



Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21



Document history

Date	Version	Editor	Description
03.12.2018	1.0	Hiep Truong Cong	First draft
08.03.2019	2.0	Hiep Truong Cong	Release

Table of Contents

[Document history](#)

[Table of Contents](#)

[Introduction](#)

[Purpose of the Safety Plan](#)

[Scope of the Project](#)

[Deliverables of the Project](#)

[Item Definition](#)

[Goals and Measures](#)

[Goals](#)

[Measures](#)

[Safety Culture](#)

[Safety Lifecycle Tailoring](#)

[Roles](#)

[Development Interface Agreement](#)

[Confirmation Measures](#)

Introduction

Purpose of the Safety Plan

A safety plan provides an overall framework for the lane assistance item and to define roles, responsibility, outlining the steps, which will be taken to achieve functional safety for this 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

In this document, the lane assistance system is the item and will be analyzed, to assess risks and find out corresponding measures to minimize them. This item alerts the driver that the vehicle has accidentally departed its lane, and attempts to steer the vehicle back toward the center of the lane.

This item has 2 main functions:

- Lane departure warning
- Lane keeping assistance

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

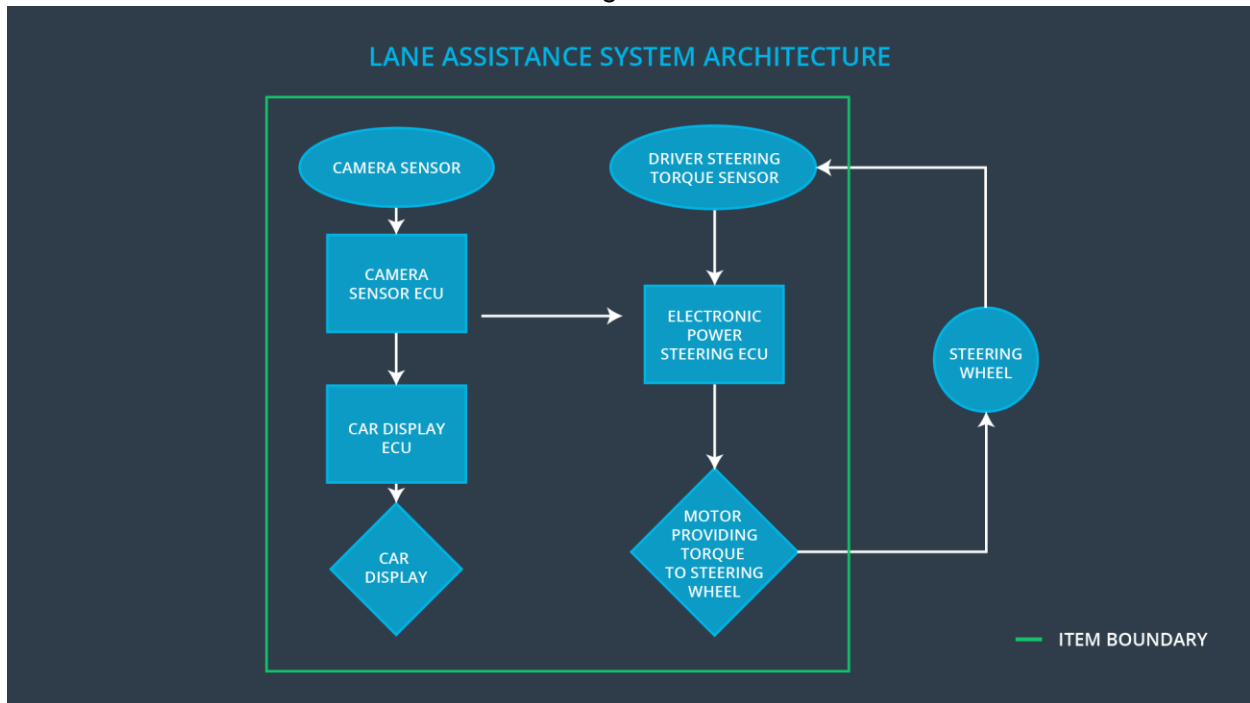
- The lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback.
- the lane keeping assistance function shall apply the steering torque when active in order to stay in ego lane

The item has three sub-systems:

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

These sub-systems are all responsible for each of the functions

The boundaries of the item are shown in the figure below:



- The item contains 3 sub-systems: camera, Electronic Power Steering system, car display. The component steering wheel is outside of the item.

Goals and Measures

Goals

- Determine risks produced by the lane assistance functions
- Derive measures to minimize the risks

Measures

Measures and Activities	Responsibility	Timeline
Follow safety processes	Safety manager	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

- 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 problem

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

A DIA (development interface agreement) defines the roles and responsibilities between companies involved in developing a product. All involved parties need to agree on the contents of the DIA before the project begins.

Responsibilities of OEM and Suppliers

OEM	Supplier
<ul style="list-style-type: none">- The OEM might provide requirements for what a vehicle system needs to do- OEM might provide a preliminary product design	<ul style="list-style-type: none">- Develops and produces the system for the OEM- Finish the details of the preliminary product design

Confirmation Measures

1. Purposes of confirmation measure are to check:

- Processes comply with the functional safety standard
- Project execution is following the safety plan
- Design really does improve safety

2. 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.

3. 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.

4. Functional safety assessment

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.