Elektrobit

UDACITY

Safety Plan
Lane Assistance

Document Version: 1.0

Submission Version 1.0, Released on 2018-01-26

Document history

Date	Version	Editor	Description
2018-01-26	1.0	Ioannis Tornazakis	First submission

Table of Contents

Introduction

Purpose of the Safety Plan

The purpose of the Safety Plan is to define all the steps that are required to achieve functional safety for the Lane Assistance System. In addition, it defines the roles and responsibilities for each member of the development team.

Scope of the Project

For the Lane Assistance System project, the following safety lifecycle phases are:

1. In scope
- Concept phase
- Product Development at the System Level
- Product Development at the Software Level

2. Out of scope
- Product Development at the Hardware Level
- Production and Operation

Deliverables of the Project

The deliverables of the project is the set of the following documents:
1. Safety Plan
2. Hazard Analysis and Risk Assessment
3. Functional Safety Concept
4. Technical Safety Concept
5. Software Safety Requirements and Architecture

Item Definition

The item under analysis is the **Lane Assistance System** and has two functions:

1. Lane Departure Warning Function
When the vehicle camera senses that the driver it is about to change lane without using the appropriate turn indicator, the Lane Departure Warning function vibrates the steering wheel in order for the driver to get a warning that an involuntary lane change is about to happen.

2. Lane Keeping Assistance Function
When the vehicle approaches the lane boundary, the Lane Keeping Assistance function adds the extra steering torque needed to move back the vehicle towards the centre of the lane.

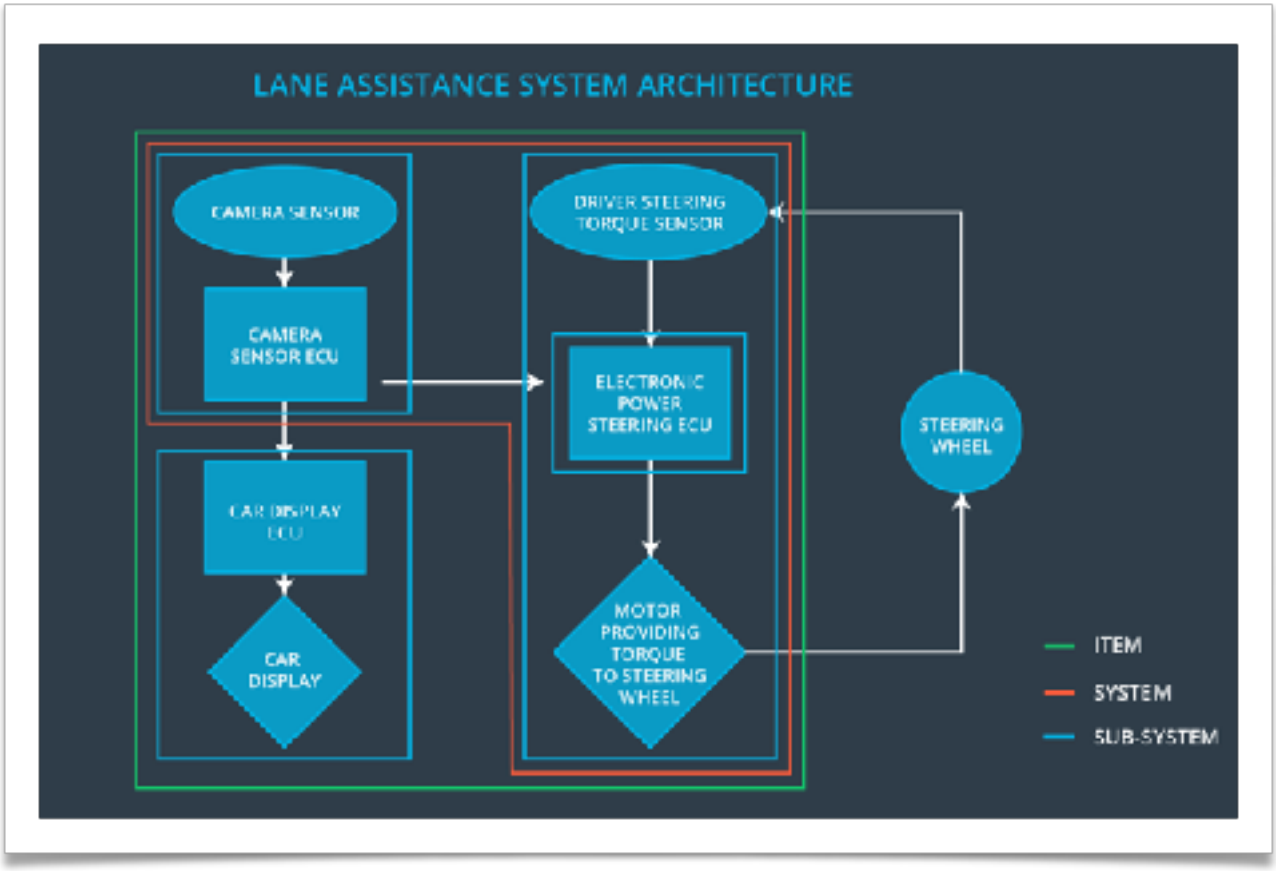

FIGURE 1. LANE ASSISTANCE SYSTEM ARCHITECTURE

The Lane Assistance System of three sub-systems: camera, power steering, and car display. However, the steering wheel is not part of the item.

When the camera sub system 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.

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 centre. The extra torque is applied directly to the steering wheel via a motor.

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. Note that the car display sub-system is outside of the system boundary.

Goals and Measures

Goals

In order for the Lane Assistance System to be compliant with the ISO 26262 we set the following goals:

1. **Identify hazards** in the vehicle's Lane Assistance System that could cause physical injury or damage to a person's health.

2. **Evaluate the risk** of the hazardous situation so that we know how much we need to lower the risk.

3. **Prevent accidents from occurring** by lowering risk to reasonable levels using a Systems Engineering methodology.

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

The safety culture of our company has the following characteristics:

1. **High priority**: safety has the highest priority among competing constraints like cost and productivity.

2. **Accountability**: processes ensure accountability such that design decisions are traceable back to the people and teams who made the decisions.

3. **Rewards**: the company motivates and supports the achievement of functional safety.

4. **Penalties**: the company penalises shortcuts that jeopardise safety or quality.

5. **Independence**: teams who design and develop a product are independent from the teams who audit the work.

6. **Well defined processes**: company design and management processes are clearly defined.

7. **Resources**: projects have necessary resources including people with appropriate skills.

8. **Diversity**: intellectual diversity is sought after, valued and integrated into processes.

9. **Communication**: communication channels encourage disclosure of problems.

Safety Lifecycle Tailoring

Since we are modifying an existing product at systems and software level, we will have the following safety lifecycle phases in scope:
- Concept phase
- Product Development at the System Level
- Product Development at the Software Level

The following phases are out of scope for this project:
- 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 (DIA)

The DIA defines the roles and responsibilities between the companies involved in developing the Lane Assistance System. It also specifies what evidence and work products each party will provide to prove that work was done according to the agreement, and ensures that all parties are developing safe products in compliance with ISO 26262. This DIA is agreed between all parties involved in the development of the Lane Assistance System.

Role	Responsibilities
Functional Safety Manager- Item Level	• Plans, coordinates and documents 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	• Item development • Integration • Tests at the software and system 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 Manager- Component Level	• Plans, coordinates and documents the development phase of the safety at the component level
Functional Safety Engineer- Component Level	• Component development • Tests at the software level

Functional Safety Auditor	• Ensures that the design and production implementation conform to the safety plan and ISO 26262 • Is independent from the team developing the project
Functional Safety Assessor	• Provides independent judgement as to whether functional safety is being achieved via a functional safety assessment • Is independent from the team developing the project

Confirmation Measures

The **Confirmation Measures** ensure that the functional safety analysis conforms to ISO 26262, and that it really does make the vehicle safer. Both the Functional Safety Auditor and the Functional Safety Assessor that will carry out the Confirmation Measures are chosen to be independent from the people who actually developed the project.

The **Confirmation Review** ensures that the project complies with ISO 26262. As the product is designed and developed, an independent Functional Safety Assessor will review the work to make sure ISO 26262 is being followed.

The **Functional Safety Audit** checks to make sure that the actual implementation of the project conforms to the safety plan and is carried out by the Functional Safety Auditor.

The **Functional Safety Assessment** confirms that plans, designs and developed products actually achieve functional safety and is performed by the Functional Safety Assessor.