Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [V1.1]

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
8/16/2017	V1.0	Kris Harikrishnan	Initial documentation
8/25/2017	V1.1	Kris Harikrishnan	Revisions

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?]

A safety plan provides an overall framework for a functional safety project.

The purpose of the Safety plan is to identify hazards, measure risks, and lower risks to reasonable levels using systems engineering.

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

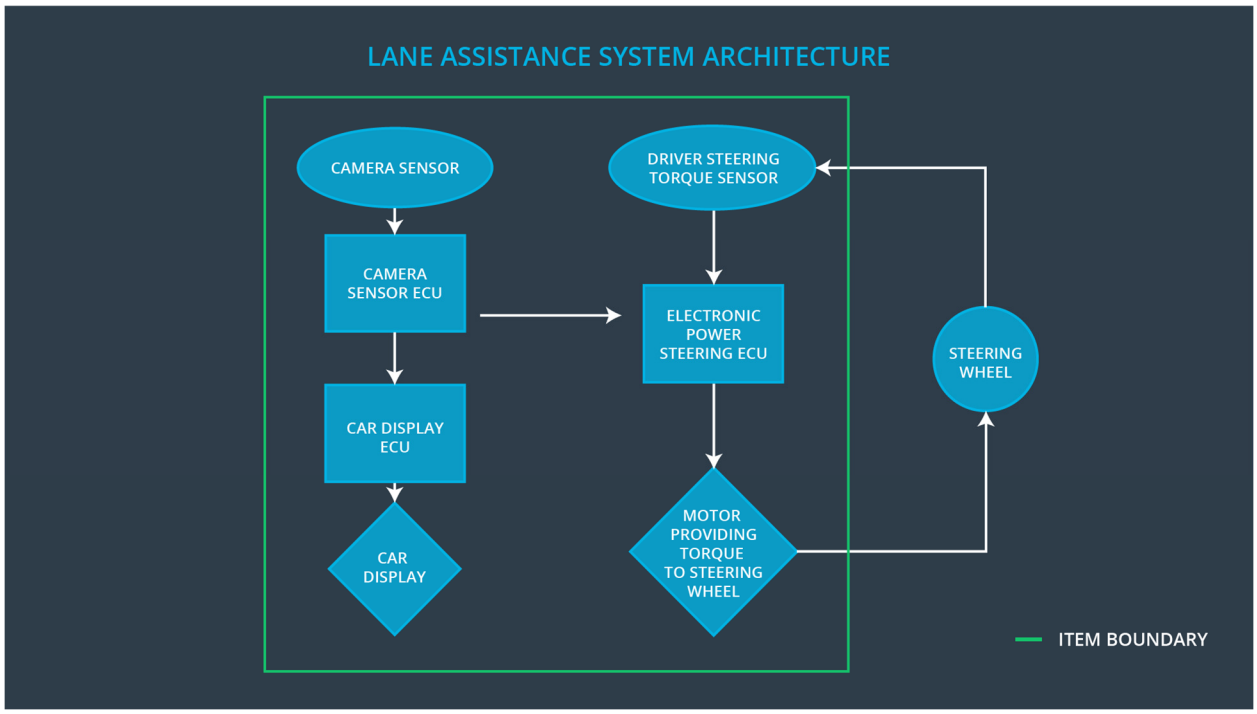
[Instructions:

REQUIRED

Discuss these key points about the system:

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

The item in question is the Lane Assistance system. Lane assistance item as shown below:



This item warns the driver if there is a lane departure and also actively steers the wheel to keep the vehicle in the lane.

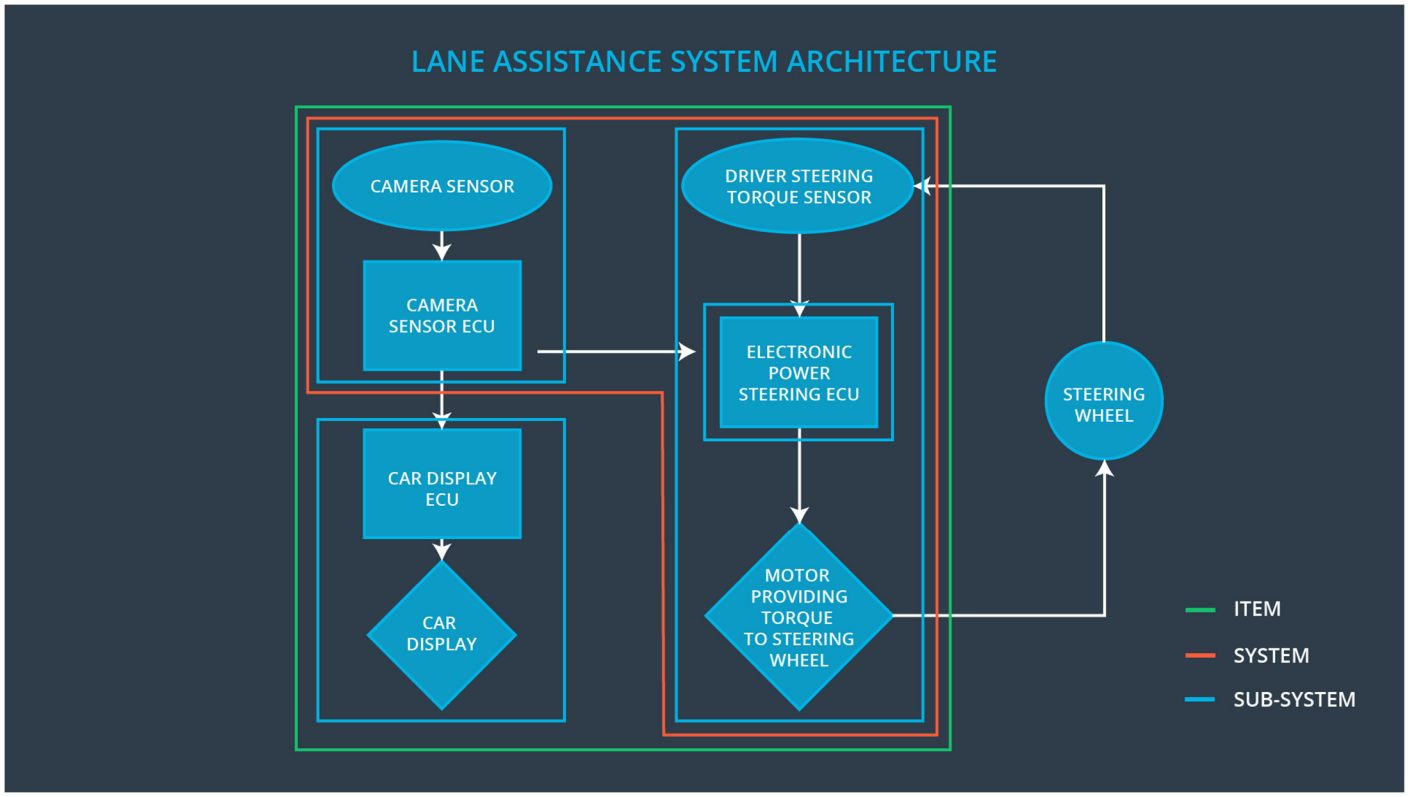
What are its two main functions? How do they work?

A lane assistance system has two functions:

- Lane departure warning
- Lane keeping assistance

If the driver departs a lane without using a turn signal, the system assumes that the driver has become distracted and did not mean to leave the lane. The system will vibrate the steering (lane departure warning) and also move the steering wheel back towards the lane center (lane keeping assistance).

Which subsystems are responsible for each function?



As seen in the above picture the lane assistance item has three subsystems:

- **Camera system**: The camera system is responsible for detecting lane departures and signaling the electronic power steering system
- **Car Display system**: The car display system is responsible for warning drivers of malfunctions or misuse of lane keeping assistance function
- **Electronic Power Steering system**: The electronic power steering system is responsible for receiving torque request from camera ECU and steering wheel. The EPS ECU also sends the torque request of the LDW and LKA functions to the steering wheel

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

The sub-systems Inside the boundary:

- Camera system
- Car Display system

- Electronic Power Steering system

Steering wheel is outside the boundary of the item.

In the above picture all sub-systems within the green box are inside the boundary.

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 goal of the project is to identify hazards, assess risks and lower risks through system engineering.

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 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
]

Here are some characteristics of a 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

These characteristics will help maintain a good safety culture. For example, if a manager is tempted to skip certain tests for a critical automatic braking system to meet costs and deadlines, following the above approach will dissuade the manager from taking that route as safety is held higher than cost and productivity. Despite this if the manager still skips the testing because of accountability the decision will be traceable to the manager. This will act as a deterrent to the manager. With proper penalties in place if inappropriate actions are taken penalties can be given out.

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?**

   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 purpose of DIA is to avoid disputes, reduce liability issues and make clear who should fix issues.

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.**

]

- OEM Project Manager: allocates resources needed for the functional safety activities at the item level. Also appoints safety manager or act as a safety manager
- Tier1 Project Manager: allocates resources needed for functional safety activities at the component level. Also appoints safety manager or act as a safety manager
- OEM Functional Safety Manager: Coordinates and documents the item level safety activities for the following functional safety phases: concept phase and product development at the system level. Also performs pre-audits before the safety auditor (3 months prior to main assessment)
- Tier1 Functional Safety Manager: Coordinates and documents the component level planned safety activities for the following functional safety phases: concept phase and product development at the sub-system level and software level which is in compliance with the item level planned and safety activities developed by OEM Functional Safety Manager/Engineer
- Safety Auditor: Perform regular functional safety audits once every 2 months
- Safety Assessor: Perform functional safety assessment at conclusion of functional safety activities

Confirmation Measures

[Instructions:
Please answer the following questions:

1. **What is the main purpose of confirmation measures?**
   Confirmation measures serve two purposes:

   - that a functional safety project conforms to ISO 26262, and
   - 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.

2. **What is a confirmation review?**
   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?**
   Functional safety audit makes sure that the actual implementation of the project conforms to the safety plan.

4. **What is a functional safety assessment?**
   Functional safety assessment confirms that 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.