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
16-05-2018	1.0	Disha Patel	Initial Submission

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 is an important part of designing autonomous vehicles and it has to be applied in designing safe, functional, self-driving cars.

Any product has certain functions about what the product should do. Safety plan is used to make sure that this functions do not lead to harm or injury. Here, it is required to reduce the risk in electronic systems. In the vehicles, increased use of hardware and software systems are done, so to avoid any harm due to those, we need to have proper safety plan in place. It will provide the evidence that our project has made the vehicle safer. Safety plan is used in many industries like automotive, avionics, medical device and railroad.

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?

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

Which subsystems are responsible for each function?

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

]

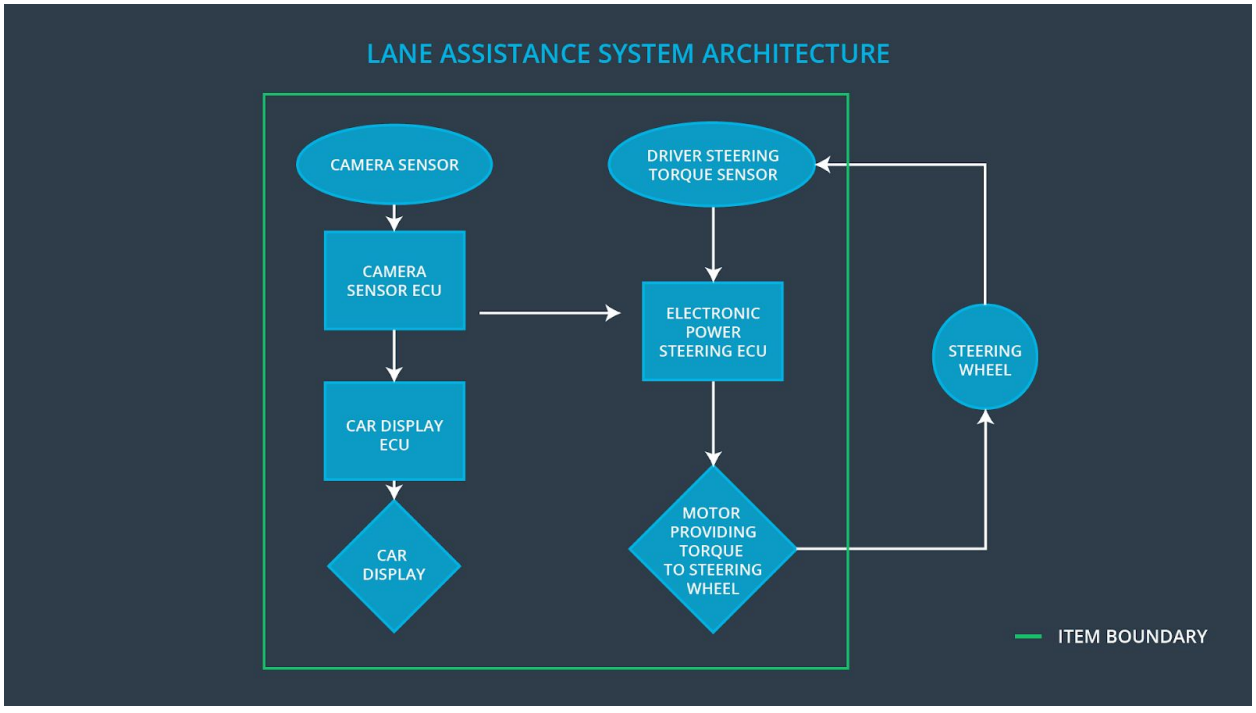
The item being considered here is Lane Assistance System. The System will be used to alert the driver when it is faced by potentially dangerous situations and accordingly he will be required to take control of the system and this way the accidents can be prevented from occurring.

The two main functions being considered are Lane departure warning and Lane Keeping Assistance.

The lane departure warning function is used to apply oscillating steering torque that will provide the driver a haptic feedback.
The lane keeping assistance function is used to apply steering torque once it is active so that it will keep the car in the same or the active lane.

Below are the subsystems responsible for the lane assistance functions:

Camera system, Electronic power steering system and Car display system.



The above diagram shows the relations between the subsystems and how they are connected. The camera sensor will detect if the vehicle is out of the lane and sends the signal for the same to the electronic power steering system which will turn the steering and keep the vehicle back

on the lane. Camera sensor will also request the warning light to be turn on so that the driver will be aware that the system is active. The electronic power steering system will detect how much the car is turned by the driver and accordingly it may add torque to get back the vehicle to the center. The car display system will display the warning if required.

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 major goal of this project is to identify risk and hazardous situations in the Lane Assistance System, if it has malfunction which can cause injuries to the person. Based on it, it will evaluate the risk of the situation and lower the risk of the malfunctions to acceptable level.

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	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

[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
]

Characteristics of company’s safety culture:

1) Communication: Different channels of communication helps and encourages disclosure of problems.
2) Well defined process: The management processes and design is very well defined.
3) High priority: Highest priority is given to safety compared to the cost and productivity.
4) Rewards: Constant motivation and support is given by the organization for achieving the functional safety.

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
]

Below phases are in scope of the safety lifecycle:

1) Concept phase
2) Produce Development at the System Level
3) Product Development at the Software Level

Below phases are out of scope:

1) Product Development at the Hardware Level
2) 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?**

The DIA, Development Interface Agreement delineates the design and production responsibilities between the OEM and Tier 1 supplier or between the Tier 1 and Tier 2 supplier. It is required to avoid disputes during the planning and development of a product and also because of liability. If a vehicle has a safety issue after being sold to consumers, a DIA provides clarity about which company is best positioned to fix the system.

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 company agrees that the above mentioned safety lifecycle will be fine to fulfill the ISO 26262 for the lane assistance system. While the OEM is responsible for the overall safety of the vehicle and also the safety actions mentioned in ISO 26262.

Tier-1 will analyze and modify few sub-systems based on the functional safety requirements. The company will fix all bugs which comes under the lane assistance system and all other issues would have to be taken care by OEM.

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?**

]

1) The main purpose of confirmation measures are: a functional safety project conforms to ISO 26262 and the project really make the vehicle safer.
2) Confirmation review ensure that the project compiles 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) Functional safety audit is checking to make sure that the actual implementation of the project conforms to the safety plan.
4) Functional safety assessment is confirming 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.