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
24-08-2017	1.0	Ahmed Ghazal	Initial 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]

Confirmation Measures

Introduction

Purpose of the Safety Plan

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

The safety plan ensures that functional safety will be achieved throughout the project by defining roles and specific responsibilites to every team member,

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 considered in this safety plan is the lane assistance item. Its function is providing assistance to the driver when the car starts moving away from the center of the lane while the turn signal isn't active, which means that the driver probably got distracted and didn't mean to change lanes.

What are its two main functions? How do they work?

The lane assistance system has two main functions:

- **Lane Keeping Assistance**
- **Lane Departure Warning**

When the lane assistance system is active, and the car starts departing the lane without a turn signal, the lane departure warning will vibrate the steering wheel to notify the driver that the car is leaving the lane, and the lane keeping assistance will move the steering wheel so that the car returns to the center of the lane.

Which subsystems are responsible for each function?

The lane keeping assistance function is the responsibility of the Electronic Power Steering Subsystem, while the lane departure warning is the responsibility of both the Electronic Power Steering Subsystem and the Display Subsystem.

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

The item contains three sub-systems: Camera Subsystem, Electronic Power Steering Subsystem and the Display Subsystem. The steering wheel is the only element outside the system boundaries.

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 of this project is to specify functional requirements which will ensure the safety of the system in case a malfunction occurs in the lane assistance function.

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 external functional safety assessor	Safety Auditor	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
]

The company creates a safety culture on all levels, starting from software, to system and functional safety. This culture is maintained through different trainings and thorough code reviews. Also, project managers make sure to communicate clearly to all team members that safety has the number one priority in all projects, so achieving functional safety is highly rewarded, and on the other hand, any activity which jeopardizes safety is penalized.

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
]

This document covers the following phases of the safety lifecycle:

- **Concept phase**
- **Product Development at the System Level**
- **Product Development at the Software Level**

The following phases are out of the scope of this document:

- **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?**
   To define the roles and responsibilities of all companies involved in the product development (OEMs, Tier 1 Suppliers, Tier 2 Suppliers). Also to avoid disputes in the planning and development phases.

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 responsibilities:

- **Providing a functioning lane assistance system.**
- **Providing all related documentation.**

Company responsibilities:

- **Analyze the provided system from functional safety point of view.**
- **Perform hazard analysis and risk assessment to set a safety goal.**
- **Modify the sub-systems to achieve the required safety goal.**

Confirmation Measures

[Instructions:
Please answer the following questions:

1. **What is the main purpose of confirmation measures?**
   To ensure that the functional safety project conforms to ISO 26262, and that the design actually makes the vehicle safer.
2. **What is a confirmation review?**
   A confirmation review is performed by an independent person not involved in the project, to ensure that all measures and procedures were compliant with ISO 26262.
3. **What is a functional safety audit?**
   A functional safety audit ensures that the safety plan is followed throughout all project steps.
4. **What is a functional safety assessment?**
   A functional safety assessment confirms that the project plan, design and product development actually achieves 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.