Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
26.10.2017	1.0	Simon Ritzel	First Draft and Submission

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

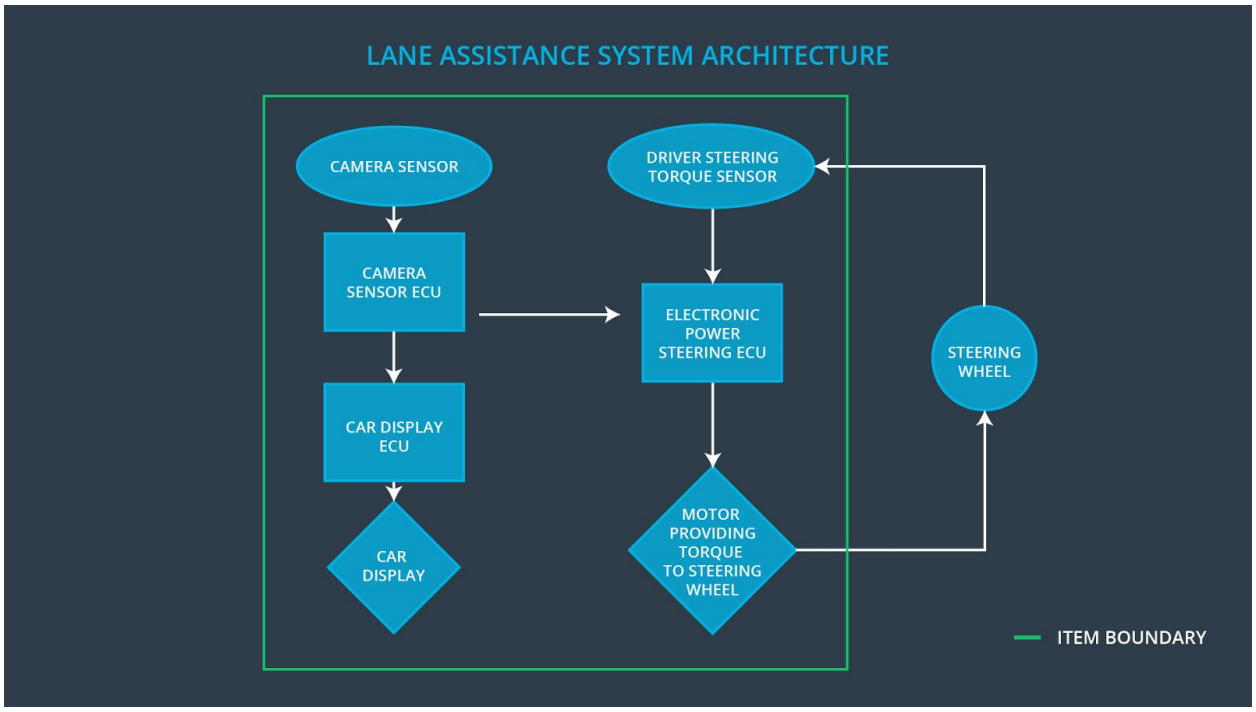
The Lane Assistance item alerts the driver that the vehicle has accidentally departed its lane and attempts to steer the vehicle back toward the center of the ego lane.

It will have two functions:

- Lane departure warning
- Lane keeping assistance

The lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback.
The lane keeping assistance function shall apply the steering torque when active in order to stay in ego lane.

The camera subsystem, the electronic power steering subsystem, and the car display system are all responsible for each of the functions.



Goals and Measures

Goals

The major goal is to reduce the risk of malfunction and therefore provide a safe operation of the lane assistance item in the vehicle. This will be ensured by compliance of the project to ISO 26262.

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

Here are some characteristics of a good 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

The Concept phase, Product Development at the System Level, and the Product Development at the Software Level are phases which are in the scope of the safety lifecycle. Whereas Product Development at the Hardware Level and Production and Operation are out of scope.

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

The purpose of a development interface agreement is to clarify responsibilities of the different parties involved in a functional safety project and who will be responsible for any safety issues in post-production, to describe the work products that each company will provide, and to avoid disputes between companies.

Our Company is going to analyze and modify the functioning lane assistance system and the various sub-systems from a functional safety viewpoint.
We will process this system based on the ISO 26262 regulations and provide prove of a successful audit by an independent party.

Confirmation Measures

The confirmation measures serve two purposes. That a functional safety project conforms to ISO 26262 and that the project really does make the vehicle safer.

A confirmation review is ensuring 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.

A functional safety audit is checking to make sure that the actual implementation of the project conforms to the safety plan.
A functional safety assessment is 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.