Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
17-May-2018	1.0	Shreya Srivastava	First Draft

Table of Contents

1. Introduction

1.1 Purpose of the Safety Plan

The main purpose if the safety plan is to provide an overall framework for lane assistance. A safety plan is required so as to define roles and then outline the steps that we will take to achieve functional safety

1.2 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

1.3 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

2. Item Definition

1. **What is the item in question, and what does the item do?**

   The item in question here is the Lane Assistance System. The Lane Assistance System alerts the driver that the vehicle has gone off the road or is about to go off the road and tries to drive it back to the lane.

2. **What are its two main functions? How do they work?**

   There are two main functions of the Lane Assistance System are listed as under:

   - Lane departure warning
   - Lane keeping assistance

   The lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback

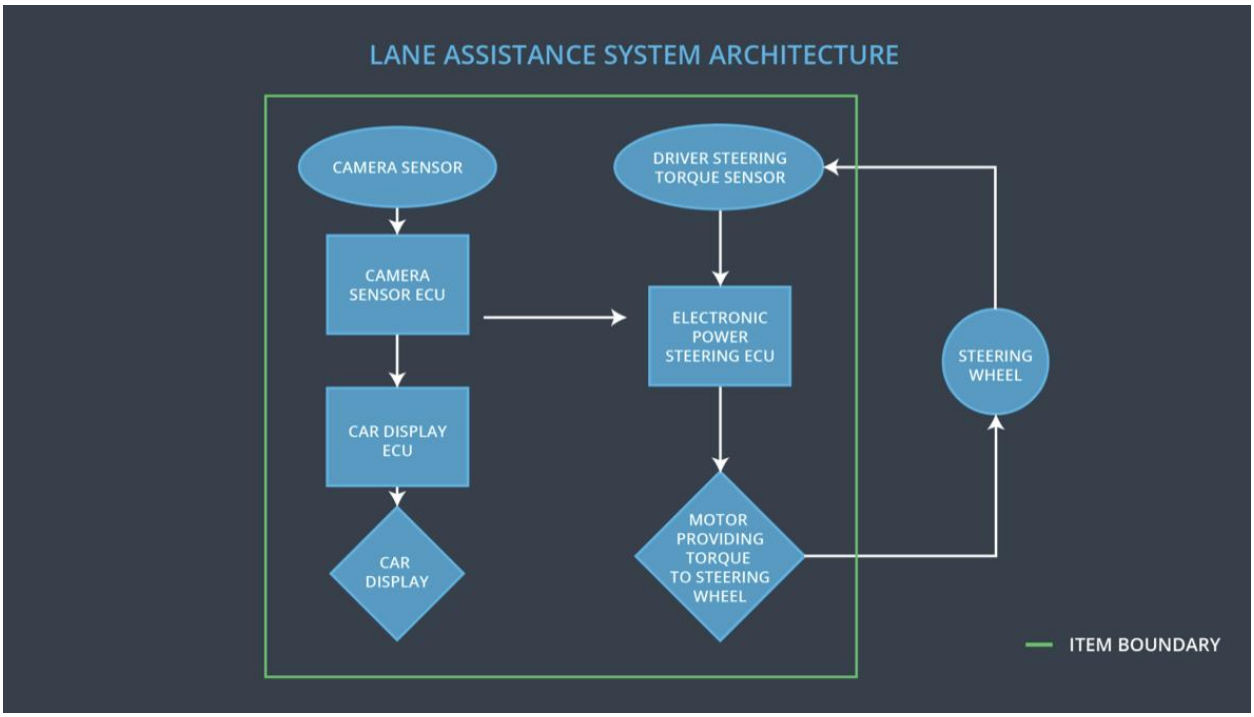
   the lane keeping assistance function shall apply the steering torque when active in order to stay in ego lane". Ego lane refers to the lane in which the vehicle currently drives.

3. **Which subsystems are responsible for each function?**

   The subsystems that are responsible for each of the functions are the camera subsystem, electronic power steering system and the car display system.

4. **What are the boundaries of the item? What subsystems are inside the item? What elements or subsystems are outside of the item?**

   The boundaries for item and the subsystems contained in the item can be aptly described by the image below. The image clearly marks the boundary of the item showing what is contained in the item and what is not contained in the item.


LANE ASSISTANCE SYSTEM ARCHITECTURE
CAMERA SENSOR
DRIVER STEERING TORQUE SENSOR
CAMERA SENSOR ECU
ELECTRONIC POWER STEERING ECU
STEERING WHEEL
CAR DISPLAY ECU
CAR DISPLAY
MOTOR PROVIDING TORQUE TO STEERING WHEEL
ITEM BOUNDARY

3. Goals and Measures

3.1 **Goals**

The main goal is to reduce the risk to the acceptable levels. By analyzing the lane assistance system, we are trying to accomplish the fact that the functions are working properly and would help us know the cause of the problem in the future, if there.

3.2 **Measures**

Measures and Activities	Responsibility	Timeline
Follow safety processes	Safety Engineer	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 Manger	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

4. Safety Culture

Some of the characteristics of a good safety culture are listed below:

- **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
- **Communication**: communication channels encourage disclosure of problems

These characteristics help in maintaining the safety culture by following the right practices for keeping the safety as the first priority and even rewarding the people adequately who follow the culture.

5. Safety Lifecycle Tailoring

The phases of the safety lifecycle that are in the scope of this project are as under:

- Item Definition
- Initiation of the safety lifecycle
- Hazard Analysis and Risk Assessment
- Functional Safety Concept
- Product Development Systems Level

The phases of the Safety Lifecycle that are out of the scope of this project are:

- Product Development Hardware Level
- Safety Validation
- Functional Safety Assessment
- Release and Production
- Production
- Operation, Service and Decommissioning

6. 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

7. Development Interface Agreement

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

   A DIA (development interface agreement) defines the roles and responsibilities between companies involved in developing a product. The purpose of the DIA is to avoid disputes during the planning and development of the product. Another reason for having a DIA is that, it makes it clear that which company is liable to fix the issue if an issue arises after the production

2. **What will be the responsibilities of your company versus the responsibilities of the OEM?**

   Responsibilities of the OEM:
   The OEM is responsible to provide a fully working lane assistance system to our company. It should be responsible for testing on all the fronts other than the electronic and electrical fronts.

   Responsibilities of our Company:
   Our company is responsible for testing the lane assistance system form the functional safety point of view. This mainly includes testing the system on the electrical and electronic front and see if it is in accordance with the ISO requirements.

8. Confirmation Measures

1. **What is the main purpose of confirmation measures?**
   The main purposes of the confirmation measures are:
   - The processes comply with the functional safety standard.
   - The project execution is following the safety plan.
   - The design really improves safety.

2. **What is a confirmation review?**
   As the product is designed and developed, an independent person would review the work to make sure ISO 26262 is being followed.

3. **What is a 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.

4. **What is a 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.