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
6/8/2018	1.0	Sindhura Buggaveeti	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]

Introduction

Purpose of the Safety Plan

The purpose of this safety plan is to provide an overall framework for the lane assistance item, and to assign roles and responsibilities for functional safety for this item.

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

[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 that the vehicle has accidentally departed its lane and attempts to steer the vehicle back toward the center of the lane.

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

The two main functions of lane assistance systemare:

1. **Lane departure warning**
2. **Lane keeping assistance**

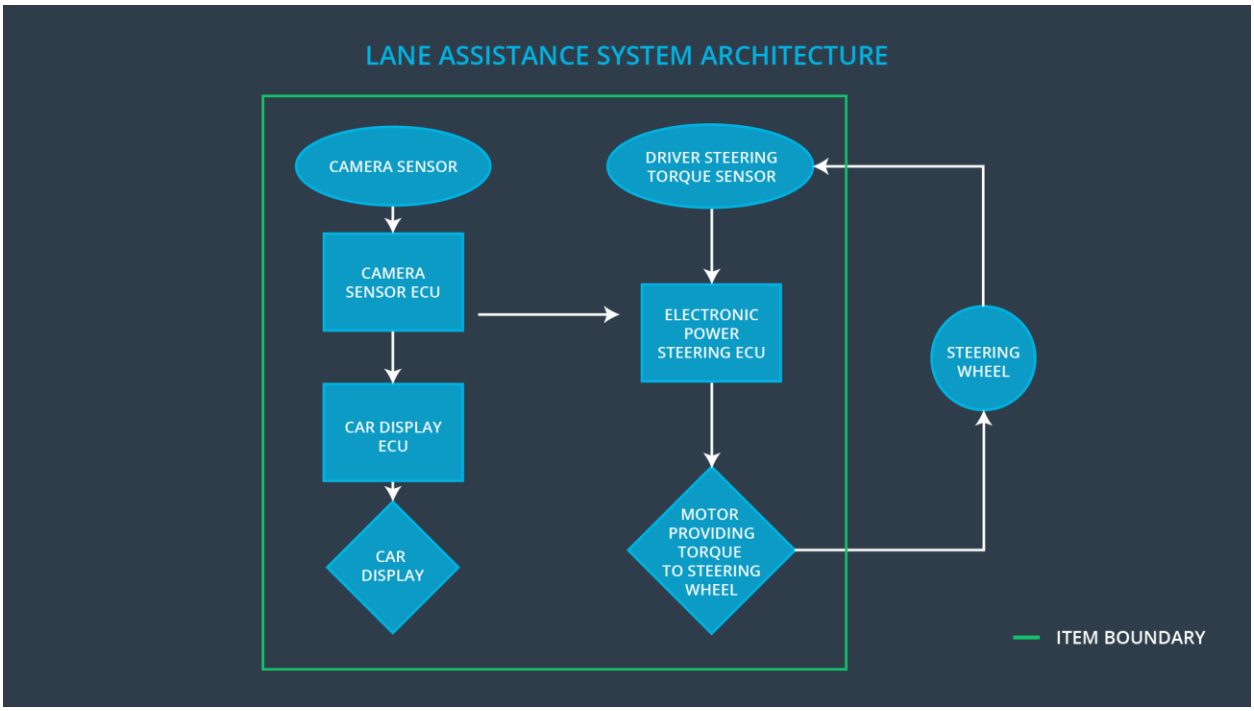
The lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback.

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

Which subsystems are responsible for each function?

The camera subsystem, the electronic power steering subsystem and the car display system are the three subsystems 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?



From the above image, we can see that the item boundaries were drawn to include camera system, electronic power steering system and car display system.
Camera system consists of a camera sensor that captures images of lanes and sends the information to camera sensor ECU. This ECU contains software that detects lane lines and determines when the vehicle leaves lane by mistake. When camera detects lane departure it communicates this information to electronic power steering system. EPS is responsible for measuring the torque provided by the driver through steering wheel and then adding appropriate amount of torque based on the lane assistance system torque request.
Steering wheel sub-system is outside of the boundaries of the item under consideration, as it in-directly interacts with the lane assistance system.

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 to develop a safe lane assistance system. Analyzing the lane assistance functions with ISO 26262 provides a methodical, state-of-the-art framework for ensuring a safe system. It involves:

1. **Identifying hazards and risks associated with lane assistance functions.**
2. **Determine effect of each unsafe function on the overall vehicle behavior and design the system to mitigate the risks**
3. **Ensure that the design really does improve through assessments, testing and validation**

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	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

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
]

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

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?**

A development interface agreement defines the roles and responsibilities between companies involved in developing a product. All the involved parties need to agree on the contents of the DIA before the project begins. It also specifies what evidence and work products each party will provide to prove that works has done according to the 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.**

]

Responsibility of OEM: **Provide functioning lane assistance system, oversee the development of the project, and participate in safety auditing/assessment of the system**
Responsibility of Tier-1: **Plan and document the practices followed to achieve functional safety, develop functional and technical safety concept, integrate, test and make sure that new lane assistance system confirms with ISO 26262**

Confirmation Measures

1. What is the main purpose of confirmation measures?
   Conformation measures serve two purposes:
   - **That a functional safety project confirms to ISO 26262**
   - **That the project really does make the vehicle safer**
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 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.