Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 4.0
Released on 2017-10-31

Document history

Date	Version	Editor	Description
10-24-2017	1.0	Brian McHugh	Set up template
10-25-2017	2.0	Brian McHugh	Initial draft
10-28-2017	3.0	Brian McHugh	Complete up to TSR
10-30-2017	4.0	Brian McHugh	Finalize

Table of Contents

Purpose of the Technical Safety Concept

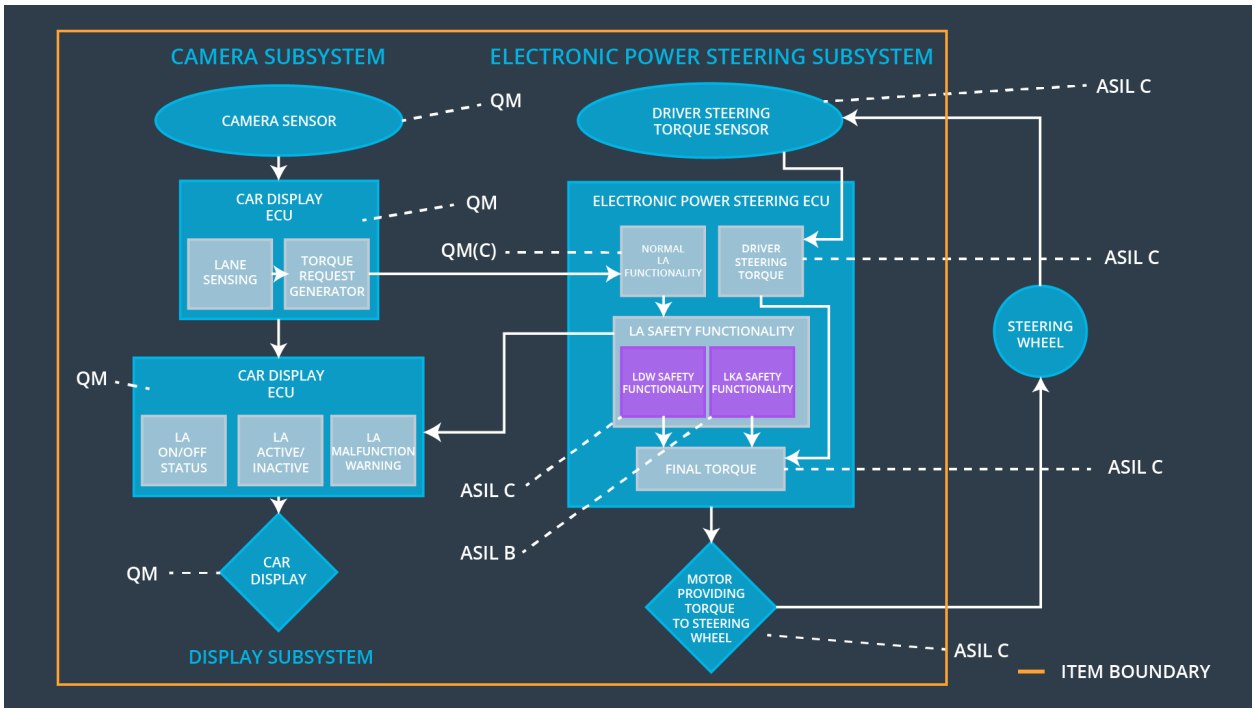
Convert functional safety requirements into technical safety requirements and allocate technical safety requirements to the system architecture.

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 lane assistance item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	OFF
Functional Safety Requirement 01-02	The lane assistance item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50 ms	OFF
Functional Safety Requirement 01-03	The lane assistance item shall ensure that the lane departure oscillating torque amplitude and oscillating torque frequency default to 0 (shut off) if the electronic power steering ECU exceeds Max_Torque_Duration	QM	50 ms	OFF
Functional Safety Requirement 02-01	The lane assistance item shall ensure that the necessary redundancies are included in the system architecture to prevent total loss of the LKA function	A	500 ms	OFF
Functional Safety Requirement 02-02	The lane assistance item shall ensure that the electronic power steering ECU limits torque usage to Max_Duration	B	500 ms	OFF

Refined System Architecture from Functional Safety Concept



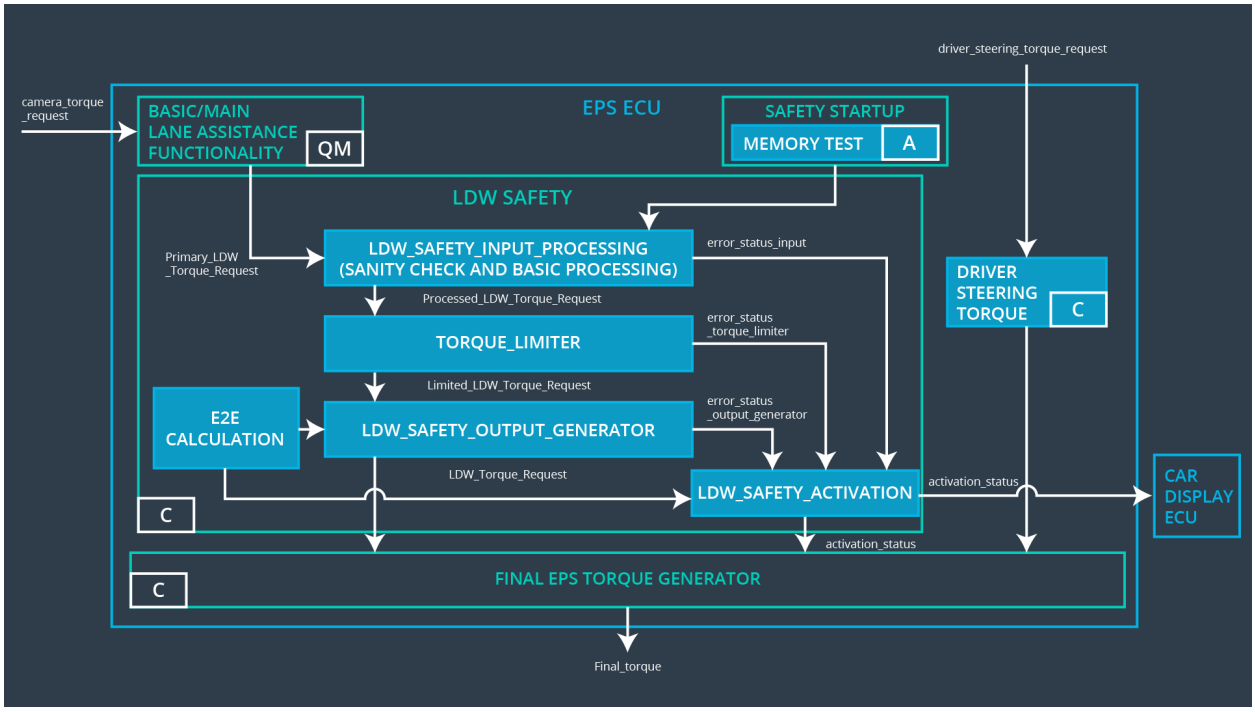
Functional overview of architecture elements

Element	Description
Camera Sensor	Captures images of the road ahead, as well as the front periphery of the vehicle and sends that data to the Camera Sensor ECU
Camera Sensor ECU - Lane Sensing	Detects ego lane and determines if vehicle is staying centered within lane markers
Camera Sensor ECU - Torque request generator	Sends torque requests to Electronic Power Steering subsystem
Car Display	Receives input from the Car Display ECU and acts as a graphical user interface for the vehicle to communicate operational status to its operator

Car Display ECU - Lane Assistance On/Off Status	Manages a light indicating to the driver whether the Lane Assistance system is turned on or not
Car Display ECU - Lane Assistant Active/Inactive	Manages a light indicating to the driver whether the Lane Assistance system is currently engaged
Car Display ECU - Lane Assistance malfunction warning	Manages a light that when lit indicates to the driver that the Lane Assistance system has malfunctioned
Driver Steering Torque Sensor	Receives input from the Steering Wheel and sends torque-level data to the Electronic Power Steering ECU
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Detects how much the driver is turning the Steering Wheel
EPS ECU - Normal Lane Assistance Functionality	Receives the vibrational torque request from the Camera Sensor subsystem
EPS ECU - Lane Departure Warning Safety Functionality	Receives the vibrational torque request from the Normal Lane Assistance Functionality block; sets amplitude and frequency limits on torque requests sent to the Final Torque block and sends operational information to the Car Display subsystem
EPS ECU - Lane Keeping Assistant Safety Functionality	Receives the vibrational torque request from the Normal Lane Assistance Functionality block; sets torque usage duration limits on torque requests sent to the Final Torque block and sends operational information to the Car Display subsystem
EPS ECU - Final Torque	Adds torque requests together to output a final torque request to the Steering Wheel Motor
Steering Wheel Motor	Acts as an actuator, applying torque and oscillations to the Steering Wheel when needed

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 Electronic Power Steering ECU shall ensure that the lane departure oscillating torque amplitude does not exceed Max_Torque_Amplitude	**X**		

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

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 EPS Torque Generator component does not exceed Max_Torque_Amplitude	C	50 ms	LDW Safety block	OFF
Technical Safety Requirement 02	As soon as the LDW function deactivates the LDW feature, the LDW Safety block shall send a signal to the Car Display ECU to turn on a warning light	C	50 ms	LDW Safety block	OFF
Technical Safety Requirement 03	As soon as a failure is detected by the LDW feature, it shall deactivate the LDW function and the LDW_Torque_Request shall be set to 0	C	50 ms	LDW Safety block	OFF
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	OFF
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	Memory Test	OFF

Functional Safety Requirement 01-02 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 Electronic Power Steering ECU shall ensure that the lane departure oscillating torque frequency does not exceed Max_Torque_Frequency	**X**		

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

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 EPS Torque Generator component does not exceed Max_Torque_Frequency	C	50 ms	LDW Safety block	OFF
Technical Safety Requirement 02	As soon as the LDW function deactivates the LDW feature, the LDW Safety block shall send a signal to the Car Display ECU to turn on a warning light	C	50 ms	LDW Safety block	OFF
Technical Safety Requirement 03	As soon as a failure is detected by the LDW feature, it shall deactivate the LDW function and the LDW_Torque_Request shall be set to 0	C	50 ms	LDW Safety block	OFF
Technical Safety Requirement 04	The validity and integrity of the data transmission for LDW_Torque_Request signal shall	C	50 ms	Data Transmission Integrity Check	OFF

	be ensured				
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	Memory Test	OFF

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

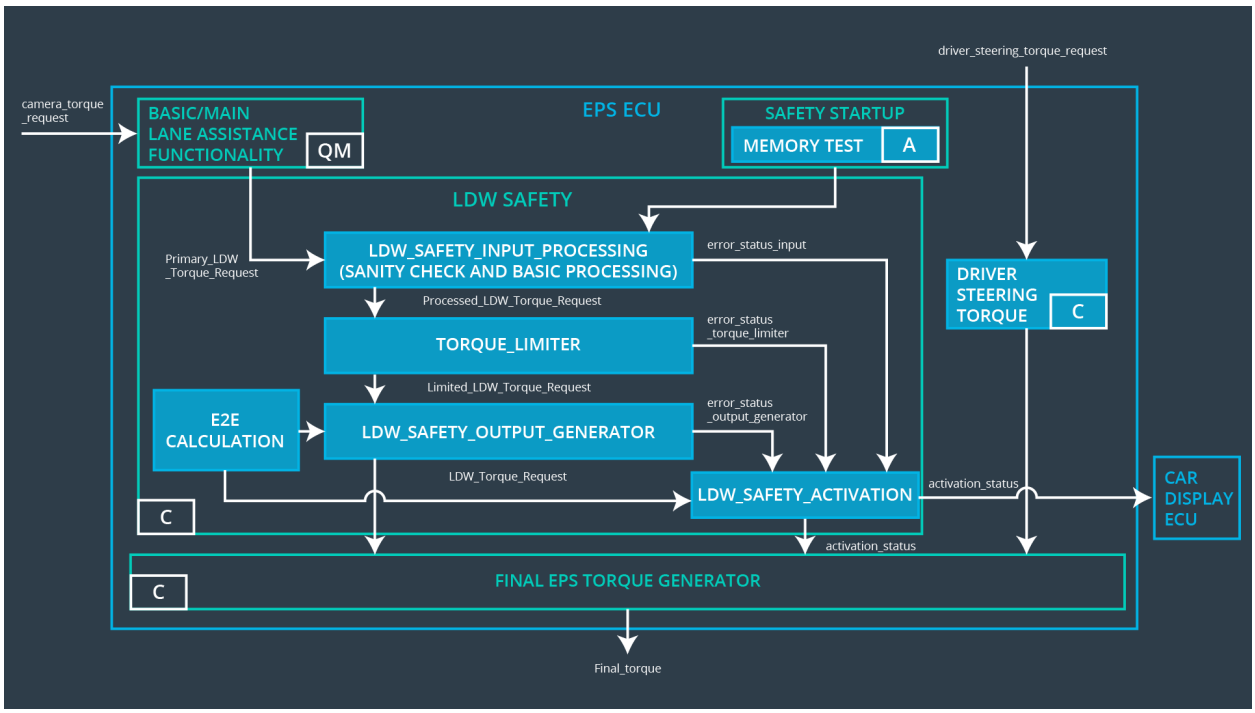
ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 01-03	The Electronic Power Steering ECU shall ensure that the lane departure oscillating torque amplitude and oscillating torque frequency default to 0 (shut off) if the electronic power steering ECU exceeds Max_Duration for torque	**X**		

Technical Safety Requirements related to Functional Safety Requirement 01-03:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 01	The LDW Safety component shall ensure that usage of the LDW feature never exceeds Max_Duration	C	50 ms	LDW Safety block	OFF
Technical Safety Requirement 02	As soon as the LDW function deactivates the LDW feature, the LDW Safety block shall send a signal to the Car Display ECU to turn on a warning light	C	50 ms	LDW Safety block	OFF

Technical Safety Requirement 03	As soon as a failure is detected by the LDW feature, it shall deactivate the LDW function and the LDW_Torque_Request shall be set to 0	C	50 ms	LDW Safety block	OFF
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	OFF
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	Memory Test	OFF

Lane Keeping Assistance (LKA) Requirements:



Functional Safety Requirement 02-01 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 02-01	The Electronic Power Steering ECU shall provide the necessary redundancies to prevent total loss of the LKA function	X		

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

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01	The Normal Lane Assistance Functionality component shall include parallel, redundant wiring and send two identical Primary_LKA_Torque_Request messages to LKA Safety block	C	500 ms	Normal Lane Assistance Functionality block / LKA Safety block	ON with "check systems" warning
Technical Safety Requirement 02	If LKA Safety block only receives one Primary_LKA_Torque_Request message from the Normal Lane Assistance Functionality component or two that don't match, the LKA Safety block shall send a signal to the Car Display ECU to turn on a warning light	C	500 ms	Normal Lane Assistance Functionality block / LKA Safety block	ON with "check systems" warning
Technical Safety Requirement 03	If LKA Safety block only receives one Primary_LKA_Torque_Request message from the Normal Lane Assistance Functionality component or two that don't	C	500 ms	Normal Lane Assistance Functionality block / LKA Safety block	ON with "check systems" warning

	match, the LKA_Torque_Request shall be set to the lesser of the two or the only measurment received				
Technical Safety Requirement 04	The validity and integrity of the data transmission for Primary_LKA_Torque_Request signal shall be ensured	C	500 ms	Data Transmission Integrity Check	ON with "check systems" warning
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	Memory Test	ON with "check systems" warning

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

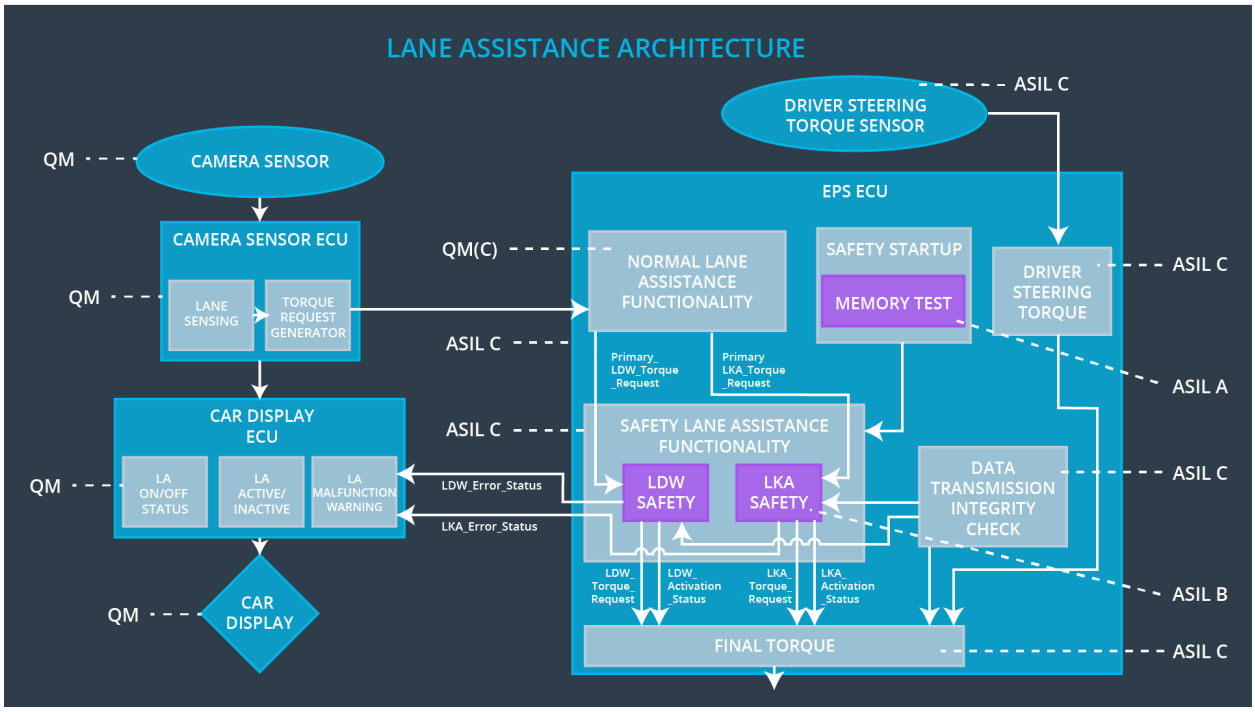
ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-02	The Electronic Power Steering ECU shall ensure that the electronic power steering ECU limits torque to Max_Duration	**X**		

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

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 the duration of torque requests never exceed Max_Duration	B	500 ms	LKA Safety block	OFF
Technical	As soon as the LKA function	B	500 ms	LKA Safety	OFF

Safety Requirement 02	deactivates the LKA feature, the LKA Safety block shall send a signal to the Car Display ECU to turn on a warning light			block	
Technical Safety Requirement 03	As soon as a failure is detected by the LKA feature, it shall deactivate the LKA function and the LKA_Torque_Request shall be set to 0	B	500 ms	LKA Safety block	OFF
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	OFF
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	Memory Test	OFF

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	OFF	Oscillating torque amplitude exceeds Max_Torque_Amplitude	YES	Car Display
WDC-02	OFF	Oscillating torque frequency exceeds Max_Torque_Frequency	YES	Car Display
WDC-03	OFF	LKA function is on and activated but fails to apply steering torque	YES	Car Display
WDC-04	OFF	Oscillating torque duration exceeds Max_Torque_Duration	YES	Car Display
WDC-05	OFF	LKA function usage exceeds Max_Duration	YES	Car Display