Technical Safety Concept Lane Assistance

Document history

[Instructions: Fill in the date, version and description fields. You can fill out the Editor field with your name if you want to do so. Keep track of your editing as if this were a real world project.

For example, if this were your first draft or first submission, you might say version 1.0. If this is a second submission attempt, then you'd add a second line with a new date and version 2.0]

Date	Version	Editor	Description
Mar. 30, 18	0.1	L. Chen	Initial version

Table of Contents

[Instructions: We have provided a table of contents. If the table of contents is not showing up correctly in your word processor of choice, please update it. The table of contents should show each section of the document and page numbers or links. Most word processors can do this for you. In Google Docs, you can use headings for each section and then go to Insert > Table of Contents. Microsoft Word has similar capabilities]

Purpose of the Technical Safety Concept

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

The purpose of a technical safety concept is
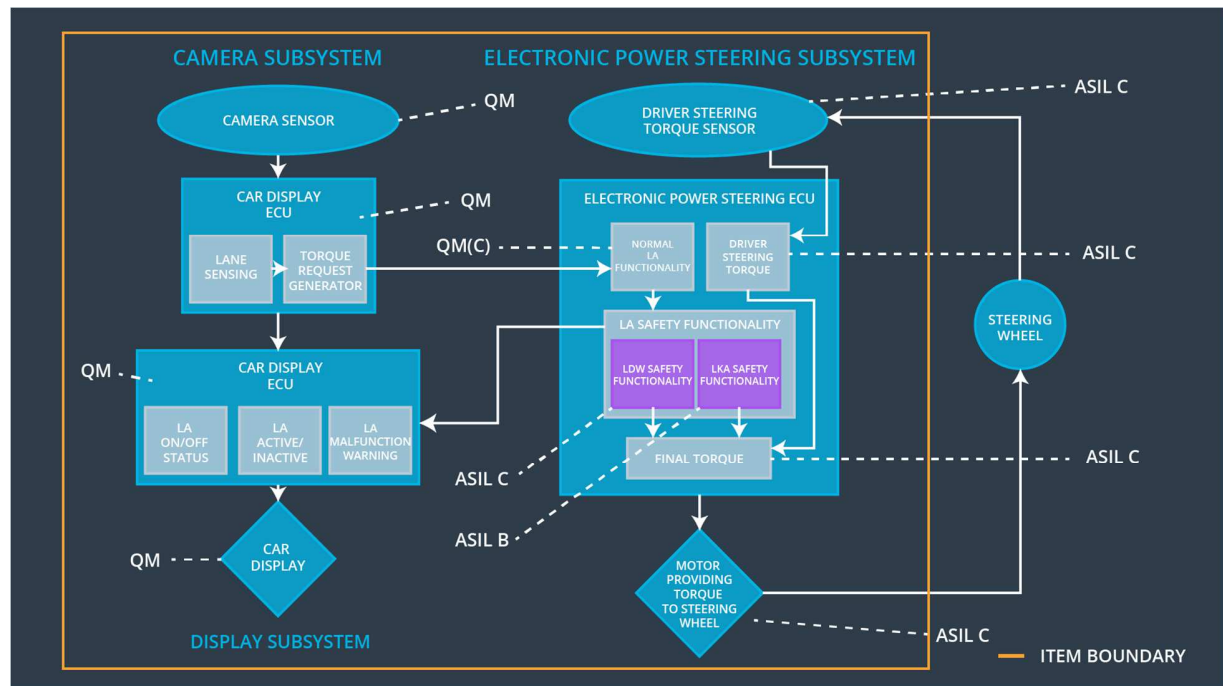
Inputs to the Technical Safety Concept

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	Electric Power Steering ECU shall ensure that the torque amplitude provided by LDW shall not exceed max_torque_amplitude	C	50ms	Off (set vibration torque to zero)
Functional Safety Requirement 01-02	Electric Power Steering ECU shall ensure that the torque frequency provided by LDW shall not exceed max_torque_frequency	C	50ms	Off (set vibration torque to zero)
Functional Safety Requirement 02-01	Electric Power Steering ECU shall ensure that the time of LKA torque application is limited to max_duration	B	500ms	Off (function turned off)

Refined System Architecture from Functional Safety Concept

Functional overview of architecture elements

Element	Description
Camera Sensor	Perception of current road environment
Camera Sensor ECU - Lane Sensing	Process image of camera sensor and calculate lane and ego vehicle's position and orientation within the lane
Camera Sensor ECU - Torque request generator	Calculate the torque needed to keep vehicle in the lane based on camera image
Car Display	Display information of lane assistance item
Car Display ECU - Lane Assistance On/Off Status	Display whether lane assistance function is on or off

Car Display ECU - Lane Assistant Active/Inactive	Display whether lane assistance function is active or inactive
Car Display ECU - Lane Assistance malfunction warning	Display warnings from lane assistance item
Driver Steering Torque Sensor	Measure steering torque of driver
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Process measurement of driver steering torque sensor data and add measurement to final torque calculation
EPS ECU - Normal Lane Assistance Functionality	Receive torque request generated by camera sensor ECU and forward this to calculate LDW and LKA torque
EPS ECU - Lane Departure Warning Safety Functionality	Receive torque request form normal lane assistance functionality and limit amplitude and frequency of this torque request
EPS ECU - Lane Keeping Assistant Safety Functionality	Receive torque request from normal lane assistance functionality and limit application time of this torque request
EPS ECU - Final Torque	Add driver steering torque and torque request of the lane assistance function and calculate output torque of the motor
Motor	apply torque calculated in EPS ECU – Final torque to steering wheel

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. Allocating the technical safety requirements to the "EPS ECU" does not provide enough detail for a technical safety concept.]

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	LDW Torque Request Amplitude shall be set to zero
lTechnical 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	LDW Torque Request Amplitude shall be 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	LDW safety	LDW Torque Request Amplitude shall be set to zero
Technical Safety Requirement	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50ms	Data transmission integrity check	LDW Torque Request Amplitude shall be set to

04					zero
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 Amplitude shall be 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	C	50ms	LDW safety	LDW Torque Request Frequency shall

	Torque' component is below 'Max_Torque_Frequency.				be 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	LDW safety	LDW Torque Request Frequency shall be 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	LDW safety	LDW Torque Request Frequency shall be 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		LDW Torque Request Frequency shall be set to zero
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		LDW Torque Request Frequency shall be set to zero

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 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 'LKA_Torque_Request' sent to the 'Final electronic power steering Torque' component is time limited to 'Max_Duration'	B	500ms	LKA safety	LKA Torque Request Amplitude shall be 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	LKA safety	LKA Torque Request Amplitude shall be set to zero
Technical Safety	As soon as a failure is detected	B	500ms	LKA safety	LKA Torque Request

|					Amplitude shall be set to zero
Requirement 03	by the LKA function, it shall deactivate the LKA feature and the 'LKA_Torque_Request' shall be set to zero.				Amplitude shall be 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		LKA Torque Request Amplitude shall be set to zero
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		LKA Torque Request Amplitude shall be set to zero

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 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.]

Refinement of the System Architecture

[Instructions: Include the refined system architecture. Hint: The refined system architecture should include the system architecture from the end of the technical safety lesson, including all of the ASIL labels.]
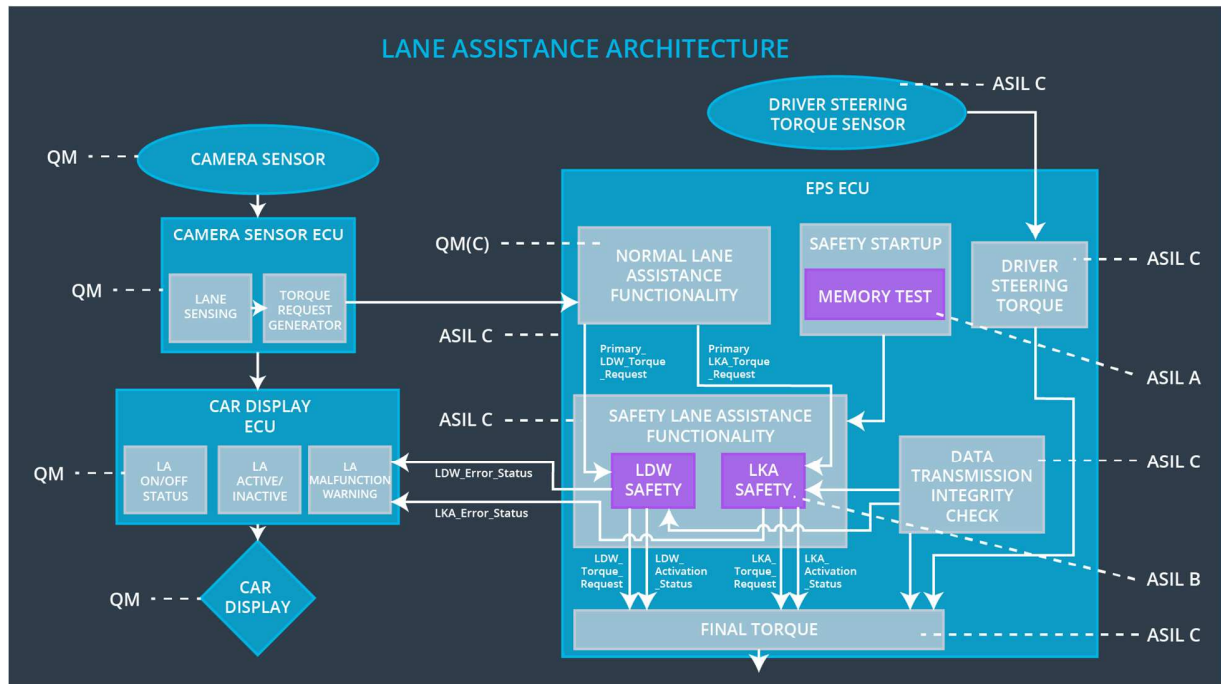
Allocation of Technical Safety Requirements to Architecture Elements

[Instructions: We already included the allocation as part of the technical requirement tables. Here you can state that for this particular item, all technical safety requirements are allocated to the Electronic Power Steering ECU]

For the lane assistance item, all technical safety requirements are allocated to LDW/LKA safety functionality, which is part of the Electronic Power Steering ECU

Warning and Degradation Concept

[Instructions: We've already identified that for any system malfunction, the lane assistance functions will be turned off and the driver will receive a warning light indication. The technical safety requirements have not changed how functionality will be degraded or what the warning will be.

So in this case, the warning and degradation concept is the same for the technical safety requirements as for the functional safety requirements. You can copy the functional safety warning and degradation concept here.

Oftentimes, a technical safety analysis will lead to a more detailed warning and degradation concept.]

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	LDW_Activation _Status = inactive LDW_Torque_R equest = 0	LDW_Torque_R equest amplitude > Max_Torque_A mplitude	Yes	Warning light on the car display
WDC-02	LDW_Activation _Status = inactive LDW_Torque_R equest = 0	LDW_Torque_R equest frequency > Max_Torque_Fr equency	Yes	Warning light on the car display
WDC-03	LKA_Activation_ status = inactive LKA_Torque_Re quest = 0	LKA_Activation_ Time > Max_Duration	Yes	Warning light on the car display