Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 4.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
2018-03-03	1.0	Abhishek Mantha	Document initialization
2018-03-04	2.0	Abhishek Mantha	Implementing document details
2018-03-13	3.0	Abhishek Mantha	Revising for Final Submission
2018-03-14	4.0	Abhishek Mantha	Final Submission

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 of 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 item under review is the Lane Assistance System. If a driver departs a lane without using a turn signal, the Lane Assistance System assumes that the driver has become distracted and did not mean to leave the lane. The Lane Assistance item alerts the driver that the vehicle has accidentally departed the lane, and attempts to steer the vehicle back toward the center of the lane.

The Lane Assistance System will have two main functions:

1. Lane Departure Warning
2. Lane Keeping Assistance

The Lane Departure Warning function shall apply an oscillating steering torque to provide the driver with haptic feedback. The Lane Keeping Assistance function shall apply the steering torque when active in order to stay in ego lane. Ego lane refers to the lane in which the vehicle currently drives.

The Lane Assistance System operates only when activated by the driver. The driver can activate or deactivate the Lane Assistance System with a button on the dashboard. If active, the Lane Assistance System deactivates when the driver uses a turn signal. If active and the driver attempts a lane change without a turn signal, the Lane Assistance System executes appropriate safety behavior. This functional safety plan assumes that the driver exhibits incorrect or unexpected driving behavior associated with lane driving operations.

There is 1 system and 3 subsystems within the boundary of the item under review. The 3 subsystems consist of: the Camera Subsystem, the Electronic Power Steering Subsystem and the Car Display Subsystem. Each subsystem consists of a primary Electronic Control Unit (ECU), with specified input and output data channels. The primary system consists of both the Camera Subsystem and the Electronic Power Steering Subsystem.

The Camera Subsystem consists of Camera Sensors and a Camera Sensor ECU. The Camera Sensor ECU collects current camera sensor data and determines whether the vehicle is leaving the lane. If the Camera Sensor ECU senses that the vehicle is leaving the lane, the camera sends a signal to the Electronic Power Steering Subsystem requesting to turn and vibrate the steering wheel. The Camera Sensors update with new data from vehicle cameras continuously.

The Electronic Power Steering Subsystem consists of a Driver Steering Torque Sensor, an Electronic Power Steering ECU, and a motor providing torque to the steering wheel. The Electronic Power Steering ECU combines data from the Camera Sensor ECU and the Driver Steering Torque Sensor to determine the amount of oscillating torque to apply, if any at all, depending on the amount the driver is already turning the steering wheel and if an unsafe lane departure has occurred. The Electronic Power Steering ECU sends a signal to the motor controlling steering wheel torque, which applies the physical force. The details of the implementing the physical force are outside the boundary of the item under review. The Driver Steering Torque Sensor updates with new data from the steering wheel continuously.

The Camera Sensor ECU will also request that a warning light turn on in the vehicle's dashboard. This message is sent to the Car Display ECU which controls the Car Display. This notifies the driver that the Lane Assistance System is active.

Refer to **Figure 1** below for a bird's-eye-view of the Lane Assistance System Architecture.

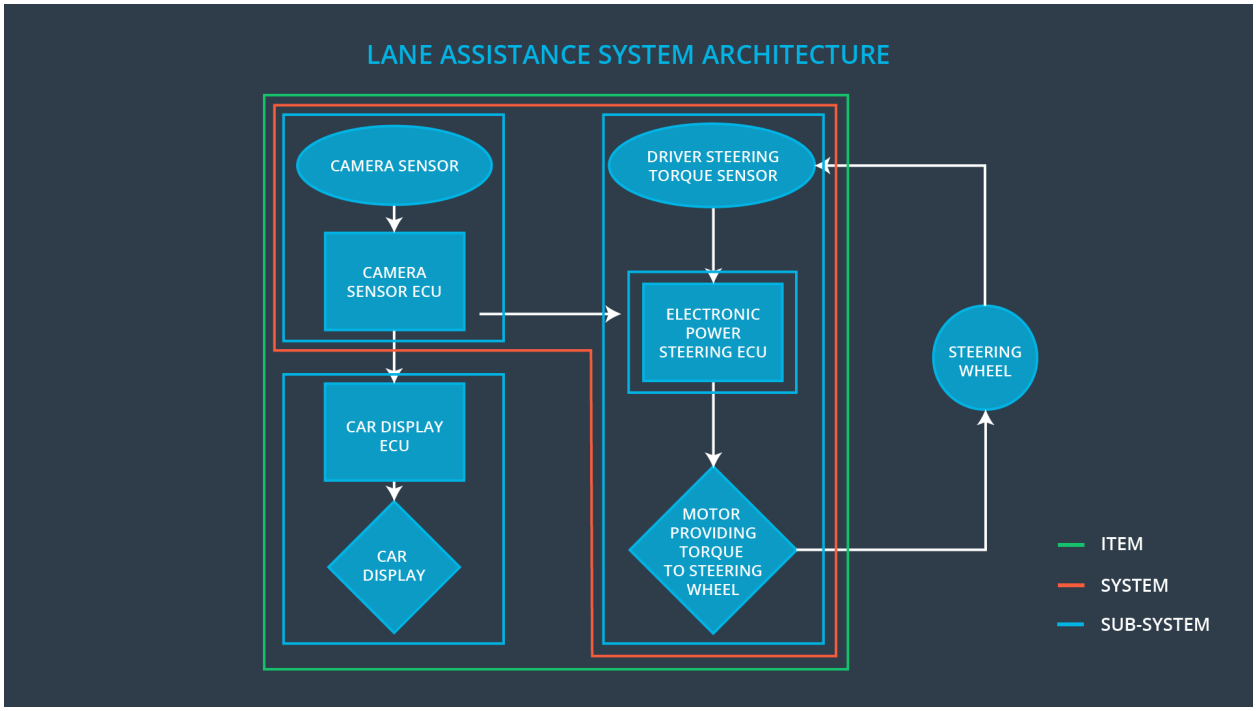

Figure 1 - Lane Assistance System Architecture

Goals and Measures

Goals

The goal of this project is to identify the functional safety of the Lane Assistance System functions. ISO 26262 provides a methodical, incremental framework for ensuring and accounting for its design, implementation and behavior. As the Lane Assistance System is a popular ADAS (Advanced Driver Assistance System) feature available in commercial vehicles, it is critical to account for its safety as drivers engage with it regularly.

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

Our company is committed to maintaining a strong safety culture. Our highest priority is to our customers, and is achieved by ensuring their safety day in and day out. We prioritize clear, constant communication and diversity in thought. Our employees are rewarded and accountable for adhering to established safety standards. Encouraging the disclosure of problems and integrating competing perspectives positions us to design and tailor solutions for the safety and needs of our customers. Maintaining a strong safety culture is a complete team effort. The strength of our commitment is a reflection of our collective desire to improve the lives of others. We promise our customers that no expense or resource will be spared to keep them safe, and for that we deeply value and thank them for their loyalty.

Safety Lifecycle Tailoring

For the Lane Assistance System, 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

This functional safety plan assumes the Lane Assistance System is a new product in development. Therefore, adequate detail will be given to identifying strategies to plan, implement, and test the Lane Assistance System at the System and Software Levels. However, any hardware implementation details are beyond the scope of this document. The details of production and deployment are outside the scope of this document.

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 (DIA) defines the roles and responsibilities between companies and partners involved in developing a product. All involved parties need to agree on the contents of the DIA before the project begins. The DIA specifies what evidence and work products each party will provide to prove that work was done according to the following agreement details. It is used to avoid disputes, establish liability, and identifies who should fix safety issues.

As a Tier-1 operator, we are responsible for analysis and modification of a supplied Lane Assistance System. The key activities of our Functional Safety Manager and Engineers include: planning, coordinating and documenting the development phase of the safety lifecycle; tailoring the safety lifecycle with OEM; maintaining an appropriate safety plan for development; monitoring progress against the safety plan; performing pre-audits; product development; system integration; testing at the system and software levels.

At the end of this development process, we hope to produce a functionally safe Lane Assistance System (with all related subsystems) to be installed and used within our partner OEM's final product offering. We take full responsibility for analysis, modification, and implementation. However, after completion of our work, all responsibility related system integration within our OEM's final product offering is our partner OEM's full responsibility.

Confirmation Measures

Confirmation Measures verify that a functional safety project conforms to ISO 26262 and that the project actually makes the vehicle safer. Personnel who carry out confirmation measures must be independent and removed from the personnel who develop the project.

A Confirmation Review ensures that the project complies with ISO 26262. An independent person must review the work to make sure ISO 26262 is adhered to during product design and development.

A Functional Safety Audit checks that the actual implementation of the project conforms to the safety plan.

A Functional Safety Assessment confirms that product plans, designs, and development 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.