Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
02/03/2018	0.1	Michael Scharf	Initial version
02/03/2018	0.2	Michael Scharf	Fill out whole document
02/03/2018	1.0	Michael Scharf	First final version after internal review and fixing.
02/02018	2.0	Michael Scharf	After submission – correcting review findings

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 lane.

The Lane Assistance System will have two functions:

- Lane departure warning
- Lane keeping assistance

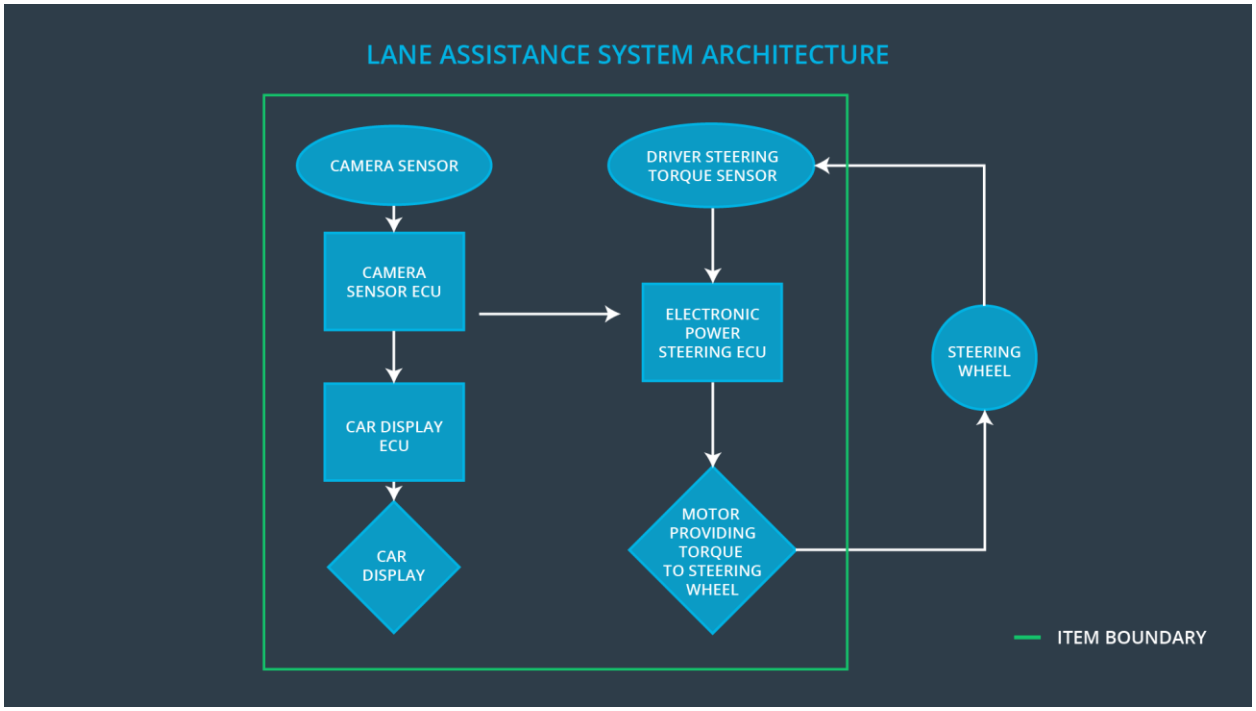
The lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback. The lane keeping assistance function shall apply the steering torque when active in order to stay in ego lane.

In other words, when the driver drifts towards the edge of the lane:

- the lane departure warning function will vibrate the steering wheel
- the lane keeping assistance function will move the steering wheel so that the wheels turn towards the center of the lane

There are three subsystems, all responsible for each the functions:

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



Goals and Measures

Goals

The main goal of this project and documentation is to reduce risk to acceptable levels. This will be done by identifying possible faults and failures in the system lifecycle and describing risk as well as counter measurements for these situations.

Measures

Measures and Activities	Responsibility	Timeline
Follow safety processes	All Team Members	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

Our Safety Culture is acting to the following characteristics and intentions
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

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

A DIA (development interface agreement) defines the roles and responsibilities between companies involved in developing a product. All involved parties need to agree on the contents of the DIA before the project begins.

The DIA also specifies what evidence and work products each party will provide to prove that work was done according to the agreement.

The ultimate goal is to ensure that all parties are developing safe vehicles in compliance with ISO 26262.

The responsibility of our company is to act as the Functional Safety Manager as well as the Functional Safety Engineer. This includes

- Planning, coordinating and documenting of the development phase of the safety lifecycle
- Tailors the safety lifecycle
- Maintains the safety plan
- Monitors progress against the safety plan
- Performs pre-audits before the safety auditor

As the Functional Safety Manager and

- Product development and prototyping
- Integration of sub systems
- Testing at the hardware, software and system levels

In the role as the Functional Safety Engineer.

Confirmation Measures

Our goal is to ensure that

- Processes comply with the functional safety standard (ISO 26262)
- Project execution is following the safety plan

- Design really does improve safety

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.

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

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.