Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

[Instructions: Fill in the date, version and description fields. You can fill out the Editor field with your name if you want to do so. Keep track of your editing as if this were a real world project.

For example, if this were your first draft or first submission, you might say version 1.0. If this is a second submission attempt, then you'd add a second line with a new date and version 2.0]

Date	Version	Editor	Description
10/31/2018	1.0	BM	First version of the document

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

This document specifies how functional safety will be ensured throughout the entire development project and in production of the Lane Assistance System.

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 under consideration is the Lane Assistance System. This system is designed to help the driver to keep the vehicle near the center of the lane it currently occupies, by providing the following two functions:

- **Lane Departure Warning** function: This function alerts the driver in the case that the vehicle drifts over the lines marking the edge of the lane. The driver is alerted via steering wheel vibrations.
- **Lane Keeping Assistance** function: In the case when the vehicle drifts over the edge of the lane it currently occupies, this function will turn the steering wheel in a way to steer the vehicle back towards the center of the lane, thus helping the driver keep the vehicle inside the lane.

The Lane Assistance System is realized by using the following subsystems:

- **Camera subsystem:** This subsystem consists of the front facing camera and the electronic control unit (ECU) that controls the camera
- **Car display subsystem:** This subsystem consists of the display inside the vehicle that the driver monitors, and the ECU to control that display
- **Electronic power steering subsystem:** This subsystem consists of the motor providing the torque to turn the steering wheel, the sensor to sense the torque currently exerted by the driver, and the ECU that controls this overall subsystem

Figure 1 shows the diagram that describes the interaction of the aforementioned subsystems when realizing the Lane Assistance System, as well as the System boundary. It is shown that the camera subsystem, the car display subsystem and the electronic power steering subsystem are completely within the item boundary, while the steering wheel itself is not.

As mentioned in the paragraphs above, the Lane Assistance System helps the driver to keep the vehicle near the centerline of the lane it is driving on (also known as ego lane), by performing the Lane Departure Warning function and the Lane Keeping Assistance function. When the camera subsystem senses that the vehicle drifts over the lane marks on either side of the lane, it will send the signal to the electronic power steering subsystem to ask it to vibrate the steering wheel to notify the driver, as well as to turn the steering wheel slightly to keep the vehicle near the centerline of the ego lane. There are three cases in which the electronic power steering subsystem will not exert additional torque as requested by the camera subsystem:

- The driver is using the turn signal: this action suggests that the drift over the lane marks was intentional, and therefore the electronic power steering subsystem decides not to interfere with the action of the driver
- The driver is exerting substantial torque on the steering wheel: again, in this situation it is safe to assume that the driver’s action was deliberate and that the vehicle crossing the lane marks is intentional. Therefore, the electronic power steering subsystem decides not to exert additional torque on the steering wheel.

- The driver turned off the Lane Assistance System manually. This suggests that the driver does not want the System to interfere with operating the vehicle, and the System stays inactive until it is turned back on by the driver or until the car is turned off and back on again.

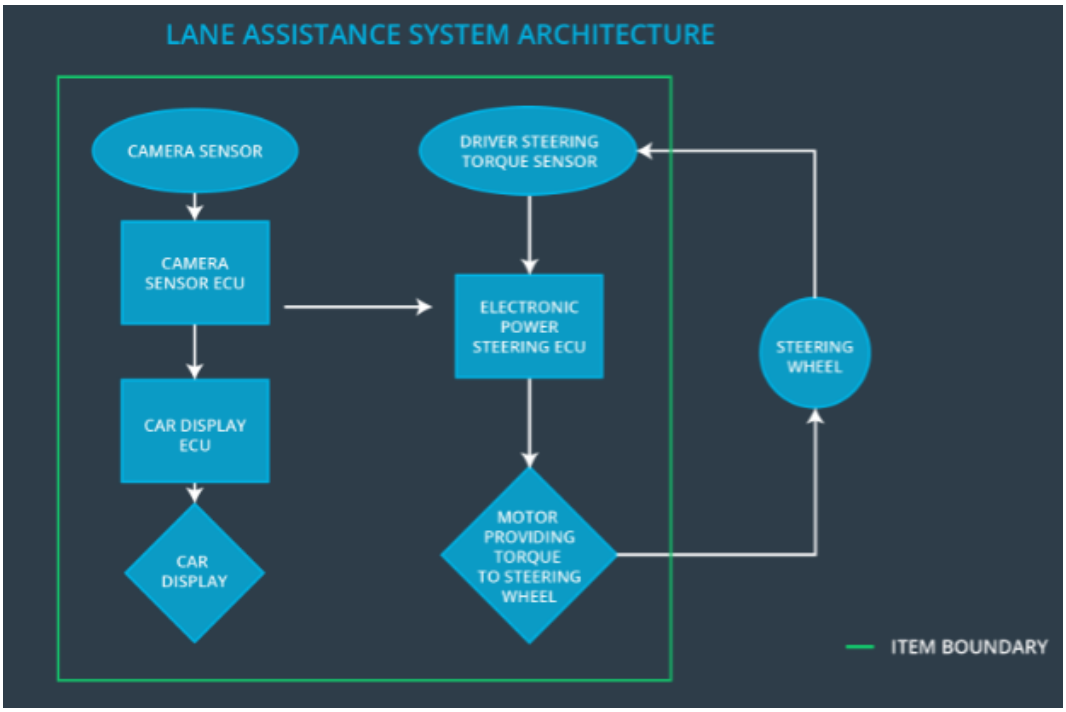

Figure 1. Lane Assistance System architecture

If none of the three conditions are currently active (no turn signal, no substantial torque from the driver, the System is not turned off), the System performs its desired function in the following way:

- The camera subsystem checks if the vehicle is drifting over the markings of the ego lane
- If so, the camera subsystem sends the signal to electronic power steering subsystem, suggesting that the steering wheel should vibrate slightly to notify the driver that the vehicle is crossing the lane markings, and that additional torque should be applied to the steering wheel to keep the vehicle near the centerline of the ego lane.
- The camera subsystem also notifies the driver visually on the vehicle display subsystem that the Lane Assistance System detected a potentially dangerous situation and is actively working to mitigate the risk.
- The electronic power steering subsystem performs the suggested actions, i.e. it vibrates the steering wheel and applies additional torque.

Goals and Measures

Goals

The goal of the safety plan that is being developed for the Lane Assistance System is to lower the risks associated with the System to the levels acceptable by the general society. In essence, the implementation of the System in the overall design of the vehicle introduces certain risk that, due to malfunction of the System, the vehicle may end up in a hazardous situation. To mitigate and lower that risk, we perform the following actions in the safety plan development:

- Identify hazardous situations
- For each of the hazardous situations, asses the level of risk
- Develop the functional safety concept to lower the risk to the acceptable levels
- Develop the technical safety concept to define the functional safety plan in more technical terms
- Develop software and hardware requirements to address the items previously described in the technical safety concept

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 Auditor	Once every 2 months

safety audits		
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 that the safety plan is developed and executed according to the highest standards possible, all of the teams involved in the design and development of the vehicle need to embrace the company's safety culture, which includes the following:

- **High priority:** safety has the highest priority in the design of the vehicle, and it overrules other design constraints with competing requirements
- **Accountability:** safety related design decisions are made traceable back to the people that made them, so that they can be held accountable. The company will reward the teams and the individuals that follow the safety rules closely, and it will likewise penalize those whose decisions and actions jeopardize safety of the products and the customers
- **Independence:** the teams that work on product design and development will be completely independent from the teams that perform the audit of safety related product features
- **Well defined processes:** the design and management processes within the company should be clearly defined and it should be ensured that they are followed
- **Resources:** projects have necessary resources including people with appropriate skills.
- **Diversity:** intellectual diversity is sought after, valued and integrated into processes.
- **Communication:** communication channels are set up in a way to encourage disclosure of problems, enable anonymous disclosure of problems, and prevent any retaliation towards people that disclose problems to the management.

Safety Lifecycle Tailoring

For the Lane Assistance System project, the safety lifecycle is tailored to include certain phases, and to take out those that are outside of the scope of the projects. The following phases fall within the project's scope:

- Concept phase
- Product development at the system level
- Product development at the software level

The following phases fall outside of the project's 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

The Development Interface Agreement document (DIA) defines the roles and responsibilities between the OEM and the Tier-1 supplier involved in the development of the Lane Assistance System. Both companies agree on the content of DIA before the project begins, so that any disputes are avoided during the development phase of the project.
The OEM is responsible for the overall vehicle safety and all of the related functional safety actions required by the ISO 26262 standard. The Tier-1 supplier is accountable for the Lane Assistance System item in the vehicle, but not any of the other subsystems within the vehicle.

The Tier-1 supplier does, however, analyze and modify any of the subsystems from the functional safety standpoint, which are required for the correct operation of the Lane Assistance System. The Tier-1 supplier is responsible for fixing all issues and bugs in the Lane Assistance System, while the OEM needs to investigate any issues that arise in any other subsystem. Any relevant information regarding the functional safety of the Lane Assistance System should be exchanged between Functional Safety Managers of OEM and Tier-1 development teams.

Confirmation Measures

The purpose of **confirmation measures** is to ensure that the development project of the Lane Assistance System conforms to ISO 26262, and that the Lane Assistance System does make the vehicle safer without any doubts. The **confirmation review** is performed during the design and development of the product, and it includes that an independent person reviews the work to ensure that the ISO 26262 standard is being followed. The **functional safety audit** checks that the actual implementation of the project conforms to the already developed safety plan. The **functional safety assessment** confirms that the plan, design and developed product 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.