Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version:1.0

Released on 2018-05-19

Document history

For example, if this were your first draft or first submission, you might say version 1.0. If this is a second submission attempt, then you'd add a second line with a new date and version 2.0]

Date	Version	Editor	Description
5/19/2018	1.0	Tariq Rafique	Initial Submission

Table of Contents

Introduction

Purpose of the Safety Plan

[Instructions: Answer what is the purpose of a safety plan?]
The purpose of this safety plan is to provide an overall framework for the Lane Assistance project and to define roles and responsibility so that important design steps are not missed and outlines the steps we will take to achieve functional safety for this project

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

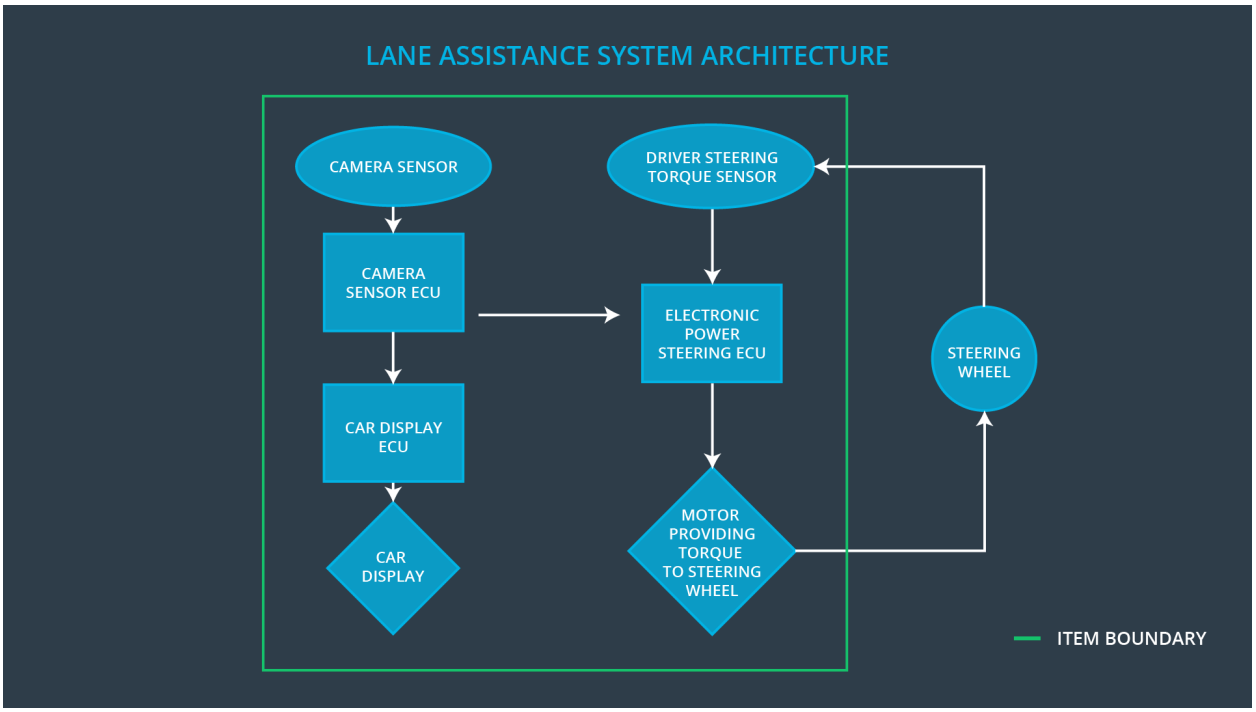
Item Definition

The lane assistance system item is a driver assist system that alerts the driver that if the vehicle unintentionally drifts out of it's lane. It then attempts to take corrective action by steering the vehicle back towards the center of it's lane.

The Lane Assistance System will have two functions

1. Lane departure warning
   The lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback
2. Lane keeping assistance
   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 camera subsystem, the electronic power steering subsystem and the car display subsystem are all responsible for each of the functions



Note that the steering wheel is outside of the Lane Assistance System.

Goals and Measures

Goals

The goal of this project is to ensure that the Lane System Assistance item is functionally safe. We will use ISO 26262 to guide our process. We will analyze which malfunctions can occur and the consequent hazards.
We want to reduce the risk of failure and minimize the consequent hazards to an acceptable level

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

Safety is our top priority.

We have processes in place to ensure that traceability and accountability of design decisions to the people and teams that made the decision
Good functional safety is recognized and rewarded. Teams and individuals are encouraged to take the time to get safety right
We have no tolerance for actions that take shortcuts and jeopardize safety or quality

Independent teams audit the design and functional safety work done by product design and development teams

We have clear processes for design and management. Our quality management system is IATF 16949 certified

We have a fully funded organization dedicated to auditing functional safety.
Projects have functional safety managers responsible for overseeing and compiling the functional safety plan for the project

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
]
This is a new product that we're building for the Lane Assistance System item.
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

[Instructions:
This section is here for your reference. You do not need to do anything here. It is provided to help with filling out the development interface agreement section.

]

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

[Instructions:
Assume in this project that you work for the tier-1 organization as described in the above roles table. You are taking on the role of both the functional safety manager and functional safety engineer.

Please answer the following questions:

1. **What is the purpose of a development interface agreement?**

A DIA (development interface agreement) defines the roles and responsibilities between companies involved in developing a product. All involved parties need to agree on the contents of the DIA before the project begins.

The DIA also specifies what evidence and work products each party will provide to prove that work was done according to the agreement.

The ultimate goal is to ensure that all parties are developing safe vehicles in compliance with ISO 26262.

2. **What will be the responsibilities of your company versus the responsibilities of the OEM? Hint: In this project, the OEM is supplying a functioning lane assistance system. Your company needs to analyze and modify the various sub-systems from a functional safety viewpoint.**

]

Tier 1 (Our) Responsibilities

Functional Safety Manager & Safety Engineer – Component Level

- Planning, coordinating and documenting of the development phase of the safety lifecycle
- Tailors the safety lifecycle
- Maintains the safety plan
- Monitors progress against the safety plan
- Performs pre-audits before the safety auditor
- Product development
- Integration
- Testing at the hardware, software and system levels

OEM Responsibilities
The OEM will be taking care of the following

- Functional Safety Manager- Item Level
- Functional Safety Engineer- Item Level
- Project Manager - Item Level
    a. Overall project management
    b. Acquires and allocates resources needed for the functional safety activities
    c. Appoints safety manager or might act as safety manager
- Functional Safety Auditor
    a. Ensures that the design and production implementation conform to the safety plan and ISO 26262.
    b. Must be independent from the team developing the project
- Functional Safety Assessor
    a. Independent judgement as to whether functional safety is being achieved via a functional safety assessment
    b. Must be independent from the team developing the project

Confirmation Measures

What is the main purpose of confirmation measures?
Confirmation measures serve two purposes:

- that a functional safety project conforms to ISO 26262, and
- that the project really does make the vehicle safer.

What is 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.

What is a 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.

What is a functional safety assessment?
Confirming that plans, designs and developed products actually achieve functional safety is called a functional safety assessment.