Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: version 2.0

Document history

Date	Version	Editor	Description
29/10/2017	1.0	Adriana Costas	First attempt
20/11/2017	2.0	Adriana Costas	Second attempt
06/12/2017	3.0	Adrian Costas	Third attempt

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, assign roles and responsabilities as well as outline the steps to achieve functional safety.

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 item alerts the driver that the vehicle has accidentally departed its lane and attempts to steer the vehicle back toward the center of the lane.
The Lane Assistance system will have two functions:

1. Lane departure warning: it shall apply an oscillating steering torque to provide the driver a haptic feedback.
2. Lane keeping assistance: it shall apply the steering torque when active in order to stay in ego lane.

The item boundary include three subsystems as shown in Figure 1 :

1. Camera system
2. Electronic Power Steering system
3. Car display system

The camera subsystem is resposible for visualizing the lane, detecting the lane departure and giving the departure alert. This subsystem is composed of two components: the sensor and the ECU. The sensor is mounted on the top of the windscreen and provides the road view. The ECU receives the camera images and applies computer vision techniques in order to detect lanes and vehicle's positions within the lane.

The electronic power steering subsystem is responsible for assiting and alerting the driver by applying torque to the steering wheel.

The car display subsystem is responsible for giving the driver visual lane departure alert on car's instrument cluster display. Moreover, if the item is active but the lane marks could not be detected, a visual warning is given.

Goals and Measures

Goals

The goals of the Lane Assitance Functional Safety Plan for the project are:

- Indentifying risk hazardous situations in a lane assitance electronic or electric system malfunction that may cause physical injury or damage to a person's health.
- Evaluate the risk level of the hazardous situation.
- Via systems engineering, lowering high risk level situations to reasonable levels to prevent accidents from ocurring.

Measures

Measures and Activities	Responsibility	Timeline
Follow safety processes	All team members	Constantly
Create and sustain a safety culture	Safety manager	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 assesor	Conclusion of functional safety activities

Safety Culture

Meeting the criteria of the safety standard is not just a technical issue. The organisation must also adopt way of work that emphasises safety of the product. This safety shall include the following principles:

- High priority: safety has the highest priority among competing constraints like cost and productivity. Human life cannot be compromised over cost.
- 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 instead of hiding them.
- Authority: people that lead safety relevant activities should be explicitly appointed in all development phases
- Continuous improvement: Dedicate resources for funtional safety skill development and promote better safety development processes.

Safety Lifecycle Tailoring

For the lane assistance project functional safety initial plan, the ISO 26262 standard have been tailored to include the following safety lifecycle phases 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 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 purpose of a development interface agreement (DIA) is to define the roles and responsabilities 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.
In this project the OEM is supplying a functioning lane keeping assistance product. The Tier-1 should analyse the product and modify it in order to achive ISO 26262 compliance. This DIA applies to lane assistance system (only within the scope defined in the introduction of this document) and onvolves OEM, the Tier-1 and an independent external audit/assessment company.

Resposibilities of the OEM:

- Providing the initial design documentation (systems functional and non-functional requirements, software and hardware specification).
- Acceptance of the plans and work product from Tier-1 on the basis of the independent assessment.
- Implementation of the afety features.

Responsibilities of the Tier-1

- Provide a Safety plan
- Provide the Hazard Analysis and Risk Assessment
- Provide the Functional Safety Concept
- Provide the Technical Safety Concept
- Software the Safety Requirements and Architecture
- Pre-assessment of the plans

Reposibilities of the Auditor/Accessor

- Independent assessment of the plan and work products.

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.

The people who carry out confirmation measures need to be independent from the people who actually developed the project.

A confirmation review is a review that 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 ISO26262 is being followed.

A functional safety audit is the process that checks that the actual implementation of the project conforms to the safety plan whereas a functional safety assessment confirm that plans, designs and developed products actually achieve functional safety.