Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version:

Version 1.0, Released on 2019/05/02

Document history

Date	Version	Editor	Description
25th April	1	John Reilly	First Attempt

Table of Contents

Introduction

Purpose of the Safety Plan

The scope of the safety plan is to give an overall framework for the lane assitance item and to assign roles and responsibilites for functional safety for 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 asstiance item alerts the driver that the vehicle has accidentally departed its lane and attempts to steer the vehicle back towards the cantre of the lane.

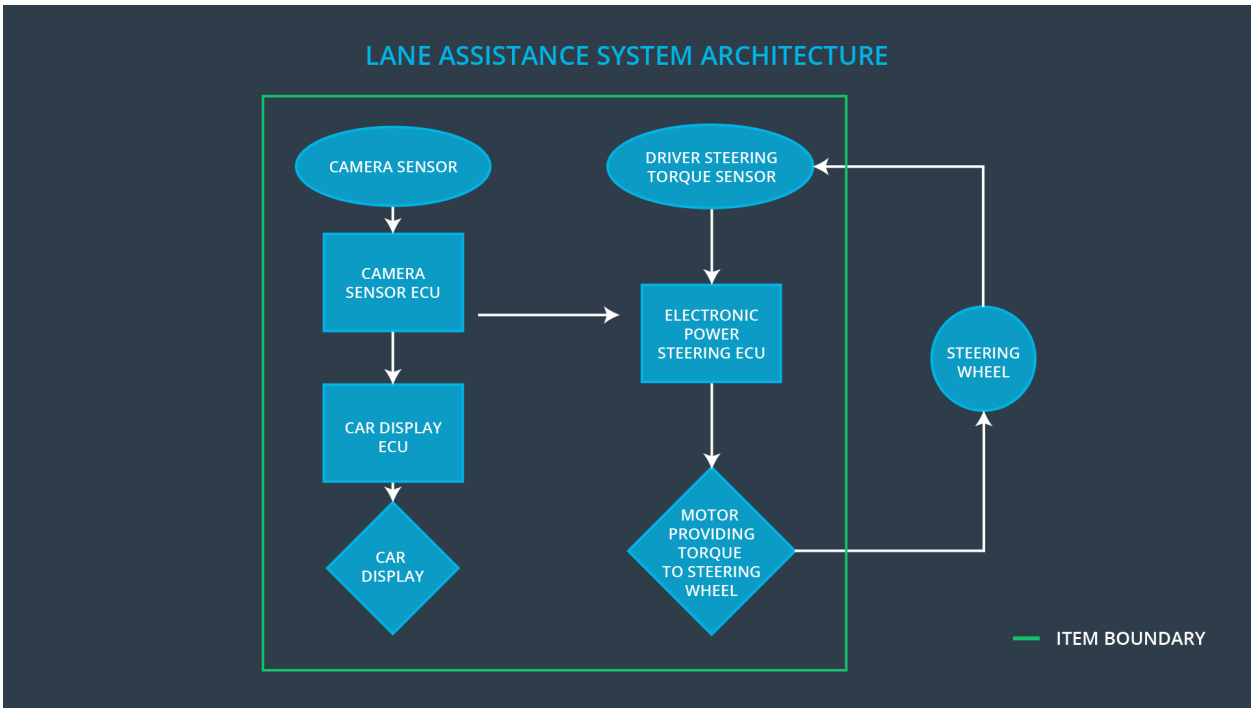
The Lane Assistance System will have two functions:

1. Lane departure warning
2. Lane keeping assistance

The lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback.

The lane keeping assistance function shall apply the steering torque when active in order to stay in ego lane.

The camera subsystem,the electronic power steering subsystem and the car display system are all responsible for each of the functions.



Goals and Measures

Goals

The goal of this project is to identify and describe risks associated with the possible use cases of the lane assistance funciton, to specifiy roles and responsbilites in the Safety Management process and to provide a framework for supplier vendors to define their responsibilites in relation to the overall project.

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

The company promotes, applies and adhere to the following principals to create and maintian a a good safety culture in the business:

- **High priority**: safety has the highest priority among competing constraints like cost and productivity
- **Accountability**: processes ensure accountability such that design decisions are traceable back to the people and teams who made the decisions
- **Rewards**: the organization motivates and supports the achievement of functional safety
- **Penalties**: the organization penalizes shortcuts that jeopardize safety or quality
- **Independence**: teams who design and develop a product should be independent from the teams who audit the work
- **Well defined processes**: company design and management processes should be clearly defined
- **Resources**: projects have necessary resources including people with appropriate skills
- **Diversity**: intellectual diversity is sought after, valued and integrated into processes
- **Communication**: communication channels encourage disclosure of problems

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

The DIA (development interface agreement) defines the roles and responsibilities between companies involved in developing this product.

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.

The distribution of responsibilites in the overall funcitonal safety rpoject are distributed between the OEM and the tier 1 supplier in accordance to the information below.

Functional Safety Manager- Item Level Responsibilites: • 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	OEM

• Performs pre-audits before the safety auditor	
Functional Safety Engineer- Item Level Responsibilites: • Product development • Integration • Testing at the hardware, software and system levels	OEM
Project Manager - Item Level Responsibilites: • Overall project management • Acquires and allocates resources needed for the functional safety activities • Appoints safety manager or might act as safety manager	OEM
Functional Safety Manager- Component Level Responsibilites: • 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	Tier-1 assigned to John Reilly
Functional Safety Engineer- Component Level Responsibilites: • Product development • Integration • Testing at the hardware, software and system levels	Tier-1 assigned to John Reilly
Functional Safety Auditor Responsibilites: • Ensures that the design and production implementation conform to the safety plan and ISO 26262. • Must be independent from the team developing the project	OEM or external
Functional Safety Assessor	OEM or external

Responsibilites: • Independent judgement as to whether functional safety is being achieved via a functional safety assessment • Must be independent from the team developing the project	

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.

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.

A Functional safety audit checks 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.