Elektrobit

UDACITY

# Safety Plan Lane Assistance

**Document Version:** [Version]

Template Version 1.0, Released on 2017-06-21

# Document history

| Date | Version | Editor | Description |
|---|---|---|---|
| 26th August, 2017 | 1.0 | Microsoft Word | Initial version of Safety plan document |
| | | | |
| | | | |
| | | | |
| | | | |

# Table of Contents

# Introduction

## Purpose of the Safety Plan

A safety plan is a document that enumerates the safety culture of an organization, the safety lifecycle, safety management roles and responsibilities, development interface agreements and confirmation measures

## 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:

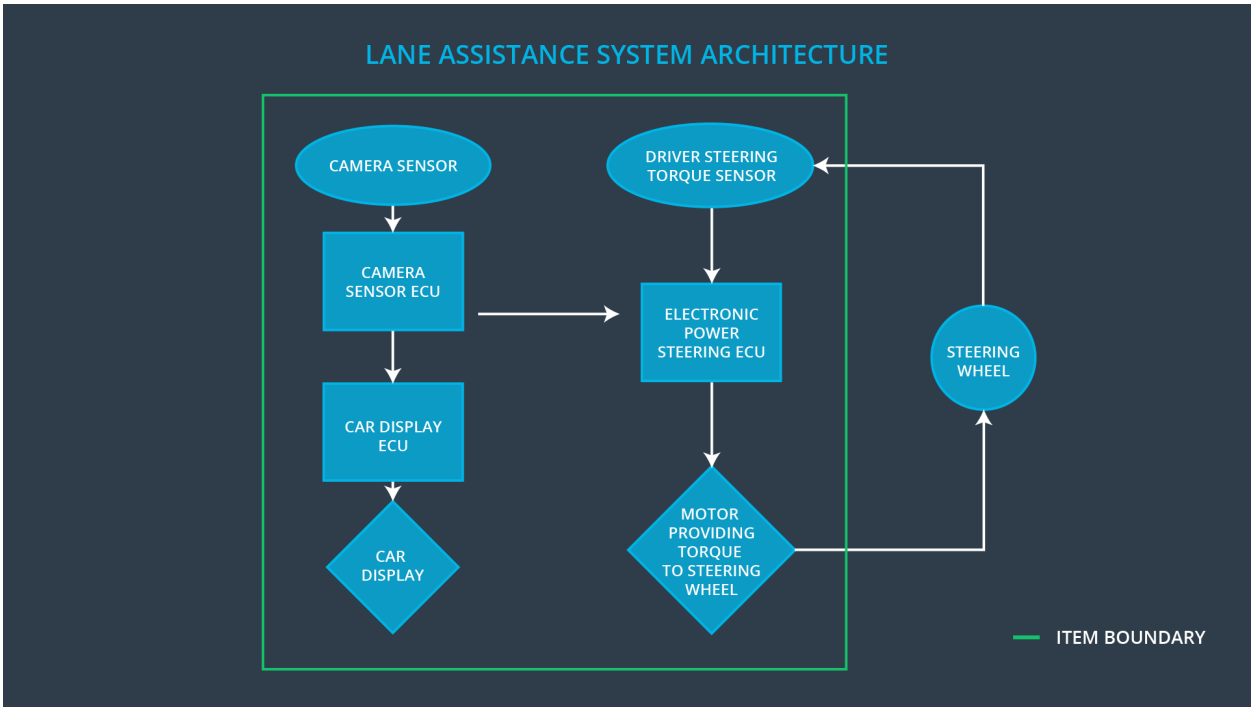
Product Development at the Hardware Level
Production and Operation

## 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?**

An Advanced Driver Assistance System, often called ADAS systems, which has two functions:

- 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?**

- Lane Departure Warning Function – Whenever a driver steers off the lane, the Lane Departure Warning function will signal this to the driver by causing vibration of the steering wheel. Lane Departures are detected by a camera subsystem which will cause the Power Steering subsystem to generate the torque to vibrate the steering wheel.
- Lane Keeping Assistance Function – Whenever a driver is steering off the lane, the Lane Keeping Assistance function will help the car get back on the lane by applying some amount of torque for a duration of time.

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

- Lane Departure Warning Function – Camera subsystem, Power Steering Subsystem, Driver Display Subsystem
- Lane Keeping Assistance Function – Camera subsystem, Power Steering Subsystem, Driver Display Subsystem

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

The item boundary was drawn to include three sub-systems:

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

Other car subsystems like the steering wheel lie outside of this item

# Goals and Measures

## Goals

To analyze the Lane Departure Warning Function and the Lane Keeping Assistance Function for possible defects and resulting hazards, and come up with a plan to minimize the risk to acceptable levels.

## Measures

| Measures and Activities | Responsibility | Timeline |
|---|---|---|
| Follow safety processes | Safety Engineer | 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

- **High priority**: safety has the highest priority among competing constraints like cost and productivity. This ensures that safety is always given the highest priority.
- **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

The Lane Assistance Project is a modification to an existing automotive system and only requires the following phases:

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

**[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.**

1. **What is the purpose of a development interface agreement?**
   In the safety plan, there is a section called the DIA(development interface agreement) which delineates the design and production responsibilities between the OEM and the Tier 1 supplier or between the Tier 1 supplier and the Tier 2 supplier

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 OEM and Tier 1 supplier take on a customer:supplier relationship. The OEM will provide requirements for what a vehicle system needs to do. Then the Tier 1 supplier develops and produces the system for the OEM. The OEM may provide a preliminary product design and then the tier 1 supplier will finish the details. In this case, the OEM will provide our company with the requirements for the lane keeping system and our company will develop and produce the system for the OEM and analyze and modify the various systems from a functional safety standpoint.

# Confirmation Measures

1. **What is the main purpose of confirmation measures?**
   Ensures that the functional safety measures have actually reduced the risk to levels acceptable by society

2. **What is a 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. **What is a 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. **What is a 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.