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
06/02/2018	1.0	Efraim Kropp	Initial revision

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]

1. Introduction

1.1. Purpose of the Safety Plan

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

The purpose of this safety plan is to provide an overall framework for the Lane Assistance project and to define roles and responsibilities between the players involved in the project.

1.2. 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

1.3. 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

2. 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 Lane Assistance item provides the driver a warning in case of accidental lane departure and automatically assists the driver to steer the vehicle towards the center of the lane.

The main two functions of Lane Assistance System are:

1. Lane departure warning

2. Lane keeping assistance

The lane departure warning function vibrates the steering wheel by applying an oscillating steering torque to provide the driver a haptic feedback.

The lane keeping assistance function shall apply the steering torque when active in order to stay in ego lane.

There are three subsystems responsible for each function:

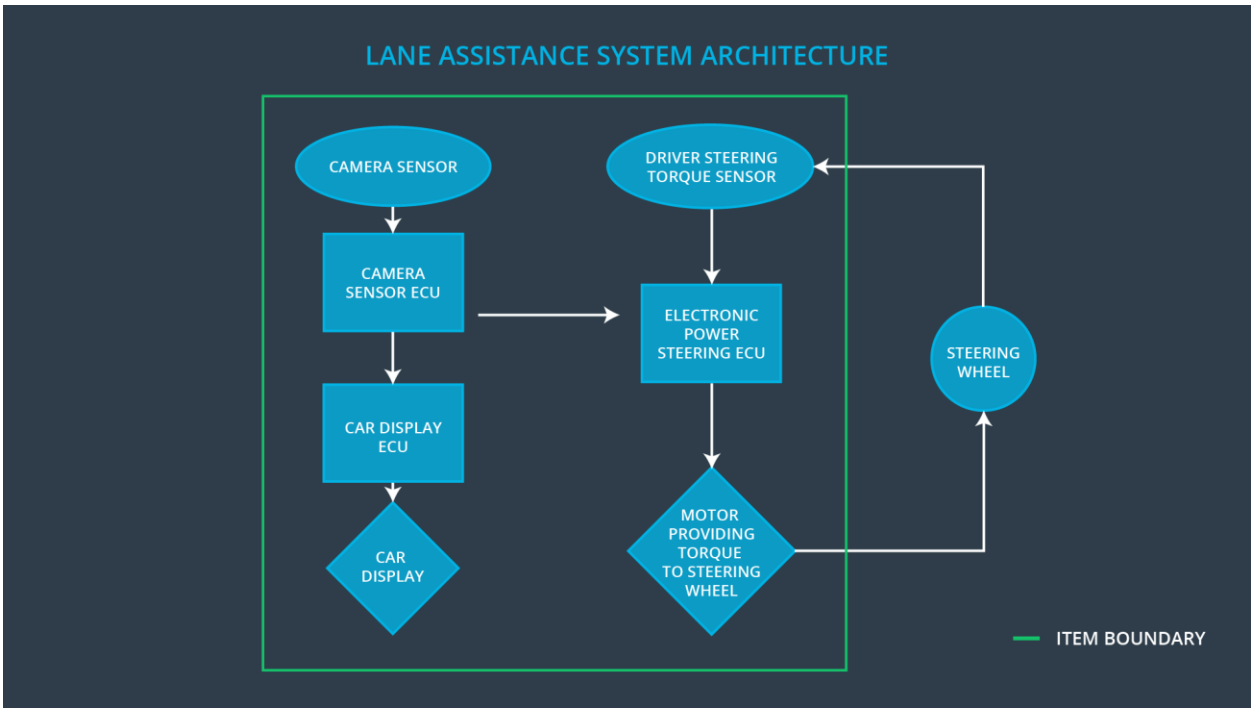
- Camera subsystem
- Electronic Power Steering subsystem
- Car Display subsystem

The Camera subsystem is responsible for detecting the 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 amount of torque based on the torque request.

The Car Display subsystem is responsible for activating a warning light on the dashboard display.

The following architectural block diagram shows the boundaries of the item:



The Camera, Electronic Power Steering and the Car Display are inside of the item. The Steering Wheel element is outside of the of the boundaries of the Lane Assistance item.

3. Goals and Measures

3.1. 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 of this safety project is to analyze the functions of the Lane Assistance item with respect to ISO 26262 in order to reduce risk to acceptable level.

3.2. 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

4. 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 supplier has developed clear policies and strategies to support the development, production and operation of safe systems. Below are some characteristics of these policies:

- Safety has the highest priority among competing constraints like cost and productivity
- The processes ensure accountability such that design decisions are traceable back to the people and teams who made the decisions
- The company motivates and supports the achievement of functional safety
- The company penalizes shortcuts that jeopardize safety or quality
- The teams who design and develop the product are independent from the teams who audit the work
- The company design and management processes are clearly defined
- The projects have necessary resources including people with appropriate skills
- Intellectual diversity is sought after, valued and integrated into processes
- The communication channels in the company encourage disclosure of problems

5. 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

6. 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

7. 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.**

]

The purpose of this development interface agreement (DIA) is to define the roles and responsibilities between the OEM customer and the Tier-1 supplier of the subsystems of the Lane Assistance system that are being supplied.

The OEM and the supplier shall mutually agree on following:
The OEM and the supplier shall follow a disciplined safety process that is consistent with ISO 26262 to identify, analyze and mitigate the system safety risks of the Lane Assistance item
The OEM shall assign a Safety Manager/Engineer responsible for the Lane Assistance item.
The supplier shall assign a Safety Manager/Engineer responsible for the sub-systems that are being supplied.
Any tailoring of the safety lifecycle of the Lane Assistance item shall be jointly reviewed and agreed by the OEM and the supplier
The OEM shall provide and maintain the System Safety Plan of the Lane Assistance item. The supplier shall provide and maintain the Safety Plan of the subsystems that are being supplied.
The OEM is responsible for the system hardware single element fault analysis. The Supplier is responsible for the analysis of the portions that are being supplied.
The OEM is responsible for development of System Safety Concept of the Lane Assistance Item. The Supplier is responsible to review and provide the safety concept that is applicable to their subsystem or component portion being supplied. The OEM is responsible to update the formal safety concept document after the tech review with the Supplier.
The OEM is responsible for vehicle level failure analysis. The Supplier is responsible for their subsystem/component level interface analysis as applicable
The OEM and the supplier shall identify the parties and persons responsible for each activity in design and production
The OEM shall define requirements to the supporting processes and tools that are used in the safety lifecycle of the Lane Assistance system. The supplier shall follow the requirements to ensure compatibility with the OEM. This includes but not limited to:
Requirements Management
Documentation Management
Configuration Management
Change management
Code Reviews
Process Quality Assurance
Production Process
System Safety Management

8. 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?**

]

The main purpose of the confirmation measures of the Lane Assistance project is to ensure that the processes comply with ISO 26262 requirements. Beside the conformation measures ensure that the project execution is following this Safety Plan and that the design of the Lane Assistance item is really makes the vehicle safer.

The OEM shall schedule periodic Confirmation Reviews to ensures that the Lane Assistance project complies with ISO 26262. One or more safety experts independent from the design team shall be present in the review process to evaluate if the safety requirements have been satisfied.

The OEM shall conduct periodic Functional Safety Audits of the project to conform that the actual implementation of the of the Lane Assistance components developed by the supplier follow the safety plan.

The OEM shall perform Functional Safety Assessment of the Lane Assistance project to confirm that the 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.