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
14/5/2018	1.0	Aakash	Started the documentation on 14th May 14, 2018

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

A safety plan provides an overall framework for a functional safety project. The safety plan also defines responsibilities between the players involved in the project like OEM's, Tier -1 etc.

Therefore, it ensures that everybody knows what to do and that somebody is covering every task.

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

Discuss these key points about the system:

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

The item discussed here is Lane Assistance System. It helps the driver to stay in the lane if the driver tried to change lanes unintentionally.

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

A lane assistance system generally has two functions:

- **lane departure warning -** vibrates the steering wheel
  The lane departure warning function works by applying an oscillating steering torque to provide the driver a haptic feedback.
- **lane keeping assistance -** moves the steering wheel so that the wheels turn towards the center of the lane
  The lane keeping assistance function works by applying the steering torque when active in order to stay in ego lane.

Which subsystems are responsible for each function?

The item functionalities are implemented by the following subsystem:

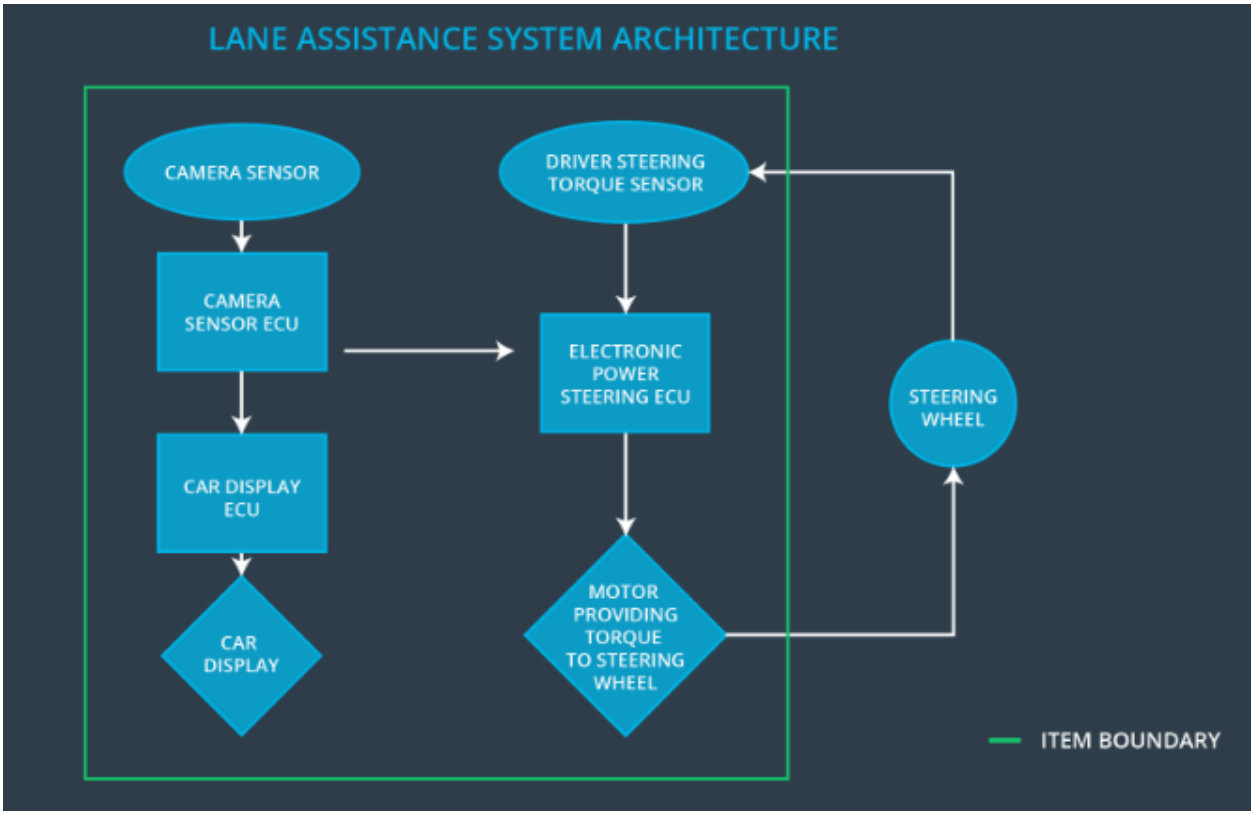
- **Camera subsystem**: This subsystem is composed by two components:
  - Camera sensor
  - Camera sensor ECU (Electronic Control Unit)
- **Electronic Power Steering subsystem**: This subsystem is composed by three components:
  - Driver Steering Torque Sensor.
  - Electronic Power Steering ECU.
  - Motor Proving Torque to Steering Wheel.
- **Car Display subsystem**: This subsystem is composed by two components:
  - Car Display ECU
  - Car Display

The camera subsystem helps in keeping in the lane by detecting the lanes. The power steering subsystem helps to turn towards the center of the road. And display subsystem helps to display lane departure warning.

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

The item here is lane assistance system/lane assistance item.

Lane Assistance System boundary:



The item boundary is drawn to include three sub-systems:

- Camera system
- Electronic Power Steering system
- Car Display system

Goals and Measures

Goals

This project goals are:

- Identify risk and hazardous situations in the Line Assistance system components malfunction causing injuries to a person.
- Evaluate the risks of the hazardous situations.
- Lower the risk of the malfunctions to a reasonable levels acceptable by current 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	All team members	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 Manager	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 Manager	Conclusion of functional safety activities

Safety Culture

Following are the characteristics that describe my company's safety culture:

- 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

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

[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

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

- The 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.
- The DIA also specifies what evidence and work products each party will provide to prove that work was done according to the agreement.
- The ultimate goal is to ensure that all parties 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.**

The responsibilities for Lane Assistance System would be:

Role	Org
Functional Safety Manager- Item Level	Planning, coordinating and documenting of the development phase of the safety lifecycle.
Functional Safety Engineer- Item Level	Product development, Product Integration, Testing the hardware, software and system levels.
Project Manager - Item Level	Project Management, Resource

	management, appoint safety manager or act as one.
Functional Safety Manager- Component Level	Planning, coordinating and documenting of the development phase of the safety lifecycle.
Functional Safety Engineer- Component Level	Product development, Product Integration, Testing the hardware, software and system levels.
Functional Safety Auditor	Ensures that the design and production implementation conform to the safety plan.
Functional Safety Assessor	Independent judgement as to whether functional safety is being achieved via a functional safety assessment.

To be precise:

ROLE	JOB DESCRIPTION
Safety Auditor	makes sure that the project conforms to the safety plan
Test Manager	planning and overseeing testing activities
Safety Manager	pre-audits, plans the development phase
Safety Assessor	judges whether the project has increased safety
Project Manager	allocates resources as needed
Safety Engineer	develops prototypes, integrates sub systems into larger systems

Source: Udacity carnd nanodegree lectures

Confirmation Measures

1. What is the main purpose of confirmation measures?

- Processes comply with the functional safety standard
- Project execution is following the safety plan
- Design really does improve safety

2. What is a confirmation review?
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?
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.