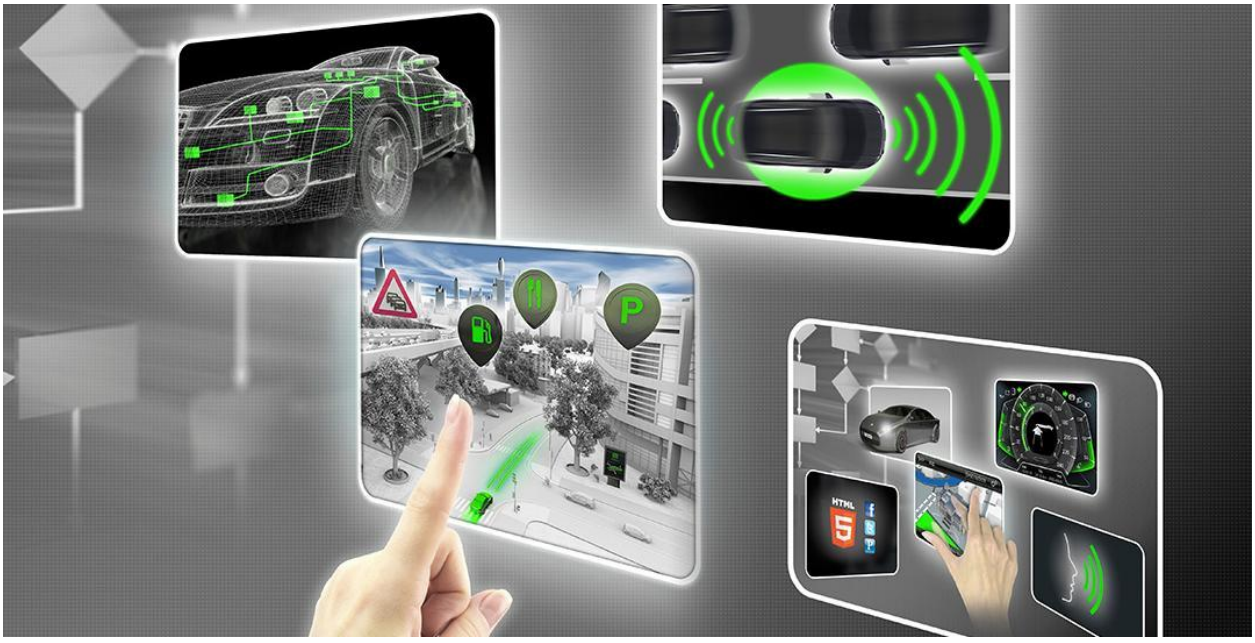
Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21



Document history

Date	Version	Editor	Description
6/6/2018	1.0	Jason Kang	Iniitial 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]

Introduction

Purpose of the Safety Plan

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

The purpose of this document is to ensure that safety is considered throughout the self-driving car development process. Self-driving cars are complex systems that have many components that have to be integrated with each other. This document ensures that no safety concerns are overlooked.

In addition, this document acts as documentation to show that best practices were followed and steps were taken to reduce risk to acceptable levels.

Scope of the Project

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

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**

]

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?]

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	Safety Manager	3 months prior to main assessment

external functional safety assessor		
Perform functional safety assessment	Safety Asessor	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
]

We stress the importance of safety at our company. First, we have a well documented procedure for making design decisions. This ensures that our processes are well thought out, and stresses that employees and teams are responsible for the decisions they make. Furthermore, there is a process for escalating safety concerns anonomously or not to a dedicated safety officer who ensures that actions are taken on safety concerns. The safety officer and and independent audit teams have quaterly safety reviews in which team leads and auditors discuss any revealed safety concerns. They also nominate a quarterly safety hero award which recognizes a team who made an exceptional contribution to system safety in the past quarter.

Safety Lifecycle Tailoring

This is a modification to an existing product. Changes will only be made to the software part of the system. Software changes will also effect the system level. However, hardware will not be changed so hardware steps are out of scope.

This document includes comcept and product development steps, but will not steps after it is released for production. Those steps will be handled by another team in another document. In other words, the safety life cycle includes item defintion, hazards/risk assessment, functional safety concept, product development (of system and software) safety validation, functional safety assessment, and release to production.

Roles

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 development interface agreement is meant to define the roles and responsibilities between our company and OEM company. This helps to ensure that both parties knows what the other party is doing and ensure that what is delivered matches expectations.

The OEM will provide a functioning lane assistance system complete with fully functioning hardware and software. Our company will analyze the sub-sytems and determine areas of improvement. We will provide a report of recommended areas of improvement and set up a meeting to discuss the findings. Actions from that meeting will drive what subsystems need to be updated for improved functional safety. These actions will be wrapped up in a new safety plan so that we can make the required improvements.

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?

]

1. Confirmation measures are meant to ensure that ISO 26262 is actually being followed, and to ensure that any changes made make the vehicle safer.
2. A confirmation revew checks to make sure ISO 26262 is being followed.
3. A functional safety audit checks to make sure the previously defined safety plan is being followed.
4. A functional safety asessment is a check to confirm that new developments improve 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.