Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.0
Released on 2017-11-09

Document history

Date	Version	Editor	Description
November 9, 2017	1.0	Sampayo, Sebastián L.	First submission

Table of Contents

Introduction

Purpose of the Safety Plan

[What is the purpose of a safety plan?]
The purpose of the Safety Plan is to provide an overall framework for the Lane Assistance. It defines the guidelines to ensure Safety Culture, Roles and Responsabilities assignment in the project so that this item is reasonably safe for the user.

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

[What is the item in question, and what does the item do?]

The Lane Assistance item alerts the driver that the vehicle has accidentally departed and attempts to steer the vehicle back towards the center of the lane.

[What are its two main functions? How do they work?]

The Lane Assistance system will have to functions:
1. Lane Departure Warning
2. Lane Keeping Assistance

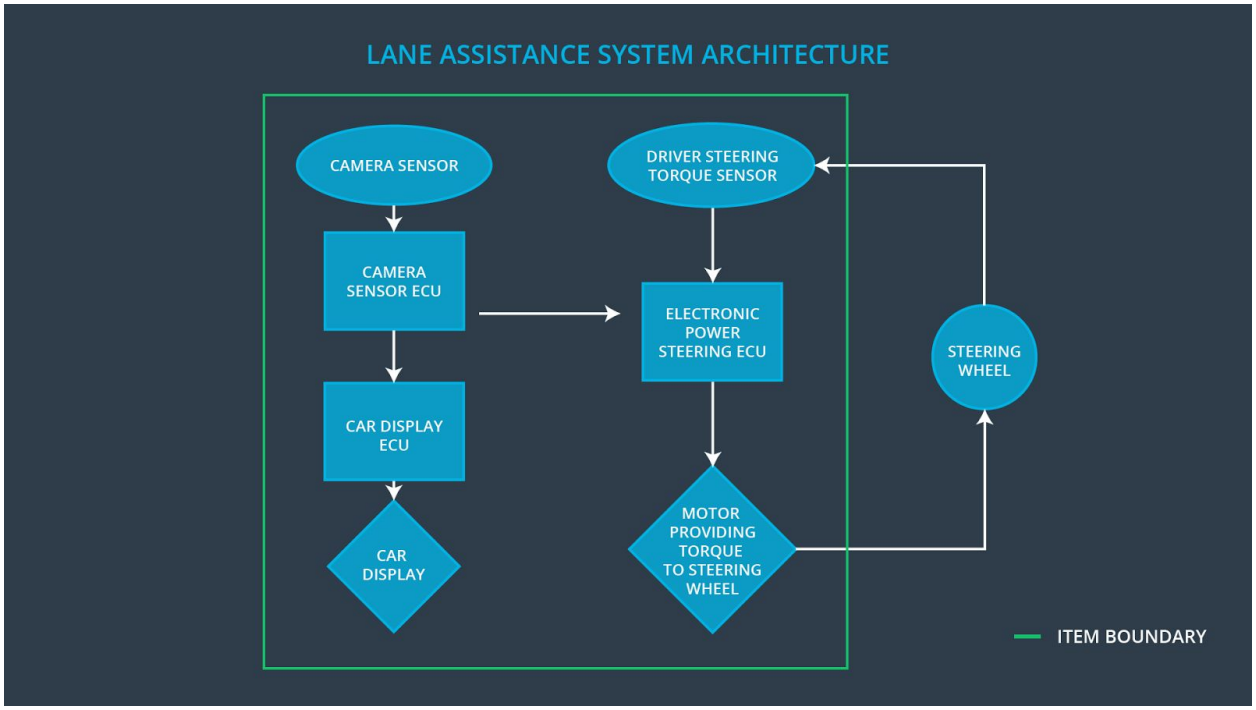
The lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback.

The lane keeping assistance shall apply the steering torque when active in order to stay in ego lane.

[Which subsystems are responsible for each function?]

Three subsystems will be included and are responsible for all of the functions:
- Camera system
- Electric power steering system
- Car display systems

[What are the boundaries of the item? What subsystems are inside the item? What elements or subsystems are outside of the item?]
The boundaries of the item are shown in the following diagram:



Goals and Measures

Goals

[Describe the major goal of this project; what are we trying to accomplish by analyzing the lane assistance functions with ISO 26262?]

The goal of this Safety Plan are:

- Identify risk hazardous situations in a lane assistance electronic or electric system malfunction that may cause physical injury or damage to a person's health.
- Minimize the risk to reasonable 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 Assesor	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.]

These are the characteristics of our company's culture:

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 are independent from the teams who audit the work

Well defined processes: company design and management processes are 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

Safety Lifecycle Tailoring

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

For the lane assistance project, the following safety lifecycle phases are in scope, in accordance with the ISO 26262 standard:

- 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

[What is the purpose of a development interface agreement?]

A Development Interface Agreement (DIA) is an agreement between the companies involved in developing a product and defines the roles and responsibilities for each one. All involved parties need to agree on the contents of the DIA before the project begins. The final objective of this document is to comply with the requirements specified in ISO 26262.

[What will be the responsibilities of your company versus the responsibilities of the OEM?]

In this project these organizations will have the following responsibilities:

- **OEM (customer)**: Provide the requirements and initial documentation regarding the design of the product. Implementation at the item level of the lane assistance system.

.

- **Tier-1 (supplier, our company)**:
    - Provide the Safety Plan
    - Provide the Hazard Analysis and Risk Assessment
    - Provide the Functional Safety Concept
    - Provide the Technical Safety Concept
    - Provide the Software Safety Requirements and Architecture
    - The safety manager will perform the pre-assessment of the plans, prior to audit by external functional safety assessor.
    - Development and production of the sub-systems for the OEM.

- **Auditor/Assessor (external)**: This will be the external auditor that will perform an independent assessment of the plans and work products.

Confirmation Measures

[What is the main purpose of confirmation measures?]

The Confirmation Measures serve two purposes:

- The Lane Assistance safety project conforms to ISO 26262 tailored.
- The Lane Assistance safety project does make the vehicle safer.

[What is a confirmation review?]

A **confirmation review** ensures that the project complies with ISO 26262. It is extremely important that the people who carry out confirmation measures be independent from the people who actually developed the project. This is addressed in the roles and responsibilities depicted in the previous sections.

[What is a functional safety audit?]

A **functional safety audit** evaluates the implementation of the project against the safety plan to make sure they agree.

[What is a functional safety assessment?]

A **functional safety assessment** is the confirmation 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.