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
2018-06-04	v0.9	Csathó, Csaba	First draft
2018-06-12	v1.0	Csathó, Csaba	Final version

Table of Contents

Contents

Introduction

Purpose of the Safety Plan

The purpose of the Safety Plan is to outline an overall framework to achieve functional safety. Our plan is to create a safe system, namely the Lane Assistance System. We are doing so by defining the steps that will be taken to guarantee safety and assign roles and staffs involved in the project. The project timeline sets goals and milestones to effectively execute the project in time.

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

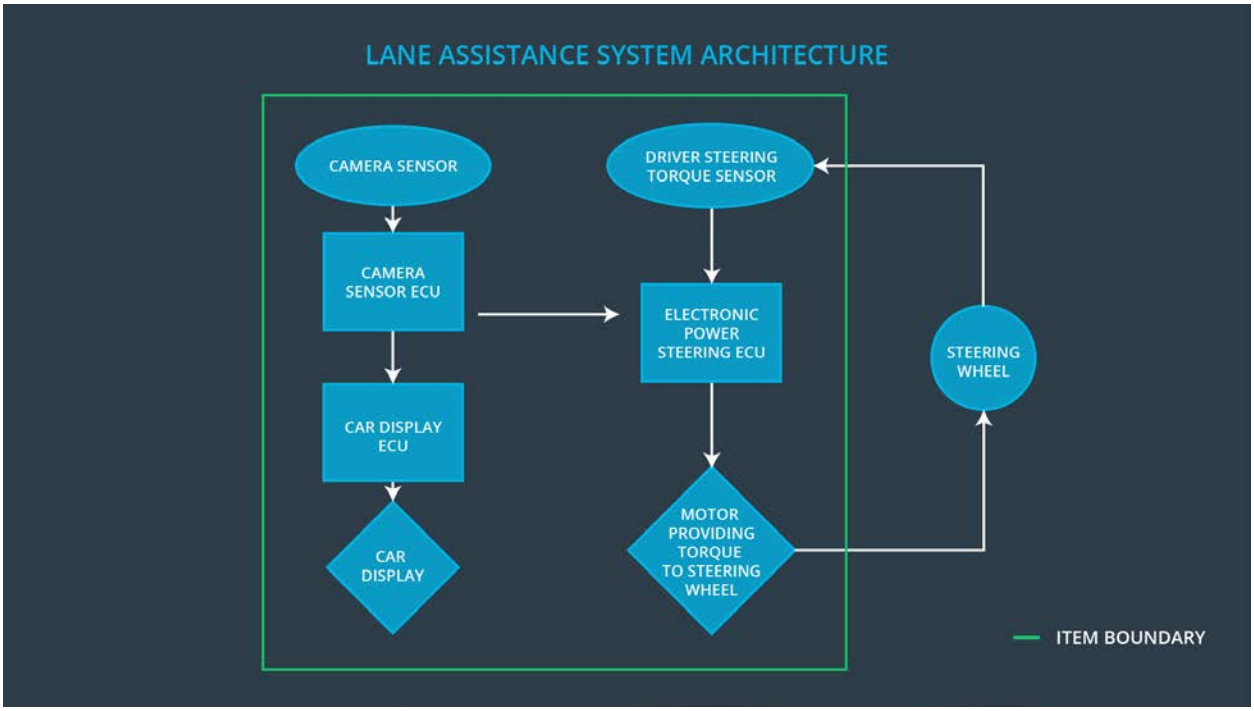
The item covered in the given project is the Lane Assistance System. It aides and warns the driver in particular driving situations, namely:

- **Lane departure warning**: When the driver drifts towards the edge of the ego-lane, the steering wheel vibrates (more precisely applies an oscillating steering torque) to inform the car driver.
- **Lane keeping assistance**: When the driver drifts towards the edge of the ego-lane, this mechanism will apply steering torque in order to turn wheels turn towards the center of the lane.

The item's functionalities are based on the following subsystems:

- **Camera subsystem** – consists of 2 components:
  - Camera sensor
  - Camera sensor ECU (Electronic Control Unit)
- **Electronic Power Steering subsystem** – consists of 3 components:
  - Driver Steering Torque Sensor.
  - Electronic Power Steering Electronic Control Unit.
  - Motor Proving Torque to Steering Wheel.
- **Car Display subsystem** – consists of 2 components:
  - Car Display Electronic Control Unit
  - Car Display

The interaction between the three subsystems:



The camera subsystem is responsible for detecting lane lines and determining when the car approaches/leaves the lane lines. Issues steering and warning request to the electronic steering ECU.

The electronic power steering subsystem detects how much the driver has already turned the wheel and adds a counter-acting extra torque required to turn the car back towards the lane center. The car display subsystem is only responsible for showing the warning when applicable.

The Lane Assistance Systems disengages when the driver uses the turn signal. Another way to turn the system off is to use the specific function button on the console.

Goals and Measures

Goals

The key goal of this project is to assure functional safety of the Lane Assistance System and ensure safe and reliable operation of all the underlying components according to ISO 26262. This can be divided into three separate parts:

1.) Identifying the risks and hazardous situations when a malfunction may cause injuries to a person.
2.) Evaluating the risk of the given hazardous situations.
3.) Lowering the risk of the malfunctions to reasonable levels that are acceptable 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

To increase functional safety, safety culture characteristics needs to be implemented. Safety has the highest priority among ALL opposing constrictions like cost and efficiency. All (sub)processes must ensure accountability so that design choices are retraceable to the specific people and teams who made those. Employees are incentivized and promoted based on obeying to company principles to produce documented, tested and verified systems. Our management sits on the board of international safety

committees which develop standards. Employees found to be in non-compliance with our safety must face immediate consequences. Project managers who compromise safety, testing and documentation to promote project schedule and budget are dismissed.

Projects have necessary resources including people with suitable skills. Intellectual diversity is sought after, valued and integrated into processes. Development and auditing teams must be independent and have to involve people of different of intellectual backgrounds. It is crucial that communication between those teams is based on full disclosure of problems. Company design and management processes should be clearly defined, and the communication channels encourage disclosure of problems.

Safety Lifecycle Tailoring

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

This product shall be integrated into an existing vehicle architecture. All relevant interfaces shall be involved in the scope. Functional safety shall be reflected for all interactions and secondary interactions with miscellaneous vehicle subsystems.

Production and Operation

Roles

Role	Level	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 goal of the development interface agreement is to delineate the roles and responsibilities between original equipment manufacturer and the Tier-1 Supplier taking part in developing this specific product. Prior to the project start both parties come to an agreement on the contents of the development interface agreement. The document also states what indication and work products the manufacturer and the first tier party will provide to demonstrate that work was done according to the contract.

Based on the joint tailoring of the safety lifecycle the partied agreed that the tailored safety lifecycle is enough to fulfill the requirements of the ISO 26262 standard in terms of the described lane assistance system.

The OEM is responsible for supplying the hardware base (both first version prototypes and the final product) and define its safety lifecycles. This shall be extended with the overall vehicle safety and all ISO 26262 required functional safety actions. Hardware specific interfaces and datasheets shall be maintained as well along with the test data created. The OEM's responsibilities include the appointment of the safety manager.

The Tier-1 Supplier is responsible for the lane assistance component only. Other parts of the vehicle are not concerned here. Based on this fact it shall examine and adjust various (sub)systems of the component from a *functional safety* standpoint. Tier-1 shall appoint its own safety manager. The system's safety lifecycle along with the systems level architecture specifications must be created. Functional safety analyses shall be provided on both software and hardware architecture levels. Verification and design documentation shall be created for both the subsystems and the integration (system) level.

Confirmation Measures

Confirmation measures ensures that the Lane Assistance functional safety project conforms to ISO 26262 and verifies whether the design actually does improve safety.

The confirmation review ensures that the development complies with ISO 26262, and during design and development of the product, compliance with ISO 26262 is guaranteed by an independent person who is independent from the design team.

The functional safety audit checks the concrete implementation of the project conforms to the safety plan.

Last but not least, the functional safety assessment checks that project plans, designs and development really 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.