Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 1.1

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
3/2/18	0.1	Ken Overholt	Initial draft
3/8/18	0.2	Ken Overholt	Candidate for final release
3/8/18	1.0	Ken Overholt	Final Release
3/8/18	1.1	Ken Overholt	Updated LKA requirements

Table of Contents

Table of Contents

Document history 2
Table of Contents 2
Purpose of the Technical Safety Concept 2
Inputs to the Technical Safety Concept 3
Functional Safety Requirements 3
Refined System Architecture from Functional Safety Concept 4
Functional overview of architecture elements 4
Technical Safety Concept 6
Technical Safety Requirements 6
Refinement of the System Architecture 10
Allocation of Technical Safety Requirements to Architecture Elements 10
Warning and Degradation Concept 10

Purpose of the Technical Safety Concept

The technical Safety Concept defines how the subsystems interact at the message level and describes how the ECUs communicate with each other. It turns functional safety requirements

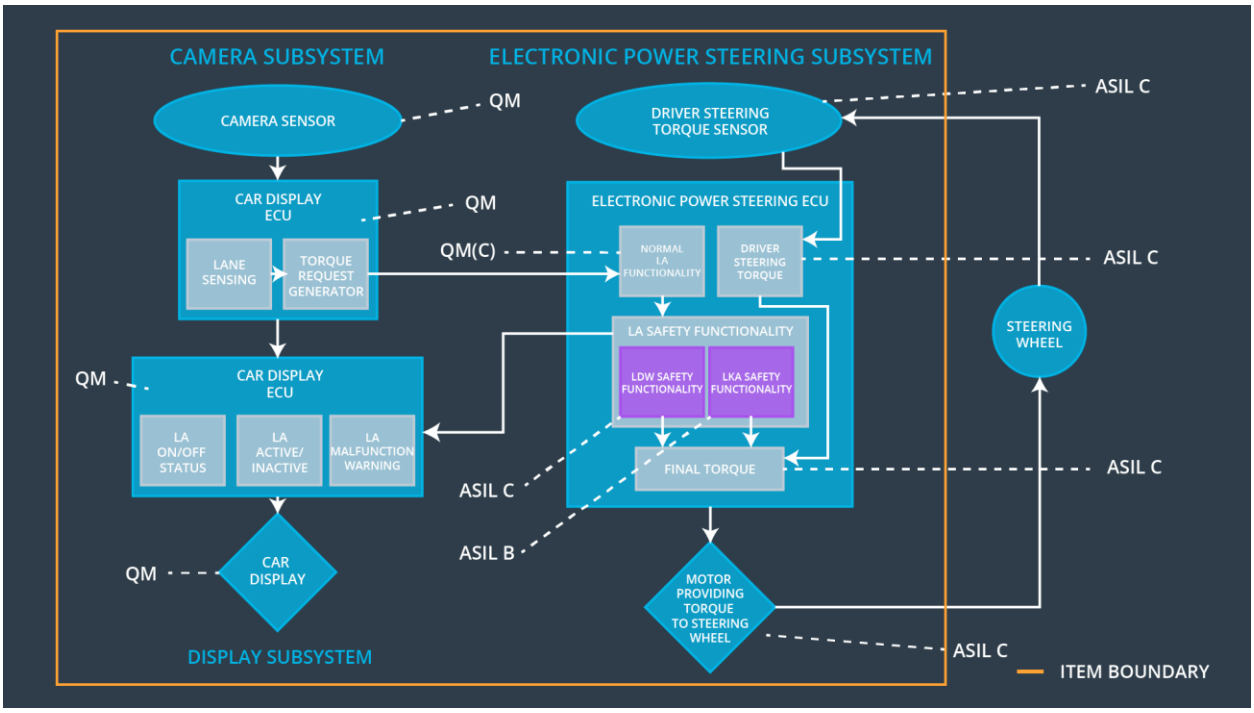
into technical safety requirements and allocates technical safety requirements to the system architecture.

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 electronic power steering ECU shall ensure that the lane departure warning oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	No torque is being applied
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure warning oscillating torque frequency is below Max_Torque_Frequency	C	50 ms	No torque is being applied
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 ms	No torque is being applied

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	The Camera Sensor reads in images from the road.
Camera Sensor ECU - Lane Sensing	The Camera Sensor ECU identifies when the vehicle has accidentally departed its lane and sends the appropriate torque request to the Electronic Power Steering ECU as well as sending a message to the Car Display ECU.
Camera Sensor ECU - Torque request generator	The Camera Sensor ECU - Torque request generator determines the amount of torque necessary to keep the car in the lane and sends this value to the EPS ECU - Normal Lane Assistance Functionality
Car Display	The Car Display shows a sign in indicating the car has veered from its lane.

Car Display ECU - Lane Assistance On/Off Status	The Car Display ECU controls a light that tells the driver if the Lane Keeping system is on or off. It also controls a light that tells the driver that the Lane Departure Warning is activated.
Car Display ECU - Lane Assistant Active/Inactive	Car Display ECU - Lane Assistant Active/Inactive turns on the light when the Lane Assistant is active and turns it off when the Lane Assistance is inactive
Car Display ECU - Lane Assistance malfunction warning	The Car Display ECU - Lane Assistance malfunction warning turns on a light when the Lane Assistance feature is malfunctioning and off when not
Driver Steering Torque Sensor	The Driver Steering Torque Sensor senses the current torque value and sends it to the EPS ECU
Electronic Power Steering (EPS) ECU - Driver Steering Torque	The Electronic Power Steering (EPS) ECU - Driver Steering Torque sends the actual torque value to the Final Torque block.
EPS ECU - Normal Lane Assistance Functionality	Sends the vibrational torque request to the LDW Safety Functionality
EPS ECU - Lane Departure Warning Safety Functionality	Checks to make sure that the torque request is below the maximum amplitude and frequency. If either maximum value is crossed, the LDW Safety Functionality deactivates the functionality and sets the LDW_Torque_Request to zero. Sends its torque request to the Final EPS ECU - Final Torque block. It sends a status signal to the Car Display
EPS ECU - Lane Keeping Assistant Safety Functionality	Checks to make sure that the torque request duration is below the maximum duration. If the value is crossed, the EPS ECU - Lane Keeping Assistant Safety Functionality deactivates the functionality and sets the LDW_Torque_Request to zero. Sends its torque request to the Final EPS ECU - Final Torque block. It sends a status signal to the Car Display
EPS ECU - Final Torque	The EPS ECU – Final Torque combines torques and sends the resulting torque to the motor.
Motor	The motor receives the torque request from the Driver Steering Torque Sensor and moves 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 the 'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Amplitude.	C	50 ms	LDW Safety software component	Lane Departure Warning Torque Request Amplitude shall be set to zero
Technical Safety Requirement 02	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 software component	Lane Departure Warning Torque Request Amplitude shall be set to zero

Technical Safety Requirement 03	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 software component	Lane Departure Warning Torque Request Amplitude 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	Lane Departure Warning Torque Request Amplitude shall be set to 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	Safety Startup Memory Test block	Lane Departure Warning Torque Request Amplitude shall be set to 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 software component	Lane Departure Warning Torque Request Frequency shall be set to zero
Technical Safety Requirement 02	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the Max_Torque_Frequency shall be set to zero.	C	50 ms	LDW Safety software component	Lane Departure Warning Torque Request Frequency shall be set to zero
Technical Safety Requirement 03	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 software component	Lane Departure Warning Torque Request Frequency shall be set to zero
Technical Safety Requirement 04	The validity and integrity of the data transmission for Max_Torque_Frequency signal shall be ensured.	C	50 ms	Data Transmission Integrity Check block	Lane Departure Warning Torque Request Frequency shall be set to 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	Safety Startup Memory Test block	Lane Departure Warning Torque Request Frequency shall be set to zero

Lane Keeping Assistance (LKA) Requirements:

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

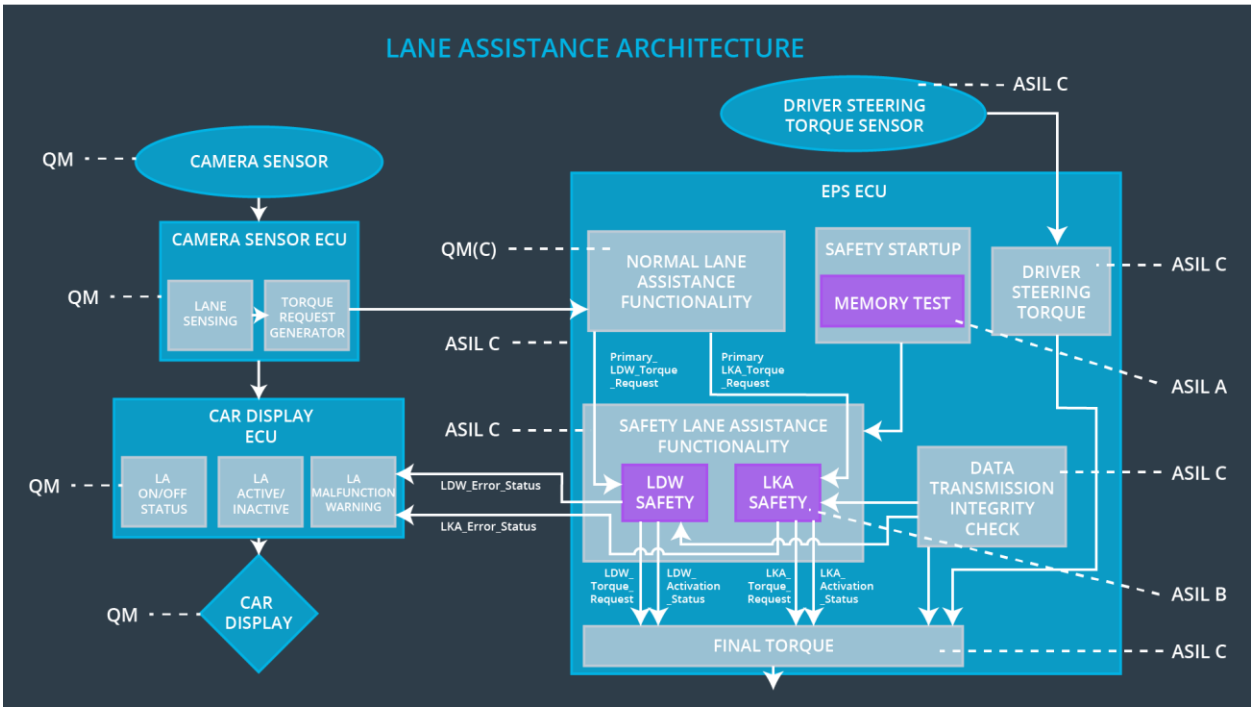
ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	X		

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 Requirement 01	The LKA safety component shall ensure that a timer is started when the ‘LKA_Torque_Request' is sent to the 'Final electronic power steering Torque' component.	B	500 ms	LKA Safety software component	LKA Torque Request shall be set to zero
Technical Safety Requirement 02	As soon as the LKA function’s timer reaches Max_Duration, it shall deactivate the LKA feature and the 'LKA_Torque_Request' shall be set to zero.	B	500 ms	LKA Safety software component	LKA Torque Request shall be set to zero
Technical Safety Requirement 03	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 software component	LKA Torque Request shall be set to 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 Request shall be set to zero
Technical	Memory test shall be conducted	A	Ignition	Safety Startup	LKA Torque

Safety Requirement 05	at startup of the EPS ECU to check for any faults in memory.		cycle	Memory Test block	Request shall be set to zero

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

For this 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 the functionality	lane departure warning function	Yes	The owner's manual will state

		applies an oscillating torque with very high torque frequency and amplitude		that the feature will be turned off if it becomes too forceful. The driver will see a warning light on the dashboard when the system malfunctions.
WDC-02	Turn off the functionality	Oscillating torque has reached the max_duration value	Yes	The owner's manual will state that the vehicle is not to be used for autonomous driving and that this feature will only be active for a short period before turning off. The driver will see a warning light on the dashboard when the lane keeping assistance is activated and it will disappear when not activated.