Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.0
08-21-2017

Document History

Date	Version	Editor	Description
08-21-2017	1.0	Neil Hiddink	Safety Plan – Lane Assistance Feature

Table of Contents

Introduction

Purpose of the Safety Plan

To provide the overall framework for the functional safety of a Lane Assistance functionality in a new model vehicle.

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 in question is a Lane Assistance functionality that automatically performs steering corrections on behalf of the driver by turning the steering wheel towards the center of the lane. While this functionality executes autonomously, it does not replace the driver and should not control the vehicle continuously for more than five seconds of course correction.

Figure 1 below is a representation of the item as a system with three sub-systems: the camera system, the ECU sub-system, and the car display system.

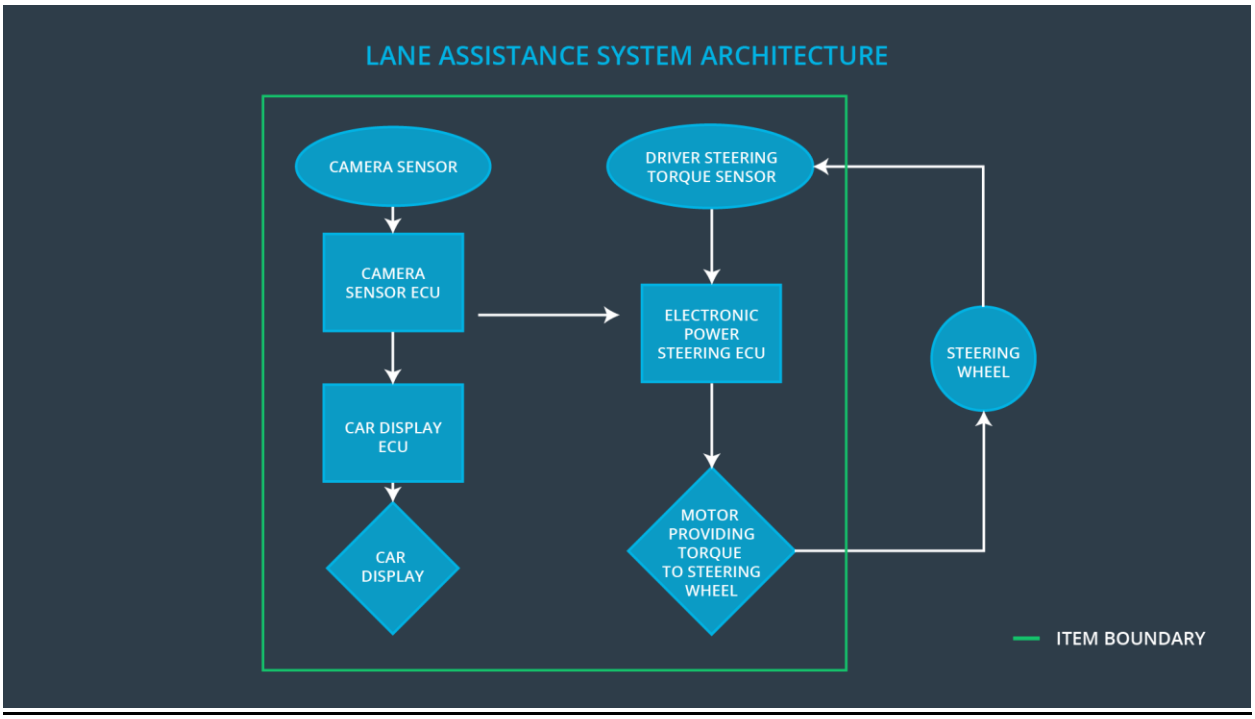

Figure 1: Lane Assistance System Architecture

The camera ECU captures lane line data from a sensor mounted on the front of the vehicle at a frame rate of 30 FPS. The camera ECU interprets the data in real-time to detect the position of the lane using computer vision techniques. Upon identifying the need for a course correction, the camera ECU simultaneously delivers signals to the power steering ECU to control the vehicle's steering wheel actions and to the car display ECU to output a lane departure warning to the driver.

Signals received by the power steering ECU authorize the vehicle to initiate the Lane Assistance functionality to take over control from the driver. First, the motor providing torque to the steering wheel actuates to account for the necessary correction, and then the steering wheel vibrates by oscillating slightly and rapidly in each direction. The steering wheel returns to the driver's control after several seconds. If the driver intends to change lanes, a turn signal overrides the Lane Assistance functionality.

The car display ECU receives signals from the camera ECU to provide a visual warning on the heads-up display that alerts the driver that they are departing a lane and that the Lane Assistance functionality is taking over control to correct the course of the vehicle.

The item boundary includes every subsystem and component mentioned in the architecture diagram in Figure 1 except the steering wheel. This means that the Lane Assistance functionality requires the coordination of the camera ECU, the power steering ECU, and the car display ECU and all of their components to perform properly.

The item will operate under several operational and environmental constraints. One operational constraint to consider is camera performance, especially when it comes to frame rate and resolution. The camera subsystem with the highest frame rate and resolution that minimizes overall cost is the most desirable. One environmental constraint to consider is weather, as rain, snow, fog, and sunny conditions all have a different effect on camera images that may distort the computer vision algorithm’s perception of the vehicle’s position in the lane.

Goals and Measures

Goals

The item conforms to ISO 26262 and provides a safe functionality that complements the driver's own operation of the vehicle.

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	All Team Members	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 strives toward a safety culture that…

…has the highest priority. Safety is and always will be our number one concern, and we will not allow competing constraints such as cost and productivity to stand in the way.

...is accountable. Our established processes ensure that design decisions are traceable back to the responsible team members and decision-makers.

…is rewarding. We strongly incentivize and reward team members that promote functional safety in their daily work.

...has integrity. Our organization penalizes shortcuts that jeopardize safety or quality. Our safety auditors operate independently from our design and development teams.

…is efficient. Projects we work on have all the necessary resources, including team members with appropriate skills required to complete assignments.

…embraces diversity. Intellectual diversity is sought after, valued, and integrated into every day processes at our company.

…encourages communication. Open communication channels between departments encourage disclosure of problems and facilitates resolution.

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

This agreement defines the roles and responsibilities between the companies involved in developing the Lane Assistance item.

Upon receiving working units of the Lane Assistance item, our company will handle the safety analysis and any subsequent modifications that are required to the various sub-systems of the Lane Assistance item from a functional safety standpoint. Please refer to the Roles outlined above for details on the appointments made for customer and supplier safety managers on this project.

Confirmation Measures

The confirmation measures provided ensure that the Lane Assistance item conforms to ISO 26262 and that the item makes the vehicle safer to drive. Independent auditors will perform the confirmation measures as a part of the confirmation review during the product design and development phases. Additionally, a functional safety audit of the actual implementation of the Lane Assistance item will be conducted to ensure conformance to the safety plan outlined in this document. The auditor is required to complete a functional safety assessment as a part of his or her report that will determine the success of the audit.