Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
19-12-2018	1.0	Usman Ijaz Malik	Initial Safety Plan

Table of Contents

Introduction

Purpose of the Safety Plan

Safety plan forces us to define roles and to outline the steps needed to achieve 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 lane assistance item alerts the driver that vehicle has accidently departed the lane and attempts to steer the car back towards the center of the lane.

Lane assistance system will have two main functions:

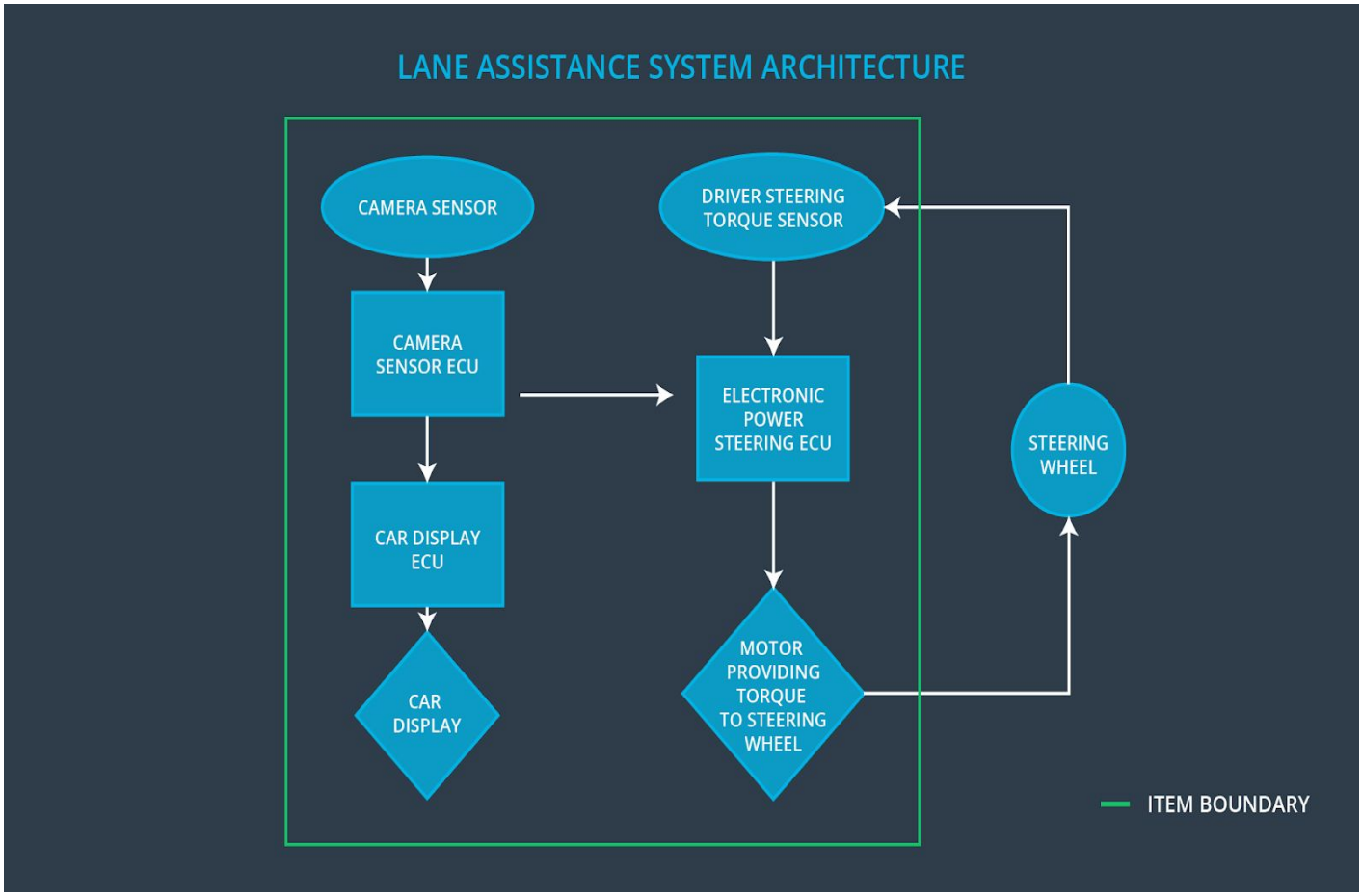
- **Lane Departure Warning**
- **Lane Keeping Assistance**

Following subsystems are responsible for each function.

- **The lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback.**
- **The lane keeping assistance function shall apply the steering torque when active in order to stay in ego lane.**

What are the boundaries of the item? What subsystems are inside the item? What elements or subsystems are outside of the item?
Item has three subsystems in it responsible for all the functions:

- **Camera Sub System**
- **Electronic Power Steering Subsystem**
- **Car Display Subsystem**



Goals and Measures

Goals

We want to develop a safe product. The goal of this project is to make a plan to achieve functional safety of lane assistance system. Also, we need to define roles and responsibilities of these roles, involved in the project. Throughout the project, we would:

- **Identify hazards in the lane assistance system**
- **Evaluate the risks from the hazardous situations**
- **Reduce the risks to acceptable level via system engineering**

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

First step for us was to clearly define the design and management processes of the company. Secondly, it is ensured that necessary resources are acquired. Communication channels have been created to make sure that problems are disclosed to all the relevant

team members. In our company, safety has the highest priority. Constraints like cost and productivity comes after the safety. We have designed a process to ensure accountability. This process ensures that design decisions are traceable back to the people and teams who made the decisions. Our company entails a reward system to motivate and support the achievement of functional safety. There is a process to penalize shortcuts that jeopardize safety or quality. Audit teams are kept independent of design and development team. We have a culture in which intellectual diversity is encouraged and celebrated.

Safety Lifecycle Tailoring

As our product is new, we will have to follow and document the entire safety lifecycle. However, as the scope of this project is already defined and limited, we will be focusing on three phases from the safety lifecycle. These include a concept phase, a product development phase at system level and a product development phase at software level. Product development at the hardware level and production and operation phases are not in the scope of this project as in this project, the OEM is supplying a functioning lane assistance system.

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

1. **What is the purpose of a development interface agreement?**

A development interface agreement is used to define the roles and responsibilities between companies involved in a product. All parties need to agree on the contents of

DIA before the project begins. Another purpose is to specify what evidence and work products each party will provide to prove that work was done according to the agreement. It is helpful to avoid disputes during the planning and development of a product. It also helps in holding the appropriate supplier responsible in case of a vehicle safety issue found after vehicles are sold to customers.

2. **What will be the responsibilities of your company versus the responsibilities of the OEM? Hint: In this project, the OEM is supplying a functioning lane assistance system. Your company needs to analyze and modify the various sub-systems from a functional safety viewpoint.**

]

The OEM is supplying a functioning lane assistance system. Our company needs to analyze and modify the various sub-systems from a functional safety viewpoint.

Confirmation Measures

1. **What is the main purpose of confirmation measures?**

The main purpose of confirmation measures is to check if the project really improves safety. Beside that, it also make sures that function safety project conforms to ISO 26262.

2. **What is a confirmation review?**

Confirmation review is done to ensure that project complies with ISO 26262. As the product is designed and developed, an independent person would review the work to make sure that ISO 26262 is being followed.

3. **What is a functional safety audit?**

Functional safety audit is done to ensure that that the actual implementation of the project conforms to the safety plan.

4. **What is a functional safety assessment?**

Functional safety assessment confirms that plans, designs and developed products 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.