Technical Safety Concept Lane Assistance

Document history

Date	Version	Editor	Description
10 Feb 2018	1.0	Vilas Chitrakaran	Initial draft

Table of Contents

Purpose of the Technical Safety Concept

[Instructions: Answer what is the purpose of a technical safety concept?]

The Technical Safety Concept provides a technical description of signal flows and how components of the system shall behave in order to achieve the Functional Safety concept.

Inputs to the Technical Safety Concept

Functional Safety Requirements

[Instructions: Provide the functional safety requirements derived in the functional safety concept]

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	50ms	Function turned off
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50ms	Function turned off
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	500ms	Function turned off

Refined System Architecture from Functional Safety Concept

[Instructions: Provide the refined system architecture from the functional safety concept]
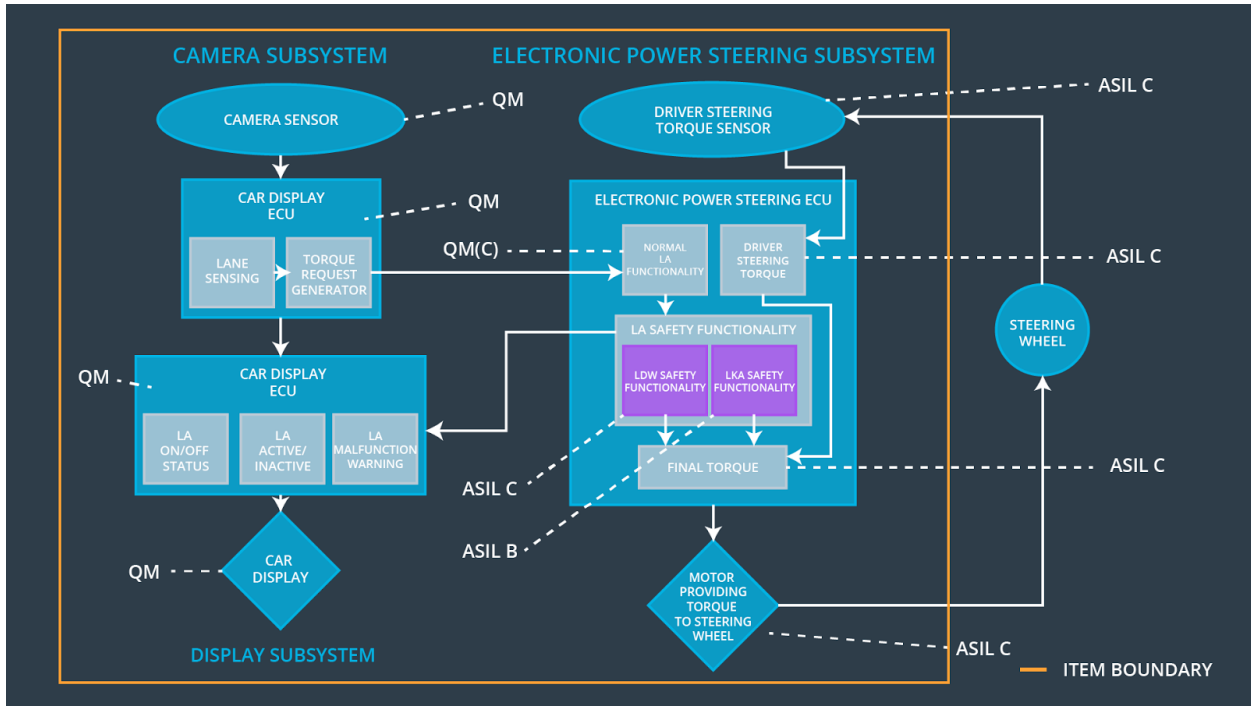
Functional overview of architecture elements

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

Element	Description
Camera Sensor	Captures video stream of the environment ahead of the vehicle.
Camera Sensor ECU - Lane Sensing	Applies computer vision algorithms to detect lane lines, computes ego-position of the vehicle relative to the lane lines, detects the event of the vehicle leaving the lane unintentionally
Camera Sensor ECU - Torque request generator	Generates corrective steering torque required to steer the vehicle back towards the center of the lane.
Car Display	Displays status information, warnings and faults to the driver, and is driven by the Car Display ECU
Car Display ECU - Lane Assistance	Receives on/of status from Camera Sensor ECU

On/Off Status	and and drives the associated display element
Car Display ECU - Lane Assistant Active/Inactive	Receives a signal from Camera Sensor ECU on whether the vision system has detected lane lines and is providing lane assistance function, and drives the associated indication on the display.
Car Display ECU - Lane Assistance malfunction warning	Receives malfunction messages from the Electronic Power Steering ECU and drives a warning light if there is a malfunction in the lane assistance system
Driver Steering Torque Sensor	Detects and measures steering torque applied by the driver.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Process the driver steering torque sensor to measure the driver applied counter torque on the steering wheel.
EPS ECU - Normal Lane Assistance Functionality	The non-safety relevant functionality of lane assistance system in the EPS ECU is implemented by this block
EPS ECU - Lane Departure Warning Safety Functionality	The safety relevant functionality of the lane departure warning function in the EPS ECU is implemented by this block
EPS ECU - Lane Keeping Assistant Safety Functionality	The safety relevant functionality of the lane keeping assistance function in the EPS ECU is implemented by this block.
EPS ECU - Final Torque	Computes the final torque request for the steering motor
Motor	Actuator that generates a steering torque to provide haptic feedback to the driver

Technical Safety Concept

Technical Safety Requirements

[Instructions: Fill in the technical safety requirements for the lane departure warning first functional safety requirement. We have provided the associated functional safety requirement in the first table below. Hint: The technical safety requirements were discussed in the lesson videos. The architecture allocation column should contain element names such as LDW Safety block, Data Transmission Integrity Check, etc.

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	LDW safety functionality block	Function turned off
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	LDW safety functionality block	Function turned off
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	LDW safety functionality block	Function turned off
Technical Safety Requirem	The validity and integrity of the data transmission for	C	50ms	Data transmission integrity block	Function turned off

ent 04	'LDW_Torque_Request' signal shall be 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 block	Function turned off

[Instructions: Fill in the technical safety requirements for the lane departure warning second functional safety requirement. We have provided the associated functional safety requirement in the table below. Hint:. Most of the technical safety requirements will be the same. At least one technical safety requirement will have to be slightly modified because we are talking about frequency instead of amplitude. These requirements were not given in the lessons]

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	50ms	LDW safety functionality block	Function turned off
Technical Safety Requirement	As soon as the LDW function deactivates the LDW feature, the 'LDW Safety' software block shall	C	50ms	LDW safety functionality block	Function turned off

02	send a signal to the car display ECU to turn on a warning light.				
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	LDW safety functionality block	Function turned off
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50ms	Data transmission integrity block	Function turned off
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 block	Function turned off

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

[OPTIONAL: For each technical safety requirement, identify both the verification and validation acceptance criteria. "Validation" asks whether or not you chose the appropriate parameters. "Verification" involves testing to make sure the vehicle behaves as expected when the parameter value is crossed. There is not necessarily one right answer. Look at your verification and validation acceptance criteria from the functional safety concept for inspiration.]

Lane Keeping Assistance (LKA) Requirements:

[Instructions: Fill in the technical safety requirements for the lane keeping assistance functional safety requirement 02-01. We have provided the associated functional safety requirement in the table below. Hint:. You can reuse the technical safety requirements from functional safety requirement 01-01. But you need to change the language because we are now looking at a different system. The ASIL and Fault Tolerant Time Interval are different as well.]

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	The lane keeping item shall ensure that the lane keeping	X		

| Requirement 02-01 | assistance torque is applied for only Max_Duration | | | |

Technical Safety Requirements related to Functional Safety Requirement 02-01 are:

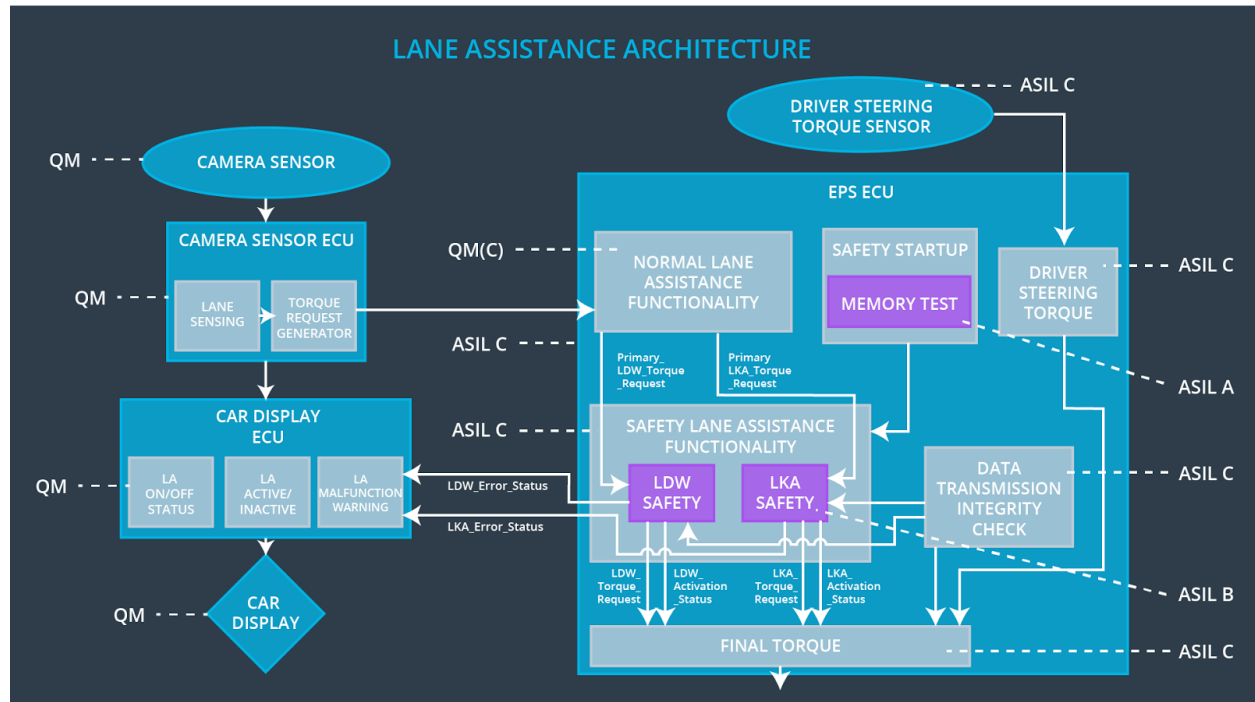| ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01	The LKA safety component shall ensure that the duration of the 'LKA_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Duration'	B	50ms	LKA Safety block	LKA function turned off
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	50ms	LKA Safety block	LKA function turned off
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	50ms	LKA Safety block	LKA function turned off
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	B	50ms	Data transmission integrity block	LKA function turned off
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 block	LKA function turned off

Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:
[OPTIONAL: For each technical safety requirement, identify both the verification and validation acceptance criteria. "Validation" asks whether or not you chose the appropriate parameters. "Verification" involves testing to make sure the vehicle behaves

Refinement of the System Architecture

Allocation of Technical Safety Requirements to Architecture Elements

All technical safety requirements are allocated to the EPS ECU.

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Function turned off.	On detection of malfunction causing steering torque amplitude or frequency to exceed limits	Yes	Warning light on dashboard to notify when disabled
WDC-02	Function turned off.	On detection of malfunction causing steering torque duration to exceed limit.	Yes	Warning note in the driver's manual to not use LKA function for autonomous driving