Elektrobit

UDACITY

Functional Safety Concept 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
14.11.2018	1.0	Suraj Lal Putta	Initial draft

Table of Contents

[Instructions: We have provided a table of contents. If you change the document structure, please update the table of contents accordingly. 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]

Purpose of the Functional Safety Concept

The functional safety concept refines the safety goals which were identified in the hazard and risk assessment analysis into functional safety requirements. Then the identified functional safety requirements are allocated to system parts which should fulfill the requirements.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	The oscillating torque provided by the lane departure warning (LDW) function shall be limited.
Safety_Goal_02	The lane keeping assistance function (LKA) shall provide additional steering torque for a limited time interval so that the driver cannot misuse the system for autonomous driving.

Preliminary Architecture

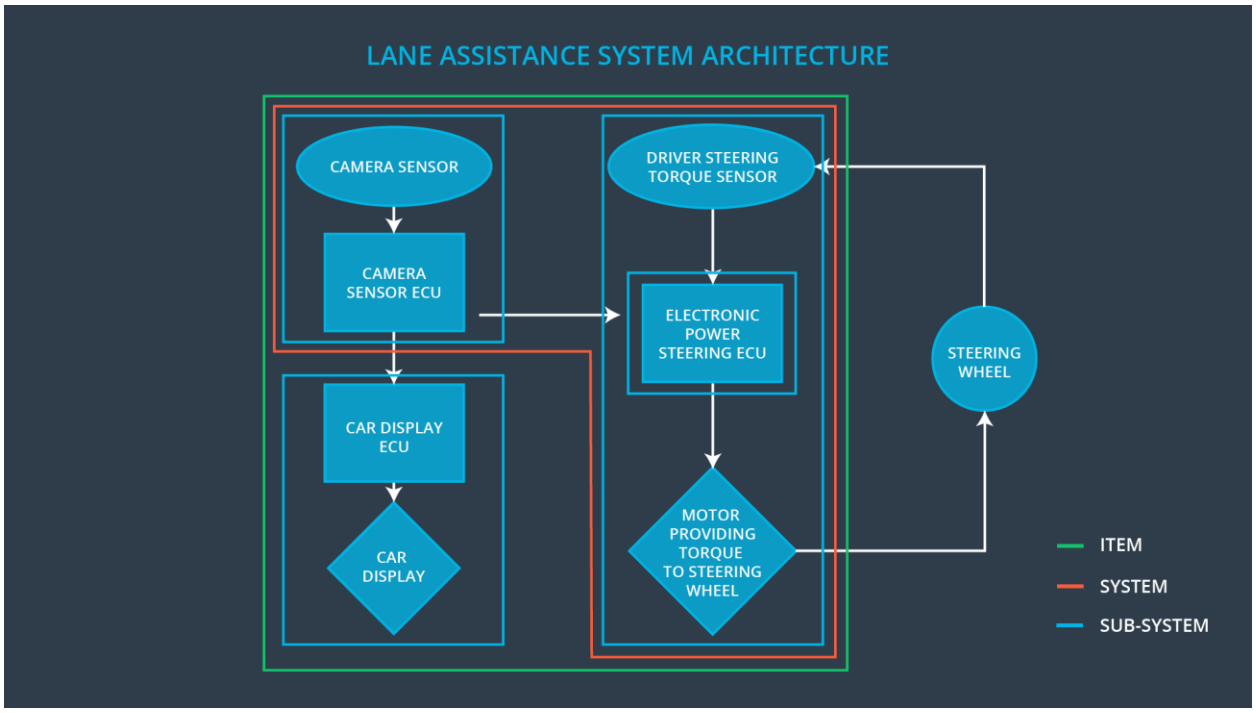

Figure 1: Preliminary Architecture of Lane Assistance Item

The above picture shows the preliminary architecture of the lane assistance item. It has three main sub-systems the camera system, electronic power steering system and the display system. The camera sub-system detects the position the vehicle in the relative to the lane boundary and detects if the vehicle is leaving the lane without driver's intention. The electric power steering sub-system provides the haptic feedback torque and the supporting steering to the steering wheel upon request from the camera sub-system. The display sub-system displays information to the drive about the status of the lane assistance item.

Description of architecture elements

Element	Description
Camera Sensor	The camera sensor is one of the main sensors of the lane assistance item. The camera sensor captures the image of the road ahead of the ego vehicle with the lane markings and sends it to camera sensor ECU.
Camera Sensor ECU	The camera senor ECU is one of controllers of the lane assistance item. It processes the image captured by the camera sensor to finds the position of the ego vehicle relative to the lane boundaries. And it detects when the vehicle leaves the lane without the driver's intention.
Car Display	The car display is the human machine interface (HMI) between the lane assistance item and the driver. It gives the information to the driver about the status of the lane assistance item. For example if the lane assistance functionalities are enabled or active, warning about the malfunctions of the lane assistance item.
Car Display ECU	The car display ECU receives information from the camera ECU and Power steering ECU about the status of the lane assistance item. Then it displays the respective information in the car display
Driver Steering Torque Sensor	Driving steering torque sensor is a part of the electric power steering sub-system. It detects the steering torque applied by the driver on the steering wheel. This information is sent to the power steering ECU
Electronic Power Steering ECU	Electronic power steering ECU is the controller for the power steering sub-system. The electronic power steering ECU calculates the supporting steering wheel torque for the lane keeping assistance function and the oscillating haptic feedback torque for the lane departure function. It controls the motor of the power steering.

Motor	The electric motor is connected to the steering wheel it provides the haptic feedback torque for LDW function and the supporting torque for the LKA function. It is controlled by the electronic power steering ECU.

Functional Safety Concept

The functional safety concept consists of:

- Functional safety analysis
- Functional safety requirements
- Functional safety architecture
- Warning and degradation concept

Functional Safety Analysis

Malfunction ID	**Main Function of the Item Related to Safety Goal Violations**	**Guidewords (NO, WRONG, EARLY, LATE, MORE, LESS)**	**Resulting Malfunction**
Malfunction_01	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	More	The lane departure warning function applies an oscillating torque with very high torque amplitude (above limit).
Malfunction_02	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	More	The lane departure warning function applies an oscillating torque with very high torque frequency (above limit).
Malfunction_03	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	No	The lane keeping assistance function is not limited in time duration which leads to misuse as an autonomous driving function.

Functional Safety Requirements

Lane Departure Warning (LDW) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	The lane assistance item shall ensure that the lane departure oscillating torque amplitude is below “Max_Torque_Amplitude”.	C	50ms	The lane departure warning function is turned off.
Functional Safety Requirement 01-02	The lane assistance item shall ensure that the lane departure oscillating torque frequency is below “Max_Torque_Frequency”.	C	50ms	The lane departure warning function is turned off.

Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria:

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Functional Safety Requirement 01-01	The Max_Torque_Amplitude is validated by testing how different drivers react to different Max_Torque_Amplitude values.	The lane assistance item should turn off lane departure warning within 50ms when the oscillating torque amplitude crosses the Max_Torque_Amplitude value. The requirement is verified by injecting a fault into the system in the software test.
Functional Safety Requirement 01-02	The Max_Torque_Frequency is validated by testing how different drivers react to different Max_Torque_Frequency values.	The lane assistance item should turn off lane departure warning within 50ms when the oscillating torque frequency crosses the Max_Torque_Frequency value. The requirement is verified by injecting a fault into the system in the software test.

Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only “Max_Duration”.	B	500ms	The lane keeping assistance function is turned off.

Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Functional Safety Requirement 02-01	The Max_Duration value is validated by conducting tests with different drivers with different Max_Duration values. An appropriate value of Max_Duration is chosen based on the driver’s reaction in the tests.	The lane assistance item should turn off the lane keeping assistance functionality within 500ms when the additional steering torque is provided for duration longer than Max_Duration. The requirement is verified by injecting a fault into the system in the software test.

Refinement of the System Architecture

The Figure 2 shown below contains the refined architecture of the lane assistance item. Compared the architecture diagram shown before here more details are present for the Camera ECU, Display ECU and Electronic Power Steering ECU. Also the ASIL levels of the functional safety requirements are allotted to the components in the refined architecture. The details in the architecture are based on the functional safety requirements. The camera sensor ECU has to software blocks lane sensing and torque request generator. The lane sensing software block detects the position of lanes from the captured image whereas the torque request generator calculates the steering oscillating torque for LDW and supporting steering torque for LKA function. The car display ECU has two software block lane assistance on/off status and the lane assistance active/inactive status. The Electronic Power Steering ECU has four software blocks “Normal Lane Assistance Functionality” which identifies faults in the system when it violates safety goals of the LDW and LKA functions, which processes the steering torque for the lane assistance item, the “LA Safety Functionality” the “Driver Steering Torque” software block which processes the steering torque from the driver and “Final Torque” software block which combines the steering torque from the driver and the lane assistance item. It can be seen that all the components belonging to the electronic power steering sub-system are assigned with ASIL C

except for “Normal LA Functionality” because all the functional safety requirements are assigned to the electronic power steering ECU. The lane assistance function in the power steering ECU is split into two software blocks; where one block contains normal functionality with ASIL QM(C) level and the other with safety functionality with ASIL C level. The ASIL level for normal functionality is reduced by decomposing the safety functionality to a different component because it is easier to develop complex software with lower ASIL level. The remaining components in the car display sub-system and camera sub-system are assigned to QM.

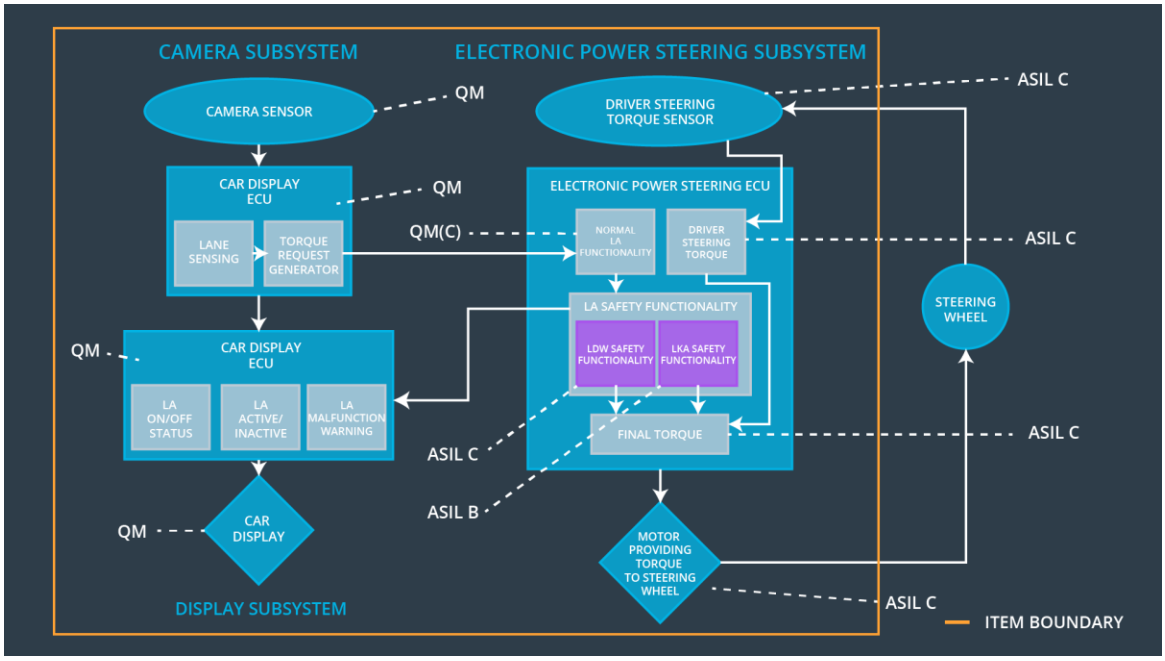

Figure 2: Refined Architecture Lane Assistance Item

Allocation of Functional Safety Requirements to Architecture Elements

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 01-01	The lane assistance item shall ensure that the lane departure oscillating torque amplitude is below “Max_Torque_Amplitude”	**Yes**	**No**	**No**
Functional Safety Requirement 01-02	The lane assistance item shall ensure that the lane departure oscillating torque frequency is	**Yes**	**No**	**No**

	below “Max_Torque_Frequency”			
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only “Max_Duration”.	**Yes**	**No**	**No**

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	LDW function turned off	The amplitude or frequency of the oscillating steering torque is greater than Max_Torque_Amplitude or Max_Torque_Frequency.	Yes	Warning lamp turned on
WDC-02	LKA function turned off	The steering torque is provided longer than Max_Duration.	Yes	Warning lamp turned on