Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
2018-07-01	1.0	Albert Zheng	First Draft of Safety Plan

Table of Contents

Introduction

Purpose of the Safety Plan

The purpose of the safety plan is provide the defined framework for the functional safety of the overall 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 in this plan is the Lane Assistance System.

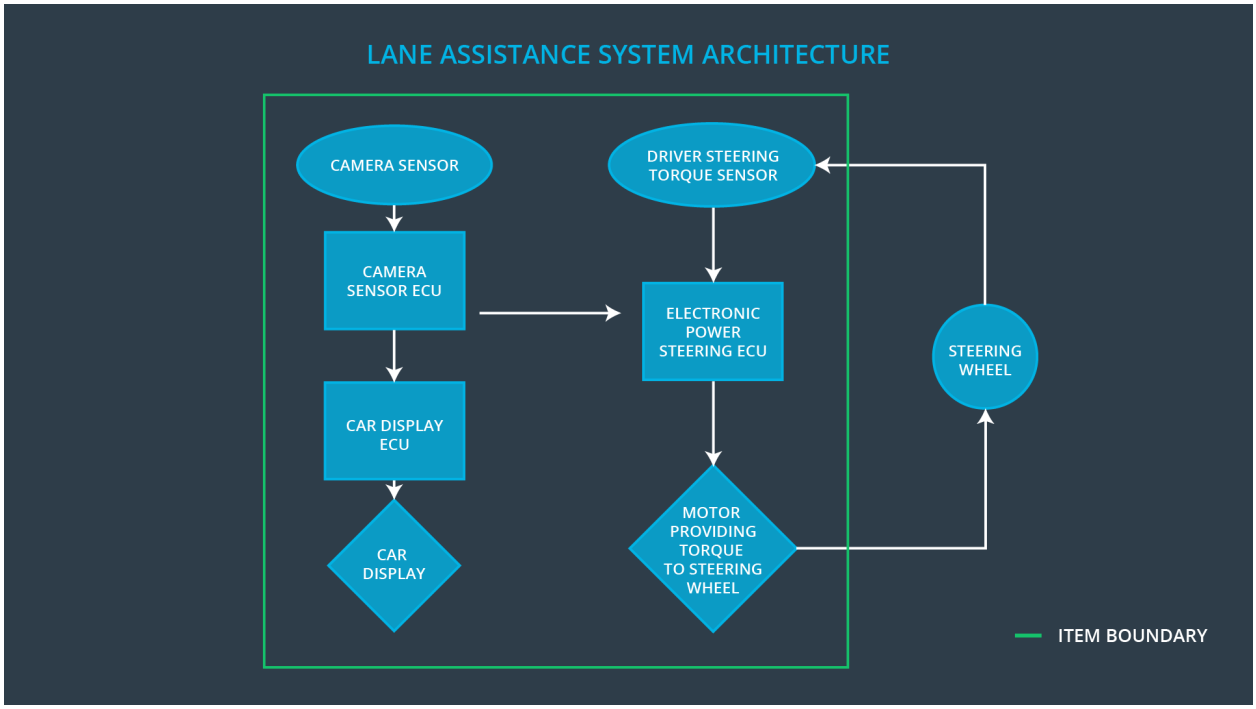
There are two main functions in this item which are:

1) **Lane departure warning function** – the functionality that will vibrate the steering wheel if the driver drifts towards the edge of an lane
2) **Lane keeping assistance function** - the functionality that will turn the steering wheel towards the center of the line if the driver begins to drift away from the center of the line.

The following subsystems are responsible for the item functionalities:

1) Camera Subsystem:
   This subsystem will be responsible for detecting the lane lines and the providing the sensing necessary to determine how far away the vehicle is from the center of the lane. This subsystem is divided into two components.
   a. Camera sensor
   b. Camera sensor Electronic control unit
2) Electronic Power Steering Subsystem:
   This subsystem will be responsible for sensing how much current torque is being used by the driver and then commanding the expected torque in order to steer the wheel back towards the center. This subsystem is divided into three components.
   a. Motor which will provide torque to steering wheel
   b. Electronic Power Steering Electronic control unit
   c. Steering Wheel Torque Sensor
3) Car Display Subsystem:
   This subsystem will be responsible for displaying the information on whether the system is active. This subsystem is divided into two components
   a. Car Display Electronic control unit
   b. Car Visual Display

The following figure represents the item boundaries for the lane assistance architecture:



Goals and Measures

Goals

The goals of this project are:

1) Identify the risk and hazardous situations associated with the Line Assistance system that could potentially cause harm to a person
2) Evaluate the risks of the hazardous situations
3) Mitigate the risk of potential malfunctions to levels accepted by societal standards

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 Assessor	Conclusion of functional safety activities

Safety Culture

The safety culture should value all the following characteristics listed below:

- **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

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 of the DIA is to ensure that all parties are developing safe vehicles in compliance with ISO 26262.

The responsibilities of the various people involved in the safety plan is as follows:

Project Manager

- Overall project management
- Acquires and allocates resources needed for the functional safety activities
- Appoints safety manager or might act as safety manager

Safety Manager

- Planning, coordinating and documenting of the development phase of the safety lifecycle
- Tailors the safety lifecycle
- Maintains the safety plan
- Monitors progress against the safety plan
- Performs pre-audits before the safety auditor

Safety Engineer

- Product development
- Integration
- Testing at the hardware, software and system levels

Safety Auditor

- Ensures that the design and production implementation conform to the safety plan and ISO 26262.
- Must be independent from the team developing the project

Safety Assessor

- Independent judgement as to whether functional safety is being achieved via a functional safety assessment
- Must be independent from the team developing the project

Test Manager

- Plans testing activities
- Coordinates testing to show that the vehicle system works correctly

Confirmation Measures

Confirmation measures serve two purposes:

1) a functional safety project conforms to ISO 26262
2) 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
Confirming that plans, designs and developed products actually achieve functional safety is called a functional safety assessment.

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.