Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.0
10/04/2018

Document history

Date	Version	Editor	Description
10/04/2018	1.0	GRANIE Guillaume	First Attempt

Table of Contents

Introduction

Purpose of the Safety Plan

The safety plan discusses what elements need to be added to the system in order to make it safe. It also provides testing evidence that shows the system functioning properly.
The documentation provides evidence that what has been added to the system really does make the vehicle safer.

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 considered item for this Safety Case is the Lane Assistance functionality. This item encompasses two distinct safety enhancing functionalities to the vehicle:

- The **Lane Departure Warning** (LDW) is an Advanced Driver Assistance System (ADAS) signaling when the vehicle inadvertently drifts off the ego lane by applying an oscillating torque to the steering wheel. It does so by detecting the lane lines on the road and understanding where the vehicle lies relative to them.

- The **Lane Keeping Assistance** (LKA) is an ADAS applying some torque on the steering wheel in order to keep the car within the ego lane when it detects that the car is inadvertently changing lane.

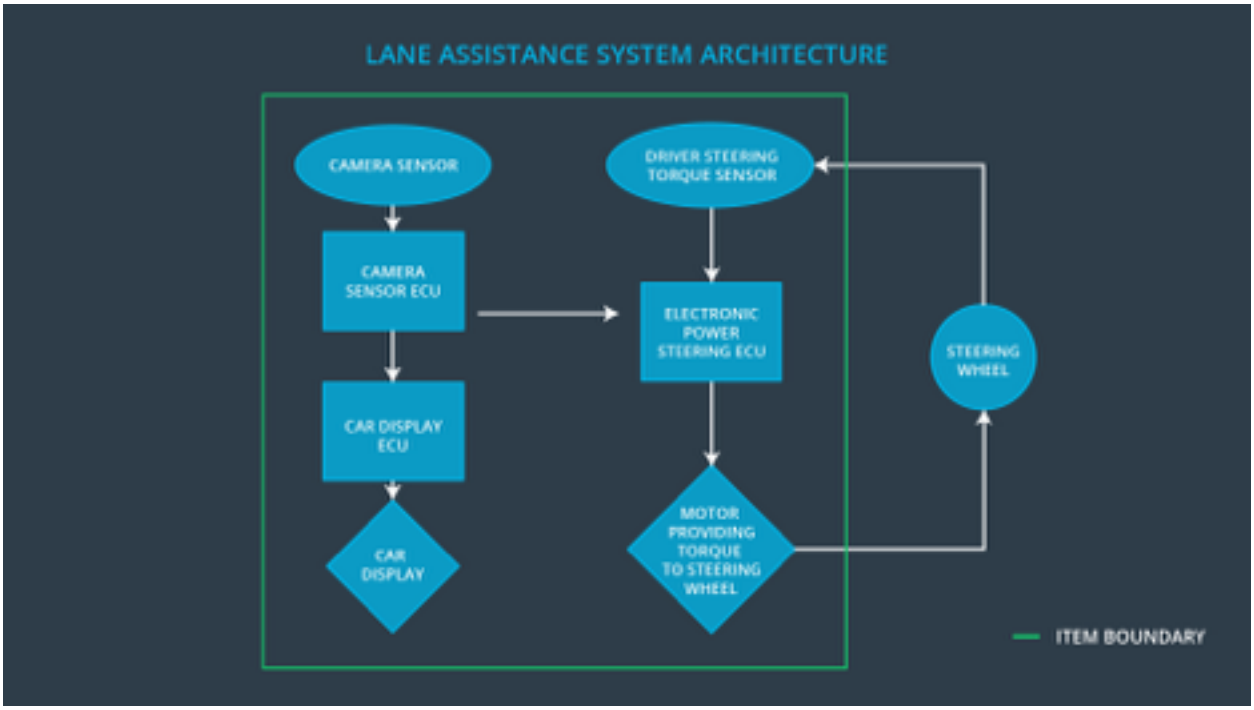
These 2 functionalities are implemented using the following subsystems:

- The **Camera** subsystem is composed of the recording device « Camera Sensor » and the hardware platform running a software component called the « Camera Sensor Electronic Control Unit (ECU) ».
- The **Electronic Power Steering** subsystem is composed of the following components:
  - Driver Steering Torque Sensor
  - Electronic Power Steering ECU
  - Motor (Provides torque to the steering wheel column)
- The **Car Display** subsystem is composed of 2 components:
  - Car Display
  - Car Display ECU

It is important to note that the ADAS functionalities described previously are not Self-Driving nor Autonomous Driving capable.

The steering wheel is not part of the considered system. This is reflected onto the diagram of the next page.

The following diagram provides a description of the overall system with the connections between the previously stated subsystems:



Goals and Measures

Goals

This project goals are:

- Identify risk and hazardous situations during the usage of the Lane Assistance item which could lead to human injuries.
- Evaluate the level of risk which represent these hazardous situations.
- Establishing measures to lower the probability that faults in the system would lead to hazards.
- Lower the risk of the Lane Assistance item to an 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

Safety Lifecycle Tailoring

In order to ensure a safety culture the 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.

Roles

Role	Position in Organisation
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 purpose of the development interface agreement (DIA) is to delineate the roles and responsibilities between the OEM and the Tier-1 involved in developing this product. Both parties 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 OEM provides a functioning lane assistance system. Tier-1 is going to analyze and modify various sub-systems according to functional safety requirements.

The following steps are part of a separate DIA documentation which will be attached to this safety plan:

- Appointment of customer and supplier safety managers
- Joint tailoring of the safety lifecycle
- Activities and processes to be performed by the customer; activities and processes to be performed by the supplier
- Information and work products to be exchanged
- Parties or persons responsible for each activity in design and production
- Any supporting processes or tools to ensure compatibility between customer and supplier technologies

This section defines the roles and responsibilities between parties involved in the Lane Assistance project to ensure its development in compliance with ISO 26262:

- **Functional Safety Manager** - Item Level : Pre-audits, plans the development phase for the Lane Assistance item.
- **Functional Safety Engineer** - Item Level : Develop prototypes, integrate subsystems combining them into the Lane Assistance item from a functional safety viewpoint.
- **Project Manager** - Item Level : Allocates the resources needed for the item.
- **Functional Safety Auditor** : Make sure the project conforms to the safety plan.
- **Functional Safety Assessor** : Judges where the project has increased safety.

This section defines my own responsibilities as the Tier-1 organization in this project:

- **Functional Safety Manager** - Component Level: Pre-audits, plan the development for the components of the Lane Assistance item.
- **Functional Safety Engineer** - Component Level: Develop prototypes and integrate components conforming the Lane Assistance item.

Confirmation Measures

Confirmation measures ensure that the applied processes comply with functional safety standards provided by ISO 26262 and that project execution is following the safety plan, therefore verifying if the design really does improve safety.

In particular by providing **confirmation review**, during design and development of the product, compliance with ISO 26262 is assured by an independent person.

A **functional safety audit** checks that the actual implementation of the project considers the safety plan.

Finally **functional safety assessment** confirms that plans, designs and developed products actually achieve functional safety.[1]

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.