Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: [Version]
Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
3/5/2018	1.0		Initial Draft
3/6/2018	1.1		Add WDC-02

Table of Contents

Purpose of the Technical Safety Concept

The technical safety concept translates high-level functional safety requirements into technical safety requirements that dictate specific performance parameters and concrete constraints for the system.

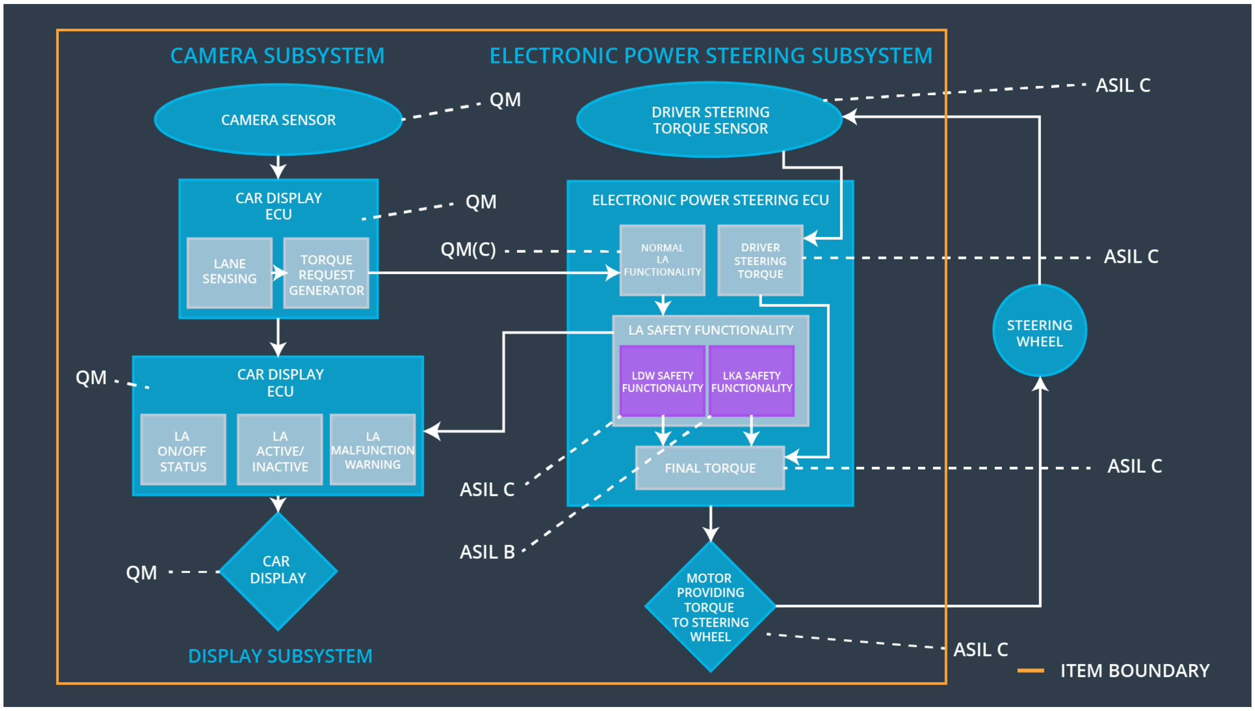
Inputs to the Technical Safety Concept

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	50 ms	The LDW system will completely stop applying haptic feedback. Warning will display on dashboard informing driver of the fault.
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	50 ms	The LDW system will completely stop applying haptic feedback. Warning will display on dashboard informing driver of the fault.
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	The LDW system will completely stop affecting the car steering. Warning will display on

				dashboard informing driver that lane keeping has stopped.

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	Camera Sensor ECU Lane Sensing element

	interprets road images to determine position, orientation, and curvature of lane lines.
Camera Sensor ECU - Torque request generator	The Camera Sensor ECU Torque Request Generator uses lane pose information to determine necessary torque for lane keeping.
Car Display	The Car Display shows the driver the current status of LDW and LK functions, including current operation and warnings.
Car Display ECU - Lane Assistance On/Off Status	The Car Display ECU LA On/Off Status element determines whether each LA function has been turned on or off.
Car Display ECU - Lane Assistant Active/Inactive	The Car Display ECU LA Active/Inactive element determines whether the lane assist is active or inactive for display on the dashboard.
Car Display ECU - Lane Assistance malfunction warning	The Car Display ECU LA Malfunction Warning element receives LDW_Error_Status messages and provides appropriate warnings on the dashboard.
Driver Steering Torque Sensor	The Driver Steering Torque Sensor measures the amount of torque applied by the driver, which must be amplified by the EPS ECU to produce a torque. The LA functions are minor contributors to torque compared to the amplification of driver steering torque.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	The Electronic Power Steering (EPS) ECU Driver Steering Torque element determines appropriate

	amplification of torque applied by the driver.
EPS ECU - Normal Lane Assistance Functionality	The EPS ECU Normal Lane Assistance Functionality element is responsible for the primary (non-safety) functions of LA.
EPS ECU - Lane Departure Warning Safety Functionality	The LDW Safety element is responsible for safety-related functions of LDW: limiting amplitude and frequency of haptic feedback.
EPS ECU - Lane Keeping Assistant Safety Functionality	The LK Safety element is responsible for safety-related functions of LK: limiting duration of usage.
EPS ECU - Final Torque	The Final Torque element combines torque contributions from driver amplification and LA elements.
Motor	The Motor provides torque for 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	Camera ECU	Car Display ECU

		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	The LDW safety component will set the LDW torque amplitude request to 0, preventing further haptic. Warning will display on dashboard informing driver of the fault.
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	The LDW safety component will set the LDW torque amplitude request to 0, preventing further haptic. Warning will display on dashboard informing driver of the fault.
Technical Safety Requirem	As soon as a failure is detected by the LDW function, it shall deactivate the LDW	C	50 ms	LDW safety	The LDW safety component

ent 03	feature and the 'LDW_Torque_Request' shall be set to zero.				will set the LDW torque amplitude request to 0, preventing further haptic. Warning will display on dashboard informing driver of the fault.
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	The LDW safety component will set the LDW torque amplitude request to 0, preventing further haptic. Warning will display on dashboard informing driver of the fault.
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	Safety startup	The LDW safety component will set the LDW torque amplitude request to 0, preventing further haptic. Warning will display on dashboard informing driver of the fault.

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	The LDW safety component will set the LDW torque frequency request to 0, preventing further haptic. Warning will display on dashboard informing driver of the fault.
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	The LDW safety component will set the LDW torque frequency request to 0, preventing further haptic. Warning will display on

					dashboard informing driver of the fault.
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	The LDW safety component will set the LDW torque frequency request to 0, preventing further haptic. Warning will display on dashboard informing driver of the fault.
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	The LDW safety component will set the LDW torque frequency request to 0, preventing further haptic. Warning will display on dashboard informing driver of the fault.
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	Safety Startup	The LDW safety component will set the LDW torque frequency request to 0, preventing further haptic. Warning will display on dashboard informing

					driver of the fault.

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		

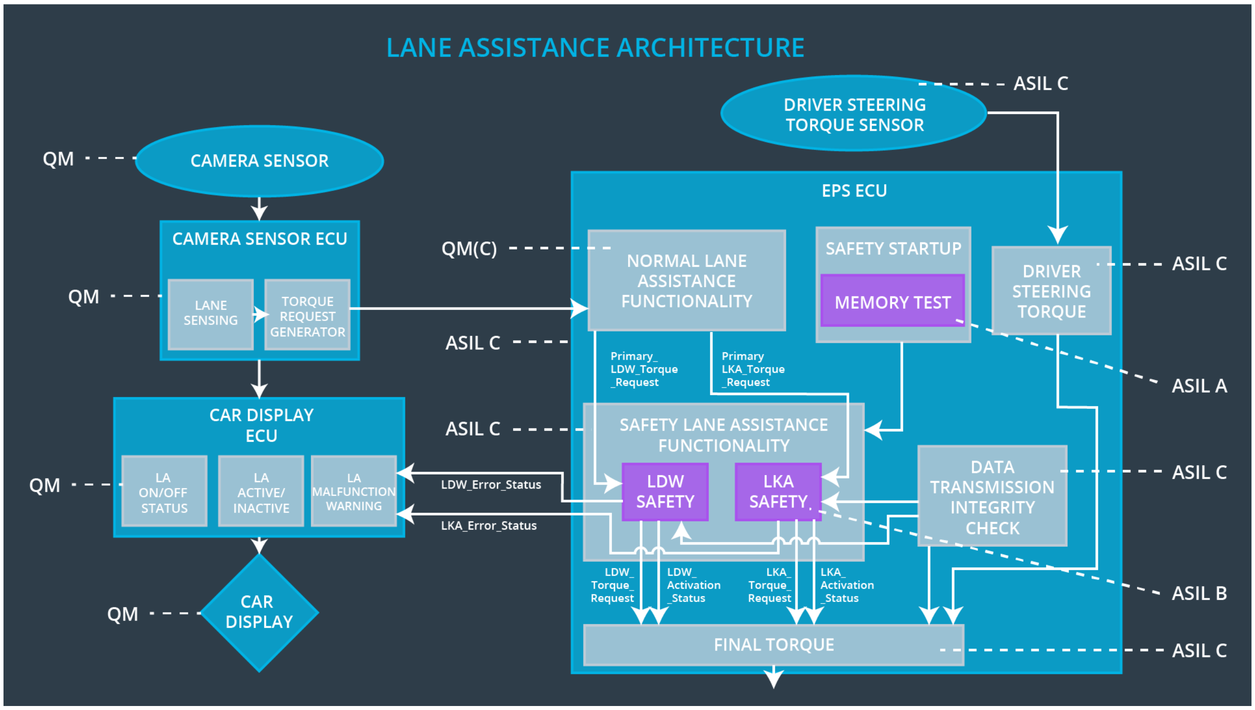
Technical Safety Requirements related to Functional Safety Requirement 02-01 are:

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 the duration of LK usage is below Max_Duration.	B	500 ms	LKA Safety	The LKA system will completely stop affecting the car steering. Warning will display on dashboard informing driver that lane keeping assistance has stopped.
Technical Safety Requireme	As soon as the LKA function deactivates the LKA feature, the 'LKA Safety' software block shall	B	500 ms	LKA Safety	The LKA system will completely

nt 02	send a signal to the car display ECU to turn on a warning light.				stop affecting the car steering. Warning will display on dashboard informing driver that lane keeping has stopped.
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	The LKA system will completely stop affecting the car steering. Warning will display on dashboard informing driver that lane keeping has stopped.
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	The LKA system will completely stop affecting the car steering. Warning will display on dashboard informing driver that lane keeping has stopped.
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	Safety Startup	The LKA system will completely stop affecting the

					car steering. Warning will display on dashboard informing driver that lane keeping has stopped.

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	Trigger for	Safe State	Driver Warning

	Mode	**Degradation Mode**	**invoked?**	
WDC-01-01	Turn off functionality.	The lane departure warning function applies an oscillating torque with very high torque amplitude (above limit).	Yes	Warning indicator on dashboard
WDC-01-02	Turn off functionality.	The lane departure warning function applies an oscillating torque with very high torque frequency (above limit).	Yes	Warning indicator on dashboard
WDC-02-01	Turn off functionality.	The lane keeping assistance function is not limited in time duration which leads to misuse as an autonomous driving function.	Yes	Warning indicator on dashboard