Technical Safety Concept Lane Assistance

Document Version: 1.0

Document history

Date	Version	Editor	Description
4-21-2018	1.0	Pablo	

Table of Contents

Purpose of the Technical Safety Concept

The purpose of the technical safety concept is to determine the safety requirements of each system that compose the lane keeping item. This involves determining the functional safety requirements of the lane keeping item.

The technical safety concept involves:

- Turning functional safety requirements into technical safety requirements
- Allocating 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 keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	Vibration torque is zero
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque is below Max_Torque_Frequency	C	50 ms	Vibration torque is zero
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	Lane Keeping Assistance torque is zero

Refined System Architecture from Functional Safety Concept

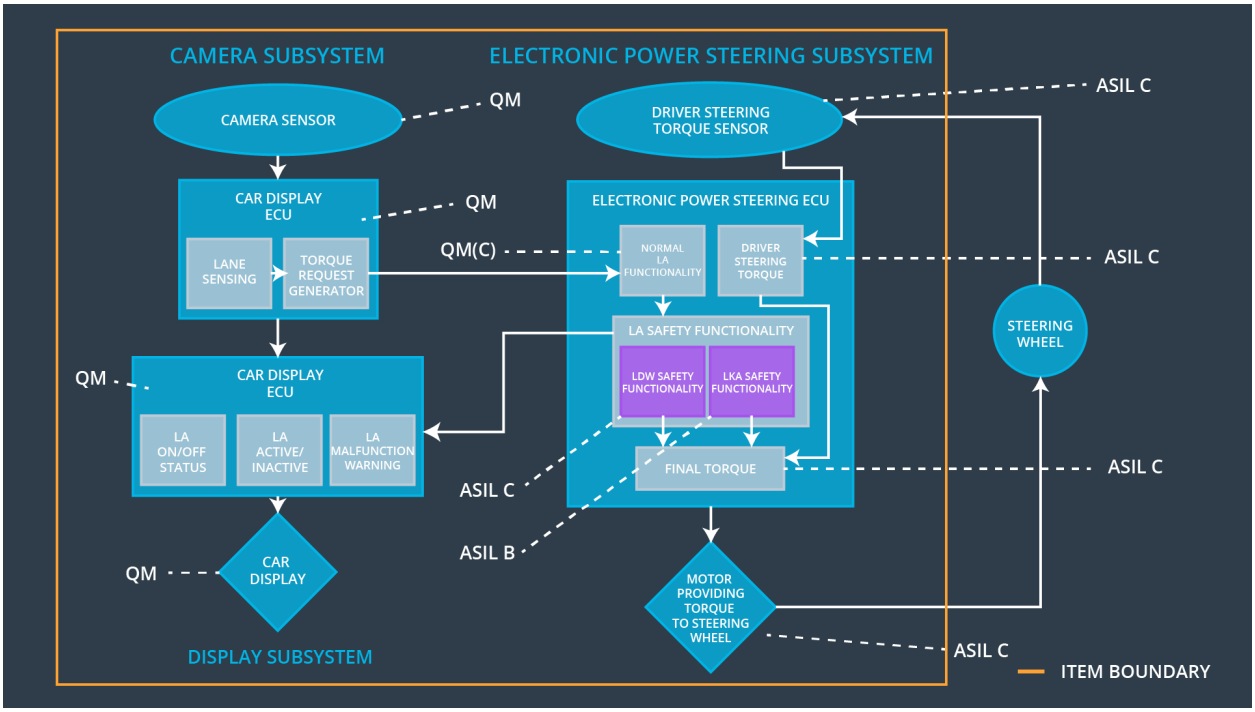

Figure 1: Refined system architecture

Functional overview of architecture elements

Element	Description
Camera Sensor	Captures road images and transmits them to the Camera Sensor ECU
Camera Sensor ECU - Lane Sensing	Based on the received images, detects lane lines and determines when the vehicle leaves the lane by mistake. Sends departure warning signal to the Car Display ECU.
Camera Sensor ECU - Torque request generator	Based on Lane Sensing result, sends estimated torque required to the Electronic Power Steering ECU.
Car Display	Displays warnings to the driver related to the Lane Keeping Assistance System.
Car Display ECU - Lane Assistance On/Off Status	Indicates warning related to the Lane Keeping Assistance System On/Off Status.
Car Display ECU - Lane Assistant Active/Inactive	Indicates warnings related to the Lane Keeping Assistance System Active/Inactive Status.

Car Display ECU - Lane Assistance malfunction warning	Indicates warnings related to the Lane Keeping Assistance System malfunction.
Driver Steering Torque Sensor	Measures the torque applied to the steering wheel. Sends torque signal to the Electronic Power Steering ECU.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Adjusts the torque required to correct the vehicle trajectory based on the driver steering torque sensor.
EPS ECU - Normal Lane Assistance Functionality	Adjusts the torque required to correct the vehicle trajectory based on the Torque Request Generator
EPS ECU - Lane Departure Warning Safety Functionality	Checks if output from Normal Lane Assistance Functionality is less than Max_Torque_Amplitude and Max_Torque_Frequency. If it is above them, sets torque to zero.
EPS ECU - Lane Keeping Assistant Safety Functionality	Checks if lane keeping assistance torque is applied for only Max_Duration. Of it is above it, sets torque to zero.
EPS ECU - Final Torque	Combines torques requested by LA Safety Functionality and Driver Steering Torque and sends it to the Motor.
Motor	Applies the torque required by the Electronic Power 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	The lane keeping item shall ensure that the lane departure	X		

Requirement 01-01	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_Request = 0
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	LDW_Torque_Request = 0
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 = 0
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	LDW_Torque_Request = 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_Request = 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 amplitude 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 = 0
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	LDW_Torque_Request = 0
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 = 0
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	LDW_Torque_Request = 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_Request = 0

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 duration of the 'LKA_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Duration'	B	500 ms	LKA Safety	LKA_Torque_Request = 0
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	LKA_Torque_Request = 0
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
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	LKA_Torque_Request = 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	LKA_Torque_Request = 0

Refinement of the System Architecture

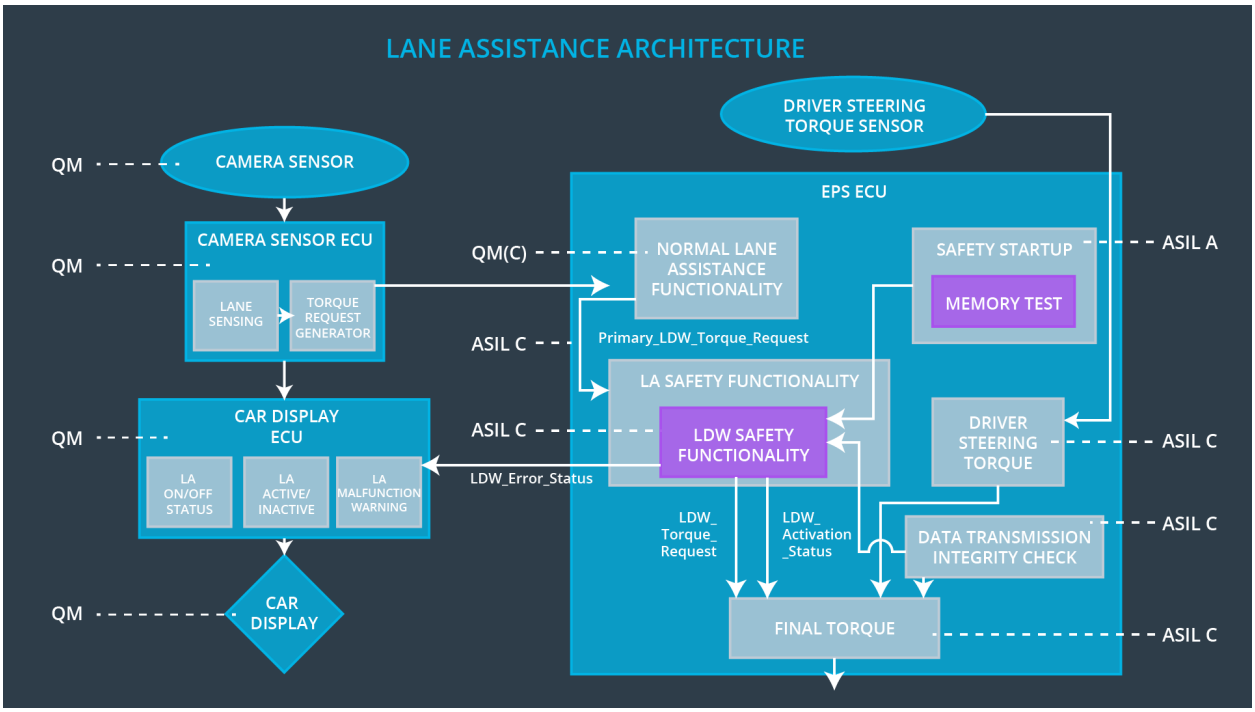

Figure 2: Refinement of the System Architecture

Allocation of Technical Safety Requirements to Architecture Elements

We already included the allocation as part of the technical requirement tables above. For this particular item, all technical safety requirements are allocated to the Electronic Power Steering ECU.

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	The torque request from the lane keeping assistance will be set to zero.	Malfunction_01, Malfunction_02	Yes	Warning light on the dashboard when the system malfunctions
WDC-02	The torque request from the lane keeping assistance will be set to zero.	Malfunction_03	Yes	Warning light on the dashboard when the system malfunctions