Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.0
Released on 2017-10-29

Document history

Date	Version	Editor	Description
10/29/17	1.0	Trevor Conley	First 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 Lane Assistance System item alerts the driver that the vehicle has accidently departed its lane, and attemps to steer the vehicle back to the center of the lane.

The two main functions involved are the lane departure warning and the lane keeping assitance. The lane departure warning function will vibrate the steering wheel to provide the driver haptic feedback. The lane keeping assistance function will apply a steering torue to the steering wheel so that the wheels turn towards the center of the lane.

There are three subsystems responsible for these functions: the camera subsystem, the electronic power steering subsystem, and the car display system.

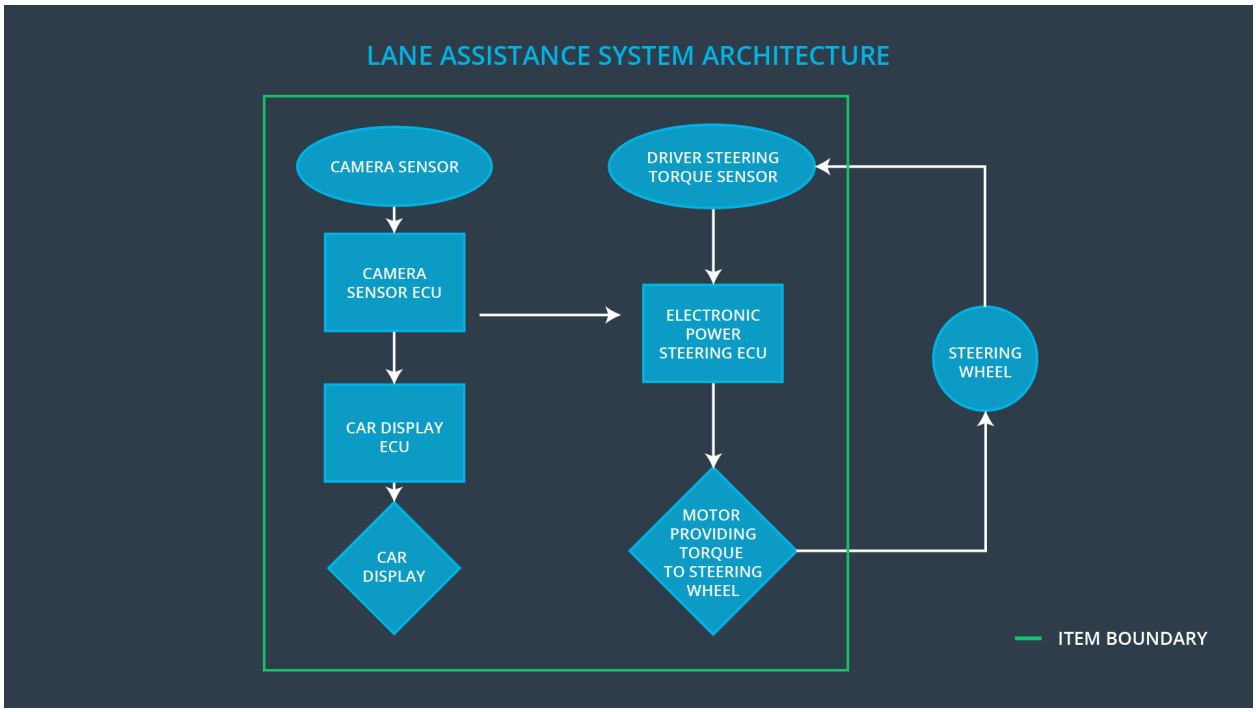

Figure 1: This illustrates the boundaries of the Lane Assistance System item. It shows the subsystems that are responsible for the assistance functions as well as what is outside of the system.

Goals and Measures

Goals

The goals of the Lane Assistance System are to identify risk hazardous situations in a lane assistance electroinc or electric system malfunction that may cause physical injury or death. We also need to evaluate the risk levels of these situations and lower high risk situations to reasonable levels to prevent accidents from occuring.

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 sets safety as the highest priority, well above cost and productivity. We make sure that everyone is held accountable for their decisions, while rewarding people for their achievments of functional safety. Employees will be held accountable for all shortcuts that jeopardize the safety or quailty of our items. We will ensure that our design and development teams work independently from the teams auditing the work. We have a well defined design and management process with all projects having the necessary resources and properly skilled, trained, and intectually diverse employees to ensure safety. Our communication channels are in place to encourage disclosure of any problems that may occur.

Safety Lifecycle Tailoring

Since the Lane Assistance System does not require any new hardware to operate, we will mainly be focusing on the concept and product development at the sytems and software levels. We will also not be focusing on the production as we are not producing any new hardware. Our conceptual phase will include a hazard analysis and risk assessment along with a functional safety concept. After this phase has been completed, we will move on to the product development phase. After creating our system, we will need to ensure that the system and software function properly.

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 a development interface agreement is to define the roles and responsibilities between companies involved in developing a product. All parties involved need to agree on the contents of the agreement before the project begins. In order to do this, we will ensure that all parties are developing safe vehicles in complaince with ISO 26262.

Being a tier-1 organization puts the responsibilities of the making sure that the project conforms to the safety plan as well as developing prototypes and integrating subsystems into larger systems for all the componenets.

Confirmation Measures

The main purposes of confirmation measures are to ensure that a functional safety plan conforms to ISO 26262 and ensure that the project really does make a safer vehicle. A confirmation review ensures 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. The functional safety audit is performed to make sure that the actual implementation of the project conforms t the safety plan. Confirming that plans, designs and developed products actually achieve functional safety is called the functional safety assessment.