Elektrobit

UDACITY

# Safety Plan Lane Assistance

**Document Version:** [Version]

Template Version 1.0, Released on 2017-06-21

## Document history

| Date | Version | Editor | Description |
|---|---|---|---|
| 2018-06-08 | 1.0 | Markus Isaksson | First attempt |
| | | | |
| | | | |
| | | | |
| | | | |

# Table of Contents

# Introduction

## Purpose of the Safety Plan
The purpose of this safety plan is to provide an overall framework for the safety aspects of the Lane Assistance Item and to assign related roles and responsibilities.

## 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
The lane assistance item alerts the driver when the vehicle unintentionally drifts towards the edge of ego lane and also attempts to steer the vehicle back to center of ego lane.

This is essentially two functions:
1. Lane Departure Warning
2. Lane Keeping Assistance

When a camera sensor detects that ego vehicle approaches the lane edge without an active turn signal, then this is considered unintentional, and the Lane Departure Warning provides an

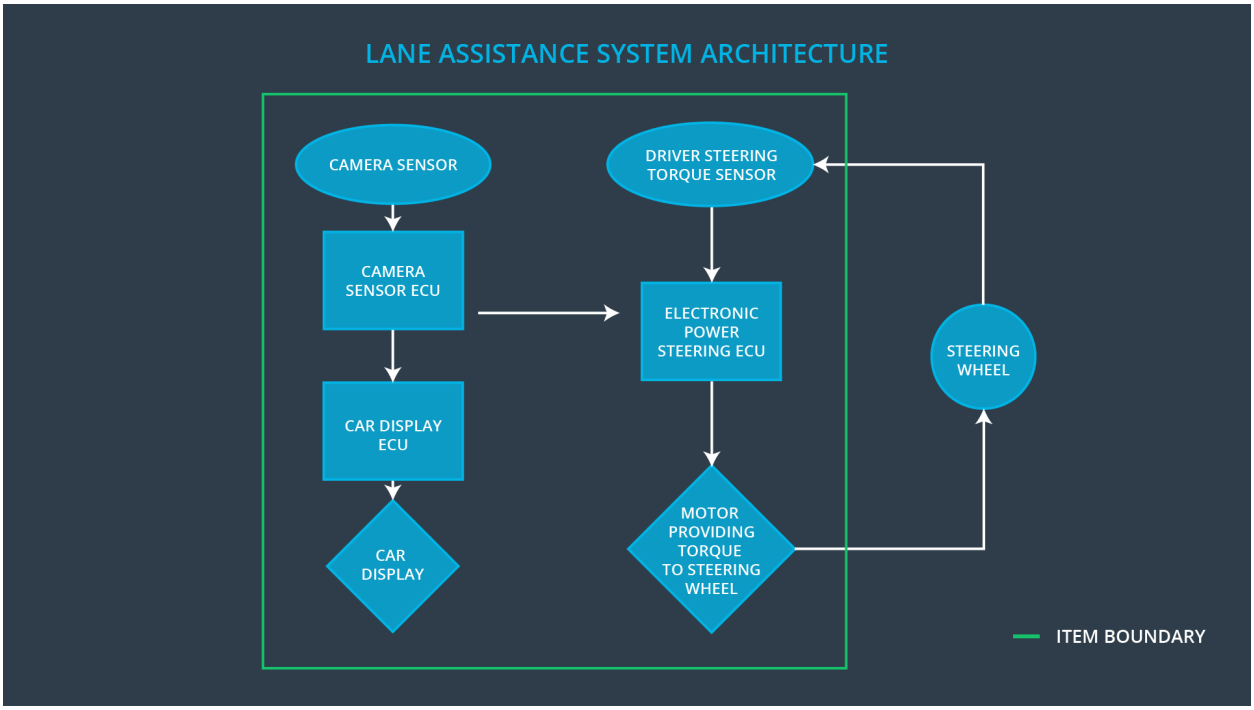
haptic feedback by vibrating the steering wheel and the Lane Keeping Assistance applies a torque on the steering wheel in an attempt to steer the vehicle back to the center of ego lane.

The lane assistance item have three subsystems:

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

All subsystems are responsible both for the Lane Departure Warning and the Lane Keeping Assistance functions.

The figure below outlines the boundaries of the item.




The Camera system includes the camera sensor and camera sensor ECU. The Car Display system includes the car display ECU and the car display. The Electronic Power Steering system includes the electronic power steering ECU, a sensor measuring the drivers steering torque and a motor providing torque to the steering wheel. Note however that the steering wheel by itself is outside of the item boundary.

# Goals and Measures

## Goals

The lane assistance functions are analyzed with ISO 26262 to

- Identify potential hazardous malfunctions.
- Evaluate the risk of sad malfunctions.
- Reduce the risk of sad malfunctions to acceptable levels.

## 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 | All Team Members | 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 Assesor | Conclusion of functional safety activities |

# Safety Culture

The company has established a culture where

- Safety has the highest priority.
- The design process ensures accountability.
- Functional safety achievements are recognized and rewarded.

- Safety or quality shortcuts are never accepted.
- The teams that design and develop a product are independent from the teams auditing the work.
- Design and management processes are clearly defined.
- Adequate resources are allocated to projects.
- Intellectual diversity is valued, sought after and integrated into processes.
- Communication channels are available to effectively disclosure any type of problem.

# Safety Lifecycle Tailoring

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

In general, the purpose of the development interface agreement is to

- Appoint a customer and a supplier Safety Manager.
- Clarify responsibilities between organizations, such as
  - Activities and processes to be performed.
  - Information and work products to be exchanged.
  - Safety issues in post-production.
- Clarify liability between organizations.

- Processes and tools needed to ensure compatibility between the organizations.

In this project, the OEM provides a lane assistance system that the tier-1 organization shall analyze and modify from a functional safety viewpoint to ensure it's compliance with ISO 26262.

The deliverables from the OEM are

- All relevant parts of the existing product, including System, HW and SW design, HW schematics/layout, SW implementation, unit tests, integration tests, system tests.
- Any updates needed on the HW level to achieve functional safety.

The deliverables from the tier-1 organization are

- All documentation building up the safety case, including the safety plan, design plans, functional safety concept, technical safety concept, as well as evidence documenting testing and integration.
- Updated System and Software design documents, including Software Safety Requirements and Architecture.
- Updated Software implementation.
- Updated test cases.

When the safety case has been approved by an external Functional Safety Assessor appointed by the OEM, then the tier-1 organization will have no further liability with this product. The OEM takes full responsibility for any unforeseeable legal or post-production issues.

# Confirmation Measures

The main purpose of confirmation measures are to make sure that the functional safety project confirms to ISO 26262 and that it really makes the vehicle safer.

In a **confirmation review,** an independent person will review the work to ensures that it complies with ISO 26262. This is done continuously as the product is being designed and developed.

In a **functional safety audit**, an independent person checks that the actual implementation conforms to the safety plan.

In a **functional safety assessment**, an independent person/organization confirms that the final plans, designs, and the developed product achieves 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.