Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 1.0
Released on 2018-05-22

Document history

Date	Version	Editor	Description
2018-05-22	1.0		Technical safety requirement document

Table of Contents

Document history

Table of Contents

Purpose of the Technical Safety Concept

Inputs to the Technical Safety Concept
- Functional Safety Requirements
- Refined System Architecture from Functional Safety Concept
  - Functional overview of architecture elements

Technical Safety Concept
- Technical Safety Requirements
- Refinement of the System Architecture
- Allocation of Technical Safety Requirements to Architecture Elements
- Warning and Degradation Concept

Purpose of the Technical Safety Concept

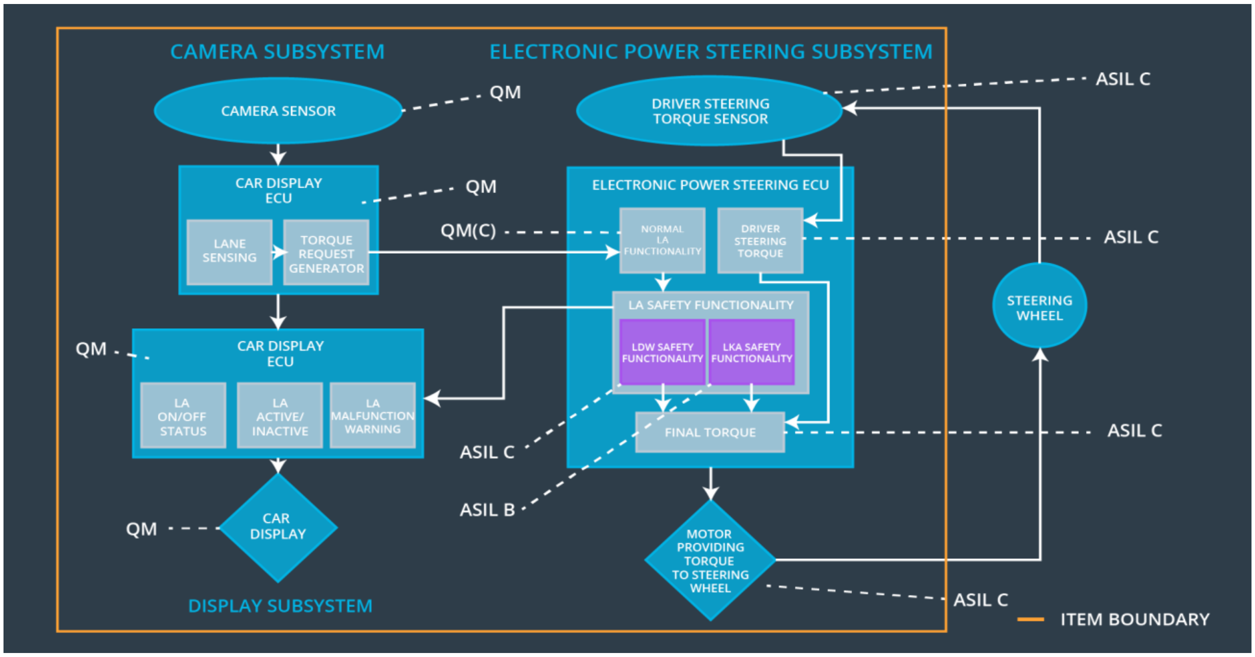
Purpose of technical safety concept is to convert functional safety requirements into technical safety requirements and assign those requirements to system architecture.

Inputs to the Technical Safety Concept

Functional Safety 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	Torque amplitude set to 0
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	Torque frequency set to 0
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	B	500 ms	Steering torque set to 0

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Sends camera images to camera sensor ECU
Camera Sensor ECU - Lane Sensing	Identifies lanes in camera images
Camera Sensor ECU - Torque request generator	Generates torque requests and sends to EPS ECU
Car Display	Displays warning
Car Display ECU - Lane Assistance On/Off Status	Sends display request to car display according to Lane Assistance system on/off status
Car Display ECU - Lane Assistant Active/Inactive	Sends display request to car display according to Lane Assistance system active/inactive status
Car Display ECU - Lane Assistance malfunction warning	Sends display request to car display according to Lane Assistance system malfunction status
Driver Steering Torque Sensor	Monitors torque applied by the driver
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Receives and processes input from Driver steering torque sensor
EPS ECU - Normal Lane Assistance Functionality	Receives torque request from camera sensor, checks it with input from driver steering torque sensor and sends appropriate torque request to Lane Departure Warning Safety functionality
EPS ECU - Lane Departure Warning Safety Functionality	Checks if Lane Departure Warning functionality is malfunctioning or not and sends torque request based on that.
EPS ECU - Lane Keeping Assistant Safety Functionality	Checks if Lane Keeping Assistance functionality is malfunctioning or not and sends torque request based on that.
EPS ECU - Final Torque	Sends final torque to motor
Motor	Applies received final torque to steering wheel.

Technical Safety Concept

Technical Safety Requirements

Lane Departure Warning (LDW) Requirements:

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

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		

Technical Safety Requirements related to Functional Safety Requirement 01-01 are:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 01	The LDW safety component shall ensure that the amplitude of the 'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Amplitude.	C	50 ms	LDW safety block	LDW torque is zero
Technical Safety Requirement 02	As soon as the LDW function deactivates the LDW feature, the 'LDW Safety' software block shall send a signal to the car display ECU to turn on a warning light.	C	50 ms	LDW safety block	LDW torque is zero
Technical Safety	As soon as a failure is detected by the LDW function, it shall	C	50 ms	LDW safety block	LDW torque is zero

Requirement 03	deactivate the LDW feature and the 'LDW_Torque_Request' shall be set to zero.				
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50 ms	Data transmission integrity check block	LDW torque is zero
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	ignition cycle	Memory test block	LDW torque is zero

Functional Safety Requirement 01-2 with its associated system elements (derived in the functional safety concept)

ID	**Functional Safety Requirement**	**Electronic Power Steering ECU**	**Camera ECU**	**Car Display ECU**
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	X		

Technical Safety Requirements related to Functional Safety Requirement 01-02 are:

ID	**Technical Safety Requirement**	**ASIL**	**Fault Tolerant Time Interval**	**Architecture Allocation**	**Safe State**
Technical Safety Requirement 01	The LDW safety component shall ensure that the frequency of the 'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Frequency.	C	50 ms	LDW safety block	LDW torque is zero

Technical Safety Requirement 02	As soon as the LDW function deactivates the LDW feature, the 'LDW Safety' software block shall send a signal to the car display ECU to turn on a warning light.	C	50 ms	LDW safety block	LDW torque is zero
Technical Safety Requirement 03	As soon as 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 safety block	LDW torque is zero
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50 ms	Data transmission integrity check block	LDW torque is zero
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Memory test block	LDW torque is zero

Lane Keeping Assistance (LKA) Requirements:

Functional Safety Requirement 02-1 with its associated system elements
(derived in the functional safety concept)

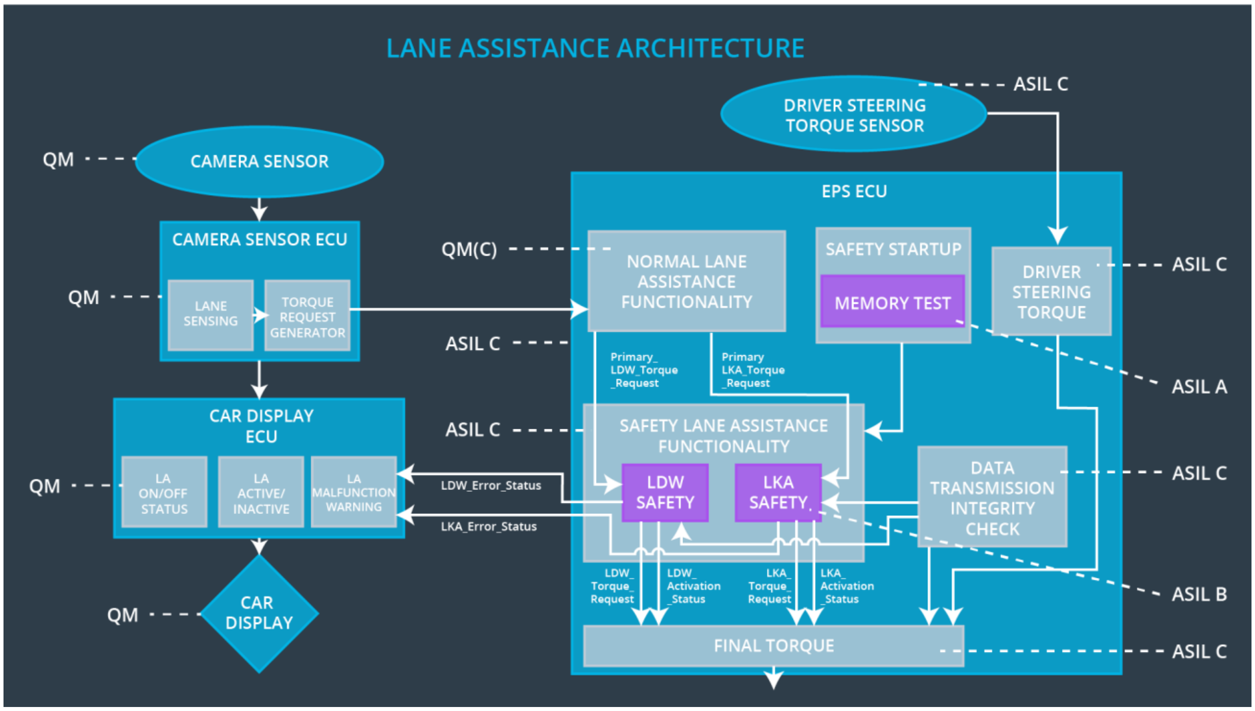
ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	X		

Technical Safety Requirements related to Functional Safety Requirement 02-01 are:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety	The LKA safety component shall	B	500 ms	LKA safety block	LKA torque is zero

Requirement 01	ensure that the torque sent to the 'Final electronic power steering Torque' component is only for 'Max_Duration.				
Technical Safety Requirement 02	As soon as the LKA function deactivates the LKA feature, the 'LKA Safety' software block shall send a signal to the car display ECU to turn on a warning light.	B	500 ms	LKA safety block	LKA torque is zero
Technical Safety Requirement 03	As soon as 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 safety block	LKA torque is zero
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	B	500 ms	Data transmission integrity check block	LKA torque is zero
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Memory test block	LKA torque is zero

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

For this particular item, all technical safety requirements are allocated to the Electronic Power Steering ECU.

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off lane assistance system	Malfunction_01	YES	Warning on Car display
WDC-02	Turn off lane assistance system	Malfunction_02	YES	Warning on Car display
WDC-03	Turn off lane assistance system	Malfunction_03	YES	Warning on Car display