Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
2018-06-04	v0.9	Csathó, Csaba	First draft
2018-06-21	v1.0	Csathó, Csaba	Final version

Table of Contents

Contents

Purpose of the Technical Safety Concept

The purpose of the technical safety concept is to refine the functional safety requirements documented in the functional safety concept into technical safety requirements. New requirements are defined and assigned to the given parts of the system architecture.

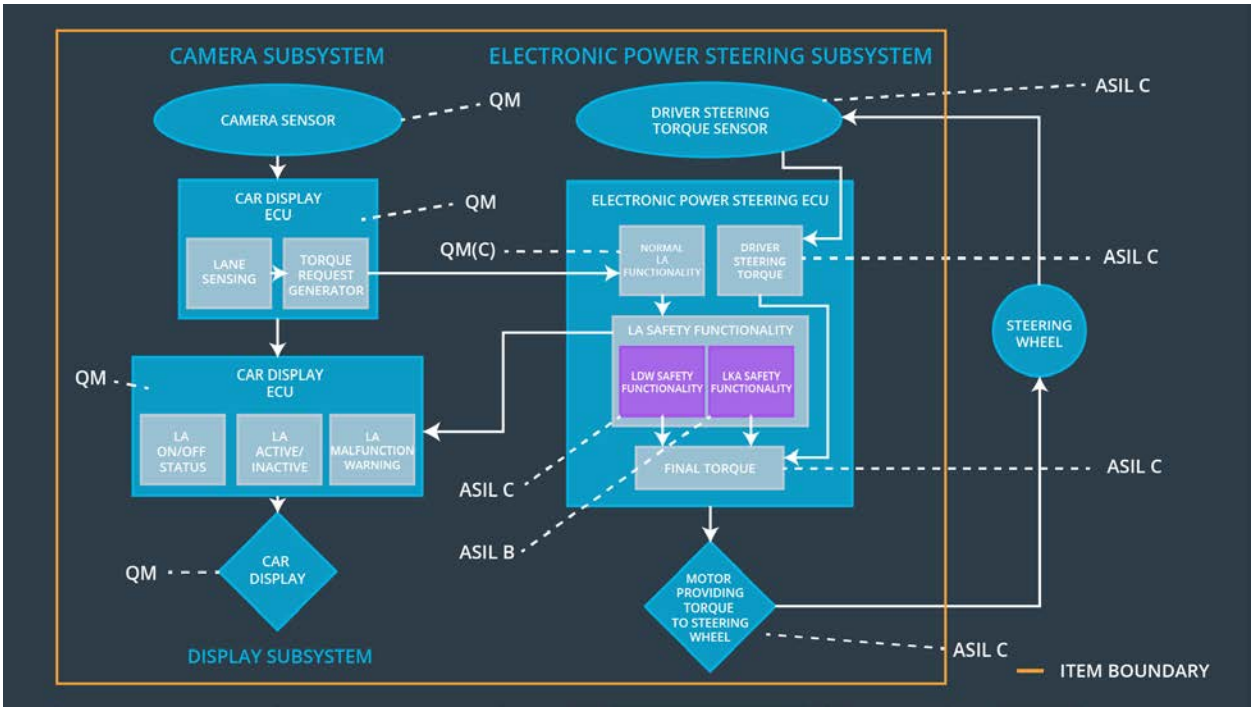
Inputs to the Technical Safety Concept

Functional Safety Requirements

F/S ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Intv.	Safe State
Requirement 01-01	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below `Max_Torque_Amplitude`	C	50 ms	limit torque amplitude
Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below `Max_Torque_Frequency`	C	50 ms	limit torque frequency
Requirement 01-03	If the camera sensor becomes unreliable the LDW system shall be deactivated.	C	25 ms	turn off the complete LDW functionality
Requirement 02-01	The item shall ensure that the LKA applies the torque for only `Max_Duration` timespan.	B	500 ms	does not apply any torque
Requirement 02-02	If the camera sensor becomes unreliable the LKA system shall be deactivated.	C	25 ms	turn off the complete LKA functionality

Refined System Architecture from Functional Safety Concept

System Diagram after Adding Extra Safety Elements



Functional overview of architecture elements

Element	Description
Camera Sensor	Optical sensor for observing lane lines.
Camera Sensor ECU – Lane Sensing	Processes image data from above and detects lane line positions.
Camera Sensor ECU – Torque request generator	Issues a torque request to the Electronic Power Steering ECU based on the information above.
Car Display	Vehicle dashboard that provides feedback of the car's status to the driver (e.g. displaying warnings sings of the LKA/LDW).
Car Display ECU – Lane Assistance On/Off Status	Indicates the On/Off status of the Lane Assistance functionality.
Car Display ECU – Lane Assistance Active/Inactive	Indicates the Active/Inactive state of the Lane Assistance functionality.
Car Display ECU – Lane Assistance malfunction warning	Indicates warnings or fault of the Lane Assistance functionality.
Driver Steering Torque Sensor	Measures the torque applied to the steering wheel by the driver.
Electronic Power Steering (EPS) ECU – Driver Steering Torque	Software module processing the driver's torque request coming from the steering wheel
EPS ECU – Normal Lane Assistance Functionality	Receives torque request from Camera Sensor ECU and forwards them to the Safety Lane Assistance Functionality.
EPS ECU – Lane Departure Warning Safety Functionality	Software module that is making sure that the torque amplitude is below `Max_Torque_Amplitude` and torque frequency is below `Max_Torque_Frequency`.
EPS ECU – Lane Keeping Assistant Safety Functionality	Software module that is making sure that the LKA functionality is not activate more than `Max_duration` time.
EPS ECU – Final Torque	A software value of the final torque which should be output to the EPS Motor based on both the Lane Assistance Function and the driver steering torque.
Motor	Receives the request from above and applies it to steering wheel.

Technical Safety Concept

Technical Safety Requirements

Lane Departure Warning (LDW) Requirements

Functional Safety Requirements 01-01/02/03 with its associated system elements (derived in the functional safety concept)

F/S ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Requirement 01-01	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below `Max_Torque_Amplitude`	X	—	—
Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below `Max_Torque_Frequency`	X	—	—
Requirement 01-03	If the camera sensor becomes unreliable the LDW system shall be deactivated.	X	—	—

Technical Safety Requirements related to Functional Safety Requirement **01-01/02/03** are …

T/S ID	Functional Safety Requirement	ASIL	F/Tol. Time Intv.	Safe State
Requirement 01-01-01	The *LDW safety component* shall ensure that the amplitude of the `LDW_Torque_Request` sent to the *Final Electronic Powersteering Torque Component* is below `Max_Torque_Amplitude`.	C	50 ms	LDW torque is set to zero
Requirement 01-02-01	The *LDW safety component* shall ensure that the frequency of the `LDW_Torque_Request` sent to the *Final Electronic Powersteering Torque Component* is below `Max_Torque_Frequency`.	C	50 ms	LDW torque is set to zero
Requirement 01-03-01	The *LDW safety component* shall ensure that the `LDW_Torque_Request`-s received from the Camera ECU are valid – that is, the camera is not malfunctioning or occluded.	C	25 ms	LDW torque is set to zero
Requirement 01-01-02 01-02-02 01-03-02	If and when the LDW is deactivated, the *LDW Safety Component* software module shall send a signal to the Car Display ECU to show a warning signal.	C	50 ms	LDW torque is set to zero

Requirement 01-01-03 01-02-03 01-03-03	When a failure is detected by the LDW function, it shall deactivate the LDW feature and the `LDW_Torque_Request` shall be set to zero.	C	50 ms	LDW torque is set to zero
Requirement 01-01-04 01-02-04 01-03-04	The validity and integrity of the data transmission for `LDW_Torque_Request` signal shall be ensured.	C	50 ms	LDW torque is set to zero
Requirement 01-01-05 01-02-05 01-03-05	Memory test shall be conducted at startup of the EPS ECU in order to rule out any faults in the memory module.	A	Ignition cycle timespan	LDW torque is set to zero

Lane Keeping Assistance (LKA) Requirements:

Functional Safety Requirements 02-01/02 with its associated system elements
(derived in the functional safety concept)

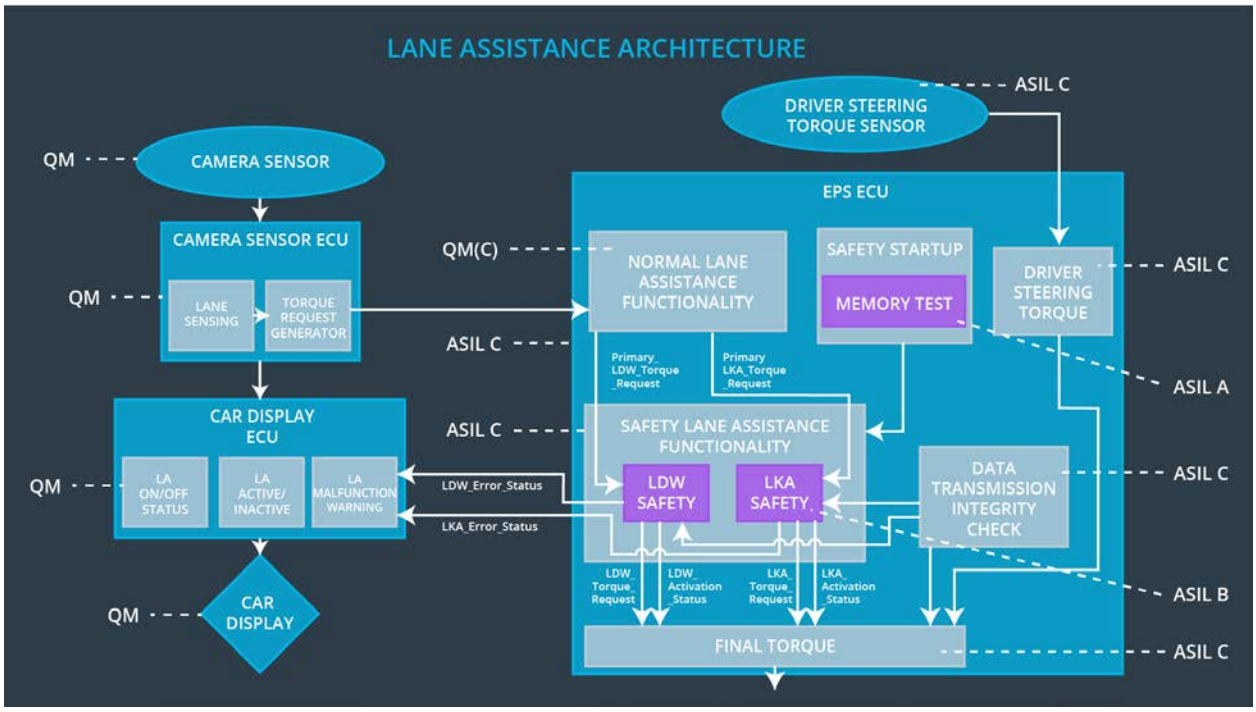
F/S ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Requirement 02-01	The item shall ensure that the LKA applies the torque for only `Max_Duration` timespan.	X	—	—
Requirement 02-02	If the camera sensor becomes unreliable the LKA system shall be deactivated.	X	—	—

Technical Safety Requirements related to Functional Safety Requirement **02-01/02** are …

T/S ID	Functional Safety Requirement	ASIL	F/Tol. Time Intv.	Safe State
Requirement 02-01-01	The *LKA safety component* shall ensure that the duration of the active LKA torque is applied for less than `Max_Duration`.	B	500 ms	LKA torque is set to zero
Requirement 02-02-01	The *LKA safety component* shall ensure that the `LKA_Torque_Request`-s received from the Camera ECU are valid – that is, the camera is not malfunctioning or occluded.	C	25 ms	LKA torque is set to zero
Requirement 02-01-02 02-02-02	If and when the LKA is deactivated, the *LKA Safety Component* software module shall send a signal to the Car Display ECU to show a warning signal.	B	500 ms	LKA torque is set to zero
Requirement 02-01-03 02-02-03	When a failure is detected by the LKA function, it shall deactivate the LKA feature and the `LKA_Torque_Request` shall be set to zero.	B	500 ms	LKA torque is set to zero
Requirement 02-01-04 02-02-04	The validity and integrity of the data transmission for `LKA_Torque_Request` signal shall be ensured.	B	500 ms	LKA torque is set to zero
Requirement 02-01-05 02-02-05	Memory test shall be conducted at startup of the EPS ECU in order to rule out any faults in the memory module.	A	Ignition cycle timespan	LKA torque is set to zero

Refinement of the System Architecture

Refined System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

All technical safety requirements were allocated to the EPS ECU. For the particular allocation within the EPS ECU compare the Technical Requirement tables above.

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 Malfunction_05	yes	“LDW Malfunction” sign shows on the Car Display
WDC-02	Turn off LKA functionality	Malfunction_03 Malfunction_04	yes	“LKA Malfunction” sign shows on the Car Display