Technical Safety Concept Lane Assistance

Document Version: 1.0

Document history

Date	Version	Editor	Description
13/9/2018	1.0	Ajinkya Bhave	Technical Safety Concept for Lane Assistance Item

Table of Contents

Purpose of the Technical Safety Concept

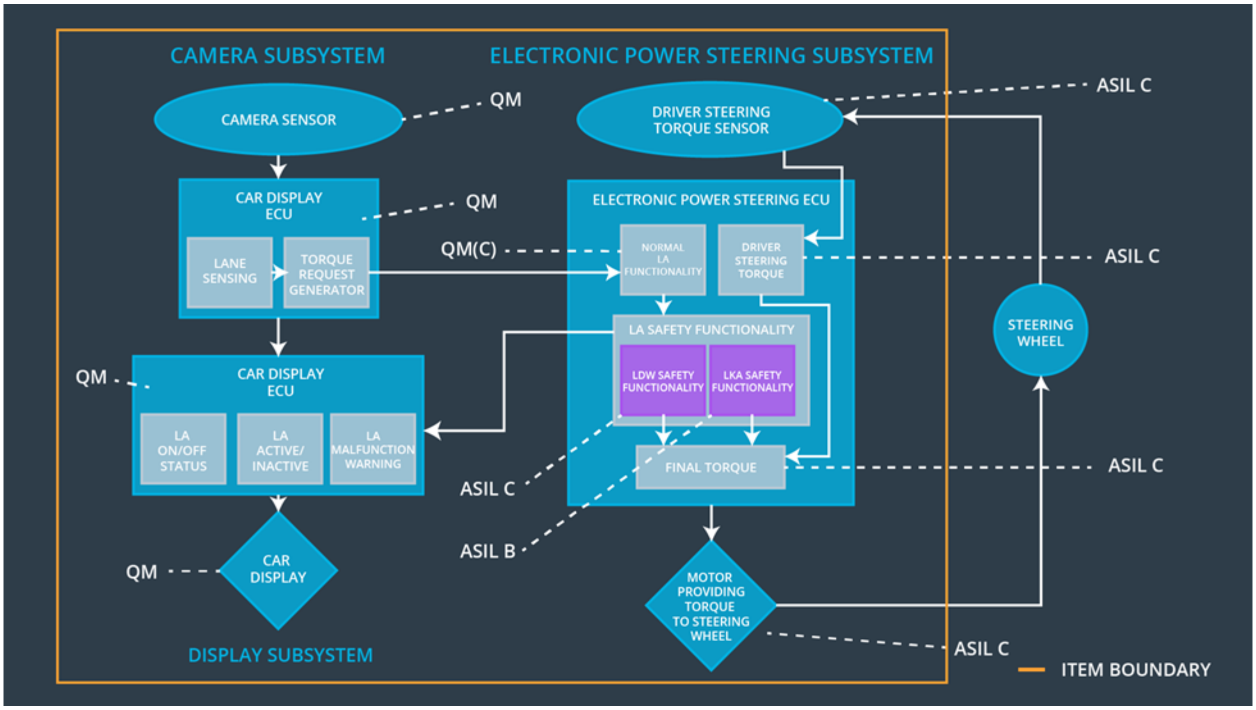
The Technical Safety Concept derives technical safety requirements at a more detailed product level from functional safety requirements, allocates each technical safety requirement to the right elements in the refined system architecture, and defines the warning and degradation concepts for each requirement.

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 LA Item shall ensure that the LDW oscillating torque amplitude is below *Max_Torque_Amplitude*	C	50 ms	Turn off LDW
Functional Safety Requirement 01-02	The LA Item shall ensure that the LDW oscillating torque frequency is below *Max_Torque_Frequency*	C	50 ms	Turn off LDW
Functional Safety Requirement 01-03	The LA Item shall ensure that the LDW oscillating torque is applied within *Max_Delay*	C	50 ms	Turn off LDW
Functional Safety Requirement 02-01	The EPS ECU shall ensure that the LKA torque is applied for only *Max_Duration*	B	500 ms	Turn off LKA
Functional Safety Requirement 02-02	The EPS ECU shall ensure that the LKA torque amplitude is greater than *Min_Torque_Amplitude*	QM	500 ms	Turn off LKA

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Captures images of road in front of the vehicle
Camera Sensor ECU - Lane Sensing	Calculates when the vehicle is leaving the lane based on images from camera sensor
Camera Sensor ECU - Torque request generator	Sends a torque request to the Normal LA component when the vehicle is leaving the lane
Car Display	Displays warning and status lights for driver
Car Display ECU - Lane Assistance On/Off Status	Controls the status light on the car display based on whether the LA function is on/off
Car Display ECU - Lane Assistant Active/Inactive	Controls the status light on the car display based on whether LA function is currently active/inactive

Car Display ECU - Lane Assistance malfunction warning	Controls the malfunction warning light on the car display based on the error status of the LA function
Driver Steering Torque Sensor	Detects how much torque the driver is applying to the steering wheel
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Calculates the driver demanded torque based on the input from the steering torque sensor
EPS ECU - Normal Lane Assistance Functionality	Generates torque requests for LDW and LKA functions based on input from the camera system
EPS ECU - Lane Departure Warning Safety Functionality	Checks torque request input against safe amplitude and frequency limits as well as maximum delay and outputs appropriate torque request and error signals
EPS ECU - Lane Keeping Assistant Safety Functionality	Checks the duration of the input torque request against safe maximum duration and outputs appropriate torque request and error signals
EPS ECU - Final Torque	Calculates the torque sent to the motor based on the driver torque demand and torque requests from the LDW and LKA safety components
Motor	Applies commanded torque directly to 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	The LA Item shall ensure that the LDW oscillating torque amplitude	X		

Requirement 01-01	is below *Max_Torque_Amplitude*			

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 Torque* component is below *Max_Torque_Amplitude*	C	50 ms	LDW Safety	*LDW_Torque_Request* is set to zero
Technical Safety Requirement 02	As soon as the LDW function deactivates the LDW feature, the *LDW Safety* component shall send a signal to the car display ECU to turn on a warning light	C	50 ms	LDW Safety	*LDW_Torque_Request* is set to zero
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	*LDW_Torque_Request* is 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	*LDW_Torque_Request* is set to zero
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	*LDW_Torque_Request* is 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 LA Item shall ensure that the LDW oscillating torque amplitude 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 Torque* component is below *Max_Torque_Frequency*	C	50 ms	LDW Safety	*LDW_Torque_Request* is set to zero
Technical Safety Requirement 02	As soon as the LDW function deactivates the LDW feature, the *LDW Safety* component shall send a signal to the car display ECU to turn on a warning light	C	50 ms	LDW Safety	*LDW_Torque_Request* is set to zero
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	*LDW_Torque_Request* is 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	*LDW_Torque_Request* is set to zero

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	*LDW_Torque_Request* is set to zero

Functional Safety Requirement 01-3 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 LA Item shall ensure that the LDW oscillating torque is applied within *Max_ Delay*	X		

Technical Safety Requirements related to Functional Safety Requirement 01-03 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 *LDW_Torque_Request* is sent to the *Final Torque* component within *Max_Delay* of the *Camera_Torque_Request* signal being received from the *Torque Request Generator* component	C	50 ms	LDW Safety	*LDW_Torque_Request* is set to zero
Technical Safety Requirement 02	As soon as the LDW function deactivates the LDW feature, the *LDW Safety* component shall send a signal to the car display ECU to turn on a warning light	C	50 ms	LDW Safety	*LDW_Torque_Request* is set to zero

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	*LDW_Torque_Request* is 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	*LDW_Torque_Request* is set to zero
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	*LDW_Torque_Request* is set to zero

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

[OPTIONAL]

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 LA Item shall ensure that the LKA 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 *LKA_Torque_Request* is sent to the *Final Torque* component for not more than *Max_Duration*	B	500 ms	LKA Safety	*LKA_Torque_Request* is set to zero
Technical Safety Requirement 02	As soon as the LKA function deactivates the LKA feature, the *LKA Safety* component shall send a signal to the car display ECU to turn on a warning light	B	500 ms	LKA Safety	*LKA_Torque_Request* is set to zero
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	*LKA_Torque_Request* is 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	*LKA_Torque_Request* is set to zero
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory	B	Ignition Cycle	Memory Test	*LKA_Torque_Request* is set to zero

Functional Safety Requirement 02-2 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 02-02	The LA Item shall ensure that the LKA torque amplitude is greater than *Min_Torque_Amplitude*	X		

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

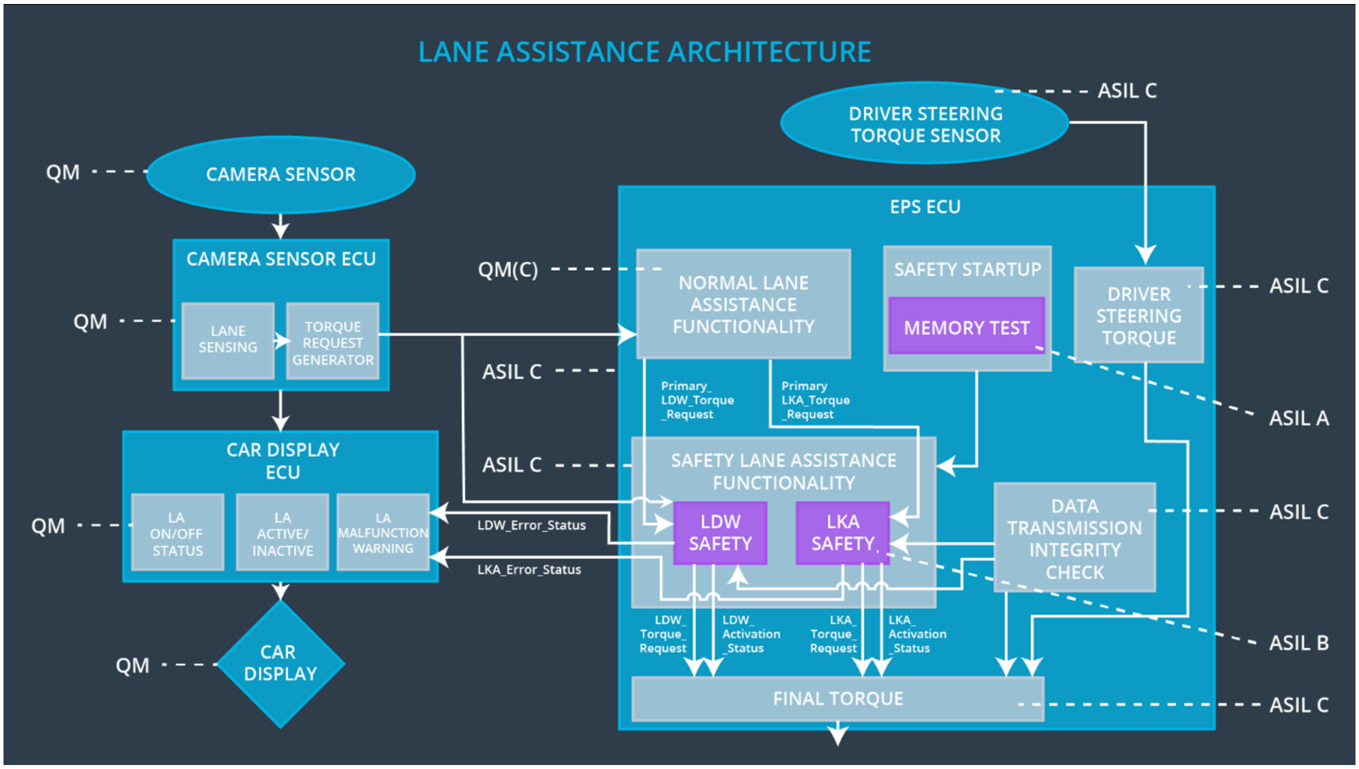
ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01	The *LKA Safety* component shall ensure that the amplitude of the *LKA_Torque_Request* sent to the *Final Torque* component is greater than *Min_Torque_Amplitude*	QM	500 ms	LKA Safety	*LKA_Torque_Request* is set to zero
Technical Safety Requirement 02	As soon as the LKA function deactivates the LKA feature, the *LKA Safety* component shall send a signal to the car display ECU to turn on a warning light	QM	500 ms	LKA Safety	*LKA_Torque_Request* is set to zero
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	QM	500 ms	LKA Safety	*LKA_Torque_Request* is set to zero
Technical Safety Requirement 04	The validity and integrity of the data transmission for *LKA_Torque_Request* signal shall be ensured	QM	500 ms	Data Transmission Integrity Check	*LKA_Torque_Request* is set to zero
Technical	Memory test shall be conducted	Q	Ignition	Memory Test	*LKA_Torqu*

Safety Requirement 05	at start up of the EPS ECU to check for any faults in memory	M	Cycle		*e_Request* is set to zero

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

[OPTIONAL]

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

For the Lane Assistance 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 LDW functionality	Malfunction_01, Malfunction_02, Malfunction_03	YES	Warning light on car display
WDC-02	Turn off LKA functionality	Malfunction_04, Malfunction_05	YES	Warning light on car display