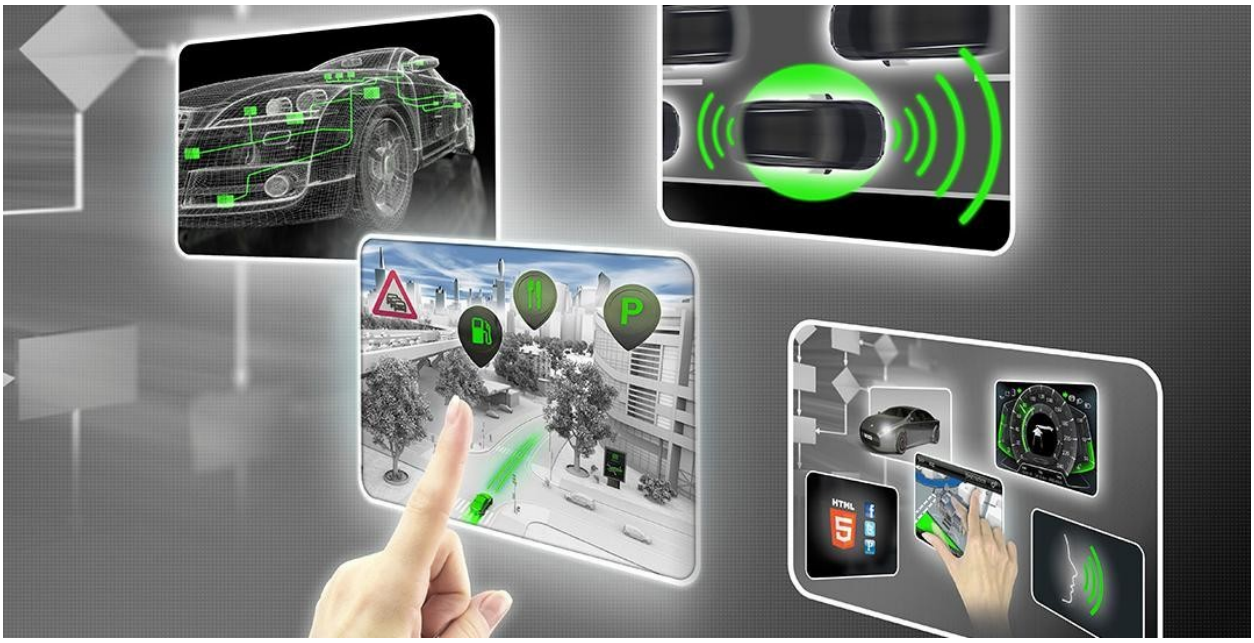
Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.1

Template Version 1.0, Released on 2017-06-21



Document history

Date	Version	Editor	Description
4/12/2018	1.0	Sara Mostafa	Intial version
6/12/2018	1.1	Sara Mostafa	Updated safe state of LKA and LDW safety requirements

Table of Contents

Purpose of the Functional Safety Concept

The purpoae of thia document is to define the functional safety concepts of LKA and LDW system.

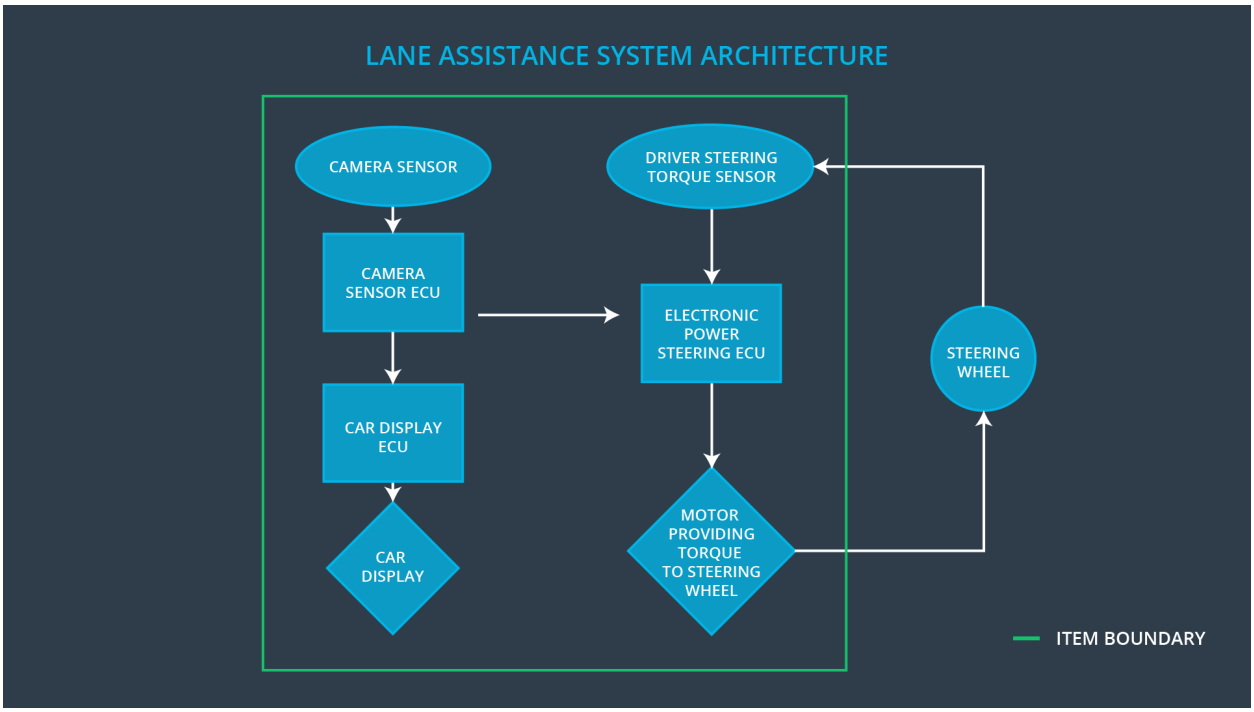
Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	The oscillating steering torque from LDW shall be limited.
Safety_Goal_02	LKA shall be time limited so that the lane keeping assistance function should only work for a certain amount of time.
Safety_Goal_03	LKA shall be deactivated if sensors can’t detect unlaned roads LKA Lamp should be blink to indicate driver that system is deactivated.
Safety_Goal_04	LKA system shall be deactivated in case of false detection.

Preliminary Architecture

[Instructions: Provide a preliminary architecture for the lane assistance item. Hint: See Lesson 3: Item Definition]



Description of architecture elements

Element	Description
Camera Sensor	Responsible for capturing and streaming road images.
Camera Sensor ECU	Responsible for detecting lanes in the images taken by Camera sensor and lane sensing and generate torque request.
Car Display	Responsible for dispaying light indicators to driver.
Car Display ECU	Responsible for Controlling light telling the driver if lane assistance feature is on or off , also control light that telling the driver if the lane departure warning is activated.
Driver Steering Torque Sensor	Responsible of measuring how much the driver is turning the steering wheel.
Electronic Power Steering ECU	Responsible of analysis of driver steering torque , recieving torque request generator from camera sensor ecu and output final steering torque to Motor.
Motor	Responsible for providing torque 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). (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
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 keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	Vibration torque amplitude less than Max_Torque_Amplitude.
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_frequency	C	50 ms	Vibration torque amplitude less than Max_Torque_frequency.

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	**validate** that we chose a reasonable value of max torque amplitude. We would need to test how drivers react to different torque amplitudes to prove that we chose an appropriate value.	**verify** that the safety requirement is met; when the torque amplitude crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval.
Functional Safety Requirement 01-02	**validate** that we chose a reasonable value of max torque frequency. We would need to test how drivers react to different torque frequencies to prove that we chose an appropriate value.	**verify** that the safety requirement is met; when the torque frequency crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval.

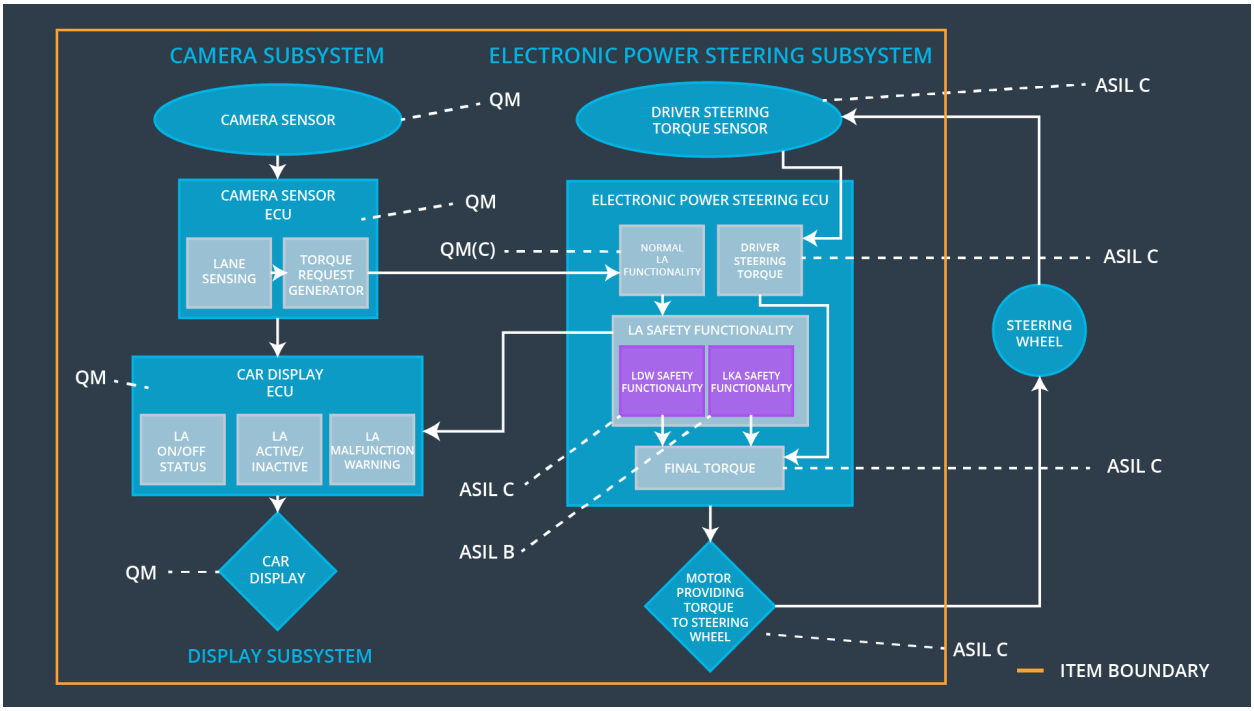
Lane Keeping Assistance (LKA) Requirements:

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	500	LKA torque set 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	validate that the max_duration chosen really did dissuade drivers from taking their hands off the wheel.	verify that the system really does turn off if the lane keeping assistance every exceeded max_duration.

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 keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	**x**	**-**	**-**
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_frequency	**x**	**-**	**-**
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	**x**	**-**	**-**

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off lane Assistant functionality	Malfunction_01	Yes	Lane Assistant Malfunction warning in the car.
WDC-02	Turn off lane Assistant functionality	Malfunction_02	Yes	Lane Assistant Malfunction warning in the car.
WDC-03	Turn off lane Assistant functionality	Malfunction_03	Yes	Lane Assistant Malfunction warning in the car.