Elektrobit

UDACITY

# Safety Plan Lane Assistance

**Document Version:** [Version]

**Template Version 1.0, Released on 2017-06-21**

# Document history

**[Instructions: Fill in the date, version and description fields. You can fill out the Editor field with your name if you want to do so. Keep track of your editing as if this were a real world project.**

**For example, if this were your first draft or first submission, you might say version 1.0. If this is a second submission attempt, then you'd add a second line with a new date and version 2.0]**

| Date | Version | Editor | Description |
|---|---|---|---|
| 9/1/2017 | 1.0 | Flora Sun | Initial Draft |
| | | | |
| | | | |
| | | | |
| | | | |

# Table of Contents

**[Instructions: We have provided a table of contents. If the table of contents is not showing up correctly in your word processor of choice, please update it. The table of contents should show each section of the document and page numbers or links. Most word processors can do this for you. In Google Docs, you can use headings for each section and then go to Insert > Table of Contents. Microsoft Word has similar capabilities]**


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

**[Instructions: Answer what is the purpose of a safety plan?]**

The safety plan defines roles and outlines the steps needed to achieve functional safety of the lane assistance. The safety plan covers the following areas: safety culture, safety lifecycle, safety management roles and responsibilities, development interface agreements, and confirmation measures.

## 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:**

Lane assistance system is part of the ADAS (Advanced Driver Assistance System), which has two functions:

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

Specifically, the Lane Assistance system will have two functions:

- Lane departure warning
- Lane keeping assistance

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

When the driver drifts towards the edge of the lane, the Lane Assistance Item will

- warn the driver of the drifting, and
- move the steering wheel so the car will move closer to the center of the lane.

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

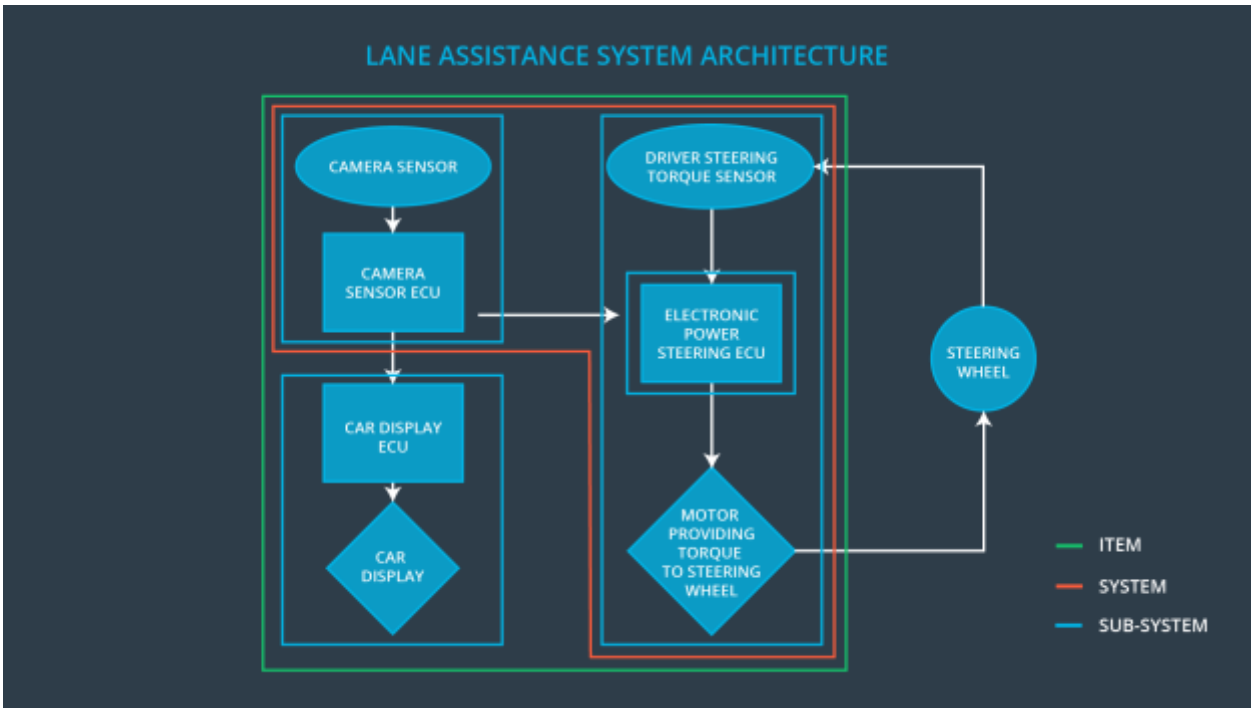
The two main functions are

- lane departure warning, which vibrates the steering wheel to warn the driver that the car has been drifting away from the center.
- lane keeping assistance, which move the steering wheel such that the car will move back towards the center of the lane.

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

As illustrated in the diagram below there are three subsystems:

- Camera subsystem includes the camera sensor and the camera sensor ECU. The camera subsystem is responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake.
- Electronic Power Steering subsystem includes the driver steering torque sensor, the ECU, and the motor providing torque to steering wheel. It is responsible for measuring the torque provided by the driver and then adding an appropriate amount of torque based on a lane assistance system torque request.
- Car Display subsystem which includes the car display ECU and the car display. It receives and display warning of the lane departure.




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

As illustrated in the above image, the following subsystems are inside the item, lane assistant system:

- Camera subsystem
- Electronic Power Steering subsystem
- Car Display subsystem

The following are outside of the item:

- Steering wheel

**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 goal is to avoid accidents by reducing risks to acceptable levels.  Analyzing the lane assistance functions with ISO 26262 can help us figure out what subsystem contain high levels of risks and what is needed to prevent accidents.

## Measures

**[Instructions:**
**Fill in who will be responsible for each measure or activity. Hint: The lesson on Safety Management Roles and Responsibilities.**

**The options are:**
**All Team Members**
**Safety Manager**
**Project Manager**
**Safety Auditor**
**Safety Assessor**
**]**

| 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

**[Instructions: Describe the characteristics of your company's safety culture. How do these characteristics help maintain your safety culture. Hint: See the lesson about Safety Culture]**

At our company, safety holds the highest priority over other competing constraints, such as cost and productivity. Design decisions are documented and traceable to those who made those decisions. We reward achieving safe systems and penalize taking shortcuts.  We are counting on the following principles to achieve a high 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

**[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]**

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

**[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?**

   The purpose of a DIA (development interface agreement) is to ensure the various parties involved in design are in compliance with ISO 26262. DIA defines the roles and responsibilities between companies involved in designing the lane assistance product. The DIA also includes evidence and work product required for each company.

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.]**

   The responsibilities of OEM are:
   - Supplying a functioning lane assistance system.
   - Provide functional safety management, engineering and project management at the item level.
   - Provide safety audit and assessment

   The responsibilities of our company (the Tier One vendor) are:
   - Analyze and modify the various sub-systems from the functional safety view point.
   - Provide functional safety management, engineering and project management at the component level.

# Confirmation Measures

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

1. **What is the main purpose of confirmation measures?**

2. **What is a confirmation review?**
3. **What is a functional safety audit?**
4. **What is a functional safety assessment?**

]

1. The three main purposes of confirmation measures are:
    a. Make sure the processes involved comply with the functional safety standard such as ISO 26262
    b. Make sure the project execution is following the safety plan,
    c. Make sure the design indeed improve safety.
2. Confirmation review ensures the project complies with ISO 26262. An independent person, who is not in the team that design and execute the functional safety, should review the work to make sure that ISO 26262 is being followed.
3. Functional safety audit checks to make sure the implementation of the project confirms to the safety plan.
4. Functional safety assessment confirms that the plans, designs and the product developed achieve the 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.