Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
03/03/2019	1.0	Madhu Hegde	Initial Version

Table of Contents

Introduction

Purpose of the Safety Plan

The document describes the framework of Lane Assistance Function item. The document provides the definition of the item and describes the sub systems of the function. The document also defines the goals, measures, roles and responsibilities for functional safety of the Lane Assistance System

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

Lane Assistance Function helps drivers to stay in ego lane and navigate the cars safely on roads with visible lane markings. There are two components in Lane Assistance System:

- **Lane departure warning system**: It is a mechanism designed to warn the driver when the vehicle begins to move out of its lane unless a turn signal is on in that direction. The purpose of this system is to minimize accidents by addressing the main causes of collisions: driver error, distractions and drowsiness. Typically, the warning is perceived as a torque feeling in the steering or loud sound signal.
- **Lane keeping assist system**: This mechanism automatically takes steps to ensure the vehicle stays in its lane. It uses image processing techniques to detect lanes and control the steering to keep the car within the lanes.

The item functionalities are implemented by the following subsystem:

- **Camera subsystem**: This subsystem is composed by two components:
  - Camera sensor
  - Camera sensor ECU (Electronic Control Unit)
- **Electronic Power Steering subsystem**: This subsystem is composed by three components:
  - Torque Sensor. It senses movement of the steering wheel.
  - Electronic Control Unit (ECU) is the heart of EPS.
  - Reduction gear which transfers turning force from motor to the steering wheel.
- **Car Display subsystem**: This subsystem is composed by two components:
  - Car Display ECU
  - Car Display

There are two types contact and non-contact type sensors. The camera sensor ECU processes the signal from the camera and if the vehicle is departing the lane, it sends an alarm signal to the electronic power steering ECU. The EPS ECU performs calculations based on sensor data and triggers steering wheel vibration if the lane change is detected without the turn signal. Simultaneously, the wheel adds extra steering torque to help the driver move back towards the center of the lane

The camera ECU also indicates the display ECU to turn on the warning light in the car display dashboard.

If the driver uses a turn signal, then the lane assistance system deactivates so that the vehicle can change 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 reduction gear.

Lane Assistance System does not include the following functionalities:

- Adaptive Cruise Control
- Automatic Parking
- Blind Spot Monitoring

- Tire Pressure Monitoring
- Pedestrian Protection

The current generation lane assistance function relies on visible lane markings and might not work well when markings are not visible due to rain or snow. Even though some argue that drivers could be less vigilant or distracted by the display unit, the overall safety is enhanced using lane assistance system. This feature is available in newer models of many car manufacturers and so far it is not a mandatory feature.

Goals and Measures

Goals

The major goal of this project is to assure safe and reliable operation of the components of vehicles lane assistance function, according to ISO 26262. Three goals are defined:

- Identify risk and hazardous situations due to malfunctions of Line Assistance system components.
- Evaluate the risks of the hazardous situations. These hazardous situations can cause personal injury and property damage
- Risk mitigation by defining safety goals.

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

To ensure a safety culture, the following characteristics are considered:

- Priority: safety has the highest priority among competing constraints like cost and productivity.
- Accountability: processes ensure accountability such that design decisions are traceable to people who made the decisions.
- Rewards: organization motivates and rewards the achievement of functional safety.
- Penalties: organization penalizes an attempt that compromises safety or quality.
- Independence: Development teams who design and develop a product should be independent from the audit teams.
- Clearly defined processes: Design and management processes, roles and responsibilities should be clearly defined.
- Resources: projects have sufficient resources and people with relevant skills.
- Diversity: intellectual diversity is sought after, valued and integrated into processes.
- Communication: communication channels among teams well defined for effective 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

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 of the Lane Assistance item.
- **Functional Safety Engineer - Item Level**: Develops prototypes, integrates subsystems into the Lane Assistance item from a functional safety viewpoint.
- **Project Manager - Item Level**: Allocates adequate resources for the item.
- **Functional Safety Manager - Component Level (Madhu Hegde)**: Pre-audits, plans development of individual components (e.g., Camera) of the Lane Assistance item.
- **Functional Safety Engineer - Component Leve l(Madhu Hegde)**: Develops prototypes of the components conforming the Lane Assistance item.
- **Functional Safety Auditor**: Ensures the project conforms to the safety plan.
- **Functional Safety Assessor**: Assess safety level of the project meets the design goals.

The purpose of the development interface agreement is to establish roles and responsibilities between OEM and tier-1 involved in the product development. There should be common

agreement among the parties regarding the contents of the DIA before the project start. The DIA also specifies metrics and quality of work products that each party will provide to check the compliance of work product to the agreement.

The OEM provides a functioning lane assistance system. Tier-1 is going to analyze and modify various sub-systems according to functional safety requirements.

The following steps are part of a separate DIA documentation which will be attached to this safety plan:

- Identifying & assigning safety managers for customers and suppliers
- Activities and tasks to be performed by the customer;
- Activities and tasks to be performed by the supplier
- Information and work products to be exchanged
- Teams or persons responsible for each activity in design and production
- Supporting processes or tools to ensure compatibility between customer and supplier technologies

Confirmation Measures

The purpose of the confirmation measures are:

- Ensure the Lane Assistance project conforms to ISO 26262.
- Ensure the Lane Assistance project really does make the vehicle safer.

The review of Confirmation Measures ensures that projects comply 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 makes sure the actual implementation of the project conforms to the safety plan. A Functional safety assessment confirms that the plan, design and developed product actually achieve functional safety.

A safety plan could have other additional sections. For example, a safety plan could 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.

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