessment is where the plans, designs, and developed products are tested to confirm that they 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.