Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [0.1]

Document history

Date	Version	Editor	Description
24.8.2017	0.1	Aneeq Mahmood	Safety plan for lane assistance

Table of Contents

Introduction

Purpose of the Safety Plan

[Instructions: Answer what is the purpose of a safety plan?]

The purpose of a safety plan document is to provide an overview on how one is going to achieve a safe system (item). There are several topics which comprise a safety plan such as which item is being analyzed for safety, which safety management roles are available and involved, interface agreements between stake holders, and confirmation measures to establish that safety has been accounted for in the manner described 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

[Instructions: Nothing to do here. This is for your information.]

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

[Instructions: Discuss these key points about the system:
What is the item in question, and what does the item do?
The item in question in this work is the lane assistance system in the car. The main ole of the item is to ensure that the car does not veer away from the lane boundary unintentionally. This can , for example, happen when the driver's grip on the steering is loosening or has lessened. This item is highlighted in the following figure

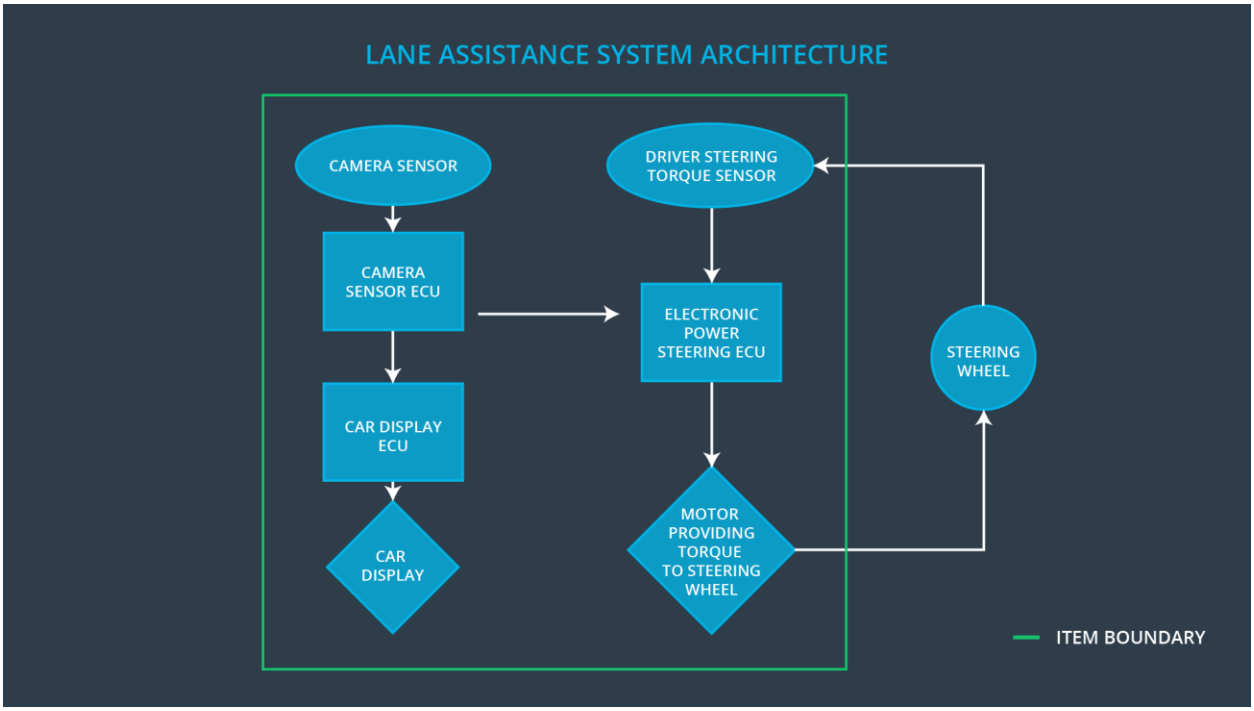

Figure 1: The lane assistance item being analyzed for safety planning for this project

What are its two main functions? How do they work?
To do so, two main functions need to be carried out

(i) Lane departure warning (LDW): A warning to highlight that car is going out of line, for example via sending vibrations to the car steering.
(ii) Lane keeping assistance (LKA): A method to check if the car is within the lane and an automated response to bring the car back within the lane marking, and to the center of the lane.

Which subsystems are responsible for each function?
The main subsystems involve in performing the above-mentioned two functions are

(i) Camera sensing
(ii) Car display unit

(iii) Electronic power steering (EPS) support

For LDW, the camera sensor electronic control unit (ECU) is responsible for finding lane lines, can send the warning to EPS ECU, and to the car display ECU. The display ECU can blink an LED light to indicate that car is veering away and EPS ECU can provide extra torque in addition to the torque provided by the driver to introduce a haptic feedback to the driver, or induce low frequency vibrations in the steering wheel.

For LKA, camera ECU can highlight if LKA support is available or not. Moreover, the EPS ECU can provide the torque to rotate the steering if the car is going out of lane.

What are the boundaries of the item? What subsystems are inside the item? What elements or subsystems are outside of the item?

The main individual subsystems inside the item are highlighted in the figure below, and have already been mentioned above.
Other subsystems such as steering ECU, braking, head lights control, automated parking, blind spot protection etc., are not part of this item.

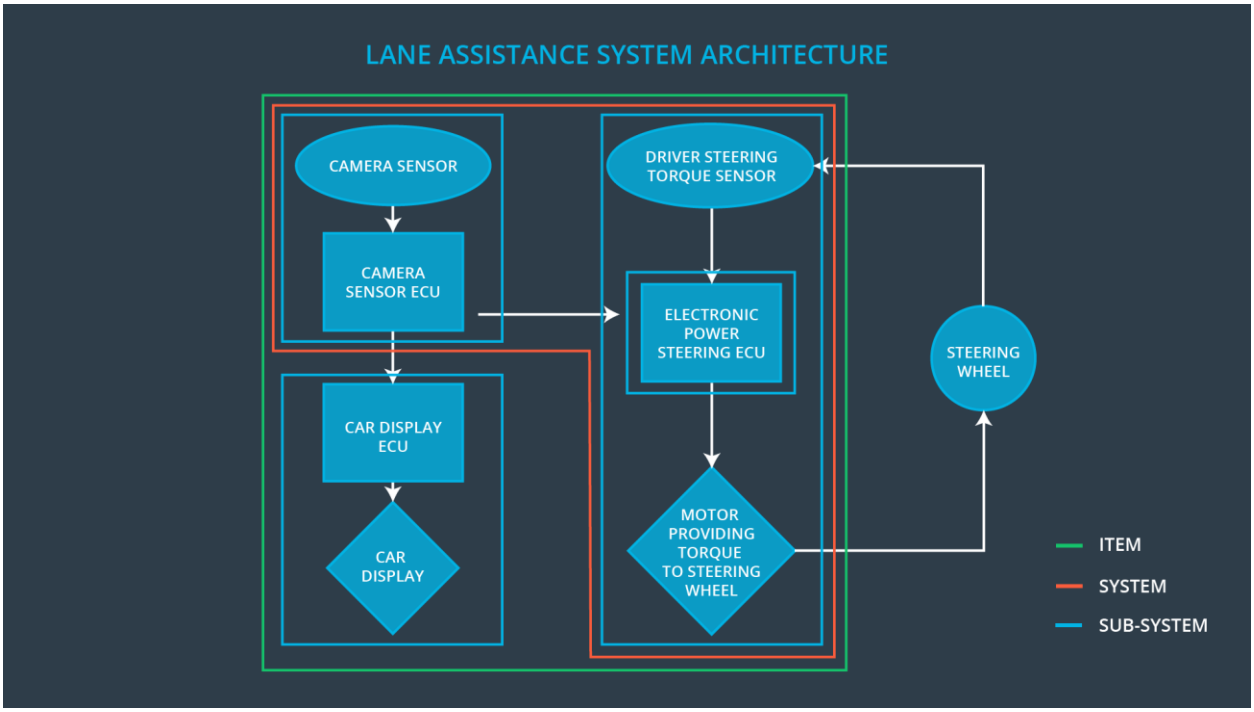

Figure 2: Different subsystem within the lane assistance system

Goals and Measures

Goals

[Describe the major goal of this project]

The goal of this project is to design the lane assistance system in an industry-compliant manner. This is achieved by analyzing the functional safety of the proposed system which will give rise to requirements for system architecture and in hardware and software modules, which must be met to minimize the risk associated with this system to an acceptable level, and increase the overall safety of the vehicle.

Measures

[Instructions:
Fill in who will be responsible for each measure or activity. Hint: The lesson on Safety Management Roles and Responsibilities.

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 Assessor	Once every 2 months
Perform functional safety pre-assessment prior to audit by external functional safety assessor	Safety Auditor	3 months prior to main assessment

Perform functional safety assessment	Safety Assessor	Conclusion of functional safety activities

Safety Culture

[Describe the characteristics of your company's safety culture. How do these characteristics help maintain your safety culture]

The main characteristic of any good safety culture should be that safety should be given the highest priority, and should not be compromised upon especially under time and cost constraints. To ensure this, persons should be held accountable for their design decisions, and good decisions should be rewarded. Safety assessments should always be done by people from outside the team which have worked on a process. Moreover, safety processes should be standardized and well defined to ensure consistency through design, task assignments, and operations.

These characteristics for a safety culture allow industry/company-wide safety policy which should be followed with complete transparency and accountability. This ensures that people are accustomed to their roles in the safety cycle; they follow best design practices and avoid shortcuts: and they become aware of sustaining a good safety culture on individual basis.

Safety Lifecycle Tailoring

[Instructions:
Describe which phases of the safety lifecycle are in scope and which are out of scope for this particular project.]

As already mentioned in the Introduction section, to accommodate safety for lane assistance system, changes need to be made in the concept phase. Afterwards, in the product development phase, at the system and software design level, changes are required in the safety lifecycle. In general, lifecycle tailoring is required on the left hand side of V-development diagrams, and are not required during product development at hardware level or during the production and operation phase.

The following diagram shows the system design diagram, where the blocks requiring safety lifecycle tailoring are surrounded by a red box.

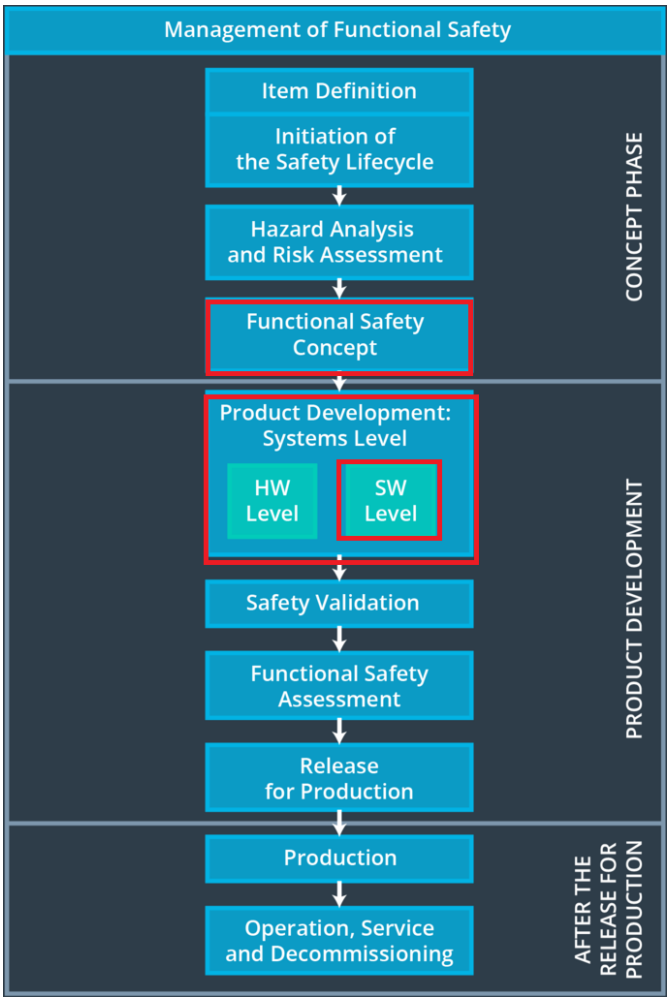

Figure 3:Blocks requiring tailoring within safety lifecycle

Roles

[Instructions:
This section is here for your reference. You do not need to do anything here. It is provided to help with filling out the development interface agreement section.
]

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)

[Instructions:
Assume in this project that you work for the tier-1 organization as described in the above roles table. You are taking on the role of both the functional safety manager and functional safety engineer.

Please answer the following questions:

1. **What is the purpose of a development interface agreement?**
   The DIA takes place between two companies whereas one company (e.g. OEM) obtains services from other company (e.g., Tier 1 company). For safety planning, the DIA clarifies the roles and responsibilities of the two parties involved in the functional safety project, outlines which products and services will be exchanged at the end of the project, and identifies who will be responsible for safety issues in post-production phase. Such agreements streamlines communication between stakeholders and avoids disputes and conflicts in future.

2. **What will be the responsibilities of your company versus the responsibilities of the OEM?**
   As a Tier 1 company, my company will be responsible for providing the development and production services for the products which is being required by the OEM. The OEM will provide the set of requirements which are sought from the product, and the Tier 1 Company will ensure that the end-product fulfills the requirements. As part of this exchange, there will be appointment of safety manager from the OEM, and he and I will be responsible for tailoring the safety lifecycle to accommodate support for lane assistance system. We will further assign people responsible for individual stages of the product design and developments, and will also exchange process and tools (such as software frameworks and libraries) to ensure seamless operation in order to achieve the safety and end-project goals.

Confirmation Measures

[Please answer the following questions:

1. **What is the main purpose of confirmation measures?**
   As mentioned in the lecture note, confirmation measures makes sure that functional safety protocols in a project conform with ISO 26262, and that the project really does make the vehicle safer. It is carried out by people which are foreign to the product design and development team.

2. **What is a confirmation review?**
   A confirmation review is a review to ascertain conformity of safety project with ISO 26262. This is done during design and development phase to ensure that the standard is being correctly followed.

3. **What is a functional safety audit?**
   This audit ensures that the safety project is being implemented according to the safety plans devised by the safety manager.
4. **What is a functional safety assessment?**
   This assessment is carried out at the conclusion of functional safety activities and determines whether the overall safety after planning, designing and developing products has increased or not.

]

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.