Elektrobit

UDACITY

# Safety Plan Lane Assistance

**Document Version:** [Version]

**Template Version 1.0, Released on 2017-06-21**

# Document history

| Date | Version | Editor | Description |
|---|---|---|---|
| 03/11/2017 | 1.0 | S. Chonavel | Initial version |
| | | | |
| | | | |
| | | | |
| | | | |

# Table of Contents

# Introduction

## Purpose of the Safety Plan

This document target is to provide an overall framework for lane Assistance function and to assign roles and responsibility for this item as defined by ISO26262 standard.

## 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 System alerts the driver that the vehicle is leaving its lane and try to steer the vehicle back toward the lane center.

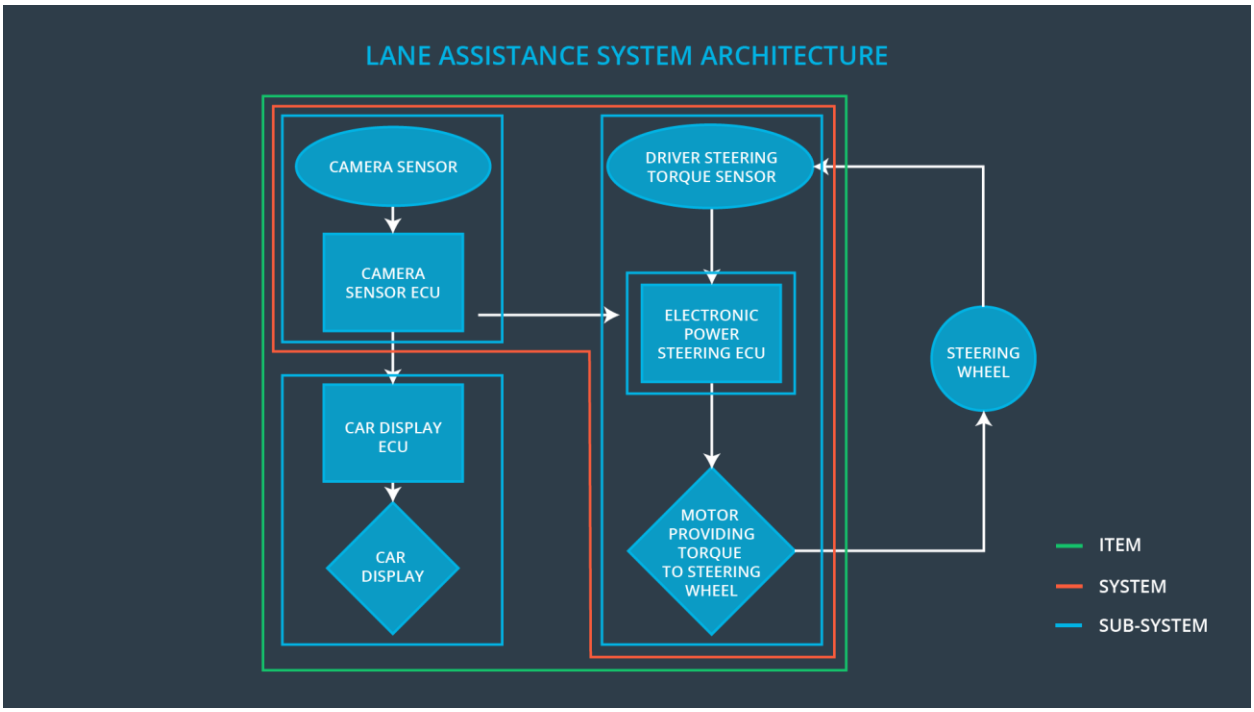
When the vehicle drifts towards the edge of the lane, two things will happen:

- The lane departure warning function will warn the driver of the drift by generating an oscillating torque in the steering wheel.
- The lane keeping assistance function will move the steering wheel so that the wheels turn towards the center of the lane.

The item boundary is composed of three sub-systems:

- Camera sub- system which responsible for detecting lane lines and determining when the vehicle leaves the lane.
- Electronic Power Steering sub- system responsible for measuring the torque provided by the driver and then adding appropriate amount of torque base on a lane assistance system torque request.
- Car Display system which is responsible to display to the driver information when the camera system request it

As described in the following block diagram.




The logic can be described as follow:

- If the camera system detects the lines
  - If the camera system detects that the vehicle is departing from its lane
    - If the driver does not use a turn signal,
      - An action request is transmitted to the electronic power sub system
        - The electronic power sub system generates a steering wheel vibration to warn the driver of the situation.
        - The electronic power sub system adds extra steering torque to help the driver move back towards the center of the lane.
      - An action request is transmitted to the display system

        - The display system light up a “line departure warning sign” on the vehicle dashboard.
    - If the driver does use a turn signal
        - The LDA is not active
        - No request is transmitted to the Display system
        - No request is transmitted to the Electronic power sub-system
- If the camera system do not detect any line departure
    - No action request is sent

- If the camera system cannot detect the lines therefore the lanes due to external conditions such as :
    - Bad visibility, meteorological conditions such as snow, heavy rain or fog
    - Camera optics being obstructed
    - Absence or unrecognizable lines on the road
- Then no request is transmitted to the Electronic power sub system
- An action request is transmitted to the display system
    - The display system light up a “LDA non active sign” on the dashboard.

The system shall be configure to comply with local regulation, for example

-The minimal speed of operation

- The maximum speed of operation
- The potential restriction for a DLA system such as to motorway or non-urban

Note: The steering wheel is outside the item considered.

Note: The line driving Assistance item do not include other ADAS functions such as:

- Adaptive cruise control
- Adaptive light control
- Automatic breaking
- Automatic parking
- Blind spot detection
- Collision avoidance system
- Driver drowsiness detection
- GPS navigation
- Hill descent control
- Intelligent speed adaptation
- Night vision
- Tyre pressure monitoring

# Goals and Measures

## Goals

**The goal of this project safety plan is to:**

- **To identify the possible item malfunction which will lead to hazardous situations**
- **To quantify the risk associated to those malfunctions**
- **To reduce the risk associated to those malfunctions to an acceptable level via system engineering.**

## 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

The safety culture of our company is characterized by:

- **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

In compliance with ISO26262, the roles and responsibilities between companies involved in developing the LDA are as follow:

OEM Safety Manager- Item Level:

- Pre-audit Item Level
- Plan the Item development phase
- Develop the Item Safety plan

OEM Safety Engineer- Item level:

- Execute the activities of the Item Safety plan
- Develop prototypes
- Integrates sub systems into Item Level

OEM Project Manager-item level:

- Allocate Item level resources

Tier1 Safety Manager- Component Level

- Pre-audit component level
- Plan the development phase
- Develop the Component safety plan

Tier1 Safety Engineer- Component Level

- Execute the activities of the component safety plan
- Develop prototypes
- Integrates sub systems into components Level

Tier 1 Project Manager- Component Level

- Allocate Component level resources
- Coordinate development activities with OEM project Manager

Safety Auditor:

- Makes sure that the project conforms to the safety plan

Safety Assessor:

- Judges if the project has increased safety

All OEM and Tier1 :

- Sustain safety culture

# Confirmation Measures

Confirmation measures help ensure that a functional safety project improves safety, conforms to the safety plan, and follows the ISO 26262 standard.

The following steps will be implemented:

***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