Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version:1.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
2017-08-20	1.0	Y.Wiyogo	Initial document
2017-08-24	1.1	Y.Wiyogo	Update layout and remove comments

Table of Contents

Document history

Table of Contents

Introduction
- Purpose of the Safety Plan
- Scope of the Project
- Deliverables of the Project

Item Definition

Goals and Measures
- Goals
- Measures

Safety Culture

Safety Lifecycle Tailoring

Roles

Development Interface Agreement

Confirmation Measures

Introduction

Purpose of the Safety Plan

This document describes a safety plan of the lane assistance. As part of the Advanced Driver Assistance System, the lane assistance functionality can introduce a new risk in a vehicle. The main goal of this safety plan is to detect risk and reduce it to the acceptance levels.

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 of this safety plan is the lane assistance system. This item has two main functions:

1. it can steer a vehicle to the center of the lane, which is called a lane keeping assistance
2. Before controlling the wheel, the system will vibrate the steering wheel. This approach is called a lane departure warning.

The lane keeping assistance function shall apply the steering torque when active in order to stay in ego lane. An ego lane refers to the lane in which the vehicle currently drives.

The lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback. When the driver drifts away the vehicle from the center by mistake, this function will vibrate the steering wheel.

The item consists three subsystems:

- Camera system
- Electronic Power Steering system
- Car Display system

A camera sensor can detect the road lanes and trigger a signal to the board computer. A warning light on the car display dashboard will be turned on to inform the driver. The camera can detect if the vehicle starts to leave the current lane. Thus, the camera and the car display system are responsible for the lane departure warning function.

The electronic power steering (EPS) system is integrated in the steering wheel. The EPS system is responsible to the lane keeping assistance function.

Figure 1 shows the system architecture of this item and its boundary.

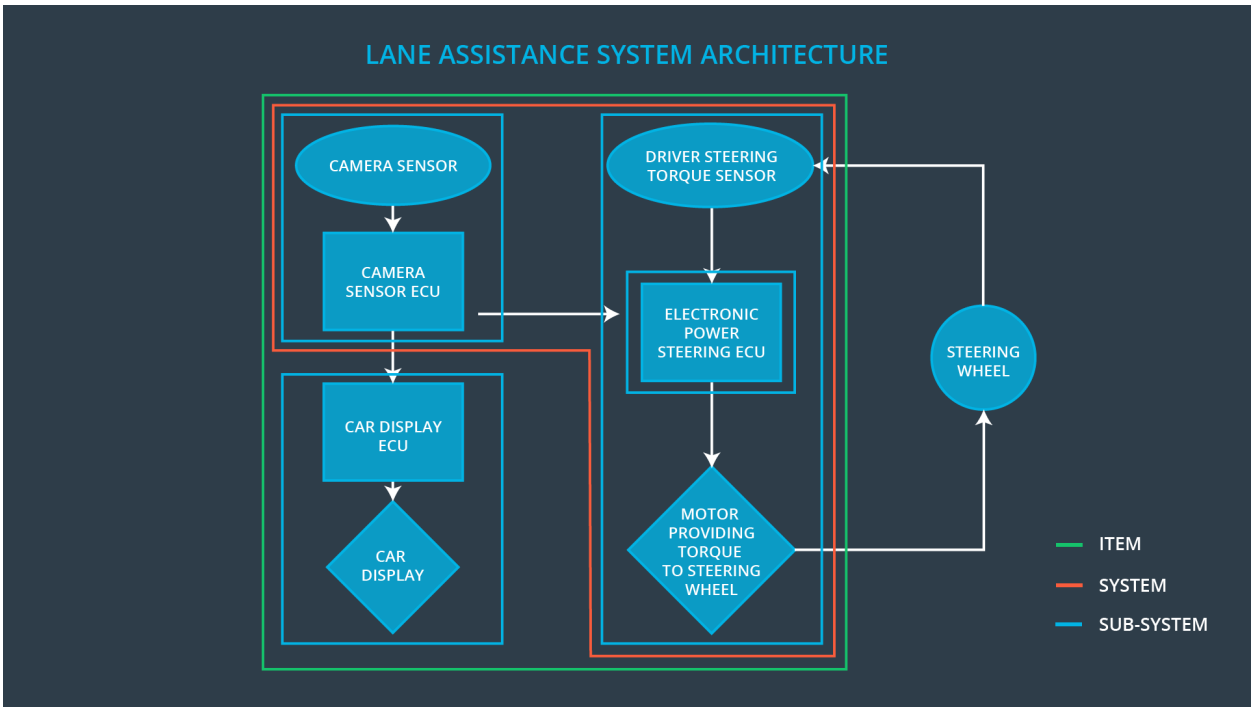

Figure 1: Lane Assistence System Architecture

The steering wheel is the element that is not included in this item because of its non-electric component.

This item has several constraints regarding the operation and environment situations, which are:

- In several conditions, such as in snow and foggy wheather, the lane detection result of the camera is not very reliable.
- During a road work, the lane can be missing. Depending on the country regulation the temporary lane color can be less contrast so that it influences the lane detection.

Goals and Measures

Goals

The major goal of this safety plan is to determine all the possible risks of the lane assistance system. Based on the risk analysis, we can classify the safety levels and define actions and policies to avoid the risks.

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

High priority
In our company, safety has the highest priority among the competing constraints like productivity and cost. Each new employee in our engineering department is assigned to the introduction of ISO 26262 training.

Accountability
We document all the development activities and decisions in order to ensure the accountability. All document changes is saved and has a version number so that each activity is traceable.

Rewards
Our Company encourages and recognizes each employee who reports any incorrect process or obscurity during day-to-day work. The employee feedbacks are documented and will be evaluated each quartal.

Penalties
We penalize shortcuts that jeopardize safety or quality of ouw product. After the first attempt, the safety manager will send a warning notice. After the second attempt the employee will be reallocated or dismissed.

Independence
We build our development, design, testing, and audit team independently.

Well defined processes
All processes are clearly defined and the documents are placed in a certain folder in our company network. Only team members with its appropriate role has a write access.

Resources
We work together with our human resource team to plan, manage and find new talented engineers with the appropriate skills. In case of shortage

Diversity
Intellectual diversity is sought after, valued and integrated into processes.

Communication
Communication channels encourage disclosure of problems.

Safety Lifecycle Tailoring

For tailoring the safety lifesycle, 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

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

The purpose of a development interface agreement (DIA) is to ensure that all parties are developing safe vehicles in compliance with ISO 26262.

The responsibilities of the OEM are to define the functionality of the lane assistance system and to conduct the activities in scope of project manager, safete manager and safety engineer in item level. Our company is responsible for conducting the activities in scope of safety manager and safety engineer of the component level.

Confirmation Measures

The main purpose of confirmation measures is :

- to ensure that a functional safety project conforms to ISO 26262, and
- tp ensure that the project really does make the vehicle safer

Confirmation review is a measurement process to ensure 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.

Functional safety audit checks to make sure that the actual implementation of the project conforms to the safety plan.

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.