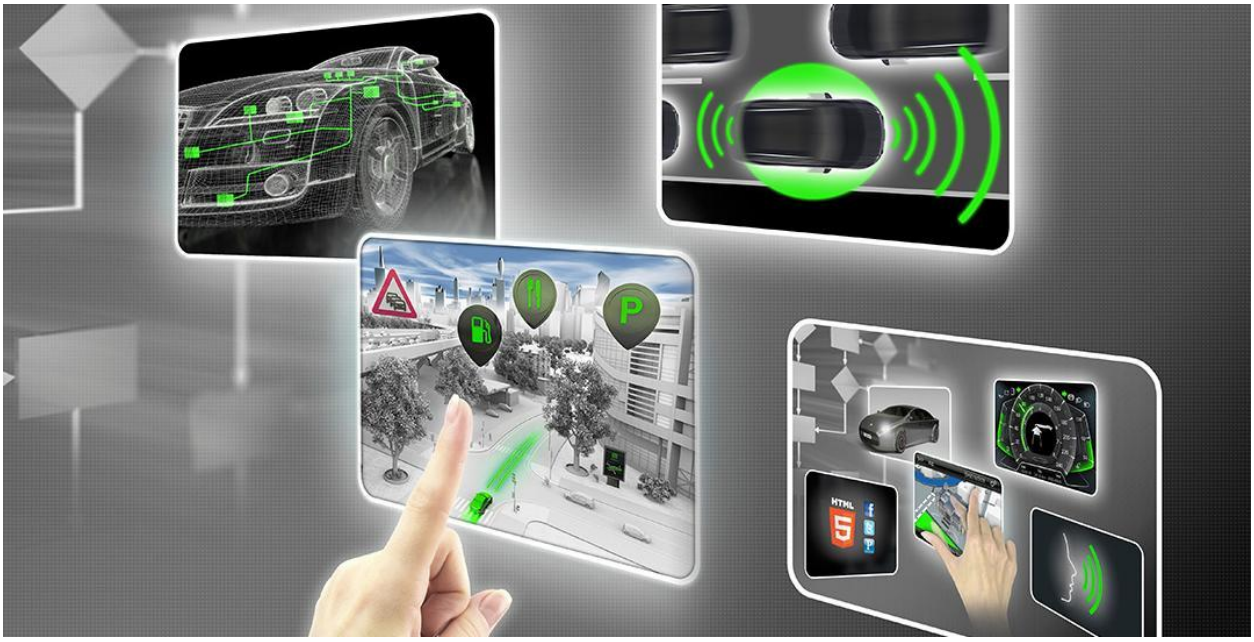


Technical Safety Concept Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
12/22/2018	1.0	Luis Güette	First Version

Table of Contents

Document history

Table of Contents

Purpose of the Technical Safety Concept

Inputs to the Technical Safety Concept
- Functional Safety Requirements
- Refined System Architecture from Functional Safety Concept
  - Functional overview of architecture elements

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

Purpose of the Technical Safety Concept

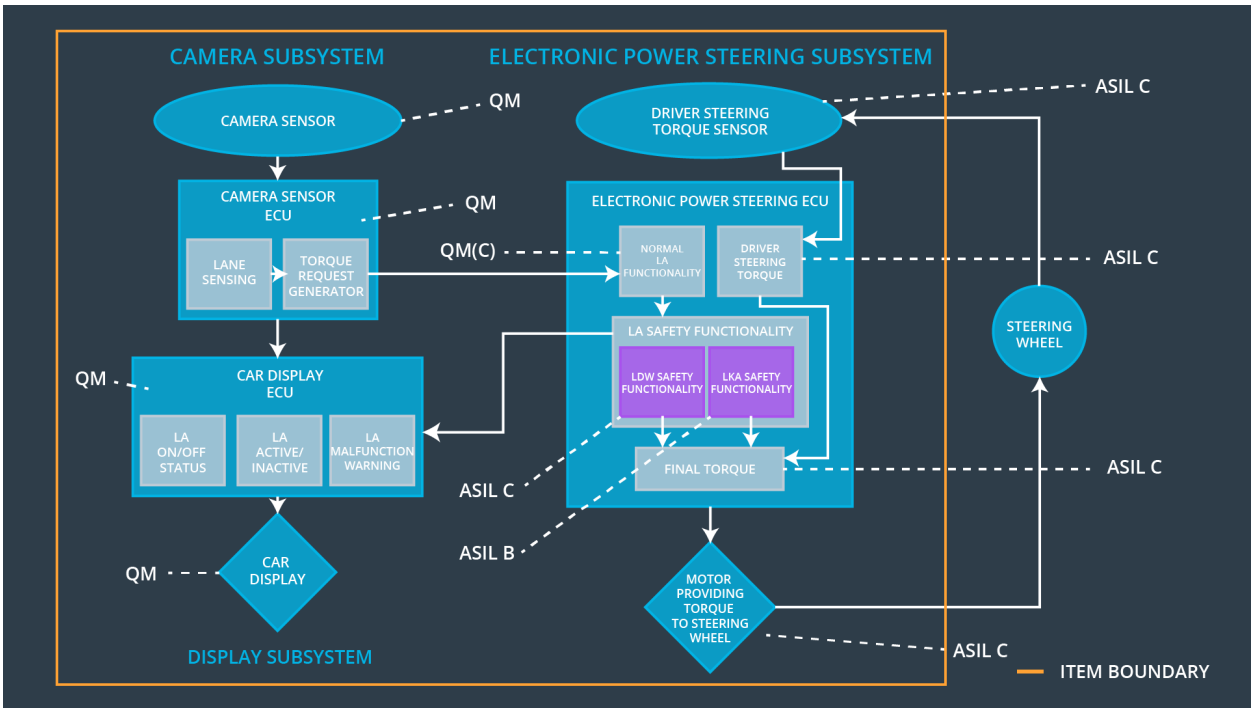
in this document, new requirements will be defined and allocated to the system architecture, these requirements are more concrete than the Functional Safety requirements.

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 Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	C	50ms	Vibration torque amplitude below Max_Torque_Amplitude.
Functional Safety Requirement 01-02	The Lane Departure Warning item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	C	50ms	Vibration frequency is below Max_Torque_Frequency.
Functional Safety Requirement 01-03	The Lane Departure Warning function shall be deactivated when the camera sensor stop working.	C	50ms	Function is deactivated
Functional Safety Requirement 02-01	The Lane Keeping Assistance function shall be time limited, and additional steering torque shall end after a Max_Duration interval so the driver cannot misuse the system for autonomous driving	B	500ms	LKS is turned of after a Max_Duration interval
Functional Safety Requirement 02-02	The Lane Keeping Assistance function shall be deactivated when the camera sensor stop working.	C	50ms	Function is deactivated

Refined System Architecture from Functional Safety Concept



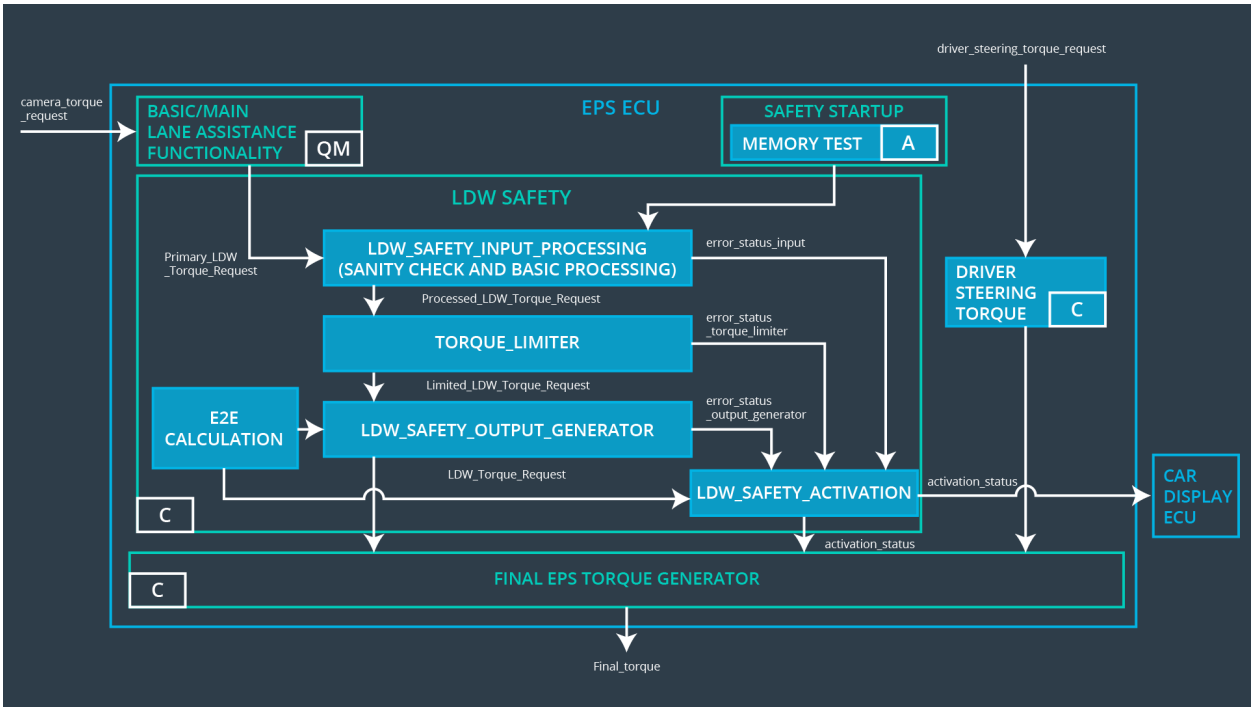
Functional overview of architecture elements

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

Element	Description
Camera Sensor	Capture road images and sends them to the Camera Sensor ECU
Camera Sensor ECU - Lane Sensing	Use Camera Sensor road images to detect lane lines
Camera Sensor ECU - Torque request generator	Use Camera Sensor road images to detect if an additional torque is required and sends it to the Electrical Power ECU
Car Display	Displays warnings to the driver
Car Display ECU - Lane Assistance On/ Off Status	Indicates LAS status
Car Display ECU - Lane Assistant Active/Inactive	Indicates if LAS is properly working

Car Display ECU - Lane Assistance malfunction warning	Indicates if LAS has a mallfunction
Driver Steering Torque Sensor	Senses the torque applied by the driver
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Receives the driver torque request from de Driver Steering Torque Sensor
EPS ECU - Normal Lane Assistance Functionality	Receives camera sensor images to decide if an torque request is needed
EPS ECU - Lane Departure Warning Safety Functionality	Ensures that the torque amplitude is below Max_Torque_Amplitude and torque frequency is below Max_Torque_Frequency
EPS ECU - Lane Keeping Assistant Safety Functionality	Ensures that the LKA active for no more than Max_Duration time
EPS ECU - Final Torque	Combine the torque requested by the driver and the torque requested by the LKA and sends it to the Motor
Motor	Applies the requested torque 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	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 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	50ms	LDW Safety	Lane Departure Warning torque to zero.
Technical Safety Requirement 02	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	50ms	LDW Safety	Lane Departure Warning torque to zero.
Technical Safety Requirement 03	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	50ms	LDW Safety	Lane Departure Warning torque to zero.
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensure	C	50ms	LDW Safety	Lane Departure Warning 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.

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 06	The Lane Departure Warning safety component shall ensure the frequency of the 'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Frequency.'	C	50ms	LDW Safety	Lane Departure Warning torque to zero.

Lane Keeping Assistance (LKA) Requirements:

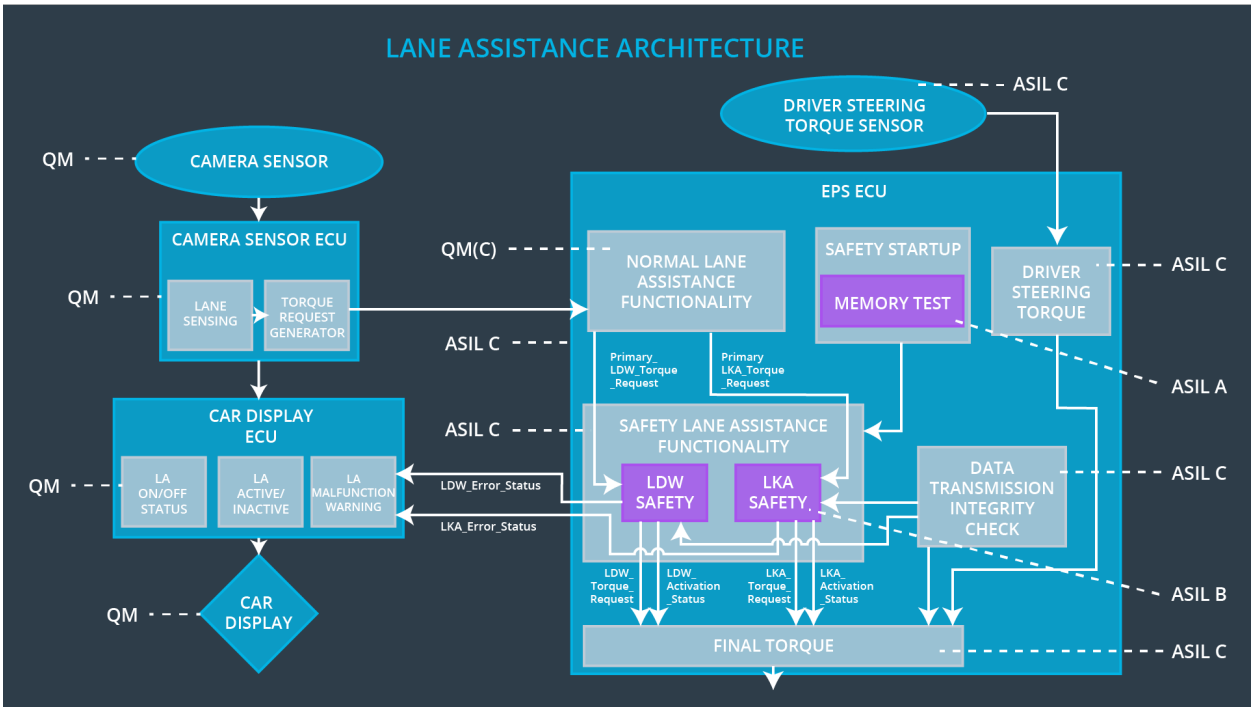
Functional Safety Requirement 02-1 with its associated system elements
(derived in the functional safety concept)

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 07	The Lane Keeping Assistance safety component shall ensure the duration of the lane keeping assistance torque is applied for less than Max_Duration.	C	500ms	LKA Safety	Lane Keeping Assistance torque to zero.
Technical Safety Requirement 08	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	500ms	LKA Safety	Lane Keeping Assistance torque to zero.
Technical Safety Requirement 09	When a failure is detected, the Lane Keeping Assistance function shall deactivate and the 'LKA_Torque_Request' shall be zero.	C	500ms	LKA Safety	Lane Keeping Assistance torque to zero.
Technical Safety Requirement 10	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	C	500ms	LKA Safety	Lane Keeping Assistance torque to zero.
Technical Safety Requirement 11	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 Keeping Assistance torque to zero.

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

ID	Technical Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
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.’	X		

Technical Safety Requirement 02	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.	X		
Technical Safety Requirement 03	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.	X		
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensure	X		
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any memory problems			
Technical Safety Requirement 06	The Lane Departure Warning safety component shall ensure the frequency of the 'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Frequency.'	X		
Technical Safety Requirement 07	The Lane Keeping Assistance safety component shall ensure the duration of the lane keeping assistance torque is applied for less than Max_Duration.	X		
Technical Safety Requirement 08	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.	X		
Technical Safety Requirement 09	When a failure is detected, the Lane Keeping Assistance function shall deactivate and the 'LKA_Torque_Request' shall be zero.	X		
Technical Safety Requirement 10	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	X		

Technical Safety Requirement 11	Memory test shall be conducted at start up of the EPS ECU to check for any memory problems			

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off Lane Departure Warning functionality	Malfunction_01, Malfunction_02, Malfunction_04	yes	LDW malfunction warning on Car Display
WDC-02	Turn off Lane Keeping Assistance functionality	Malfunction_03, Malfunction_05	yes	LKA malfunction warning on Car Display