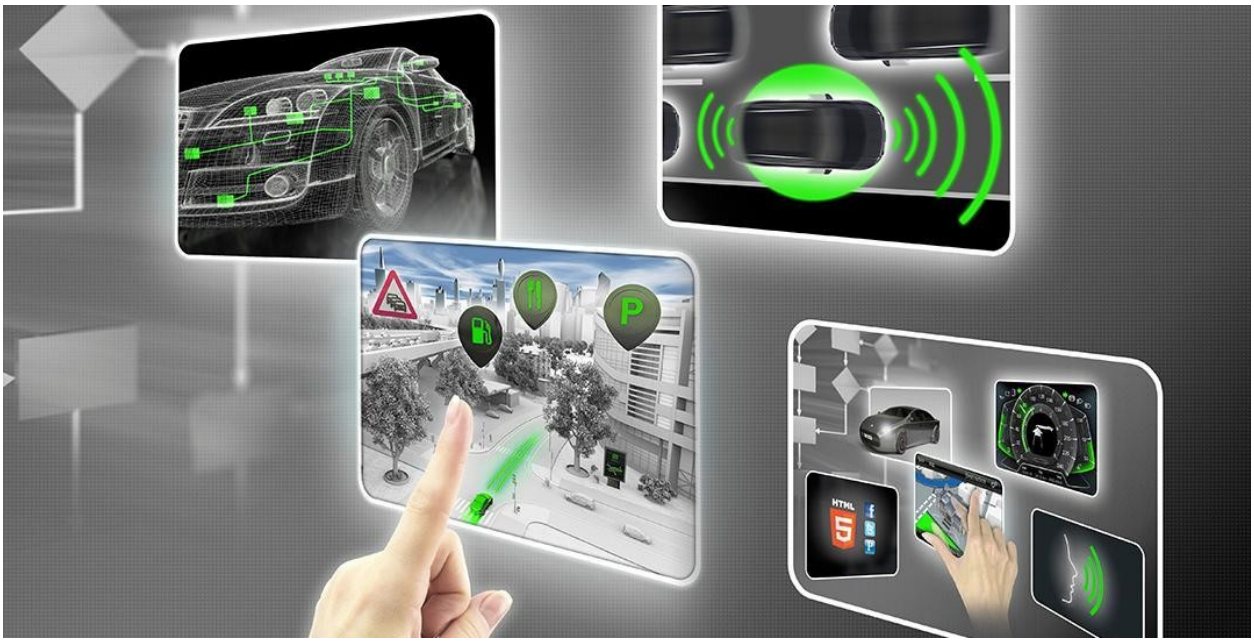
Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.0



Document history

Date	Version	Editor	Description
11/26/18	1.0	Kapy Kangombe	First draft of safety plan

Table of Contents

Introduction

Purpose of the Safety Plan

The purpose of the safety plan is to define the roles and outline the steps we will take to achieve functional safety of the lane assistance system. At a high level, it provides an overall framework for the functional safety of the system.

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

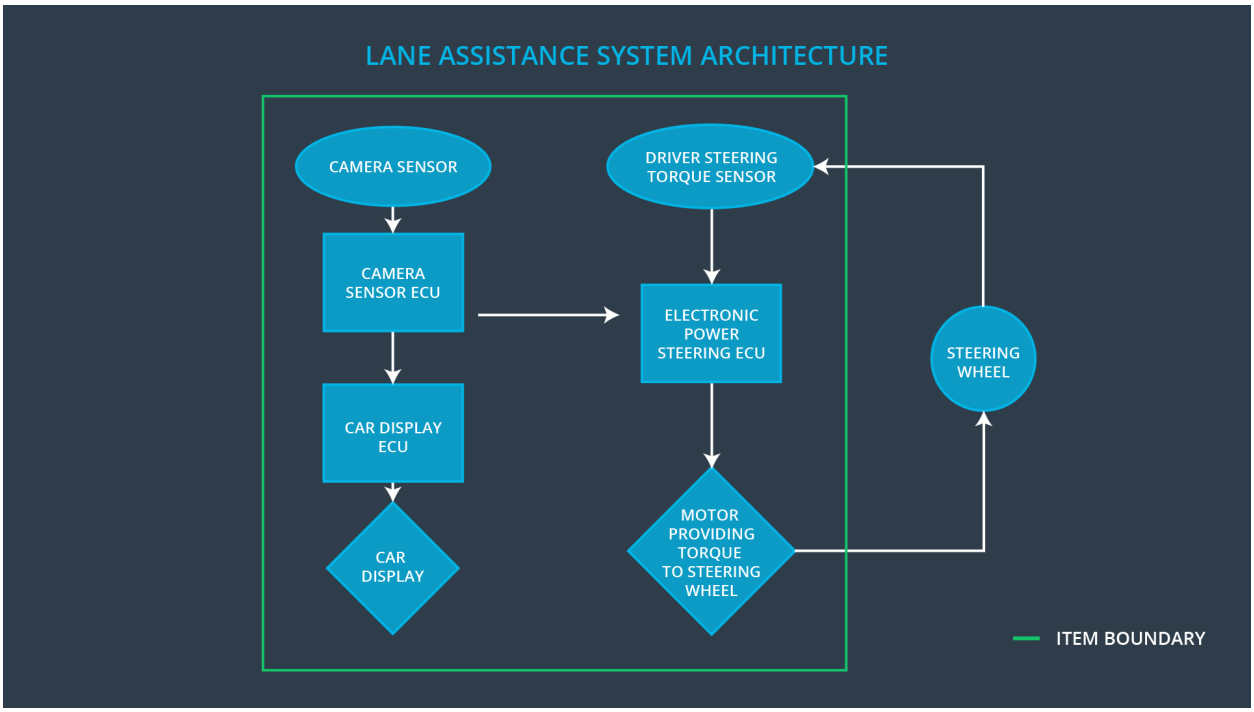
The item in question is a lane assistance system (LAS). It automatically assists the driver in keeping the vehicle safely within the lane. The LAS has two main functions:

1. Lane departure warning
2. Lane keeping assistance

The lane departure warning function will vibrate the steering wheel whenever the vehicle accidently departs from the center of the lane. It shall apply an oscillating steering torque to provide the driver a haptic feedback.

The lane keeping assistance system will automatically assist the driver by steering the vehicle toward the center of the lane. It shall apply the steering torque when active in order to stay in ego lane.

The lane assistance system consists of two subsystems: the camera subsystem and the electronic power steering subsystem. The camera subsystem is responsible for the lane departure warning function, whereas the electronic power steering subsystem is responsible for the lane keeping assistance function. Below is a diagram showing the item boundary, the subsystems within the item and the subsystems outside the item.



Goals and Measures

Goals

The goal of this project is to lower the risk of malfunction of the lane assistance system to an acceptable level according to ISO 26262. That is, to lower the risk of malfunction of the lane departure warning and lane keeping assistance systems.

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 Accessor	Conclusion of functional safety activities

Safety Culture

Here are some characteristics of the company’s 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
- **Quality Management**: comply with the quality management system outlined in IATF 16949

Safety Lifecycle Tailoring

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 purpose of a development interface agreement (DIA) is to:

- Clarify the responsibilities of the different parties involved in a functional safety project
- Describe the work products that each company will provide
- Help avoid disputes between companies
- Clarify who will be responsible for any safety issues in post-production

As we will be taking on the role of both functional safety manager and functional safety engineer, our company will have the following responsibilties at the subsystem/component level only:

- Planning, coordinating and documenting of the development phase of the safety lifecycle
- Tailoring the safety lifecycle
- Maintaining the safety plan
- Monitoring progress against the safety plan
- Performing pre-audits before the safety auditor
- Product development of subsystems
- Integration of subsystems
- Testing all the hardware and software at the subsystem level

The first five responsibilities will be as safety manager and the last three as safety engineer.

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.

The people who carry out confirmation measures need to be independent from the people who actually developed the project.

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.

A functional safety audit involves checking to make sure that the actual implementation of the project conforms to the safety plan is called a functional safety audit.

Confirming that plans, designs and developed products actually achieve functional safety is called a functional safety assessment.

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.