Technical Safety Concept Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
2017-08-23	1.0	Y.Wiyogo	Initial Document
2017-08-24	1.1	Y.Wiyogo	Complete LKA requirements and warning
2017-08-26	1.2	Y.Wiyogo	Correct ASIL of LKA and extend the description of the EPS ECU elements

Table of Contents

Purpose of the Technical Safety Concept

The purpose of the technical safety concept is to specify the realization of the defined functional safety concept.

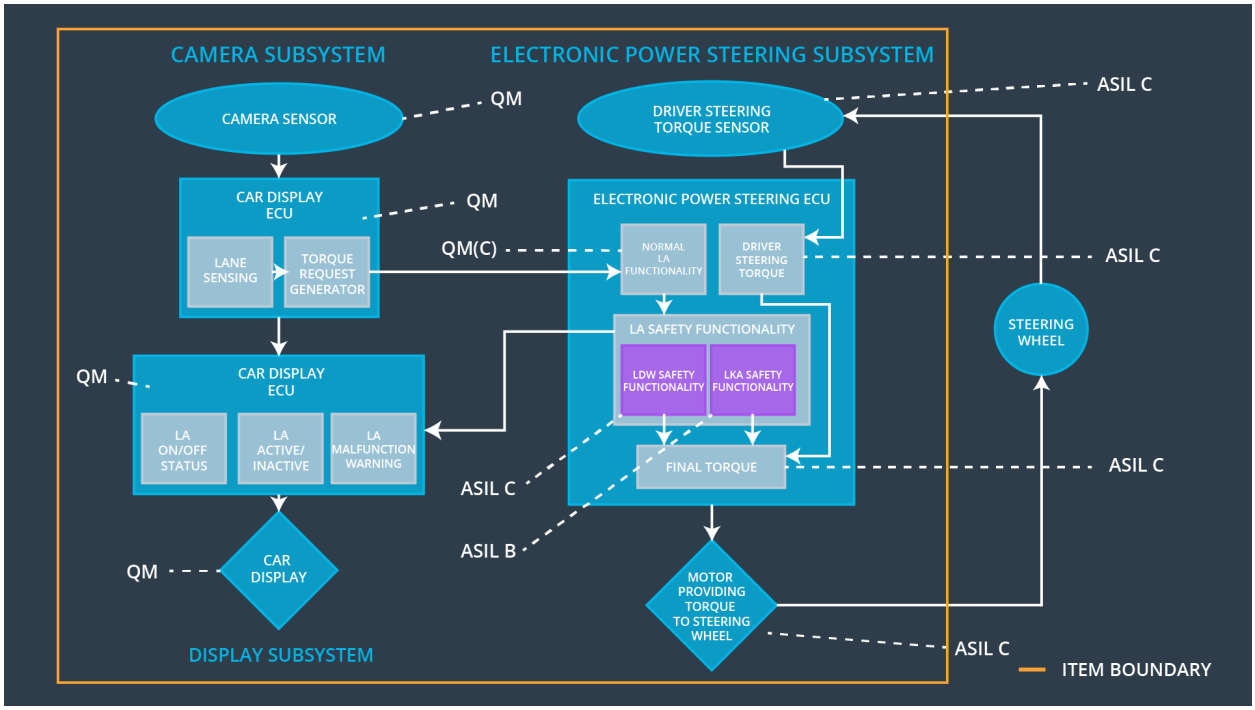
Inputs to the Technical Safety Concept

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 the lane departure oscillating torque amplidute is below Max_Torque_Amplitude	C	50 ms	Turn off LDW
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50 ms	Turn off LDW
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	Turn off LKA

Refined System Architecture from Functional Safety Concept

[Instructions: Provide the refined system architecture from the functional safety concept]



Functional overview of architecture elements

[Instructions: Provide a description for each functional safety element; what is each element's purpose in the lane assistance item?]

Element	Description
Camera Sensor	A sensor for aquiring environment information as image.
Camera Sensor ECU - Lane Sensing	A function that extracts the lane detection
Camera Sensor ECU - Torque request generator	A function that generates
Car Display	A display device for visualizing the activation of the function to the driver.
Car Display ECU - Lane Assistance On/Off Status	A function to control the on/off status on the display
Car Display ECU - Lane Assistant Active/Inactive	A function to control the active/inactive status on the display
Car Display ECU - Lane Assistance malfunction warning	A function to control the malfunction warning on the display

Driver Steering Torque Sensor	A sensor that acquires the torque value of the steering wheel
Electronic Power Steering (EPS) ECU - Driver Steering Torque	A processor chip for processing data from camera sensor ECU and torque sensor.
EPS ECU - Normal Lane Assistance Functionality	A function to process the data from the torque request generator
EPS ECU - Lane Departure Warning Safety Functionality	A function to ensure the LDW safety functionality
EPS ECU - Lane Keeping Assistant Safety Functionality	Sends LKA_Torque_Request and LKA_Activation_Status to the EPS ECU Final Torque. The LKA_Torque_Request tells about the torque to be applied and the LKA_Activation_Status tells about whether LKA
EPS ECU - Final Torque	Find the final torque that needs to be applied to the steering wheel. Takes into account the inputs from LDW Safety, LKA Safety, Data Transmission and Integrity Check.
Motor	An electric motor that interpret the EPS ECU data to control 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	The lane keeping item shall	X		

Requirement 01-01	ensure that the lane departure oscillating torque amplitude 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 electronic power steering Torque' component is below 'Max_Torque_Amplitude.	C	50 ms	LDW safety	LDW_Torque_Output= 0
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	N/A
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_Output= 0
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_Output= 0
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_Output= 0

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_Output = 0
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	N/A
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_Output = 0
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_Output = 0

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_Output= 0

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

[OPTIONAL: For each technical safety requirement, identify both the verification and validation acceptance criteria. “Validation” asks whether or not you chose the appropriate parameters. “Verification” involves testing to make sure the vehicle behaves as expected when the parameter value is crossed. There is not necessarily one right answer. Look at your verification and validation acceptance criteria from the functional safety concept for inspiration.]

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:

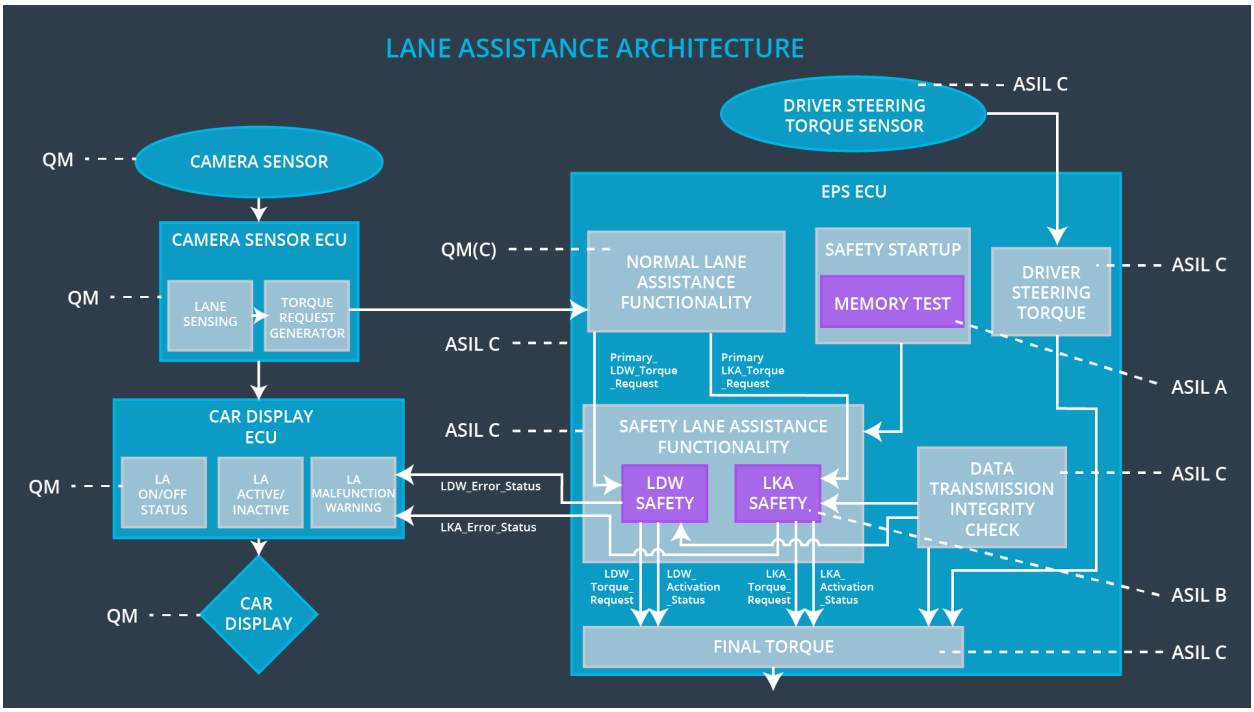
ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01	The LKA safety component shall ensure that the active duration time is below Max_Duration.	B	500 ms	LKA safety	LKA_Torque_Output = 0

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	N/A
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_Output = 0
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_Output = 0
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory	A	500 ms	Memory Test	LKA_Torque_Output = 0

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

[OPTIONAL: For each technical safety requirement, identify both the verification and validation acceptance criteria. “Validation” asks whether or not you chose the appropriate parameters. “Verification” involves testing to make sure the vehicle behaves as expected when the parameter value is crossed. There is not necessarily one right answer. Look at your verification and validation acceptance criteria from the functional safety concept for inspiration.]

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

Based on the above tables, all technical safety requirements are allocated to the Electronic Power Steering ECU.

Warning and Degradation Concept

The technical safety requirements have not changed how functionality will be degraded or what the warning will be. Thus, the warning and degradation concept is the same for the technical safety requirements as for the functional safety requirements.

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	turn off the function	Is_Max_Torque_ Exceeded	Yes	Turn on warning light on car display
WDC-02	turn off the function	Is_Max_Duration _Exceeded	Yes	Turn on warning light on car display