



Safety Plan Lane Assistance

Document Version: 1.1

Template Version 1.0, Released on 2017-06-21



Document history

Date	Version	Editor	Description
20-Jun-18	1.0	Nikhil Sinnarkar	First Draft of Safety plan
22-Jun-18	1.1	Nikhil Sinnarkar	Minor changes in safety measures & DIA after review

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

The Safety plan gives an overview of how to achieve a safe system. Among others this includes the system under consideration and to set up a goal for the project. It also includes the assignment of roles and responsibilities for the item's functional safety.

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

This safety plan covers the Lane Assistance System which is an Advanced Driver Assistance system (ADAS). The Lane Assistance System alert the driver to potentially dangerous situations and take control over the vehicle to prevent accidents from occurring.

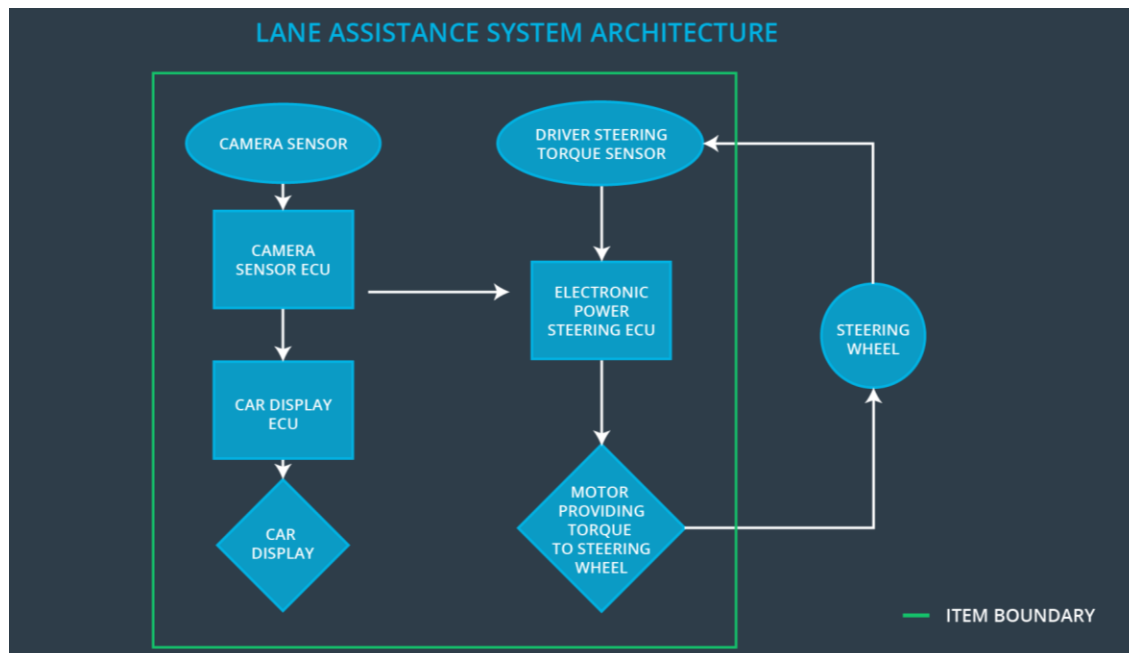
The two main function of this item are:

- **Lane departure warning function:** The Lane departure warning function vibrates the steering wheel in case the car drifts towards the edge of the lane.
- **Lane Keeping assistance function:** The Lane keeping assistance function moves the car turns back towards the center of the lane.

The item consists of three subsystems with their own components:

- Camera subsystem consisting of 2 components:
 - Camera sensor
 - Camera sensor with Electronic Control Unit (ECU)
- Electronic power steering subsystem consisting of 3 components:
 - Driver Steering Torque sensor
 - Electronic Power Steering
 - Motor providing torque to steering wheel
- Car Display subsystem consisting of 2 components:
 - Car Display ECU
 - Car Display

The following diagram shows the interaction between the 3 subsystems:



The camera subsystem is responsible for detecting and monitoring the position of the car in the ego lane and informing the car display and Electronic Power Steering subsystem if the car drifts towards the edge.

The Electronic Power Steering subsystem detects how much the driver is already turning the vehicle and add an extra torque to get the vehicle back towards the center.

The Car Display subsystem is only responsible for displaying the warning if necessary.

The Lane assistance system deactivates itself if the driver uses a turn signal or uses a button on the dashboard to turn off the system.

Other car subsystem like the steering wheel lie outside of this item.

Goals and Measures

Goals

This project goals are:

- Identify risk and hazardous situations in the Lane Assistance System components malfunction causing injuries to a person.
- Evaluate the risks of the hazardous situations.
- Lower the risk of the malfunctions to a reasonable levels acceptable by current society.

Measures

Measures and Activities	Responsibility	Timeline
Follow safety processes	All Team Members	Constantly
Create and sustain a safety culture	Safety Manager	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

To increase functional safety our organization provides a safety culture. This includes the following characteristics:

- **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 this project the safety plan is tailored. The following 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

Development Interface Agreement defines the roles and responsibilities all the companies which are involved in product development (OEM and Tier-1). DIA helps to avoid disputes during planning and development of the lane assistance system as it defines the above roles and responsibilities between the involved companies. All the parties who are involved in this needs to mutually agree on the contents of DIA before the project starts. The DIA also specifies what evidence and work products each party have to provide in order to prove that work was as per the agreement.

Responsibilities of OEM include defining the lane assistance system functionality and conducting activities which are in scope of Safety Manager, Project Manager and Safety Engineer.

The ultimate goal is to ensure that all parties are developing safe vehicles in compliance with ISO 26262. The major roles and responsibilities include:

- Appointment of customer and supplier safety managers
- Joint tailoring of the safety lifecycle

- Activities and processes to be performed by the customer; activities and processes to be performed by the supplier
- Information and work products to be exchanged
- Parties or persons responsible for each activity in design and production
- Any supporting processes or tools to ensure compatibility between customer and supplier technologies

Confirmation Measures

The *Confirmation measures* ensures that the applied processes comply with functional safety standards provided by ISO 26262 and that project execution is following the safety plan, therefore verifying if the design really does improve safety.

In particular, by providing *confirmation review*, during design and development of the product, compliance with ISO 26262 is assured by an independent person.

A *Functional Safety Audit* checks that the actual implementation of the project considers the safety plan.

Finally, *Functional Safety Assessment* confirms that plans, designs and developed products 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.