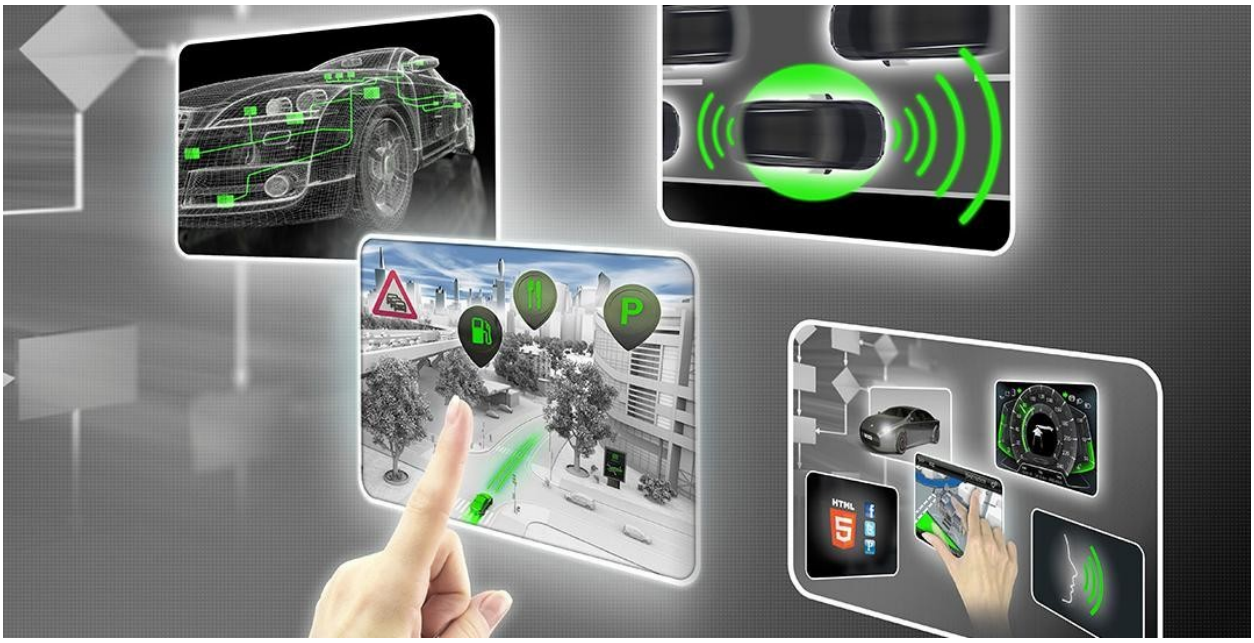
Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 2.0



Document history

Date	Version	Editor	Description
July 24, 2017	1.0	John Chen	Initial Draft
July 28, 2017	2.0	John Chen	Edit after feedback from Andrew Paster.

Table of Contents

1 Introduction

1.1 Purpose of the Safety Plan

The purpose of the plan is to provide an overall framework for the lane assistance functional safety project as pertain to the potential malfunctions of the electrical and electronic systems as defined by **ISO 26262** standard, tailored.

1.2 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

1.3 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

2 Item Definition

The Lane Assistance Item is a simplified version of an Advanced Driver Assistance System (ADAS) that warns the driver of unintended steering drifts and assists the driver in steering back to the center of the lane. The item will have two functions:

1. Lane departure warning
2. Lane keeping assistance

When the driver drifts towards the edge of the lane when this item is engaged, two things will happen:

1. The **lane departure warning function** shall apply an oscillating steering torque to provide the driver a haptic feedback (vibration).
2. The **lane keeping assistance function** shall apply the steering torque when active in order to stay in ego (current active) lane.

The item boundary include three sub-systems as shown in *Figure 1*:

- Camera system
- Electronic Power Steering system
- Car Display system

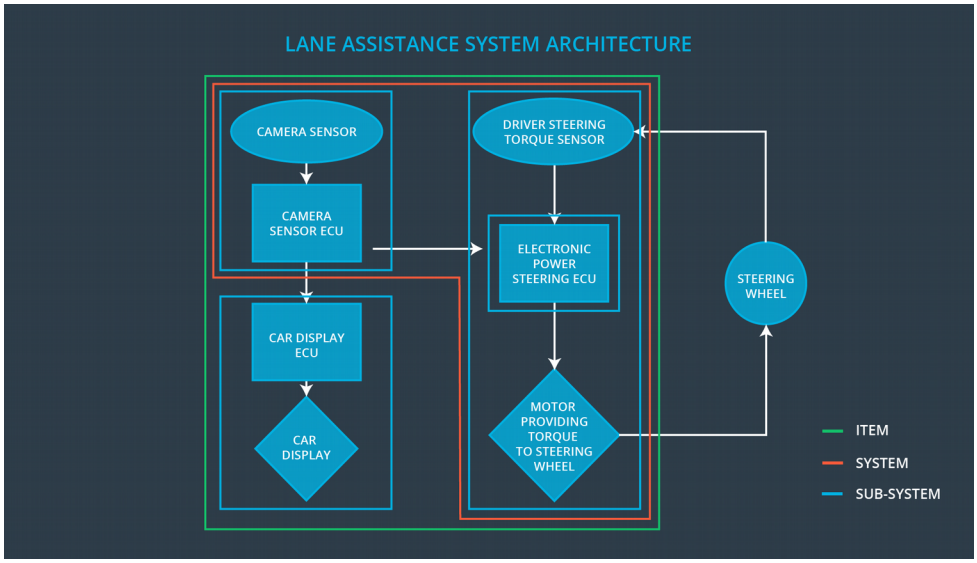


Figure 1: Lane Assistance System Architecture

When the camera senses that the vehicle is leaving the lane, the camera sends a signal to the electronic power steering system asking to turn and vibrate the steering wheel. The camera sensor will also request that a warning light turn on in the car display dashboard. That way the driver knows that the lane assistance system is active. When the driver uses a turn signal, then the lane assistance system deactivates so that the vehicle can leave the lane. The driver can also turn off the system completely 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. As shown in *Figure 1*, the Lane Assistance Item does not include the following systems normally found in a fully implemented ADAS system:

- Adaptive Cruise Control
- Automatic Parking
- Blind Spot Monitoring
- Tire Pressure Monitoring
- Pedestrian Protection

3 Goals and Measures

3.1 Goals

The goals of the Lane Assistance Functional Safety Plan for the project are:

- Identify risk hazardous situations in a lane assistance electronic or electric system malfunction that may cause physical injury or damage to a person's health.
- Evaluate the risk level of the hazardous situation
- Via systems engineering, lowering high risk level situations to reasonable levels to prevent accidents from occurring.

3.2 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

4 Safety Culture

We believe and will behave in the following manner to achieve the highest safety record in the industry:

- **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

5 Safety Lifecycle Tailoring

For the lane assistance project functional safety initial plan, the ISO 26262 standard have been tailored to include the following safety lifecycle phases 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

We welcome our selected Tier-1 supplier to help us tailor the ISO 26262 standard further to build safe vehicles.

6 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

7 Development Interface Agreement

All parties involved in the Lane Assistance project agree to and in the following operating principals to ensure that we are developing safe vehicles in compliance with ISO 26262 standard, tailored:

- **OEM Project Manager:** Item Level resources allocation with adequate functional safety competency, and appointment of external Functional Safety Auditor and Assessor. Lane assistance system functional safety plan, and confirmation measures acceptance.
- **Tier-1 Project Manager**: Component Level resources allocation with adequate functional safety competency.
- **Appointed OEM Functional Safety Manager/Engineer (John Chen):** Coordinate and document the item level planned safety activities including: concept phase, and product development at the system and software level. Perform functional safety pre-assessment prior to audit by external functional safety assessor three months prior to main assessment.
- **John Chen/Tier-1 Safety Manager:** Joint tailoring of the safety lifecycle.
- **All OEM, Tier-1 and their selected suppliers team members:** Follow safety processes and Create and sustain a safety culture as identified in *section 4* of this plan.
- **Appointed Tier-1 Safety Manager/Engineer:** Coordinate and document the component level planned safety activities including: concept phase, and product development at the component and sub-system software level in compliance with the item level planned and

safety activities as developed by OEM Functional Safety Manager/Engineer (John Chen).

- **Appointed Safety Auditor:** Plan the safety activities of the safety lifecycle once every two months.
- **Appointed Safety Assessor:** Perform functional safety assessment at conclusion of functional safety activities.

8 Confirmation Measures

The Confirmation Measures serve the following two purposes:

- The Lane Assistance safety project conforms to ISO 26262 tailored
- The Lane Assistance safety project does make the vehicle safer.

The **Confirmation review** will ensure that the safety project complies with ISO 26262 as tailored by an independent appointed safety auditor. The **Functional Safety Audit** will ensure that the actual implementation of he project conforms to the safety plan by an independent appointed safety auditor. The Functional Safety assessment will ensure that plans, designs and developed products actually achieve functional safety by an independent appointed safety assessor.