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
2018-12-01	1.0	Flash Yuan	First Release of Safety Plan for Lane Assistance

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 purpose of the safety plan is to provide an overall framework for the Lane Assistance item and assign roles and responsibilities for the functional safety of this item, so that important steps are not missed. The documentation of these steps helps the auditor in understanding what standards are followed.

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:

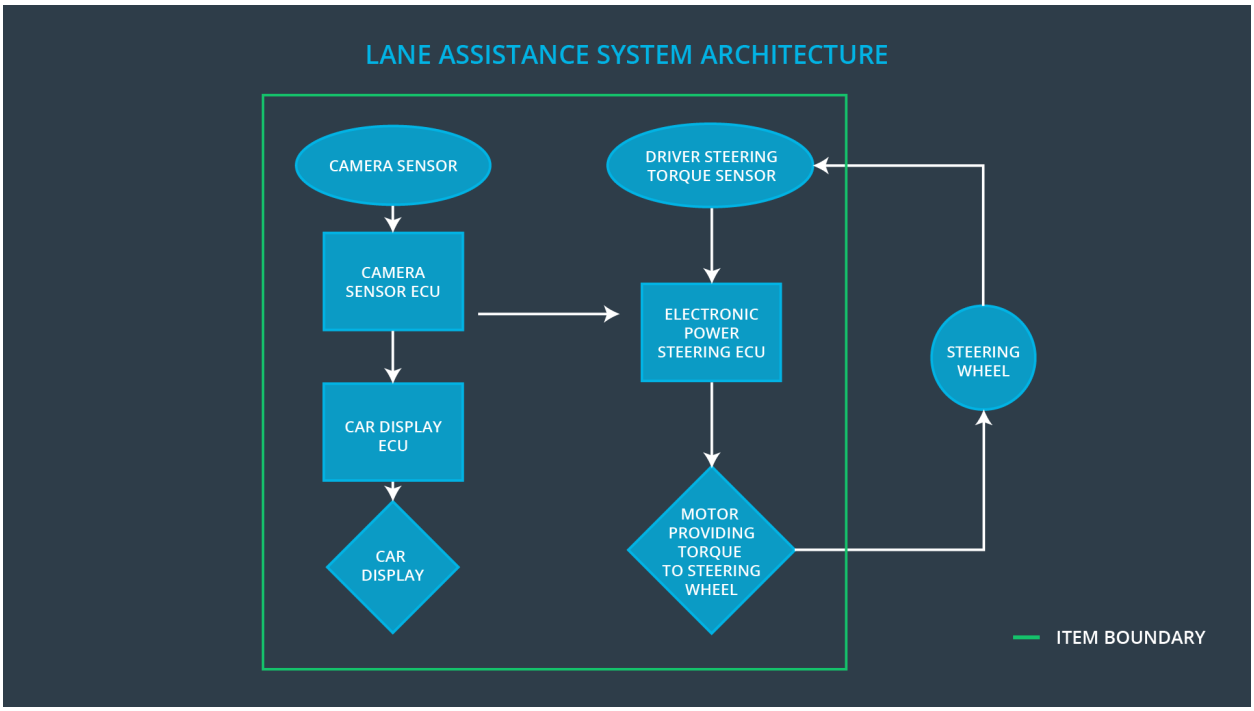
What is the item in question, and what does the item do?
The item in question is Land Assistance System. Lane Assistance System, is part of the Advanced Driver Assistance System (ADAS) which alerts the driver that the vehicle has accidentally departed its lane and attempts to steer the vehicle back towards the center of the lane.

What are its two main functions? How do they work?
The item is a lane assistance system with two main functions:

1. Lane departure warning – This will apply the oscillating steering torque to provide the driver with the haptic feedback.
2. Lane keeping assist - it automatically assists the driver such that the steering turns towards the center of the lane, via the steering torque when active.

Which subsystems are responsible for each function?
Vehicle Assistance System will be relying on the following three subsystem (diagram also below):

- Camera Sensing Unit - In case the driver leaves the lane, camera detects and send 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?

Boundaries can be seen in the diagram above. The steering wheel is not included in this item, but the camera with its ECU detects the lane change by mistake, Display ECU displays the leaving of the ego lane. Electronic power steering and motors are also included in the 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 reduce the risk of the lane assistance system down to acceptable levels. This makes the system safe and provides as an evidence to the auditors what safety standards were 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 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
]

Our company follows the culture with safety at heart when designing, developing and producing the vehicle system. Here are the characteristics of our company:
High priority: safety has the highest priority among competing constraints like cost and productivity
Accountability: The processes ensure accountability such that design decisions are traceable back to the people and teams who made the decisions
Rewards: Our organization motivates and supports the achievement of functional safety
Penalties: Our organization penalizes shortcuts that jeopardize safety or quality
Independence: In our organization, the 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: The projects have necessary resources including people with appropriate skills
Diversity: The 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 of this document
]

Safety lifecycle of Lane Assistance system will have following phases:

- Concept Phase
- Product development at the system levels – HW levels and SW 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

OEM: original equipment manufacturer
Tier-1: development & production
Tier-2: software & hardware components

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?**

   Development Interface Agreement (DIA) defines the roles and responsibilities between the companies involved in developing a product. All involved parties need to agree on the contents of the DIA before the project begins. For example, it is important for developing the safe vehicle if the original equipment manufacturer (OEM) will be engaging services of other companies for the development of the system.

DIA are crucial documents for the future in case there is any dispute or conflicts between the involved parties. The ultimate goal is to ensure that all parties are adhering to the ISO 26262 compliance when developing the vehicles.

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 is a Tier1 company and in a customer supplier relationship with Original Equipment Manufacturer (OEM). As per DIA, OEM will provide the set of requirements what lane assistance system needs to do and our company has to deliver a product to the OEM in compliance with ISO 26262. The OEM and our processes have to be aligned and made compatible. Also, OEM will also check if our delivered product is displaying the correct behavior.

Confirmation Measures

[Instructions:
Please answer the following questions:

1. **What is the main purpose of confirmation measures?**
   There are three main purposes of confirmation measures:
   - Processes comply with the functional safety standard ISO 26262.
   - Project execution follow the safety plan
   - Product should be safe from the design itself
2. **What is a confirmation review?**
   The confirmation review ensures that the project complies with ISO 26262. It is carried out by an independent person during the design and development phase of the vehicle system, to comply with ISO 26262.
3. **What is a functional safety audit?**
   Functional safety audit is an independent examination done to ensure that actual project implementation is in line with the safety plan
4. **What is a functional safety assessment?**
   Functional safety assessment is the assessment of the plans, designs and developed products such that they 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.