Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
Feb 28, 2018	1.0	Junxun Luo	First submission

Table of Contents

Introduction

Purpose of the Safety Plan

This document provides an overall framework for a functional safety Lane Assistance Item. It includes the assignment of roles and responsibilities for the item's 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 item in this plan is a simplified version of a Lane Assistance item. It should alert the driver when the car departure from ego lane and it should also move the steering wheel to turn towards the lane center.

The two main functions of this item are:

1. Lane departure warning
   The lane departure waning function shall apply an oscillating steering torque to provide the driver a haptic feedback.
2. Lane keeping assistance
   The lane keeping assistance function shall apply the steering torque in order to stay in the ego lane.

The functions in this item are implemented by the following subsystems:

1. Camera subsystem
   The camera subsystem is responsible for detecting lanes. After detecting lanes, it will report the vehicle's position with respect to the lanes.

   This subsystem is composed by the following components:
   - Camera sensor
   - Camera sensor ECU

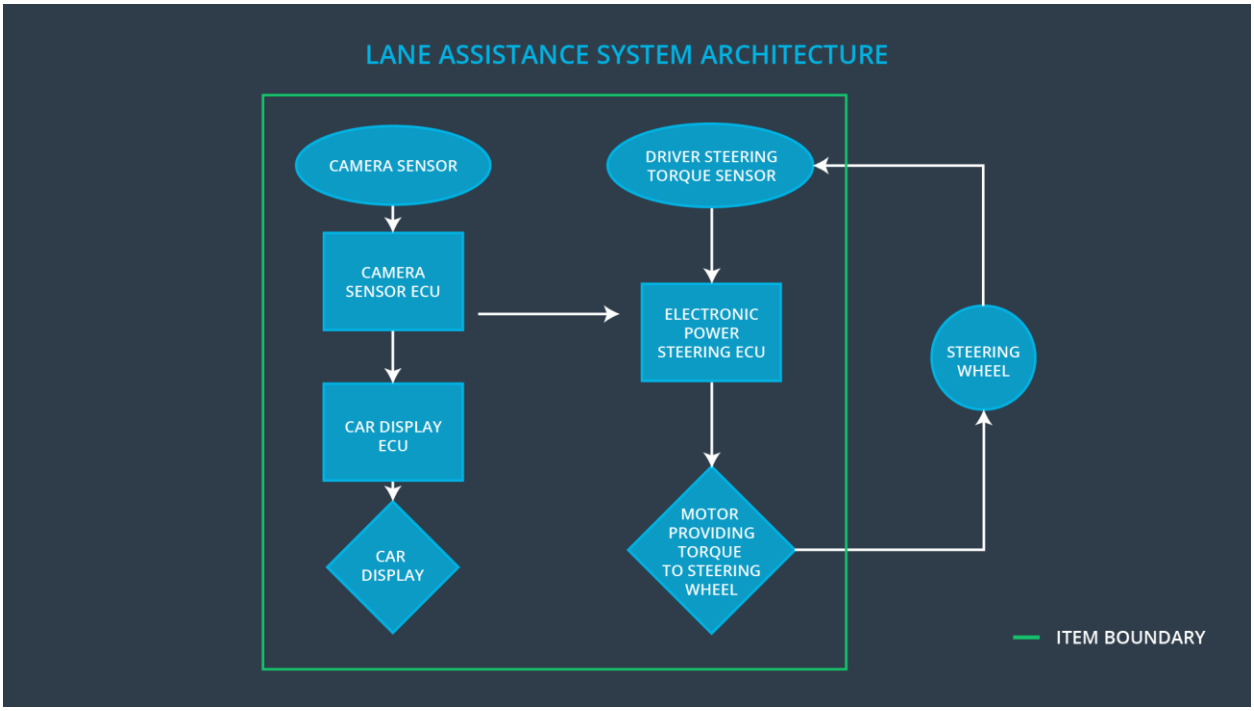
2. Electronics Power Steering subsystem
   The Electronics Power Steering subsystem is responsible for keeping the vehicle centered in its lane.

   This subsystem is composed by the following components:
   - Driver Steering Torque Sensor
   - Electronics Power Steering ECU
   - Motor Proving Torque to Steering Wheel

3. Car Display subsystem
   The Car Display subsystem is responsible for alerting the driver with changes in vehicle position and the current steering angle.

   This subsystem is composed by the following components:
   - Car Display ECU
   - Car Display

The following diagram shows the interaction between different subsystems.



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 vehicle display dashboard so that the driver knows the lane assistance system is active.

If the driver uses a turn signal, 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 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 extra torque required to get the car back towards the center. The extra torque is applied directly to the steering wheel via a motor.

The Steering Wheel is outside the Lane Assistance item.

Goals and Measures

Goals

The goals of the project are:

- Identify risk and hazardous situations in the Lane Assistance System components malfunction causing injuries to a person.
- Evaluate the risks of the hazardous situations.
- Lower the risk of the malfunctions to a reasonable level that is acceptable by 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	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

In order to ensure the 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

The purposes of a development interface agreement are:

- Clarify the responsibilities of different parties involved in a functional safety project
- Describe the work that each party will deliver
- Avoid disputes between parties
- Clarify who will be responsible for any safety issues

Tier-1 responsibilities:

- Derive safety requirements from OEM
- Provides the system that matches the requirements and ISO 26262 safety standards.

OEM responsibilities:

- Provide safety requirements
- Test the system that make sure it conforms ISO 26262

The responsibilities of each roles are:

- **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**: Pre-audits, plan the development for the components of the Lane Assistance item.
- **Functional Safety Engineer - Component Level**: 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.

Confirmation Measures

The purposes of the confirmation measures are:

- Ensure the Lane Assistance project conforms to ISO 26262.

- Ensure the Lane Assistance project makes the vehicle safer.

The confirmation review ensures the 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.

A functional safety audit makes sure the actual implementation of the project conforms the safety plan.

A functional safety assessment confirms that the plan, design and product actually achieve the 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.