Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

[Instructions: Fill in the date, version and description fields. You can fill out the Editor field with your name if you want to do so. Keep track of your editing as if this were a real world project.

For example, if this were your first draft or first submission, you might say version 1.0. If this is a second submission attempt, then you'd add a second line with a new date and version 2.0]

Date	Version	Editor	Description
2019.07.07	1.0	Zhilong Lu	First submission

Table of Contents

[Instructions: We have provided a table of contents. If the table of contents is not showing up correctly in your word processor of choice, please update it. The table of contents should show each section of the document and page numbers or links. Most word processors can do this for you. In Google Docs, you can use headings for each section and then go to Insert > Table of Contents. Microsoft Word has similar capabilities]

Contents

Introduction

Purpose of the Safety Plan

This document defines an overall planning of a functional safety project for the Lane Assistance item. By executing this plan, it ensures the developed item's safety. It also 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 considered in this plan is a simplified version of a Lane Assistance System. The two main function of this item are:

- **Lane departure warning function:** When the driver drifts out toward 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.
- **Lane keeping assistance function:** When the driver drifts out toward 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:

- **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:
    - Driver Steering Torque Sensor.
    - Electronic Power Steering ECU.
    - Motor Proving Torque to Steering Wheel.
- **Car Display subsystem:** This subsystem is composed by two 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 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 always still expected to have both hands on the steering wheel. 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 level acceptable by current society.

Measures

Measures and Activities	Responsibility	Timeline
Follow safety processes	All Team Members	Constantly
Create and sustain a safety culture	Project Manager	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

Here are some characteristics of our company's safety culture:

- **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 achievements 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 development interface agreement (DIA) defines the roles and responsibilities between companies involved in developing a product. The purpose of the DIA is:

- Clarifying the responsibilities of the different parties involved in a functional safety project
- Describe the work products that each company will provide
- Help avoid disputes between companies
- Clarifies who will be responsible for any safety issues in post-production

Responsibilities of our company (Tier-1): Component Level

- Functional Safety Manger – Component Level
  - Planning, coordinating and documenting of the development phase of the safety lifecycle
  - Tailors the safety lifecycle
  - Maintains the safety plan
  - Monitors progress against the safety plan
  - Performs pre-audits before the safety auditor
- Functional Safety Engineer – Component Level
  - Product development
  - Integration
  - Testing at the hardware, software and systems levels

Responsibilities of OEM: Item Level

- Functional Safety Manager – Item Level
  - Planning, coordinating and documenting of the development phase of the safety lifecycle
  - Tailors the safety lifecycle
  - Maintains the safety plan
  - Monitors progress against the safety plan
  - Performs pre-audits before the safety auditor
- Functional Safety Engineer – Item Level
  - Product development
  - Integration
  - Testing at the hardware, software and systems levels
- Project Manager – Item Level
  - Overall project management
  - Acquires and allocates resources needed for the functional safety activities
  - Appoints safety manager or might act as safety manager
- Functional Safety Auditor
  - Ensures that the design and production implementation conform to the safety plan and ISO 26262
  - Must be independent from the team developing the project
- Functional Safety Assessor
  - Independent judgement as to whether functional safety is being achieved via a functional safety assessment
  - Must be independent from the team developing the project

Confirmation Measures

[Instructions:
Please answer the following questions:

1. **What is the main purpose of confirmation measures?**
2. **What is a confirmation review?**
3. **What is a functional safety audit?**
4. **What is a functional safety assessment?**

]

1. The confirmation measures serve two purposes:
   - that a functional safety project conforms to ISO 26262
   - that the project really does make the vehicle safer

2. *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.

3. *Functional safety audit*
Checking to make sure that the actual implementation of the project conforms to the safety plan.

4. *Functional safety assessment*
Confirming 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.

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.