Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.0

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
30-10-2017	1.0	Pablo Elizalde	First draft
28-11-2017	1.1	Pablo Elizalde	Fixed responsibilities table

Table of Contents

[Instructions: We have provided a table of contents. If the table of contents is not showing up correctly in your word processor of choice, please update it. The table of contents should show each section of the document and page numbers or links. Most word processors can do this for you. In Google Docs, you can use headings for each section and then go to Insert > Table of Contents. Microsoft Word has similar capabilities]

Introduction

Purpose of the Safety Plan

[Instructions: Answer what is the purpose of a safety plan?]
The purpose of a safety plan is the creation of a document that describes the process for identifying the physical and health hazards. Safety plan defines roles and the steps to achieve functional safety.

Scope of the Project

[Instructions: Nothing to do here. This is for your information.]

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

[Instructions: Nothing to do here. This is for your information.]

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

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

The system is a simplified version of a Lane Assistance System that alerts the driver if the car moves out accidentally from the lane and attempts to steer the vehicle back to the lane.

What are its two main functions? How do they work?

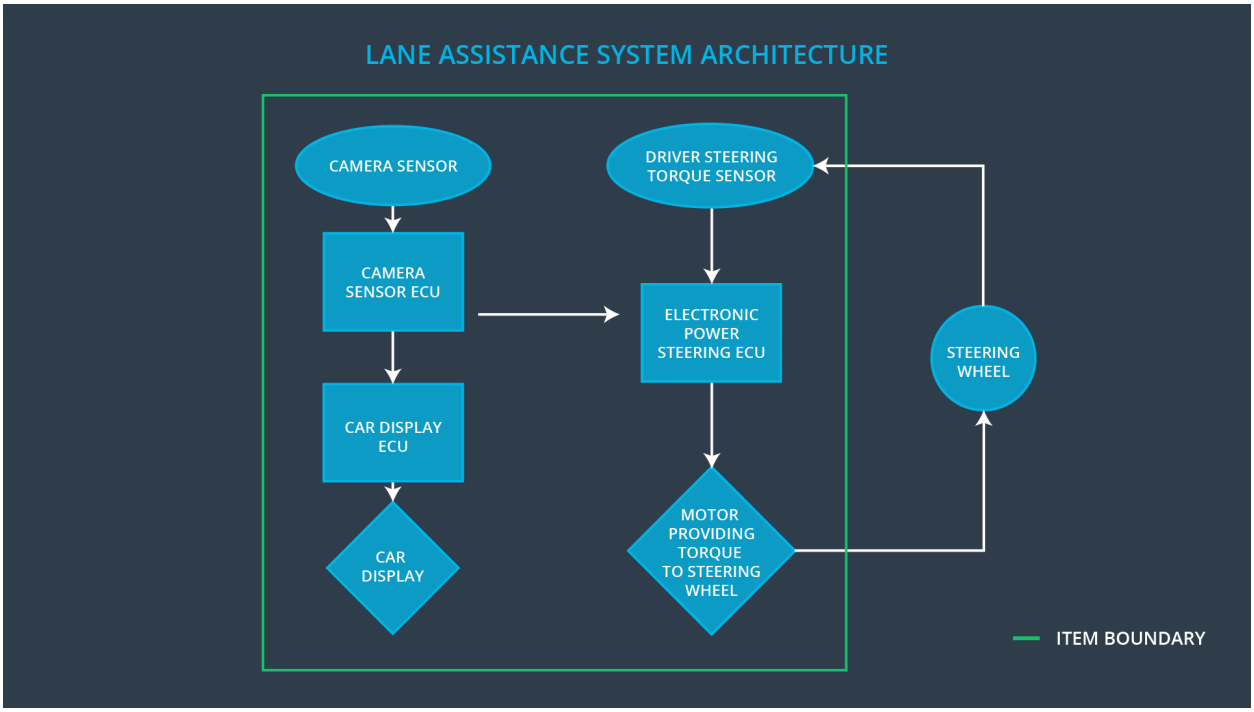
The two main functions for the system lane departure warning and lane keeping assistance.
The lane departure warning applies a vibration to the steering wheel to provide the driver a haptic feedback.
The lane keeping assistance functionality assists the driver applying a steering torque in order to stay in ego lane.

Which subsystems are responsible for each function?

There are three subsystems:

- Camera subsystem, responsible for detecting lanes and determining when the vehicle leaves the lane by mistake.
- Electronic Power Steering subsystem, responsible for measuring the torque provided by the driver and then adding an appropriate amount of torque based on a lane assistance system torque request.
- Car Display subsystem, responsible for displaying to the driver when is departing the ego lane by mistake.

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



OPTIONAL

Optionally, include information about these points as well. These were not included in the lectures, but you might be able to find this information online:

- **Operational and Environmental Constraints. This could especially be limited to camera performance; lane lines are difficult to detect in snow, fog, etc**
- **Legal requirements in your country for lane assistance technology**
- **National and International Standards Related to the Item**
- **Records of previously known safety-related incidents or behavioral shortfalls**

]

According to the DGT (Direccion General de Trafico), the Spanish national organism in charge of the road safety, in 2014 there where 13.314 accidents due to the departure of the road, of which 383 had fatal consequences with 476 deceased. Here we can see the importance of a lane keeping assistance system.

But is not only important to include these technologies into the modern vehicles, since there is a strong dependency with the roads. For this system to work is important that the lanes are clearly delimited, and that the roads are clean and well maintained. Other factor that could affect the system are the snow, mud or heavy rain on the road.

A probe of the importance of the system is that the EuroNCAP (European New Car Assessment Programe), who values the safety level of vehicles, takes in consideration the presence of the lane assistance system.

Goals and Measures

Goals

[Instructions:
Describe the major goal of this project; what are we trying to accomplish by analyzing the lane assistance functions with ISO 26262?]
The goal of this project is to create a safety case for a lane assistance, to reduce risk to acceptable levels. It is important to document, so the auditors can assess the work, and provide an evidence that the project has made the vehicle safer. Documentation also provides a reference when modifying a system.

Measures

[Instructions:
Fill in who will be responsible for each measure or activity. Hint: The lesson on Safety Management Roles and Responsibilities.

The options are:
All Team Members
Safety Manager
Project Manager
Safety Auditor
Safety Assessor
]

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 Assessor	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 Auditor	Conclusion of functional safety activities

Safety Culture

[Instructions:
Describe the characteristics of your company's safety culture. How do these characteristics help maintain your safety culture. Hint: See the lesson about Safety Culture
]

Not just accidents come from the technology malfunctions, but also from social and organization factors. That is why there are clear policies and strategies to support the development, production and operation of safe systems.
Safety is the highest priority in our company, above other values as cost and productivity.
All design decisions must be clearly traceable back to the people/teams who made those decisions.
The company rewards and motivate the achievement of functional safety, and penalizes any kind of shortcut.
The company encourages to create free and safe environment of communication channels.

Safety Lifecycle Tailoring

[Instructions:
Describe which phases of the safety lifecycle are in scope and which are out of scope for this particular project. Hint: See the Intro section of this document
]

The phases included in scope are:

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

- Product development at the software level.

Out of scope:

- Product development at the hardware level.
- Production and operation.

Roles

[Instructions:
This section is here for your reference. You do not need to do anything here. It is provided to help with filling out the development interface agreement section.
]

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

[Instructions:
Assume in this project that you work for the tier-1 organization as described in the above roles table. You are taking on the role of both the functional safety manager and functional safety engineer.

Please answer the following questions:

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. All involved parties need to agree on the contents of the DIA before the project begins.
The DIA also specifies what evidence and work products each party will provide to prove that work was done according to the agreement.
The ultimate goal is to ensure that all parties are developing safe vehicles in compliance with ISO 26262.

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 responsibility of the company will be deliver a product to the OEM, following its requirements. From those sub-systems we will need to analyze if we need to outsource to a Tier 2 company, and in that case, create a DIA between us and the provider. We will be responsible of developing the sub-systems in compliance with the ISO 26262, but the OEM will be the responsible of testing the correct behavior of sub-systems delivered together with other sub-systems in the lane assistance system.

Confirmation Measures

[Instructions:
Please answer the following questions:

1. **What is the main purpose of confirmation measures?**
2. **What is a confirmation review?**
3. **What is a functional safety audit?**
4. **What is a functional safety assessment?**

]

The confirmation measure checks three things:

- Processes comply with the functional safety standard ISO26262.
- Project execution is following the safety plan.
- Design really does improve safety.

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.

Functional safety audit
It makes sure that the actual implementation of the project conforms to the safety plan.

Functional safety assessment
It 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.