



Elektrobit



UDACITY

Functional Safety Concept Lane Assistance

Document Version: [1.0]

Template Version 1.0, Released on 2018-05-24



Document history

Date	Version	Editor	Description
2018-05-22	1.0	Aman Gupta	Initial version

Table of Contents

[Document history](#)

[Table of Contents](#)

[Purpose of the Functional Safety Concept](#)

[Inputs to the Functional Safety Analysis](#)

[Safety goals from the Hazard Analysis and Risk Assessment](#)

[Preliminary Architecture](#)

[Description of architecture elements](#)

[Functional Safety Concept](#)

[Functional Safety Analysis](#)

[Functional Safety Requirements](#)

[Refinement of the System Architecture](#)

[Allocation of Functional Safety Requirements to Architecture Elements](#)

[Warning and Degradation Concept](#)

Purpose of the Functional Safety Concept

The functional safety concept is a high level approach to look at the general functionality of the item without going into technical detail. The goal is to identify safety requirements and then allocate those requirements to different parts of the item architecture. From the result of the functional safety concept technical safety requirements can be derived within a subsequent technical safety concept. Functional safety requirements also have attributes that are specified in the functional safety concept. Finally to prove that a system actually meets requirements, they have to be verified and validated.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	The oscillating steering torque from the lane departure warning (LDW) function shall be limited.
Safety_Goal_02	lane keeping assistance (LKA) function shall be time limited and the additional steering torque shall end after a given timer interval so that the driver can not misuse the system for autonomous driving.

Preliminary Architecture

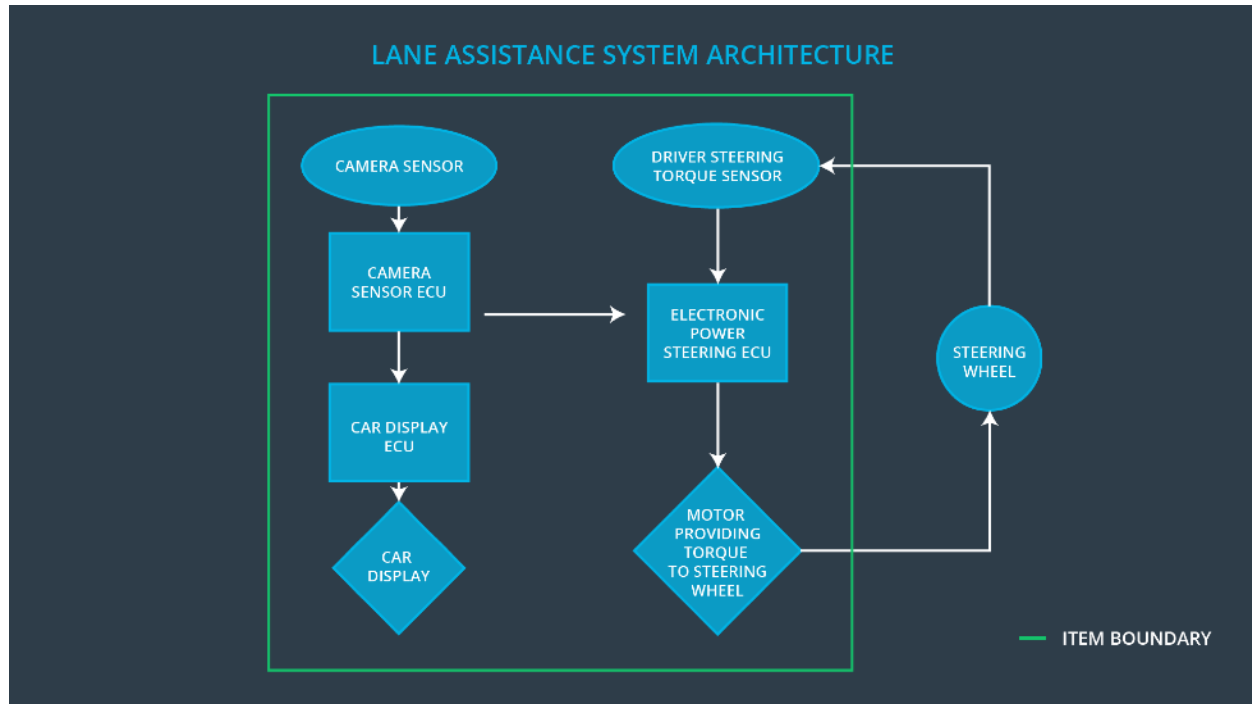


Fig 1.0 Describes the preliminary architecture for the lane assistance item

Description of architecture elements

Element	Description
Camera Sensor	Provides camera images to the Camera Sensor ECU.
Camera Sensor ECU	Detects laneline positions from camera images and generates a torque request to the Electronic Power Steering ECU.

Car Display	Shows warning to driver.
Car Display ECU	Generates warning signals triggered by input from Camera Sensor ECU and Electronic Power Steering ECU.
Driver Steering Torque Sensor	Delivers steering torque intensity provided by driver to Electronic Power Steering ECU.
Electronic Power Steering ECU	Processes inputs from Camera Sensor ECU, Driver Steering Torque Sensor and computes appropriate Lane Assistance functionality resulting in final torque which is transferred to the steering wheel motor.
Motor	Receives final torque calculated by Electronic Power Steering ECU and applies it to steering wheel.

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	A S IL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below MAX_Torque_Amplitude	C	50 ms	Lane Assistant functionality off
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque <i>frequency</i> is below Max_Torque_Frequency	C	50 ms	Lane Assistant functionality 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	Test how drivers react to different torque amplitudes to prove that an appropriate value was chosen.	Verify that system turns off if LKA ever exceeds Max_Torque_Amplitude.

Functional Safety Requirement 01-02	Test how drivers react to different torque frequencies to prove that an appropriate value was chosen.	Verify that system turns off if LKA ever exceeds Max_Torque_Frequency.
-------------------------------------	---	--

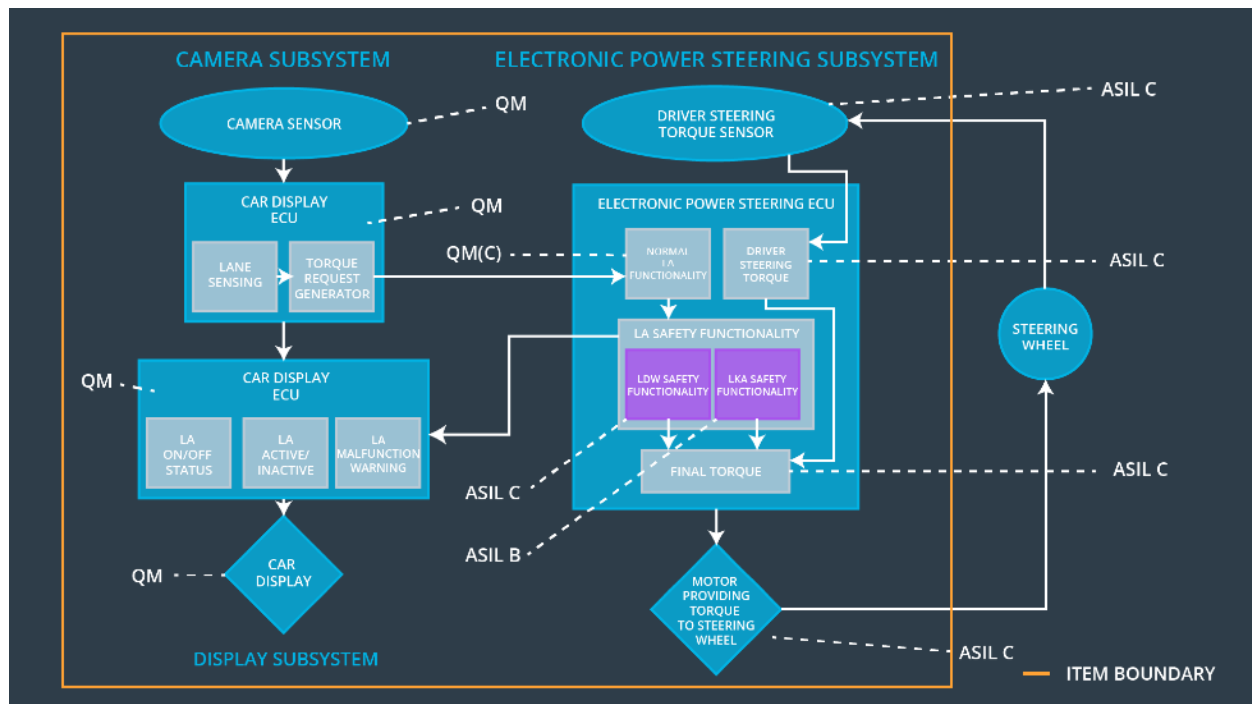
Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	A S IL	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	500 ms	Set lane keeping assistance torque to zero
Functional Safety Requirement 02-02	The electronic power steering ECU shall ensure that the lane keeping assistance torque is set to zero when the camera sensor ECU stops detecting road markings and shall send its off status to the Car Display.	B	500 ms	Set lane keeping assistance torque to zero

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	<p>Acceptance Criteria : Max_Duration shall be sufficient enough to provide enough feedback to driver and simultaneously not allowing him/her to misuse as Autonomous driving</p> <p>Method: Validation at vehicle level</p>	<p>Acceptance Criteria : the LDW function shall deactivate after MAX_Duration</p> <p>Method: testing at vehicle level</p>
Functional Safety Requirement 02-02	<p>Acceptance Criteria : The direction of the additional torque shall be always in the same direction as steering wheel</p> <p>Method: Validation at vehicle level</p>	<p>Acceptance Criteria : test whether the direction of additional torque is same as that of the steering wheel direction</p> <p>Method: testing at vehicle level</p>

Refinement of the System Architecture



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 Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	X		

Functional Safety Requirement 01-02	The Lane Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Frequency.	x		
Functional Safety Requirement 02-01	The Lane Keeping Assistance function shall be time limited, and additional steering torque shall end after a given time interval so the driver cannot misuse the system for autonomous driving.	x		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off LDW functionality	Malfunction_01 Malfunction_02	Yes	Lane departure warning malfunction Warning will be set in the Car Display ECU

WDC-02	Turn off LKA functionality	Malfunction_03	Yes	Lane Keeping Assist malfunction Warning will be set in the Car Display ECU
--------	----------------------------	----------------	-----	--