Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.0, Submitted on 2018-08-21
Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
8/10/2018	1.0	Nathan	First Creation

Table of Contents

Introduction

Purpose of the Safety Plan

The purpose of this safety plan is to provide an overall framework for the Lane Assistance item, and to assign roles and responsibilities for functional safety.

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

Item in question and what it does:
Lane Assistance System (LAS) identifies road lanes and warns the driver, in this case through haptic vibration, if the vehicle deviates from the lane, and steers back to the center of the lane if lane keeping assistance function was turned on. Usually, LAS is designed to operate on highways with minimum speed requirement to be activated because of more frequent lane changes, stop and turns in city roads.

Main functions:
In general, lane assistance item includes two functions:

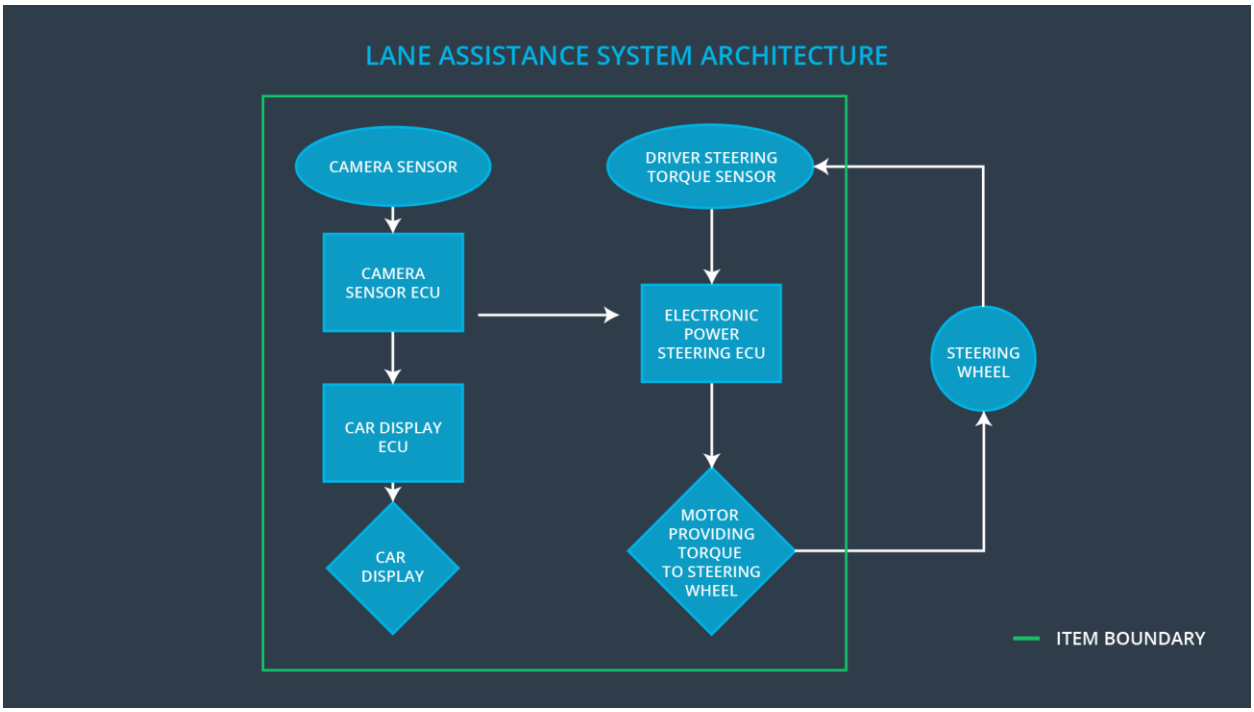
1. Lane Departure Warning (LDW)
2. Lane Keeping Assistance (LKA)

How main functions work:
The LDW function shall alert the driver with beeping sound as a feedback while deviated from the lane.

The LKA function shall apply steering torque when turned on, in order for vehicle to stay in the lane.

Subsystems responsible for each function:
Subsystems included in lane assistance system responsible for each function are the camera subsystem, the car display subsystem, the electronic power steering subsystem.

Boundaries (what subsystems are included or not):



Besides of above required key points, following points will also be addressed.
Environmental constraint (geographic consideration):
In some countries, tunnels are more common road environment type than others because of their geographic characteristics. For example, it is very rare to drive through a tunnel in U.S. than in Korea or Japan. Base on this, appropriate modification in component level shall be required.

Operational constraint (Version control requirement):
Usually, any defect found from production level is either assembly issue or shipping damages. However, there are a rare occasion where a different version of software feeds into the product during the manufacturing process. Therefore, version control at not only the development level but also at manufacturing / operation level is required.

Goals and Measures

Goals

The goal of this activity is to promote safety culture, to increase transparency and ultimately to reduce risks of hazardous situations by defining the safety improvement process and by keeping record in traceable, written documents.

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

A good safety culture have following characteristics:

1. Prioritize safety over cost reduction or productivity and penalize taking shortcuts
2. Organizational structure and processes are well defined so that responsibilities are clear and traceable who made a particular decision
3. Development team and auditing or testing team are independent from each other
4. Appropriate skills are well allocated in right places with diverse background so that any opinion of a group is not biased
5. Effective communication helps problems solved quickly and efficiently

Safety Lifecycle Tailoring

In this project, the lane assistance item is to be modified as the scope is limited to Concept phase, Product Development at the System Level and Product Development at the Software Level with a few documents. Some hardware detail and production process will be discussed as part of analysis and requirement, not as separate, formal documents and stay out of the scope.

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 purpose of development interface agreement (DIA) is to draw a clear legal boundary which party is in charge of what by define the roles and responsibilities between companies involved in developing a product.

In general,
OEM holds rights to perform tests on products supplied, to request disclosure of information for any part designs in case of incident and to perform an audit. OEM is responsible to provide item/system level concept and sufficient information to develop a product that complies system requirements. OEM is also liable to expense any cost associated from development of the system, or recall that was caused from system design or from any manufacturing process after the product was supplied.

Supplier holds rights to appoint component level functional safety personnel and to request disclosure information for product compatibility with another product composing the item or the system. Supplier is responsible to develop part product that meets OEM’s system requirements, has obligation to disclose sufficient information on development schedule and specifications of the product. Supplier is also liable to expense any cost associated from development of the component, or recall that was caused from part design or from any manufacturing/shipping process until the product was supplied.

Confirmation Measures

The purpose of confirmation measures is to make sure a functional safety project conforms to ISO 26262, and the project really does make the vehicle safer.

Confirmation review
Ensuring 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.