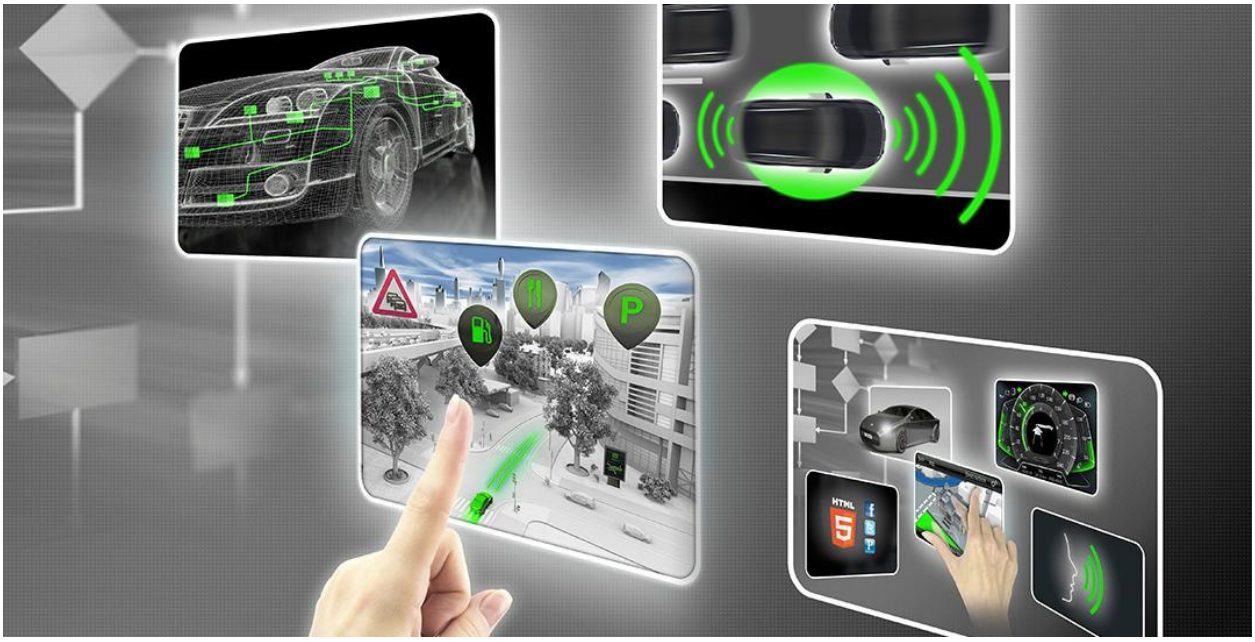
Elektrobit

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
August 13,2017	1.0	Ryosuke Honda	Initial Draft
August 14,2017	2.0	Ryosuke Honda	Revised Item definition

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 purposes of the Safety Plan are following.

- Identify hazards
- Measuring risk
- Using systems engineering to lower risk to reasonable levels

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. The item does two tasks.
One is warn drivers of the lane departure by vibrating the steering. Another is lane keeping assistance.

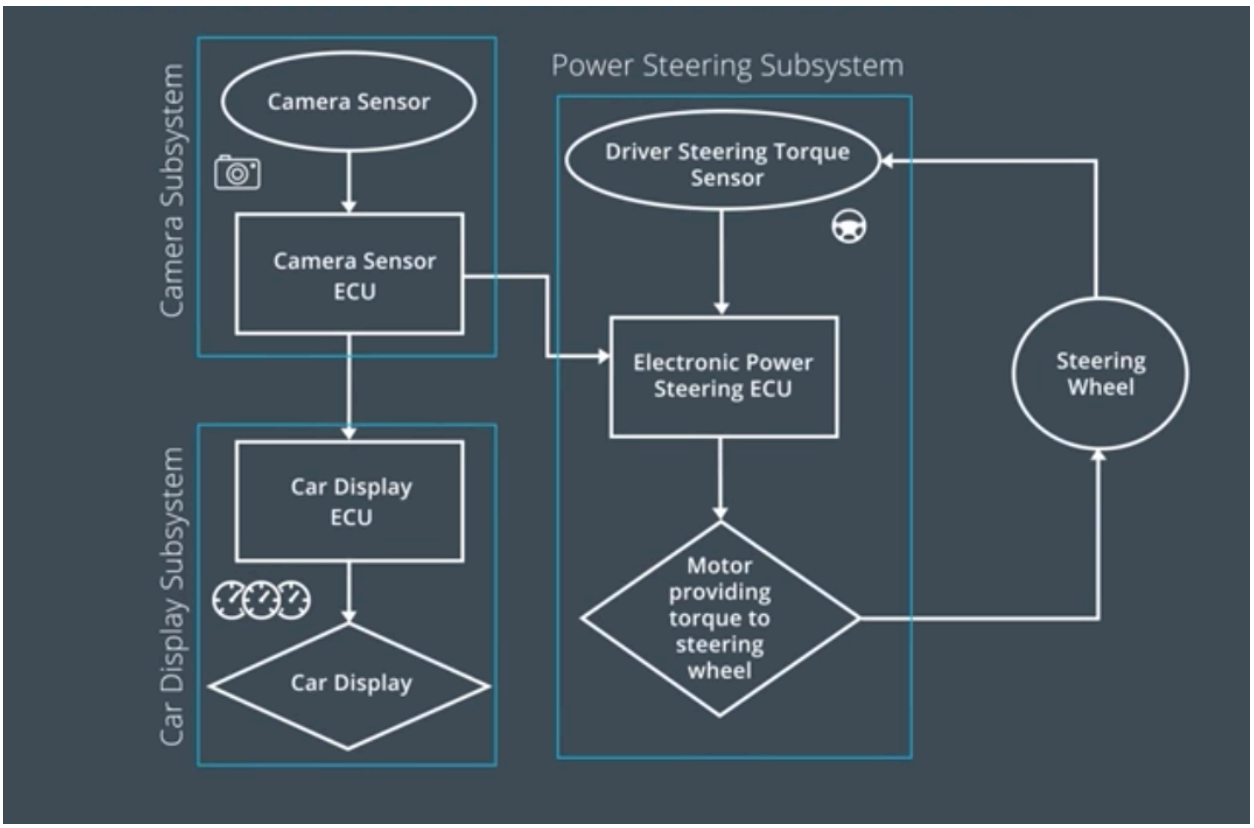
What are its two main functions? How do they work?
The lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback.

The lane keeping assistance function shall apply the steering torque when active in order to stay in ego lane.

Which subsystems are responsible for each function?
Camera sub-system is responsible for sending signals to the Electronic Power Steering System. When the camera senses that the vehicle is leaving the lane, the camera sends a signal to the electronic power steering system. Car Display sub-system is resonsible for warning drivers of malfunctions or misuse of the lane keeping assistance function. Power Steering sub-system is responsible for receiving torque request from camera sensor ECU and steering wheel. Also Power Steering sub-system is responsible for sending torque request of the lane departure warning function and the lane keeping assistance function to the Steering wheel.

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

The item is composed of three sub-systems. Camera sub-system which is composed of camera sensor and camera sensor ECU. DIsplay sub-system which is composed of car display ECU and car display. Electronic power steering sub-system which is composed ot torque sensor, electronic power steering ECU and motor providing torque to steering wheel. The boundaries are illustrated in the picture below.



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 goal is to identify high risk situations and measure risk and then to lower the risk to reasonable levels by using systems engineering to lower risk.

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 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 decision 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 independence from the teams who audit the work

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

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
]

For the lane assistance project functional safety plan, the ISO26262 standard has been tailored to include following safety lifecycle phases 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?**

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 purposes are following.

- Avoid disputes
- Liability
- Makes clear who should fix issues

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.**

]

OEM Project Manager: He/She allocates resources needed for the functional safety activities in Item Level. Also he/she appoints safety manager or might act as a safety manager.

Tier1 Project Manager: He/She allocates resources needed for functional safety activiteis in component level. Also he/she appoints safety manager or might act as a safety manager.

OEM Functional Safety Manager/Engineer:Coordinate and documenti the item level planned safety activities at the following functional safety phases:concept phase and product development at the system level. Also performs pre-audits before the safety auditor(3 months prior to main assessment)

Tier1 Functional Safety Manager/Engineer:Coordinate and document the component level planned safety activities at the following functional safety phases:concept phase and product development at the sub-system level and software level which is in compliance with the item level planned and safety activities developed by OEM Functional Safety Manager/Engineer.

Safety Auditor:Perform regular functional safety audits once every 2 months.

Safety Assessor:Perform functional safety assessment at conclusion of functional safety activities.

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 purposes of confirmation measures are following.

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

Confirmation review:Ensure that the project complies with ISO 26262. As the product is designed and developed, an independent person would review the work to make sure ISO26262 is beign followed.

Functional safety audit: Checking to make sure that the actual implementation of the project conforms to the safety plan.

Functional safety assessment: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.