Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
12-25-2018	1.0	Eduardo Paz	Initial release

Table of Contents

Introduction

Purpose of the Safety Plan

The safety plan will provide an overall framework for the Lane Assistance item and will define the roles, the steps and the measures to be taken in order to achieve functional safety for this item in compliance with ISO26262.

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

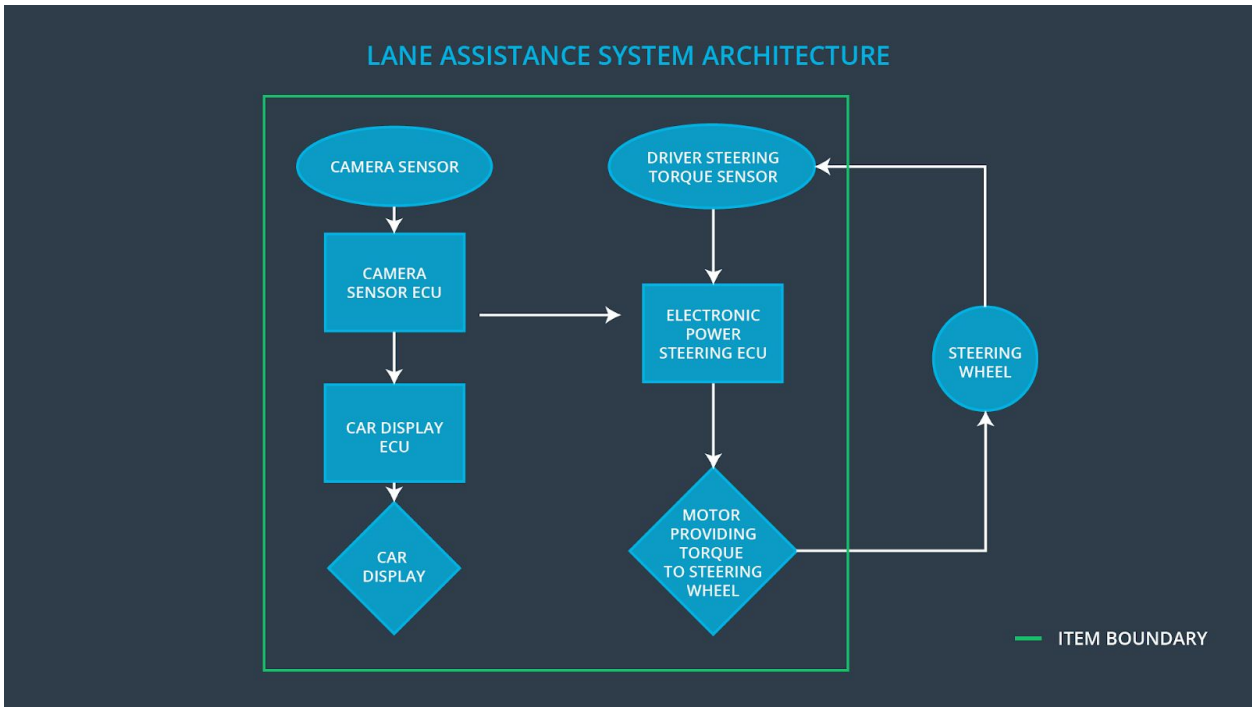
The Lane Assistance Item alerts the driver that the vehicle has accidentally departed its lane, and attempts to steer the vehicle back toward the center of the lane.

The Lane Assistance Item will have two functions:

- Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback.
- Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane.

There are three subsystems responsible for these functions:

- Camera subsystem.
- Electronic power steering subsystem.
- Car display subsystem.



Goals and Measures

Goals

The main goal in functional safety is to reduce risk to acceptable levels. This documents discuss what elements were added to the system in order to make it safe, and provide testing evidence that shows the system functioning properly.

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 Manager	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

- **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.
- **Independence**: teams who design and develop a product should be independent from the teams who audit the work.
- **Diversity**: intellectual diversity is sought after, values and integrated into processes.

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 project begins.

Our company will be responsible of analyzing and modifying the various subsystems in order to reduce risks to acceptable levels in compliance with ISO 26262.

Confirmation Measures

Confirmation measures serve two purposes:

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

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.

Functional safety audit:

Checking to make sure that the actual implementation of the project conforms to the safety plan is called a functional safety audit.

Functional safety assessment:

Confirming that plans, designs and developed products actually achieve functional safety is called a functional safety assessment.

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.