Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 0.1

Document history

Date	Version	Editor	Description
3/24/2019	1.0	Jian Li	Initial version

Table of Contents

Introduction

Purpose of the Safety Plan

The purpose of this safety plan is to provide an overall framework for the Lane Assistant item, assign roles and responsibilities for functional safety of this item. As the project passes through the design, implementation and production phases, the output will be checked against the safety plan.

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

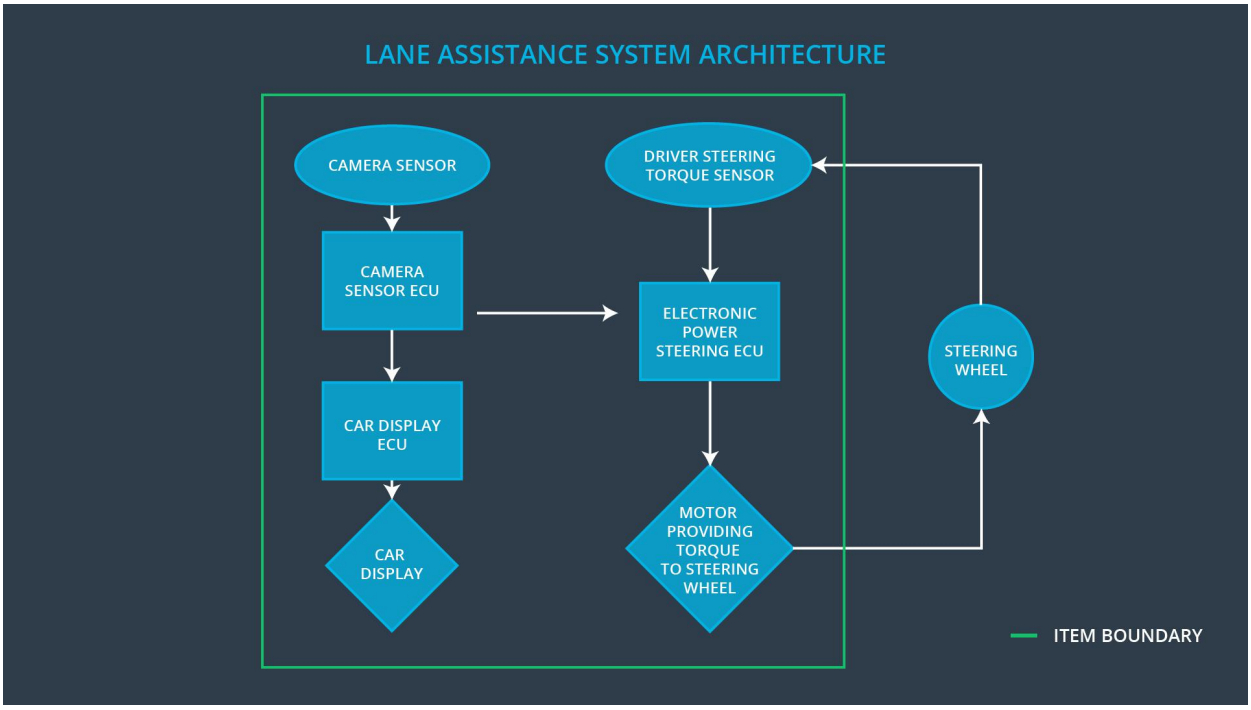
The item in question is Lane Assistance. Lane Assistance item alerts the driver that the vehicle has accidentally departed its lane, and attempts to steer the vehicle back toward to the center of the lane.

The Lane Assistance System will have two functions:

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

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

Three sub-systems: Camera system, Electronic Power Steering system, Car Display system are responsible for each function.



Goals and Measures

Goals

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	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 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

The following characteristics will help to maintain the 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
- **Penalties**: the organization penalizes shortcuts that jeopardize safety or quality
- **Independence**: teams who design and develop a product should be independent from the teams who audit the work
- **Well defined processes**: company design and management processes should be 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

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

The development interface agreement defines the roles and responsibilities between companies involved in developing a lane assistance to ensure that all parties are developing safe vehicles in compliance with ISO 26262.

- Project Manager:
  - Acquires and allocates resources needed for the functional safety activities
  - Appoints safety manager or might act as safety manager

- Safety Manager
  - Planning, coordinating and documenting of the development phase of the safety lifecycle
  - Tailors the safety lifecycle
  - Maintains the safety plan
  - Monitors progress against the safety plan
  - Performs pre-audits before the safety auditor

- Safety Engineer
  -Product development and Integration
  - Testing at the hardware, software and system levels

- Safety Auditor
  Ensures that the design and production implementation conform to the safety plan and ISO 26262.

- Safety Assessor
  Independent judgment as to whether functional safety is being achieved via a functional safety assessment

- Test Manager
  Plans testing activities
  Coordinates testing to show that the vehicle system works correctly

Confirmation Measures

Confirmation measures serve two purposes:
- that a functional safety project conforms to ISO 26262, and
- that the project really does make the vehicle safer.

Confirmation review ensures that the project complies with and followed ISO 26262 as the product is designed and developed.

Functional safety audit will check to make sure that the actual implementation of the project conforms to the safety plan.

Functional safety assessment will confirm 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.