Safety Plan Lane Assistance

Document history

Date	Version	Editor	Description
05/25/2018	1.0	Shaurya Dwivedi	Initial attempt

Table of Contents

Introduction

Purpose of the Safety Plan

This document describes the framework of item in Lane Assistance. It consists of the roles and responsibilities for the functional safety of an item.

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 described here is the Lane Assistance System's brief version.

The two main function of this item are:
- **Lane departure warning**: Whenever there's a case when the car is about to go out of the lane, the steering wheel vibrates to warn the driver. The vibration is produced by moving steering wheel back and forth.

- **Lane keeping assistance**: Whenever there's a chance that vehicle is going out of the track, this functionality will keep the vehicle on the track by steering it towards the center of the road. This is done by applying steering torque.

The subsystems required to implement functional safety are as follows:
- **Camera Sub Systems** which consists of:
    - Camera sensor.
    - Camera sensor electronic control unit.
- **Electronic Power Steering Sub Systems** which consists of:
    - Sensors to measure torque for driver steering.
    - Electronic Power Steering electronic control unit.
    - Motor Proving Torque to Steering Wheel.
- **Car Display Sub Systems** which consists of: components:
    - Car Display electronic control unit.
    - Car Display.

The interaction between different systems is shown in diagram below:

LANE ASSISTANCE SYSTEM ARCHITECTURE
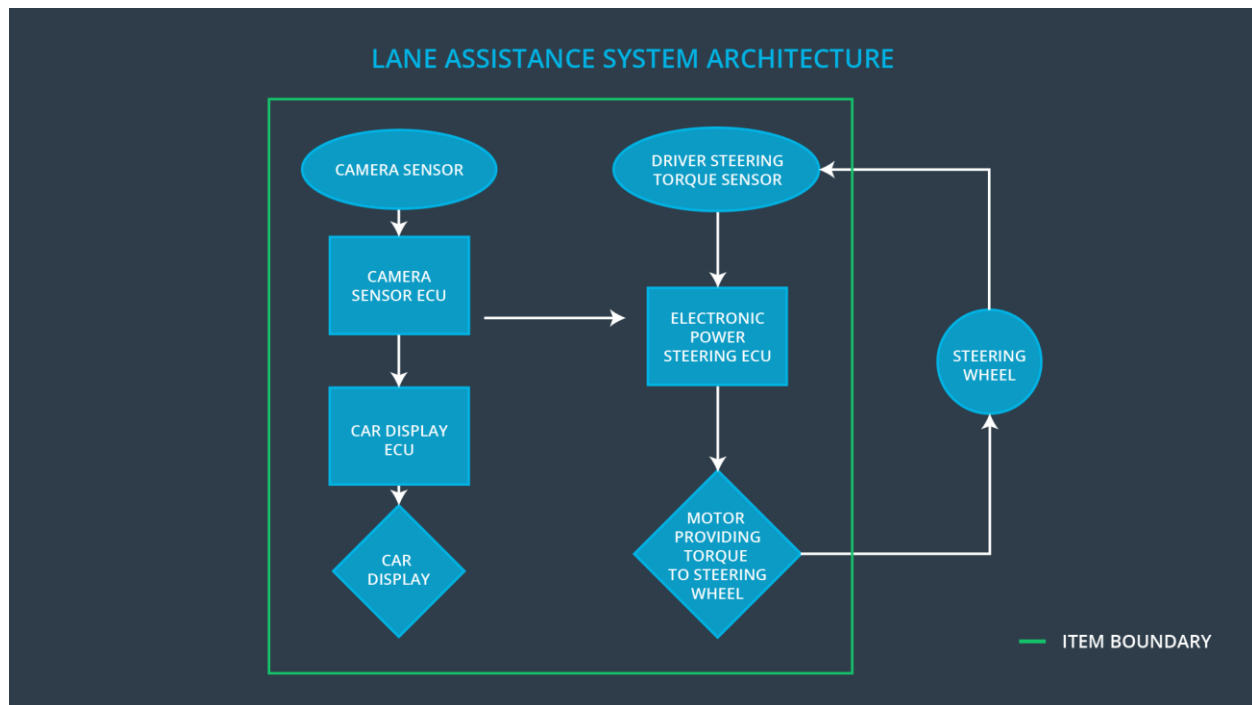
Whenever the camera senses that vehicle might go off track it sends signal to electronic power steering system which in turn vibrates the steering and steers the vehicle to the center of the road and will also request to turn warning light on in the display of car at dashboard.

That's how driver realizes that the assistance system is active.

If the driver wants to turn he/she switch on the turn signal which deactivates the assistant so that vehicle can change lane. It can also be turned off manually with a button on the dashboard.

The driver is still expected to have both hands on the steering wheel at all times. The electronic power steering subsystem has a sensor to detect how much the driver is already turning. The lane keeping assistance function will merely add the extra torque required to get the car back towards center. The extra torque is applied directly to the steering wheel via a motor.

The Lane Assistance System does not include subsystems like:
- Adaptive Cruise Control
- Automatic Parking

Goals and Measures

Goals

The aim of this project is to analyze the components of the Lane Assistance system, to identify and assess the risks and hazards, and finally to apply system engineering to reduce the risk to a reasonable level.

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

Safety is a top priority for every business. To ensure the safety culture, the following features must be taken into account:
• High Priority: Despite the importance of cost and productivity for successful organization, safety is a top priority.
• Accountability: Decisions are attributable to the individuals and teams who made the decisions to ensure accountability.
• Rewards: Organizations support and motivate functional safety by rewarding when functional safety is maintained on a daily basis.
• Penalties: If the basic requirements for functional safety are not met and neglected, the organization imposes penalties.
• Independence: auditing team and design team should be independent. i.e. Teams designing and developing a product should be independent of the teams testing the work
• Well-defined processes: The company should clearly define its design and management process.
• Resources: A functional safety project should have all necessary resources together with the people with the appropriate skills.
• Communication: Communication between the team should include full disclosure of issues.

Safety Lifecycle Tailoring

The following phases of the safety lifecycle are planned for the Lane Assistance project:

- Design phase
- Product development at the system level
- Product development on the software level

The following phases are not valid:

- 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 purpose of a Development Interface Agreement (DIA) is to delineate the roles and responsibilities between OEM and Tier-1 involved in the development of this product to ensure its development in accordance with ISO 26262.

- The responsibility of the OEM is to make the request to a lane keeping system, and our corporate responsibility will be to design and produce the system for the OEM and to analyze and modify the various systems from a functional safety point of view

Confirmation Measures

The purpose of the confirmation measures are:

- Make sure that the Lane Assistance project complies with ISO 26262.
- Make sure the Lane Assistance project makes the vehicle really safer.

The confirmation test ensures that the projects comply with ISO 26262. If the product is designed and developed, an independent person would review the work to make sure it

complies with ISO 26262. A functional safety audit ensures that the actual implementation of the project complies with the safety plan. A functional safety assessment confirms that the plan, design, and product being developed 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.