Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
2017-10-16	0.1	Wilhelm Nagel	Initial Version

Table of Contents

Introduction

Purpose of the Safety Plan

The purpose of the Safety Plan is to document how Functional Safety will be realized in the Lane Assistance project. The plan covers the complete life cycle of the product from development to production and operation. The plan describes how potential malfunctions of the involved electrical and electronic systems as defined by ISO 26262 will be considered, i.e. mechanical or chemical systems are outside the scope of the plan according to 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 item in question is a simplified Lane Assistance System for passenger vehicles. The main task of the Lane Assistance System is to support the human driver to keep driving within the current lane, i.e. to avoid unintentionally crossing lane boundaries. To achieve this, the Lane Assistance System applies additional torque to the steering so that the vehicle steers towards the center of the lane.
To avoid endangering the passengers of the vehicle and other traffic participants at high speeds, Functional Safety aspects have to be considered for the Lane Assistance system.

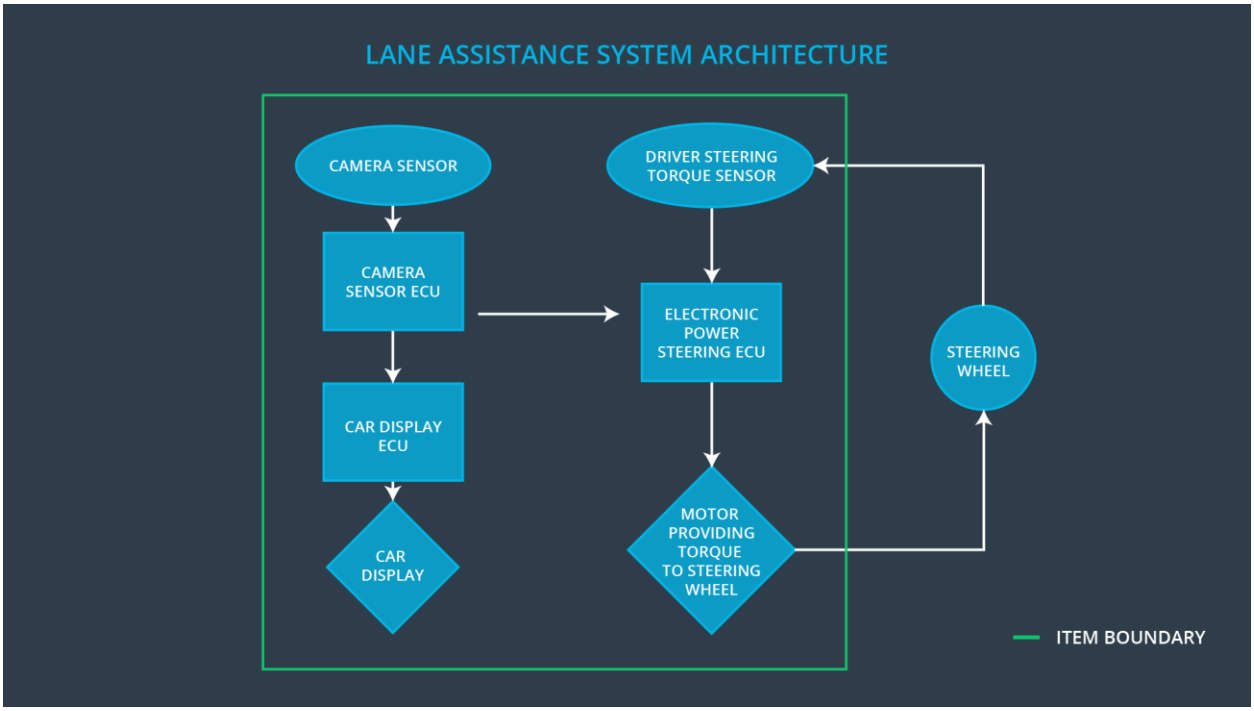

Figure 1: Architectural diagram of Lane Assistance

The Lane Assistance System is comprised of two main functions which are shown in Figure 1:

- The Lane Departure Warning (LDW) alerts the human driver if vehicle is assumed to leave the lane by
    - optical hints in the Car Display
    - haptical hints by vibrating the steering wheel
- The Lane Keeping Assistance (LKA) actively steers the vehicle towards the center of the current lane when the system detects that the vehicle is unintentionally approaching a lane boundary. To avoid interfering with intentional lane changes,
    - the system checks if the turn signal was activated by the driver and
    - only corrects steering if the turn signal is off

The Lane Assistance System can be divided into the following sub systems as can be seen in Figure 2:

- The Camera Sensor is responsible for determining the position of the vehicle within the current lane by detecting lane markings.
    - in case of corrective actions, the Camera Sensor signals the Car Display to display a warning and the Electronic Power Steering to do corrective actions
    - the Lane Detection status, i.e. the ability of the Camera Sensor to detect the boundaries of the current lane is signaled to the Car Display to display the availability of the Lane Assistance function
- The Car Display is responsible for displaying the current state of the Lane Assistance System, e.g. by displaying visual warnings when the system assumes unintentional leaving of the current lane
    - the Car Display receives its inputs from the Camera Sensor
        - unintentional approach of a lane boundary
        - availability of Lane Assistance Function
- The Electronic Power Steering is responsible for correcting the unintentional divergence from the center of the current lane and to give haptical feedback about system activity by vibrating the steering wheel
    - the Electronic Power Steering receives its inputs from the Camera Sensor and from the Steering Wheel

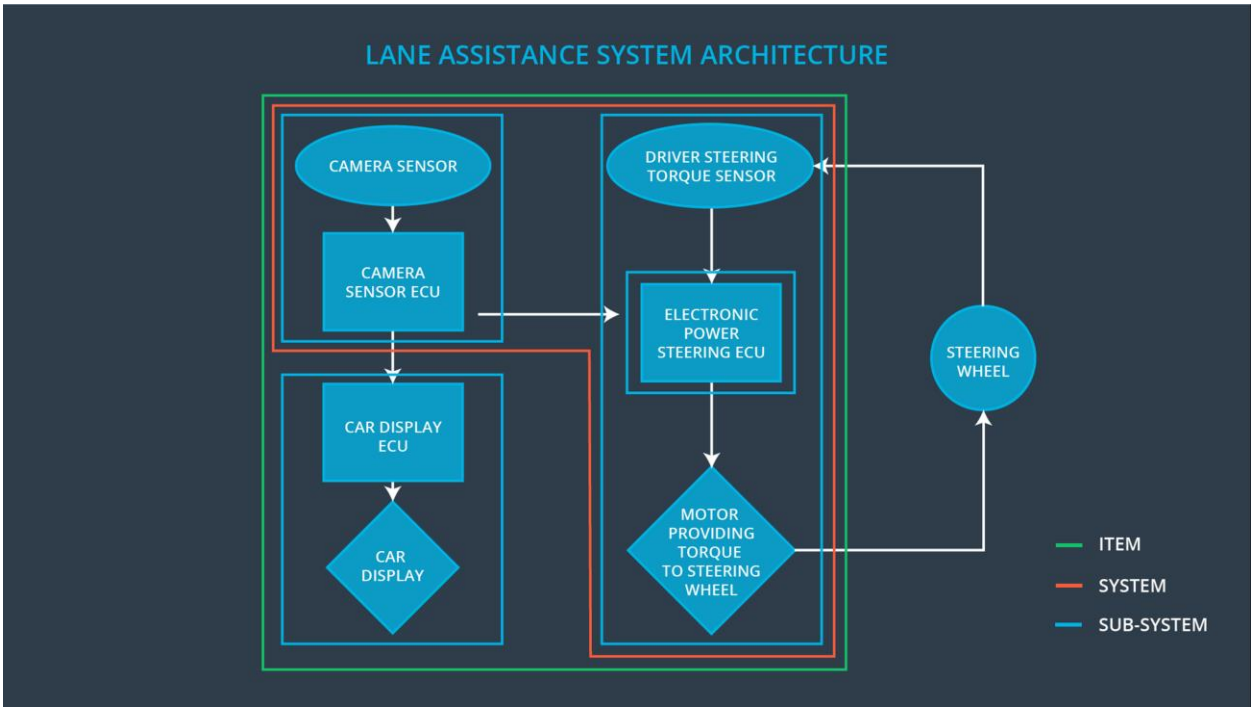

Figure 2: Sub systems of Lane Assistance

The subsystems and their connections are shown with blue boundaries in Figure 2:

- Camera Sensor
- Car Display
- Electronic Power Steering

The following common ADAS functions do not belong to the Lane Assistance System item and are not treated in this document:

- Adaptive Cruise Control
- Automatic Parking
- Blind Spot Monitoring
- Tire Pressure Monitoring
- Pedestrian Protection

Environmental Constraints:

- The Camera Sensor can’t detect lane boundaries in bad weather conditions, e.g. rain, fog and snow.
- The Lane Assistance System is intended to operate at typical speeds on highways, i.e. the system is not intended to be used in urban traffic.

Goals and Measures

Goals

Lane Assistance System should be designed in a way that the currently available technology is used to achieve an acceptable safety level. To achieve this, the Functional Safety of the system will be analyzed by

- Identifying hazardous situations that could arise from malfunctions of the Lane Assistance System and that may cause physical injuries to a person.
- Evaluating the risk of identified hazardous situations.
- Lowering the risk by means of systems engineering to reasonable levels so that accidents are prevented.

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	Safety 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 establish a good Safety Culture, the Lane Assistance System is developed by following these principles:

- **High Priority**: safety has the highest priority among competing constraints like cost and productivity
- **Accountability**: processes ensure accountability such that design decisions are traceable back to the people and teams who made the decisions.
- **Rewards**: the organization motivates and supports the achievement of functional safety
- **Penalties**: the organization penalizes shortcuts that jeopardize safety or quality
- **Independence**: teams who design and develop a product should be independent from the teams who audit the work
- **Well defined processes**: Company design and management processes should be clearly defined
- **Resources**: projects have necessary resources including people with appropriate skills
- **Diversity**: intellectual diversity is sought after, valued and integrated into processes
- **Communication**: communication channels encourage disclosure of problems

Safety Lifecycle Tailoring

The ISO 26262 standard was tailored for the Lane Assistance System to include the following safety lifecycle phases:

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

The activities on the left side of the V-Model are subject to tailoring, while the activities on the right side are outside the scope:

- Product Development at 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 Development Interface Agreement is a contract between two parties involved in the development of the Lane Assistance System where one party (e.g. the OEM) orders the services of the other party (e.g. Tier 1). The contract

- details the roles and responsibilities between the two parties
- defines the artifacts and services that have to be provided to achieve the project goal
- identifies the extend of responsibilities for Functional Safety issues after product development, i.e. in the postproduction phase

The DIA provides guidelines for communication between the involved parties and has to contain enough details to avoid disputes during planning, development and in the postproduction phase.

As a Tier 1 supplier our company will analyze the Lane Assistance System of the OEM in regards to Functional Safety according to ISO 26262.

- The OEM is responsible for providing requirements with all details necessary to perform the Functional Safety analysis.
- Our company will ensure that the Functional Safety analysis will be performed in accordance to the ISO 26262 and also that the created documents conform to the standard

The OEM appoints a Functional Safety Manager who collaborates with Tier 1 to coordinate the planned Functional Safety activities including

- Tailoring of the Safety Lifecycle
- Concept Phase
- Product Development at System and Software Level

]

Confirmation Measures

The main purpose of Confirmation Measures is to ensure that

- The performed processes comply with the Functional Safety Standard
- The project execution follows the Safety Plan
- The design really does improve safety

The Confirmation Measures are carried out by independent people who are not involved in the design and implementation of the product.

Confirmation Review
A 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

Functional Safety Audit
A Functional Safety Audit makes sure that the actual implementation of the project conforms to the Safety Plan.

Functional Safety Assessment
A Functional Safety Assessment confirms that the plans, designs and developed products 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.