Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: [2.0]

Template Version 1.0, Released on 2017-06-21

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
08-06-2019	1.0	Vaidehi Venkatesan	Initial Draft
08-07-2019	2.0	Vaidehi Venkatesan	Proof-read + minor edits

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]

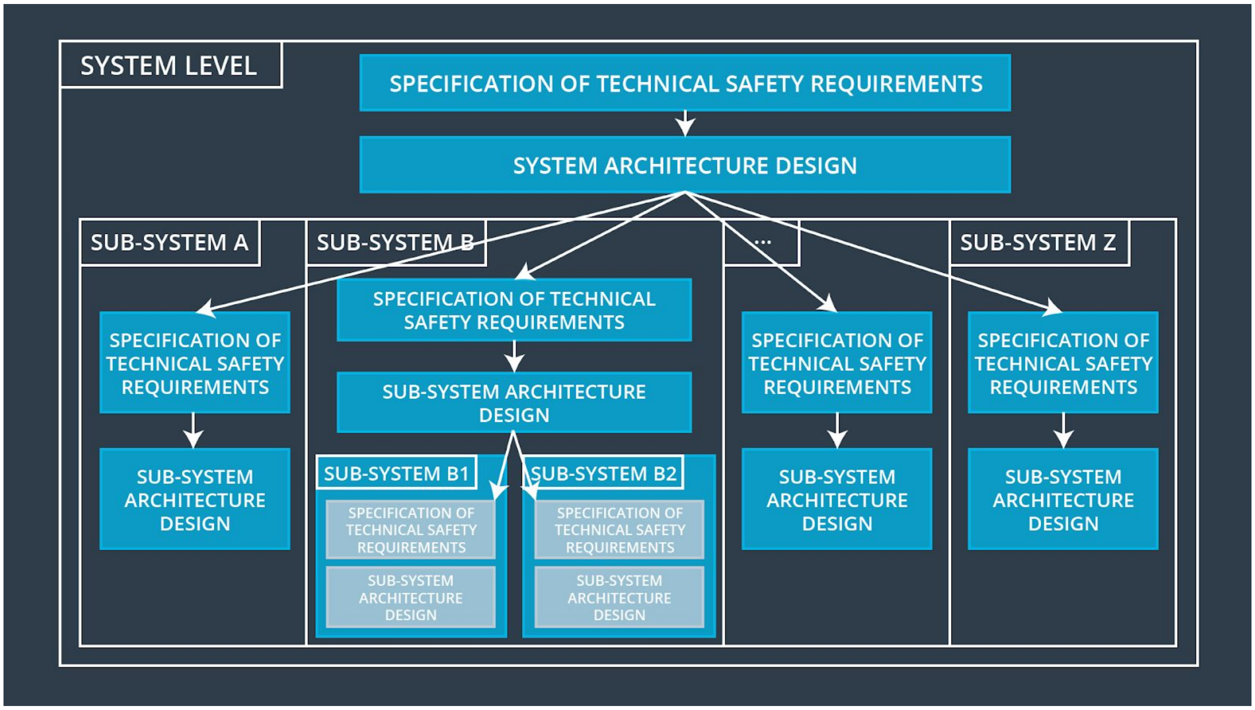
Purpose of the Technical Safety Concept

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

Technical safety concept is part of the product development phase of a Flattened V-Model. The purpose of Technical Safety Concept is to

1. detail the item’s technology
2. convert the item’s functional safety requirements into technical safety requirements
3. allocate the derived technical safety requirements to the system architecture and identify risk levels

Technical safety concepts can be documented at the System Level as well as at sub-system / component level. The system level document is responsible for detailing how the different subsystems will interact with each other. For each individual safety relevant subsystem, a detailed drill-down version of technical safety concept document will be available. The following figure showcases how technical safety concept is documented for a high level system vs. individual subsystems.


SYSTEM LEVEL
SPECIFICATION OF TECHNICAL SAFETY REQUIREMENTS
SYSTEM ARCHITECTURE DESIGN
SUB-SYSTEM A
SUB-SYSTEM B
...
SUB-SYSTEM Z
SPECIFICATION OF TECHNICAL SAFETY REQUIREMENTS
SUB-SYSTEM ARCHITECTURE DESIGN
SPECIFICATION OF TECHNICAL SAFETY REQUIREMENTS
SUB-SYSTEM ARCHITECTURE DESIGN
SUB-SYSTEM B1
SUB-SYSTEM B2
SPECIFICATION OF TECHNICAL SAFETY REQUIREMENTS
SUB-SYSTEM ARCHITECTURE DESIGN
SPECIFICATION OF TECHNICAL SAFETY REQUIREMENTS
SUB-SYSTEM ARCHITECTURE DESIGN
SPECIFICATION OF TECHNICAL SAFETY REQUIREMENTS
SUB-SYSTEM ARCHITECTURE DESIGN
SPECIFICATION OF TECHNICAL SAFETY REQUIREMENTS
SUB-SYSTEM ARCHITECTURE DESIGN

Inputs to the Technical Safety Concept

Functional Safety Requirements

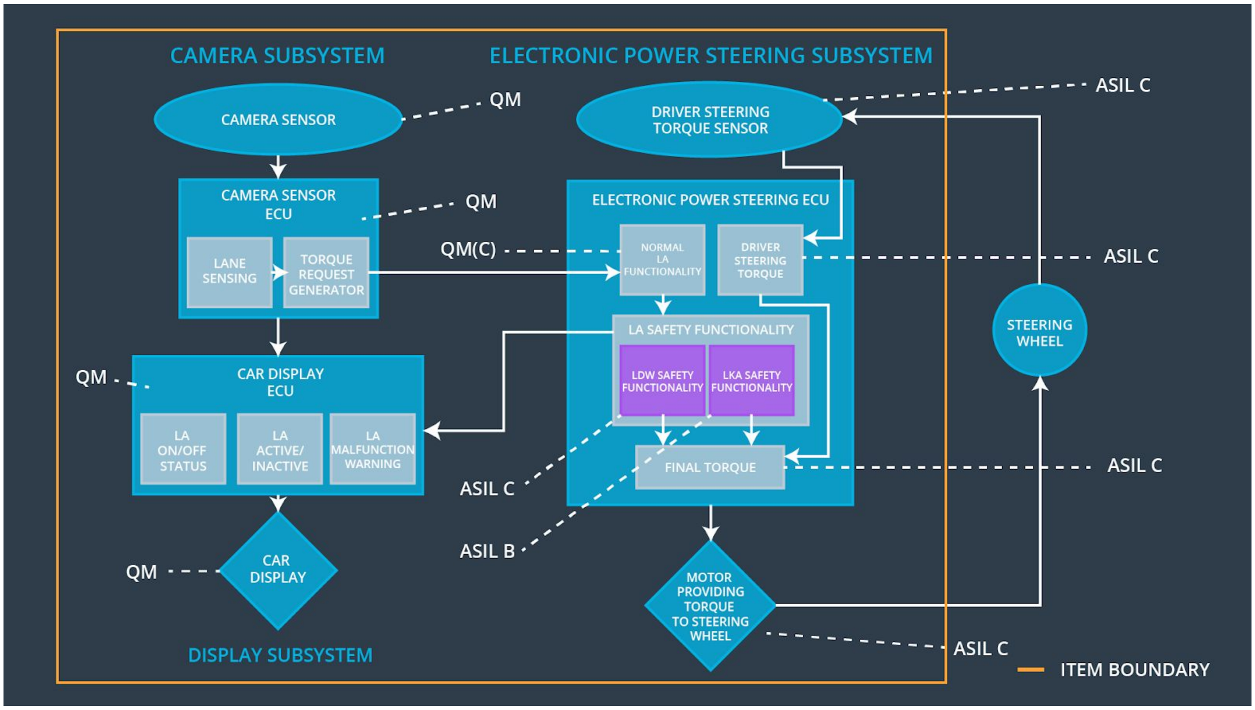
[Instructions: Provide the functional safety requirements derived in the functional safety concept]

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	The electronic power steering ECU shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50ms	The lane departure oscillating torque amplitude will be set to zero
Functional Safety	The electronic power steering ECU shall ensure that the lane departure	C	50ms	The lane departure oscillating

Requirement 01-02	oscillating torque frequency is below Max_Torque_Frequency			torque frequency will be set 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	500ms	The lane keeping assistance steering torque angle is set to zero and the lane keeping function is 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	Camera Sensor captures video feed of the lane lines on the road and passes the information to Camera Sensor ECU
Camera Sensor ECU - Lane Sensing	Camera Sensor ECU is responsible for detecting lane lines from the video feed and determine if vehicle is close to the center of ego lane. When the vehicle departs from the center, it sends a message to Torque Request Generator/
Camera Sensor ECU - Torque request generator	Torque request generator computes oscillating torque and steering torque required for notify the driver about the lane departure and keeping the vehicle within ego-lane. Once the oscillating torque and steering torque are computed, if the torque computed is non-zero, the car display ECU is notified
Car Display	Displays the different symbols and their current status in the car's dashboard
Car Display ECU - Lane Assistance On/Off Status	Responsible for showing the status of Lane Assistance functionality in the car – on / off. This status can be explicitly controlled by the user using a button in the car.
Car Display ECU - Lane Assistant Active/Inactive	Responsible for showing if status of Lane Assistance function is active / inactive. In the advent of user misusing the lane assistance functions as an autonomous driving capability beyond max_duration threshold, the lane assistance function turns inactive. This status

	is not controlled by the user.
Car Display ECU - Lane Assistance malfunction warning	If the lane departure function is throwing an oscillating torque with either amplitude or frequency greater than their respective thresholds, the malfunction warning sign will be turned on. The lane assistance status in such cases can be set to Off and Inactive. Similarly, if lane assistance function is kept on beyond a max_duration, the malfunction warning will be turned on.
Driver Steering Torque Sensor	Gets torque data from steering wheel and passes it on to EPS ECU.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Computes the oscillating and steering torque angle from the data input by the sensor
EPS ECU - Normal Lane Assistance Functionality	When notified by Camera ECU, Normal Lane assistance functionality is responsible for passing the torque request generator data to Safety Functionality
EPS ECU - Lane Departure Warning Safety Functionality	When torque request is received from Camera ECU, the requested torque is compared with amplitude and frequency thresholds and then additional torque to be added is determined and passed on to the Final Electronic Power Steering Torque Output
EPS ECU - Lane Keeping Assistant Safety Functionality	When torque request is received from Camera ECU, the requested steering torque is checked against the duration for which it has been requested. If the max_duration is not reached, the new steering torque is passed on to the Final Torque component
EPS ECU - Final Torque	Computes the final oscillating and steering torque required for the steering wheel taking into account, the torque request from LDW, LKA Safety Functionality and the current driver steering torque values. Sends the updated value to the motor.

Motor	Responsible for applying the oscillating torque and steering torque to the 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	EPS ECU - Safety Lane Assistance Functionality – LDW Safety Functionality	On detecting a faulty state, the LDW_Torque_Request amplitude 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 Functionality Car Display ECU - LA On, Active Warning	On detecting a faulty state, LA Malfunction warning state is turned on in Car Display
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 Functionality	On a faulty state, the safe state is to send LDW_Error_Status to the LA Malfunction Warning component
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50ms	EPS ECU	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	EPS ECU	On fault state, the LDW_Error_Status is sent to LA Malfunction

					Warning component

[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	The LDW safety component shall ensure that the frequency of the 'LDW_Torque_Request' sent to the 'Final electronic	C	50ms	EPS ECU - Safety Lane Assistance Functionality	On detecting a faulty

01	power steering Torque' component is below 'Max_Torque_Frequency.			– LDW Safety Functionality	state, the LDW_Torque_Request frequency 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 Functionality Car Display ECU - LA On, Active Warning	On detecting a faulty state, LA Malfunction warning state is turned on in Car Display
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 Functionality	On a faulty state, the safe state is to send LDW_Error_Status to the LA Malfunction Warning component

Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50ms	EPS ECU	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	EPS ECU	On faulty state, the LDW_Error_Status is sent to LA Malfunction Warning component

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

[OPTIONAL: For each technical safety requirements, 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.]

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Technical Safety Requirement 01-01-01	Amplitude of the 'LDW_Torque_Request' < 'Max_Torque_Amplitude is the validation criteria Method: The Max_Torque_Amplitude	Acceptance criteria: When LDW_Torque_Request < Max_Torque_Amplitude, the LDW safety component should set the LDW_Torque_Request to zero within the 50 ms FTTI.

	value is chosen after conducting experiments with different amplitudes and testing how drivers react	Method: Do a software test inserting a fault into the system and check if the system behaves within the acceptance criteria.
Technical Safety Requirement 01-01-02	Acceptance criteria: Car display to turn on LA warning when the LDW feature is turned off Method: Test with drivers if the “Expectation” of seeing a warning light on removing some automated driver assistance features is expected.	Acceptance criteria: The warning light should be turned on within 50 ms of FTTI once the LDW feature is turned off Method: Do a software test by inserting a LDW_feature off signal to Car Display ECU and check if the warning light turns on.
Technical Safety Requirement 01-01-03	Acceptance criteria: LDW oscillating torque request is set to zero on deactivating LDW feature. Method: Test with real world experiments in an controlled environment that when an excessive haptic feedback in the form of high amplitude torque is provided, the driver expectation is to turn off the feature and not reduce the torque gradually / or have a manual turn off.	Acceptance Criteria: The steering wheel should stop providing haptic feedback within 50 ms of FTTI once the LDW Feature is turned off. At a unit level, this can also be verified by measuring the output of LDW Safety component when LDW Feature is turned off. Method: Do a software test by inserting LDW_Feature off signal and check if the LDW Safety module resets the LDW_Torque_Request to zero.
Technical Safety Requirement 01-01-04	Acceptance criteria: Ensure the final torque request received by Final Torque component is indeed the same as the LDW Safety component output and does not have any quantization error. Method: Numerical value match before and after sending data. Validate that this module does not require to undergo any quantization errors or data corruption	Acceptance Criteria: Data sent out of LDW_Safety module is the same as the data fed into the Final Torque module in terms of bit stream and number of bits encoded Method: Do a software bit stream test to ensuring the same number of bits are encoded at the start of the transmission and received at the end of the transmission to Final Torque module and does not involve any corruption.

Technical Safety Requirement 01-01-05	Acceptance criteria: No memory faults found in ignition time Method: Ensure no other memory faults are possible other than ignition time	Acceptance Criteria: No memory faults at ignition time. Method: Do a software bit stream test to ensure no memory faults are found.
Technical Safety Requirement 01-02-01	Frequency of the 'LDW_Torque_Request' < 'Max_Torque_ Frequency is the validation criteria Method: The Max_Torque_Frequency value is chosen after conducting experiments with different Frequency and testing how drivers react	Acceptance criteria: When LDW_Torque_Request < Max_Torque_ Frequency, the LDW safety component should set the LDW_Torque_Request to zero within the 50 ms FTTI. Method: Do a software test inserting a fault into the system and check if the system behaves within the acceptance criteria.
Technical Safety Requirement 01-02-02	Acceptance criteria: Car display to turn on LA warning when the LDW feature is turned off Method: Test with drivers if the “Expectation” of seeing a warning light on removing some automated driver assistance features is expected.	Acceptance criteria: The warning light should be turned on within 50 ms of FTTI once the LDW feature is turned off Method: Do a software test by inserting a LDW_feature off signal to Car Display ECU and check if the warning light turns on.
Technical Safety Requirement 01-02-03	Acceptance criteria: LDW oscillating torque request is set to zero on deactivating LDW feature. Method: Test with real world experiments in an controlled environment that when an excessive haptic feedback in the form of high frequency torque is provided, the driver expectation is to turn off the feature and not reduce the torque gradually / or have a manual turn off.	Acceptance Criteria: The steering wheel should stop providing haptic feedback within 50 ms of FTTI once the LDW Feature is turned off. At a unit level, this can also be verified by measuring the output of LDW Safety component when LDW Feature is turned off. Method: Do a software test by inserting LDW_Feature off signal and check if the LDW Safety module resets the LDW_Torque_Request to zero.
Technical Safety	Acceptance criteria: Ensure the final torque request received by Final Torque	Acceptance Criteria: Data sent out of LDW_Safety module is the same as

Requirement 01-02-04	component is indeed the same as the LDW Safety component output and does not have any quantization error. Method: Numerical value match before and after sending data. Validate that this module does not require to undergo any quantization errors or data corruption	the data fed into the Final Torque module in terms of bit stream and number of bits encoded Method: Do a software bit stream test to ensuring the same number of bits are encoded at the start of the transmission and received at the end of the transmission to Final Torque module and does not involve any corruption.
Technical Safety Requirement 01-02-05	Acceptance criteria: No memory faults found in ignition time Method: Ensure no other memory faults are possible other than ignition time	Acceptance Criteria: No memory faults at ignition time. Method: Do a software bit stream test to ensure no memory faults are found.

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 Requiremen	The lane keeping item shall ensure that the lane keeping assistance torque is applied	X		

t 02-01	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 sending 'LKA_Torque_Request' to the 'Final electronic power steering Torque' component is below 'Max_Duration'.	B	500ms	EPS ECU - Safety Lane Assistance Functionality – LKA Safety Functionality	On detecting a faulty state, the LKA_Torque_Request frequency is 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 Functionality Car Display ECU - LA On, Active Warning	On detecting a faulty state, LA Malfunction warning state is turned on in Car Display
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 Functionality	On a faulty state, the safe state is to send LKA_Error_Status to the LA Malfunction Warning component

Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	B	500ms	EPS ECU	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	EPS ECU	On faulty state, the LKA_Error_Status is sent to LA Malfunction Warning component

Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:

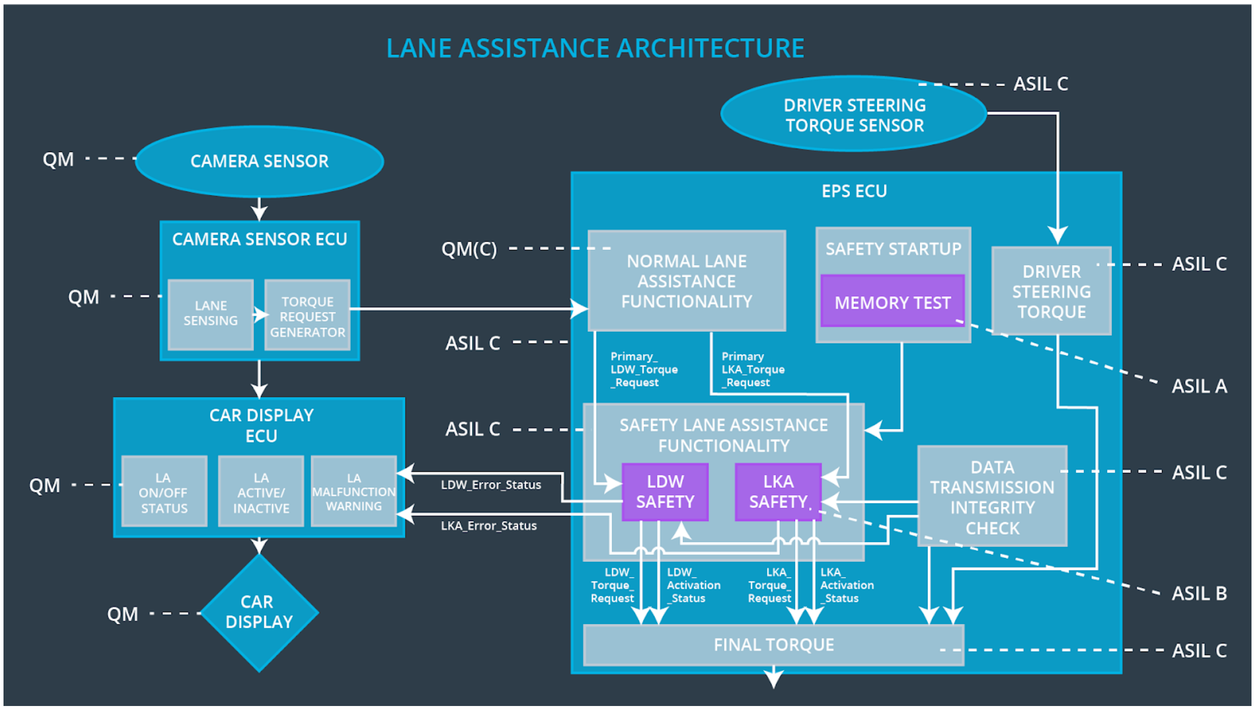
[OPTIONAL: For each technical safety requirement, identify both the verification and validation acceptance criteria. “Validation” asks whether or not you chose the appropriate parameters. “Verification” involves testing to make sure the vehicle behaves as expected when the parameter value is crossed.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

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Technical Safety Requirement 02-01-01	Acceptance Criteria: Duration of LKA_Torque_Request from LKA safety component < Max_Duration. Method: Conduct experiments with drivers to ensure the max_duration	Acceptance Criteria: LKA function should set the LKA_Torque_Request to zero when duration exceeds max_duration within 500ms of FTTI. Method: Do a software test to check if the system behaves within the acceptance criteria within 500ms of FTTI.
Technical Safety Requirement 02-01-02	Acceptance criteria: Car display to turn on LA warning when the LKA feature is turned off Method: Test with drivers if the “Expectation” of seeing a warning light	Acceptance criteria: The warning light should be turned on within 500 ms of FTTI once the LKA feature is turned off Method: Do a software test by

	on removing some automated driver assistance features is expected.	inserting a LKA_feature off signal to Car Display ECU and check if the warning light turns on.
Technical Safety Requirement 02-01-03	Acceptance criteria: LKA steering torque request is set to zero on deactivating LKA feature. Method: Test with real world experiments for the duration when lane keeping assistance functionality can be kept on to ensure the drivers hands are always one the steering wheel.	Acceptance Criteria: The steering wheel should stop auto-steering and keeping in the lane within 500 ms of FTTI once the LKA Feature is turned off. At a unit level, this can also be verified by measuring the output of LKA Safety component when LKA Feature is turned off. Method: Do a software test by inserting LKA_Feature off signal and check if the LKA Safety module resets the LKA_Torque_Request to zero.
Technical Safety Requirement 02-01-04	Acceptance criteria: Ensure the final torque request received by Final Torque component is indeed the same as the LKA Safety component output and does not have any quantization error. Method: Numerical value match before and after sending data. Validate that this module does not require to undergo any quantization errors or data corruption	Acceptance Criteria: Data sent out of LKA_Safety module is the same as the data fed into the Final Torque module in terms of bit stream and number of bits encoded Method: Do a software bit stream test to ensuring the same number of bits are encoded at the start of the transmission and received at the end of the transmission to Final Torque module and does not involve any corruption.
Technical Safety Requirement 02-01-05	Acceptance criteria: No memory faults found in ignition time Method: Ensure no other memory faults are possible other than ignition time	Acceptance Criteria: No memory faults at ignition time. Method: Do a software bit stream test to ensure no memory faults are found.

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]

All newly added architectural modules are added to Electronic Power Steering ECU. Newly added modules are

1. Safety Startup
2. Data transmission integrity Check

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	Turn off the functionality	Malfunction in Technical Safety Requirements 01-01-01 through 01-01-05 and 01-02-01 through 01-02-05	Yes	The haptic feedback given to the user stops.
WDC-02	Turn off the functionality	Malfunction in Functional Safety Requirement 02-01-01 through 02-01-05	Yes	The driver will see a warning light on the dashboard when the system malfunctions.