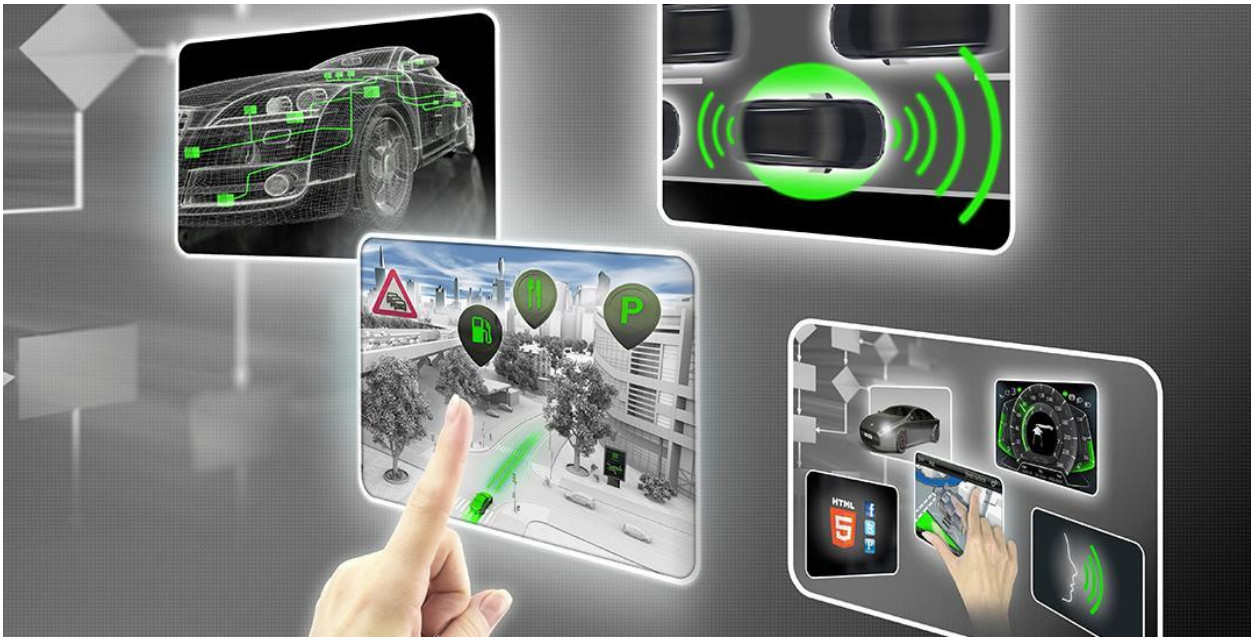
Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21



Document history

Date	Version	Editor	Description
2018-06-14	1.0	H. Kube	Initial version

Table of Contents

Table of Contents

Introduction
- Purpose of the Safety Plan
- Scope of the Project
- Deliverables of the Project

Item Definition

Goals and Measures

Document history
- Measures

Safety Culture

Safety Lifecycle Tailoring

Roles

Development Interface Agreement

Confirmation Measures

Introduction

Purpose of the Safety Plan

The purpose of the safety plan is to provide an overall framework for the Lane Assistance item, and to assign roles and responsibilities for functional safety for this item.

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 the Lane Assistance item which will alert the driver in case that the car accidentally departs its lane, and attempts to steer the car back toward the center of its lane. So, the Lane Assistance System has two functions:

- Lane departure waring
- Lane keeping assistant

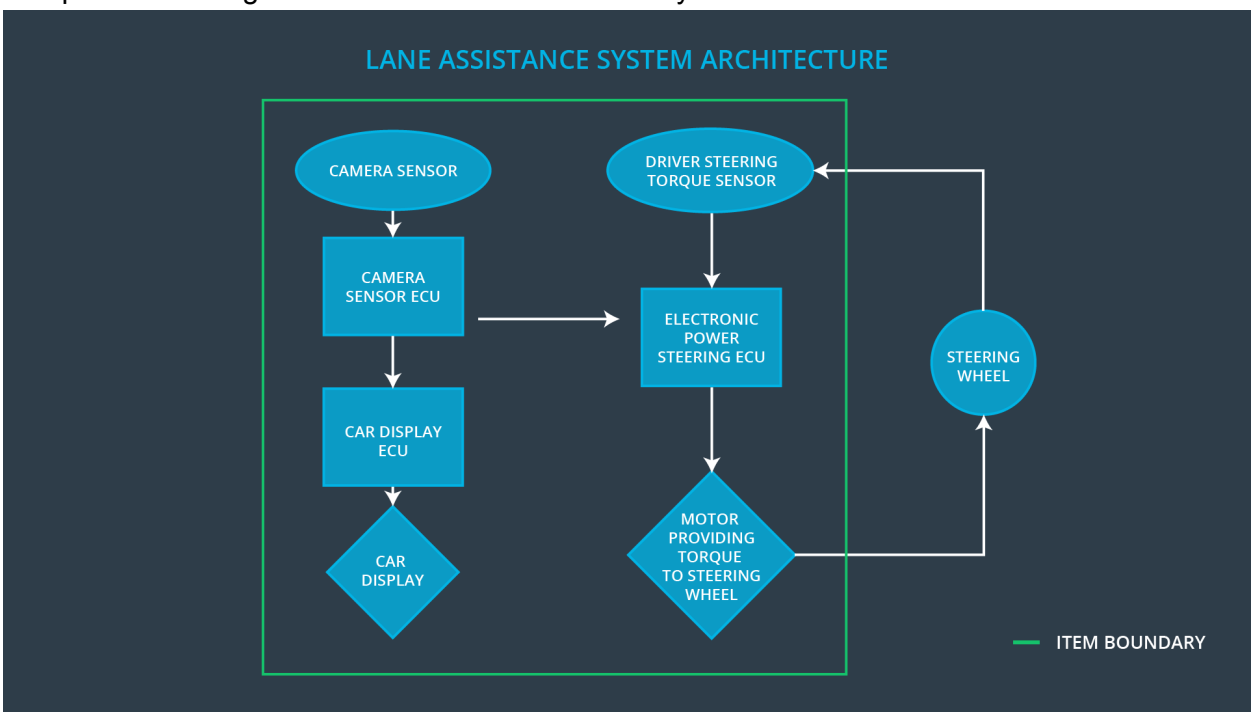
The lane departure warning shall apply an oscillating torque to the steering wheel to alert the driver.

The lane keeping assistant shall apply a torque to the steering wheel to steer the ego car back toward the center of the current lane.

The Lane Assistance item will use the following subsystems to fulfill its task:

- the Camera Sensor ECU is responsible for detecting the departure of the current lane
- the Electronic Power Steering ECU is responsible for shaking the steering wheel to alert the driver and for applying a torque to the steering wheel to steer the car back toward the center of the current lane
- the Car Display ECU is responsible for providing visual feedback to the driver

The picture below gives an overview about the subsystems of the Lane Assistance item:



Goals and Measures

Goals

The goal of this project is to assure the safe and reliable operation of the Lane Assistance item according to ISO 26262 by:

- identifying potential hazards in the Lane Assistance System
- evaluate the risk of the hazards
- lower the risk 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 characteristics of the safety culture is described by:

- **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

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

The purpose of the development interface agreement is to define the roles and responsibilities between the OEM and the tier-1 involved in developing this system. Both parties agree on the content of the development interface agreement before the project begins.

The development interface agreement also specifies what evidence and work products each party will provide to prove that work was done according to the agreement.

The ultimate goal is to ensure that all parties are developing safe vehicles in compliance with ISO 26262.

The tier-1 supplier is responsible for design and safety at the subsystem level. The OEM is responsible for design and safety at the system level.

The following steps are part of the development interface agreement and will be attached to this safety plan:

- Appointment of customer and supplier safety managers
- Joint tailoring of the safety lifecycle
- Activities and processes to be performed by the customer; activities and processes to be performed 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 customer and supplier technologies

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.

The confirmation review ensures that the project complies with the ISO 26262.

The functional safety audit makes sure that the actual implementation of the project conforms to the safety plan.

The functional safety assessment confirms that plans, designs and developed products actually achieve functional safety.