Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.0

Document history

Date	Version	Editor	Description
2018-01-26	1.0	Josef Steinbaeck	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 Lane Assistance item and to assign roles and responsibilities for functional safety for this 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

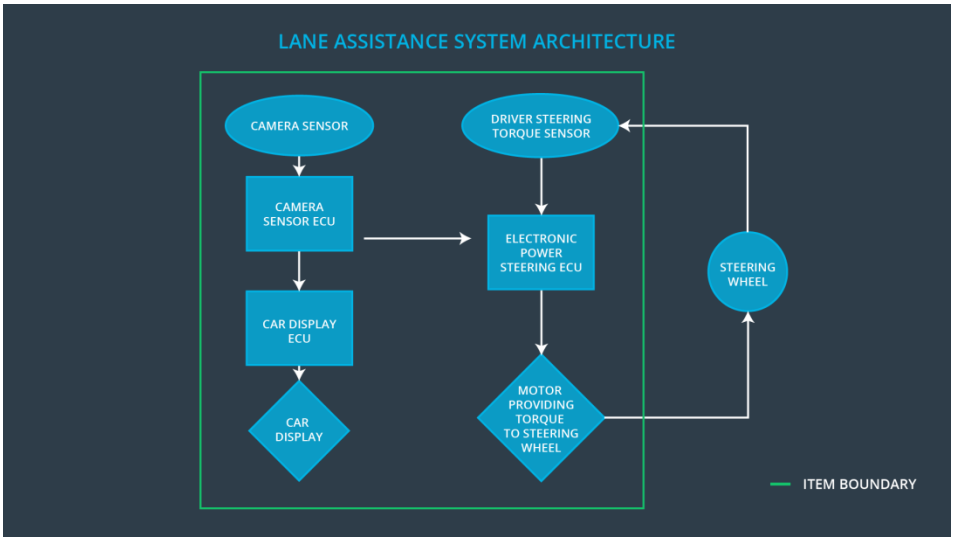
What is the item in question, and what does the item do?
The lane assistance item alerts the driver that the vehicle has accidentally departed its lane and attempts to steer back toward the center of the lane.

What are its two main functions? How do they work?
The system has two functions:

- Lane departure warning
    - Functionality that vibrates the steering wheel when the driver drifts away from the center by mistake
- Lane keeping assistance
    - Functionality that turns the steering wheel back towards the center of the lane if the driver starts to drift away from the center

Which subsystems are responsible for each function?
The camera subsystem is responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake.
The electronic power steering subsystem is responsible for measuring the torque provided by the driver and then adding an appropriate amount of torque based on the lane assistance system torque request.

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



Inside: Camera System, Electronic Power Steering System, Car Display System
Outside: Steering Wheel

Goals and Measures

Goals

The overall goal of the project is to make the vehicle safer. The lane keeping assistance functionality is inspected in detail and potential malfunctions are identified. Then new requirements are added in order to ensure a safe system.

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

Important points of my companies safety culture are:

- **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

<u>For the lane assistance project, the following safety lifecycle phases are in scope:</u>

- Concept phase
- Product Development at the System Level
- Product Development at the Software Level

<u>The following phases are out of scope:</u>

- 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

What is the purpose of a development interface agreement?
A DIA defines the roles and responsibilities between companies involved in developing a product. The ultimate goal is to ensure that all parties are developing safe vehicles in compliance with ISO 26262.

What will be the responsibilities of your company versus the responsibilities of the OEM?
The OEM is supplying a functioning lane assistance system.
Our company analyzes and modifies the various sub-systems from a functional safety viewpoint.

Confirmation Measures

- Confirmation measures report what will be done to prove that functional safety has been achieved.
- 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.
- Checking to make sure that the actual implementation of the project conforms to the safety plan.
- Confirming that plans, designs and developed products actually achieve 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.