Technical Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
24/5/2018	1.0	Vivek Pathak	First Attempt
25/5/2018	1.1	Vivek Pathak	Second Attempt

Table of Contents

Purpose of the Technical Safety Concept

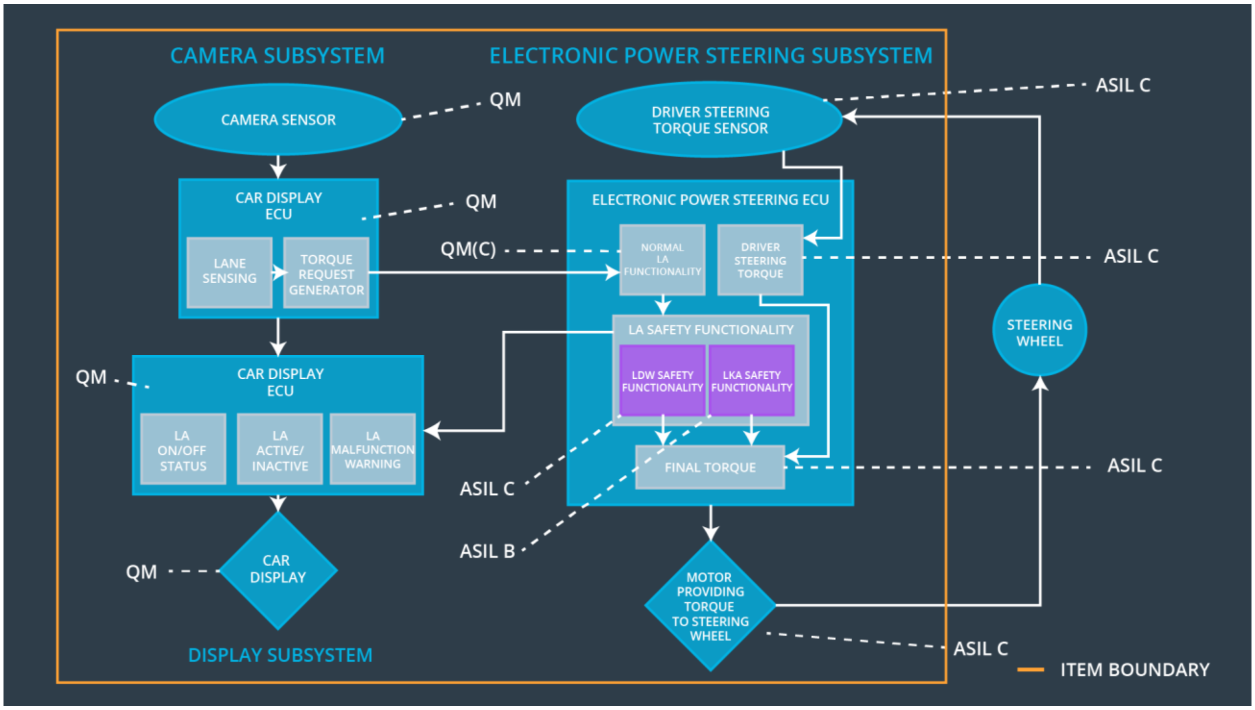
In this document we look into technical safety of every sub-systems and we separately define safety concept for each sub-systems as according to ISO-26262 they are more specific and underlie what is happening in more deep.

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 keeping item shall ensure that torque is below Max_Torque_Amplitude.	C	50 ms	Vibration torque amplitude below Max_Torque_Amplitude.
Functional Safety Requirement 01-02	The Lane keeping item shall ensure that lane departure oscillating torque frequency is below Max_Torque_Frequency.	C	50 ms	Vibration frequency is below Max_Torque_Frequency.
Functional Safety Requirement 02-01	LKA function shall be time limited for max_duration	B	500 ms	Set the LKA torque to zero

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Capture images and provide them to the Camera Sensor ECU.
Camera Sensor ECU - Lane Sensing	Detect lane line and calculate position of the car with respect to lane
Camera Sensor ECU - Torque request generator	Generate torque request to the car for ECU.
Car Display	Display status of malfunctioning of the system.
Car Display ECU - Lane Assistance On/Off Status	Indicate the status of the Lane Assistance functionality (On/Off.)
Car Display ECU - Lane Assistant Active/Inactive	Indicate if the Lane Assistance functionality is properly functioning (Active/Inactive.)
Car Display ECU - Lane Assistance malfunction warning	Indicate a malfunction on the Lane Assistance functionality.
Driver Steering Torque Sensor	Measure the torque applied to the steering wheel

	by the driver.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	On receiving the driver's torque request from the steering wheel.
EPS ECU - Normal Lane Assistance Functionality	On receiving the Camera Sensor ECU torque request.
EPS ECU - Lane Departure Warning Safety Functionality	On ensuring the torque amplitude is below Max_Torque_Amplitude and torque frequency is below Max_Torque_Frequency.
EPS ECU - Lane Keeping Assistant Safety Functionality	On ensuring the Lane Keeping Assistance functionality application is not activate more than Max_duration time.
EPS ECU - Final Torque	Combine the torque request from the Lane Keeping and Lane Departure Warning functionalities and sends them to the Motor.
Motor	Applies the required torque to the steering wheels.

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	LDW system shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	Responsible	Not Responsible	Not Responsible

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 Lane Departure Warning 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	LDW torque shall be set to zero.
Technical Safety Requirement 02	As soon as the Lane Departure Warning is deactivated, the 'LDW Safety' software module shall send a signal to the Car Display ECU to turn on a warning signal.	C	50 ms	LDW Safety	LDW torque shall be set to zero.
Technical Safety Requirement 03	As soon as when a failure is detected by the Lane Departure Warning functionality, it shall deactivate the Lane Departure Warning feature and set 'LDW_Torque_Request' to zero.	C	50 ms	LDW Safety	LDW torque 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	LDW Safety	LDW torque shall be set to zero.
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any memory problems	A	Ignition cycle	Data Transmission Integrity Check	LDW torque 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	Responsible	Not Responsible	Not Responsible

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 Lane Departure Warning 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	LDW torque shall be set to zero.
Technical Safety Requirement 02	With time when the Lane Departure Warning is deactivated, the 'LDW Safety' software module shall send a signal to the Car Display ECU to turn on a warning signal.	C	50 ms	LDW Safety	LDW torque shall be set to zero.
Technical Safety Requirement 03	With time when a failure is detected by the Lane Departure Warning functionality, it shall deactivate the Lane Departure Warning feature and set 'LDW_Torque_Request' to zero.	C	50 ms	LDW Safety	LDW torque 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	LDW Safety	LDW torque shall be set to zero.
Technical	Memory test shall be conducted at	A	Ignition	Data	LDW

Safety Requirement 05	start up of the EPS ECU to check for any memory problems		cycle	Transmission Integrity Check	torque 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	Responsible	Not Responsible	Not Responsible

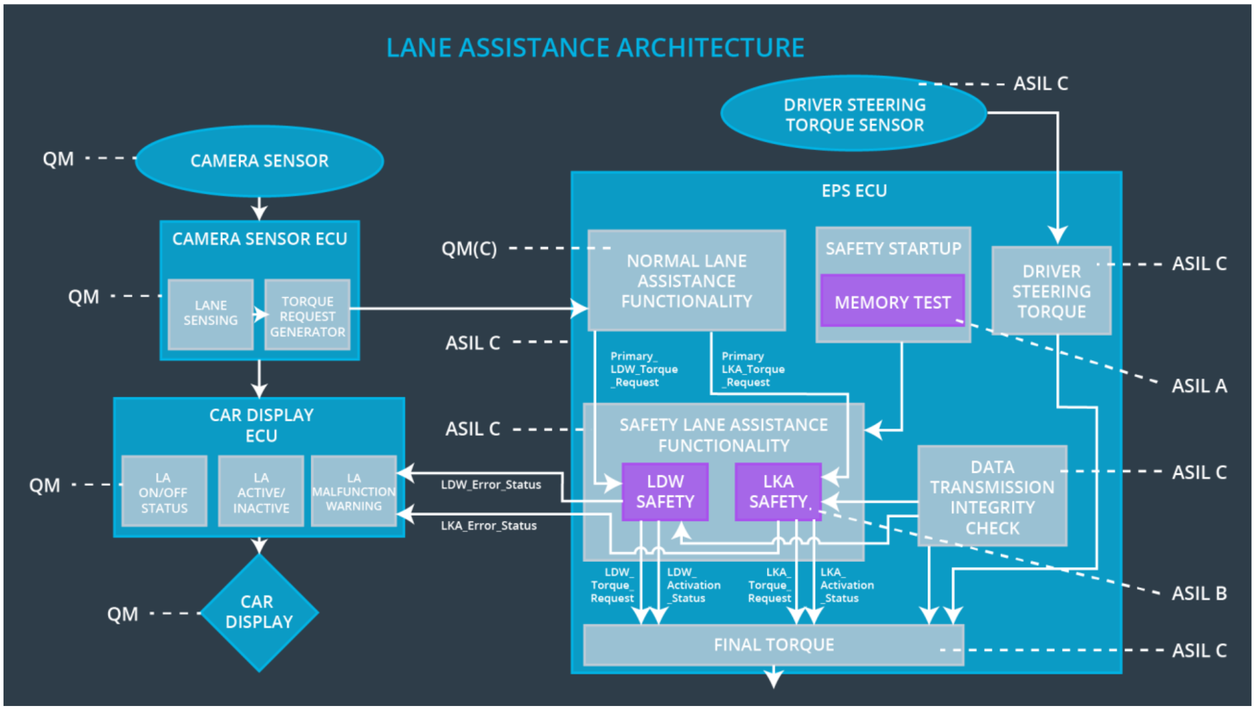
Technical Safety Requirements related to Functional Safety Requirement 02-01 are:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01	The Lane Keeping Assistance safety component shall ensure the duration of the lane keeping assistance torque is applied for less than Max_Duration	C	500 ms	LKA Safety	Lane Keeping Assistance torque to zero.
Technical Safety Requirement 02	With time when the Lane Keeping Assistance function deactivates, the ‘LKA Safety’ shall send a signal to the Car Display ECU to turn on a warning light.	C	500 ms	LKA Safety	Lane Keeping Assistance torque to zero.
Technical Safety Requirement 03	With time when a failure is detected, the Lane Keeping Assistance function shall deactivate and the ‘LKA_Torque_Request’ shall be zero.	C	500 ms	LKA Safety	Lane Keeping Assistance torque to zero.

Technical Safety Requirement 04	The validity and integrity of the data transmission for ‘LKA_Torque_Request’ signal shall be ensured.	C	500 ms	LKA Safety	Lane Keeping Assistance torque to zero.
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any memory problems	A	Ignition cycle	Data Transmission Integrity Check	Lane Departure Warning torque to zero.

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

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

ID	**Functional Safety Requirement**	**Electronic Power**	**Camera ECU**	**Car Display ECU**

		Steering ECU		
Functiona l Safety Requirement 01-01	The Lane Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	**Responsible**	**Not Responsible**	**Not Responsible**
Functional Safety Requirement 01-02	The Lane Departure Warning item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	**Responsible**	**Not Responsible**	**Not Responsible**
Functional Safety Requirement 01-03	The Lane Departure Warning function shall be deactivated when the camera sensor stop working.	**Responsible**	**Not Responsible**	**Not Responsible**

Warning and Degradation Concept

ID	**Degradation Mode**	**Trigger for Degradation Mode**	**Safe State invoked?**	**Driver Warning**
WDC-01	Turn off Warning functionality	Malfunction_01, Malfunction_02	Yes	Light displayed on dashboard and on car as warnings
WDC-02	Turn off Assistance functionality	Malfunction_03	Yes	Light displayed on dashboard and on car as warnings