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
3/22/18	1.0	David G	First draft

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

To outline a safe architecture in regard to ISO 26262 for a lane assistance function onboard a passenger vehicle.

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

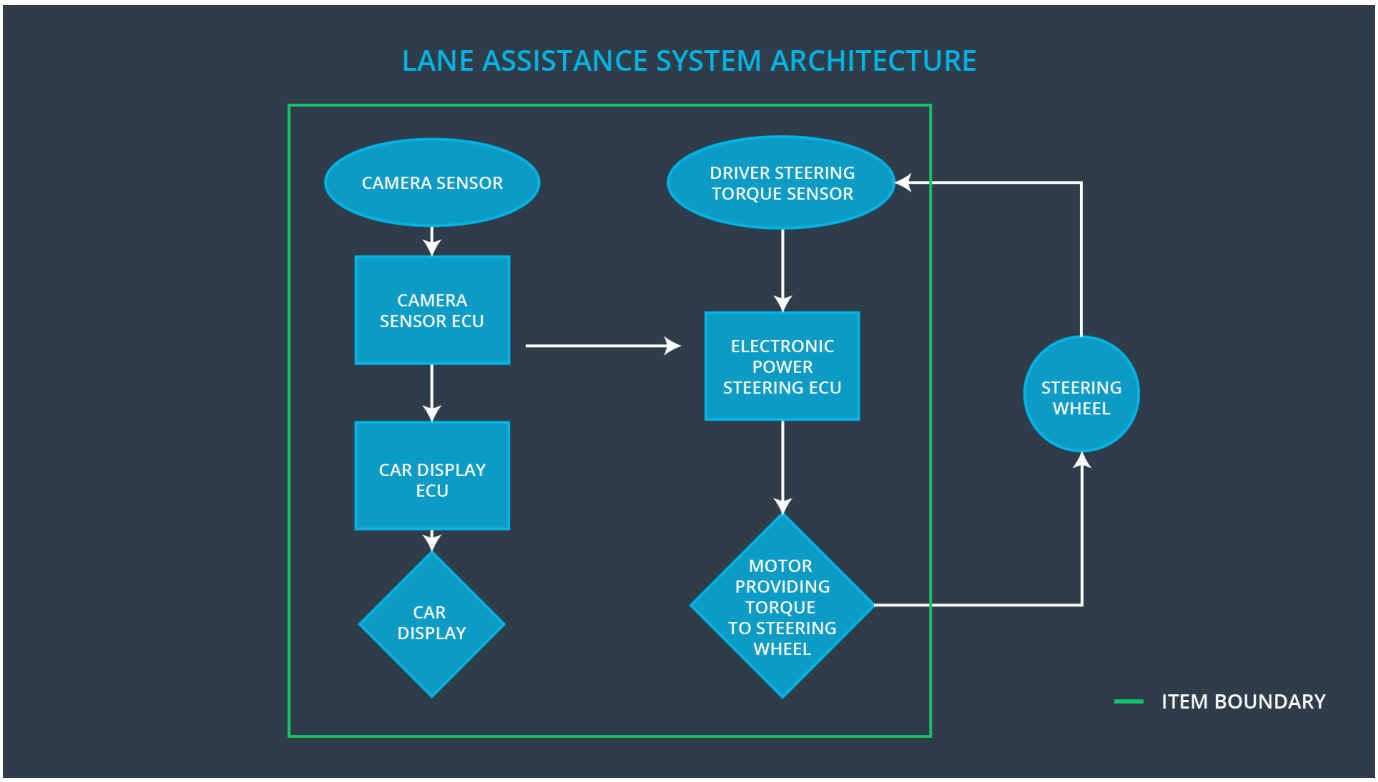
Item Definition

The item in question is a lane assistance function that provides a both LDW(Lane Departure Warning) and LKA(Lane Keeping Assistance) functionality:

- The functionality for the LDW system is that it monitors lanes on the road and provides vibrational torque to the steering wheel when the driver starts to depart from the ego lane.

- The functionality of the LKA function is that it also monitors lanes on the road, but provides steering torque to the wheel to help the driver steer back towards the center of the ego lane during accidental departure. An accidental lane departure is denoted by the driver's departure from a lane while not using a turn signal. The system will not attempt to steer towards the center of the lane in the event of turn signal use. It is worth noting that while the system can be used autonomously, it is not the intended purpose of the system. The functionality is to provide additional steering torque in combination with that of the driver to **assist** steering back to the center of the lane.

The lane assistance system architecture can be seen in this diagram:



A description of each subsystem's responsibilites can be seen in this chart:

Element	Description
Camera Sensor	Visual observation of driving surface for lane detection. Signal sent to camera sensor ecu.
Camera Sensor ECU	Lane sensing and torque request generator. Signal

	sent to electronic power steering ecu.
Car Display	Visual display to driver of LDW/LKA status from car display ecu.
Car Display ECU	From camera sensor ecu, receives LDW and LKA on/off status, active/inactive status, malfunction warning.
Driver Steering Torque Sensor	Measures driver torque input. Sends input to electronic power steering ecu.
Electronic Power Steering ECU	Recieves torque request from camera sensor ECU and driver torque sensor and computes amount of torque to request from the motor.
Motor	Recieves torque request from electronic power steering ecu and applies to steering wheel.

The lane assistance function involves every part of the system outlined in the diagram. It relies on each sub-system working in tandem to provide functional output.

Goals and Measures

Goals

The major goal is to identify hazards and risks with the system, and implement ways to reduce those risks. By conforming to ISO 26262 standards, we can create a safe and functional system.

Measures

Measures and Activities	Responsibility	Timeline
Follow safety processes	All Team Members	Constantly
Create and sustain a safety culture	All Team Members / 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 company strives to adhere to these guidelines on safety:

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.

Upon the OEM is supplying a functioning lane assistance system, our company will analyze and modify the various sub-systems from a functional safety viewpoint in accordance to ISO 26262.

Confirmation Measures

A confirmation review primarily serves the purpose of ensuring that a functional safety project conforms to ISO 26262, and that the project really does make the vehicle safer.

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

A functional safety assessment Confirms 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.