Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.1

Document history

Date	Version	Editor	Description
31.12.2018	1.0	Michael Ikemann	Definition of the initial safety concept of the LGA
12.01.2019	1.1	Michael Ikemann	Finalized version of safety plan

Table of Contents

Introduction

Purpose of the Safety Plan

The purpose of the safety plan is to define how the safety of a newly developed lane assistant system which shall automatically keep the car within road lanes and/or warn the driver if he unintentionally crosses one of the lanes markers / leaves the raid without prior activating the indicator can be guaranteed. It further defines which precautions can and need to be taken to secure the driver's and traffic participants safety in case of a malfunction of one or multiple of the system's items and how to prevent such fault behavior in advance.

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

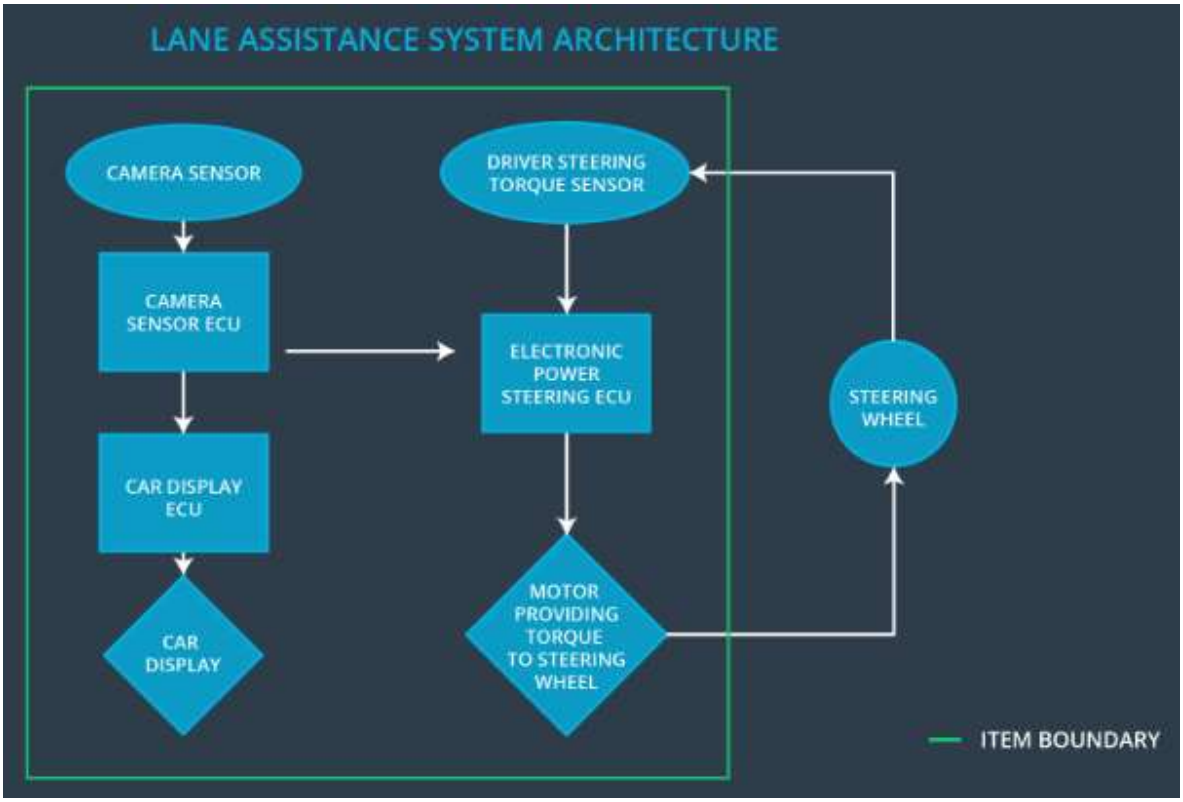
We want to develop a new device called Lane Guidance Assistant – hereinafter known as LGA – with the following features:

- Detection of the lines of the lane the car is currently driving on with the help of a camera system mounted at the top of the windshield – such as the one already used in our just released automatic high beam optional feature. See MBC-2844-2211.
- Centering of the vehicle within the lane by applying a slight torque to the steering wheel if a given threshold distance to the optimal driving line was exceeded and the lane lines were detected with a high certainty level.
- Enabling a slight vibration at the steering wheel to inform the driver if he unintentionally or without activated turn signal crosses one of the detected lines.

Limitations

- The system is not intended to be used as a fully autonomous solution. As it uses just the already proven high beam assistant camera system without further backup such as radar, lidar or a secondary camera system and is not able to detect complex lane situations such as in road work areas it shall also not be mistaken as such.
- To prevent the usage as autonomous system the system will automatically be deactivated (after a prior warning sound and visual signal in the dashboard) if the LGA needs to provide the major amount of torque to keep the car in the center of the lane and/or no touch of the steering wheel was detected for a short amount of time.
- The system can only work if it is able to detect the lane lines with a high amount of certainty. This is not given if
    - The street is covered by snow
    - It’s raining intensively, and the camera sensor may be covered, and/or the lane lines are not clearly detectable
    - The lane lines are withered and/or not clearly detectable (for example caused by road works)

Sub systems



The system consists of overall two major sub systems:

- The camera system which is currently already in use for our high beam assistant system.
  It tries to detect the lanes to the left and right of the vehicle.
  If lane lines were detected it calculates if the vehicle currently inadvertently crosses one of the lane lines or how far it drifted away from the optimal lane center.
  When a lane is crossed and no matching turn signal was activated it informs the car display to enable a warning while at the same time sending a request to the electronic power control unit to enable a vibration of the steering wheel to catch his attention.
  In addition it senses a request to the ECU to apply a given amount of torque to the steering wheel to correct the vehicle's course back to the center of the lane.
- The EPS ECU (Electronic Power Steering Unit) which receives the requests from the camera ECU if it shall enable a vibration of the steering wheel and/or apply torque to the steering wheels motor to correct the vehicle's course.

Goals and Measures

Goals

The goal of this project is to ensure that all participants of this project are in compliance with ISO 26262.

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 Auditor	3 months prior to main assessment
Perform functional safety assessment	Safety Assessor	Conclusion of functional safety activities

Safety Culture

Safety has the highest priority in our company - we ensure this by planning our projects including an extensive quality assurance step after each development phase. In addition we create a detailed protocol of every decision meeting to track the accountability of our decisions.

Every employee is encouraged to follow this bonus and is highly awarded for especially successful assessments of the products developed in theirs teams.

The auditions of our products is performed by QNA Corporation, an independent Quality Assurance company which provides ISO 26262 compliant auditions and consulting support.

Safety Lifecycle Tailoring

The following phases are within the scope of this project

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

The following phases are not within the scope of this project because already existing hardware will be used to implement the LGA:

- 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 Developer Interface Agreement (DIA) is to define the role of each participating company of the project, to ensure that all of the parties involved develop theirs products in an ISO 26262 compliant manner, the responsibilities in each company to fulfill this are clearly defined, a clear definition of the safety life cycle is provided and how this is ensured by each of the companies

Our job as tier 1 supplier is to develop the software which provides the LGA functionality using the already existing hardware, to ensure that the subsystems are – when extended with the new LGA system– still ISO 26262 compliant, that the system is designed in a way that he will not use or get the impression he could use the LGA system in a pure autonomous way, that the lane-leave alerting function will not irritate the user in a way it could lead to an accident and to ensure that the driver will at all times be able to take the control of the car again in the very rare case of functional failures or detection errors of the camera system.

Confirmation Measures

The goal of the confirmation measurement is to ensure that the project conforms to ISO26262 and that the project will increase the driver’s safety.

The confirmation review ensures that all requirements of ISO26262 are met. This will be verified within a safety audit.

When all requirements are met a functional safety assessment will be performed to confirm that the project really actually does achieve functional safety.