Technical Safety Concept
Lane Assistance

Document Version: 1.0

Submission Version 1.0, Released on 2018-01-29

Document history

Date	Version	Editor	Description
2018-01-28	1.0	Ioannis Tornazakis	First submission

Table of Contents

Purpose of the Technical Safety Concept

The purpose of this document to turn the functional safety requirements into technical safety requirements and to allocate the technical safety requirements into 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 keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50 msec	LDW vibration torque amplitude less than Max_Torque_Amplitude
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 msec	LDW vibration torque frequency less than 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 Max_Duration	B	500 msec	LKA torque equals zero

Refined System Architecture from Functional Safety Concept

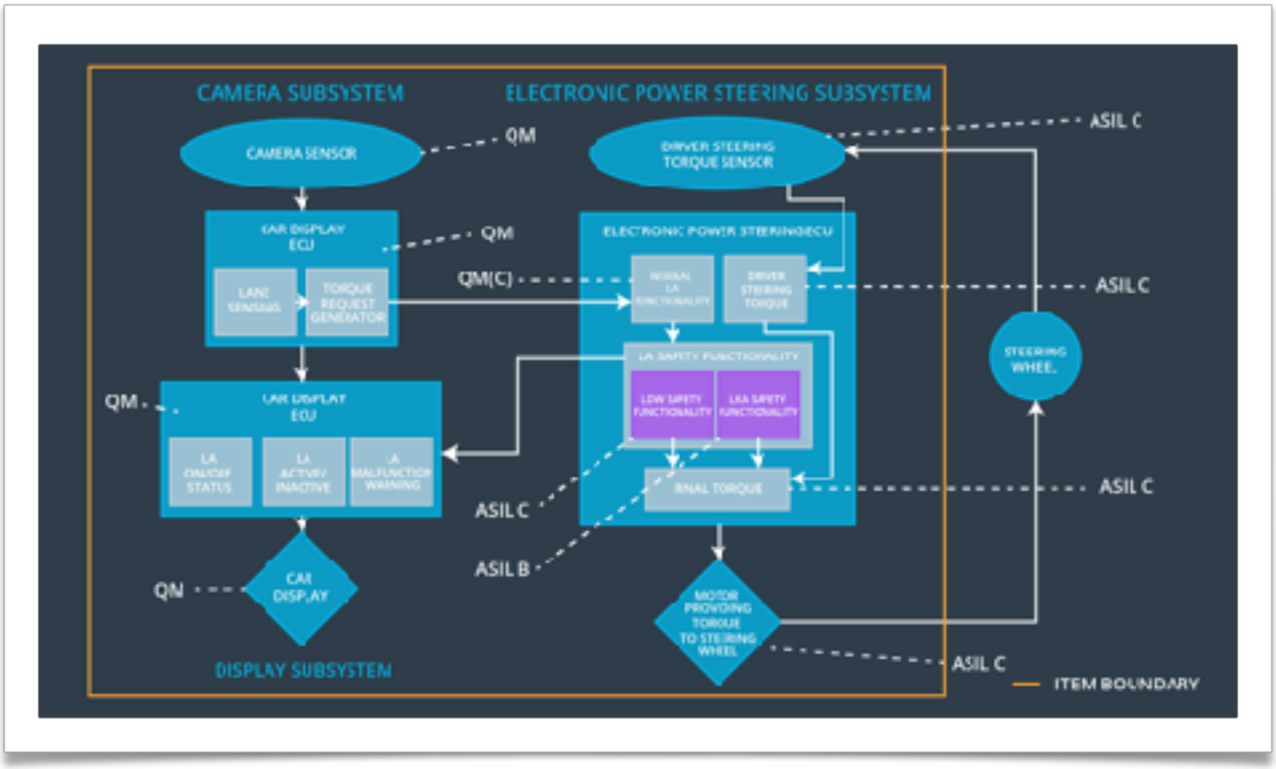

FIGURE 1. LANE ASSISTANCE SYSTEM REFINED ARCHITECTURE

Functional overview of architecture elements

Element	Description
Camera Sensor	The camera sensor captures images of the road in front of the vehicle and sends them to the Camera ECU
Camera Sensor ECU - Lane Sensing	Processes the images it receives from the Camera Sensor and applies computer vision techniques to extract the relative position of the vehicle within the lane
Camera Sensor ECU - Torque request generator	Receives a signal from the Lane Sensing unit when the car approaches the lane boundary, generates an appropriate torque request and sends it to the Electronic Power Steering ECU
Car Display	Informs the driver for the status of the Lane Assistance System
Car Display ECU - Lane Assistance On/Off Status	Informs the driver if the Lane Assistance is On or Off
Car Display ECU - Lane Assistant Active/Inactive	Informs the driver if the Lane Assistance is Active or Inactive

Car Display ECU - Lane Assistance malfunction warning	Receives status signals from the Electronic Power Steering ECU and issues warnings to the driver
Driver Steering Torque Sensor	Measures the torque that is applied to the steering wheel
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Receives the requested torque from the Driver Steering Torque Sensor, calculates the torque to be applied and forwards the signal to the Final Torque block
EPS ECU - Normal Lane Assistance Functionality	Receives a signal from the Camera Sensor ECU and issues a Primary_LDW_Torque_Request to the Lane Keeping Assistant Safety Functionality
EPS ECU - Lane Departure Warning Safety Functionality	Receives signals from the Normal Lane Assistance Functionality, Safety Startup and Data Transmission Integrity Check and checks whether a torque is safe to be issued. It sends the LDW_Torque_Request and LDW_Status_Signal signals to the Final Torque and the LDW_Error_Status to the Car Display ECU
EPS ECU - Lane Keeping Assistant Safety Functionality	Receives signals from the Normal Lane Assistance Functionality, Safety Startup and Data Transmission Integrity Check and checks whether a torque is safe to be issued. It sends the LKA_Torque_Request and LKA_Activation_Status signals to the Final Torque and the LKA_Error_Status to the Car Display ECU
EPS ECU - Final Torque	Receives signals from Driver Steering Torque, Data Transmission Integrity Check and Lane Departure Warning Safety Functionality and sends the torque that should be applied to the Motor
Motor	Provides the torque requested from the Electronic Steering ECU 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	A S IL	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 msec	LDW Safety Functionality	LDW torque output is set to zero
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 msec	LDW Safety Functionality	LDW torque output is 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 msec	LDW Safety Functionality	LDW torque output is 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 msec	Data Transmission Integrity Check	N/A
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 is 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 msec	LDW Safety Functionality	LDW torque output is set to zero
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 msec	LDW Safety Functionality	LDW torque output is 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 msec	LDW Safety Functionality	LDW torque output is 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 msec	Data Transmission Integrity Check	N/A

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 is 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 Functionality shall ensure that the LKA_Torque_Request is sent to the Final Torque for only Max_Duration	B	500 msec	LKA Safety Functionality	LKA_Torque_Request equals zero
Technical Safety Requirement 02	As soon as the LKA Safety Functionality 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 msec	LKA Safety Functionality	LKA_Torque_Request equals 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 msec	LKA Safety Functionality	LKA_Torque_Request equals zero
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured	B	500 msec	Data Transmission Integrity Check	N/A

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	LKA_Torque_Request equals zero

Refinement of the System Architecture

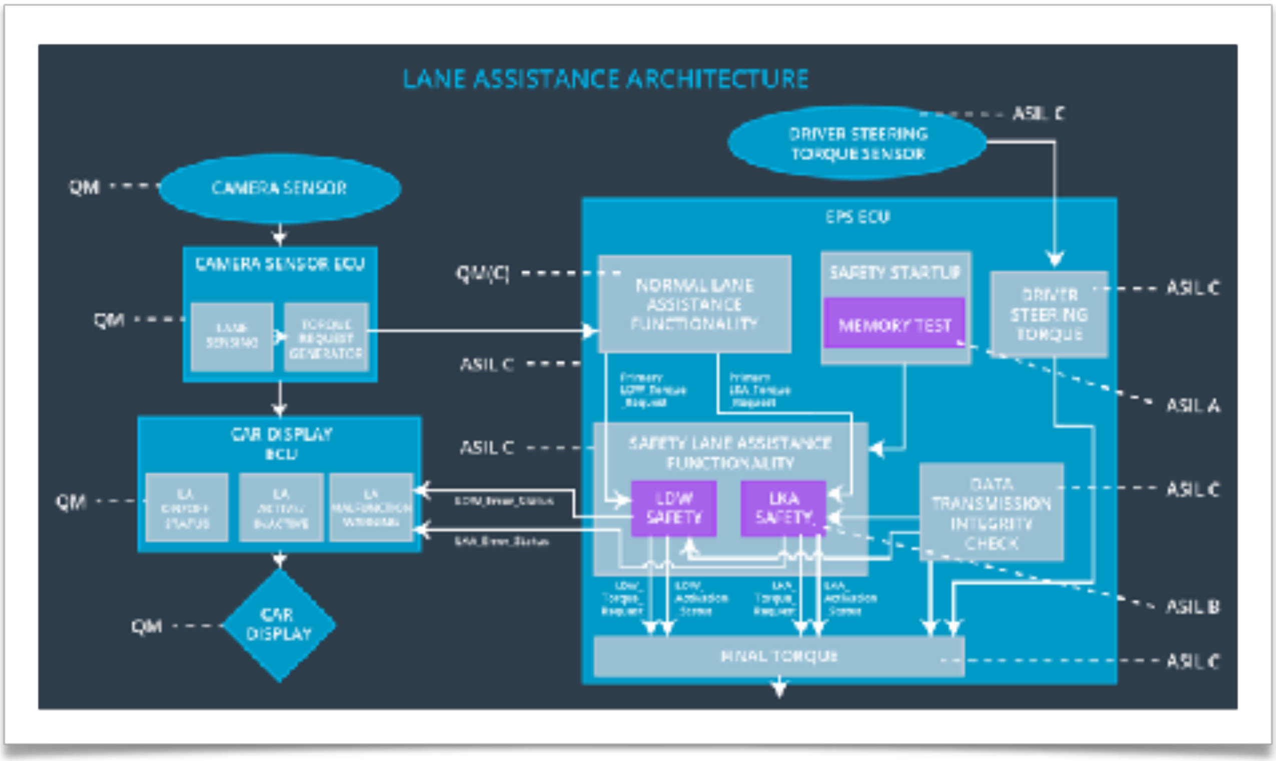

FIGURE 2. REFINED LANE ASSISTANCE SYSTEM REFINED ARCHITECTURE

Allocation of Technical Safety Requirements to Architecture Elements

All technical safety requirements are allocated to the Electronic Power Steering ECU. Please refer to the Technical Safety Requirements tables above for more details.

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off the Lane Departure Warning	Malfunction_01 Malfunction_02	Yes	Turn on Lane Assistant malfunction warning light
WDC-02	Turn off the Lane Keeping Assistant	Malfunction_03	Yes	Turn on Lane Assistant malfunction warning light