Technical Safety Concept Lane Assistance

Document Version: 1.0

Document history

Date	Version	Editor	Description
2019-04-19	1.0	Justin Simerly	First submission.

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....3
  - Functional overview of architecture elements....4

Technical Safety Concept....5
- Technical Safety Requirements....5
- Refinement of the System Architecture....11
- Allocation of Technical Safety Requirements to Architecture Elements....11
- Warning and Degradation Concept....12

Purpose of the Technical Safety Concept

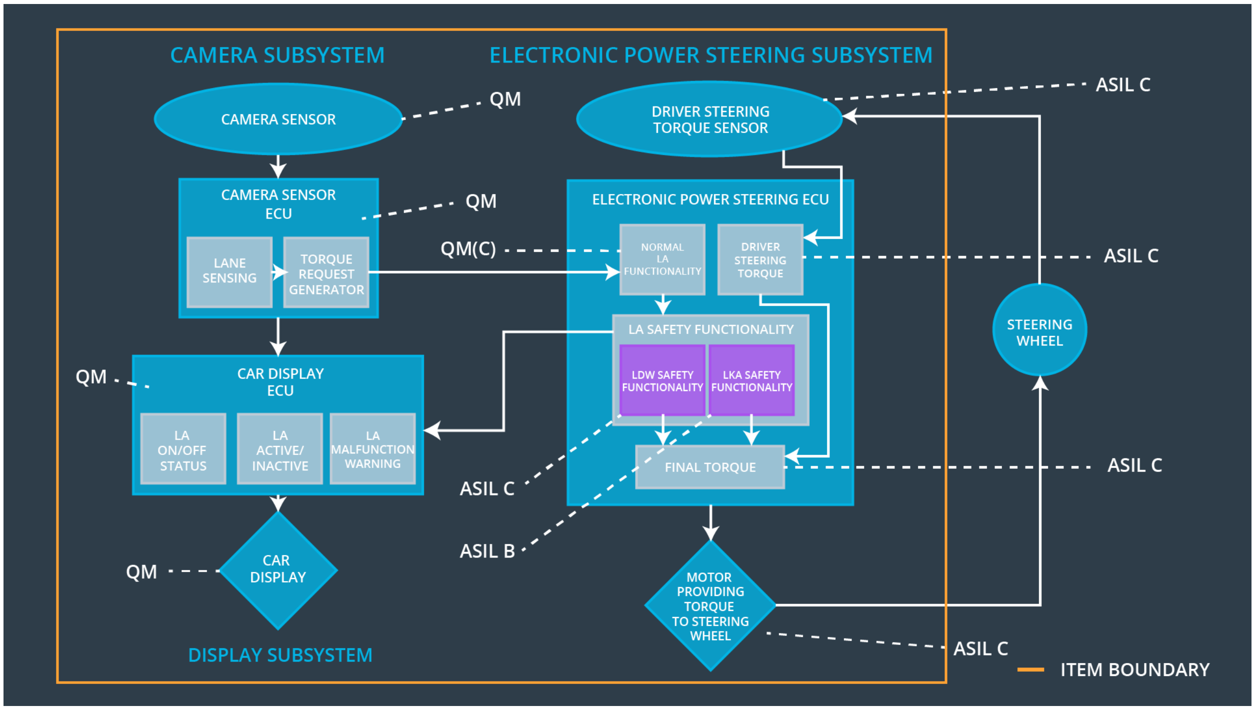
The technical safety concept turns functionality safety requirements into technical safety requirements and allocates technical safety requirements to the system architecture.

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	The torque request from the lane keeping assistance item will be set to 0.
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	The torque request from the lane keeping assistance item will be set to 0.
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 torque request from the lane keeping assistance item will be set to 0.

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	**Description**
Camera Sensor	Provides the camera input.
Camera Sensor ECU - Lane Sensing	Derives lanes from the camera sensor.
Camera Sensor ECU - Torque request generator	Requests the desired steering wheel torque.
Car Display	Controls the output of the car dashboard.
Car Display ECU - Lane Assistance On/Off Status	Stores the status of the Lane Assistant.
Car Display ECU - Lane Assistant Active/Inactive	Stores the activation status of the Lane Assistant.
Car Display ECU - Lane Assistance malfunction warning	Stores if the Lane Assistant has detected a malfunction.
Driver Steering Torque Sensor	Measures the torque applied to the steering wheel.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Receives the torque measured from the Driver Steering Torque Sensor.
EPS ECU - Normal Lane Assistance Functionality	Processes the requested steering wheel torque.
EPS ECU - Lane Departure Warning Safety Functionality	Requests the final steering wheel torque while ensuring the safety of the Lane Departure Warning function.
EPS ECU - Lane Keeping Assistant Safety Functionality	Requests the final steering wheel torque while ensuring the safety of the Lane Keeping Assistant function.
EPS ECU - Final Torque	Receives the final steering wheel torque.
Motor	Applies the Final Torque to 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	‘LDW_Torque_Request’ Amplitude shall be set to zero.
Technical Safety Requirement 02	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’ Amplitude shall be 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’ Amplitude shall be set to zero.
Technical Safety Requirement 04	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	‘LDW_Torque_Request’ Amplitude shall be set to zero.
Technical Safety Requirement 05	Memory test shall be coonducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Safety Startup	‘LDW_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	‘LDW_Torque _Request’ Frequency shall be set to zero.
Technical Safety Requirement 02	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’ Frequency shall be 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’ Frequency shall be set to zero.
Technical Safety Requirement 04	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	‘LDW_Torque _Request’ Frequency shall be set to zero.
Technical Safety Requirement 05	Memory test shall be coonducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Safety Startup	‘LDW_Torque _Request’ Frequency shall be set to zero.

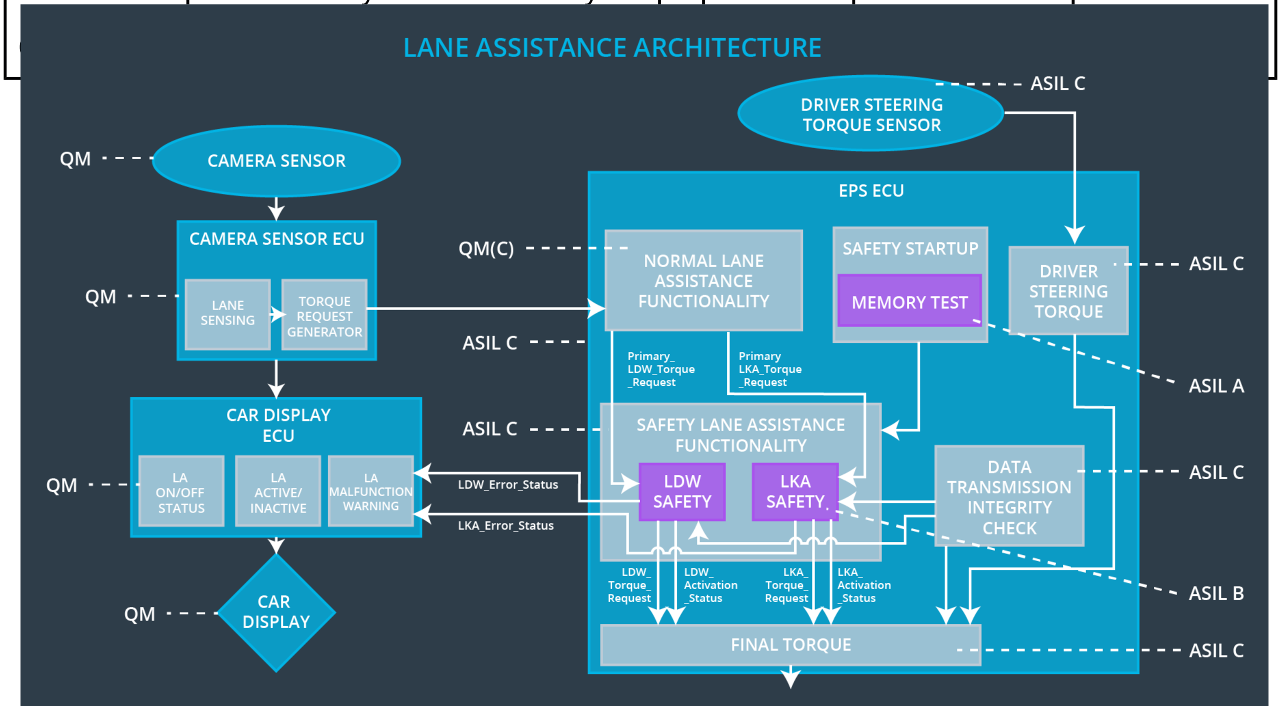
Lane Keeping Assistance (LKA) Requirements:

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 the ‘LKA_Torque_Request’ is sent to the ‘Final electronic power steering Torque’ component for only Max_Duration.	B	500 ms	LKA Safety	‘LKA_Torque _Request’ shall be set to zero.
Technical Safety Requirement 02	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’ shall be 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’ shall be set to zero.
Technical Safety Requirement 04	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	‘LKA_Torque _Request’ shall be set to zero.
Technical Safety Requireme	Memory test shall be coonducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Safety Startup	‘LKA_Torque _Request’ shall be set



Warning and Degradation Concept

ID	**Degradation Mode**	**Trigger for Degradation Mode**	**Safe State invoked?**	**Driver Warning**
WDC-01	Turn off the Lane Departure Warning functionality.	The lane departure warning function applies an oscillating torque with very high torque amplitude (above limit).	yes	Car Display shows a Lane Assist Malfunction Warning.
WDC-02	Turn off the Lane Keeping Assistance functionality.	The lane keeping assistance function is not limited in time duration which leads to misuse as an autonomous driving function.	yes	Car Display shows a Lane Assist Malfunction Warning.