



Elektrobit



UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21



Document history

Date	Version	Editor	Description
08/13/2017	1.0	Yuesong Xie	First Draft

Table of Contents

Contents

Document history	1
Table of Contents.....	2
Introduction	3
Purpose of the Safety Plan	3
Scope of the Project.....	3
Deliverables of the Project	3
Item Definition.....	3
Goals and Measures	5
Goals	5
Measures	5
Safety Culture	5
Safety Lifecycle Tailoring	6
Roles	6
Development Interface Agreement.....	6
Confirmation Measures	7

Introduction

Purpose of the Safety Plan

The Safety Plan provides an overall framework to achieve Functional Safety for the lane assistance system. It defines roles and responsibilities for the development process and lists measures that will be used to achieve the targeted ASIL.

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 system warns the driver of an unplanned lane departure and takes corrective measures if necessary.

It is designed to minimize accidents by addressing human error in the form of a distracted or drowsy driver.

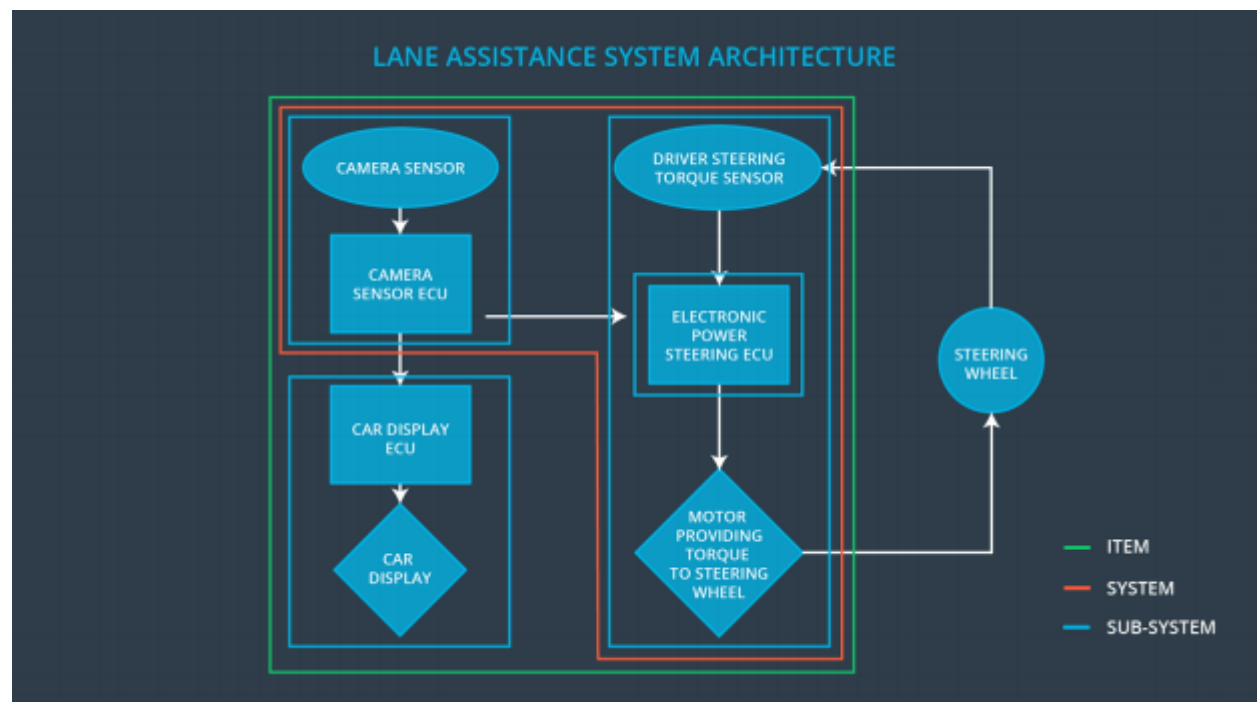
Main Functions of the lane assistance system include:

1. Lane departure warning
The lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback.
2. Lane keeping assistance
The lane keeping assistance function shall apply steering torque when active in order to stay in ego lane.

Architecture

The following subsystems are responsible for both functions:

1. Camera system: detects lane departures and tells the steering wheel how hard to turn.
2. Car Display system: displays a warning to driver.
3. Electronic Power Steering system: adds extra steering torque to help the driver move back towards the center of the lane.



Goals and Measures

Goals

Ensure the safe operation and functional safety of the Lane Assistance System.

To capture electric and electronic failures that could lead to a hazardous situation and to minimize the risk of failures by transitioning the system into a safe state

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	Project 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

- Safety has the highest priority among competing constraints like cost and productivity
- Processes ensure accountability such that design decisions are traceable back to the people and teams who made the decisions
- The organization motivates and supports the achievement of functional safety
- The organization penalizes shortcuts that jeopardize safety or quality

- Teams who design and develop a product are independent from the teams who audit the work
- Company design and management processes are clearly defined
- Projects have necessary resources, including people with appropriate skills
- Intellectual diversity is sought after, valued and integrated into processes
- Communication channels encourage disclosure of problem

Safety Lifecycle Tailoring

For the lane assistance project, the following safety lifecycle phases are in scope:

1. Concept phase
2. Product Development at the System Level
3. Product Development at the Software Level

The following phases are out of scope:

1. Product Development at the Hardware Level
2. 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

Purpose

A DIA (development interface agreement) defines 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 DIA 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.

Responsibilities

OEM shall supply a functioning lane assistance system.

Tier-1 shall analyze and modify the following sub-systems from a functional safety viewpoint:

- Camera system
- Car Display system
- Electronic Power Steering system

OEM shall arrange safety audits and the final safety assessment.

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 ISO 26262. As the product is designed and developed, an independent person would review the work to make sure ISO 26262 is being followed.

The functional safety audit checks to make 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.

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.