Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
6/24/18	1.0	Pascal Irminger	Safety Plan (init)

Table of Contents

Document history

Table of Contents

Introduction
- Purpose of the Safety Plan
- Scope of the Project
- Deliverables of the Project

Item Definition

Goals and Measures
- Goals
- Measures

Safety Culture

Safety Lifecycle Tailoring

Roles

Development Interface Agreement

Confirmation Measures

Introduction

Purpose of the Safety Plan

The safety plan gives an overview of how to achieve a safe Lane Assistant system. Among others, it includes the definition of roles and responsibilities for the system'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 investigated in this project is a simplified Lane Assistance System which is an Advanced Driver Assistance System (ADAS). The Lane Assistance System alerts the driver in potentially dangerous situations and takes control over the vehicle to prevent accidents from occurring.

The two main functions of this system are:

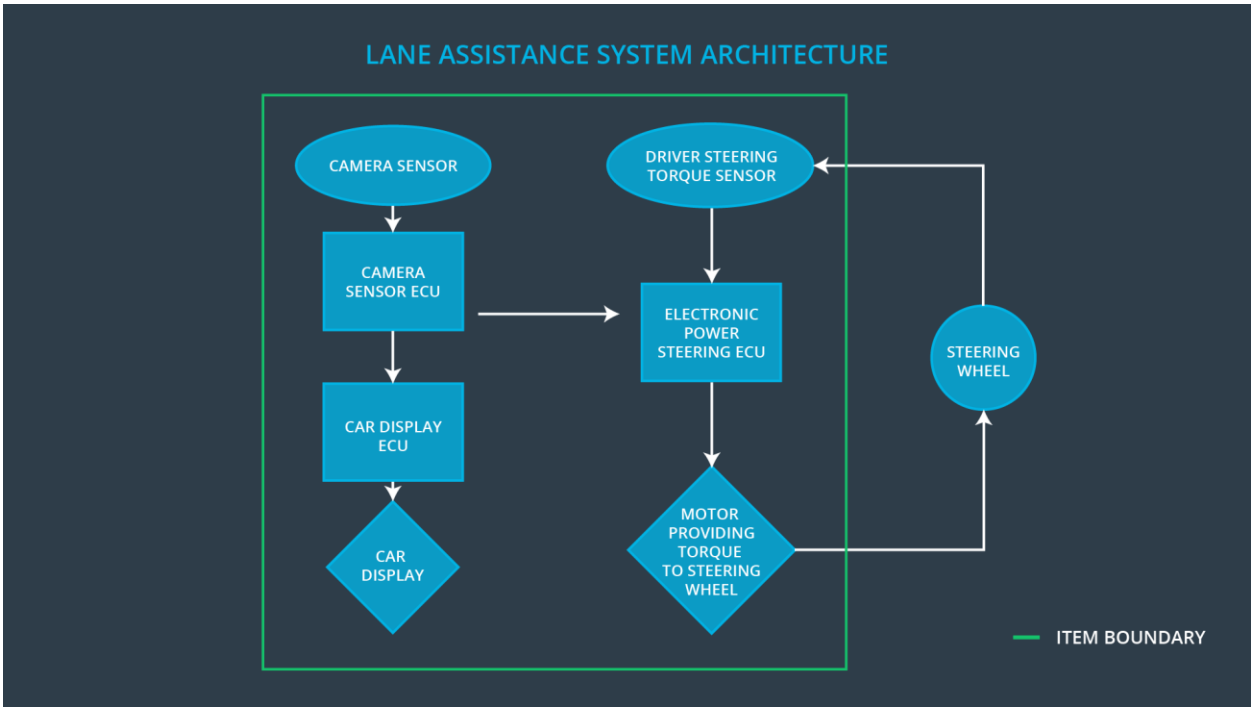
- Lane departure warning function
- Lane keeping assistance function

The lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback in case the car drifts towards the edge of the ego lane. The lane keeping assistance function shall apply the steering torque when active in order to stay in ego lane. Both functions shall act automatically and additionally to the vibrating steering wheel a warning light shall be displayed on the car display dashboard.

The item consists of three sub-systems with their own responsibilities:

- Camera sub-system
  - Camera sensor
  - Camera sensor ECU (Electronic Control Unit)
- Electronic Power Steering sub-system
  - Driver steering torque sensor
  - Electronic Power Steering ECU
  - Motor providing torque to steering wheel
- Car Display sub-system
  - Car Display
  - Car Display ECU

The following diagram shows the interactions between the sub-systems:



Goals and Measures

Goals

The major goal of this project is to assure safe and reliable operation of the Line Assistance System, according to ISO 26262. To achieve functional safety, we are going through the following steps:

- Identify hazardous situations in the Line Assistance System.
- Evaluate the risks of hazardous situations.
- Decrease the risks to an acceptable level 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	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

In order to ensure the safety culture within our company, the following characteristics need 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 process

Safety Lifecycle Tailoring

For this project, the safety plan is tailored.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 OEM and tier-1 involved in developing this system. Both parties agree on the contents of the DIA before the project begins. The ultimate goal is to ensure that all parties are developing safe vehicles in compliance with ISO 26262.

The OEM provides a functioning lane assistance system. Tier-1 is going to analyze and modify the various sub-systems from a functional safety viewpoint.

Here are major sections of a DIA:

- Appointment of customer and supplier safety managers.
- Joint tailoring of the safety lifecycle.

- Activities and processes to be performed by the customer; activities and processes to be performed by the supplier.
- Information and work products to be exchanged.
- Parties or persons responsible for each activity in design and production.
- Any supporting processes or tools to ensure compatibility between customer and supplier technologies.

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.

The people who carry out confirmation measures need to be independent from the people who actually developed the project.

The 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.

The functional safety audit makes sure that the actual implementation of the project conforms to the safety plan.

The 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.