Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
2018.05.25	1.0	A. Fuchs	Initial revision

Table of Contents

Introduction

Purpose of the Safety Plan

The purpose of the Safety Plan is to achieve a safe system. It defines the roles and outlines steps that are required to achieve functional safety.
The scope of Functional Safety is to reduce risk of potential hazardous situations of the system to levels acceptable to society.

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

The system is a lane assistance system as a part of a vehicle. The lane assistance system issues a warning if the vehicle is leaving the lane or/and steers back to the center of the lane. The main functions are:

- **Lane departure warning**
  If the vehicle is leaving the lane without lane change indicators activated the system assumes that the driver is distracted or not in condition to steer the vehicle safely. It issues a warning by a haptic signal through vibration of the steering wheel.
- **Lane keeping assistance**
  The vehicle steers autonomous back to the center of the lane to keep a safe driving state.

Which subsystems are responsible for each function?

Subsystems:

- Camera system
  Responsible for lane departure warning
- Electronic Power Steering system
  Responsible for lane keeping assistance
- Car display system
  Responsible for lane departure warning (maybe by additional visual warning)

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

Inside the item lane assistance system are the following subsystems:

- Camera system
- Electronic Power Steering system
- Car display system

Outside the item is the following subsystem:

- Steering wheel

Goals and Measures

Goals

[

The major goal is to achieve functional safety of the lane assistance functions. Thereby the risk of hazardous failures is mitigated to a minimum (to a level acceptable by society).

Measures

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 Manager	3 months prior to main assessment
Perform functional safety assessment	Safety Assessor	Conclusion of functional safety activities

Safety Culture

The Safety Culture of my company makes sure that safety is the highest priority. All of our company processes ensure accountability that design decisions are traceable back to the responsible persons.
We make sure to have well defined processes and detailed documentation of each step of the Safety Plan. It is important to have independence between the design and development teams and the safety audit team.
The different roles within the project are occupied by employees with appropriate skills to master the tasks.
We reward the achievements of functional safety and careful documentation and on the other hand penalize any shortcut that could jeopardize functional safety.
Communication between all team members is considered as highly important.
We take care of diversity is integrated in all processes a

Safety Lifecycle Tailoring

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

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

1. **What is the purpose of a development interface agreement?**

- Avoid disputes between OEMs, tier 1 and tier 2 suppliers
- Resolving issues of liability
- Makes clear who should fix safety issues

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.**

]

Responsibility:

- Functional safety of the sub systems and the lane assistance system.

Confirmation Measures

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

To check if the processes comply with the functional safety standard, the project execution if following the safety plan, design really improves functional safety.

2. **What is a confirmation review?**

A confirmation review ensures compliance with ISO26262

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

A functional safety audit is required to evaluate if actual implementations are conform to the Safety Plan.

4. **What is a functional safety assessment?**

The functional safety assessment is the confirmation that plans, designs and developed products 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.