Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [RC1]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
08.10.2017	0.1	Gustavo Espindola	First draft
11.10.2017	1.0	Gustavo Espindola	Release candidate 1
18.10.2017	1.1	Gustavo Espindola	Correct assignees in the table.

Table of Contents

Inhalt

Introduction

Purpose of the Safety Plan

This document is intended to create a global structure and to delineate the reach of the safety efforts, and to assign responsibilities for all the parts involved. The outcome of this document shall be a clear item definition and provide an understanding so that each activity of the safety life-cycle can be performed.

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

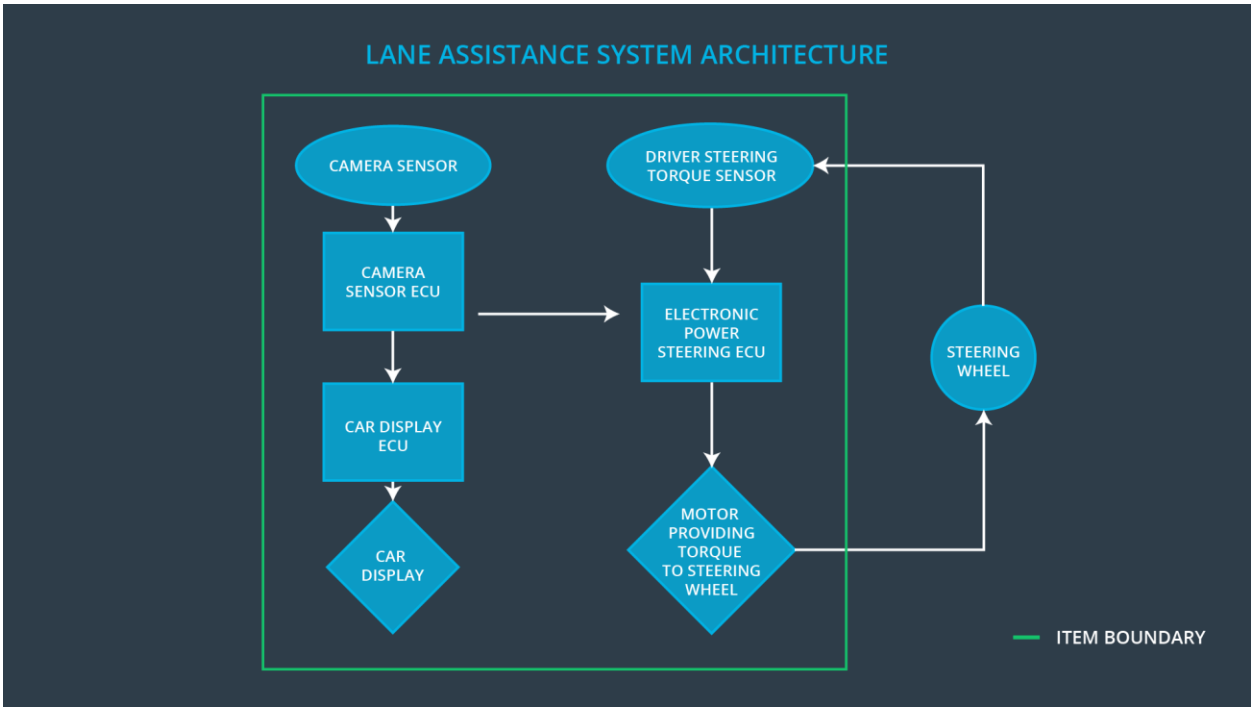
Item Definition

The present plan is targeted to a keep lane assistance feature, this helps the driver in maintaining the traffic lane in case of unwanted deviation, by unwanted we refer to the situation where the driver has not set the change lane light on, and the car is leaving its current lane. In that situation, the system will correct the course and will alert the driver by vibrating the steering wheel.

The system can be divided in two functionalities:

1. Detect and correct the direction of the vehicle if it's detected as unintended behavior.
2. Alert the driver about the possible deviation.

The system's functional architecture is described in the next image:



The complete item can be divided by its responsibility in the overall function in the next subsystems:

Lane detection:

This system includes the camera sensor and the camera sensor ECU. Its purpose is to detect the lane and alert to the correction and feedback subsystem about it.

Correction and feedback:

This system is comprised of driver steering torque sensor, electronic power ECU and the actuation unit which is the motor. It is the responsible of correct the trajectory to stay in the lane and to give feedback to the driver by causing a vibration in the steering wheel.

The car display ECU and the display itself do NOT form part of this system but part of the functionality of the item is reflected on the display as well as in the steering wheel.

Car Display:

This display gives the information to the driver regarding the state of the system, whether or not is activated and if it's activated whether or not the system is applying force control action over the vehicle.

Operational constraints

The current safety plan is developed with the next assumptions:

- The system has not been tampered.
- The climate conditions are acceptable for driving.
- The road conditions are acceptable for the vehicle and the speed.
- The lanes on the road are visible.
- This system is intended to be used on-road.

Goals and Measures

Goals

The main result of this analysis is to reduce the risk up to an acceptable limit, taking into consideration the costs, severity and probability of an incident. The outcome of this analysis is a set of organization rules and processes which will evidence the quality of the system

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

In our company, the client's safety is above all the concerns, to ensure this we have incorporated this guidelines to every engineer involved in the production process.

- We must prioritize safety above costs and productivity.
    - The cost of a failure increases exponentially as goes through the development phase.
    - A failure can damage the trust of the customer and damage the complete company.
- Every one of us must be accountable for the decisions made in the development.

    - We shall be proud of what is being delivered to our customer, and take responsibility of our mistakes.
- We perform audits on our processes and products to ensure their quality.
    - We must ensure the correctness and completeness of our products at every phase of the production cycle.
- We are constantly updating our knowledge in the newest regulations related to our products.
    - As new technologies emerge new challenges will come with it, we need to stay updated.
- Keep traceability in every requirement, from the design phase to the product delivery.
    - We need to measure the completeness of the implementation and ensure the correct testing of each functionality.

Safety Lifecycle Tailoring

For this project, as it is an update we won't cover the complete Safety lifecycle, the elements that will be covered are:

- Concept phase of the safety lifecycle.
- Product development at the system level.
- Product development at the software level.

The next phases are out of the scope for this project:

- 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

The purpose of development interface agreement is to define the boundaries in both, roles and responsibilities in this project as well as the deliverables from each part to ensure completeness and compliance with ISO26262.

The status of the project is the following: Our client has requested to update the system of lane assistance which was developed 2 years ago. The used libraries will be updated to the newest version.

The OEM is responsible to provide the following:

- Previous requirements
    - Functional
    - Non-functional
- Results of compliance audits
- MISRA C compliant source code
- Previous system architecture
- Contact information of functional responsible for the past project

Based on the provided information the OEM expects this company to deliver the next items:

- Updated requirements for the feature
- Evidence of a successful ISO 26262 audit
- Updated source code and compliance quality reports
- Report of requirement/implementation/test traceability
- Contact information of the new functional responsible for the project

Confirmation Measures

The next confirmation measurements are to be performed to ensure that this project is complaint with the ISO 26262 and that it’s being applied in a way that improves the system safety. These confirmation measurements will be carried out by an external company.

The external company is expected to:

- Ensure project’s compliance with ISO 26262, this implies that the project was executed following the standard.
- Ensure that the project implementation was made following the safety plan.
- Confirm that the changes made in the system to comply the ISO26262 made it safer.

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.