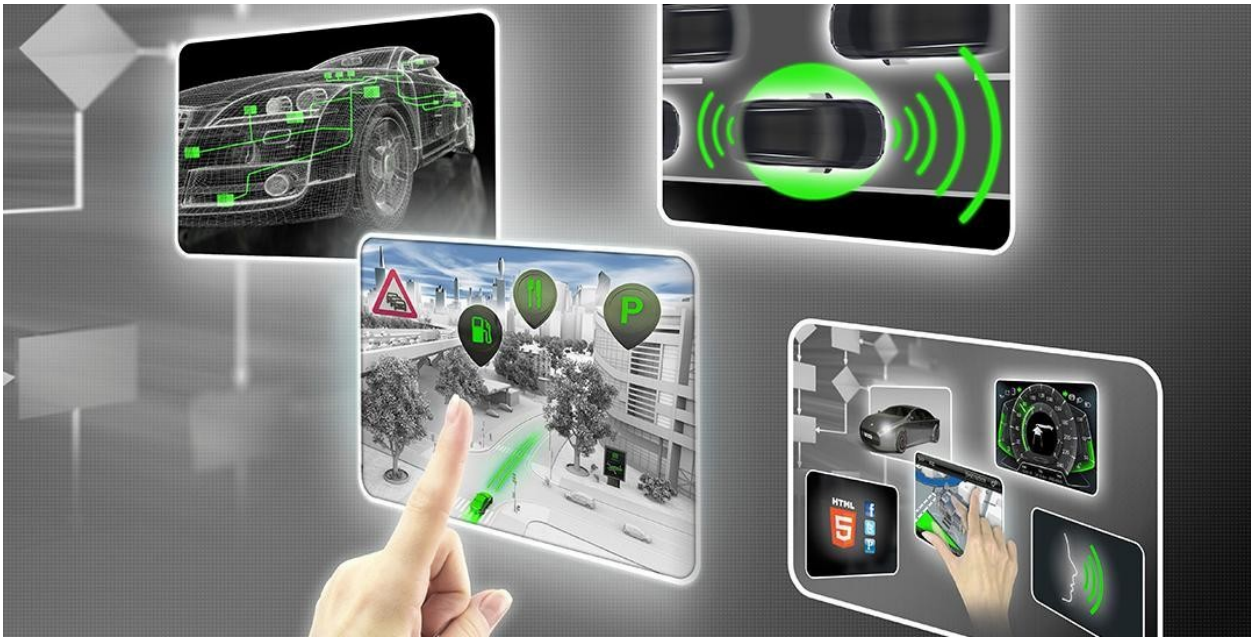
Elektrobit

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
31.05.2018	1.0	Description	Safety Plan for Lane assistance

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

Safety plan documents the use case and the roles and responsibilities of carrying out a safety analysis for a E/E system according to ISO 26262 specifications. It also includes task needed to be performed and tracks the schedule of the associated tasks. The end product is a document stating a particular system under development has been designed in a way to be safe and reduce the impact of a hazard if occurs.

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

The system under test is the Lane assistance system. Lane assistance system includes two main functionalities namely

- **Lane keep assist**
- **Lane departure warning**

The lane assistance system assists the driver in keeping the lane and warns the driver if the vehicle is deviating from the current lane.

The lane keep assist assist the driver by keeping the lane, reducing the drivers effort and does so only when the drivers hands are on the steering wheel.

The lane departure warning warns the driver if the vehicle is deviating from the current lane into the adjacent lanes .

The lane assistance systems work on detecting the lane lines from a camera. The system for lane assistance would work given good infrastructure in the roads namely visible lane markings. The lane assistance system is limited to work in good visible conditions and would not work under snowy and heavy rainy conditions. The driver is expected to not get any assistance from the lane assistance system under snowy or heavy rain conditions.

Both the functions are a mere assistance functions which assumes the driver is always in control of the steering wheel. The lane assistance function should not be assumed to be autonomous driving functions. Any Deviation from the above mentioned behaviour and the results of a mishappen, then the driver would be responsible for the consequences.

Goals and Measures

Goals

The goal of the current document is to document a safety plan for a lane assistance system to adhere with ISO 26262 standards and make the system functionally safe for release into public roads.

Measures

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

The compancy safety culture has the following points

- **Clear roles and resposibilities definition**
- **Highest priority to safety**
- **Experienced safety manpower**
- **Clear development process adhering to safety**
- **Flat hierarchy for open communication**
- **Efficient documentation of roles and resposibilities**

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 of this document
]

The scope of the safety concept and its life cycle

- **Ceoncept phase**
- **Product development at the system level**
- **Product development at the software level**

The safety lifecycle does not inlude the

- **Product development at the hardware level**

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?**
   Clearly defines the roles and responsiblities assigned to between various teams within or outside the company. The DIA also helps in keeping a record of performed tasks so in case of a malfunction or a recall, appropriate teams can be notified and issues could be fixed faster.

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.**

   Being a tier 1 company the responsiblities include developing a functionally safe system (e.g Lane assitance system) as per the requirements of the OEM. OEM resposibilites include using the developed function and to integrate into the vehicle system and testing the complete vehicle system along with the developed sub system is functionally safe.

Confirmation Measures

[Instructions:
Please answer the following questions:

1. **What is the main purpose of confirmation measures?**

   Confirmation measures takes care whether the development process adheres to the safety plan development during the concept phsae and also checks how close the project progress with the functional safety plan.
2. **What is a confirmation review?**

   Ensures that the project complies 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.

3. **What is a functional safety audit?**

   Checking to make sure that the actual implementation of the project conforms to the safety plan is called a functional safety audit.
4. **What is a functional safety assessment?**

   Confirming that plans, designs and developed products actually achieve functional safety is called a functional safety assessment.

]

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.