Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
Jan 2 2018	1.0	Tarun Kandala	First draft/submission
Jan 6th 2018	1.1	Tarun Kandala	Modified based on responses

Table of Contents

Document history

Table of Contents

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

Item Definition

Goals and Measures
- Goals
- Measures

Safety Culture

Safety Lifecycle Tailoring

Roles

Development Interface Agreement

Confirmation Measures

Introduction

Purpose of the Safety Plan

To provide an overall framework for the Lane Assistance System, and to assign roles and responsibilities 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 Lane Assistance system will make sure that the steering wheel vibrates when a lane departure is detected and move the steering wheel towards the center of the lane.

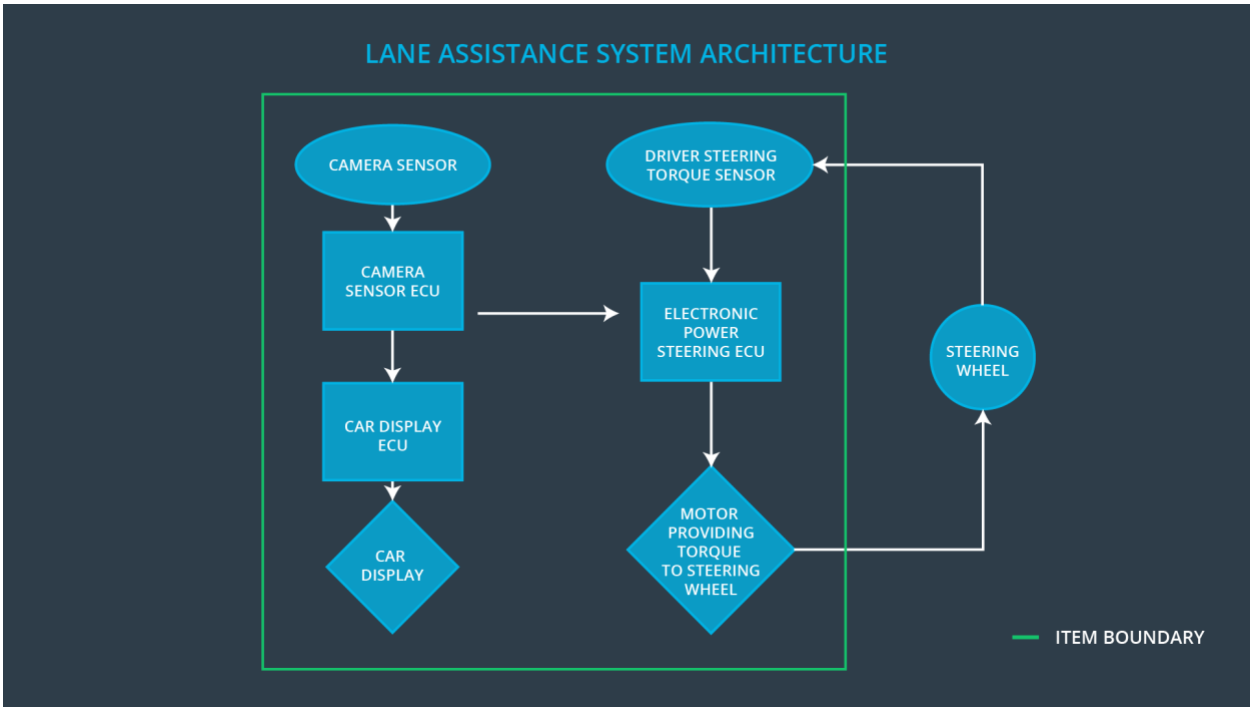
The two main functions are:

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 the steering torque when active in order to stay in ego lane

There are three sub-systems that are responsible for this item:

1) Camera system – Responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake
2) Electronic Power Steering system – Responsible for measuring the torque provided by the driver and then adding an appropriate amount of torque based on lane assistance system torque request
3) Car Display system – Display an icon in the vehicle dashboard when lane departure or lane assistance is activated

The item boundary includes the three subsystems mentioned above. Any other sub-system that is part of the vehicle is not part of this item including the Steering system itself as shown inside the figure below.



Goals and Measures

Goals

The major goal of this project is to present a system that conforms to ISO 26262 and the project really does make the vehicle safer. By analyzing the lane assistance functions with ISO 26262, we are trying to set a Development Interface Agreement (DIA) in place so that people who carry out confirmation measures are independent from the people who actually developed the project.

Also at the same time make sure that a clear delineation of roles are responsibilities are followed throughout the planning of this project.

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	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 of the characteristics of our company's 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**: our organization motivates and supports the achievement of functional safety
- **Penalties**: our organization penalizes shortcuts that jeopardize safety or quality

- **Independence**: teams who design and develop a product are independent from the teams who audit the work
- **Well defined processes**: company design and management processes are 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 following safety lifecycle phases are in scope for this project:

- 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

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.

Following are the responsibilities as a Functional Safety Manager and Engineer:

- Planning, coordinating and documenting of the development phase of the safety lifecycle
- Tailor the safety lifecycle
- Maintain the safety plan

- Monitor progress against the safety plan
- Perform pre-audits before the safety auditor
- Product development
- Integration
- Testing at the hardware, software and system levels

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

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