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
2017-12-26	1.0	Sven Eriksson	Initial release
2017-12-26	2.0	Sven Eriksson	Updated Measures after feedback

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?]

A safety plan provides an overall framework for a functional safety project. It defines roles and responsibilities in order to prevent that important steps are missed. By documenting it is possible to later use it for audits and to show that the standard was followed. It would also be used evidence in the functions safety case.

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?

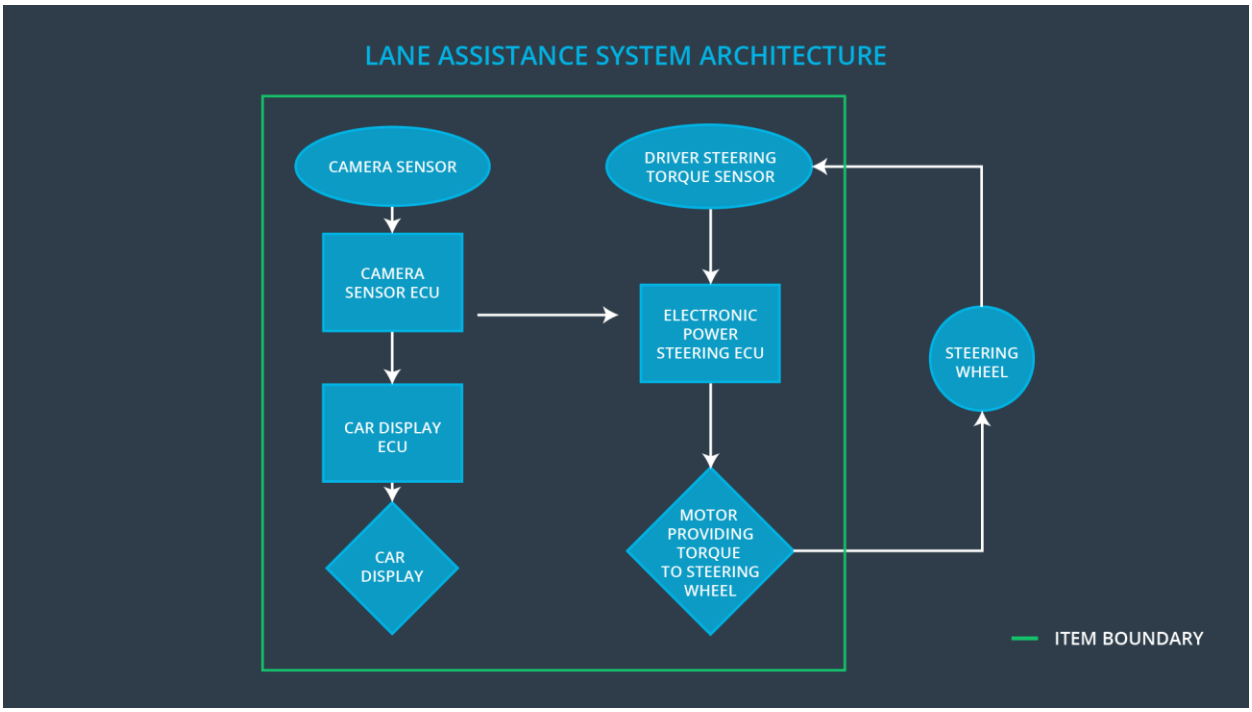
OPTIONAL
Optionally, include information about these points as well. These were not included in the lectures, but you might be able to find this information online:

- **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 is a lane assistance system with two main functions, lane departure warning and lane keeping assist. The lane departure warning will vibrate the steering wheel to notify the driver of

imminent unintended lane departure. The lane keep assist functionality is to turn the wheels in such a way so that the vehicle moves towards the center of the lane.



Taken from Udacity's project folder

The steering wheel is not included in this item, but the camera with its ECU, the display with its ECU, and the electronic steering ECU with its sensors and motors are included within the lane assistance item.

All subsystems within the lane assisting item are responsible and used for all functions. See the figure above to see the different parts of the lane assisting item on a very high level.

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?]

We are trying to reduce the risk of the lane assistance function down to acceptable levels. We are also documenting this process in order to convince ourselves and others that we have

reduced the risk to acceptable levels. The documentation also aids us in the case that we change something in the system later on, in that case we might not have to redo all the work.

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
]

Our company should prioritize safety over productivity and have well defined process that help us develop safe products. We should reward focus on safety and penalize shortcuts among our employees. Teams taking design decision should be accountable by having design decisions traceable back to the team who made the decision.

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
]

In this project the entire concept phase is included in the scope, as is product development at system and software level.

The concept phase consists of item definition, initiation of the safety lifecycle, hazard analysis and risk assessment, and functional safety concept.

Both product development at hardware level and production and operation are outside the scope of this project.

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.**

]
The development interface agreement is meant to clarify responsibility to avoid disputes between the two parties. It clarifies liability and who has responsibility to fix safety issues.

The OEM is responsible for the function design as well as the functional safety work on a item level. We, the tier 1, have a functional safety manager and functional safety engineers on component level. We are responsible for the functional safety work on component level for some or all of the previously mentioned components. The extent of our responsibility needs to be clarified together with the OEM so that both parties are in agreement. This is the purpose of the development interface agreement.

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 main purpose of confirmation measures is to make sure that the design really does improve safety. These measures shall also make check if the processes used complies with the functional safety standard and that the project follows the safety plan.

Confirmation review: A review of the project that makes sure that project is planned and executed is such a ways so it complies with ISO 26262. The review is done by someone independent from the project team.

Functional safety audit: A review of the project to ensure that the safety plan is being followed during execution of the project.

Functional safety assessment: An assessment of the plans, design and the product to check if they 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.