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

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?]
Safety project provides an overall framework for functional safety project.

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**

]

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		Constantly
Create and sustain a safety culture		Constantly
Coordinate and document the planned safety activities		Constantly
Allocate resources with adequate functional safety competency		Within 2 weeks of start of project
Tailor the safety lifecycle		Within 4 weeks of start of project
Plan the safety activities of the safety lifecycle		Within 4 weeks of start of project

Perform regular functional safety audits		Once every 2 months
Perform functional safety pre-assessment prior to audit by external functional safety assessor		3 months prior to main assessment
Perform functional safety assessment		Conclusion of functional safety activities

Safety Culture

[Instructions:
High priority: company set safety as the highest priority among design decisions;
Accountability: processes ensure accountability such that design decisions are traceable back to the people and teams who made the decisions;
Rewards & Penalties: support the achievement of functional safety, and 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: design and management processes is clearly defined;
Resources: employee with appropriates skills;
Diversity: intellectual diversity is sought after, valued and integrated into process;
Communication: company have clear communication channel, and 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

In scope:

- **Concept phase;**
- **Product development on system level;**
- **Product development on software level;**

Out scope:

- **Product development on 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?**

   Make sure all parts involved are developing safe vehicles in compliance with iso 26262.

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 is responsible for describing details requirements, system requirements on lane assistance system, and appointment functional safety auditor and assessor. Our company (Tier1) is responsible for provide final products to OEMs based on their requirements and the product will be design and produced as follow ISO 26262 standard.

]

Confirmation Measures

[Instructions:
Please answer the following questions:

1. **What is the main purpose of confirmation measures?**
   - **Function safety process conforms to iso 26262**
   - **Project execution follow the safety plan**
   - **Design really improve safety**
2. **What is a confirmation review?**
   To ensure project follow complies with ISO 26262, an independent person would review the work to make sure ISO 26262 is being worked.
3. **What is a functional safety audit?**
   Make sure that actual implementation of the project is conforms to the safety plan.
4. **What is a functional safety assessment?**
   Confirming that plans, designs 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.