Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
2019.05.05	1.0	Chenglei Qiao	Initial revision

Table of Contents

Introduction

Purpose of the Safety Plan

The purpose of the Safety Plan is to manage the development of a safe product and specify how functional safety will be ensured throughout the entire development project and in production.
The Safety Plan identifies the various roles and responsibilities as they apply to the development process and lists the various techniques and measures that will be implemented as part of the development project to ensure that the targeted ASIL is achieved.

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 in this project is a simplified version of a Lane Assistance System, as a part of the Advanced Driver Assistance System, the two main functions of the item are:

- **Lane departure warning function**: When the vehicle begins to unintentionally move out of its lane, the function will warn the driver by vibrating the steering wheel.
- **Lane keeping assistance function**: When the vehicle begins to unintentionally move out of its lane, the function can automatically take steps (apply steering torque) to ensure the vehicle stays in its lane.

The item functionalities are implemented by the following subsystem:

- **Camera subsystem**: This subsystem is mainly responsible for lane departure warning function, it is composed by two components:
    - Camera sensor
    - Camera sensor ECU (Electronic Control Unit)
- **Electronic Power Steering subsystem**: This subsystem is mainly responsible for lane keeping assistance function and it is composed by three components:
    - Driver Steering Torque Sensor.
    - Electronic Power Steering ECU.
    - Motor Proving Torque to Steering Wheel.
- **Car Display subsystem**: This subsystem is mainly responsible for lane departure warning function by additional visual warning (e.g. warning light), it is composed by two components:
    - Car Display ECU
    - Car Display

Figure 1 shows the architecture and the boundaries of the item.

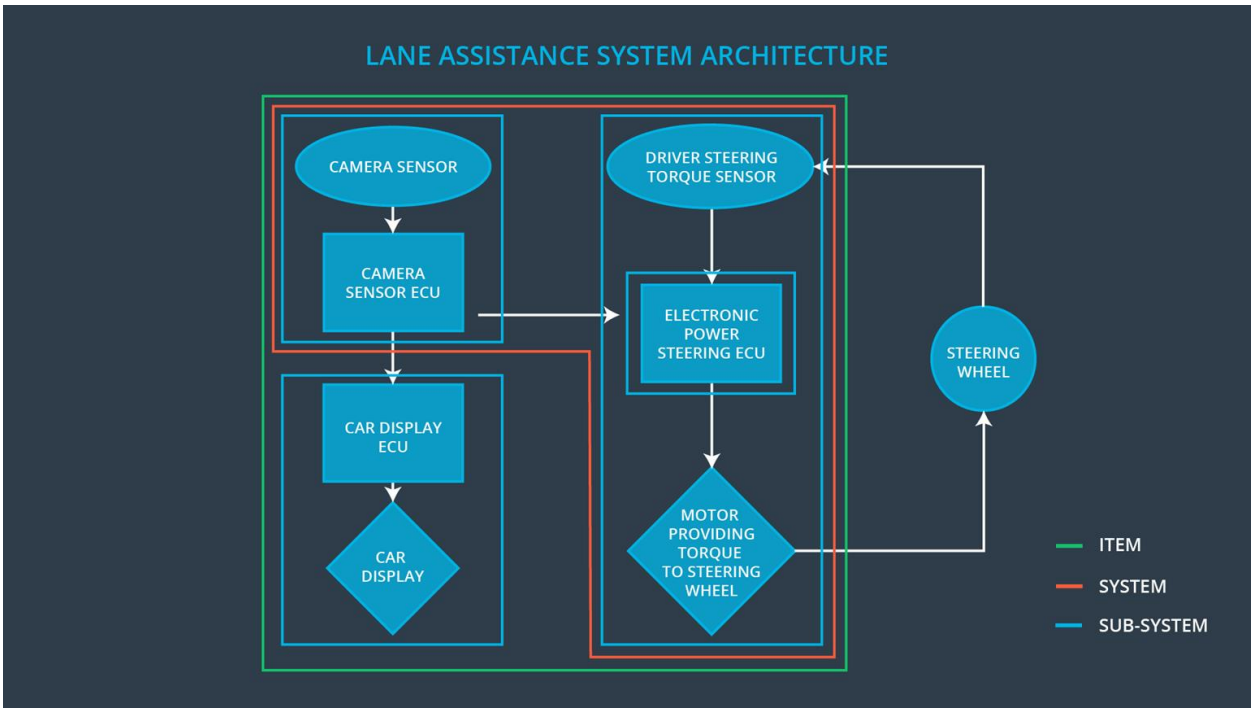

Figure 1 The architecture of Lane Assistance System

When the camera senses that the vehicle is leaving the lane, the camera sends a signal to the electronic power steering system asking to turn and vibrate the steering wheel.
The camera sensor will also request that a warning light turn on in the car display dashboard. That way the driver knows that the lane assistance system is active.
If the turn signal is on, the system assumes the driver is intentionally crossing over the lane, and there's no alert.

The driver is always expected to have both hands on the steering wheel. The electronic power steering subsystem has a sensor to detect how much the driver is already turning. The lane keeping assistance function will merely add the extra torque required to get the car back towards center. The extra torque is applied directly to the steering wheel via a motor.

This item doesn't work 100% of the time since no machine vision system is perfect. The item has several constraints regarding the operation and environment situations, for example:

- In several conditions, such as in rain, snow or foggy weather, the camera subsystem works less capably;
- If there are no clear lane markings, for example, covered by snow, or during the road work.
- 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 main goal of this project is to achieve the functional safety of the lane assistance system, including:

- Identify risk and hazardous situations in the Line Assistance system components malfunction causing injuries to a person.
- Evaluate the risks of the hazardous situations.
- Low to risk of the malfunctions to a reasonable level acceptable by current sociality.

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	All Team Members	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

To ensure a safety culture, the following characteristics are observed in my company:

- High priority: in my company, safety has the highest priority among the competing constraints like cost and productivity. We have strict safety rules and every employee needs to get training on the rules and make sure to obey the rules.
- Accountability: we document all the development activities and decisions to ensure the accountability. All document changes are saved and has a version number so that each activity is traceable.
- Rewards: my company motivates and encourages all employees to give feedback on the incorrect process what may affect safety in daily work. For the valuable feedback/suggestions, there will be rewards for the related employees.
- Penalties: my company penalizes shortcuts that jeopardize safety or quality.
- 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 lifecycle, 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 involved in the project are developing safe functions/systems in compliance with ISO 26262.

- **Functional Safety Manager (OEM) - Item Level**: Pre-audits, plans the development phase for the Lane Assistance item.
- **Functional Safety Engineer (OEM) - Item Level**: Develop prototypes, integrate subsystems combining them into the Lane Assistance item from a functional safety viewpoint.
- **Project Manager (OEM) - Item Level**: Allocates the resources needed for the item.
- **Functional Safety Manager (Tier-1) - Component Level**: Pre-audits, plan the development for the components of the Lane Assistance item.
- **Functional Safety Engineer (Tier-1) - Component Level**: Develop prototypes and integrate components conforming the Lane Assistance item.
- **Functional Safety Auditor (OEM or external)**: Make sure the project conforms to the safety plan.
- **Functional Safety Assessor (OEM or external)**: Judges where the project has increased safety**.**

Confirmation Measures

The main purposes of confirmation measures are:

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

The confirmation review ensures 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.

The functional safety audit checks to make sure that the actual implementation of the project conforms to the safety plan is called a functional safety audit.

The functional safety assessment confirms 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.