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
18 Mar 2018	1.0	Ong Whee Cheng	Initial version
19 Mar 2018	1.1	Ong Whee Cheng	Updated the safe state of Functional Safety Requirements after review

Table of Contents

Purpose of the Technical Safety Concept

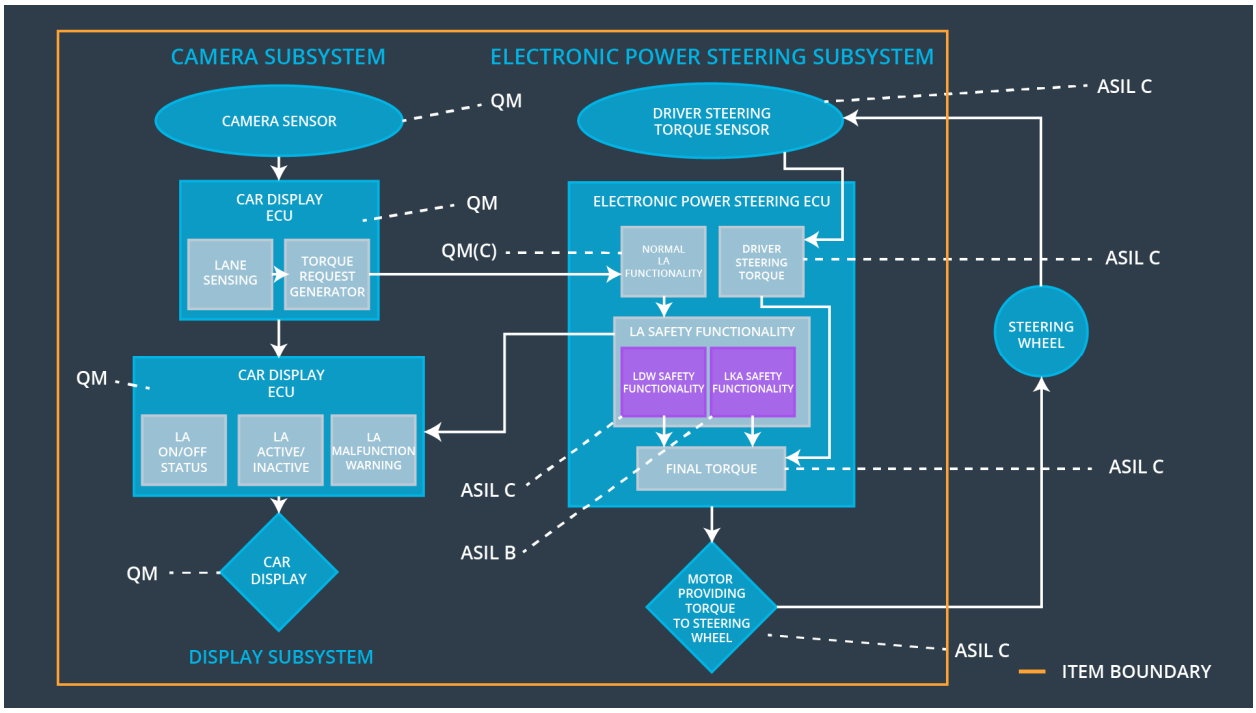
The Technical Safety Concept looks at the technical details and implementation of the item in the product development phase. It turns functional safety requirements in the functional safety concept into technical safety requirements, and allocates these requirements to the relevant parts of the system architecture. The technical safety requirements are general hardware and software requirements; and do not get into specific details.

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	50ms	Set oscillating torque amplitude 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		Set oscillating torque frequency to 0
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	Set LKA torque to 0

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Provides camera images to the Camera Sensor ECU
Camera Sensor ECU - Lane Sensing	Detects lane line positions from camera images
Camera Sensor ECU - Torque Request Generator	Generates a torque request to the Electronic Power Steering ECU if it determines the vehicle is departing from lane
Car Display	Provides visual feedback to the driver: • ACTIVE/INACTIVE status of Lane Departure Warning function • ON/OFF status of Lane Keeping Assistance function
Car Display ECU - Lane Assistance On/Off Status	Indicates On/Off status of Lane Assistance
Car Display ECU - Lane Assistant Active/Inactive	Indicates Active/Inactive status of Lane Assistance

Element	Description
Car Display ECU - Lane Assistance malfunction warning	Indicates malfunction status of Lane Assistance
Driver Steering Torque Sensor	Senses the current steering torque applied to the steering wheel
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Analyzes the steering torque applied by the driver
EPS ECU - Normal Lane Assistance Functionality	Receives torque request from Camera Sensor ECU and sends the amplitude- and frequency-limited torque request to the Lane Assistance Safety Functionality
EPS ECU - Lane Departure Warning Safety Functionality	Checks for LDW malfunction and sends the torque request to the final torque componenet
EPS ECU - Lane Keeping Assistant Safety Functionality	Checks for LKA malfunction and sends the torque request to the final torque component
EPS ECU - Final Torque	Determines final torque from LDW and LKA torque requests, and sends the final torque to the motor
Motor	Applies the final steering torque from Electronic Power Steering ECU to the 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 'LDW_Torque_Request' is sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Amplitude'	C	50ms	LDW Safety	LDW torque output is set to 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			
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 0	C			
Technical Safety Requirement 04	Validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured	C		Data Transmission Integrity Check	
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in mermory	A	Ignition Cycle	Memory Test	

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

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 'LDW_Torque_Request' is sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Frequency'	C	50ms	LDW Safety	LDW torque output is set to 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			
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 0	C			
Technical Safety Requirement 04	Validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured	C		Data Transmission Integrity Check	
Technical Safety Requirem	Memory test shall be conducted at start up of the EPS ECU to check for any faults in mermory	A	Ignition Cycle	Memory Test	

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
ent 05					

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

Lane Keeping Assistance (LKA) Requirements:

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

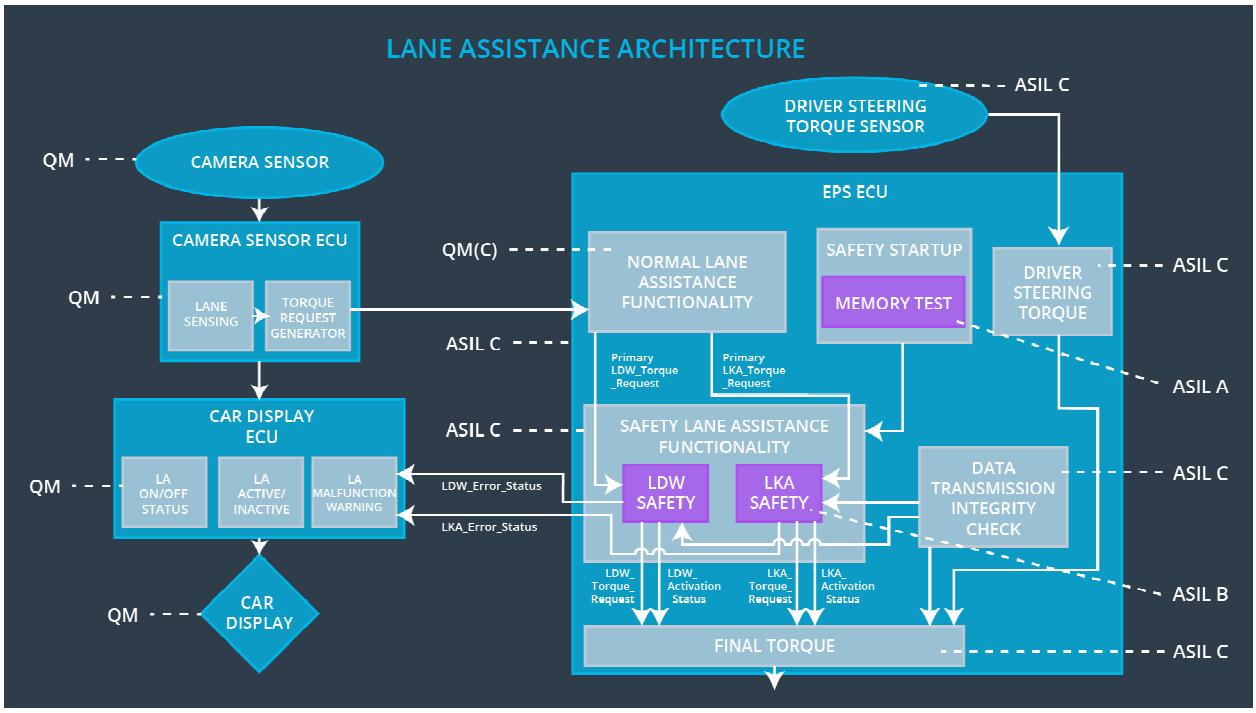
ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	X		

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 Requirement 01	The LKA safety component shall ensure that 'LKA_Torque_Request' is sent to the 'Final electronic power steering Torque' component for only 'Max_Duration'.	B	500ms	LKA Safety	LKA torque output is set to zero
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	B			

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
	warning light				
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 0	B			
Technical Safety Requirement 04	Validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured	B		Data Transmission Integrity Check	
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in mermory	A	Ignition cycle	Memory Test	

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

All technical safety requirements are allocated to the Electronic Power Steering ECU.

Warning and Degradation Concept

For any system malfunction, the lane assistance functions will be turned off and the driver will receive a warning light indication on the vehicle dashboard.

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Lane Assistance is turned off	Malfunction_01	Yes	Lane Assistance Malfunction Warning on Car Display
WDC-02	Lane Assistance is turned off	Malfunction_02	Yes	Lane Assistance Malfunction

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
				Warning on Car Display
WDC-03	Lane Assistance is turned off	Malfunction_03	Yes	Lane Assistance Malfunction Warning on Car Display
WDC-04	Lane Assistance is turned off	Malfunction_04	Yes	Lane Assistance Malfunction Warning on Car Display
WDC-05	Lane Assistance is turned off	Malfunction_05	Yes	Lane Assistance Malfunction Warning on Car Display