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
01/02/19	1.0	C. Wong	Initial version

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]

Confirmation Measures

Introduction

Purpose of the Safety Plan

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

This safety plan provides an overall framework for Lane Assistance functional safety. It is a guide to achieve functional safety. This plan will define roles and responsibilities for all members involved on this project in order that every tasks is identified and can be traced back to functional safety requirements. Design, implementation and production phases will be evaluated against this 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?

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**

]

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

The system considered in this safety plan is the Advanced Driver Assistance System (ADAS). The item discussed in this plan is the Lane Assistance item. This item provides information to the ADAS to alert the driver if the vehicle has departed its intented lane and take corrective physical action by attempting to steer the vehicle back to the center of the target lane.

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

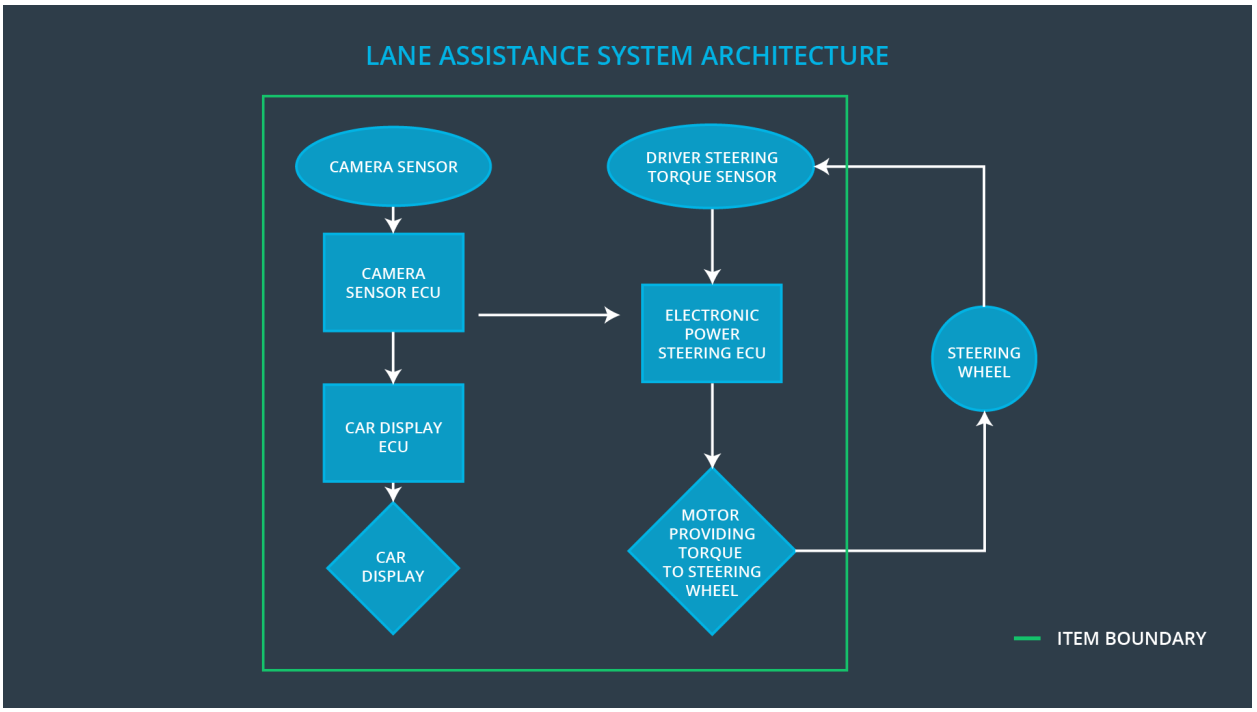
The Lane Assistance item has two main functions:

1. Lane departure warning - The lane departure warning function shall apply an oscillating sterring torque to provide the driver haptic feedback.

2. Lane keep assistance - The lane assistance function shall apply the steering torque when active in order to stay in ego lane (the target lane).

Which subsystems are responsible for each function?

Within the Vehicle Lane Assistance System, the camera sensor ecu, the electronic power steering ecu, and the car display ecu are all responsible for each of the functions.



- Camera Sensing Unit - In case the driver leaves the lane, camera detects and send a signal to ECU to activate the turning of the steering wheel as well as send haptic feedback alert to the driver.

- Car Display Unit – Displays the leaving of the ego lane by mistake

- Electronic Power Steering unit – Measures the torque provided by the driver and calculates the amount of torque based on the request by the system

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 subsystem are as follows:

- The steering wheel is NOT included in this system.
- If the camera input detects a false positive, it can display a lane departure accidentially. Camera errors that can lead to false positives maybe caused by environmental conditions (rain, snow, fog).
- If the motor is already at an end stop where as the lane assistance system continues to command a correction value. Also motors reaching MTBF, life expectancy and actually commanded motion outside positional tolerances.
- Driving requirements based on country may not be programmed into the system (legal needs).

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 to reduce the risk of the lane assistance system failure down t to acceptable levels. This makes the system safe and provides as an evidence to the auditors what safety standards are followed.

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 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	Within 4 weeks of start of project

safety lifecycle	Manager	
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
]

Good safety culture is taken in high regards for this project. The company takes safety seriously and promotes the following characteristics of good 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

[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 Hardware and Software Levels

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?**

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 delineates the design and production responsibilities between OEM and Tier 1 suppliers in order to avoid disputes during development of the project. In addition it can define libability and makes clear who should fix safety issues.

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.**

]

Our company is a Tier 1 company. We develop and produce the Lane Assistance System as a product to the Original Equipment Manufacturer (OEM). In order to produce the Lane Assistance System, the OEM will provide requirements that the product must meet and perform in compliance of ISO 26262. The OEM will inspect and confirm that our delivered product is functioning/behaving properly and verifies it meets asigned requirements.

Confirmation Measures

[Instructions:
Please answer the following questions:

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

Confirmation measures serve two purposes:

a) that a functional safety project conforms to ISO 26262, and

b) that the project really does make the vehicle safer.

The people who carry out confirmation measures need to be independent from the people who actually developed the project. In addition, having a independent party verify the project is management and follows a safety plan is beneficial.

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

The 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?**

The audit ensures 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?**

]

A functional safety assessment confirms that plans, designs and developed products actually achieve functional safety. In a safety plan, it 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.