Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.1
Released on 2017-10-30

Document history

Date	Version	Editor	Description
2017-10-21	1.0	Martin Hintz	Initial Version
2017-10-30	1.1	Martin Hintz	Layout and spelling corrections

Table of Contents

Introduction

Purpose of the Safety Plan

This document provides an overall framework for the functional safety of the Lane Assistance Functionality of the new model vehicle. This safety plan ensures compliancy with ISO 26262.

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 Lane Assistance Functionality detects if the vehicle is deviating from its traffic lane and subsequently performs automatic corrections to the steering of the vehicle back towards the center of the lane. The driver of the vehicle will also receive a visual warning on case the Lane Assistance Functionality is being activated.

The following figure depicts an overview of the system architecture of the Lane Assistance Functionality and its main components.

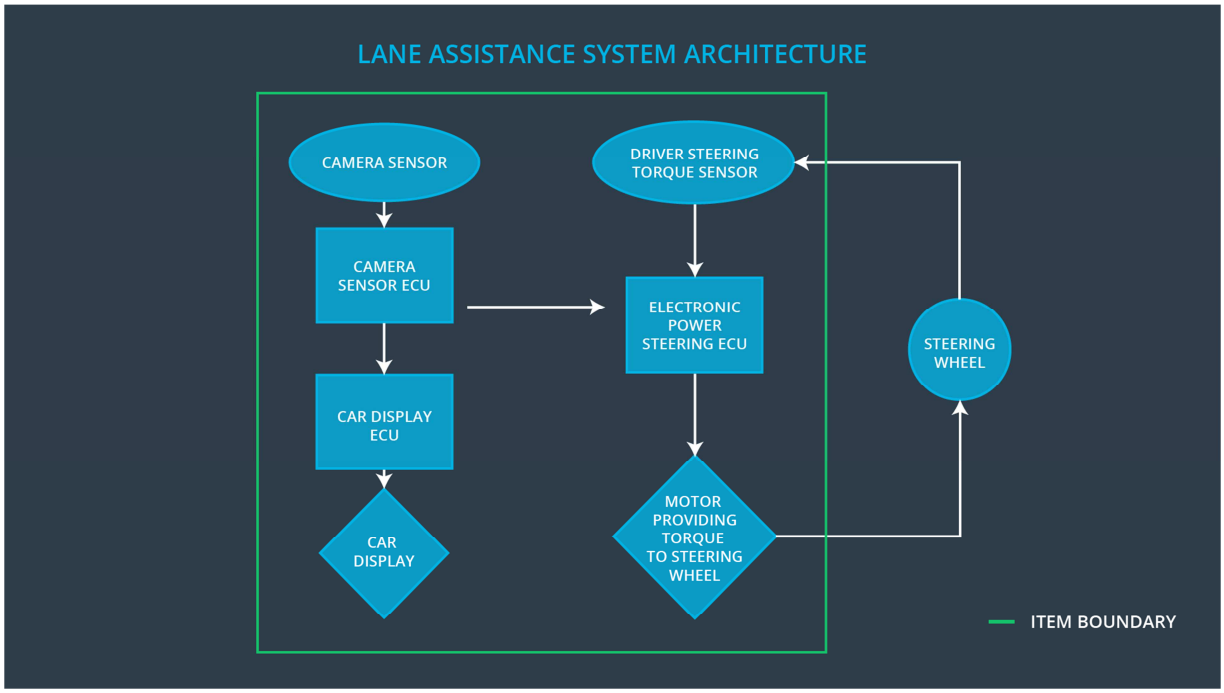

Figure 1: Lane Assistance System Architecture

The Lane Assistance Functionality has two main functions

- audio-visual warning
- steering assistance

Audio-visual warnings are visible in the car's display in front of the driver. Warnings will be activated when the system senses the vehicle deviates from its lane and before the steering assistance kicks in to allow the driver to correct the vehicle's trajectory. Warnings include a flashing sign as well as a distinguishable sound.

Steering assistance is activated when the driver does not react to the audio-visual warnings and the vehicle continues to drift away from its lane. Steering assistance will autonomously turn the steering wheel to return the vehicle back to the center of the lane. At any point of time the driver can interrupt this process by turning the steering wheel.

The following subsystems can be defined for the Lane Assistance Functionality:

- Camera sensor and its ECU
- Car display and its ECU
- Electronic power steering, consisting of ECU, motor and torque sensor

The camera sensor captures lane line data from multiple sensors on the front of the vehicle. The camera ECU processes the incoming data in real-time and detects the position of lane lines by using a combined computer vision and deep learning approach. Whenever the need for a course correction is detected the camera ECU simultaneously sends a signal to the power steering to take control of the vehicle's steering and another signal to the car display to display a warning to the driver.

The car display receives signals from the camera and displays audio-visual warnings if required. These warnings alert the driver of an ongoing deviation from its lane and the imminent activation of the steering assistance.

The electronic power steering, consisting of ECU, motor and torque sensor, is responsible to execute the action to correct the vehicle's trajectory in a feed-back loop. When a signal arrives from the camera ECU to active steering assistance, the power steering ECU calculates the required angles that must be applied to the steering wheel. Then, the motor is providing torque to the steering wheel to account for the necessary correction. A torque sensor on the steering wheel ensure that at any point of time the driver can interrupt this process by turning the steering wheel.

The Lane Assistance Functionality boundary includes all subsystems and components mentioned in the system architecture diagram in Figure 1, except the steering wheel. This includes the camera sensor and its ECU, the car display and its ECU, the electronic power steering ECU, the motor that provides torque to the steering wheel as well as the driver steering torque sensor.

The Lane Assistance Functionality will have to work under various operational and environmental constraints. One operational constraint is the performance of the camera. A camera with sufficient resolution and framerate must be chosen that minimizes cost at the same time. The camera subsystem with the highest frame rate and resolution that minimizes overall cost is the most desirable. Environmental constraints mostly result from varying weather conditions that impact on the camera image and make it more difficult for the algorithms to detect lane lines. The algorithms and especially the deep learning training set must include enough training data to cover these scenarios.

Goals and Measures

Goals

The project ensures compliance with to ISO 26262 and thereby provides a safe operation of the lane assistance functionality of the vehicle.

Measures

Measures and Activities	Responsibility	Timeline
Follow safety processes	All Team Members	Constantly
Create and sustain a safety culture	Safety Manager	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 safety culture in our company perceives safety as:

- **highest priority!** Safety has the highest priority, even among competing constraints like cost and productivity.
- **accountable!** Our established processes ensure that design decisions are traceable back to the people and teams who made the decisions.
- **rewarding!** Our whole organization motivates and supports the achievement of functional safety.
- **behaving with integrity!** The company penalizes shortcuts that jeopardize safety or quality.
- **Independent!** Our teams who design and develop a product are independent from the teams who audit the work.
- **well defined in its**
    - **processes!** Design and management processes are clearly defined across our organization.
    - **resources!** Projects in our company have necessary resources and people with appropriate skills.
- **multifaceted!** Intellectual diversity is sought after, valued and integrated into all our processes every day.
- **communicative!** Open communication channels encourage disclosure of problems across hierarchy levels and departments.

Safety Lifecycle Tailoring

The safety lifecycle is tailored to any new features of the lane assistance function derived from the previous model. Focus is laid on the changes in functionality and processes.
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

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

This development interface agreement defines the roles and responsibilities between the all companies involved in developing the Lane Assistance Functionality of the new model vehicle and ensure its compliance with ISO 26262.

Our company will develop and provide the source code for Lane Assistance Functionality In addition we will conduct a first safety analysis before handing it over to and independent safety assessor. Successive modifications to the system or any sub-systems of the Lane Assistance Functionality from a functional safety standpoint are also handled by our organization. For details on the appointments of safety managers (customer as well as supplier), please refer to the roles defined in the previous section (“Roles”).

Confirmation Measures

The confirmation measures provided ensure that the Lane Assistance Functionality:

- conforms to ISO 26262
- makes the vehicle safer to drive

In a confirmation review, an independent auditor will perform a review of the work as the product is designed and developed.
In addition, a functional safety audit of the actual implementation of the Lane Assistance Functionality will be conducted to ensure its conformance to the safety plan, which is also outlined in this document.
The final step is a functional safety assessment of the independent auditor that confirms that the Lane Assistance Functionality fulfills all functional safety requirements.