Technical Safety Concept Lane Assistance

Document Version: 1.0, Released on 2018-07-01

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
07/01/2018	1.0	Anand Mandapati	Initial Version

Table of Contents

Purpose of the Technical Safety Concept

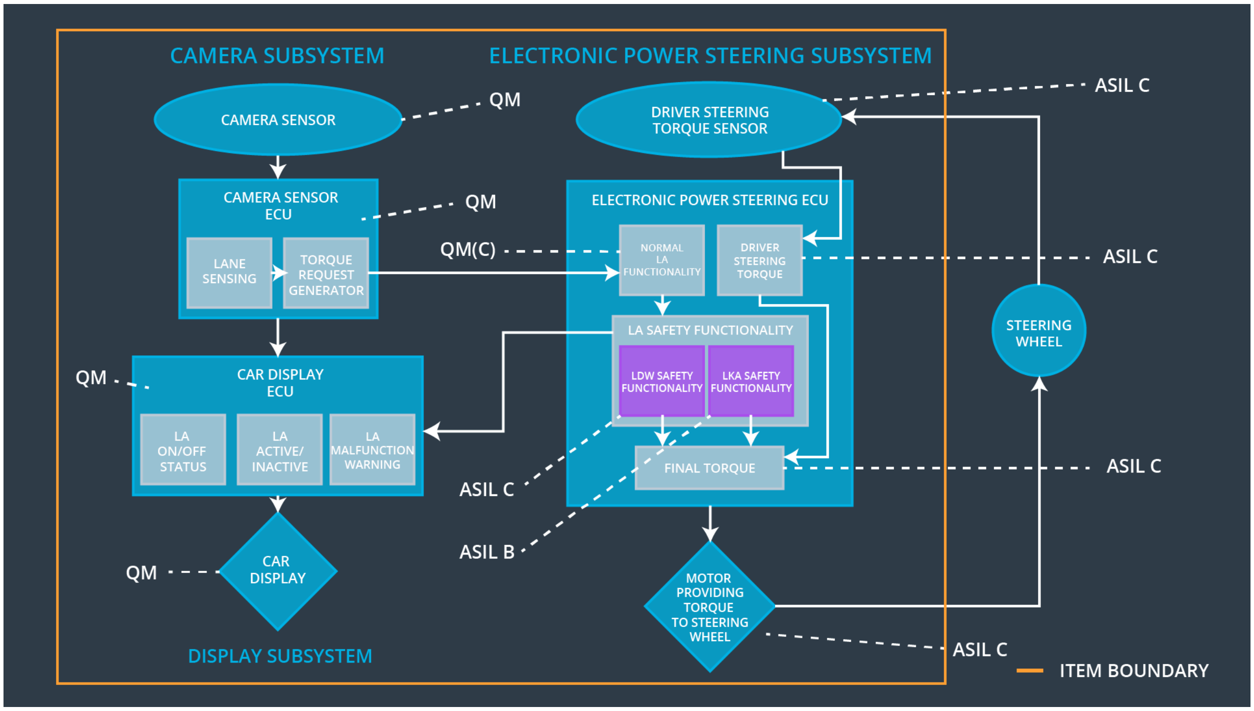
The purpose of the Technical Safety Concept portion of the Safety Plan is to derive more detailed technical hardware and software requirements from the functional safety requirements to mitigate the identified risks in the electrical and electronic components that constitute the Lane Assistance System. The requirements are then allocated to the appropriate location in 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 Electronic Power Steering ECU shall ensure that the lane departure oscillation torque amplitude is below Max_Torque_Amplitude.	C	50 ms	Reduce steering torque to zero
Functional Safety Requirement 01-02	The Electronic Power Steering ECU shall ensure that the lane departure oscillation torque frequency is below Max_Torque_Frequency.	C	50 ms	Reduce steering torque to 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	Reduce steering torque to zero

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Provides the Camera Display ECU with images of the roadway in front of the vehicle.
Camera Sensor ECU - Lane Sensing	Detects lane lines, the vehicle position with respect to the lanes, and whether the vehicle is outside the ego lane.
Camera Sensor ECU - Torque request generator	Provides a correction torque if the vehicle is departing the ego lane.
Car Display	Displays various information to the driver.
Car Display ECU - Lane Assistance On/ Off Status	Provides the Car Display with information of the On/Off state of the Lane Assistance System.
Car Display ECU - Lane Assistant Active/Inactive	Provides the Car Display with information of the Active/Inactive state of the Lane Assistance system.
Car Display ECU - Lane Assistance malfunction warning	Provides the Car Display with information of a possible malfunction of the Lane Assistance system.
Driver Steering Torque Sensor	Senses the steering torque provided by the driver.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Measure the steering torque sensed by the Driver Steering Torque Sensor.
EPS ECU - Normal Lane Assistance Functionality	Implements both Lane Assistance functions. Receives torque requests from Camera Sensor ECU and generates any augmented steering torque.
EPS ECU - Lane Departure Warning Safety Functionality	Ensures that torque amplitude and frequency are below Max_Torque_Amplitude and Max_Torque_Frequency.
EPS ECU - Lane Keeping Assistant Safety Functionality	Ensures that the LKA function is not activated for longer than Max_Duration time.
EPS ECU - Final Torque	Combines torque requests from LKA and LDW functions with the Driver Steering Torque to generate the final torque to be sent to the motor.
Motor	Applies the final torque to the steering wheel of the vehicle.

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	50ms	EPS ECU - LDW Safety Component	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	50ms	EPS ECU - LDW Safety Component	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	50ms	EPS ECU - LDW Safety Component	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	50ms	EPS ECU – Data Transmission Integrity Check	LDW torque output is set to zero.
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	Ignition cycle	EPS ECU – Safety Startup 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 amplitude of the 'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Frequency.	C	50 ms	EPS ECU - LDW Safety Component	Torque Freq. 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 ms	EPS ECU - LDW Safety Component	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	EPS LDW Safety Software Component	Torque 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 ms	EPS ECU - 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	Safety Startup	N/A

Lane Keeping Assistance (LKA) Requirements:

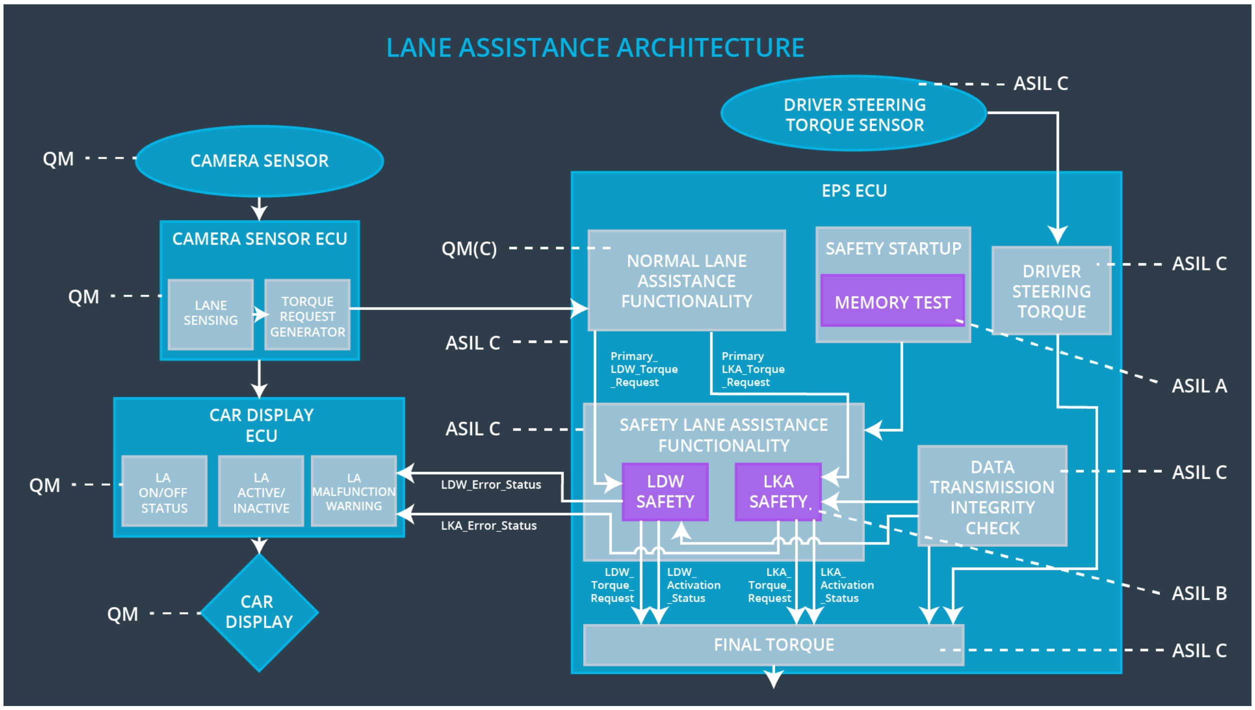
Functional Safety Requirement 02-1 with its associated system elements
(derived in the functional safety concept)

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 lane keeping assistance torque applied is less than Max_Duration.	B	500ms	EPS ECU - LKA Safety Component	Torque set to zero.
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	500ms	EPS ECU - LKA Safety Component	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	500ms	EPS ECU - LKA Safety Component	Torque set to zero.
Technical Safety Requirement 04	The validity and integrity of the data transmission for ‘LKA_Torque_Request’ signal shall be ensured.	B	500ms	EPS ECU – Data Transmission Integrity Check	N/A
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	Ignition cycle	EPS ECU – Safety Startup	N/A

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

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	Turn off LDW functionality	Vibration amplitude too high or frequency too high.	Yes, LDW oscillating torque shall be set to zero	Lane assistance functionality set inactive and malfunction warning to the driver via car display.
WDC-02	Turn off LKA functionality	Lane keeping assistance duration exceeds Max_Duration	Yes, LKA added extra torque shall be set to zero	Lane assistance functionality set inactive and malfunction warning to the driver via car display.