Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 0.1

Document history

Date	Version	Editor	Description
Aug 17,2017	1.0	Jian Liang Linn	Initial Draft

Table of Contents

Introduction

Purpose of the Safety Plan

This document states an overall safety plan for “Lane Assistance” system that is a part of ADAS system and it documents how the system was designed and tested as by following ISO26262 standard. This document also captures Item definition, Goals and Measures, Safety Culture, Safety Life Cycle, Roles, Development Interface Agreement, and Confirmation Measures.

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 is a part of ADAS (Advanced Driver Assistance System) in automotive vehicles that gives driver warning upon unintentional steering wheel drifts and keep the vehicle back to the center of the lane. The two main features in this system are as follows:

- Lane Departure Warning System (LDWS)
- Lane Keeping Assistance System (LKAS)

The system will warn the driver when the vehicle goes to the edge of the lane.
LDWS feature shall apply an oscillating steering torque to generate haptic feedback to the driver through steering wheel.
LKAS feature shall apply steering torque when activated in order to stay in the current lane.

The ECU (Electronic Control Unit) subsystems that are in Lane Assistance System are as follows as shown in figure 1:

- Camera Sensor ECU
- Car Display ECU
- Electronic Power Steering ECU

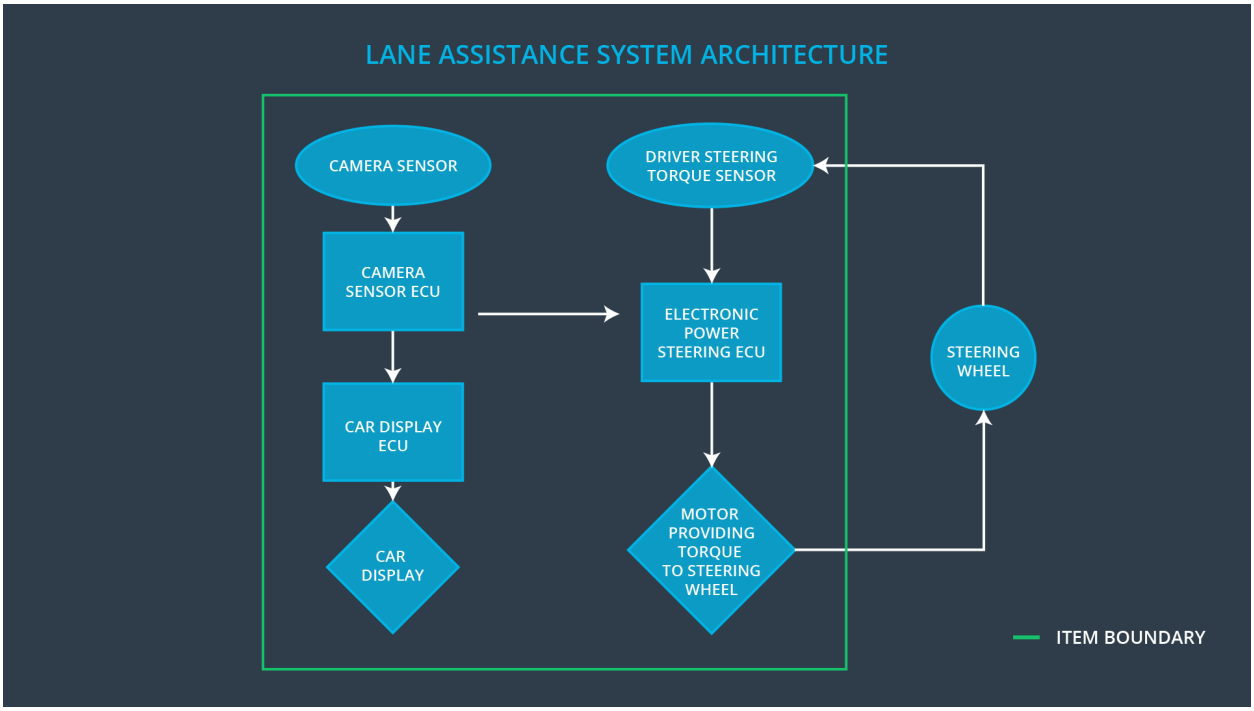

figure 1: Lane Assistance System Architecture

Camera Sensor is for getting the images in sequence of the frames then sends it off to Camera Sensor ECU to detect whether vehicle is on the current lane or leaving the current lane then sends the lane leaving signals to Electronic Power Steering (EPS) ECU if the vehicle is leaving the lane. The signal request is to EPS to turn and vibrate the steering wheel. At the same time Camera Sensor ECU will send a request to Car Display ECU to turn the warning light on in Instrument Cluster (dashboard) so the driver of the vehicle will see it.

The Lane Assistance System deactivates when the driver turn the turn signal on before changing the lane. The driver can turn on and off the Lane Assistance System with a button on Instrument panel control. The driver is expected to have both of his or her hands on the steering wheel the whole times during his driving. The Driver Steering Torque Sensor is to detect how much the driver is turning. In the case of the driver getting off of the current lane, the LKAS function will then add the extra torque that required the vehicle to get back on the center of the current lane by applying torque to the Motor providing torque to steering wheel.

The Lane Assistance Function documented here does not include the following functions:

- Blind Spot Detection and/or Warning
- Pedestrian or Object Detection
- Adaptive Cruise Control
- Automatic Parking

Goals and Measures

Goals

The safety plan goals of the Lane Assistance Function are as follow:

- Identify hazardous situational risks due to electric or electronic system malfunction of the Lane Assistance Functions
- Analyze and evaluate the risk level of the hazardous situations
- Lower the risk level of the situations by Safety System Engineering with 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	Safety Manager	Constantly
Allocate resources with adequate functional safety competency	Project Manager	Within 2 weeks of start of project
Tailor the safety lifecycle	Safety	Within 4 weeks of start of project

	Manager	
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 Manager	Conclusion of functional safety activities

Safety Culture

Safety is the most important factor in our products. Our organization follows the following 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 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

[Instructions:
Describe which phases of the safety lifecycle are in scope and which are out of scope for this particular project. Hint: See the Intro section of this document
]

The following safety lifecycle phases are included to be tailored by the ISO 26262 standard in the Lane assistance functions.

- Concept
- Product Development (System)
- Product Development (Software)

The following phases are out of scope:

- Product Development (Hardware)
- Production and Operation

Design and production implementation are ensured to conform to the safety plan and ISO 26262.

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 development interface agreement defines the roles and responsibilities between companies involved in developing a product and also specifies what evidence and work products each party will provide to prove that work was done according the agreement.

All stakeholders involved in this Lane Assistance Function Development project agree to the following roles and responsibilities:

- **Project Manager**: allocate resources as needed.
- **Safety Manager**: plan the development phase, tailor the safety lifecycle and pre-audit

- **Test Manager**: plan and oversee the testing activities
- **Safety Engineer**: develop prototypes and integrate sub systems into larger systems
- **Safety Assessor**: judge whether the project has increased safety
- **Safety Auditor**: make sure that the project conform to the safety plan

Confirmation Measures

Confirmation measures serve the following two purposes:

- The Lane Assistance Functional project conforms to ISO 26262, and
- The Lane Assistance Functional project really does make the vehicle safer.

This will ensure that the project complies with ISO 26262 as the product is designed and developed, an independent auditor would review the work to make sure ISO 26262 is being followed. The functional safety audit will be performed accordingly. The functional safety assessment ensures that plans, designs and developed products actually achieve functional safety by the independent functional safety assessor.