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
9/1/2017	1.0	Xu fuqiang	submit version

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 safety plan gives an overview of how you are going to achieve a safe system, and defines safety roles and responsibilities involved in the project.

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 in question is Lane Assistance item.
Lane Assistance item alerts the driver that the vehicle has accidentally departed its lane, and attempts to steer the vehicle back towards the center of the lane.

Two main functions:
1. Lane departure warning
2. Lane keeping assistance

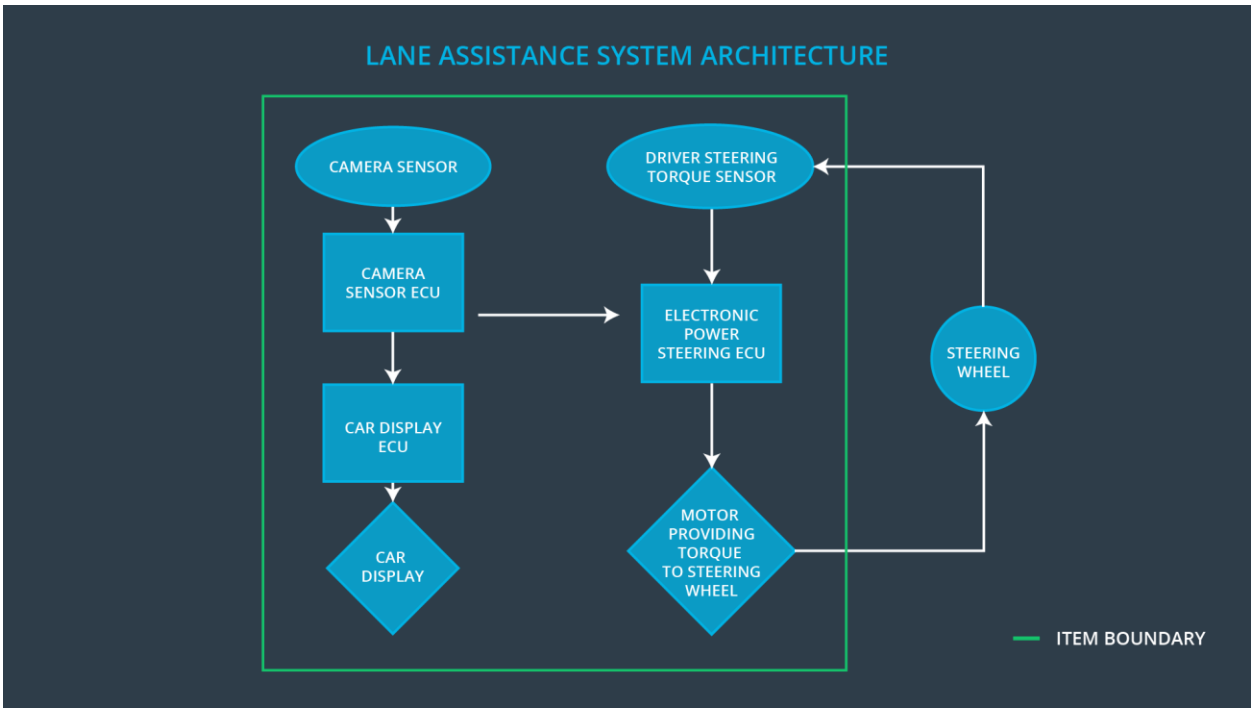
The lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback.
The lane keeping assistance function shall apply the steering torque when active in order to stay in ego lane

Three subsystems:
1. Camera system
2. Electronic Power Steering system

3. Car Display system

Camera system is responsible for detecting lane lines and determining whether the vehicle leaves the lane by mistake.
Electronic power steering system is 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 system is responsible for turning on a warning light in the car display dashboard to make sure the driver knows that the lane assistance system is active.

The boundaries of the item are shown below diagram.
There are Camera subsystem, Electronic power steering subsystem and Car display subsystem inside of item.
The element Steering wheel is outside of item.



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 reduce risk identified for Lane Assistance system to acceptable levels by society and provide evidence that your project has made the vehicle safer.

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 Member	Constantly
Create and sustain a safety culture	All Team Member	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
]

High priority: safety has the highest priority among competing constraints like cost and productivity
Accountability: processes ensure accountability such that design decisions are traceable back to the people and teams who made the decisions
Rewards: the organization motivates and supports the achievement of functional safety
Penalties: the organization penalizes shortcuts that jeopardize safety or quality
Independence: teams who design and develop a product should be independent from the teams who audit the work
Well defined processes: company design and management processes should be clearly defined
Resources: projects have necessary resources including people with appropriate skills
Diversity: intellectual diversity is sought after, valued and integrated into processes
Communication: communication channels encourage disclosure of problems

The most critical issues to make Lane Assistance system popular is gaining customer’s trust that LA is really improve safety and will not lead to any unexpected accidence.
This is same for autonomous driving technology development.
The only solution is to establish safety culture and bring up safety branding from beginning.

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
]

According to Scope of Projects above, 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

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?**

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.**

]

A DIA (development interface agreement) defines the roles and responsibilities between companies involved in developing a product, also specifies what evidence and work products each party will provide to prove that work was done according to the agreement.

The ultimate goal of DIA is to ensure that all parties are developing safe vehicles in compliance with ISO 26262.

The OEM's responsibilities cover the lane assistance system while my company's responsibilities only cover related Tie1 sub-systems. Our company will not responsible for whole lane assistance system and other sub-systems.
DIA defines the roles and responsibilities between OEM, Tie1 and Tie2 in order to avoid dispute and make easy to find who should fix safety issues if there are some safety issues.

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?**

]

Main purposes:

1. Process complies with safety standard, e.g. ISO 26262
2. Project follows the safety plan
3. Design really does improve safety

Confirmation Review Ensures an independent person would review the work to make sure ISO 26262 is being followed.

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

Functional safety assessment 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.