Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
10/10/2018	V1.0	Yan Cui	Initial draft
10/31/2018	V1.1	Yan Cui	Revision for first submission
11/03/2018	V2.0	Yan Cui	Revised based on review feedback

Table of Contents

Introduction

Purpose of the Safety Plan

This document provides 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

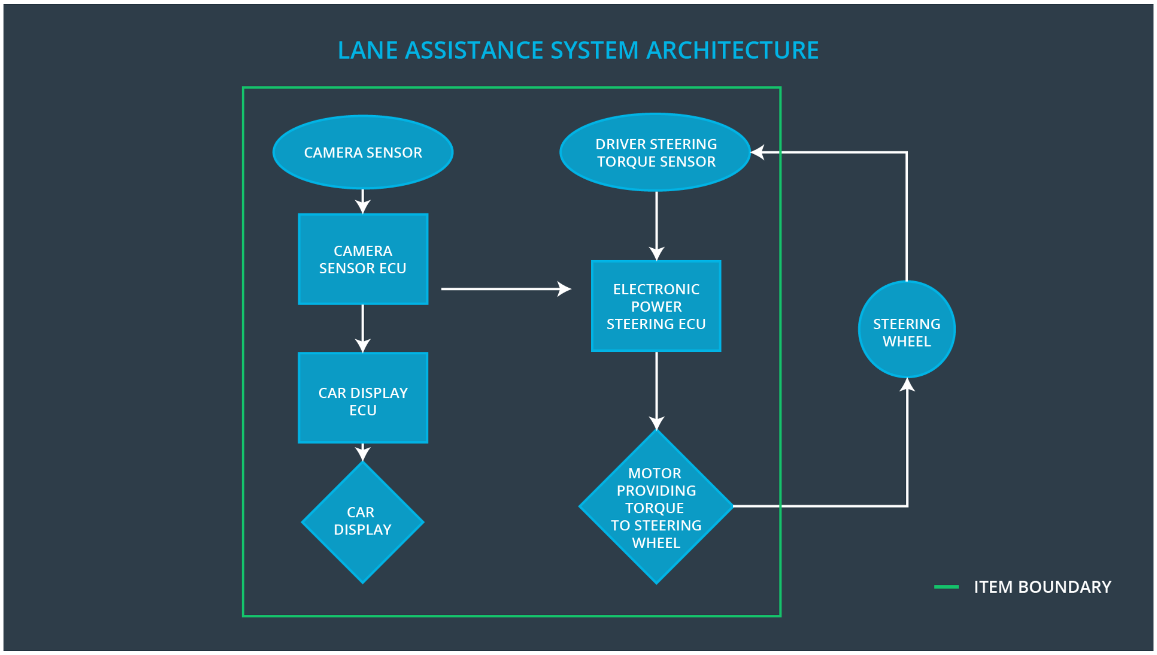
The deliverables of the project are:

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

Item Definition

The lane assistance item alerts the driver that the vehicle has accidentally departed its lane, and attempts to steer the vehicle back toward 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.


LANE ASSISTANCE SYSTEM ARCHITECTURE
CAMERA SENSOR
DRIVER STEERING TORQUE SENSOR
CAMERA SENSOR ECU
ELECTRONIC POWER STEERING ECU
STEERING WHEEL
CAR DISPLAY ECU
MOTOR PROVIDING TORQUE TO STEERING WHEEL
CAR DISPLAY
ITEM BOUNDARY

The camera subsystem, the electronic power steering subsystem, and the car display system are all responsible for each of the functions.

The boundaries are show in the figure above, including each of the three sub-systems.
Camera subsystem: this subsystem includes two components:
-- camera sensor
-- camera sensor ECU
Electronic power steering subsystem: this subsystem includes three components:
-- driver steering torque sensor
-- electronic power steering ECU
-- motor proving torque to steering wheel
Car display subsystem: this subsystem includes two components:
-- car display ECU
-- car display

Goals and Measures

Goals

The project goals are:
-- For the Lane Assistance system, identify risk and hazardours situations in the system components`s mulfunction which may cause injuries to person.
-- Evaluate risk of hazardous situations.
-- Lower the risk of mulfunctions to a reasonable level.

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

The safe culture must have these characteristics:
-- **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 is to ensure that all parties are developing safe functions involved in the Lane Assistance project, in compliance with ISO 26262.

A summary of the different roles in the project is as following:

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 (Yan Cui)
-- 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 (Yan Cui)
-- 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:
-- Ensure the Lane Assistance project conforms to ISO 26262, and

-- Ensure the Lane Assistance project really does make the vehicle safer.

The confirmation review ensures that the Lane Assistance 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 is checking to make sure that the actual implementation of the Lane Assistance project conforms to the safety plan is called a functional safety audit.

The functional safety assessment is to confirm 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.