Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.0

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
09.02.2018	1.0	Sascha Moecker	Initial Submission

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]

Inhalt

Introduction

Purpose of the Safety Plan

[Instructions: Answer what is the purpose of a safety plan?]

The safety plan provides a high-level overview about the item under development and its approach to gain functional safety. It consists of the following parts:

- The **Introduction** section gives an overview of the project and discusses the documentation that will be included in the entire report.
- The **Item Definition** describes which particular vehicle system will be under analysis.
- **Goals and Measures** discuss the goals of the project and what activities will be included.
- **Safety LifeCycle Tailoring** mentions which parts of the V model will be included in the project.
- **Resources Required In Project** defines the different roles on the team.
- **Supporting Process Management** talks about the systems engineering management methods to be used.
- **Project Schedule Plan** gives a calendar of when tasks will be completed.
- **Confirmation Measures** reports what will be done to prove that functional safety has been 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:

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.]**

The item in question is the Lane Assistance feature. It is part of the Advanced Driver Assistance System (ADAS) and shall help the driver to keep in his lane during driving. The lane is detected by the camera which recognize lane boundaries using CV techniques.

It will get active when the driver drifts towards the edge of the lane. Those two things will happen:

- the **lane departure warning function** will vibrate the steering wheel
- the **lane keeping assistance function** will move the steering wheel so that the wheels turn towards the center of the lane

The Lane Assistance System will hence have two functions:

- Lane departure warning → Already done during the classroom videos
- Lane keeping assistance → Scope of this safety analysis.

The **lane departure warning** quickly moves the steering wheel back and forth to create a vibration.
The **lane keeping assistance functionality** will automatically **assist** the driver by turning the steering wheel towards the center of the lane.

It consists of the subsystems:

- Camera Sensor: Takes an image of the street in the front of the vehicle
- Camera ECU: Detects the lane boundaries and the lane from the images
- ECU Power Steering: Computes based on the detected lane the vibration (lane departure warning) and the torque of the steering wheel (lane keeping assistance)
- Driver steering torque sensor: Detects the current torque of the steering wheel
- Motor of steering wheel: Is responsible for actually moving the steering wheel

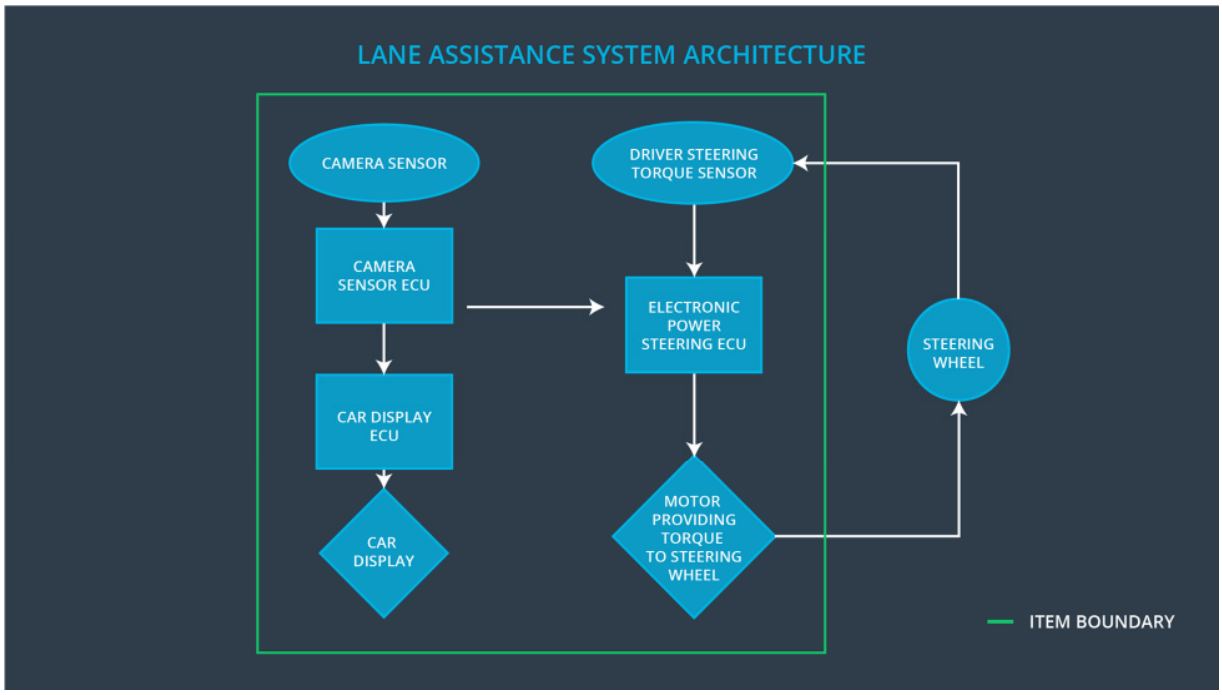

Image 1: Lane Assistance System Architecture

- Camera Subsystem: Responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake
- Lane Assistance: Functionality that turns the steering wheel back towards the center of the lane if the driver starts to drift away from center
- Electronic Power Steering Subsystem: 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
- Lane Departure Warning: Functionality that vibrates the steering wheel when the driver drifts away from center by mistake
- Lane Keeping Assistance: The name of the item under consideration in the functional safety module

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?]

This analysis of the lane assistance feature and its documentation provides a reference when modifying a system. It elaborates on how the system was designed and tested. It proves that best practices was followed.

The main goal in functional safety is to reduce risk to acceptable levels. To prove that the design solutions actually lower risks, we state arguments in this documentation. Here we provide evidence that the project has made the vehicle safer.

The evidence includes all the ISO 26262 documentation such as the safety plan, design plans, functional safety concept, technical safety concepts, as well as evidence documenting testing and integration.

The safety case discusses what elements are added to the system in order to make it safe. It provides testing evidence that shows the system functioning properly. The document provides evidence that what has been added to the system really does make the vehicle safer.

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, in	Constantly

	particular the Safety Manager	
Coordinate and document the planned safety activities	Safety Manager	
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 Auditor	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]

An established safety culture guides the entire development process and guarantees that safety has always highest priority. A good culture helps overcoming tough time plans and sloppy code as everyone shall not hesitate to report behavior which is against the safety culture. Point which define a good safety culture are:

- **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]

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

[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?**
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.]**

1. 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.

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.

Major sections of a DIA:

- Appointment of customer and supplier safety managers
- Joint tailoring of the safety lifecycle
- Activities and processes to be performed by the customer; activities and processes to be performed by the supplier
- Information and work products to be exchanged
- Parties or persons responsible for each activity in design and production
- Any supporting processes or tools to ensure compatibility between customer and supplier technologies

2. The OEM is supplying a functioning lane assistance system, our company needs to analyze and modify the various sub-systems from a functional safety viewpoint.

Confirmation Measures

[Instructions:
Please answer the following questions:

1. **What is the main purpose of confirmation measures?**
2. **What is a confirmation review?**
3. **What is a functional safety audit?**
4. **What is a functional safety assessment?]**

1. Confirmation measures serve two purposes:
   - A functional safety project must conform to ISO 26262, and
   - The project really does make the vehicle safer.

2. 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. 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. 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.