Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.0
Released on 2018-09-08

Document history

Date	Version	Editor	Description
09/08/2018	1.0	Vianney Monestel	Initial draft

Table of Contents

Introduction

Purpose of the Safety Plan

This document describes how to ensure safety in a car Lane Keeping Assistance of system. It shows the scope of the project; that is the safety lifecycle phases covered and the deliverables to guarantee functional safety in the new product. The final goal of functional safety is to minimize the risks of producing physical damage to the car's passengers when the Lane Keeping Assistance is used.

This plan determines the roles of the people enrolled in the project and their responsibilities within the team. It also defines the goals and measures to ensure that the project conforms to ISO 26262 standard.

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 product defined in this plan is a Lane Assistance System. The intention of this mechanism is to minimize car accidents; the driver is informed when the vehicle is moving out of its lane (unless the turn signal is on that direction).

Features:

- **Lane departure warning:** this mechanism vibrates the steering wheel to warn the driver when the car is moving outside of the lane edges.
- **Lane keeping assistance:** warns the driver by vibrating the steering wheel, if the driver does not perform any actions; the systems takes control of the steering wheel and it moves it back to its lane.

Lane Assistant subsystems:

- **Lane detection subsystem:** this part of the system is in charge of detecting the lane lines and determine when the vehicle is leaving its lane. Also, this subsystem is in charge of sending a signal to the Electronic Power Steering Subsystem to make vibrations on the steering wheel to alert the driver. The parts of this subsystem are the camera sensor and the Camera Sensor Electronic Control Unit (ECU).
- **Electronic Power Steering Subsystem:** this subsystem adjusts the steering wheel in case that the car is leaving its lane and the driver is not doing the enough steering correction to avoid it. There is a sensor which determines how much the driver is turning. The main parts of this subsystem are: Driver Steering Sensor, Steering ECU and a motor that provides torque to the steering angle.
- **Display Subsystem:** provides visual assistance to the driver. A warning light is shown in the car dashboard when the Lane Assistance System is activated.

Elements outside of this item:

- GPS
- Steering wheel
- Blind Spot Monitoring
- Car Reverse System
- Tire Pressure System

Goals and Measures

Goals

The goals of this project are:

- Guarantee functional safety on a car Lane Assistance System and its components according to ISO 26262 standard.
- Identify hazards in the Lane Assistance System system that could cause physical injury or damage to a person's health.
- Evaluate the risk of the hazardous situations.
- Reduce the risk to accepted levels.

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

Safety is a high priority topic in our organization. Productivity and cost are important, but safety is always consider to deliver products with high quality. The ISO 26262 standard is followed in our processes to guarantee functional safety. During all the project phases, the design decisions are traced to the people who make those decisions. There are penalties established when the safety rules, requirements or standards are not met and decreases the quality. Everyone is encouraged and motivated to achieve functional safety.

As a responsible organization, the processes are well documented and clearly defined. Our people (managers, engineers, testers, designers, auditors) have the skills and tools to create safety products. The independence in our processes plays an important role, where the people who design and develop a product are independent from the teams who audit the work.

Safety Lifecycle Tailoring

The lifecycle phases described in the Scope of the Project section are followed and documented in this project. The hardware components and their development, production and operations phases are excluded from the safety lifecycle and analysis.

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 a safe Lane Assistance System in compliance with ISO 26262. All involved parties need to agree on the contents of the DIA before this 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.

Sections of the DIA:

- Appointment of customer and supplier safety managers
- Joint tailoring of the safety lifecycle
- Activities and processes to be performed by the customer; activities and processes to be performed by the supplier
- Information and work products to be exchanged
- Parties or persons responsible for each activity in design and production
- Any supporting processes or tools to ensure compatibility between customer and supplier technologies.

The OEM company supplies the functioning lane assistance system. Our company (TIER-1) is going to analyze and modify the various subsystems involved from a functional safety approach.

Confirmation Measures

The confirmation measures ensures that the project is in compliance with the ISO 26262 and it makes the vehicle safer.

The confirmation review ensures that the project conforms to ISO 26262. As the product is designed and developed, this review is performed by an independent person to make sure the standard is being followed.

The functional safety audit makes sure that the actual implementation of the project conforms to this safety plan.

The functional safety assessment check and confirms that plans, designs and developed products actually achieve functional safety.

A safety plan could have other sections that we are not including here. For example, a safety plan would probably contain a complete project schedule.

There might also be a "Supporting Process Management" section that would cover "Part 8: Supporting Processes" of the ISO 26262 functional safety standard. This would include descriptions of how the company handles requirements management, change management, configuration management, documentation management, and software tool usage and confidence.

Similarly, a confirmation measures section would go into more detail about how each confirmation will be carried out.