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
08/27/2018	1.0	[NOT_PUBLIC]	First submission of the completed safety plan

Table of Contents

Introduction

Purpose of the Safety Plan

The ISO 26262 functional safety standard applies to automotive passenger vehicle electrical and electronic systems. Its goal is to reduce risk as a result of malfunctioning behavior of E/E systems and thus covers only one part of the overall vehicle safety. Functional safety means to identify high risk situations and lower the risks to reasonable levels. As systems can become quite complex, the standard provides guidelines to structure the process and requires documentation for transparency and auditability. Among others, the safety plan is one required document. It gives an overview of how a safe system is achieved. The safety plan describes the system under consideration, the goal of the project, the steps taken to ensure safety, the roles and personnel involved, and the project timeline.

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 project considers a simplified version of a Lane Assistance System (LAS). The LAS alerts the driver when the vehicle detects an unintended attempt to leave the lane and takes over control to steer the vehicle back to the center of the lane. The system categorizes attempts as unintended, when the vehicle is approaching the edge of the lane without the turn signal being on. The system is deactivated, when the turn signal is on or it was shut down by the driver by pushing a button.
The LAS consists of two main functions which are Lane Departure Warning (LDW) and Lane Keeping Assistance (LKA).

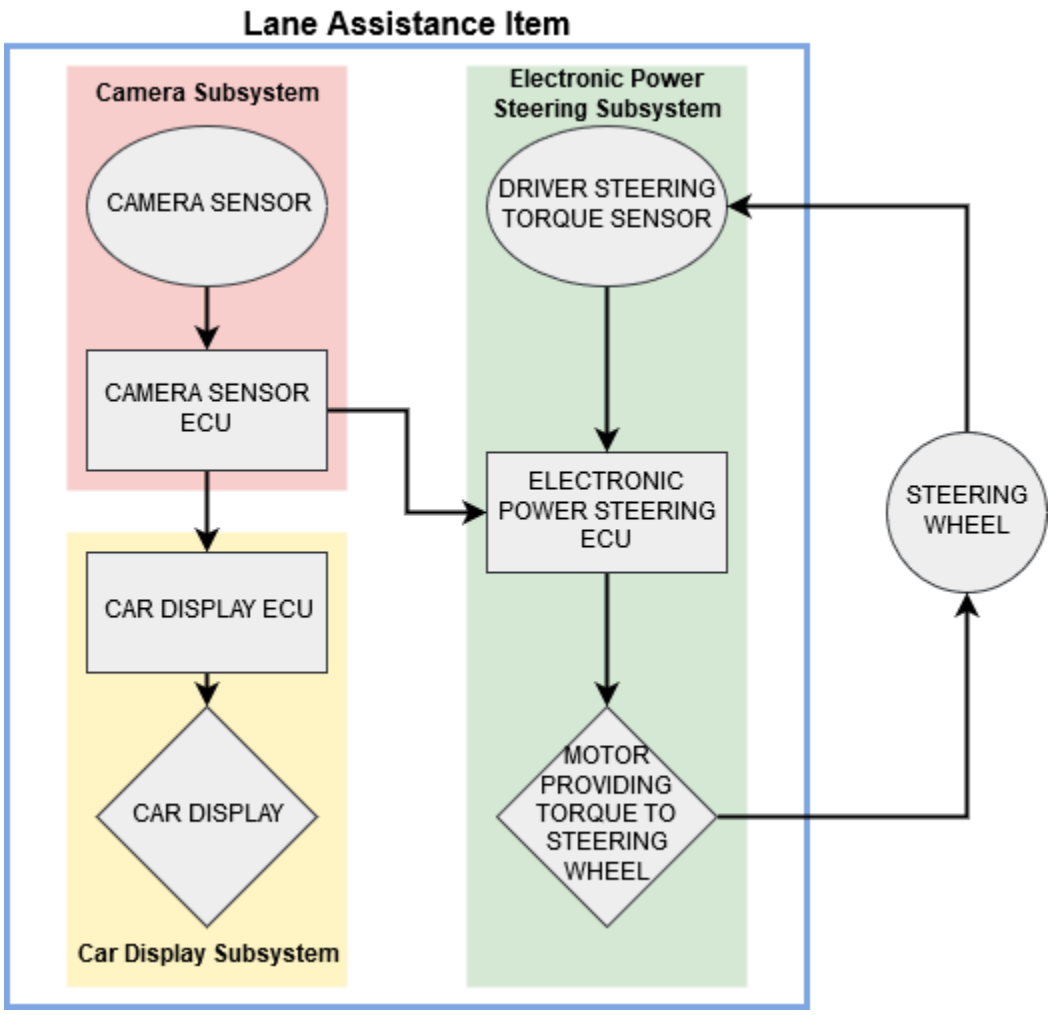
- Lane Departure Warning (LDW): The steering wheel will vibrate to indicate to the driver that the vehicle is drifting towards the edge of the lane.
- Lane Keeping Assistance (LKA): The function applies a steering torque to move the vehicle from the edge of the lane back to the center of the ego lane, which is the lane where the car is currently driving in).

In addition to these two functions, a warning light shall be displayed on the display dashboard to inform the driver about the system interaction.

There are three subsystems involved to implement the LAS functionality:

- Camera subsystem consisting of:
    - Camera Sensor
    - Camera Sensor Electronic Control Unit (ECU)
- Electronic Power Steering subsystem consisting of:
    - Driver Steering Torque Sensor
    - Electronic Power Steering ECU
    - Motor Providing Torque to Steering Wheel
- Car Display subsystem:
    - Car Display
    - Car Display ECU

The camera subsystem (light red) takes images of the camera sensor and extracts the position of the car in the ego lane. It detects when the car drifts towards the edge of the lane and informs the car display subsystem (light yellow) and the electronic power steering system (light green) about that. The car display subsystem shows a warning light in the car display dashboard when necessary. The electronic power steering subsystem takes the reading of the driver steering torque sensor to detect how much steering torque the driver is already applying. It then calculates how much additional torque is necessary to steer the vehicle back towards the center of the lane and lets the motor apply that torque to the steering wheel.
The LAS does not provide autonomous driving functionality and the driver is expected to have both hands on the steering wheel the whole time.
The following image shows the boundaries of the item, the subsystem, and the interactions between them:



Goals and Measures

Goals

The goal of this project is to analyze the Lane Assistance System (LAS) to assure safe operation according to ISO 26262. Therefore, the item's components must be analyzed to identify risks and hazardous situations where LAS components malfunction could cause injuries. Those risks of hazardous situations need to be evaluated and lowered to an 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

The highest priority in a company that lives a safety culture is safety. No matter what constraints regarding costs or productivity the company has to comply, safety remains at the top. Additionally, a good safety culture has the following characteristics:

- Accountability: Design decisions are traceable back to the people and teams who made them
- Rewards: The organization motivates and supports the achievement of functional safety
- Penalties: The organization penalizes shortcuts that jeopardize safety or quality
- Independence: Design and development are independent from auditing
- Defined Processes: Company design and management processes are clearly defined
- Resources: Projects have necessary resources including people with appropriate skills
- Diversity: Intellectual diversity is sought after, valued, and integrated into processes
- Communication: Channels encourage disclosure of problems

The top-level management as well as every employee works and acts by those values. They are the base for guaranteeing functional safety and improving overall product quality.

Safety Lifecycle Tailoring

When updating existing products and not developing something new from scratch, the safety lifecycle can be tailored to the project. This means only necessary steps of the V model (specified in ISO 26262) need to be applied.
The Lane Assistance System project is an update project and thus only considers the following phases:

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

On the other hand, 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 automotive supply chain typically follows a pyramidical structure where the Original Equipment Manufacturer (OEM) sits at the top and the suppliers sit in the levels below. The suppliers are categorized regarding the number of intermediaries between them and the OEM. The suppliers that directly interact with an OEM are called Tier-1 suppliers and the suppliers of Tier-1s are called Tier-2 suppliers, etc.
The Development Interface Agreement (DIA) delineates the design and production responsibilities between the OEM and the Tier-1 or the Tier-1 and the Tier-2 supplier. The involved parties agree on the contents of the DIA before the project begins. The DIA includes:

- Appointment of customer (OEM) and supplier safety managers
- Joint tailoring of the safety lifecycle

- Activities and processes to be performed by the customer (OEM) and by the supplier
- Information and work products to be exchanged
- Parties or persons responsible for each activity in design and production
- Any supporting processes or tools to ensure compatibility between the customer (OEM) and supplier technologies

The DIA helps to avoid disputes during the project and manifests liability for the components of the product.
In this project the OEM provides a functioning Lane Assistance System (LAS) and is responsible for the functional safety of the item. The OEM will provide item-level requirements which are the basis for the work of the Tier-1 supplier on the component level. The Tier-1 supplier analyzes some of the subsystems and modifies them according to functional safety requirements. The safety managers of both companies will in close contact to exchange necessary know-how, documentation, and to agree on the tailored safety lifecycle.

Confirmation Measures

Confirmation measures check whether the processes comply with the functional safety standard, the project execution is following the safety plan, and the design really improves the safety. It is important that those measures are executed by independent parties to make sure as little bias as possible is involved. The three aforementioned goals of the confirmation measures are achieved with a confirmation review, a safety audit, and a functional safety assessment. The confirmation review ensures that the project complies with ISO 26262. The functional safety audit makes sure the actual implementation of the project conforms to the safety plan. Finally, the functional safety assessment confirms that plans, designs and implementations 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.