Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.0

Document history

Date	Version	Editor	Description
2018-10-20	1.0	Rodrigo Vasconcelos	Initial Functional Safety Plan

Table of Contents

Introduction

Purpose of the Safety Plan

Define the roles, responsibilities and steps required to achieve functional safety of the **lane assistance system** of a car.

Here, we will list:

- The elements that make up the resulting item of the project.
- What tasks need to be done to ensure functional safety and when they will be carried out.
- Who is responsible for each phase of the project and the resulting work.
- How the functional safety of the system will be assessed and audited.

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 lane assistance item is a new system in a car that shall detect when the car is veering far from the lane's center without a turn signal activated and either: vibrate the steering wheel when small deviations are detected to let the driver know there is an issue, or gently steer the car back to the center of the lane when more significant deviations are detected.

The main functions of the system are:

- Lane departure warning: The system shall notify the driver when the car is drifting from the lane's center and a turn light has not been engaged.
- Lane keeping assistance: The system shall steer the car back to the center of the lane when the car is at risk of changing lanes and the turn light has not been engaged.

In order to achieve these functions, the following components are required:

- Camera sub-system: Shall identify the lane and the car's position within the lane. Shall detect unintended lane center departure and activate corrective actions in two levels. Shall calculate the amount of steering required to safely drive back to the center of the lane.
- Car display sub-system: Shall display the lane assistance system status (on/off/disabled). Shall enable the driver to disable the system. Shall display if the system presents a malfunction.
- Steering sub-system: Shall engage the vibration when indicated to do so. Shall turn the wheels to direct the car without the driver's help when indicated to do so.

The camera sub-system is further divided in:

- Camera sensor: Shall capture the scene in front of the car.
- Camera sensor ECU: Using camera data, the system shall identify the lane size, boundaries and center. It shall also measure the current deviation of the car from the lane's center. Shall determine if the car is within an acceptable distance to the lane's center or if it is within warning or corrective action ranges. Shall determine the steering torque necessary to direct the car towards the center of the lane given the driving direction.

The car display sub-system is further divided in:

- Car display ECU: Shall store information on the system status (on/off/disabled/malfunction). Shall pick up the information on the turn signal status.
- Car display: Shall provide a light to identify if the system is on or off. Shall provide a light to identify if the system is engaged or disengaged. Shall provide a light to indicate system malfunction. Shall provide a button to enable or disable the system.

The steering sub-system is further divided in:

- Driver steering torque sensor: Shall detect the torque the driver is applying to the steering wheel.

- Steering ECU: Shall calculate the appropriate torque to apply to steering given the driver's applied torque and the torque required to get back on the center of the lane.
- Motor providing torque to steering wheel: Shall apply the torque calculated by the Steering ECU.

The driver is in one end of the system's boundary. The steering wheel is at the other end of the system's boundary. Items outside the boundary of the system are outside of the scope of the project. As such, there is no claim to control the driver or the systems that convert the steering wheel's angle to car wheel's motion.

In order for the system to provide lane assistance (i.e. its intended objective), the camera must have an unobstructed view of the scene in front of the car. The road's lanes must also be clearly marked and visible.

We have not found any standards mandated for Lane Assistance systems, nor any legislation in Mexico for it.

Goals and Measures

Goals

The goal of this project is to reduce the risk of a collision when the vehicle is travelling by making sure that the car is shifting lanes only when the driver intends to do so.

In order to do this, the driver will have to activate turn signals previous to engaging in a lane change. Any other course of action will result in the system warning the driver first and then attempting to steer the car back into the lane if the course is not corrected after the warning.

We aim to prove that use of the lane assistance system reduces collision risks.

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

As a company, we pride ourselves in having Health and Safety as the top priority, as requested by our CEO. We build safety into our offices, our practices and our products and services.

Examples of safety in our offices can be found in the form of outward swinging doors, emergency signaling and lightning, see-through door panels, stair handrails, step highlighting and grip enhancements, electrical equipment guards, etc.

Examples of safety in our practices include going up and down the stairs with three points of contact, avoiding looking at mobile phone screens while walking, providing safety inductions on the building to new personnel and visitors, encouragement by management to identify hazards and report near-misses and accidents, etc.

Our products and services are imbued with safety as we build and provide them since we: prioritize safety, document design decisions and approvals, separate the design, testing and audit teams to prevent conflicts of interest, conduct risk assessment meetings with a diverse cross-functional group, and provide constant training on safety and functional safety to all the teams involved.

Safety Lifecycle Tailoring

As stated in the introduction, for this 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

This decision stems from the fact that hardware elements are provided by the OEM and as such are out of the scope. Changes to the production process or for maintenance and repair are within the OEM’s responsibilities (see Roles and Development Interface Agreement).

We will be focusing then on the following steps (linearized V model):

1. Item definition
2. Initiation of the safety lifecycle
3. Hazard Analysis and Risk Assessment (HARA)
4. Functional safety concept
5. Initiation of product development at the system level
6. Specification of the technical safety requirements
7. System design
8. Initiation of product development at the software level
9. Specification of software safety requirements
10. Software architectural design
11. Software unit design and implementation
12. Software unit testing
13. Software integration and testing
14. Verification of software safety requirements
15. Item integration and testing
16. Safety validation
17. Functional safety assessment
18. Release for production

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
Test Manager- Component Level	Tier 1
Test Manager- Item Level	OEM
Functional Safety Auditor	OEM or external
Functional Safety Assessor	OEM or external

Development Interface Agreement

Since this project will be carried out as jointly developed system between the OEM and the Tier 1 supplier, it is critical to clearly identify the roles and responsibilities of each party.

The OEM will provide a Functional Safety Manager to plan and coordinate the project at the system level. Functional Safety Engineers will also be provided to generate the technical specifications and system design.

The Tier 1 supplier will provide a Functional Safety Manager to plan and coordinate the project at the component level. One or more Functional Safety Engineers from the Tier 1 supplier will generate the software architectural and unit design.

The Tier 1 supplier will then build the Lane Departure Warning and Lane Keeping Assistance elements according to these specifications.

The Tier 1 supplier will guarantee the functional safety of the components with the help pf a Testing Manager and Engineers, while the OEM will provide its own Test Manager to ensure correct integration with other systems.

Lastly, Safety Assessment and Safety Auditing are the responsibility of the OEM; either with own resources or through the use of an external entity.

Confirmation Measures

Confirmation measures for this project will ensure that functional safety standards are being followed (ISO 26262) and that the developed system actually increases the safety of the vehicle.

The first measure is a confirmation review, which will certify the project is adhering to functional safety standards. It is paramount that the review be carried out by an independent person from the project.

The second measure (a functional safety audit) must be executed once every two months to confirm that the safety plan is actually being followed.

The third and final measure will be a functional safety assessment to determine whether the new system actually makes the vehicle safer.

While the fist measure can be executed by someone in the company (but outside the project), the second and third measures are recommended to be performed by external parties to ensure a lower bias towards the result.

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.