Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

[Instructions: Fill in the date, version and description fields. You can fill out the Editor field with your name if you want to do so. Keep track of your editing as if this were a real world project.

For example, if this were your first draft or first submission, you might say version 1.0. If this is a second submission attempt, then you'd add a second line with a new date and version 2.0]

Date	Version	Editor	Description
6/2/2018	1.0	Ruixuan.li	First release

Table of Contents

Confirmation Measures

Introduction

Purpose of the Safety Plan

The purpose of the 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.

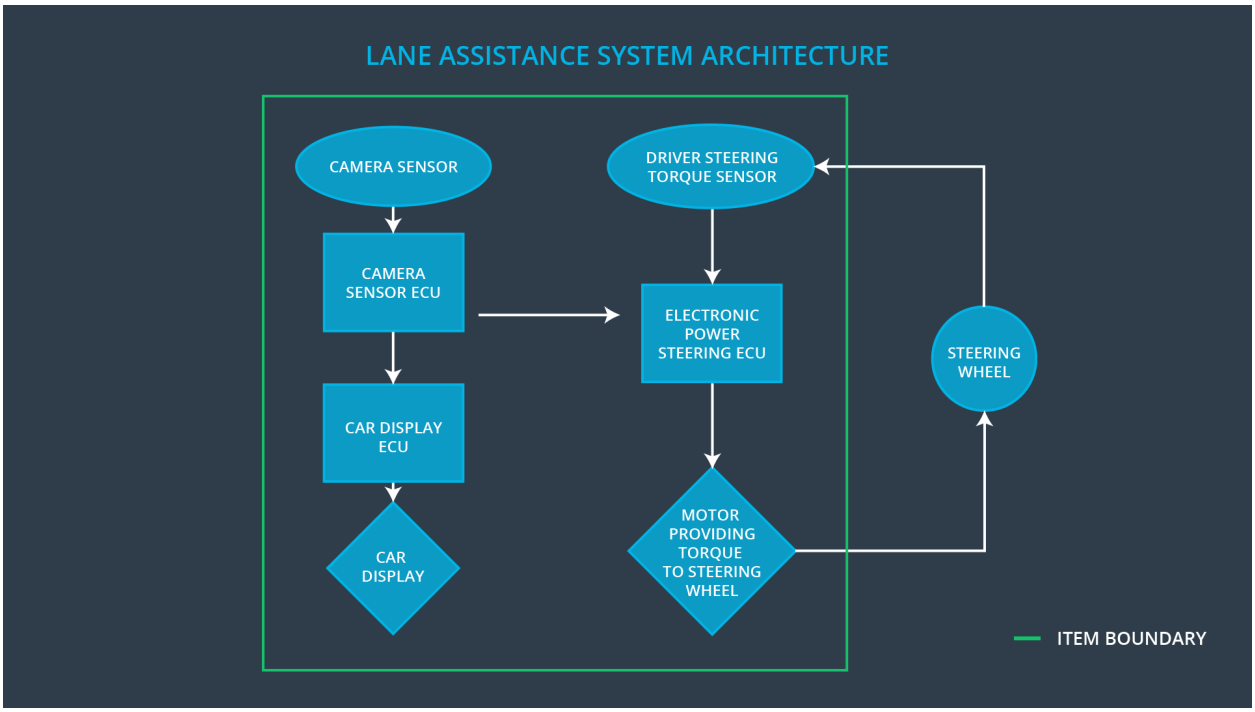
The Lane assistance system will have two functions:

1. Lane departure warning
2. 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 goals of this functional safety project are:

1. Identify the hazardous situation from electronic malfunctions that could cause injury to human or damage human health.
2. Assess the risk level of hazards
3. Lower the high risk level of hazardous situation to an acceptable risk level via system engineering.

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	Safety Manager	3 months prior to main assessment

external functional safety assessor		
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

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

The development interface agreement (DIA) defines the roles and responsibilities between companies involved in the product development. All involved parties need to agree on the contents of the DIA before 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 OEM shall be responsible for supplying a functioning lane assistance system. The tier-1 organization has following responsibilities:

1. Provide functional safety requirements.
2. Work with the OEM partner to develop safety plan to software and hardware level.
3. Validate and verify that the final product meets the functional safety requirements.

The responsibilities and personals of the tier-1 organization involved in the project include:

A Tier-1 program manager who will communicate with OEM partners on product schedule, resource allocation and component selections. Functional safety plan shall be provided to OEM partner at the beginning and ensure the confirmation of requirements by working with third party auditor and safety assessor.

Tier-1 Safety manager who will develop safety plan and work with OEM safety manager during the whole safety lifecycle.

The personal interfaces to tier-1 organization in the OEM team include:

- A project manager who will manage the resource to develop the lane assistance system based on the requirement provided by the vendor. The manager also communicates with vendor program manager on product requirement and development schedule.

- Safety manager who will work with tier-1 organization's safety manager to ensure the product confirms the safety requirement.

Confirmation Measures

The confirmation measures serve two purposes:

- The lane assistance system safety project conforms to ISO26262, and

- The project does make the vehicle safer.

The confirmation review ensures that the product compiles with ISO26262. As the product is developed, a third party safety auditor will review the work to ensure its compliance with standard. The functional safety audit will ensure the actual implementation of the project conforms to safety plan. The functional safety assessment will ensure that plans, designs and product development 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.