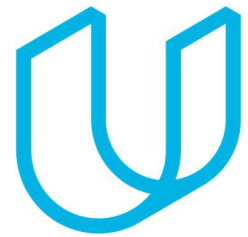




Elektrobit



UDACITY

# Technical Safety Concept Lane Assistance

Document Version: [Version]

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 |
|-------------|---------|-----------|-------------|
| 04 Apr 2019 | 1.0     | Soumen De | First Draft |
|             |         |           |             |
|             |         |           |             |
|             |         |           |             |
|             |         |           |             |

# 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]

[Document history](#)

[Table of Contents](#)

[Purpose of the Technical Safety Concept](#)

[Inputs to the Technical Safety Concept](#)

[Functional Safety Requirements](#)

[Refined System Architecture from Functional Safety Concept](#)

[Functional overview of architecture elements](#)

[Technical Safety Concept](#)

[Technical Safety Requirements](#)

[Refinement of the System Architecture](#)

[Allocation of Technical Safety Requirements to Architecture Elements](#)

[Warning and Degradation Concept](#)

## Purpose of the Technical Safety Concept

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

In this document, new requirements are defined and assigned to the system architecture. These new requirements are more concrete and gets into details of the item's technology as specified by ISO 26262.

## Inputs to the Technical Safety Concept

### Functional Safety Requirements

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

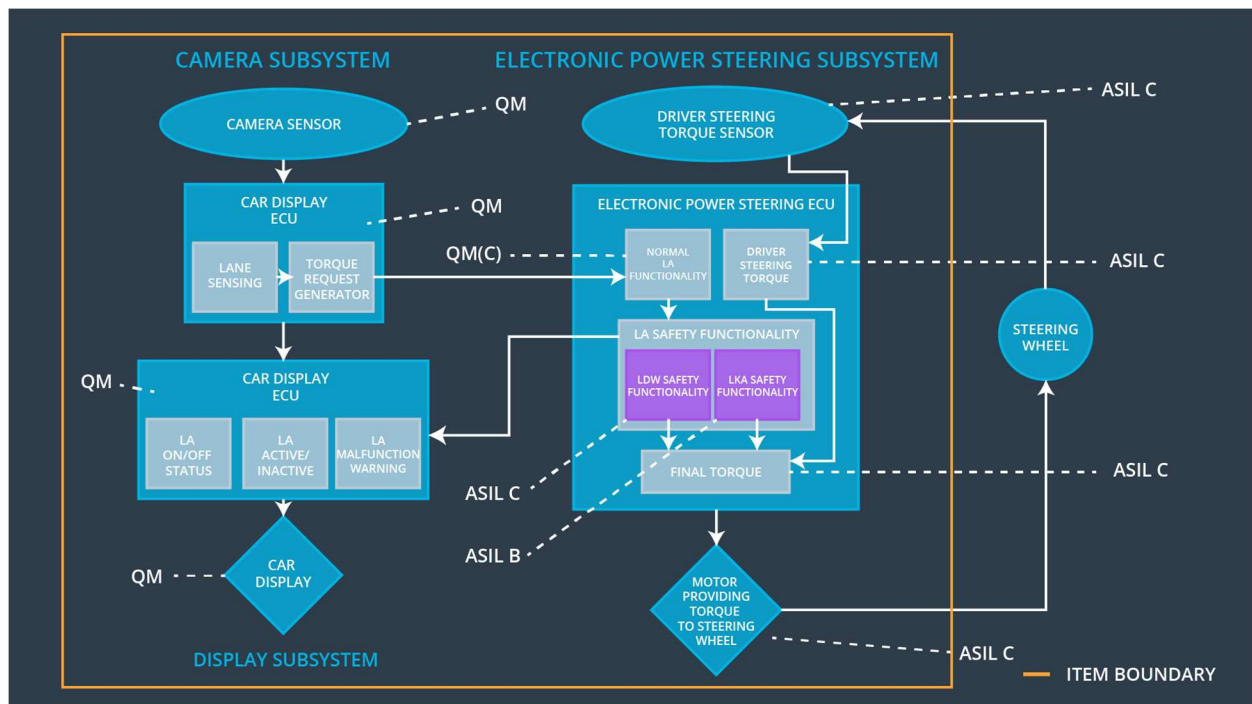
### Refined System Architecture from Functional Safety Concept

[Instructions: Provide the refined system architecture from the functional safety concept]

| ID   | Functional Safety Requirement  | A<br>S<br>I<br>L | Fault<br>Tolerant<br>Time<br>Interval | Safe State   |
|--|--|------------------|---------------------------------------|--|
| Functional<br>Safety<br>Requirement<br>01-01 | The Lane Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude. | C                | 50 ms                                 | Vibration torque amplitude below Max_Torque_Amplitude. |
| Functional<br>Safety<br>Requirement<br>01-02 | The Lane Departure Warning item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency. | C                | 50 ms                                 | Vibration frequency is below Max_Torque_Frequency.     |

|                                     |  |   |        |   |
|-------------------------------------|--|---|--------|---|
| Functional Safety Requirement 02-01 | The electronic power steering ECU shall ensure that the Lane Keeping Assistance torque is applied only for Max_Duration. | B | 500 ms | Lane Keeping Assistance torque is zero. |
|-------------------------------------|--|---|--------|---|

## Refined System Architecture from Functional Safety Concept



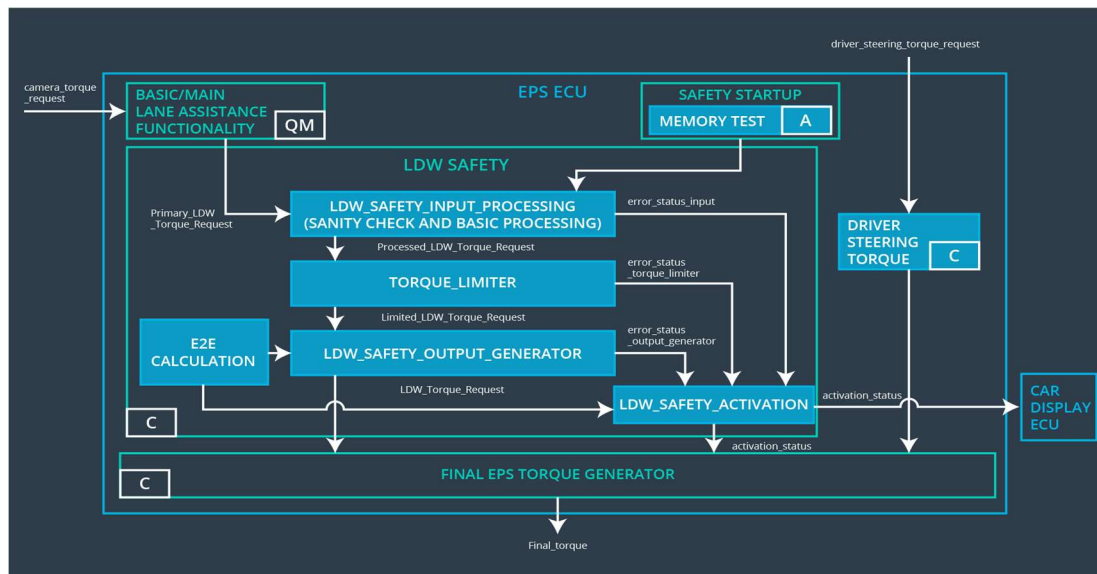
## Functional overview of architecture elements

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

| Element  | Description   |
|--|---|
| Camera Sensor  | Capture road images and provide them to the Camera Sensor ECU.  |
| Camera Sensor ECU - Lane Sensing                             | Software module detecting the lane line positions from the Camera Sensor images.  |
| Camera Sensor ECU - Torque request generator                 | Software module calculating the necessary torque to be requested to the Electronic Power Steering ECU.                          |
| Car Display  | Display warning for the driver.   |
| Car Display ECU - Lane Assistance On/Off Status              | Indicate the status of the Lane Assistance functionality (On/Off.)  |
| Car Display ECU - Lane Assistant Active/Inactive             | Indicate if the Lane Assistance functionality is properly functioning (Active/Inactive.)  |
| Car Display ECU - Lane Assistance malfunction warning        | Indicate a malfunction on the Lane Assistance functionality.  |
| Driver Steering Torque Sensor                                | Measure the torque applied to the steering wheel by the driver.   |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | Software module receiving the driver's torque request from the steering wheel.  |
| EPS ECU - Normal Lane Assistance Functionality               | Software module receiving the Camera Sensor ECU torque request.   |
| EPS ECU - Lane Departure Warning Safety Functionality        | Software module ensuring the torque amplitude is below Max_Torque_Amplitude and torque frequency is below Max_Torque_Frequency. |
| EPS ECU - Lane Keeping Assistant Safety Functionality        | Software module ensuring the Lane Keeping Assistance functionality application is not activate more than Max_duration time.     |

|                        |  |
|------------------------|--|
| EPS ECU - Final Torque | Combine the torque request from the Lane Keeping and Lane Departure Warning functionalities and sends them to the Motor. |
| Motor                  | Applies the required torque to the steering wheels.  |

## 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.]

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  | A<br>S<br>I<br>L | Fault Tolerant Time Interval | Architecture Allocation           | Safe State                             |
|---------------------------------------|---|------------------|------------------------------|-----------------------------------|--|
| Technical Safety Requirement 01-01-01 | The Lane Departure Warning 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                        | Lane Departure Warning torque to zero. |
| Technical Safety Requirement 01-01-02 | When the Lane Departure Warning is deactivated, the 'LDW Safety' software module shall send a signal to the Car Display ECU to turn on a warning signal.  | C                | 50 ms                        | LDW Safety                        | Lane Departure Warning torque to zero. |
| Technical Safety Requirement 01-01-03 | When a failure is detected by the Lane Departure Warning functionality, it shall deactivate the Lane Departure Warning feature and set 'LDW_Torque_Request' to zero.                                    | C                | 50 ms                        | LDW Safety                        | Lane Departure Warning torque to zero. |
| Technical Safety Requirement 01-01-04 | The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.   | C                | 50 ms                        | LDW Safety                        | Lane Departure Warning torque to zero. |
| Technical Safety Requirement 01-01-05 | Memory test shall be conducted at start up of the EPS ECU to check for any memory problems  | A                | Ignition cycle               | Data Transmission Integrity Check | Lane Departure Warning torque 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 01-02-01 | The Lane Departure Warning safety component shall ensure the frequency of the 'LDW_Torque_Reques' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Frequency.' | C    | 50 ms                        | LDW Safety              | Lane Departure Warning torque to zero. |



### 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:

[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]

| ID                                    | Technical Safety Requirement  | ASIL | Fault Tolerant Time Interval | Architecture Allocation | Safe State                             |
|---------------------------------------|---|------|------------------------------|-------------------------|--|
| Technical Safety Requirement 01-01-01 | The Lane Departure Warning 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              | Lane Departure Warning torque to zero. |
| Technical                             | When the Lane Departure   | C    | 50 ms                        | LDW Safety              | Lane                                   |

|                                       |  |   |                |                                   |  |
|---------------------------------------|--|---|----------------|-----------------------------------|--|
| Safety Requirement 01-01-02           | Warning is deactivated, the 'LDW Safety' software module shall send a signal to the Car Display ECU to turn on a warning signal.                                     |   |                |                                   | Departure Warning torque to zero.      |
| Technical Safety Requirement 01-01-03 | When a failure is detected by the Lane Departure Warning functionality, it shall deactivate the Lane Departure Warning feature and set 'LDW_Torque_Request' to zero. | C | 50 ms          | LDW Safety                        | Lane Departure Warning torque to zero. |
| Technical Safety Requirement 01-01-04 | The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.  | C | 50 ms          | LDW Safety                        | Lane Departure Warning torque to zero. |
| Technical Safety Requirement 01-01-05 | Memory test shall be conducted at start up of the EPS ECU to check for any memory problems   | A | Ignition cycle | Data Transmission Integrity Check | Lane Departure Warning torque 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 | A | Fault | Architecture | Safe |
|----|------------------------------|---|-------|--------------|------|
|----|------------------------------|---|-------|--------------|------|

|                                       |  | S<br>I<br>L | Tolerant<br>Time<br>Interval | Allocation | State                                  |
|---------------------------------------|--|-------------|------------------------------|------------|--|
| Technical Safety Requirement 01-02-01 | The Lane Departure Warning safety component shall ensure the frequency of the 'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Frequency.' | C           | 50 ms                        | LDW Safety | Lane Departure Warning torque 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.]

| ID                                    | Validation Acceptance Criteria and Method   | Verification Acceptance Criteria and Method  |
|---------------------------------------|---|--|
| Technical Safety Requirement 01-01-01 | Validate the Max_Torque_Amplitude is the chosen from the Lane Departure Warning Validation  | Verify the Lane Departure Warning functionality is turned off.                             |
| Technical Safety Requirement 01-01-02 | Validate the 'TORQUE_LIMITER' sends the error_status_torque_limiter signal to the LDW_SAFETY_ACTIVATION.  | Verify the Car Display ECU displays the Lane Departure Warning malfunction warning signal. |
| Technical Safety Requirement 01-01-03 | Validate the 'TORQUE_LIMITER' sends 'LDW_Torque_Request' with zero.   | Verify the Final EPS Torque generator receives a LDW_Torque_Request of zero.               |
| Technical Safety Requirement 01-01-04 | Validate the 'TORQUE_LIMITER' calculate and sends the correct cyclic redundancy check (CRC) and Alive counter for data transmission validity and integrity. | Verify the functionality is turn off if there is a CRC or Alive counter discrepancy.       |
| Technical                             | Validate the Safety Startup Memory  | Verify the Lane Departure Warning is   |

|  |  |  |
|--|--|--|
| Safety Requirement<br>01-01-05           | test to check memory faults catch memory faults.   | turned off when the Safety Startup Memory fails.   |
| Technical Safety Requirement<br>01-02-01 | Validate the Max_Torque_Frequency set is the chosen from the Lane Departure Warning Acceptance Criteria. | Verify the functionality is turned off if the 'LDW_Torque_Request' frequency exceeds Max_Torque_Request. |

### 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<br>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 02-01-01 | The Lane Keeping Assistance safety component shall ensure the duration of the lane keeping assistance torque is applied for less than Max_Duration | C | 500 ms         | LKA Safety                        | Lane Keeping Assistance torque to zero. |
| Technical Safety Requirement 02-01-02 | When the Lane Keeping Assistance function deactivates, the 'LKA Safety' shall send a signal to the Car Display ECU to turn on a warning light.     | C | 500 ms         | LKA Safety                        | Lane Keeping Assistance torque to zero. |
| Technical Safety Requirement 02-01-03 | When a failure is detected, the Lane Keeping Assistance function shall deactivate and the 'LKA_Torque_Request' shall be zero.                      | C | 500 ms         | LKA Safety                        | Lane Keeping Assistance torque to zero. |
| Technical Safety Requirement 02-01-04 | The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.  | C | 500 ms         | LKA Safety                        | Lane Keeping Assistance torque to zero. |
| Technical Safety Requirement 02-01-05 | Memory test shall be conducted at startup of the EPS ECU to check for any memory problems  | A | Ignition cycle | Data Transmission Integrity Check | Lane Departure Warning torque to zero.  |

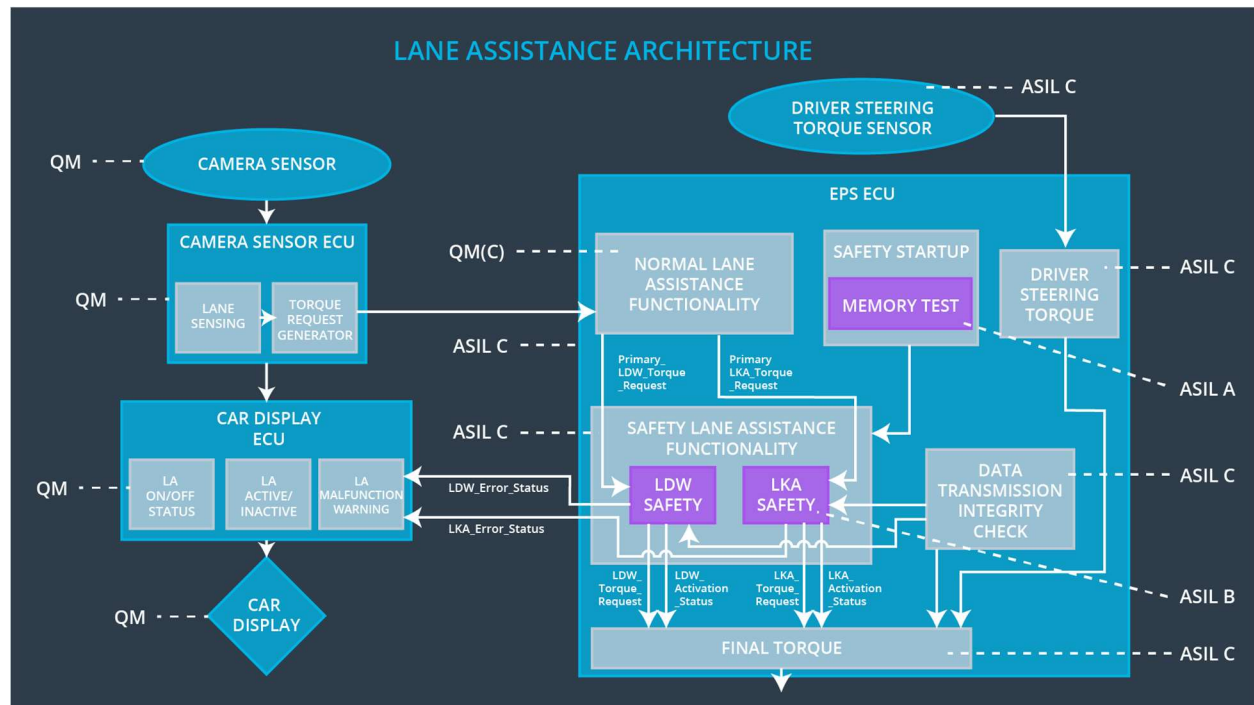
### Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:

[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.]

| ID                                    | Validation Acceptance Criteria and Method   | Verification Acceptance Criteria and Method   |
|---------------------------------------|---|---|
| Technical Safety Requirement 02-01-01 | Validate the Max_Duration is set to the chosen value from LKA Validation Assistance Criteria  | Verify the functionality is turned off after it is applied for Max_Duration.                |
| Technical Safety Requirement 02-01-02 | Validate the 'TORQUE_LIMITER' sends the error_status_torque_limiter signal to the LKA_SAFETY_ACTIVATION.  | Verify the Car Display ECU displays the Lane Keeping Assistance malfunction warning signal. |
| Technical Safety Requirement 02-01-03 | Validate the 'TORQUE_LIMITER' sends 'LKA_Torque_Request' with zero.   | Verify the Final EPS Torque generator receives a LKA_Torque_Request of zero.                |
| Technical Safety Requirement 02-01-04 | Validate the 'TORQUE_LIMITER' calculate and sends the correct cyclic redundancy check (CRC) and Alive counter for data transmission validity and integrity. | Verify the functionality is turn off if there is a CRC or Alive counter discrepancy.        |
| Technical Safety Requirement 02-01-05 | Validate the Safety Startup Memory test to check memory faults catch memory faults.   | Verify the Lane Keeping Assistance is turned off when the Safety Startup Memory fails.      |

## 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]

| ID                                    | Technical Safety Requirement  | Electronic Power Steering ECU | Camera ECU | Car Display ECU |
|---------------------------------------|---|-------------------------------|------------|-----------------|
| Technical Safety Requirement 01-01-01 | The Lane Departure Warning safety component shall ensure that the amplitude of the 'LDW_Torque_Request' sent to | X                             |            |                 |

|                                       |   |   |  |  |
|---------------------------------------|---|---|--|--|
|                                       | the 'Final electronic power steering Torque' component is below 'Max_Torque_Amplitude.'   |   |  |  |
| Technical Safety Requirement 01-01-02 | When the Lane Departure Warning is deactivated, the 'LDW Safety' software module shall send a signal to the Car Display ECU to turn on a warning signal.  | X |  |  |
| Technical Safety Requirement 01-01-03 | When a failure is detected by the Lane Departure Warning functionality, it shall deactivate the Lane Departure Warning feature and set 'LDW_Torque_Request' to zero.                              | X |  |  |
| Technical Safety Requirement 01-01-04 | The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.   | X |  |  |
| Technical Safety Requirement 01-01-05 | Memory test shall be conducted at start up of the EPS ECU to check for any memory problems  | X |  |  |
| Technical Safety Requirement 01-02-01 | The Lane Departure Warning safety component shall ensure the frequency of the 'LDW_Torque_Reques' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Frequency.' | X |  |  |
| Technical Safety Requirement 02-01-01 | The Lane Keeping Assistance safety component shall ensure the duration of the lane keeping assistance torque is applied for less than Max_Duration  | X |  |  |
| Technical Safety Requirement 02-01-02 | When the Lane Keeping Assistance function deactivates, the 'LKA Safety' shall send a  | X |  |  |



|                                       |   |   |   |   |
|---------------------------------------|---|---|---|---|
|                                       | signal to the Car Display ECU to turn on a warning light.   |   |   |   |
| Technical Safety Requirement 02-01-03 | When a failure is detected, the Lane Keeping Assistance function shall deactivate and the 'LKA_Torque_Request' shall be zero. | X |   |   |
| Technical Safety Requirement 02-01-04 | The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.                         | X |   |   |
| Technical Safety Requirement 02-01-05 | Memory test shall be conducted at start up of the EPS ECU to check for any memory problems                                    | X | X | X |

## 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](#).

Ofentimes, 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 Lane Departure Warning functionality  | Malfunction_01,<br>Malfunction_02,<br>Malfunction_04 | Yes                 | Lane Departure Warning<br>Malfunction Warning on Car Display  |
| WDC-02 | Turn off Lane Keeping Assistance functionality | Malfunction_03,<br>Malfunction_05                    | Yes                 | Lane Keeping Assistance<br>Malfunction Warning on Car Display |