Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.0

Document history

Date	Version	Editor	Description
23-May-2018	1.0	Gautam Sareen	First Attempt

Table of Contents

Introduction

Purpose of the Safety Plan

Safety plan provides an overview of how to achieve a safe system. It helps us define roles for each task and outline the steps to be taken to achieve functional safety.
Purpose of safety plan is to manage and guide safety related activities such as safety culture, safety lifecycle, safety roles and responsibilities, coming up with DIA (development interface agreement) and confirmation measures.

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

The item being discussed is Lane assistance system. Lane assistance system warns the driver in case car is unintentionally straying out of the current lane and will try to steer back to the center of lane.

The two main functions of Lane Assistance Systems are:

1. Lane departure Warning: shall apply an oscillating steering torque to provide the driver a haptic feedback.
2. Lane keeping Assistance: shall apply the steering torque when active in order to stay in current lane.

Camera subsystem, Car Display Subsystem and Electronic Power Steering system are all responsible for each of functions. This can be seen in below image.

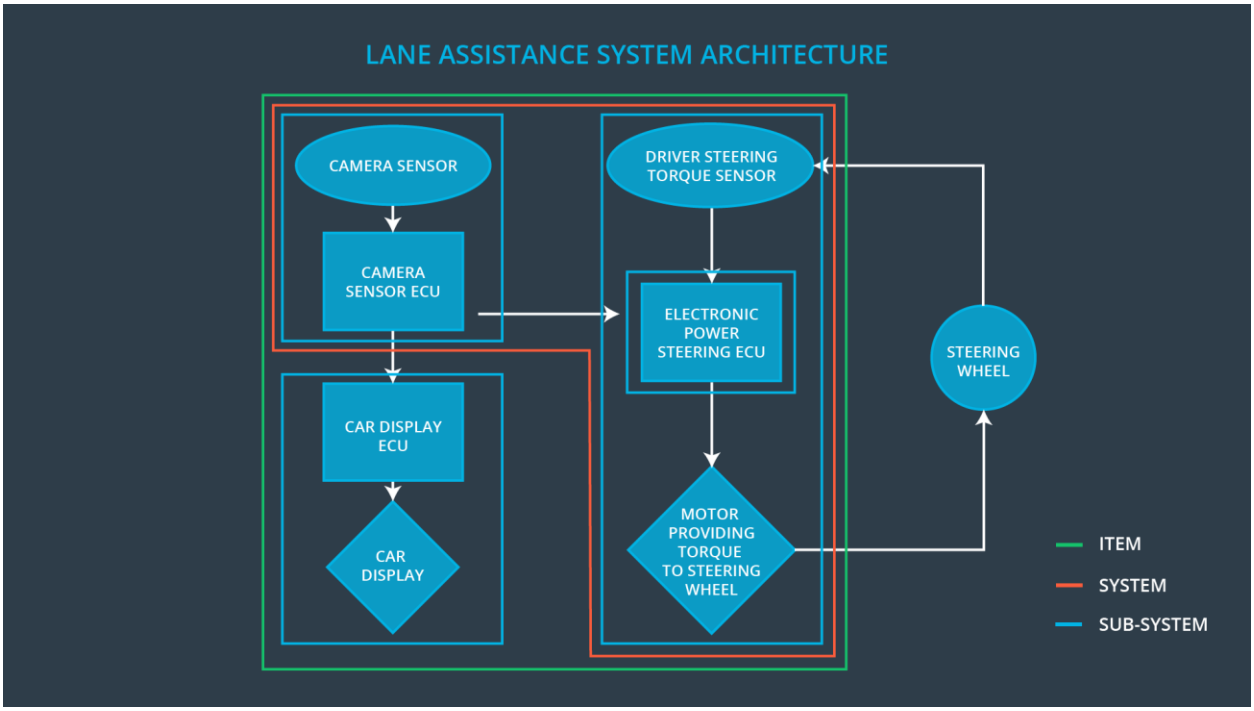

Fig 1. Lane Assistance System Architecture
[image source Udacity course content]

Item boundary for Lane Assistance System includes camera subsystem, electronic power subsystem and car display subsystem.
Steering wheel subsystem is outside of lane assistance system boundary.

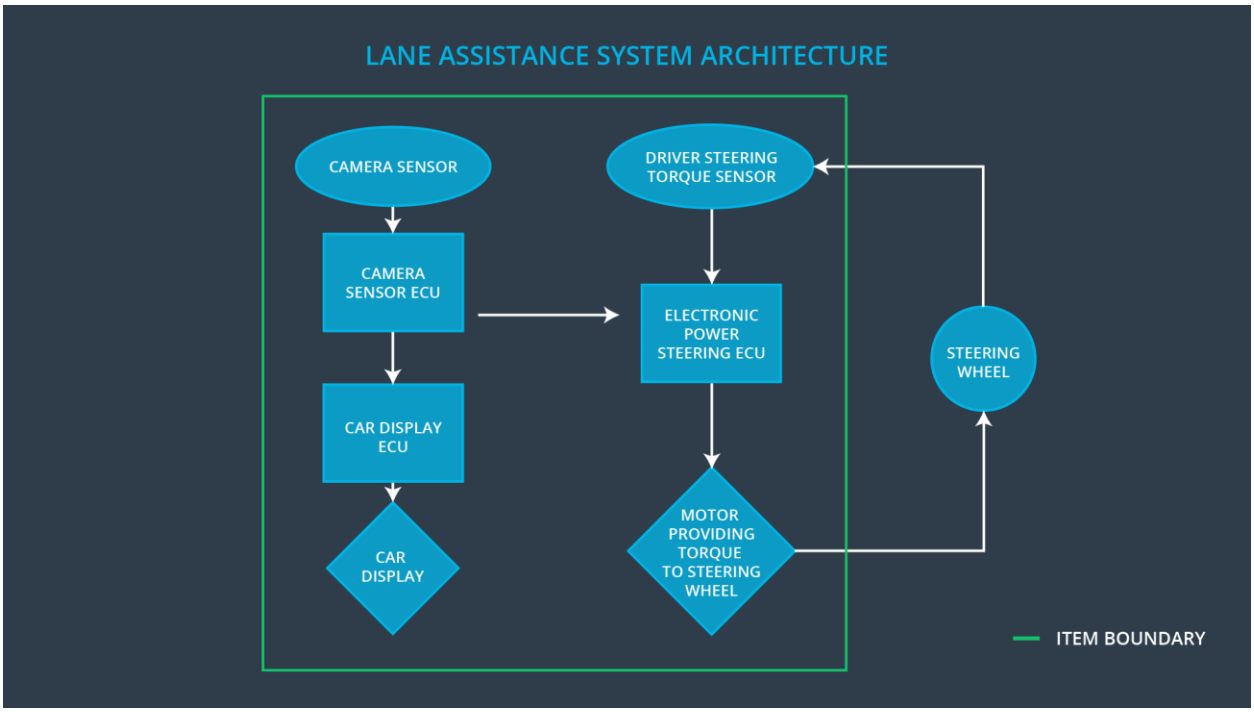

Fig 2. Item boundary Lane Assistance System
[image source Udacity course content]

Goals and Measures

Goals

The main goal of this project to adhere to ISO 26262 standard for functional safety. This way we can understand the system and detect hazardous risk linked to lane assistance function and try to minimize to acceptable level.

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

Below are some characteristics of our company safety culture.

- **High priority:** safety is placed at the highest priority among all other constraints such as cost, quality and productivity.
- **Accountability:** processes are enabled to ensure accountability of various tasks back to the people or teams who were involved in decision making or designing.
- **Rewards:** the organization motivates and supports the achievement of functional safety
- **Penalties:** the organization penalizes shortcuts that jeopardize safety or quality of the product.
- **Independence:** Its achieved by keeping separate teams for designing and auditing tasks.
- **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 Lane Assistance System below phases are in-scope

- Product Development at the System Level
- Product Development at the Software Level

For Lane Assistance System below 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

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 goal is to ensure that all parties are developing safe vehicles in compliance with ISO 26262.

In this Project OEM is responsible for supplying functioning lane assistance system and our company role is to analyze and modify the system to ensure the final system adheres to functional safety guidelines.

Confirmation Measures

Confirmation measures servers two main purposes: -

- Functional safety project conforms to ISO 26262 standards
- Project really makes the vehicle safer

Confirmation review
ensures that the project complies with ISO 26262 standard. As the product is designed and developed, an independent person would review the work to make sure ISO 26262 is being followed.

Functional safety audit
It’s to make sure that actual implementation of the project conforms to the safety plan set.

Functional safety assessment
It’s to confirm that plans, designs and developed products 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.