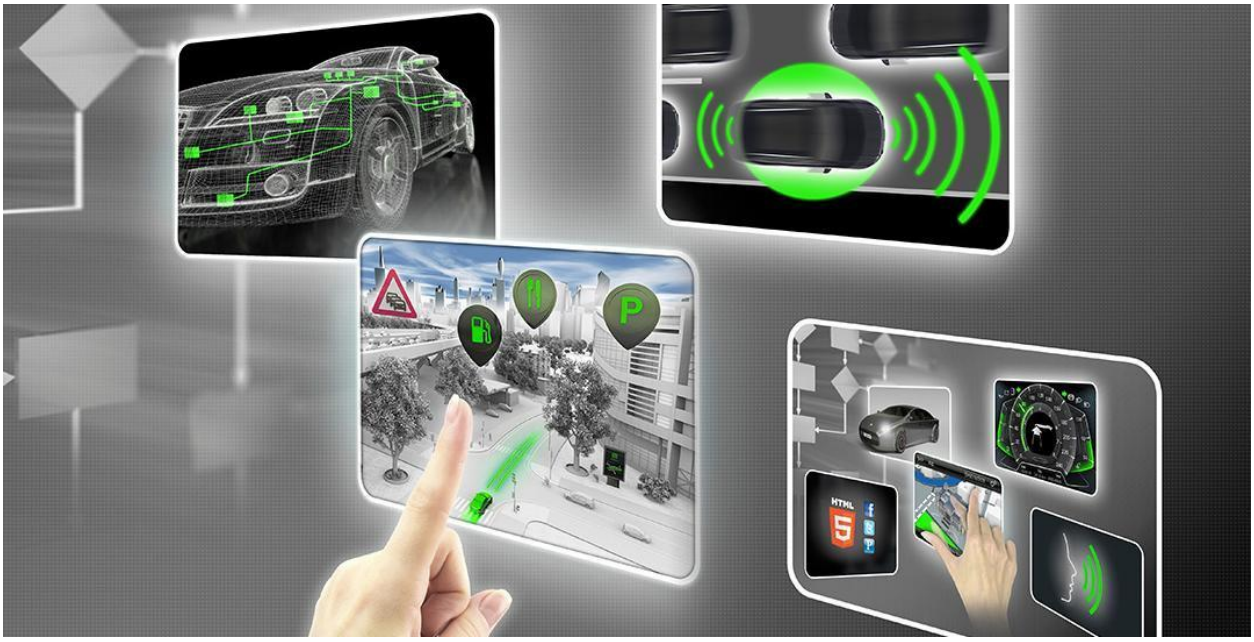


Technical Safety Concept Lane Assistance

Document Version: 1.2, Submitted on 2019-05-02
Template Version: 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
8/30/2018	1.0	Nathan	First Creation
9/2/2018	1.1	Nathan	Error Corrected
5/2/2019	1.2	Nathan	ASIL Level Corrected

Table of Contents

Purpose of the Technical Safety Concept

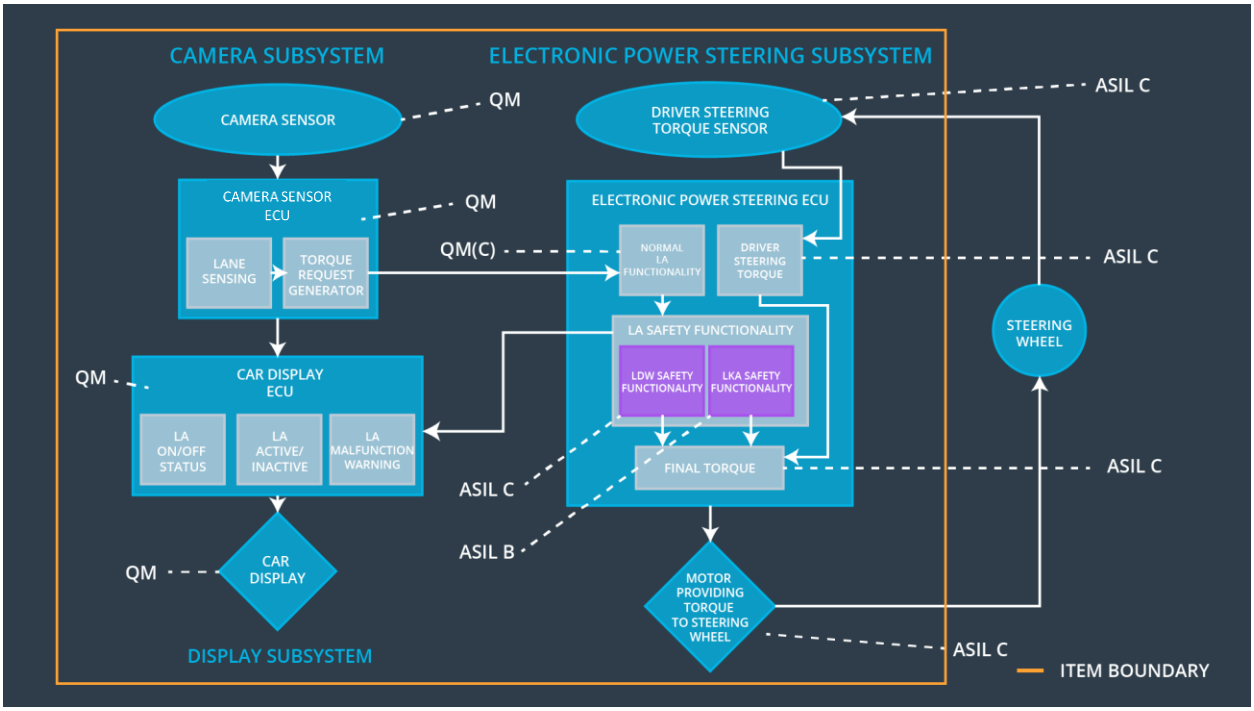
The purpose of the technical safety concept is to turn functional safety requirements into technical safety requirements and to allocate technical safety requirements to the system architecture.

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 lane assistance item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	The lane departure oscillating torque amplitude is below Max_Torque_Amplitude
Functional Safety Requirement 01-02	The lane assistance item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50 ms	The lane departure oscillating torque frequency is below Max_Torque_Frequency
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only up to Max_Duration	B	500 ms	The lane keeping assistance torque apply duration is below Max_Duration
Functional Safety Requirement 03-01	The lane keeping item shall ensure that the light sensitivity change of lane departure camera ECU is higher than Min_Lumen_Change	B	20 ms	The light sensitivity change of lane departure camera sensor is higher than Min_Lumen_Change
Functional Safety Requirement 03-02	The lane keeping item shall ensure that the light sensitivity change of lane departure camera sensor is below than Max_Lumen_Frequency	B	20 ms	The light sensitivity change of lane departure camera sensor is below than Max_Lumen_Frequency
Functional Safety Requirement 04-01	The electronic power steering ECU shall ensure its heat temperature is lower than Max_Temp	QM	100 ms	The lane keeping assistance electronic power steering ECU heat temperature is below Max_Temp

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Continuously read in images from the road
Camera Sensor ECU - Lane Sensing	Identify lanes from the images captured by camera, ensure the light sensitivity requirements are enforced
Camera Sensor ECU - Torque request generator	Request torque value base on how much the vehicle is deviated from the ego lane
Car Display	Let driver aware of lane assistance systems status
Car Display ECU - Lane Assistance On/Off Status	Light on/off on the dashboard to show the lane assistance is turned on or off
Car Display ECU - Lane Assistant Active/Inactive	Light on/off on the dashboard to show the lane keeping assistance status is active or inactive
Car Display ECU - Lane Assistance malfunction warning	Light on/off on the dashboard to show there is an issue with the lane assistance system

Driver Steering Torque Sensor	Read torque value how much steering torque the driver applied through the steering wheel
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Convert torque value the driver steering torque sensor read and sends messages to final torque ECU
EPS ECU - Normal Lane Assistance Functionality	Read request messages from the camera sensor ECU
EPS ECU - Lane Departure Warning Safety Functionality	Ensure that the lane departure warning related requirements are enforced
EPS ECU - Lane Keeping Assistant Safety Functionality	Ensure that the lane keeping assistant related requirements are enforced
EPS ECU - Final Torque	Generate final torque value and controls the EPS motor
Motor	Generate physical torque base on final torque value

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	Amplitude of the 'LDW_Torque_Request' < 'Max_Torque_Amplitude'
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	Lane Assist Malfunction warning light ON
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	Amplitude of the 'LDW_Torque_Request' = 0 if > 'Max_Torque_Amplitude'
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 validity and integrity of the data transmission ensured
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	Memory check run at safety startup

Functional Safety Requirement 01-2 with its associated system elements

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	Frequency of the 'LDW_Torque_ Request' < 'Max_Torque_ Frequency’
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	Lane Assist Malfunction warning light ON
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	Freqeuncy of the 'LDW_Torque_ Request' = 0 if > 'Max_Torque _Frequency’
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 validity and integrity of the data transmission ensured
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	Memory check run at safety startup

Functional Safety Requirement 03-1 with its associated system elements

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 03-01	The lane keeping item shall ensure that the light sensitivity change of lane departure camera ECU is higher than Min_Lumen_Change		X	

Technical Safety Requirements related to Functional Safety Requirement 03-01 are:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 01	The Camera safety component shall ensure that the light sensitivity change of camera ECU is higher than Min_Lumen_Change	B	20 ms	Camera Safety	The light sensitivity change of camera ECU is higher than Min_Lumen_ Change
Technical Safety Requirement 02	As soon as the LDW function deactivates the LDW feature, the 'Camera Safety' software block shall send a signal to the car display ECU to turn on a warning light.	B	20 ms	Camera Safety	Lane Assist Malfunction warning light ON
Technical Safety Requirement 03	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and 'Primary_LDW_Torque_Request' from ‘Torque Request Generator’ shall be set to zero.	B	20 ms	Camera Safety	'Primary_LDW_Torque_ Request' = 0 if failure is detected
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'Primary_LDW_Torque_Request' signal shall be ensured.	B	20 ms	Data Transmission Integrity Check	The validity and integrity of the data transmission ensured
Technical Safety Requirement 05	Memory test shall be conducted at start up of the Camera ECU to check for any faults in memory.	A	Ignition Cycle	Safety Startup	Memory check run at safety startup

Functional Safety Requirement 03-2 with its associated system elements

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 03-02	The lane keeping item shall ensure that the light sensitivity change of lane departure camera sensor is below than Max_Lumen_Frequency		X	

Technical Safety Requirements related to Functional Safety Requirement 03-02 are:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 01	The Camera safety component shall ensure that the light sensitivity change of camera ECU is lower than Max_Lumen_Frequency	B	20 ms	Camera Safety	The light sensitivity change of camera ECU is lower than Max_Lumen_ Frequency
Technical Safety Requirement 02	As soon as the LDW function deactivates the LDW feature, the 'Camera Safety' software block shall send a signal to the car display ECU to turn on a warning light.	B	20 ms	Camera Safety	Lane Assist Malfunction warning light ON
Technical Safety Requirement 03	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and 'Primary_LDW_Torque_Request' from ‘Torque Request Generator’ shall be set to zero.	B	20 ms	Camera Safety	'Primary_LDW_Torque_ Request' = 0 if failure is detected
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'Primary_LDW_Torque_Request' signal shall be ensured.	B	20 ms	Data Transmission Integrity Check	The validity and integrity of the data transmission ensured
Technical Safety Requirement 05	Memory test shall be conducted at start up of the Camera ECU to check for any faults in memory.	A	Ignition Cycle	Safety Startup	Memory check run at safety startup

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

(Technical Safety Requirements related to Functional Safety Requirement 03-01 and 03-02 are not addressed)

Validation: Perform experiment to test how drivers react to different torque amplitudes and frequencies. Acceptance criteria is the torque amplitude and frequency values low enough that the drivers can regain steering control easily during the vibration but higher than the vibration value that the driver can notice the LDW when the vehicle deviate from the ego lane.

Verification: Perform a software test, inserting a fault into the system - when the torque amplitude or frequency crosses the limit. Acceptance criteria is when the lane assistance output set to zero within the 50 ms fault tolerant time interval if either amplitude or frequency exceeded 'Max_Torque_Amplitude’ or 'Max_Torque_Frequency.’

Lane Keeping Assistance (LKA) Requirements:

Functional Safety Requirement 02-1 with its associated system elements

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 the 'LKA_Torque_Request' sent to the 'Final electronic power steering Torque' component is below ‘Max_Duration’	B	500 ms	LKA Safety	Duration of the 'LKA_Torque_ Request' < 'Max_Duration’
Technical Safety Requirement 02	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	Lane Assist Malfunction warning light ON
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' = 0 if > 'Max_Duration’
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 validity and integrity of the data transmission ensured
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	Memory check run at safety startup

Functional Safety Requirement 04-1 with its associated system elements

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 04-01	The electronic power steering ECU shall ensure its heat temperature is lower than Max_Temp	X		

Technical Safety Requirements related to Functional Safety Requirement 04-01 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 its heat temperature is lower than Max_Temp	QM	100 ms	LKA Safety	EPS ECU heat temperature is below Max_Temp
Technical Safety Requirement 02	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.	QM	100 ms	LKA Safety	Lane Assist Malfunction warning light ON
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	100 ms	LKA Safety	'LKA_Torque_Request' = 0 if > 'Max_Duration’
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	QM	100 ms	Data Transmission Integrity Check	The validity and integrity of the data transmission ensured
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	Memory check run at safety startup

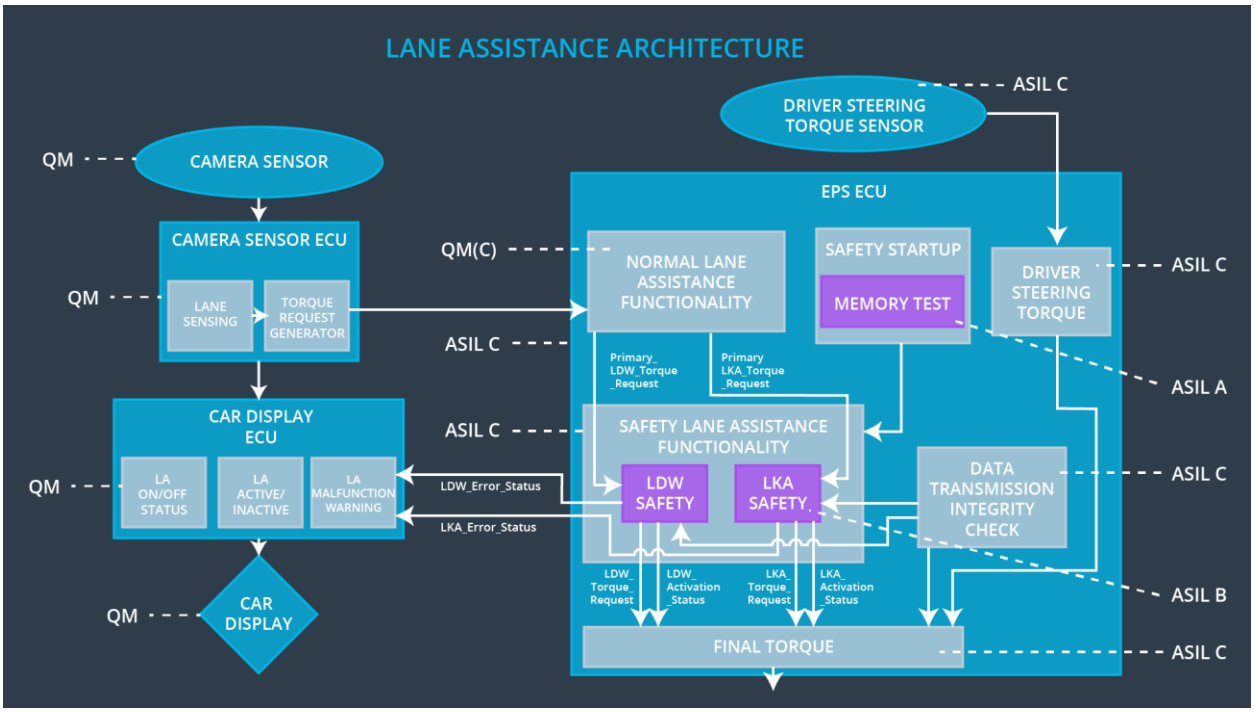
Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:
(Technical Safety Requirements related to Functional Safety Requirement 04-01 are not addressed)

Validation: Perform experiment to test what is the maximum duration of LKA function activated that dissuade drivers from taking their hands off the steering wheel. Acceptance criteria is the duration where drivers keep their hands on the steering wheel all the time.

Verification: Perform a software test, inserting a fault into the system - when the LKA system exceeds the duration limit. Acceptance criteria is the system turns off if the duration exceeded 'Max_Duration.'

Refinement of the System Architecture

(Technical Safety Requirements related to Functional Safety Requirement 03-01 and 03-02 are not reflected in the refinement)



Allocation of Technical Safety Requirements to Architecture Elements

For this project, all technical safety requirements are allocated to the Electronic Power Steering ECU. See Technical Safety Requirements tables for detailed allocation.

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01_01	Turn off	Oscillating torque amplitude is higher than Max_Torque_Amplitude	Yes	Warning light on the dashboard
WDC-01_02	Turn off	Oscillating torque frequency is higher than Max_Torque_Frequency	Yes	Warning light on the dashboard
WDC-02_01	Turn off	The lane keeping assistance stays on for longer than Max_Duration	Yes	Warning light on the dashboard
WDC-03_01	Turn off	The light sensitivity change exceeds a threshold Min_Lumen_Change	Yes	Warning light on the dashboard
WDC-03_02	Turn off	The light sensitivity change exceeds a threshold Max_Lumen_Frequency	Yes	Warning light on the dashboard
WDC-04_01	Turn off	The lane keeping assistance electronic power steering ECU heat temperature is higher than Max_Temp	Yes	Warning light on the dashboard