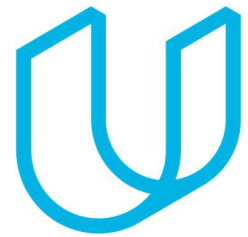




Elektrobit



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
06 Apr 2019	1.0	Soumen De	First Draft

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]

[Document history](#)

[Table of Contents](#)

[Introduction](#)

[Purpose of the Safety Plan](#)

[Scope of the Project](#)

[Deliverables of the Project](#)

[Item Definition](#)

[Goals and Measures](#)

[Goals](#)

[Measures](#)

[Safety Culture](#)

[Safety Lifecycle Tailoring](#)

[Roles](#)

[Development Interface Agreement](#)

[Confirmation Measures](#)

Introduction

Purpose of the Safety Plan

[Instructions: Answer what is the purpose of a safety plan?]

A safety plan provides an overall framework for a functional safety project. It also includes the assignment of 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?

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?

The item considered in this plan is a simplified version of a Lane Assistance System.

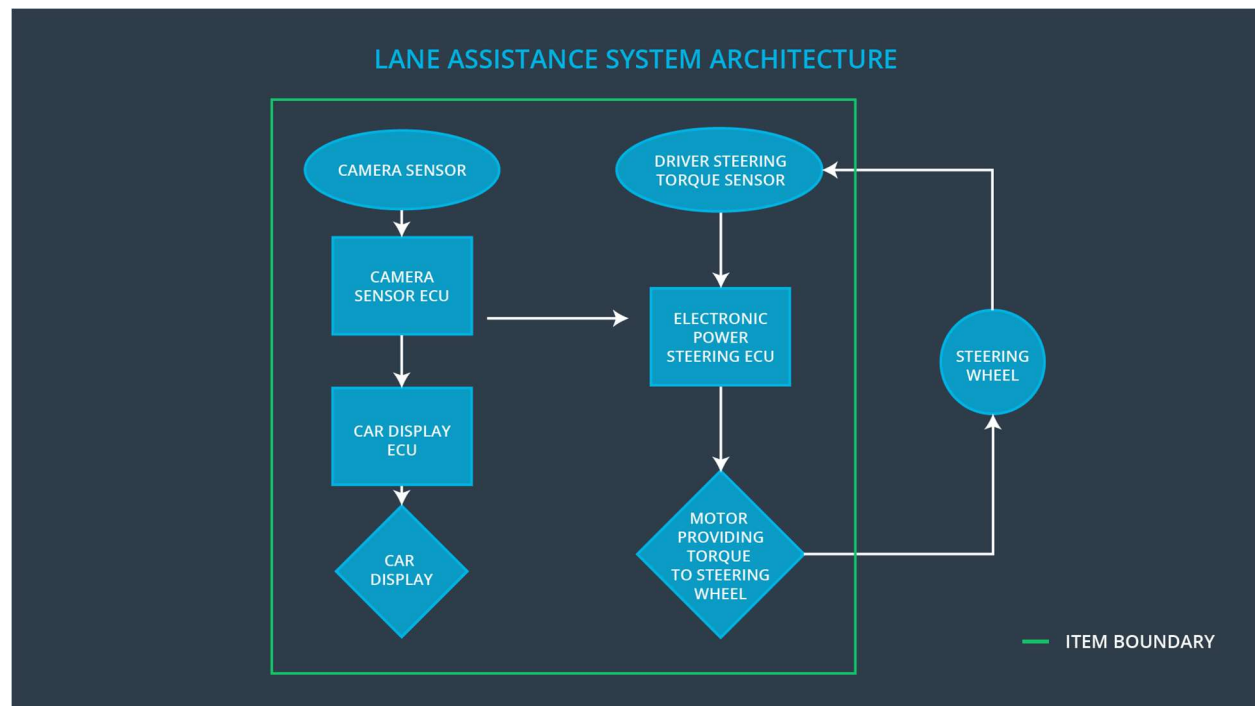
The two main function of this item are:

- **Lane departure warning function:** When the driver drifts out toward the edge of the lane, the steering wheel provides vibration to warn the driver. The vehicle will move the steering wheel backward and forward to produce the necessary vibration.
- **Lane keeping assistance function:** When the driver drifts out toward the edge of the lane, this functionality will move the steering wheel so that the wheels turn toward the center of the lane. It should apply steering torque in order to stay in the ego lane (this is the lane where the car is at present.)

The item functionalities are implemented by the following subsystem:

- **Camera subsystem:** This subsystem is composed by two components:
 - Camera sensor
 - Camera sensor ECU (Electronic Control Unit)
 -
- **Electronic Power Steering subsystem:** This subsystem is composed by three components:
 - Driver Steering Torque Sensor.
 - Electronic Power Steering ECU.
 - Motor Providing Torque to Steering Wheel.
 -
- **Car Display subsystem:** This subsystem is composed by two components:
 - Car Display ECU
 - Car Display

The following diagram shows the interaction between different subsystems.



When the camera senses that the vehicle is leaving the lane, the camera sends a signal to the electronic power steering system asking to turn and vibrate the steering wheel.

The camera sensor will also request that a warning light turn on in the car display dashboard. That way the driver knows that the lane assistance system is active.

If the driver uses a turn signal, then the lane assistance system deactivates so that the vehicle can leave the lane. The driver can also turn off the system completely with a button on the dashboard.

The driver is still expected to have both hands on the steering wheel at all times. The electronic power steering subsystem has a sensor to detect how much the driver is already turning. The lane keeping assistance function will merely add the extra torque required to get the car back towards center. The extra torque is applied directly to the steering wheel via a motor.

The Lane Assistance System does not include the following functionalities:

- Adaptive Cruise Control
- Automatic Parking
- Blind Spot Monitoring
- Tire Pressure Monitoring
- Pedestrian Protection

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?]

This project goals are:

- **Identify risk and hazardous situations in the Lane Assistance system components malfunction causing injuries to a person.**
- **Evaluate the risks of the hazardous situations.**
- **Lower the risk of the various malfunctions to a reasonable level acceptable by current society and existing safety policies.**

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

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	All Team Members	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

]

In order to ensure a safety culture, the following characteristics needs to be observed:

- **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.

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, 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.

]

This section defines the roles and responsibilities between parties involved in the Lane Assistance project to ensure its development in compliance with ISO 26262.

- **Functional Safety Manager - Item Level:** Pre-audits, plans the development phase for the Lane Assistance item.
- **Functional Safety Engineer - Item Level:** Develop prototypes, integrate subsystems combining them into the Lane Assistance item from a functional safety viewpoint.
- **Project Manager - Item Level:** Allocates the resources needed for the item.
- **Functional Safety Manager - Component Level (Soumen):** Pre-audits, plan the development for the components of the Lane Assistance item.
- **Functional Safety Engineer - Component Level (Soumen):** Develop prototypes and integrate components conforming the Lane Assistance item.
- **Functional Safety Auditor:** Make sure the project conforms to the safety plan.
- **Functional Safety Assessor:** Judges where the project has increased safety.

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 purpose of the confirmation measures is:

- Ensure the Lane Assistance project conforms to ISO 26262.
- Ensure the Lane Assistance project makes the vehicle safer.

The Confirmation review ensure the projects comply 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. A Functional safety audit makes sure the actual implementation of the project conforms to the safety plan. A Functional safety assessment confirms that the plan, design and developed product 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.