Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 2.0
Released on 2017-08-27

Document history

Date	Version	Editor	Description
Aug 24, 2017	1.0	Sampath Vanimisetti	Initial draft with outline.
Aug 27, 2017	2.0	Sampath Vanimisetti	Final draft with comments added.

Table of Contents

Contents

Introduction

Purpose of the Safety Plan

The purpose of this safety plan is to provide the overview of strategy adopted for lane assistance feature. This safety plan only addresses the electrical and electronic systems failure and does not cover mechanical or hydraulic failures as governed by ISO 26262.

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 an Advanced Driver Assistance System or Active Safety feature that servers the following two functions:

1. **Lane Departure Warning (LDW):** This function warns the driver if he is unintentionally departing a lane.
2. **Lane Keep Assist (LKA)**: This function helps or aides the driver to return the vehicle to the centre of the lane by making small and incremental changes to the steering. This

function is designed in a manner that it cannot be misused by the driver as an autonomous feature.

The item boundary include three sub-systems as shown in following Figure 1 re-used from the video lectures. It demonstrates the lane assistance system item and the participating sub-systems:

i. Camera sensor module
ii. Electronic power steering control module
iii. Car instrument panel display

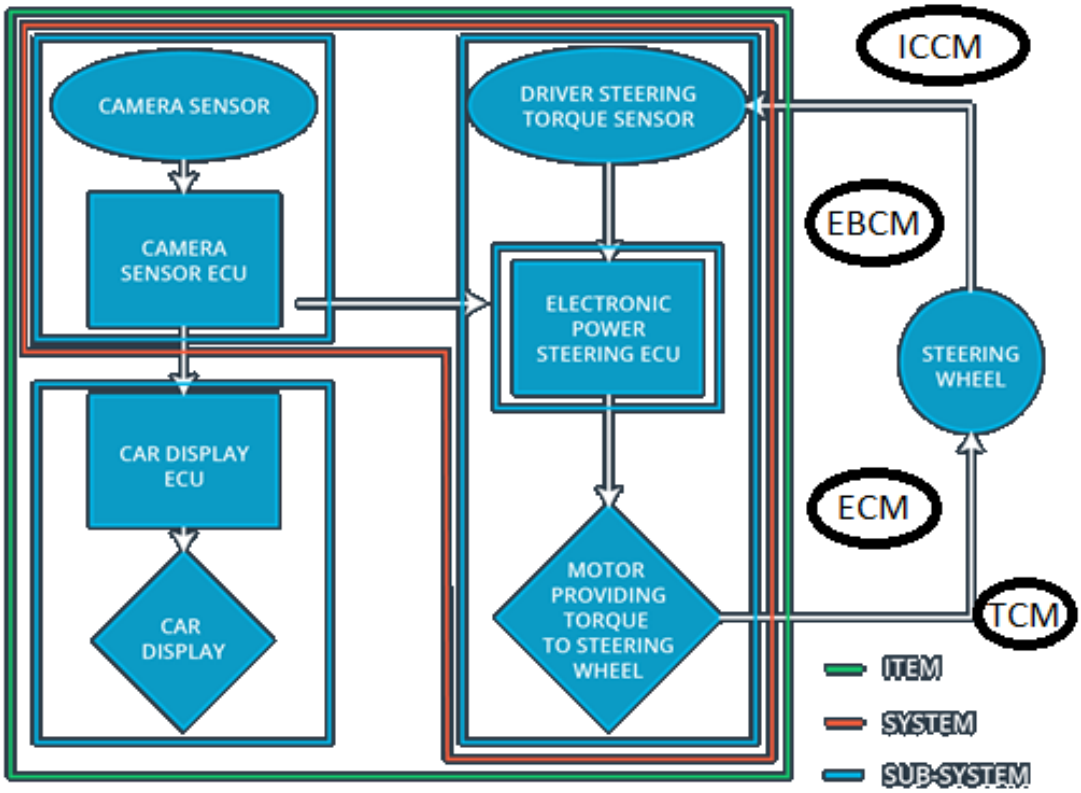

Figure 1. Item (feature), system, sub-system and component boundaries for lane assistance.

Overview of the system function:

A typical ADAS or active safety systems relies on four different elements: (a) sensor, (b) controller (compute / decisions), (c) actuation, and optionally (d) driver information.

For the lane departure warning (LDW), the sensor is a camera which continuously monitors the road ahead and computes the position of vehicle in the ego-lane (e.g., center offset). When the center-offset is large, the vehicle is about to leave the lane. At this time, the camera module algorithms send signal to the steering module to first warn the driver by vibrating the steering

wheel. The LDW warning light is also turned-on on the driver information console or instrument panel. Audible alerts are also issued to driver.

For the lane keep assist (LKA), the camera sensor continuously monitors the road ahead. It estimates the curvature of the ego-lane ahead of the vehicle. It also, keep monitors other vehicles ahead in the lane. Depending on the strength of curvature of the road ahead, the algorithms in the camera module provide information to the steering control module. The steering control module then determines how much steering torque and rate of steering angle change to apply based on constraints imposed by safety and comfort requirements. The steering control module internally has other sensor which identify how much the steering wheel is already turning. The steering control module then command the steering motor to turn the steering wheel by precise amount to keep vehicle in the centre of the lane. In order to ensure that the driver does not misuse the item as an autonomous feature, the driver is required to keep both hands on the steering wheel at all times. Furthermore, the duration for which the steering torque is applied is also limited. The driver can take control of the steering function at any time. Furthermore, the driver can disable the feature at any instant by pressing a button.

The boundary of this item is shown in green line in Figure 1. The item includes subsystems such as the front camera module (FCM), electronic power steering module (EPS), and car display (IPC or DIC). The boundary of the control system is shown in red line in Figure 1. The subsystem boundaries are shown in blue lines. Other subsystems and elements in the vehicle that are outside this item boundary are also shown in Figure 1. For example, the integrated chassis control module (ICCM), EBCM (electronic brake control module), ECM (engine control module) or TCM (transmission control module) do not interact with this feature. However, these susbstems may interact with the EPS or IPC/DIC for other items/features.

Other constraints for the item and subsystem are:

- The camera sensing module should be able to work in adverse external conditions: when it is raining, road is covered in snow, low visibility fog conditions.
- Special considerations need to be given to cases where the system has to operate in undivided highways. For example, in markets such as India, a majority of highways are undivided. This would require the features and subsystems to be able to automatically identify if the highway is divided or not. If it is not divided, the side toward the on-coming traffic needs to be penalized and the algorithms have to account for these factors.
- Lane keep assistance features have known to previously fail near merge or exit lanes. The system can also interface with the GPS position / localization module to improve performance and reliability of feature.

Goals and Measures

Goals

The goals of the Lane Assistance Functional Safety Plan project is to:

1. Perform Hazard Identification and Risk Analysis using ISO 26262 to identify hazards and risks for the lane assistance system if a malfunction were to occur, which may cause injury to passenger or damage to property.

2. Evaluate each hazard and risk.

3. Define an ASIL level for each hazard.

4. Finally, utilize systems engineering techniques to lower risk to acceptable levels.

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

Following organizational cultural priorities can help improve safety:

- ✓ **Highest priority on safety**: over and above all other constraints like cost, timing, quality and productivity
- ✓ **Process definition & RASIC**: Management processes should be clearly defined using tools such as team charters and RASIC.
- ✓ **Accountability, Rewards and Penalties**: System engineering processes should ensure accountability such that design decisions are traceable back to the people and teams who made the decisions. The organization motivates, encourages and reinforces safety-driven behaviour with rewards. More importantly, the organization should penalize individuals or teams taking shortcuts that compromise safety.
- ✓ **Independence and Segregation**: Teams who design and develop a product should be independent and segregated from the teams who audit the work. The organization should remove any conflict-of-interest in the audit processes.
- ✓ **Resources**: Safety-related items should get highest priority for resources.
- ✓ **Diversity, Inclusiveness:** Intellectual diversity is sought after, valued and integrated into processes. Safety improvement or risk mitigation ideas should be welcome from anywhere in the organization, even from outside the Systems Engineering teams.
- ✓ **Communications**: Continuous communication on safety-related issues should become a culture within the organization.

Safety Lifecycle Tailoring

For the lane assistance project functional safety initial plan, following lifecycle phases in scope:

1. Concept phase
2. Product Development at the System Level
3. Product Development at the Software Level

The following phases are out of scope:

1. Product Development at the Hardware Level
2. 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

The development interface agreement (DIA) is a document that defines the roles, responsibilities and work output evidence among companies (for example, OEM, Tier-I supplier, Tier-II supplier, etc.) involved in developing a product which typically is a safety-related product. The ultimate goal is to ensure that all parties are developing safe vehicles in compliance with ISO 26262.

The DIA also covers the charter and appointment of OEM and supplier safety managers and defines the following aspects. In the document, the customer (OEM) and supplier jointly tailor the safety lifecycle. The document also clearly defines the activities and processes that must be

performed by the customer and the supplier. It also define the interface, data exchange and communications aspects as well as the RASIC for design, production and quality assessment activities. The DIA also includes any supporting processes or tools to ensure compatibility between customer and supplier technologies.

The following roles and responsibilities are defined for the lane assistance item functional safety project.

Role	**Responsibility**	**Remark**
Customer (OEM) Project Manager	• Overall project management • Acquires and allocates resources needed for the functional safety activities • Appoints safety manager or might act as one	• Appointed at the supplier (Tier-I).
Supplier (Tier-I) Project Manager	• Subsystem & component level resources allocation for functional safety activities • Joint project management with customer project manager	• Appointed at the customer (OEM)
Customer (OEM) Safety Manager	• Planning, coordinating, tailoring and documenting the development phase of the safety lifecycle • Monitors progress against the safety plan	• Pre-audits, plans the development
Supplier (Tier-I) Safety Manager	• Joint tailoring of the safety lifecycle with customer (OEM) safety manager	• Appointment by supplier (Tier-I).
Supplier (Tier-I) Safety Engineer	• Product development and integration • Testing at the hardware, software and system levels	• Responsible for final integration in vehicle
Test Manager	• Plan and oversee testing activities • Coordinates testing to show that the vehicle system works correctly	• Appointment by supplier (Tier-I).
Safety Auditor	• Ensure project conforms to the safety plan and safety lifecycle. • Ensures design and production implementation conform to the safety plan and ISO 26262.	• Appointed at the customer (OEM) • Independent from the project team
Safety Assessor	• Perform functional safety assessment • Judge if functional safety is being achieved	• Appointed at the customer (OEM)

Confirmation Measures

The confirmation measures process is executed by individuals or teams that are independent of the systems engineering and design teams. The confirmation measures process serves two main purposes:

- ✓ Functional safety project conforms to ISO 26262 standard
- ✓ Ensure that the functional safety project indeed does make the vehicle safer.

The **confirmation review** ensures that the project complies with ISO 26262. As the product is designed and developed, an independent person would review the work to make sure ISO 26262 is being followed. The **functional safety audit** ensures that actual implementation of the project conforms to the safety plan is called a functional safety audit. The **functional safety assessment** ensures 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.