Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [1.1]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
Mar. 23, 2018	1.1	Yi-Ching Chung	First draft from the template.

Table of Contents

Introduction

Purpose of the Safety Plan

This document is to provide an overall framework of the Land Assistance item in order to to reduce risk to acceptable levels. The corresponding roles and their responsibilities are included as well.

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

Introduction

The system is a set of elements that have at least a sensor, controller and an actuator whereas the item is is just a high level system in the vehicle. An item can be thought of as a system made up of systems. In general, the item definition will mention information including:

- Functional concept of the product
- Operational and Environmental Constraints
- Legal Requirements
- National and International Standards Related to the Item
- Records of previously known safety-related incidents or behavioral short-falls

The item in this plan refers to a simplified version of Lane Assistance System. The Lane Assistance System will have two functions:

- Lane departure warning: The lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback." In other words, the vehicle quickly moves the steering wheel back and forth to create a vibration.
- Lane keeping assistance: It will automatically assist the driver; the steering wheel turns towards the center of the lane. We will formally list the requirement as "the lane keeping assistance function shall apply the steering torque when active in order to stay in ego lane". Ego lane refers to the lane in which the vehicle currently drives.

Structure

The Lane Assistance System includes subsystem and the corresponding components as follows (also shown in Fig. 1):

- Camera subsystem
  - Camera sensor
  - Camera sensor ECU (Electronic Control Unit)
- Electronic Power Steering subsystem
  - Driver Steering Torque Sensor.

- Electronic Power Steering ECU.
- Motor Proving Torque to Steering Wheel.

- Car Display subsystem
  - Car Display ECU
  - Car Display

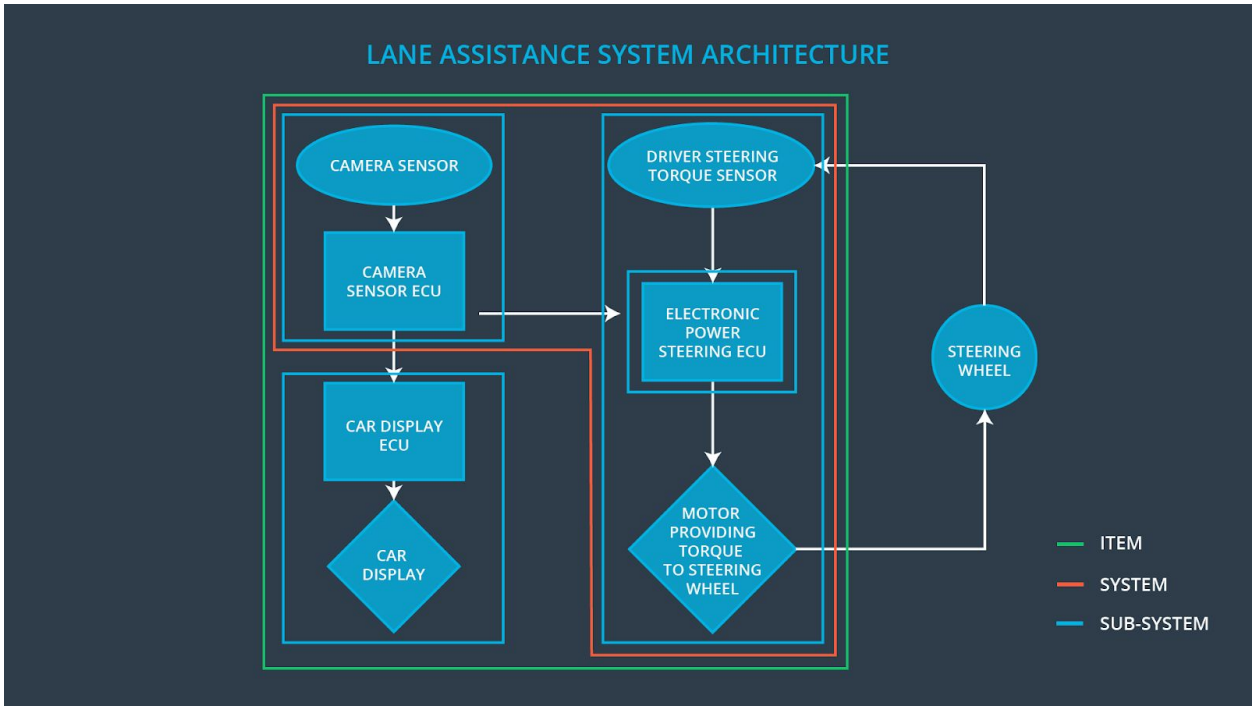

Fig. 1 Lane assistance system architecture (Udacity. *Fucntional Safety: Hazard Analysis and Risk Assessment*. Retrieved from https://classroom.udacity.com/nanodegrees/nd013/parts).

Mechanism

When the camera 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. When the driver drifts towards the edge of the lane, the camera detects and transmits signals to the electronic power steering system. Because the electronic power steering subsystem has a sensor to detect the magnitude of vehicle turning, the lane keeping assistance function will apply the extra torque directly to the steering wheel via a motor to get the car back towards center.
To be simplified, the functions activate as follows:

- the lane departure warning function will vibrate the steering wheel, and
- the lane keeping assistance function will move the steering wheel so that the wheels turn towards the center of the lane.

A warning light will turn on in the car display dashboard to let the driver know that the lane assistance system is active. If the driver uses a turn signal, The lane assistance system will deactivate if the driver uses a turn signal and the vehicle can leave the lane. The system can also be turned off completely with a button on the dashboard.

Constraint

The driver needs to both hands on the steering wheel at all times.
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

The goals are listed below:

- identify risk and hazardous situations by the system malfunction causing injuries to a person;
- evaluate the risks of the hazardous situations; and
- mitigate those risks to an acceptable/allowable degree.

Measures

The activities/responsibilities of each role in safety teams is listed in Table 1.

Table 1 Activities, responsibilities, and timeline.

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

The characteristics of safety culture are listed as follows:

- 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: the company designs processes 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: appropriate communication channels facilitate disclosure of problems.

Safety Lifecycle Tailoring

In this project, the safety lifecycle phases in scope are described as follows:

- 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

The organization is listed in Table 2.

Table 2 Description of 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 is to define the roles and responsibilities between parties involved in this project to ensure its development in compliance with ISO 26262. According to Table 2, responsibilities of the company versus those of the OEM 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(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.

Confirmation Measures

The purpose of the confirmation measures are:

- Ensure the Lane Assistance project conforms to ISO 26262.
- Ensure the Lane Assistance project actually makes the vehicle driven safer.

The confirmation review allows the projects to comply with ISO 26262. As the product is designed and developed, an independent person reviews the work to verify if ISO 26262 is being followed. A functional safety audit is to ensure the actual implementation of the project following the safety plan. A functional safety assessment confirms that the plan, design and developed product achieves 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.