Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

[Instructions: Fill in the date, version and description fields. You can fill out the Editor field with your name if you want to do so. Keep track of your editing as if this were a real world project.

For example, if this were your first draft or first submission, you might say version 1.0. If this is a second submission attempt, then you'd add a second line with a new date and version 2.0]

Date	Version	Editor	Description
14.12.2017	1.0	Dhanasekaran	

Table of Contents

Confirmation Measures

Introduction

Purpose of the Safety Plan

The purpose of the safety plan is to identify & plan the safety activities that are required to develop functionally safe product 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:

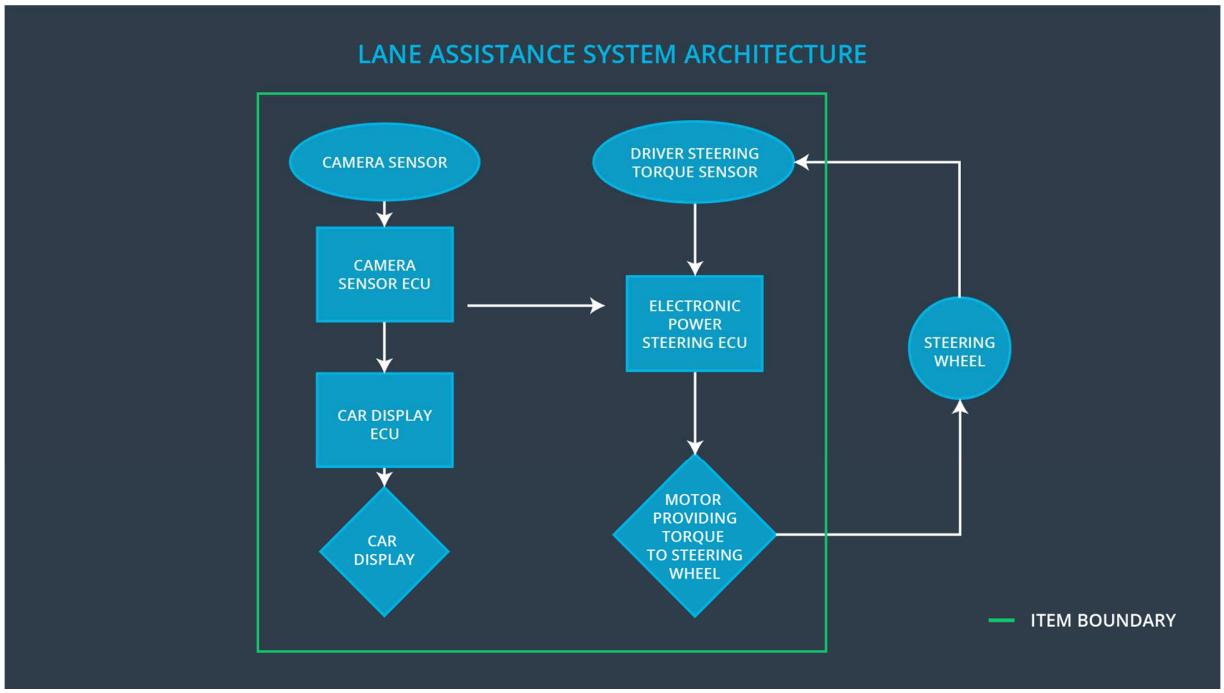
- Safety Plan
- Hazard Analysis and Risk Assessment
- Functional Safety Concept
- Technical Safety Concept
- Software Safety Requirements and Architecture

Item Definition

The Item name is “Lane assistance system”. It’s purpose is to assist the driver so that vehicle always stays in the center of the lane

The two main functions of the item are:
Lane Departure Warning: Applies an oscillating steering torque to provide the driver a haptic feedback
Lane Keeping Assistance: Apples an additional steering torque when active in order to stay in ego lane

Overview of Lane assistance system:



Subsystems:

- Camera subsystem: monitors the lane line and generate torque requests
- Electronic power steering subsystem: provides the final torque to the steering wheel
- Display system: displays the warning message to the driver

Goals and Measures

Goals

The goal of this project is to develop a lane assistance system that is functionally safe and compliant to the requirements of 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	All team Members	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 Auditor	Conclusion of functional safety activities

Safety Culture

Following are some of the key characteristics of our company to maintain a good safety 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

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 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 of OEM

- Item definition
- Functional requirements
- Hazard Analysis and Risk Assessment
- Safety goals with ASIL Levels
- Safety Validation @ Vehicle level
- Functional Safety assessment
- Functional safety concept

Responsibilities of Tier-1

- Technical Safety concept
- Software development
- Item Integration and testing
- Safety Audit

Confirmation Measures

- Confirmation Measures Purpose
  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 people who carry out confirmation measures need to be independent from the people who actually developed the project

- 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
  Checking to make sure that the actual implementation of the project conforms to the safety plan is called a functional safety audit

- Functional safety assessment
  Confirming that plans, designs and developed products actually achieve functional safety is called a functional safety assessment.