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
28 Oct 2017	1.0	R Hariharan	Safety Plan 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 Safety Plan provides an overall framework to achieve Functional Safety for the lane assistance system. It defines roles and responsibilities for the development process and lists measures that will be used to achieve the targeted ASIL.

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 lane assistance system which is part of the Advanced Driver Assistance System (ADAS) warns the driver of an unplanned lane departure and takes corrective measures if necessary. It is designed to minimize accidents by addressing human error in the form of a distracted driving.

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

The two Main Functions are,

Lane Departure Warning" This function will apply the oscillating steering torque feedback to a steering wheel to provide a feedback to the driver.

"Lane Keeping Assistance" This function will turn the steering wheel towards the center of the ego lane.

Which subsystems are responsible for each function?

The item includes three subsystems:

1. Camera subsystem
2. Electronic Power Steering subsystem (EPS)
3. Car Display subsystem

In Lane Departure Warning functionality, when the vehicle is leaving the lane, camera will detect it and it will simultaneously send signal to ECU to activate the turning of the steering wheel as well as send haptic feedback, i.e., vibrations to the steering wheel to alert the driver.

In Lane Keeping Assistance functionality, if lane departure signal is activated, ECU will provide enough torque in addition to the torque applied by the driver, to return the car to the center of the ego lane.

In addition, same signal will turn on warning light in the car display unit.

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

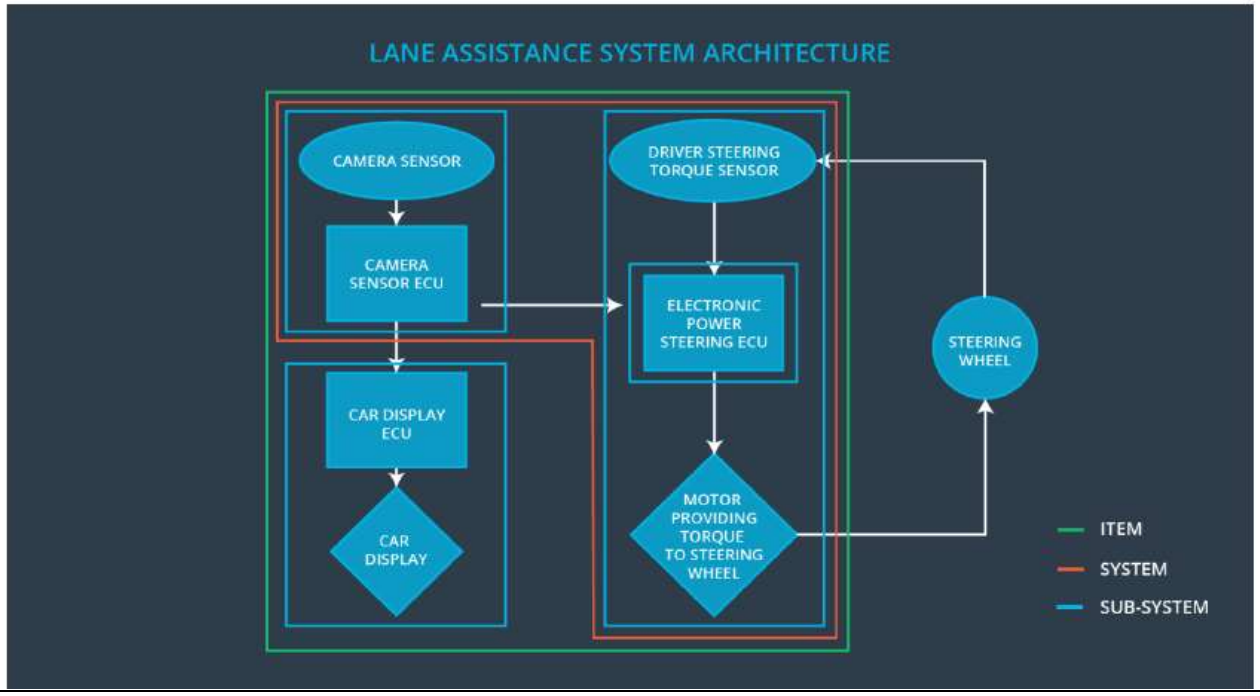
As Indicated below in the Architecture Diagrams (ADAS

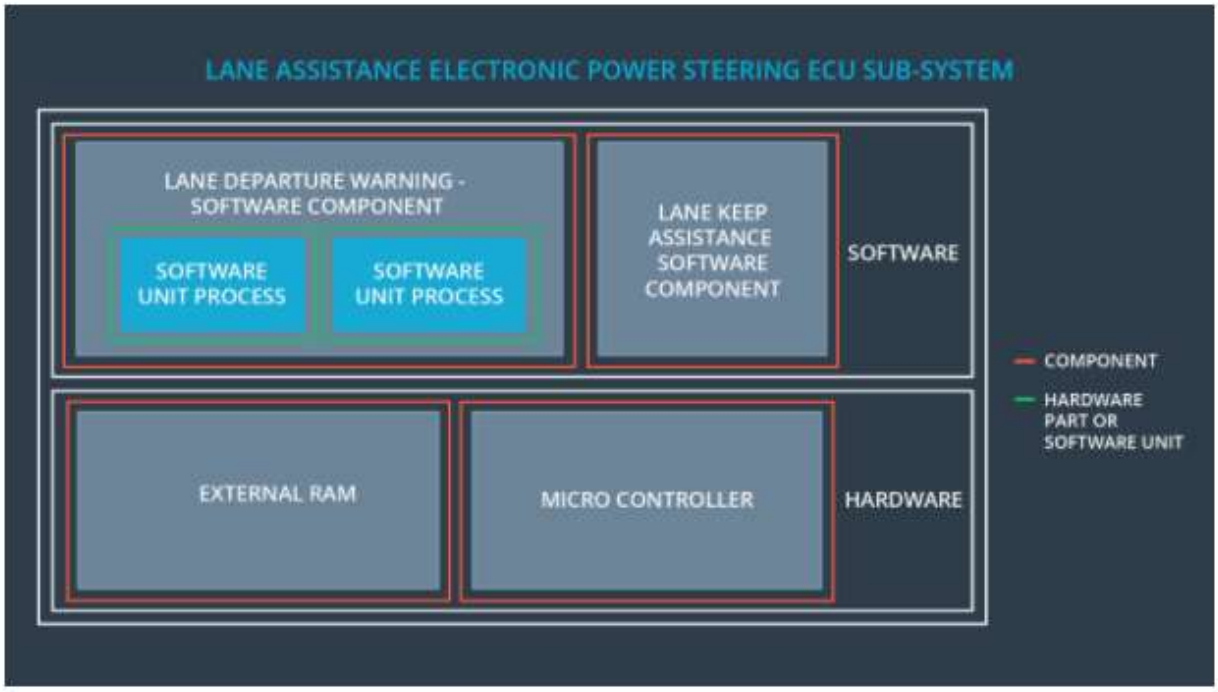
Lane Assistance System is limited to two functionalities –
Lane departure warning and Lane keeping assistance.

If the driver is using the signal indicator to change the lane, then Lane Assistance System will remain inactive.

Lane Assistance system is made up of three subsystems. Each subsystem will have its own elements, as follows.

- Camera Sensor Unit will have Camera Sensor, Camera sensor ECU (Electronic Controller Unit)
- Car Display Unit will have Car Display ECU, Car Display
- Electronic Power Steering will have its own ECU, driver steering torque sensor and motor to provide torque to steering wheel.





Subsystem Architecture

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**

]

- In general, line lanes must be detectable by the camera sensor and require proper illumination, line patterns must also correspond with normal road marking patterns. Some examples of situations outside of the ADAS' capabilities are listed below.

- Driving on a dirt road - No legible lane markings that can be detected
- Driving with snow on the ground - Lane markings hidden under snow
- Driving in fog - Lane markings may not be visible
- Driving at night without headlights on - Lane markings invisible

- Legal Requirements in India : TBD (Not included in this submission)
- National / International Standards Related to the item: **ISO 17361:2017**
- Records of previously known safety-related incidents or behavioral shortfalls:
  Refer Report - http://www.sciencedirect.com/science/article/pii/S0386111214601655

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 this project is to Ensure the safe operation and functional safety of the Lane Assistance System as per ISO 26262. This will allow identification of hazards and quantification of risk. Systems engineering will be used to minimize risk to a level such that it is acceptable to the public and does not further minimize the risk of failures by transitioning the system into a safe state.

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	Everybody on a Team	Constantly

Create and sustain a safety culture	Everybody on a Team. However, It is the Safety Manager's responsibility to ensure safety oriented workplace.	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 Manager	Once every 2 months
Perform functional safety pre-assessment prior to audit by external functional safety assessor	Safety Auditor	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
]

- My Company is committed to ensuring that our people stay safe and healthy. We have robust policies and practices in place throughout our operations to measure our health

and safety performance, demonstrate progress and identify areas for improvement.

- Our safety vision is to achieve no fatalities or serious injuries, and to protect and continually improve the health of our workforce.

- Accountability for health and safety performance is established through business planning, policies and scorecards. Business operation and plant managers are responsible for health and safety in the operations they manage, and safety performance forms part of the scorecards of relevant salaried employees.

- Our Senior Leadership, global Operating Committees and regional Occupational Health and Safety (OHS) committees all review safety performance regularly.

- Our efforts are guided by our OHS policy, established through corporate Policy Letters and Directives, and our global OHS standards cover all relevant issues, from workplace safety to ergonomics and occupational hygiene to toxicology.

- Our Safety Operating System (SOS), part of our overall manufacturing strategy, provides for the health and safety of our employees, and most of our manufacturing facilities have joint union/management safety committees to guide, develop and implement safety programs.

- Our strong safety culture relies on effective communication and reinforcement through a variety of channels, engaging all employees and contractors in understanding and adhering to safety programs and policies.

- We hold regular safety talks and occasional safety stand-downs at our plants to focus on key issues, and also use the START Card process to identify when to conduct pre-task briefings and safety assessments.

- All employees are encouraged to alert management to every injury or hazard, so that we can take corrective actions and create a safer workplace for everyone.

- Should a significant incident occur, we can alert health and safety experts at our other facilities so that appropriate action can be taken if necessary.

- Our efforts to make safety a core value across our operations have gone beyond response, toward prevention.

- We are also striving to predict and eliminate risks during the design stage using “virtual manufacturing” technology, we rely on good relationships with our stakeholders to identify, analyze and eliminate other potential risks.

- We continue to collaborate with all stakeholders to help address unsafe behaviors, and maintain external relationships with regulatory agencies and professional organizations such as the Government Occupational Safety and Health Administration.

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:

1. Concept phase
2. Product Development at the System Level
3. Product Development at the Software Level

The following phases are out of scope:

1. Product Development at the Hardware Level
2. Production and Operation

- This product shall be integrated into existing vehicle architecture.
- All relevant interfaces and integration to the vehicle shall be included in the scope.
- Functional safety shall be considered for all interactions and 2nd order interactions with other vehicle systems.
- Examples include: the car display, the car cruise control.

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 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.

Here are major sections of a DIA:

- Appointment of customer and supplier safety managers
- Joint tailoring of the safety lifecycle
- Activities and processes to be performed by the customer; activities and processes to be performed by the supplier
- Information and work products to be exchanged
- Parties or persons responsible for each activity in design and production
- Any supporting processes or tools to ensure compatibility between customer and supplier technologies

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 will provide the set of requirements what lane assistance system needs to do.
- My company (assumed Tier 1) in a customer supplier relationship with OEM
- will develop and supply functioning lane assistance system to the OEM which will include meeting the original requirements.
- OEM can also provide the preliminary product design and My company to finish the details of the product.
- Before Tier1 company can begin the work, both OEM and Tier1 will agree on the DIA.
- Tier1 company will follow the same V process model in developing the product.
- Bother OEM and Tier1 will have safety manager to see the overall progress and delivery.
- There will be clear communication between the parties which will include exchanging of information and work products.
- Both parties will have compatible processes or tools between their technologies used in the product development.

]

Confirmation Measures

[Instructions:
Please answer the following questions:

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

There are two main purpose of the confirmation measures.

1. To make sure processes involved in the project comply to Function Safety Standard ISO 26262.
2. The project does make the vehicle safer.

Confirmation measures are carried out by the people who are independent from the design and the implementation team of the project.

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

The confirmation review ensures that the project complies with ISO 26262. This is carried out as the product is designed and developed by an independent person.

3. **What is a functional safety audit?**

The functional safety audit confirms the actual implementation of the project conforms to the safety plan

4. What is a functional safety assessment?

The 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.