Elektrobit

UDACITY

# Safety Plan Lane Assistance

**Document Version:** [Version]

Template Version 1.0, Released on 2017-06-21

# Document history

| Date | Version | Editor | Description |
|---|---|---|---|
| 9/23/2917 | 1.0 | Sumit Chhabra | Safety plan for Lane Assistance |
| | | | |
| | | | |
| | | | |
| | | | |

# Table of Contents

# Introduction

## Purpose of the Safety Plan

Functional Safety is a concept to assess the risk and taking the necessary steps to reduce the risk to the acceptable level. The purpose of the safety plan document is to provide an overall framework how functional safety will be achieved and ensured during the entire development of any vehicle system and later in the production and the operation. As safety is given highest priority over the cost and the production, this document will also reflect that good safety culture is practiced in the organization. This document must adhere to the standards set for Electrical and Electronics for the Automotive industry called ISO 26262. Safety plan document will cover what vehicle system is considered for the goal of the project, what steps will be taken to ensure the safety, different roles involved in the project and the project timeline to accomplish the goal. ISO 26262 requires independent audits. Auditors will rely on these documents to ensure the steps outlined in the standard were followed and made vehicle systems safer.

## Scope of the Project

**[Instructions: Nothing to do here. This is for your information.]**

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

**[Instructions: Nothing to do here. This is for your information.]**

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

**[Instructions:**

**REQUIRED**

**Discuss these key points about the system:**

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

An Item definition specifies which high level vehicle system is being considered. For this project, Lane Assistance System is chosen as an Item. This item, i.e. Lane Assistance System, is part of the Advanced Driver Assistance System (ADAS). This item will warn the driver if the vehicle is going outside the lane and signal indicator is not turned on. Subsequently this item will provide the torque to the steering vehicle to bring the vehicle back to center of the ego lane. Vehicle will also have a button in the dashboard to turn off this item.

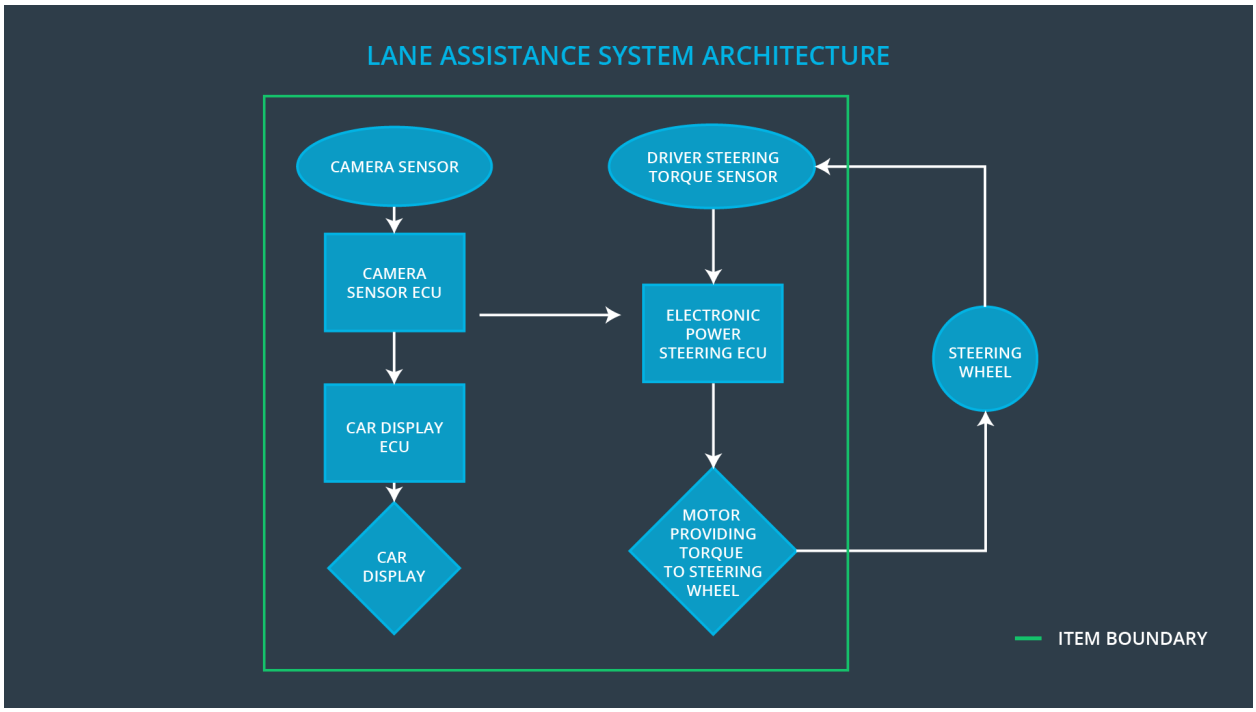


Figure 1: High level System Architecture of Lane Assistance Functionality

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

This item, i.e. Lane Assistance System, will have two functions.

- “Lane Departure Warning” This function will apply the oscillating steering torque feedback to a steering wheel to provide a feedback to the driver.
- “Lane Keeping Assistance” This function will turn the steering wheel towards the center of the ego lane.

**Which subsystems are responsible for each function?**

Vehicle Assistance System will be relying on the following subsystem in order to function effectively

- Camera Sensing Unit
- Car Display Unit
- Electronic Power Steering unit

In Lane Departure Warning functionality, when the vehicle is leaving the lane, camera will detect it and it will simultaneously send signal to ECU to activate the turning of the steering wheel as well as send haptic feedback, i.e., vibrations to the steering wheel to alert the driver. In addition, same signal will turn on warning light in the car display unit.

In Lane Keeping Assistance functionality, if lane departure signal is activated, ECU will provide enough torque in addition to the torque applied by the driver, to return the car to the center of the ego lane.

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

Lane Assistance System is limited to two functionalities – Lane departure warning and Lane keeping assistance. If the driver is using the signal indicator to change the lane, then Lane Assistance System will remain inactive. As mentioned above, Lane Assistance system is made up of three subsystems. Each subsystem will have its own elements, as follows.

- Camera Sensor Unit will have Camera Sensor, Camera sensor ECU (Electronic Controller Unit)
- Car Display Unit will have Car Display ECU, Car Display
- Electronic Power Steering will have its own ECU, driver steering torque sensor and motor to provide torque to steering wheel.

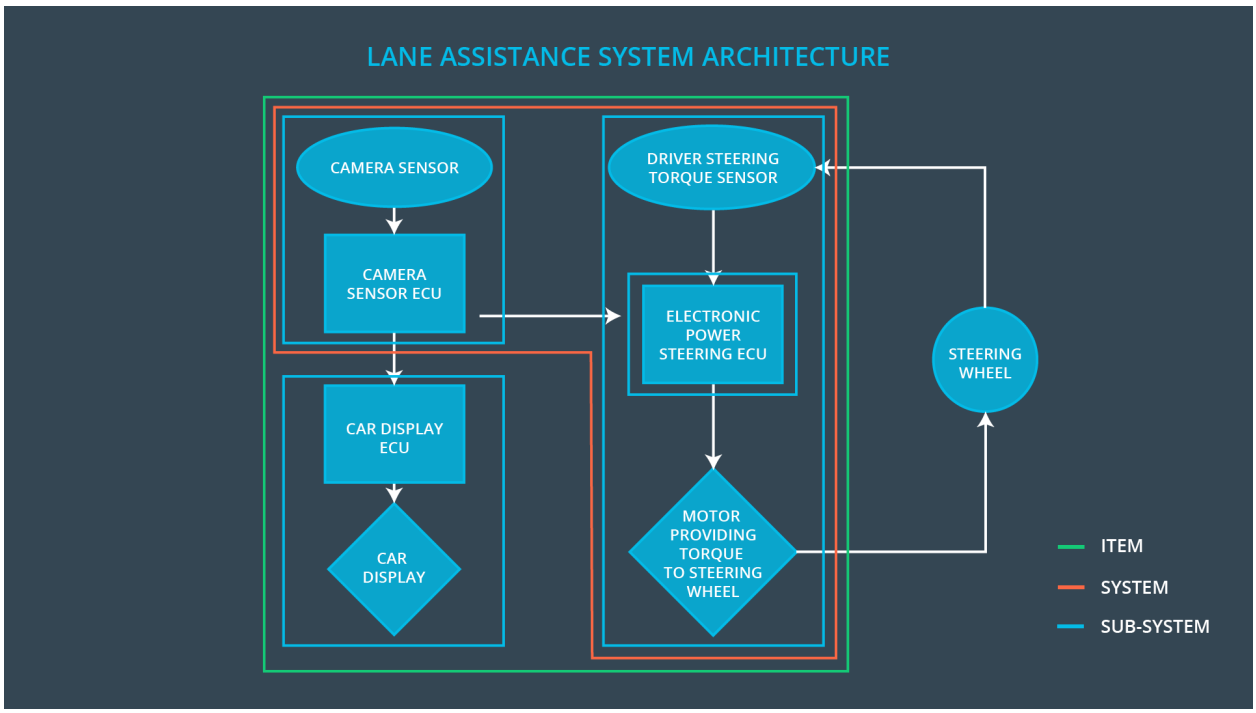

Figure 2: Different subsystems of Vehicle Lane Assistance System.

**OPTIONAL**

**Optionally, include information about these points as well. These were not included in the lectures, but you might be able to find this information online:**

- **Operational and Environmental Constraints. This could especially be limited to camera performance; lane lines are difficult to detect in snow, fog, etc**
- **Legal requirements in your country for lane assistance technology**
- **National and International Standards Related to the Item**
- **Records of previously known safety-related incidents or behavioral shortfalls**

**]**

# Goals and Measures

## Goals

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

The main goal of ISO 26262 is to reduce the risk to the acceptable level and make the vehicle system safer. By analyzing this project with ISO 26262, we are ensuring designing, development and production of Lane Assistance System are following the industry standard procedure. This will include the software and hardware used in the project are meeting the standards of the automotive industry. When this system is in operation, its doing its job by altering the driver about the hazardous situation and taking appropriate action to prevent any accident and/or injury.

## 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 | Saftety Auditor | Once every 2 months |
| Perform functional safety pre- | Safety | 3 months prior to main |

| | | |
|---|---|---|
| assessment prior to audit by external functional safety assessor | Manager | assessment |
| Perform functional safety assessment | Safety Assessor | Conclusion of functional safety activities |

# Safety Culture

Safety culture is a good practice followed by an organization to develop clear policies, communications and strategies to promote the design, development, production and operation of the vehicle systems. Some key characteristics of the safety culture as follows

- Safety is given the highest priority as compared to the project cost and production.
- Every person or team involved in any phase of the project are responsible for their decisions.
- Organization will promote and motivate the achievement of functional safety.
- Organization will penalize if any shortcuts taken which can impact the functional safety.
- The team which will design and develop the system will be independent from the team which will audit or assess the system.
- 
- Organization will clearly define design, roles and management process.
- Project will include the necessary resources including the appropriate skilled persons.
- Intellectual diversity will be promoted in the workplace.
- Clear communication channels will be set between the different teams involved in conceptual and implementation phases.

# Safety Lifecycle Tailoring

**[Instructions:**
**Describe which phases of the safety lifecycle are in scope and which are out of scope for this particular project. Hint: See the Intro section of this document**
**]**

Safety lifecycle of Lane Assistance system will have in scope  the concept phase and partially product development of the V process model as per ISO 26262 standard. Concept phase will include Hazard Analysis and Risk Assessment, Function Safety concept. product development will include at the System level as well the Software level.
Safety lifecycle will have the product development at the hardware level and Production and Production and operation phase out of scope.

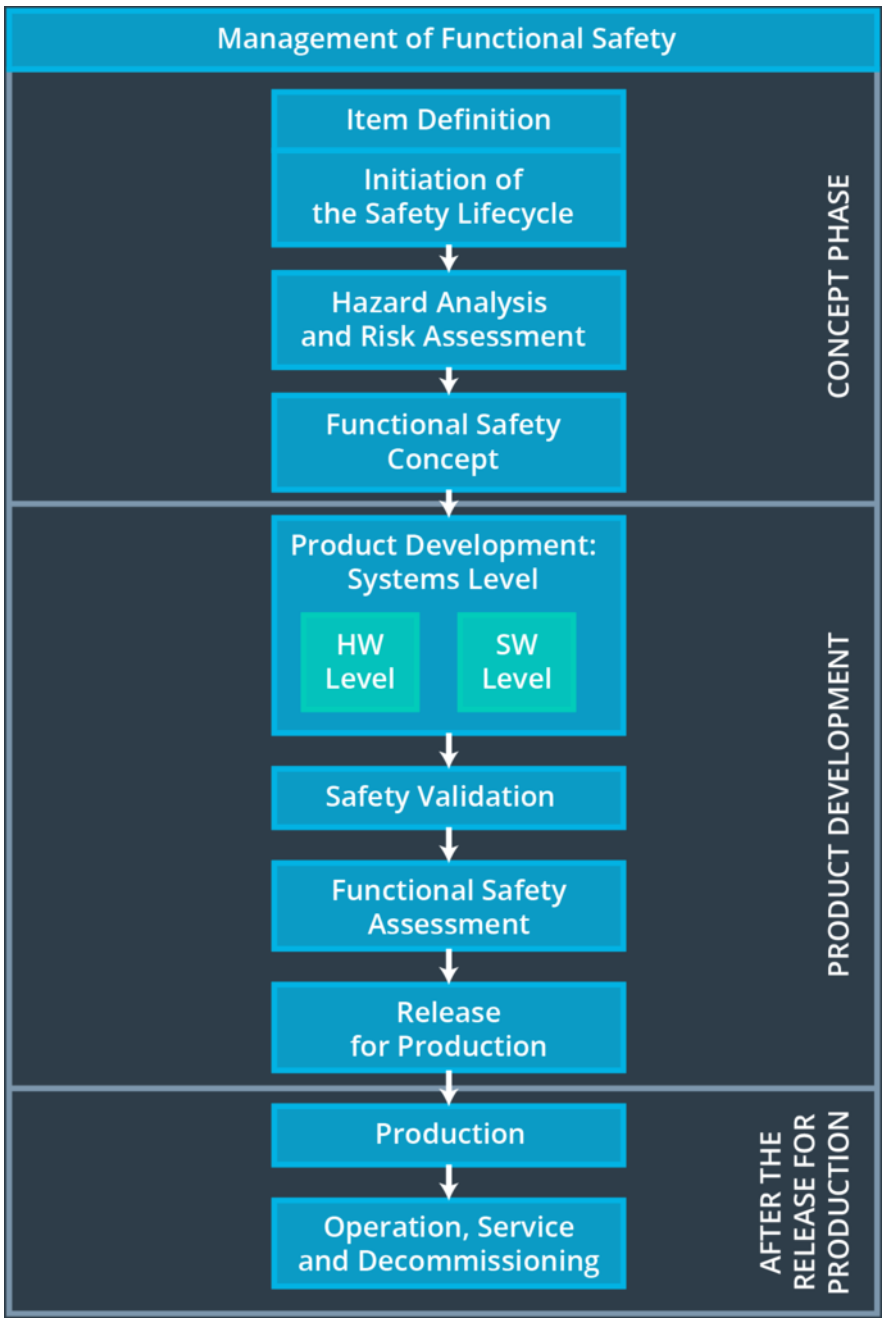

Figure 3: Flatten V Process Model to reflect the Safety Lifecycle Tailoring.

# Roles

**[Instructions:**
**This section is here for your reference. You do not need to do anything here. It is provided to help with filling out the development interface agreement section.**
**]**

| 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

**[Instructions:**
**Assume in this project that you work for the tier-1 organization as described in the above roles table. You are taking on the role of both the functional safety manager and functional safety engineer.**

**Please answer the following questions:**

1. **What is the purpose of a development interface agreement?**

Development Interface Agreement (DIA) is very important for developing the safe vehicle if the original equipment manufacturer (OEM) will be engaging services of other companies for the development of the system. Roles and responsibilities will be defined in DIA for the involved parties, that way each party will responsible for the design and development of the system. They will work together for tailoring the safety lifecycle. Information and work products will be exchanged among the involved parties. DIA are crucial documents for the future incase any dispute or conflicts are involved between the parties.

2. **What will be the responsibilities of your company versus the responsibilities of the OEM? Hint: In this project, the OEM is supplying a functioning lane assistance system. Your company needs to analyze and modify the various sub-systems from a functional safety viewpoint**

My company will be a Tier1 company and in a customer supplier relationship with OEM (Original Equipment Manufacturer). OEM will provide the set of requirements what lane assistance system needs to do. My company, Tier 1 company,  will develop and supply functioning lane assistance system to the OEM which will include meeting the original requirements. OEM can also provide the preliminary product design and Tier1 company can

finish the details of the product. Before Tier1 company can begin the work, both OEM and Tier1 will agree on the DIA. Tier1 company will follow the same V process model in developing the  product. Bother OEM and Tier1 will have safety manager to see the overall progress and delivery. There will be clear communication between the parties which will include exchanging of information and work products. Both parties will have compatible processes or tools between their technologies used in the product development.

# Confirmation Measures

**[Instructions:**
**Please answer the following questions:**

1. **What is the main purpose of confirmation measures?**
   There are two main purpose of the conformation measures. First one is to make sure processes involved in the project comply to Function Safety Standard ISO 26262. Second is the project really does make the vehicle safer. Conformation measures are carried out by the people who are independent from the design and the implementation team of the project.

2. **What is a confirmation review?**
   The confirmation review is carried out by an independent person during the design and development phase of the vehicle system, to ensure the processes are compiling with Functional Safety Standard ISO 26262.

3. **What is a functional safety audit?**
   Functional safety audit is an independent examination of the project to ensure the actual implementation of the project conforms to the safety plan and effectively achieve the specified objective.

4. **What is a functional safety assessment?**
   Functional safety assessment is the conformation of plans, design and developed products are actually achieving the functional saftey.

---

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.

# Glossary

| | |
|---|---|
| Ego Lane | Lane in which the vehicle is currently driving. |
| Fault | A defect or unexpected behavior of a system. |
| Hazard | A situation that could cause injury or harm a person’s health. |
| Item | Specifies which vehicle system is being considered. |
| Malfunction | When something goes wrong with a system. |
| Risk | The probability that a harmful situation could occur. |