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
27/11/2018	1.0	Joseph Magdy	Initial Version
1/12/2018	1.1	Joseph Magdy	First Release of the Safety Plan Document
6/12/2018	1.2	Joseph Magdy	Fix Reviewer Comments

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?]
Safety Plan define the followed steps to ensure the Lane Assistance safety analysis and assign the rules and responsibilities

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

[Instructions:

REQUIRED

Discuss these key points about the system:

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

The lane assistance system which assist the driver to keep the vehicle in the center of the lane and in case the vehicle is moving outside the lane which turning on the indicators it produces haptic feedback on the steering wheel and steer the vehicle to the center of the ego lane again.

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

There are two functions :
1- Lane departure warning : will vibrate the steering wheel .

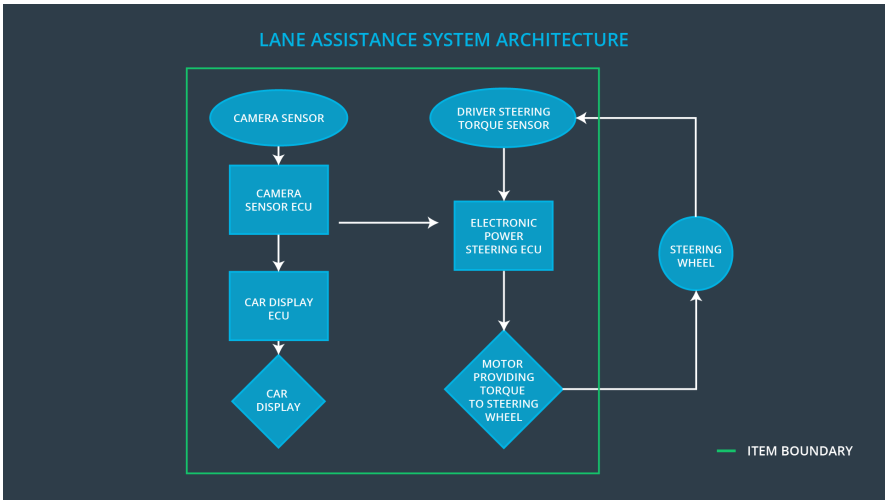
2- Lane keeping assistance : will move the steering wheel so that the wheels turn towards the center of the lane.

Which subsystems are responsible for each function?

Camera Subsystem : Responsible for detecting the lanes and determine when the vehicle leaves the lane by mistake.

EPS Subsystem : Responsible for measuring the applied torque by the driver and applied appropriate amount of torque based on the lane assistance value request.

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**

]

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 lane departure warning is done by applying an amount of torque to the steering wheel , the safety is that the applied value is not too high that can lead the driver to not able to handle the steering and cause accident.

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	Safety Engineer	Constantly
Create and sustain a safety culture	Project 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

[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
]

Priority : Safety is considered a high priority in the project that need to bb taken into consideration with any decision that could affect the SW safety.

Configuration Management : Configuration management and ticketing system is mandatory to use with any safety document or safety bug in the SW to ensure the traceability . fix and test of this ticket.

Reward and Penalty : Ignoring the safety plan and guidelines in designing and testing SW component is considered one of the high risks that can't be ignored , managers always encourage reporting SW safety issues and reward such an attitude.

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
]

Phases are in scope:

- **Concept phase**
- **Product Development at the System Level**
- **Product Development at the Software Level**

Phases are 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?**

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.**

]

My company is responsible to get the OEM requirements and ensure it complained with ISO26262 , modify sub-systems in the lane assistance system and provide the safety plan and tests to ensure the product safety.

Confirmation Measures

[Instructions:
Please answer the following questions:

1. **What is the main purpose of 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.

2. **What is a 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.

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.