Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 1.1

Document history

Date	Version	Editor	Description
2017-09-20	1.0	Yifei Li	First Submission
2017-09-25	1.1	Yifei Li	Updated Technical Requirements 02-01

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
  - Lane Departure Warning (LDW) Requirements:
  - Lane Keeping Assistance (LKA) Requirements:
- Refinement of the System Architecture
- Allocation of Technical Safety Requirements to Architecture Elements
- Warning and Degradation Concept

Purpose of the Technical Safety Concept

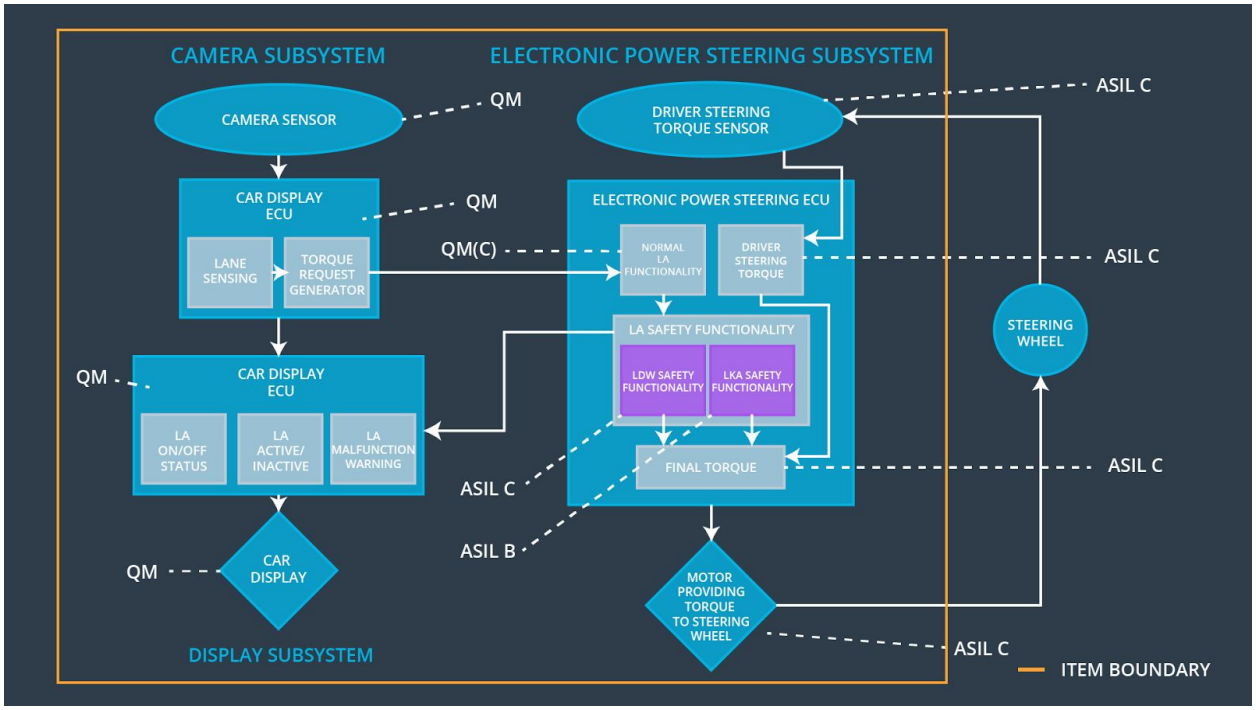
The purpose of Technical Safety Concept is to define functional safety goals and define functional safety requirements at product development phase so that the system is designed to be functional safe and risks can be avoided and the reduced to acceptable levels.

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 electronic power steering ECU shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50ms	Lane departure system is turned off
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50ms	Lane departure system is turned off
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	Lane keeping assistance system is turned off

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Detect road in front of the car and transform it into digital pixels and a streamline of digital information for camera sensor ECU to process
Camera Sensor ECU - Lane Sensing	Process raw data from camera sensor for lane detection and identification
Camera Sensor ECU - Torque request generator	Generate torque request from camera sensor ECU - Lane Sensing unit to electronic power steering ECU
Car Display	A LCD or LED panel that displays human interpretable information
Car Display ECU - Lane Assistance On/Off Status	A LCD or LED panel that displays lane assistance on/off status
Car Display ECU - Lane Assistant Active/Inactive	A LCD or LED panel that displays lane assistance active/inactive status
Car Display ECU - Lane Assistance malfunction warning	A LCD or LED panel that displays malfunction warnings
Driver Steering Torque Sensor	Detect torque applied and convert it to digital information
Electronic Power Steering (EPS) ECU - Driver Steering Torque	An element within EPS ECU that receives torque data from steering torque sensor and process it to motor in order to adjust the steering wheel to maintain the car inside the lane
EPS ECU - Normal Lane Assistance Functionality	An element within EPS ECU that receives torque request from car display ECU and process it to motor in order to adjust the steering wheel
EPS ECU - Lane Departure Warning Safety Functionality	An element with EPS ECU that is responsible for lane departure warning functionality

EPS ECU - Lane Keeping Assistant Safety Functionality	An element within EPS ECU that is responsible for lane keeping assistance functionality
EPS ECU - Final Torque	An element within EPS ECU that is responsible for generating the final torque request to motor
Motor	Applied torque to mechanical components

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	C	50ms	EPS ECU - Lane Departure Warning Safety Functionality	LDW is turned off, warning displayed

	‘Max_Torque_Amplitude’				
Technical Safety Requirement 02	As soon as the LDW function deactivates the LDW feature, the ‘LDW Safety’ software block shall send signal to the car displays ECU to turn on a warning light	C	50ms	EPS ECU - Lane Departure Warning Safety Functionality	LDW is turned off, warning displayed
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	50ms	EPS ECU - Lane Departure Warning Safety Functionality	LDW is turned off, warning displayedf
Technical Safety Requirement 04	The validity and integrity of the data transmission for ‘LDW_Torque_Request’ signal shall be ensured	C	50ms	EPS ECU - Data Transmission Integrity Check	LDW is turned off, warning displayed
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory	A	Ignition cycle	EPS ECU - Memory Test	LDW is turned off, warning displayed

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 Requiremen	The lane keeping item shall ensure that the lane departure oscillating torque frequency is	X		

t 01-02	below Max_Torque_Frequency			

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	50ms	EPS ECU - Lane Departure Warning Safety Functionality	LDW is turned off, warning displayed
Technical Safety Requirement 02	As soon as the LDW function deactivates the LDW feature, the 'LDW Safety' software block shall send signal to the car displays ECU to turn on a warning light	C	50ms	EPS ECU - Lane Departure Warning Safety Functionality	LDW is turned off, warning displayed
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	50ms	EPS ECU - Lane Departure Warning Safety Functionality	LDW is turned off, warning displayed
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured	C	50ms	EPS ECU - Data Transmission Integrity Check	LDW is turned off, warning displayed
Technical Safety Requirement	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory	A	Ignition cycle	EPS ECU - Memory Test	LDW is turned off, warning

t 05					displayed

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

ID	Technical Safety Requirement	Verification Acceptance Criteria	Validation Acceptance Criteria
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'	Max_Torque_Frequency is specified not too high nor too low	LDW_Torque_Request < Max_Torque_Frequency
Technical Safety Requirement 02	As soon as the LDW function deactivates the LDW feature, the 'LDW Safety' software block shall send signal to the car displays ECU to turn on a warning light	LDW feature is successfully deactivated and a signal is sent to the display ECU	Warning light is turned on car display when LDW is deactivated
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	LDW feature is successfully deactivated and LDW_Torque_Request is set to zero	LDW_Torque_Request is set to zero and LDW feature deactivated
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured	LDW_Torque_Request signal is valid and no loss of information	Signal is correctly transmitted and received
Technical Safety Requiremen	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory	Memory test is tested without any bugs	Memory test is correctly implemented at

t 05			start of EPS ECU

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 lane keeping safety component shall ensure that the duration of torque applied is below ‘Max_Duration’	B	500ms	EPS ECU - Lane Keeping Assistant Safety Functionality	LKA is turned off, warning displayed
Technical Safety Requirement 02	As soon as the LKA function deactivates the LKA feature, the LKA Safety’ software block shall send signal to the car displays ECU to turn on a	B	500ms	EPS ECU - Lane Keeping Assistant Safety Functionality	LKA is turned off, warning displayed

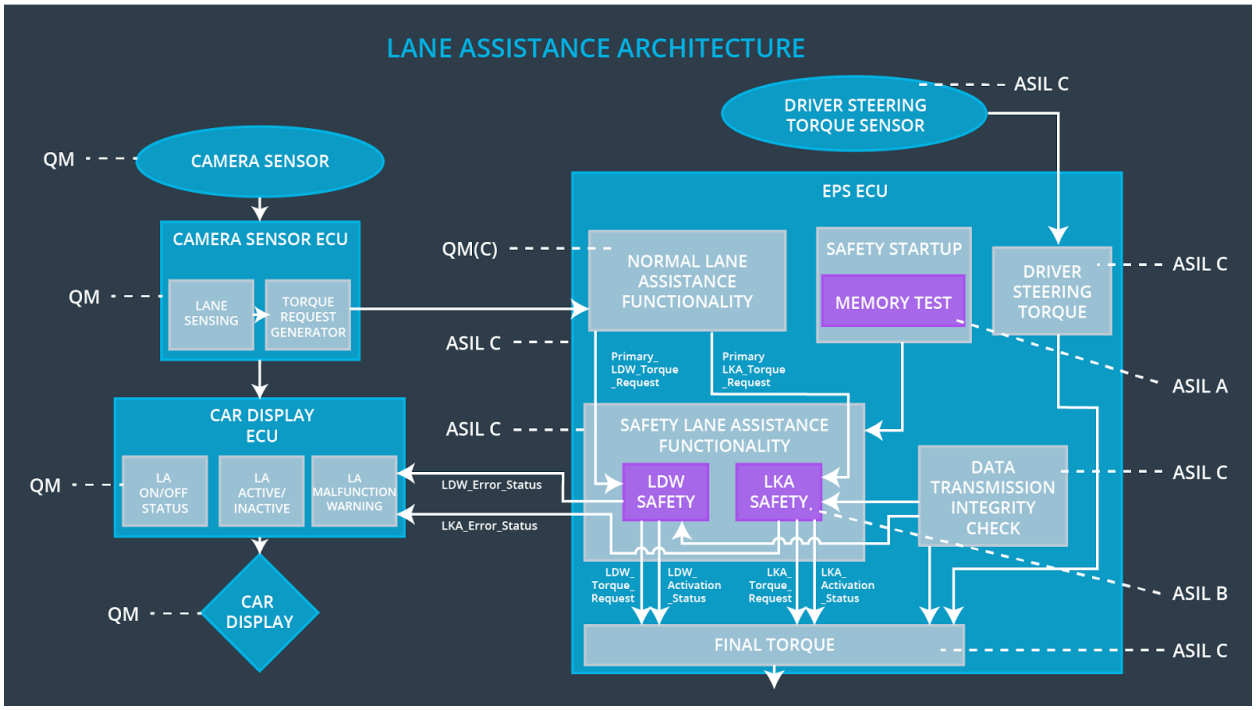
	warning light				
Technical Safety Requirement 03	As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and the 'LKA_Torque_Request' shall be set to zero	B	500ms	EPS ECU - Lane Keeping Assistant Safety Functionality	LKA is turned off, warning displayed
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured	B	500ms	EPS ECU - Data Transmission Integrity Check	LKA is turned off, warning displayed
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory	A	Ignition cycle	EPS ECU - Memory Test	LKA is turned off, warning displayed

Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:

ID	Technical Safety Requirement	Verification Acceptance Criteria	Validation Acceptance Criteria
Technical Safety Requirement 01	The LKA safety component shall ensure that the duration of the 'LKA_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Frequency'	Max_Torque_Frequency is specified not too high nor too low	LKA_Torque_Request < Max_Torque_Frequency
Technical Safety Requiremen	As soon as the LKA function deactivates the LKA feature, the LKA Safety' software block shall	LKA feature is successfully deactivated and a signal is sent to	Warning light is turned on car display when LKA

t 02	send signal to the car displays ECU to turn on a warning light	the display ECU	is deactivated
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	LKA feature is successfully deactivated and LKA_Torque_Request is set to zero	LKA_Torque_Request is set to zero and LKA feature deactivated
Technical Safety Requirement 04	The validity and integrity of the data transmission for ‘LKA_Torque_Request’ signal shall be ensured	LKA_Torque_Request signal is valid and no loss of information	Signal is correctly transmitted and received
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory	Memory test is tested without any bugs	Memory test is correctly implemented at start of EPS ECU

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

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Lane departure warning output is set to zero	Oscillating torque amplitude greater than Max_Torque_Ampltidue	Yes	Warning messages displayed on car display
WDC-02	Lane departure warning output is set to zero	Oscillating torque frequency greater than Max_Torque_Frequency	Yes	Warning messages displayed on car display
WDC-03	Lane keeping assistance output is set to zero	Fault Tolerant Time Interval > 500ms	Yes	Warning messages displayed on car display