Elektrobit

UDACITY

Safety Plan Lane Assistance

Document history

Date	Version	Editor	Description
31.08.2017	1.0	Klemens Esterle	Initial Version

Table of Contents

Introduction

Purpose of the Safety Plan

The safety plan shows roles and dresponsibilities and outlines the steps taken to achieve functional safety.

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

What is the item in question, and what does the item do?

The item in question is the Lane Assistance System. It alerts the driver once he is unintentionally drifting away from the center of the lane and steers the vehicle back to the center of the lane.

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

The function is active if a driver drifts torwards lane edge. It's two main functions are a Lane departure warning function and a lane keeping assistance function.
The lane departure function will vibrate the steering once the situation is detected.
The lane keeping assistance function will then move the steering wheel so that the wheels turn towards the center of the lane.

Which subsystems are responsible for each function?

The Lane Assistance System consists of three subsystems. The Camera subsystem, the Electronic Power Steering subsystem and the Car Display subsystem.
The Camera subsystem is responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake.
The Electronic Power Steering subsystem is responsible for measuring the torque provided by the driver and then adding an appropriate amount of torque based on a lane assistance system torque request.
The Car Display substystem displays when the Lane Assistance System is active.

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

Camera subsystem, Electronic Power Steering subsystem and the Car Display subsystem are all parts of the system. The steering wheel is not part of the system.

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 is to methodically reduce risks of the Lane Assistance Function that could harm people's health.

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

Safety Culture

Our organisation has clear policies and strategies to support the development, production and operation of safe systems.
First of all, safety has the highests priority among competing constraints like costs and productivity. Our well-defined implemented processes ensure accountability such that design decisions are traceable back to the decision-making teams. Not only does our organization motivates and support the achievement of functional safety, but also we penealize any shortcut that jeopardizes the safety or quality of our product.
When setting up projects, we make sure to allocate the necessary resources to achieve functional safe products by establishing a junior-senior system for all safety manegement roles, so that there is always seniority available for every task.

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
]

As the described item is a modified version of an already existing function, this safety plan will only include the parts imparcted by the new functionality.

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

The DIA defines the roles and responsibilities between companies involved in developing a product (such as OEM and Tier 1).

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.**

Coming from the system requirements stated by the OEM, our company will develop and produce the system ensuring functional safety of this system.
]

Confirmation Measures

[Instructions:
Please answer the following questions:

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

Confirmation measures confirm that the design really improves safety.

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

The confirmation review ensures that the project complies with ISO 26262. As the product is designed and developed, the Safety Auditor (independent person) reviews the work every two months to make sure the functional safety stand is being followed.

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

The safety audit is the person performing the confirmation review. He makes sure the project conforms to the saqfety plan.

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

A safety assessment confirms 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.