Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
25.02.2020	1.0	Uwe Ehmann	Initial document

Table of Contents

Introduction

Purpose of the Safety Plan

The safety plan provides a framework for methodical planning and execution in order to develop a safe product. It also defines responsibilities between players involved in the project.

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 is a ADAS (Advance Driver Assistance System) called lane assistance system. Generally, the item warns the driver about unintendingly leaving the lane (LDW) and keeps the car in the lane accordingly (LKA).

It consists of two major functions:

1. Lane departure warning (LDW)
2. Lane keeping assistance (LKA)

The LDW tracks the current position of the vehicle in the lane and the lane lines by using onboard sensors like the camera. It applies a high frequent oscillating torque (vibration) to the steering wheel as soon as it detects a possibly unintended shift towards the lane lines.

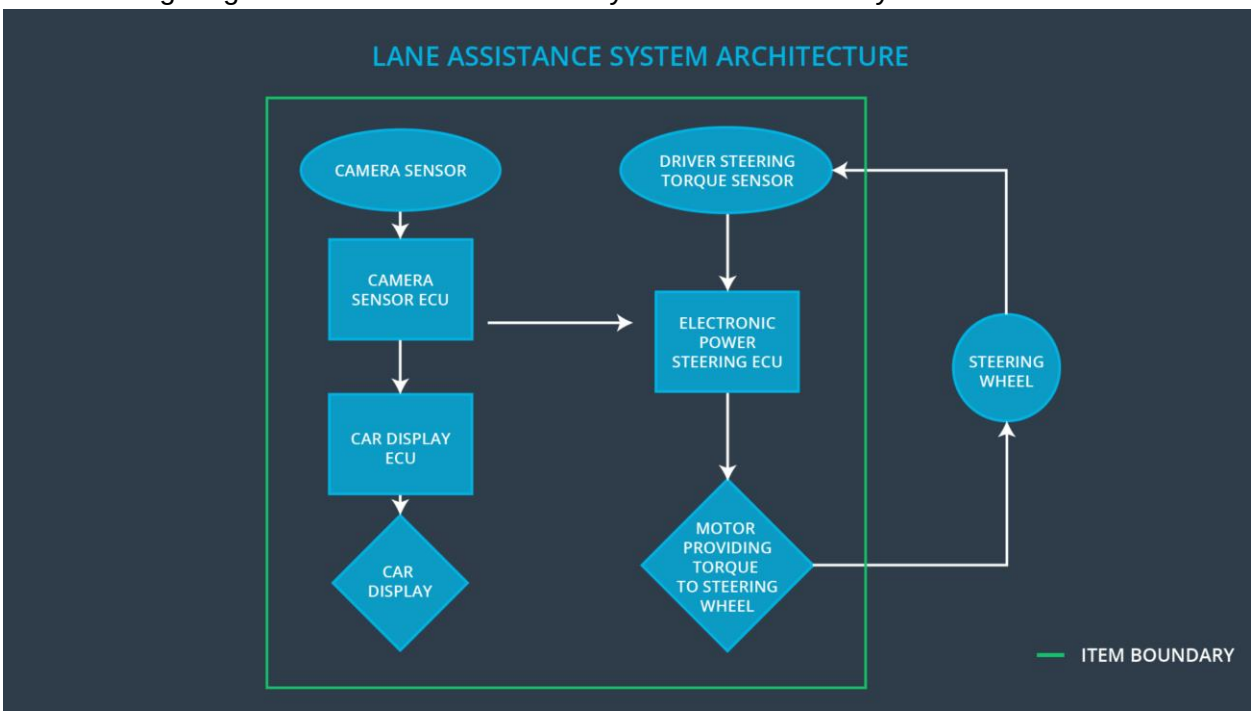
The LKA applies finally a steering torque that moves the vehicle back to the center of the line.

The item consists of three subsystems:

- Camera subsystem
- Electronic power steering subsystem
- Car display subsystem

All subsystem are involved to establish overall functionality for both LDW and LKA.

The following diagram show the item with subsystems and boundary.



Goals and Measures

Goals

The goal of this safety plan is to reduce risks of the item to acceptable levels.

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

Here are some characteristics of our safey culture:

- **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 safety lifecycle comes with the phases of the V-model.
In scope for this item are:

- 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

The purpose of the DIA is to define the roles and responsibilities between companies involved in developing a product. All involved parties need to agree on the contents of the DIA before the project begins. The ultimate goal is to ensure that all parties are developing safe vehicles in compliance with ISO 26262.

The roles of Tier-1:

- Functional Safety Manager- Component Level: Plan the development phase, pre-audits
- Functional Safety Engineer- Component Level: Develop prototypes, integrate subsystems into component

The roles of the OEM:

- Functional Safety Manager- Item Level: Plan the development phase, pre-audits
- Functional Safety Engineer- Item Level: Develop prototypes, integrate subsystems into the final lane assistance item
- Project Manager - Item Level: Overall project management. Allocates resources as needed
- Functional Safety Auditor: Makes sure that the project conforms to the safety plan
- Functional Safety Assessor: Judges whether the project has increased safety

Confirmation Measures

Confirmation measures serve two purposes:

- that a functional safety project conforms to ISO 26262, and
- that the project really does make the vehicle safer.

A confirmation review ensures that the project complies with ISO 26262.
A functional safety audit checks whether the project confirms to the safety plan
A functionanl safety assessment confirms that plans, design 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.