Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
19/6/2018	1.0	Akhil Suri	Initial Submission

Table of Contents

Introduction

Purpose of the Safety Plan

The purpose of the safety plan is to provide an overview of the safety framework for the Lane Assistance System. It also aims to clearly assign responsibilities at the inter-organization level using the DIA as well as the intra-organization level by defining roles and responsibilities for each task.

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

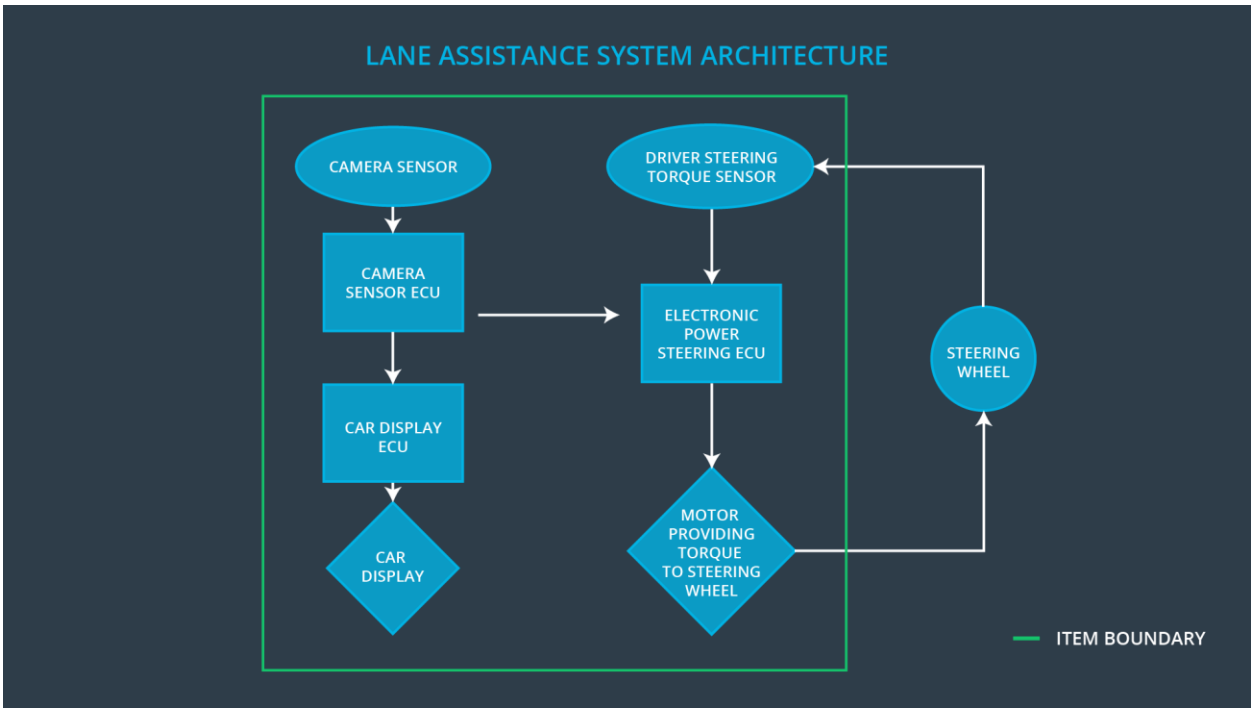
Item Definition

This safety plan covers the Lane Assistance System which is an Advanced Driver Assistant System(ADAS). The Lane Assistant System alert the driver to potentially dangerous situations and take control over vehicle to prevent accidents from occurring. To do this the item has two main functions.

- Lane Departure Warning
- Lane Keeping Assistance

The lane departure warning function is responsible for alerting the driver if the system determines that there is an unintentional or inadvertent change of lanes. This could be done by providing driver a haptic feedback by vibrating the steering wheel to draw the driver's attention or through audio cues in order to stay in the ego lane.

The lane keeping assistance function shall apply the steering torque when active in order to stay in the correct lane. The system is responsible for identifying the correct boundaries and making sure the vehicle is able to safely maintain its course within these boundaries.



The above diagram shows the relations between the subsystems and how they are connected. The camera sensor will detect if the vehicle is out of the lane and sends the signal for the same to the electronic power steering system which will turn the steering and keep the vehicle back on the lane. Camera sensor will also request the warning light to be turn on so that the driver will be aware that the system is active. The electronic power steering system will detect how much the car is turned by the driver and accordingly it may add torque to get back the vehicle to the center. The car display system will display the warning if required.

Goals and Measures

Goals

The primary goals of this project are:

1. To identify the hazard associated with the Lane Assistant System and to minimize the risk associated with the hazards.
2. To clearly define the responsibilities of the various team members so that the work is handled efficiently.
3. To ensure that the safety measures adhere to ISO 26262 – extensively documenting all the features of the system, risks and measures taken to reduce the risks to a reasonable level accepted by current society.

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

The company's focus is on giving the highest priority to safety. The company's culture emphasizes the fact that safety can at no point be compromised. In order to ensure a safety culture, the following characteristics needs to be observed.

1) **Communication**: Potential safety problems have to be reported immediately to the developers for further investigation. Different channels of communication help and encourages disclosure of problems.
2) **Well defined process**: The management processes and design is very well defined.

3) **High priority**: Highest priority is given to safety compared to the cost and productivity.
4) **Resources**: Projects have necessary resources including people with appropriate skills.
5) **Rewards**: Constant motivation and support is given by the organization for achieving the functional safety.
6) **Penalties**: The organization penalizes shortcuts that jeopardize safety or quality.
7) **Independence**: The teams who designs and develop a product should be independent from the teams who audit the work.

Safety Lifecycle Tailoring

For this project the safety plan in tailored. The following 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 hardware level.
- Production and Operations

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

Purpose:
The purpose of the development interface agreement(DIA) is to define the roles and responsibilities between OEM and tier-1 involved in developing this project.

Responsibility:
The company agrees that the above mentioned safety lifecycle will be fine to fulfill the ISO 26262 for the lane assistance system. While the OEM is responsible for the overall safety of the vehicle and also the safety actions mentioned in ISO 26262.

Tier-1 will analyze and modify few sub-systems based on the functional safety requirements. The company will fix all bugs which comes under the lane assistance system and all other issues would have to be taken care by OEM

Confirmation Measures

Purpose of confirmation measure:
The purpose of confirmation measure is:

- Ensure the lane assistant project conforms to ISO 26262.
- Ensure the lane assistant project really does make the vehicle safer.

Confirmation Review:
The confirmation review ensures that the projects comply with ISO 26262. As a product is designed and developed, an independent person would review the work to make sure ISO 26262 standard is being followed.

Functional Safety Audit:
A functional safety audit makes sure that the actual implementation of the project conforms to the safety plan.

Functional Safety Assessment:
A functional safety assessment confirms that the plan, design and developed product 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.