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
18-Dec-2017	1.0	Carsten MIELENZ	First version
24-Dec-2017	1.1	Carsten MIELENZ	Updated according review suggestions

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

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

The safety plan provides the overall framework for the Lane Assistance item.

- It serves as guide to achieve functional safety.
- It defines and assigns the roles & responsibilities (R&R) within the project.
- The outputs of design / implementation phase will be checked against the safety plan.

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?

The Lane Assistance item alerts the driver when vehicle departed from its lane and corrects the steering of the vehicle in order to go back to the center of the lane if there was no lane change considered by the driver.

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

The Lane Assistance item has two functions.
These will be performed in the case that there was no lane change considered by the driver (which is done by setting the direction indicator)

Function 1: Lane Departure Warning (LDW)
The LDW function oscillates the steering wheel quickly back and forth giving a haptic feedback to the driver in case the vehicle departed from its lane. It also switches on a warning lamp for lane departure inside the vehicle's display.

Function 2: Lane Keeping Assistance (LKA)
The LKA function assists the driver to turn the steering wheel towards to the center of the lane in case the vehicle departed from its lane.

Which subsystems are responsible for each function?

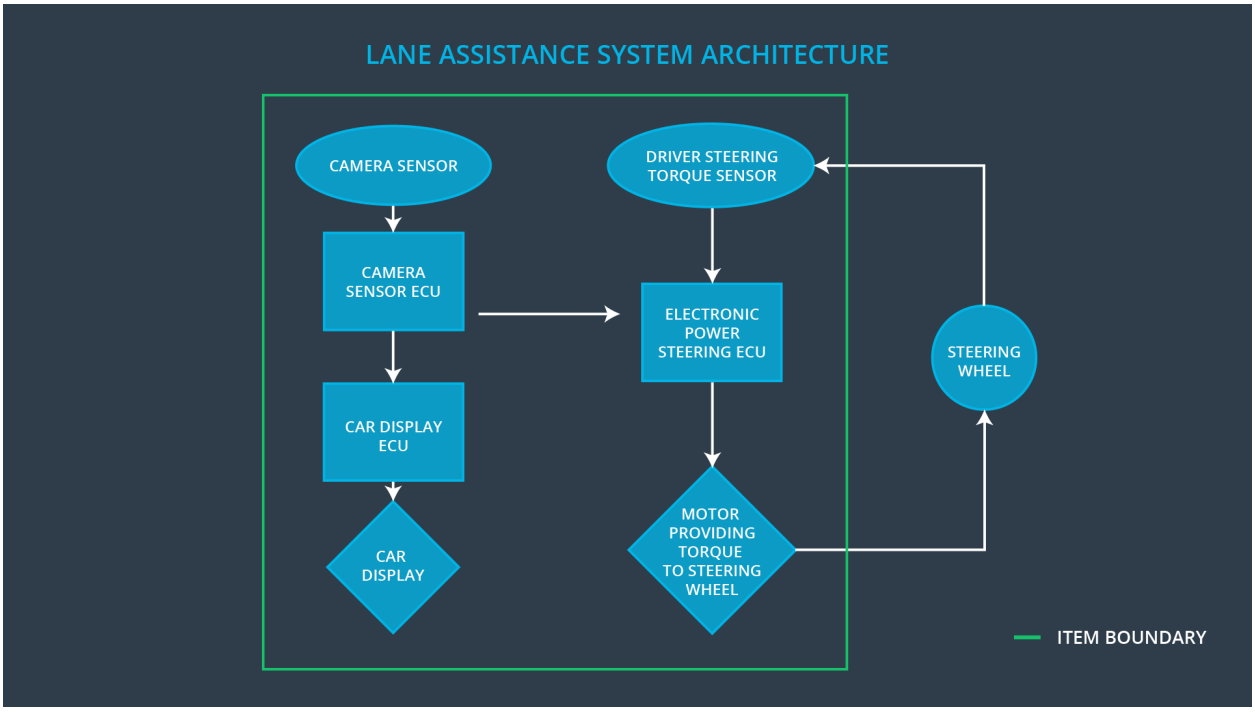
There are 3 subsystems:

1. The Camera subsystem:
   It identifies if a lane is departed (no lane change considered) and sends the according information to Electronic Power Steering (EPS) and Display subsystem.
2. The Electronic Power Steering (EPS) subsystem:
   It measures the current turn of the steering wheel. In case of lane departure it gets a torque request by the Camera subsystem and will provide a) the torque which is required to get the vehicle back into lane and b) the haptic feedback to the driver.

3. Display Subsystem
   in case of lane departure it will switch on a “lane departure” warning lamp.

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

- The boundaries of the item are the Steering Wheel interfaces:
  - Input: turn angle of steering wheel
  - Output: torque to steering wheel
- There is the element Steering Wheel outside of the item.
- There are 3 subsystems inside the item: Camera (Sensor + Camera ECU), Display (Car Display ECU + Display) and Electronic Power Steering (Torque Sensor + EPS ECU + Motor)



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 major goal of this project is identify the high risk situations for the Lane Assistance item and reducing these risks to a reasonable level, which is accepted by the society.
The ISO26262 functional safety standard provides framework for reducing risks that could harm people's health in the context of electric and electronic malfunctions in passenger vehicle systems. It follows the V model.

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	Safety Manager	Constantly
Coordinate and document the planned safety activities	Safety Manager	Constantly
Allocate resources with adequate	Project Manager	Within 2 weeks of start of project

functional safety competency		
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

[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
]

The main characteristics of my company's safety culture are described in the following:

1. **Safety has the highest priority** among other competing constraints like cost or productivity. This guarantees that functional safety is always considered, and there is no trade-off versus other competing constraints. Safety always comes 1st.
2. **There is a safety plan** for a product which defines safety processes, roles & responsibilities, documents & traces design decisions, and ensures accountability among the different stakeholders.
3. **The safety project is stuffed** (allocated) with adequate people in terms of safety competence to ensure that safety items can be handled sufficiently.
4. **Rewards safety** which motivates people to support safety, i.e. people are welcome to report safety issues and get rewarded when reporting or providing solutions for these.
5. **Penalize safety shortcuts** in order to avoid jeopardizing on safety or quality. There is no way to work around on safety issues if you do so you will be punished.

6. **Safety review or audits** are performed by independent persons, i.e. developers of a system will not review / audit safety items of that system, therefore, these safety items will be reviewed / audited by independent persons.

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
]

The following phases according to the V model are in the scope of the Lane Assistance item:

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

The following phases according to the V model are NOT in the scope of this Lane Assistance item:

- 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?**
   The DIA (Development Interface Agreement) defines the roles and responsibilities between companies for developing a product in compliance to ISO26262. It also specifies the deliverables and its acceptance criteria for each party.
   Therefore, disputes are avoided during the planning and development of a product and liability is defined, i.e. it makes it clear which party has to fix safety issue.

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.**

]

My company in charge of designing & developing subsystems for the Lane Assistance item from a functional safety point which includes defining, planning, tailoring the subsystem safety plan, coordinate and document the corresponding safety activities; and develop subsystem prototypes and integrate (smaller) components into subsystems.

The OEM or external will audit the subsystem versus the safety plan and judges whether the subsystem has increased safety.

Confirmation Measures

[Instructions:
Please answer the following questions:

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

   The confirmation measures that

- the functional safety project conforms to ISO26262
- the project really improves safety of the vehicle

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

   Ensures that the project complies with ISO26262. An independent person reviews that the product development follows ISO26262.

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

   Checks that the actual implementation of the project conforms to the safety plan.

4. **What is a functional safety assessment?**
   Assesses that plans, designs and developed products really 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.