Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
17/08/2018	1.0	Jumana MP	First Attempt

Table of Contents

Introduction

Purpose of the Safety Plan

The purpose of this safety plan is to provide an overall framework for the Lane Assistance item, and to assign roles and responsibilities for functional safety for this item.

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

This safety plan covers the Lane Assistance System which is one of the Advanced Driver Assistance System(ADAS)s. This item alerts the driver that the vehicle has accidentally departed it's lane and attempts to steer the vehicle back on track towards the center of the lane, to prevent accidents.

The Lane Assistance System will have two functions:

1. Lane departure warning:
   The lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback.
2. Lane keeping assistance:
   The lane keeping assistance function shall apply the steering torque when active towards the center of the lane, in order to stay in the ego lane.

There are three main subsystems for the item. They are,

1. **The camera subsystem:**
   This subsystem is composed of camera sensor and camera sensor ECU, to detect the vehicle departing out of the lane. It does so by monitoring the position of the car.
2. **The electronic power steering system:**
   This subsystem is composed of the drive steering torque sensor, electronic power steering ECU and the motor providing torque to the steering
   wheel to steer vehicle back on track
3. **The car display subsystem:**
   This subsystem has the car display ECU and the car display, which displays the warning light on the display dashboard to alert the driver
   that the item is active.

Figure 1 below shows the item, it's subsystems and components as well as the boundaries. Steering wheel is the only component of the system
that is outside the item.

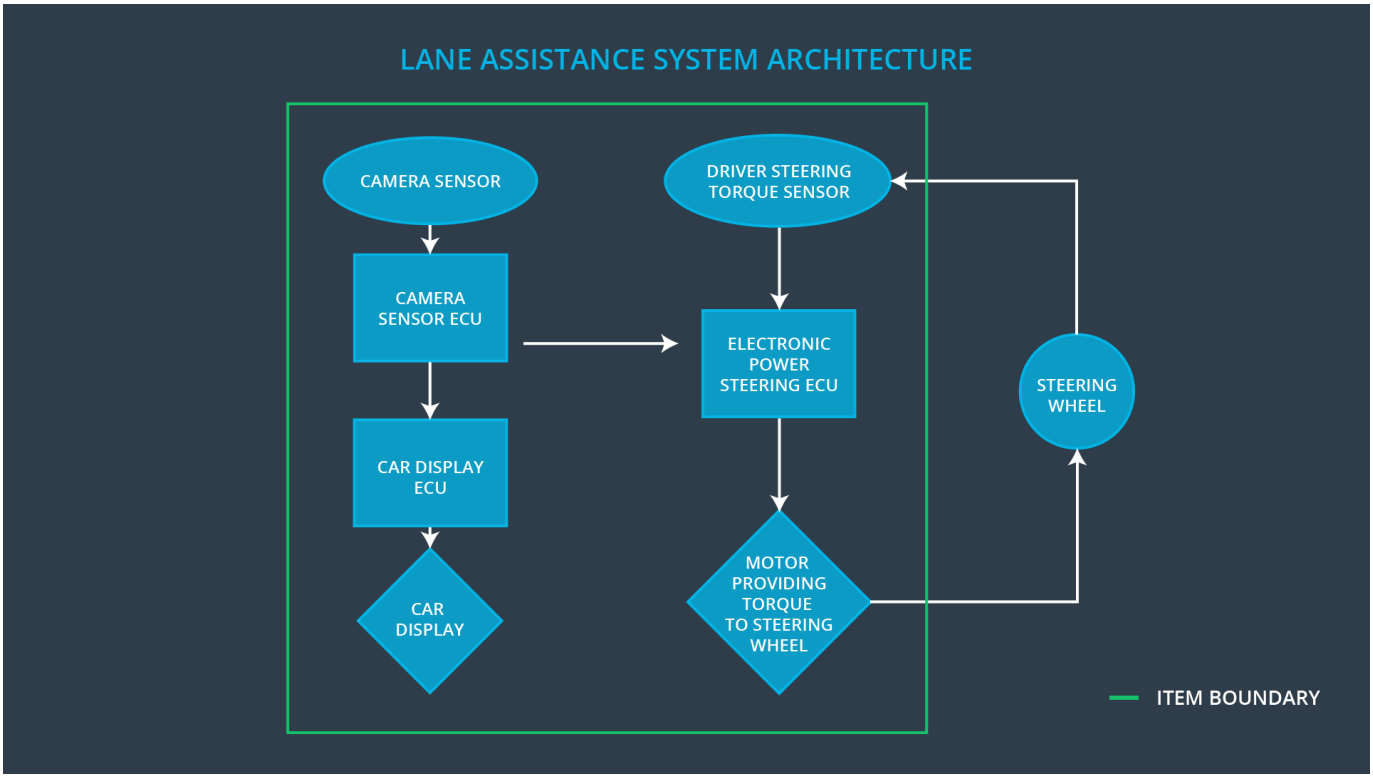

Figure 1 Lane Assistance System Architecture

Operational and Environmental Constraints

Normal driving on country roads during normal conditions with high speed (the driver is misusing the lane keeping assistance function as an autonomous function)

Goals and Measures

Goals

The major goals of this project are:

- Identify risk and hazardous situations in the lane assistance system components malfunction causing injuries to a person.
- Evaluate risks associated with hazardous situations.
- Lower the risk of the malfunctions in the system to reasonable levels acceptable by the current society.

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

To increase functional safety, our organization follows a safety culture. Some of them are:

- **High priority**: Safety has the highest priority even if it means poor productivity or higher cost,
- **Accountability**: Design decisions are well documented with traceability.
- **Rewards**: Motivates and supports the achievement of functional safety by broadcasting it on internal communication channels.
- **Independence**: Design and development team for a product are independent from the teams who audit and assess the work.
- **Well defined processes**: Clearly defined company design and management processes.

- **Resources**: It is made sure that the projects have necessary resources including people with appropriate skills.
- **Diversity**: While choosing team players, intellectual diversity is sought after, valued and integrated into processes.
- **Communication**: Potential threat to safety is clearly communication across channels to encourage disclosure of problems to the parties
  Concerned.

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

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. The DIA also specifies what evidence and work products each party will provide to prove that work was done according to the agreement. The ultimate goal is to ensure that all parties are developing safe vehicles in compliance with ISO 26262.

OEM is responsible for the overall vehicle safety and all the required ISO26262 are met in the item. Both the companies have agreed that the safety lifecycle tailored is enough to comply with the ISO26262 standards. Both the companies must appoint customer and supplier safety managers. All the activities and processes to be undertaken by both the customer and supplier are clearly stated and agreed.

Agreement was made with OEM that all on information and tools related to achieving functional safety for the item will be exchanged between both the companies through a common channel. Tier-1 will take the responsibilities involved in the design and production of every subsystem component and making sure that they are functional as well as they meet the functional safety requirements. Tier-1 will not be responsible for the functionality of the full system or it’s safety requirements.

Confirmation Measures

The main purpose of the confirmation measures is to ensure that:

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

Confirmation review is the review work done as the product is designed and developed, ensuring that the project complies with ISO 26262.
Functional safety audit is the process of checking to make sure that the actual implementation of the project conforms to the safety plan.
Functional safety assessment is the process of 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.