Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
5/24/2018	1.0	Kiran Acharya	Safety Plan Lane Assistance – attempt 1

Table of Contents

Introduction

Purpose of the Safety Plan

Safety Plan focuses on defining roles and then outlining the steps, one has to take to achieve 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 here is that of Lane Assistance System.
The two main function of this item are:

- **Lane departure warning function**
- **Lane keeping assistance function**

If a driver departs a lane without using a turn signal, the system assumes that the driver has become distracted and did not mean to leave the lane. The system will vibrate the steering (lane departure warning) and also move the steering wheel back towards the lane center (lane keeping assistance).

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

There are few constraints that the Sub-Systems imply on the vehicle,

- **Operational and Environmental Constraints**.
  This could especially be limited to camera performance; lane lines are difficult to detect in snow, fog, etc.
  Lidar may take a back step in performance, during bad weather conditions.
  GPS may not work well in tunnels.
- **Legal requirements in your country for lane assistance technology**
  The lane markings or the sign boards would vary from country to country in terms of language used on sign boards, some country has a different lane keeping methodology. These factors may have to be considered while making a plan for Lane Assistance.
- **National and International Standards Related to the Item**
  Most of the automotive companies and automotive parts suppliers strive to make their products compliant with the ISO 26262 standard.

Goals and Measures

Goals

- Identifying Hazards
- Lowering risks to acceptable level.

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, 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 Roles

If we are designing a new product then we may need to follow the entire Safety Lifecycle, but if we modify an existing product in the system, we may need to make changes only in those phases which are affected by the product.

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

A DIA (development interface agreement) defines the roles and responsibilities between companies involved in developing a product. All involved parties need to agree on the contents of the DIA before the project begins.

Role		Job Description
Functional Safety Auditor	-	make sure the project conforms to safety plan.
Test Manager	-	Planning and overseeing testing activities.
Functional Safety Manager	-	pre-audits, plans the development phase.
Functional Safety Assessor	-	judges whether the project has increased safety.
Project Manager	-	Allocates resources.
Functional Safety Engineer	-	Develop prototypes, integrate sub-systems into larger systems

Confirmation Measures

Confirmation measures serve two purposes:

1. that a functional safety project conforms to ISO 26262, and
2. that the project really does make the vehicle safer

Confirmation Review ensures that the project complies with ISO 26262.

Functional Safety audit is a check to make sure that the actual implementation of the project conforms to the safety plan.

Functional Safety assessment is a confirmation that the 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.