Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.0
Released on 2018-05-16

Document history

Date	Version	Editor	Description
2018-05-16	1.0		Safety Plan for lane assistance system

Table of Contents

Introduction

Purpose of the Safety Plan

The purpose of this document is to define a framework for safety plan for lane assistance system. The document also includes details about roles and responsibility for the lane assistance's functional safety.

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 main functions of Lane Assistance system are as below:

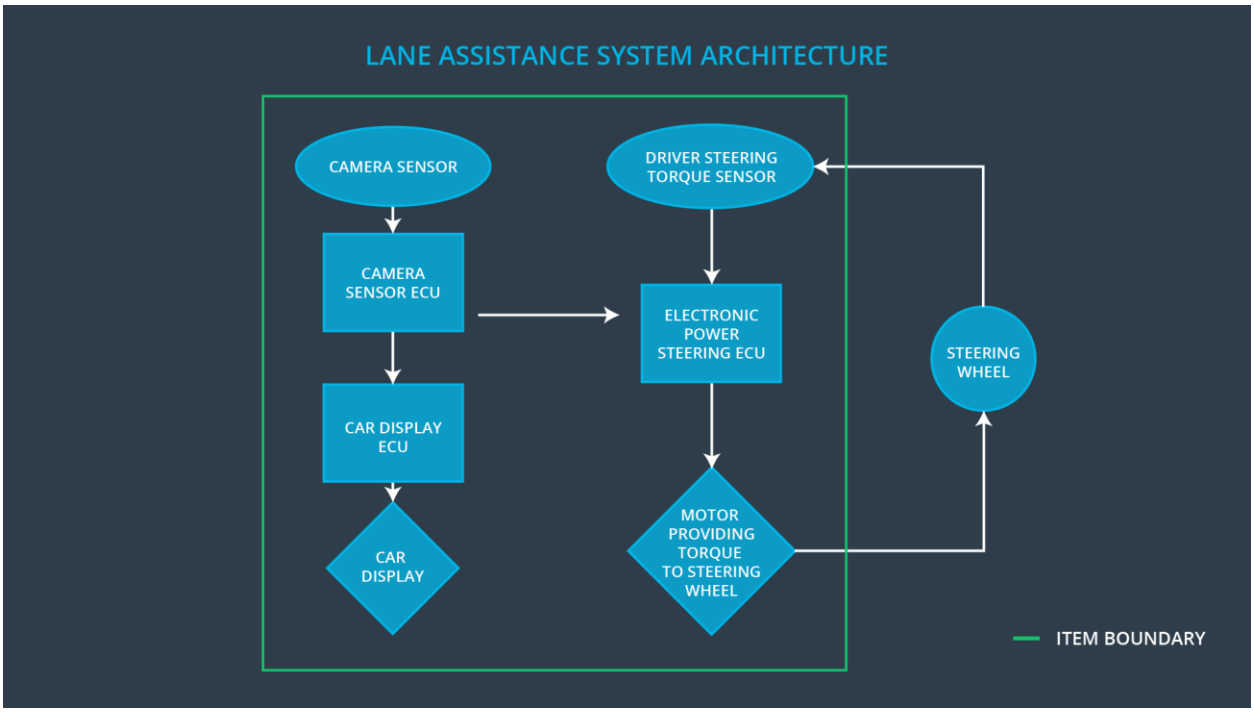
1) Lane keeping assistance function: When car drifts off the lane, this system turns steering wheel towards the center of lane to keep car in lane.
2) Lane departure warning function: When car drifts off the lane, steering wheel vibrates to warn the driver.

Subsystems used to implement lane assistance are as below:

1) Camera subsystem:
    a. Camera Sensor
    b. Camera Sensor ECU
2) Power Steering subsystem:

a. Electronic Power steering ECU
b. Driver steering torque sensor
c. Motor providing torque to steering wheel.

3) Display subsystem:
   a. Car display
   b. Car display ECU



When car starts drifting towards side of lane, camera sensor senses that and sends a signal to car display system and steering wheel torque provider system. Car display system will display warning on car dashboard and steering wheel torque provider system will vibrate steering wheel and will turn steering wheel towards the center of the lane. When driver turns on the lane change indicator or switches off the lane assistance system, the system will stop applying torque on steering wheel and displaying warning on car dashboard.

The Lane Assistance system does not support functionalities listed below:

1) Collision detection and collision avoidance
2) Pedestrian detection

Goals and Measures

Goals

1) Identify potential risks associated with malfunctioning of lane assistance system.

2) Measure severity of risk.
3) Lower the risk up to the current Standard of society.

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

Safety culture should have following characteristics:

1) **High priority:** safety has the highest priority among competing constraints like cost and productivity.
2) **Accountability:** processes ensure accountability such that design decisions are traceable back to the people and teams who made the decisions.
3) **Rewards:** the organization motivates and supports the achievement of functional safety.
4) **Penalties:** the organization penalizes shortcuts that jeopardize safety or quality.

5) **Independence:** teams who design and develop a product should be independent from the teams who audit the work.
6) **Well defined processes:** company design and management processes should be clearly defined.
7) **Resources:** projects have necessary resources including people with appropriate skills.
8) **Diversity:** intellectual diversity is sought after, valued and integrated into processes.
9) **Communication:** communication channels encourage disclosure of problems.

Safety Lifecycle Tailoring

Safety lifecycle phases are as below:

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

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. The DIA also specifies what evidence and work products each party will provide to prove that work was done according to the agreement. The ultimate goal is to ensure that all parties are developing safe vehicles in compliance with ISO 26262.

Responsibilities of OEM: To provide functioning Lane Assistance system.

Responsibilities of Tier 1: To verify lane assistance system as well as various subsystems adhere to ISO 26262 standards.

Confirmation Measures

Purposes of Confirmation Measures are as listed below:

1) project conforms to ISO 26262
2) project really does make the vehicle safer.

Confirmation Review is process to ensure that the project complies with ISO 26262.

Functional Safety Audit is to check that the actual implementation of the project conforms to the safety plan.

Functional safety assessment is process of confirming that 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.