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
18 Mar 2018	1.0	Ong Whee Cheng	Initial version

Table of Contents

Introduction

Purpose of the Safety Plan

This safety plan provides an overall framework for the Lane Assistance item, and to assign roles and responsibilities for functional safety for the Lane Assistance 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

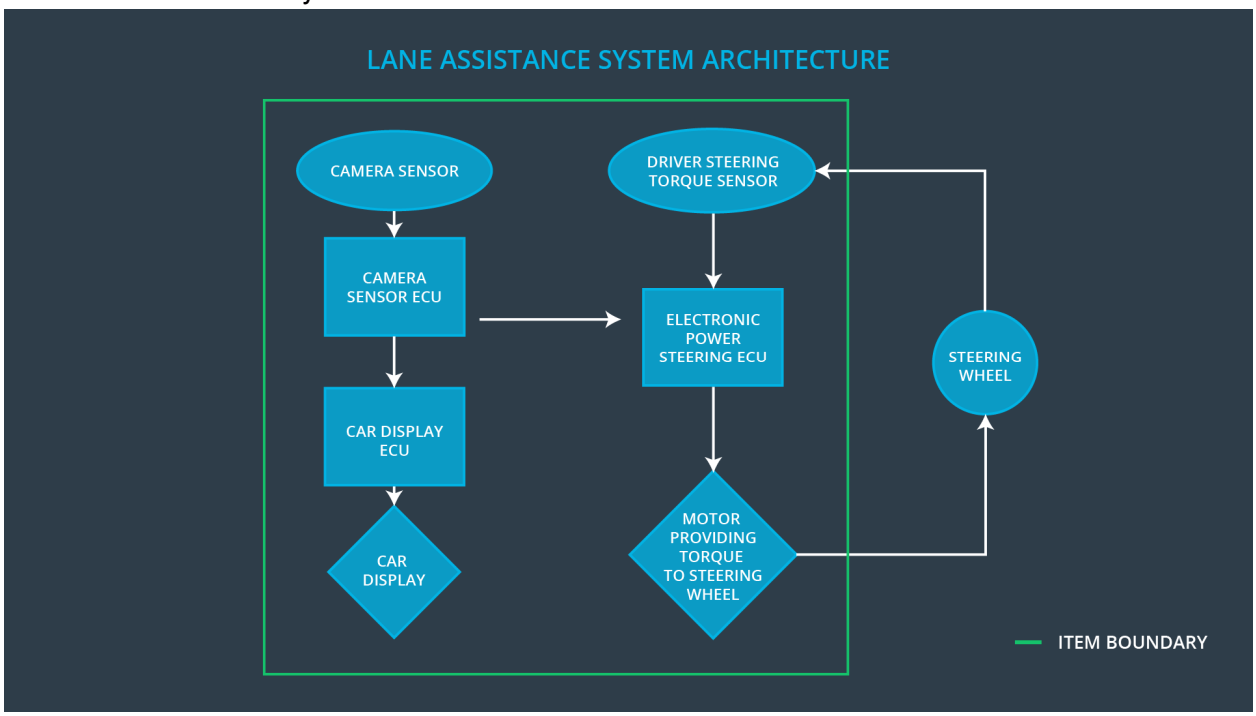
Item Definition

The Lane Assistance item alerts the driver that the vehicle has accidentally departed its lane, and attempts to steer the vehicle back towards the centre of the lane.

The Lane Assistance system has 2 functions:

- Lane Departure Warning – applies an oscillating steering torque to provide the driver a haptic feedback
- Lane Keeping Assistance – applies the steering torque when active in order to keep the vehicle centered in ego lane

The Lane Assistance System architecture is shown below:



The Lane Assistance item comprises of 3 subsystems:

- Camera subsystem – detects lane lines and determines when the vehicle leaves the lane by mistake
- Electronic Power Steering subsystem – measures the torque provided by the driver and then add an appropriate amount of torque based on a lane assistance system torque request
- Car Display subsystem – provides visual warning on the vehicle display dashboard to alert the driver

The Lane Assistance item excludes the steering wheel, and hence, is not part of the project.

Goals and Measures

Goals

The goal of the project is to assure safe operations of the electrical and electronic (E/E) components in a vehicle's Lane Assistance System, according to ISO 26262. Achieving functional safety involves 3 steps:

- identifying hazards
- measuring risks

- using systems engineering to lower risk to reasonable levels

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	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

Everyone, from CEO to rank-and-file workers, at the company holds safety as a core value; safety has the highest priority among constraints like cost and productivity. The company has well-defined processes to support the development, production and operation of safe systems. Safety is integrated into daily decisions and work processes – design decisions are traceable back to the people and teams who made the decisions.

The company rewards the people and teams that meet the functional safety goals; conversely, taking shortcuts that undermine or jeopardize safety or quality are penalized. The company

allocates all necessary resources, including people with appropriate skills, to ensure the projects meet the functional safety goals. The development and audit teams are independent, and include people of different intellectual backgrounds. Communications between teams are open to encourage full disclosure of problems and subsequently, their resolutions.

Safety Lifecycle Tailoring

Refer to the Scope of the Project section.

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 *Development Interface Agreement (DIA)* delineates the design and production responsibilities between the OEM and the Tier-1 supplier or between the Tier-1 supplier and the Tier-2 supplier. This is to avoid disputes between companies and to clarify who will be responsible for any safety issues in post-production. The DIA also specifies what evidence and work products each party will provide to prove that work was done according to the agreement. The goal is to ensure that all parties are developing safe vehicles in compliance with ISO 26262. All involved parties agree on the contents of the DIA before the project begins.

The OEM provides a functioning Lane Assistance System. The company, a Tier-1 supplier, analyzes and modifies the various subsystems according to functional safety requirements.

Confirmation Measures

Confirmation measures ensure that the applied processes comply with the functional safety standards defined in ISO 26262 and project execution follows the safety plan, thereby achieving a safe vehicle.

Confirmation review ensures that an independent person reviews the project complies with ISO 26262 as the product is designed and developed.

Functional safety audit carries out checks to make sure that the actual project implementation conforms to the safety plan.

Functional safety assessment confirms that plans, designs and developed products actually achieve functional safety.