Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 2.0

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
11/12/2017	1.0	Sam Adelman	Started Editing
11/26/2017	2.0	Sam Adelman	Completed with information from the lessons

Table of Contents

[Instructions: We have provided a table of contents. If the table of contents is not showing up correctly in your word processor of choice, please update it. The table of contents should show each section of the document and page numbers or links. Most word processors can do this for you. In Google Docs, you can use headings for each section and then go to Insert > Table of Contents. Microsoft Word has similar capabilities]

Introduction

Purpose of the Safety Plan

This safety plan provides an overall framework for the functional safety of the Lane Assistance item. In addition, this document defines roles and responsibilities to ensure that all aspects of functional safety are covered.

Scope of the Project

[Instructions: Nothing to do here. This is for your information.]

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

[Instructions: Nothing to do here. This is for your information.]

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 System Item assists the driver operating the vehicle by helping the driver keep the car centered in the current travel lane. The Lane Assistance System will have two functions:

1. Lane departure warning
2. Lane keeping assistance

When the driver drifts towards the edge of the lane, two things will happen:

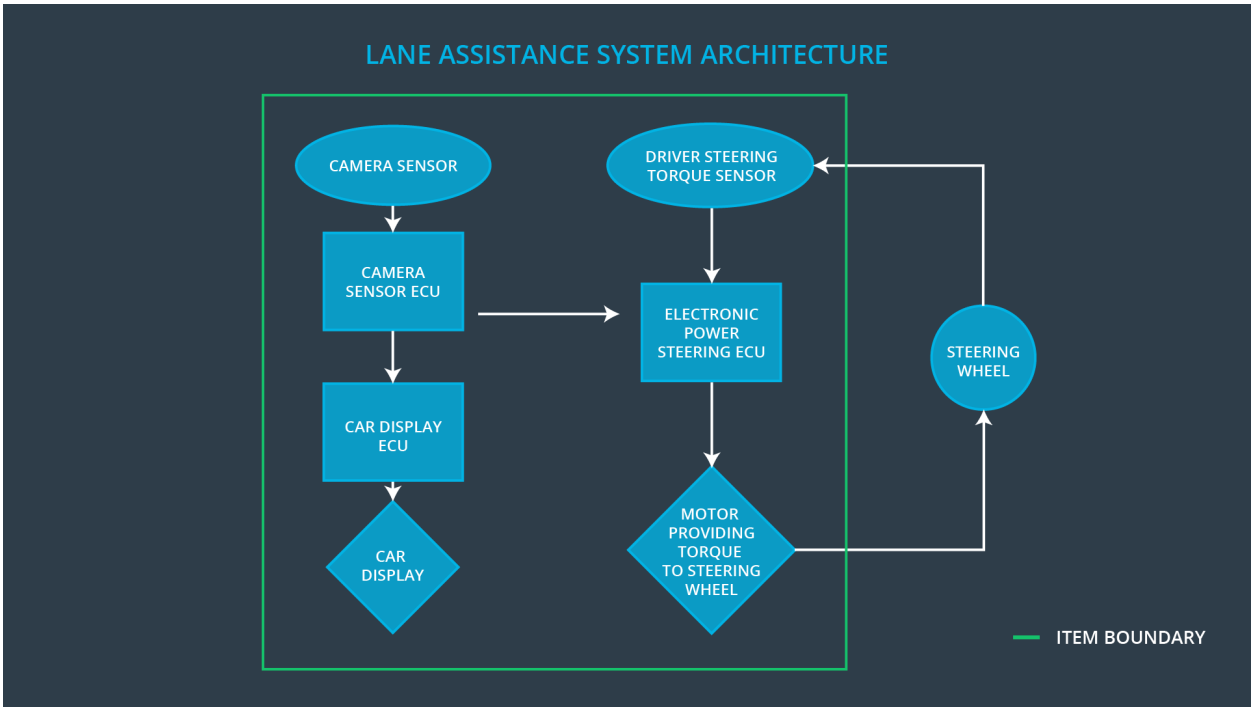
- "the lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback."
- "the lane keeping assistance function shall apply the steering torque when active in order to stay in ego lane".

This item includes three sub-systems:

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

The Steering Wheel, throttle, and other vehicle propulsion items are outside of the item boundary for this item.

The camera subsystem shall be responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake. The electronic power steering subsystem shall be responsible for measuring the torque provided by the driver and then adding an appropriate amount of torque based on a lane assistance system torque request. The car display system shall be responsible for providing visual feedback to the driver to notify them when the system is being engaged or when the system has been engaged for too long and is about to be disengaged.


LANE ASSISTANCE SYSTEM ARCHITECTURE
CAMERA SENSOR
CAMERA SENSOR ECU
CAR DISPLAY ECU
CAR DISPLAY
DRIVER STEERING TORQUE SENSOR
ELECTRONIC POWER STEERING ECU
MOTOR PROVIDING TORQUE TO STEERING WHEEL
STEERING WHEEL
ITEM BOUNDARY

Goals and Measures

Goals

The goal of this project is to create a safety plan to ensure functional safety for the Lane Assistance Item under ISO 26262.

Measures

Measures and Activities	Responsibility	Timeline
Follow safety processes	All Team Members	Constantly
Create and sustain a safety culture	All, esp. 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

- **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 Item we will be considering the following safety lifecycles:

- Concept Phase
- Product Development

This document will not consider: After the Release for Production.

Roles

[Instructions:
This section is here for your reference. You do not need to do anything here. It is provided to help with filling out the development interface agreement section.
]

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.

For this Item, the OEM will supply a functioning lane assistance system. Our company will analyze and modify the various sub-systems from a functional safety viewpoint. Specifically, we will perform pre-audits, plan the development phase, develop prototypes, and integrate these subsystems into the lane assistance system.

Confirmation Measures

Confirmation measures serve two purposes:

- that a functional safety project conforms to ISO 26262, and
- that the project really does make the vehicle safer.

The people who carry out confirmation measures need to be independent from the people who actually developed the project.

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 means checking to make sure that the actual implementation of the project conforms to the safety plan.

A Functional safety assessment is confirmation 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.