



Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21



Document history

Date	Version	Editor	Description
21/5/2018	1.0	Krishna	1 st version of functional safety

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 is a formal documented procedure that is to be followed by all the members of the workplace in case of an emergency. Safety plan is a practical system of policies, procedures and practices for the prevention and elimination of injuries, and health hazards. This document describes the safety plan for lane assistant 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

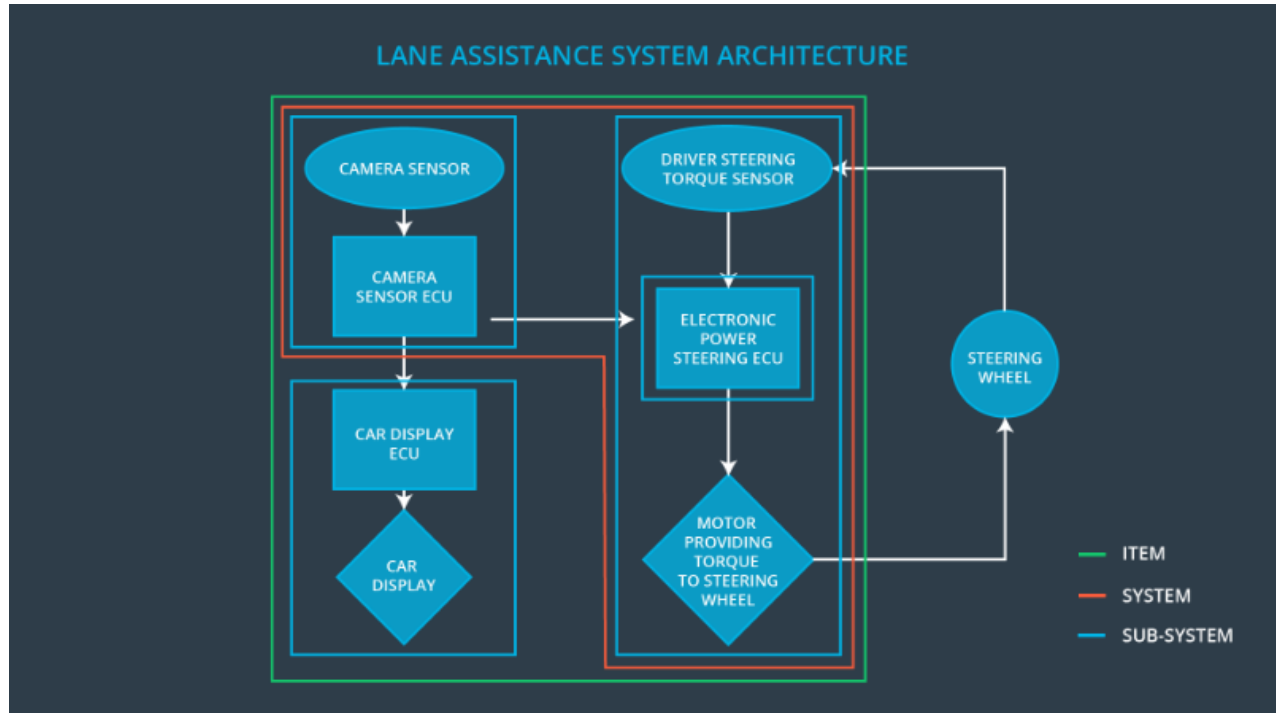
The deliverables of the project are:

- Safety Plan
- Hazard Analysis and Risk Assessment
- Functional Safety Concept
- Technical Safety Concept
- Software Safety Requirements and Architecture

Item Definition

What is the item in question, and what does the item do?

The item in consideration here for the safety plan is the Lane Assistance System. The Architecture for the Lane Assistance System is shown below:



The Lane Assistance System does the following two things:

- Alert the driver to potentially dangerous situations
- Take control over the vehicle to prevent accidents from occurring

What are its two main functions? How do they work?

The Lane Assistance System has the following two functions:

- Lane Departure Warning: When the driver moves to the edge of the lane, then the lane departure warning system will vibrate the steering wheel by moving it back and forth to notify the driver.
- Lane Keeping Assistance: Whenever the driver moves to the edge of the lane or removes his hand off the steering wheel then, this function will turn the steering wheel in order to bring the car back to the center of the ego lane, i.e., the lane in which the car is driving.

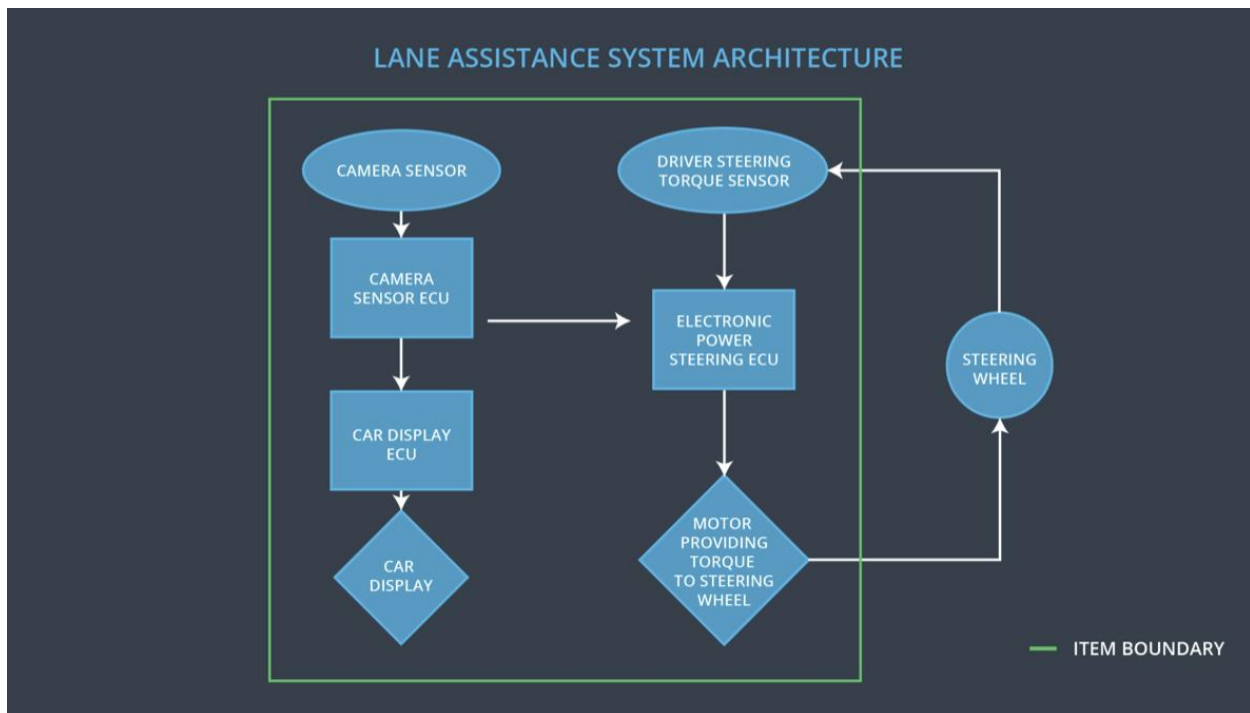
Which subsystems are responsible for each function?

The following mentioned subsystems are responsible for Lane Assistance System:

1. Camera sensor sub-system: To detect the drift from the lane

2. Power Steering Subsystem: Takes input from camera subsystem and outputs to the motor of steering wheel
3. Driver Display Subsystem: Visual feedback for the driver

What are the boundaries of the item? What subsystems are inside the item? What elements or subsystems are outside of the item?



The elements inside are: Camera sensor subsystem, Power Steering Subsystem, Driver Display Subsystem

The elements outside are: Steering Wheel

Goals and Measures

Goals

Describe the major goal of this project; what are we trying to accomplish by analyzing the lane assistance functions with ISO 26262?

The major goal of the project is to develop a Lane Assistance System which serves the following goals:

- Identify risk and hazardous situations in the Lane Assistance System which may cause harm to a person

- Evaluate the risks of situations and lower the malfunction chances to acceptable level as per society norms

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

Describe the characteristics of your company's safety culture. How do these characteristics help maintain your safety culture?

Here are some characteristics of a good 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

Safety Lifecycle Tailoring

Describe which phases of the safety lifecycle are in scope and which are out of scope for this particular 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

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

1. What is the purpose of a 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.

The DIA also specifies what evidence and work products each party will provide to prove that work was done according to the agreement.

The ultimate goal is to ensure that all parties are developing safe vehicles in compliance with ISO 26262.

2. What will be the responsibilities of your company versus the responsibilities of the OEM?

The OEM provides design details of a functioning lane assistance system. The OEM will provide requirements for the component of the system.

The Tier-1 company is going to analyze and modify the various sub-systems of the lane assistance system. It is going to supply various parts to the OEM keeping in mind the functional safety.

Thus, the relation between the OEM and Tier-1 company is a type of customer-supplier relationship where OEM is the customer and the Tier-1 company is the supplier.

Confirmation Measures

1. What is the main purpose of confirmation measures?

The purpose of the confirmation measures are:

- Ensure the Lane Assistance project conforms to ISO 26262.
- Ensure the Lane Assistance project really does make the vehicle safer.

2. What is a confirmation review?

The Confirmation review main goal is to ensure 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. What is a functional safety audit?

A functional safety audit makes sure that the actual implementation of the project confirms to the safety plan.

4. What is a functional safety assessment?

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