Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
May 25, 2018	1.0	Aftab Engaria	Initial Draft

Table of Contents

Document history

Table of Contents

Introduction

- Purpose of the Safety Plan
- Scope of the Project
- Deliverables of the Project

Item Definition

Goals and Measures

- Goals
- Measures

Safety Culture

Safety Lifecycle Tailoring

Roles

Development Interface Agreement (DIA)

- Purpose of a DIA
- Responsibilities of the Company vs OEM

Confirmation Measures

- Purpose
- Confirmation review
- Functional Safety Audit
- Functional Safety Assessment

Introduction

Purpose of the Safety Plan

The purpose of the functional safety concept is to identify new system level requirements and allocate these requirements to high level system diagrams for the lane assistance functional safety project as pertain to the potential malfunctions of the electrical and electronic systems as defined by ISO 26262 standard, tailored.

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 item considered in this plan is a simplified version of a Lane Assistance System.

The two main function of this item are:

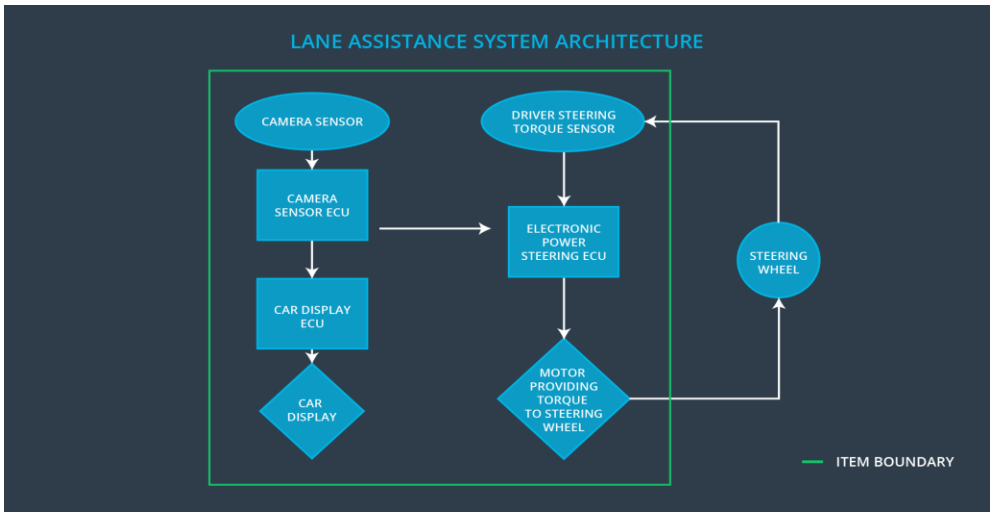
a) **Lane departure warning function**: When the driver drifts out towards the edge of the lane, the steering wheel vibrates to warn the driver. The vehicle will move the steering wheel back and forward to create vibration.
b) **Lane keeping assistance function**: When the driver drifts out towards the edge of the lane, this functionality will move the steering wheel so that the wheels turn toward the center of the lane. It should apply steering torque in order to stay in the ego lane (this is the lane where the car is.)

The item functionalities are implemented by the following subsystem:

a) **Camera subsystem**: This subsystem is composed by two components:
   i. Camera sensor
   ii. Camera sensor ECU (Electronic Control Unit)

b) **Electronic Power Steering subsystem**: This subsystem is composed by three components:
   i. Driver Steering Torque Sensor.
   ii. Electronic Power Steering ECU.
   iii. Motor Proving Torque to Steering Wheel.

c) **Car Display subsystem**: This subsystem is composed by two components:
   i. Car Display ECU
   ii. Car Display



When the camera senses that the vehicle is leaving the lane, the camera sends a signal to the electronic power steering system asking to turn and vibrate the steering wheel.The camera sensor will also request that a warning light turn on in the car display dashboard. That way the driver knows that the lane assistance system is active.

If the driver uses a turn signal, then the lane assistance system deactivates so that the vehicle can leave the lane. The driver can also turn off the system completely with a button on the dashboard.

The driver is still expected to have both hands on the steering wheel at all times. The electronic power steering subsystem has a sensor to detect how much the driver is already turning. The lane keeping assistance function will merely add the extra torque required to get the car back towards center. The extra torque is applied directly to the steering wheel via a motor.

The Line Assistance System does not include the following functionalities:

- Adaptive Cruise Control
- Automatic Parking
- Blind Spot Monitoring
- Tire Pressure Monitoring
- Pedestrian Protection

Goals and Measures

Goals

This project goals are:

- Identify risk and hazardous situations in the Line Assistance system components malfunction causing injuries to a person.
- Evaluate the risks of the hazardous situations.
- Low to risk of the malfunctions to a reasonable levels acceptable by current sociality.

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

In order to ensure a safety culture, the following characteristics needs to be observed:

- **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 (DIA)

This section defines the roles and responsibilities between parties involved in the Lane assistance project to ensure its development in compliance with ISO 26262.

- **Functional Safety Manager - Item Level**: Pre-audits, plans the development phase for the Lane Assistance item.

- **Functional Safety Engineer - Item Level**: Develop prototypes, integrate subsystems combining them into the Lane Assistance item from a functional safety viewpoint.
- **Project Manager - Item Level**: Allocates the resources needed for the item.
- **Functional Safety Manager - Component Level (Darien Martinez)**: Pre-audits, plan the development for the components of the Lane Assistance item.
- **Functional Safety Engineer - Component Level (Darien Martinez)**: Develop prototypes and integrate components conforming the Lane Assistance item.
- **Functional Safety Auditor**: Make sure the project conforms to the safety plan.
- **Functional Safety Assessor**: Judges where the project has increased safety.

Purpose of a DIA

In the safety plan, there is a section called the DIA which delineates the design and production responsibilities between the OEM and the Tier 1 supplier or between the Tier 1 supplier and the Tier 2 supplier

Responsibilities of the Company vs OEM

The OEM and Tier 1 supplier take on a customer- supplier relationship. The OEM will provide requirements for what a vehicle system needs to do. Then the Tier 1 supplier develops and produces the system for the OEM. The OEM may provide a preliminary product design and then the tier 1 supplier will finish the details. In this case, the OEM will provide our company with the requirements for the lane keeping system and our company will develop and produce the system for the OEM and analyze and modify the various systems from a functional safety standpoint.

Confirmation Measures

Purpose

Ensures that the functional safety measures have actually reduced the risk to levels acceptable by society

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.

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.

Functional Safety Assessment

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

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.