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
23/05/2018	1.0	Shubhadeep	First Attempt

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 this safety plan is to provide an overall framework for the Lane Assistance item and to assign roles and responsibilities for the item's 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

[Instructions:

REQUIRED

Discuss these key points about the system:

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

The item in question is **Lane Assistance System**. It alerts the driver when car accidentally drifts out from its lane and tries to steer the car back to the lane center.

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

The two main functions of Lane Assistance System are:

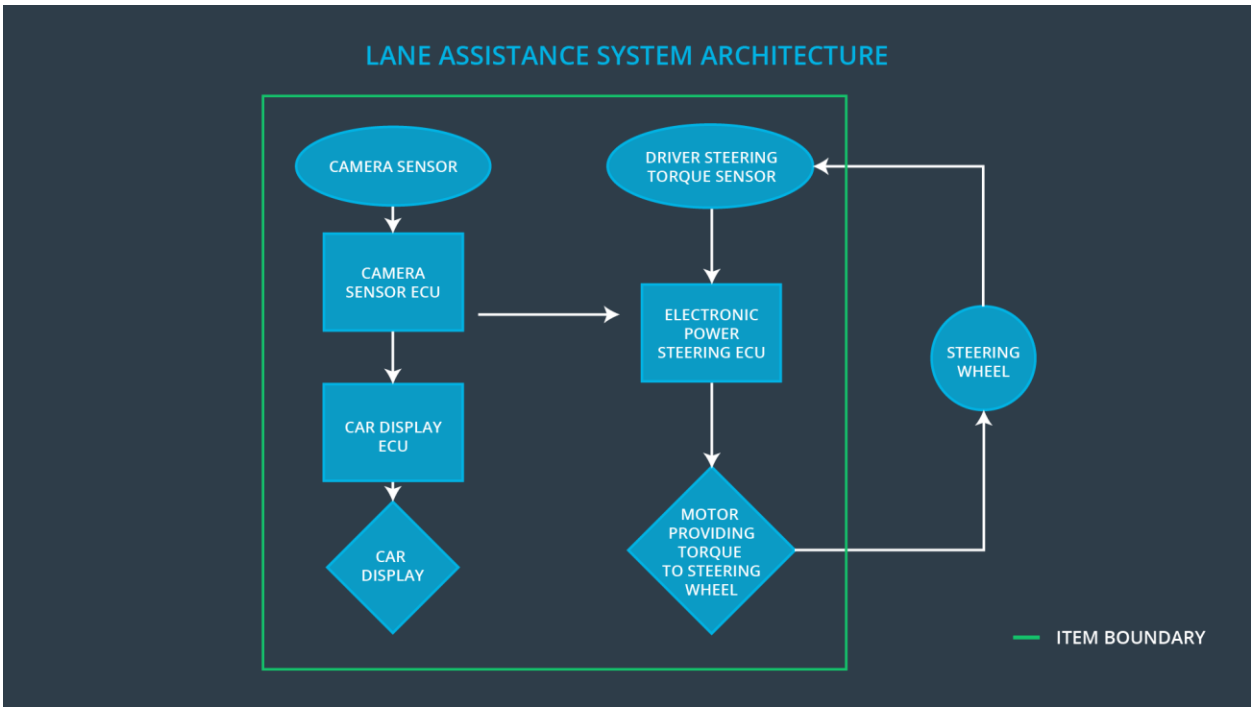
1. **Lane Departure Warning** : The lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback. In other words, the vehicle quickly moves the steering wheel back and forth to create a vibration.
2. **Lane Keeping Assistance** : The lane keeping assistance function shall apply the steering torque when active in order to stay in ego lane. Ego lane refers to the lane in which the vehicle currently drives.

Which subsystems are responsible for each function?

The Camera system, Electronic Power Steering system, and Car Display system are the subsystems which 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?

Boundaries of the item are shown in the figure given below. Only the Steering Wheel system is outside the item and rest all (Camera System, Electronic Power Steering system, Car Display system) are inside 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 major goals of this project are :

1. to identify the hazardous situations in the Line Assistance system components which can cause injury to a person.
2. to evaluate the risk involved in that hazardous situations.
3. to lower the risk of the hazardous situation to a level acceptable by current society.

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
]

The characteristics which help maintain the safety culture are :

1. **High priority** : safety has the highest priority among other constraints like cost and productivity.
2. **Accountability** : processes ensure accountability such that design decisions are documented and traceable back to the people and teams who made the decisions.
3. **Rewards** : the organization motivates and supports the achievement of functional safety.
4. **Penalties** : the organization penalizes shortcuts that jeopardize safety or quality.
5. **Independence** : teams who design and develop a product should be independent from the teams who audit the work.
6. **Well defined processes** : company design and management processes should be clearly defined.

7. **Resources** : projects have necessary resources including people with appropriate skills.
8. **Diversity** : intellectual diversity is sought after, valued and integrated into processes.
9. **Communication** : communication channels encourage disclosure of problems.

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 following safety lifecycle phases are in scope for this particular project:

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

The following safety lifecycle phases are out of scope for this particular project:

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 purpose of a development interface agreement is to define roles and responsibilities of the parties involved in this project to ensure the development 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 responsibilities of our company will be :

1. to provide requirements to OEM about what the lane assistance system needs to do.
2. to test the lane assistance system provided by OEM and make sure it is in compliance with ISO 26262.

The responsibilities of OEM will be :

1. to make and provide a lane assistance system according to the requirements provided and ISO 26262 safety standards.

]

Confirmation Measures

[Instructions:
Please answer the following questions:

1. **What is the main purpose of confirmation measures?**

The main purpose of the confirmation measures is to check whether the functional safety project conforms to ISO 26262 and makes the vehicle safe.

2. **What is a confirmation review?**

A confirmation review is a review provided by an independent person on the product when designed and developed, to make sure that the project is in compliance with ISO 26262.

3. **What is a functional safety audit?**

A functional safety audit is an audit/check to make sure that the actual implementation of the project conforms to the safety plan.

4. **What is a functional safety assessment?**

A functional safety assessment is a test/assessment which 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.