



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
01.04.2018	1.0	Siddarth Kothiwale	First Try

Table of Contents

[Document history](#)

[Table of Contents](#)

[Introduction](#)

[Purpose of the Safety Plan](#)

[Scope of the Project](#)

[Deliverables of the Project](#)

[Item Definition](#)

[Goals and Measures](#)

[Goals](#)

[Measures](#)

[Safety Culture](#)

[Safety Lifecycle Tailoring](#)

[Roles](#)

[Development Interface Agreement](#)

[Confirmation Measures](#)

Introduction

Purpose of the Safety Plan

Answer: Safety Plan first defines the broad scope for functional safety and steps needed and also roles and responsibilities of the people involved so that functional safety can be achieved

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:

Answer: The system under consideration is the lane assistance system

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

Answer: The item will alert the driver if the vehicle leaves the lane by vibrating the steering and then helps the driver in bringing the car back to the center.

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

Answer: When the driver drifts towards the edge of the lane, two things will happen:

1. the lane departure warning function will vibrate the steering wheel
2. the lane keeping assistance function will move the steering wheel so that the wheels turn towards the center of the lane

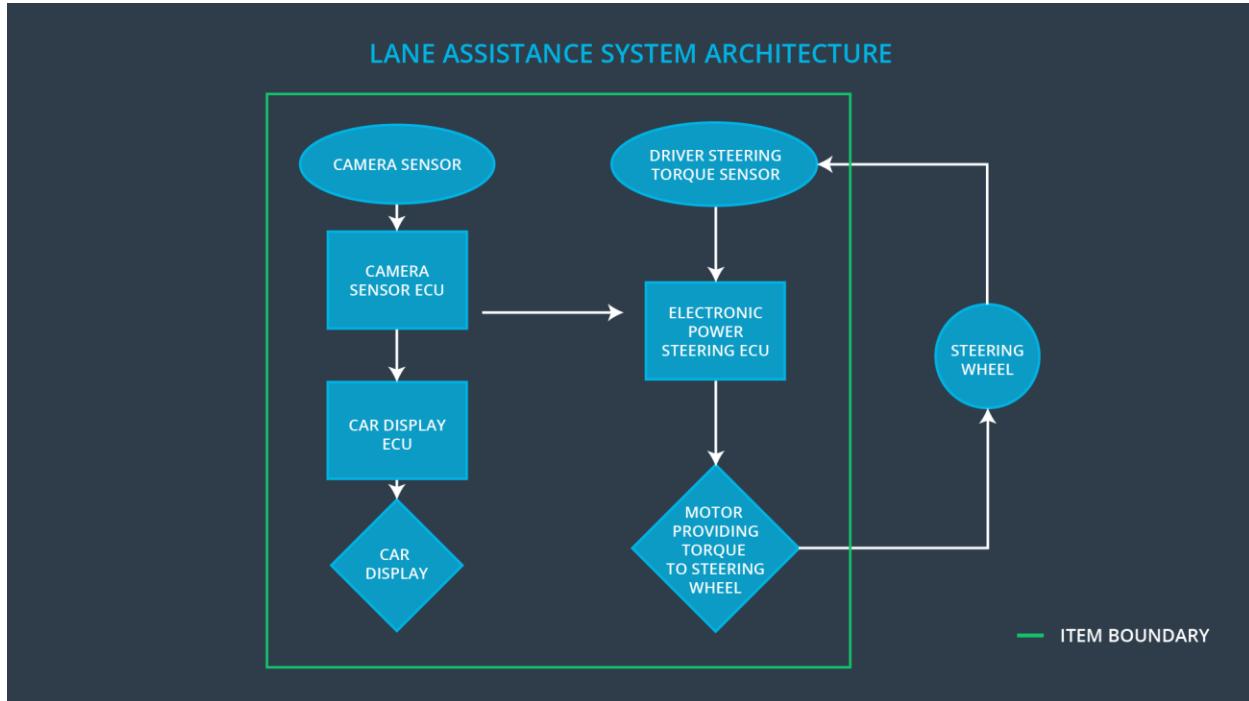
Which subsystems are responsible for each function?

1. Camera system

2. Electronic Power Steering system
3. Car Display system

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

Answer:



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?]

Answer: The goal of this project is functional safety. We are trying to bring down the risks involved in the driver assistance system to acceptable level.

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	Safety Auditor	Constantly

Create and sustain a safety culture	Safety Auditor	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	Test 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

[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

]

Answer:

- High priority: safety has the highest priority among competing constraints like cost and productivity
- Accountability: processes ensure accountability such that design decisions are traceable back to the people and teams who made the decisions
- Rewards: the organization motivates and supports the achievement of functional safety
- Penalties: the organization 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: company design and management processes should be clearly defined
- Resources: projects have necessary resources including people with appropriate skills
- Diversity: intellectual diversity is sought after, valued and integrated into processes
- Communication: communication channels 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

]

Answer: Safety Lifecycle Tailoring aims at using as many pre-existing steps in the safety lifecycle as possible and concentrating only on the parts impacted by the changes.

The following phases are in scope:

- 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?

Answer: A DIA (development interface agreement) defines the roles and responsibilities between companies involved in developing a product. All involved parties need to agree on the contents of the DIA before the project begins.

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.

]

Answer: The Tier-1 supplier will analyze and modify the subsystem in the roles of Functional safety engineer and functional safety manager.

SafetyManager: The roles include writing the safety plan and monitoring

Safety Engineer: Architectural design and implementation

Confirmation Measures

[Instructions:

Please answer the following questions:

1. What is the main purpose of confirmation measures?

Answer: Confirmation measures serve two purposes:

- that a functional safety project conforms to ISO 26262, and
- that the project really does make the vehicle safer.

2. What is a confirmation review?

Answer: 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?

Answer: 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.