

Software Safety Requirements and Architecture

Lane Assistance

**Document Version:1.0**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 27/11/2018 | 1.0 | Atul Kumar | Draft version |
| 29/11/2018 | 2.0 | Atul Kumar | Adding more feature |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# Table of Contents

[Document history](#_1t3h5sf)

[Table of Contents](#_pyp8fd3vpmy3)

[Purpose](#_c1lz2bx22jid)

[Inputs to the Software Requirements and Architecture Document](#_hjpgfzcjxim1)

[Technical safety requirements](#_lc6owg9q3amb)

[Refined Architecture Diagram from the Technical Safety Concept](#_db3hhee81tpq)

[Software Requirements](#_pul4igmpfvr0)

[Refined Architecture Diagram](#_b7fyegncumoz)

# Purpose

The purpose of the software safety requirements and architecture document is to identify new

detailed requirements and allocate these software requirements to component level diagrams

for the lane assistance functional safety project as pertain to the potential malfunctions of the

electrical and electronic systems as defined by ISO 26262 standard or tailored version as per organization.

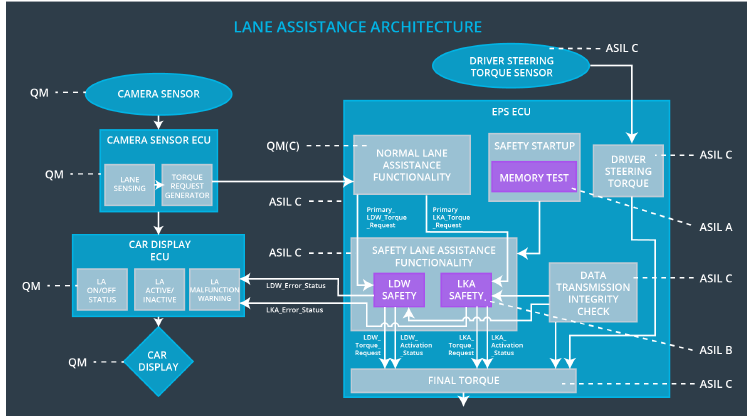
# Inputs to the Software Requirements and Architecture Document

## Technical safety requirements

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 block | Set lane departure warning torque 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 block | Set lane departure warning torque 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 block | Set lane departure warning torque to zero |
| Technical  Safety  Requirement  04 | The validity and integrity of  the data transmission for  'LDW\_Torque\_Request'  signal shall be ensured | A | 50ms | LDW Safety block | Set lane departure warning torque 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 | Data Transmission Integrity Check | Set lane departure warning torque to zero |
| Technical  Safety  Requirement  06 | The LDW safety component  shall ensure that the  fequency of the  'LDW\_Torque\_Request' sent  to the 'Final electronic power  steering Torque' component  is below  'Max\_Torque\_Fequency | C | 50ms | LDW Safety block | Set lane departure warning torque to zero |
| Technical  Safety  Requirement  07 | The LKA safety component  shall ensure that the duration  of the lane keeping  assistance torque applied is  less than Max\_Duration. | C | 500ms | LKA Safety block | Set lane keeping assistance torque to zero |
| Technical  Safety  Requirement  08 | 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 | C | 500ms | LKA Safety block | Set lane keeping assistance torque to zero |
| Technical  Safety  Requirement  09 | 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. | C | 500ms | LKA Safety block | Set lane keeping assistance torque to zero |
| Technical  Safety  Requirement  10 | The validity and integrity of  the data transmission for  'LKA\_Torque\_Request' signal shall be ensured | C | 500ms | LKA Safety block | Set lane keeping assistance torque to zero |
| Technical  Safety  Requirement  11 | Memory test shall be  conducted at start Up of the  EPS ECU to check for any  faults in memory. | A | Ignition Cycle | Data Transmission Integrity Check | Set lane keeping assistance torque to zero |
| Technical  Safety  Requirement  12 | The LKA safety component  shall ensure that the loss of  camera sensor torque  request transmission will  deactivate the LKA feature  and the 'LKA\_Torque\_Request' shall  be set to zero. | C | 500ms | LKA Safety block | Set lane keeping assistance torque to zero |

## Refined Architecture Diagram from the Technical Safety Concept



# Software Requirements

**Lane Departure Warning (LDW) Amplitude Malfunction Software Requirements:**

**[Instructions: Fill in the software safety requirements for the LDW amplitude malfunction technical safety requirements. We have provided the associated technical safety requirements. Hint: The software safety requirements were discussed in the text from the software and hardware lesson.**

**OPTIONAL:**

**CHALLENGE ONE**

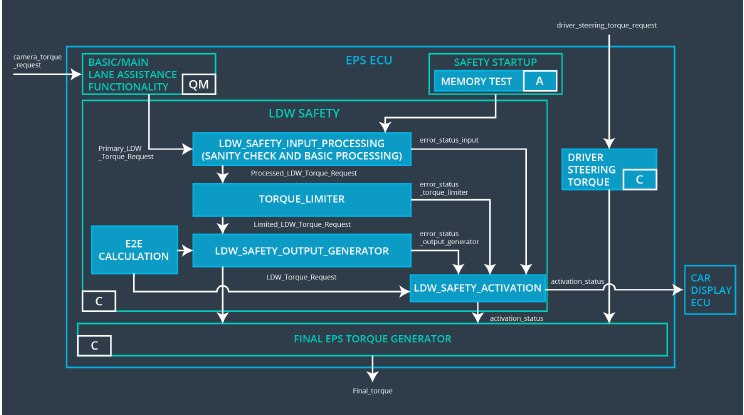
**Develop software safety requirements for the Lane Departure Warning (LDW) frequency function and modify the system architecture as needed.**

**CHALLENGE TWO**

**Develop software safety requirements for the Lane Keeping Assistance (LKA) function and modify the system architecture as needed.**

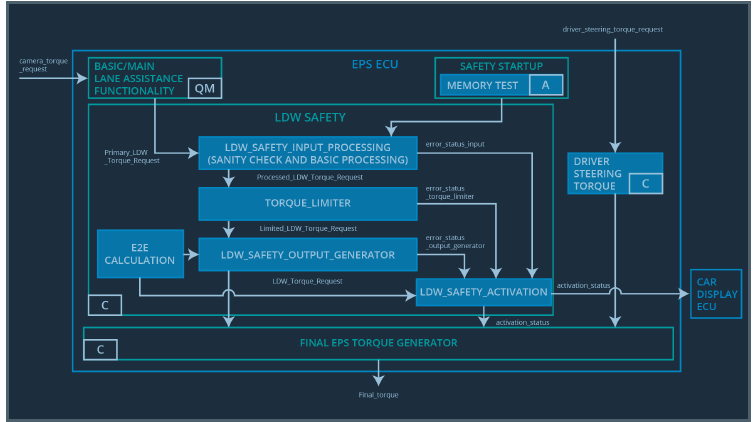
**]**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **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 block | Set lane departure warning torque to zero |



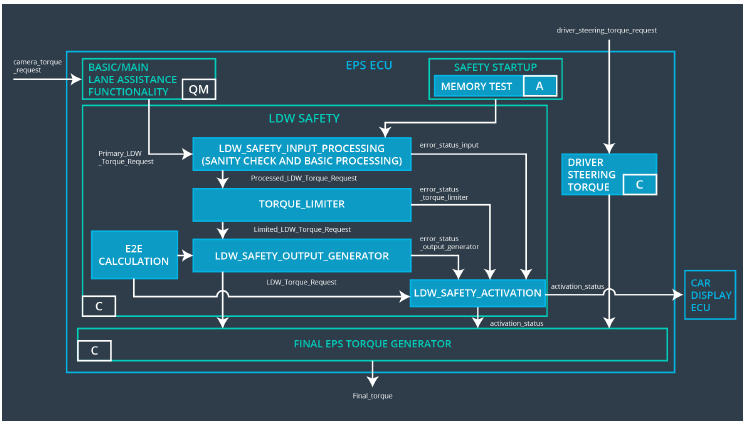
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Software Safety Requirement | ASIL | Allocation Software Elements | Safe State |
| Software  Safety  Requirement  01-01 | The input signal  “Primary\_LDW\_Torq\_Req” shall  be read and pre-processed to  determine the torque request  coming from the “Basic/Main  LAFunctionality” SW  Component.  Signal“processed\_LDW\_Torq\_R  eq”shall be generated at the end  of the processing | C | LDW\_SAFETY\_INPUT\_P  ROCESSING | Not Applicable |
| Software Safety Requirement 01-02 | In case the  “processed\_LDW\_Torq\_Req”  signal has a value greater  than“Max\_Torque\_Ampltide\_LD  W”(maximum allowed safe  torque), the torque signal  “limited\_LDW\_Torq\_Req” shall  be set to 0,  else“limited\_LDW\_Torq\_Req”  shall take the value of  “processed\_LDW\_Torq\_Req” | C | TORQUE\_LIMITER | “limited\_LDW\_T  orq\_Req” =  0(Nm=Newtonmeter) |
| Software Safety Requirement 01-03 | The“limited\_LDW\_Torq\_Req”shall be transformed into a signal  “LDW\_Torq\_Req” which is  suitable to be transmitted outside of the LDW Safety component (“LDW Safety”) to the “Final EPS Torque” component. | C | LDW\_SAFETY\_OUTPUT  \_GENERATOR | LDW\_Torq\_Req  = 0 (Nm) |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| Technical  Safety  Requirement  02 | 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 block | Set lane  departure  warning  torque to  zero |
|  |  |  |  |  |  |



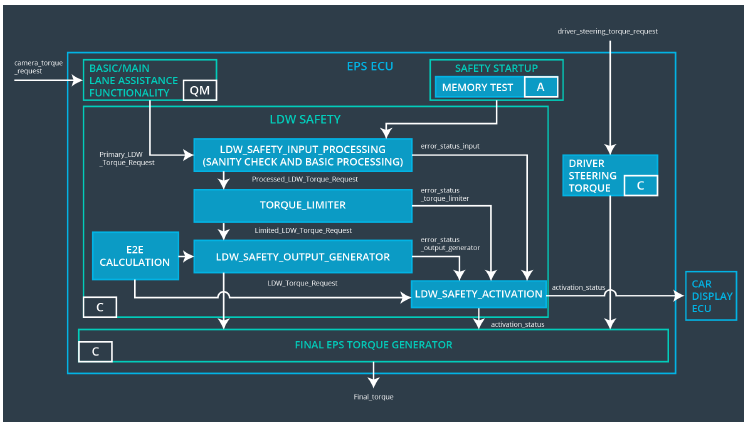
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | **ASIL** | **Allocation Software Elements** | **Safe State** |
| Software Safety Requirement 02-01 | Each of the SW elements shall  output a signal to indicate any  error which is detected by the  element. Error signal =  error\_status\_input(LDW\_SAFET  Y\_INPUT\_PROCESSING),  error\_status\_torque\_limiter(TOR  C All N/A  8  QUE\_LIMITER),  error\_status\_output\_gen(LDW\_  SAFETY\_OUTPUT\_GENERAT  OR) | C | All | Not Applicable |
| Software Safety Requirement 02-02 | A software element shall  evaluate the error status of all  the other software elements and  in case any 1 of them indicates  an error, it shall deactivate  theLDW  feature(“activation\_status”=0) | C | LDW\_SAFETY  \_ACTIVATION | Activation\_status = 0  (LDW function  deactivated) |
|  | In case of no errors from the  software elements, the status of  the LDW feature shall be set to  activated (“activation\_status”=1) |  | LDW\_SAFETY  \_ACTIVATION | Not Applicable |
|  | In case an error is detected by  any of the software elements, it  shall set the value of its  corresponding torque to 0 so  that “LDW\_Torq\_Req” is set to 0 |  | ALL | LDW\_Torq\_Req= 0  (Nm) |
|  | Once the LDW functionality has  been deactivated, it shall stay  deactivated till the time the  ignition is switched from off to on  again. | C | LDW\_SAFETY  \_ACTIVATION | Activation\_status = 0  (LDW function  deactivated) |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| Technical  Safety  Requirement  03 | 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 block | Set lane  departure  warning  torque to  zero |



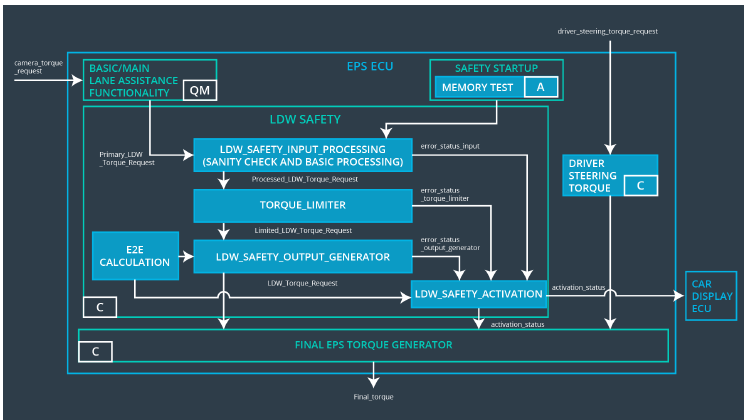
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | **ASIL** | **Allocation Software Elements** | **Safe State** |
| Software Safety Requirement03-01 | When the LDW function is  deactivated (activation\_status  set to 0), the activation\_status  shall be sent to the car  displayECU. | C | LDW\_SAFET  Y\_ACTIVATIO  N, CarDisplay  ECU | Not Applicable |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| Technical  Safety  Requirement  04 | 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 block | Set lane departure warning torque to zero |

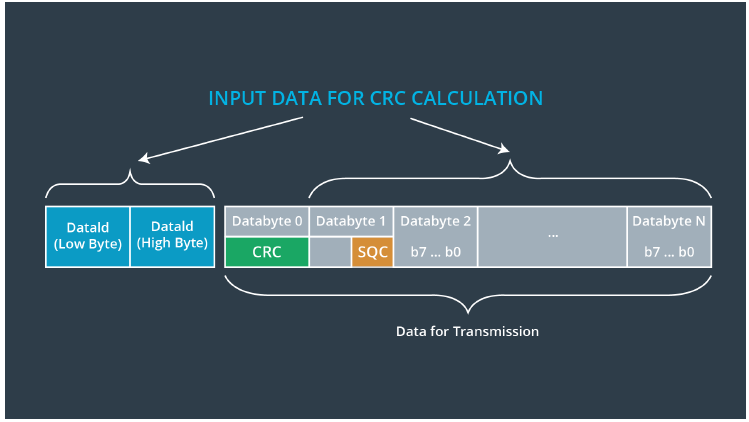


|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | **ASIL** | **Allocation Software Elements** | **Safe State** |
| Software Safety Requirement 04-01 | When the LDW function is  deactivated (activation\_status  set to 0), the activation\_status  shall be sent to the car  displayECU | C | LDW\_SAFETY\_ACTIVATION,CarDisplay ECU | Not Applicable |

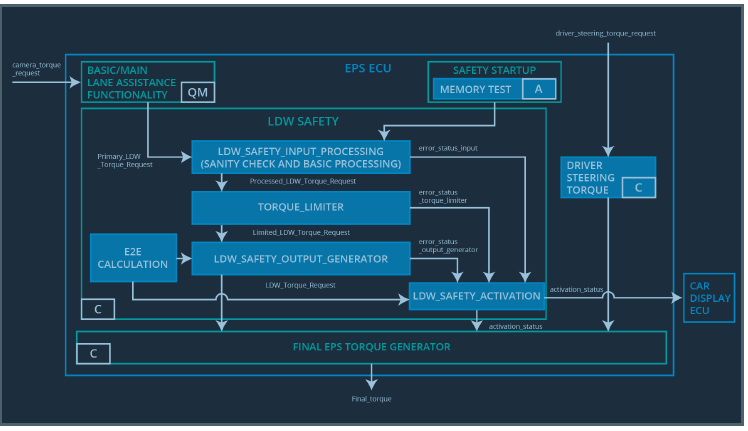
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| Technical  Safety  Requirement  04-01 | The validity and integrity of the  data transmission for  LDW\_Torque\_Request signal  shall be ensured | C | 50ms | Data Transmission Integrity Check | Not Applicable |



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | **ASIL** | **Allocation Software Elements** | **Safe State** |
| Software Safety Requirement 04-01 | Any data to be transmitted  outside of the LDW  Safety component (“LDW  Safety”)including  "LDW\_Torque\_Req" and  “activation\_status” shall be protected by an End2End protection mechanism | C | E2ECalc | LDW\_Torq\_Req=0(Nm) |
|  | The E2E protection protocol  shall contain and attach the  control data: alive counter (SQC)  and CRC to the data to be  transmitted. | C | E2ECalc | LDW\_Torq\_Req=0(Nm) |



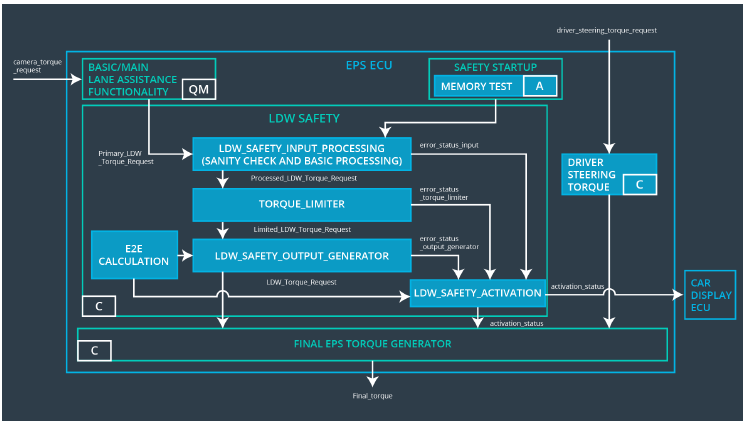
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| Technical  Safety  Requirement  05 | Memory test shall be conducted  at startup of the EPS ECU to  check for any faults in memory | A | Ignition Cycle | Data Transmission Integrity Check | Set lane  departure  warning  torque to  zero |



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | **ASIL** | **Allocation Software Elements** | **Safe State** |
| Software Safety Requirement 04-01 | A CRC verification check over  the software code in the Flash  memory shall be done every  time the ignition is switched from  off to on to check for any  corruption of content. | A | MEMORYTEST | Activation\_status=0 |
| Software Safety Requirement 04-01 | Standard RAM tests to check the data bus, address bus and  device integrity shall be done  every time the ignition is  switched from off to on. | A | MEMORYTEST | Activation\_status=0 |
| Software Safety Requirement 04-01 | The test result of the RAM or  Flash memory shall be indicated  to the LDW\_Safety component  via the “test\_status” signal | A | MEMORYTEST | Activation\_status=0 |
| Software Safety Requirement 04-01 | In case any fault is indicated via  the “test\_status” signal the  INPUT\_LDW\_PROCESSING  shall set an error on  error\_status\_input (=1) so that  the LDW functionality is  deactivated and the LDWTorque  is set to 0 | A | LDW\_SAFETY\_PROCESSING | Activation\_status=0 |
|  |  |  |  |  |

Lane Departure Warning(LDW) Frequency Malfunction Software Requirements:

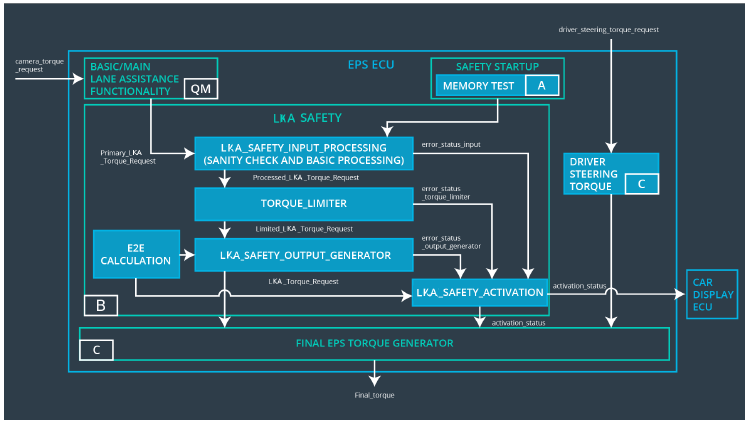
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| Technical  Safety  Requirement  05 | The LDW safety component  shall ensure that the frequency  of the LDW\_Torque\_Request  sent to the Final Electronic  Power Steering Torque  component is below  Max\_Torque\_Frequency | C | 50 ms | LDW safety block | Set lane  departure  warning  torque to  zero |



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | **ASIL** | **Allocation Software Elements** | **Safe State** |
| Software Safety Requirement 04-01 | The input signal  “Primary\_LDW\_Torq\_Req” shall  be read and pre-processed to  determine the torque request  coming from the “Basic/Main LA  Functionality” SW Component.  Signal“processed\_LDW\_Torq\_R  eq”shall be generated at the end  of the processing. | C | LDW\_SAFETY\_INPUT\_PROCESSING | Not Applicable |
| Software Safety Requirement 04-02 | In case the  “processed\_LDW\_Torq\_Req”  signal has a value greater  than“Max\_Torque\_Frequency\_L  DW”(maximum allowed safe  torque), the torque signal  “limited\_LDW\_Torq\_Req” shall  be set to 0,  else“limited\_LDW\_Torq\_Req”  shall take the value of  “processed\_LDW\_Torq\_Req”. | C | TORQUE\_LIMITER | “limited\_LDW\_T  orq\_Req” =  0(Nm=Newtonmeter) |
| Software Safety Requirement 04-03 | The “limited\_LDW\_Torq\_Req”shall  be transformed into a signal  “LDW\_Torq\_Req” whichis  suitable to be transmitted  outside of the LDW  Safetycomponent (“LDW  Safety”) to the “Final EPS  Torque”component. | C | LDW\_SAFETY\_OUTPUT  \_GENERATOR | LDW\_Torq\_Req  = 0 (Nm) |
|  |  |  |  |  |

Lane Keeping Assistance(LKA) sensor Malfunction Software Requirements:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| Technical  Safety  Requirement  05 | The LKA safety component shall  ensure that the loss of camera  sensor torque request  transmission will deactivate the  LKA feature and the  'LKA\_Torque\_Request' shall be  set to zero. | B | 50ms | LDW Safety block | Set Lane keeping assistance torque to zero |



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | **ASIL** | **Allocation Software Elements** | **Safe State** |
| Software Safety Requirement 05-01 | The input signal  “Primary\_LKA\_Torq\_Req” shall  be read and pre-processed to  determine the torque request  coming from the “Basic/Main LA  Functionality” SW Component.  Signal“processed\_LKA\_Torq\_Re  q” shall be generated at the end  of the processing. | B | LKA\_SAFETY\_INPUT\_PR  OCESSING | Not Applicable |
| Software Safety Requirement 05-02 | In case the  “processed\_LKA\_Torq\_Req”  signal has an invalid Alive  counter (SQC), the camera  sensor ECU is no longer  detecting lane lines, the torque  signal “limited\_LKA\_Torq\_Req”  shall be set to 0,  else“limited\_LKA\_Torq\_Req”  shall take the value of  “processed\_LKA\_Torq\_Req”. | B | TORQUE\_LIMITER | “limited\_LKA\_To  rq\_Req” =  0(Nm=Newtonmeter) |
| Software Safety Requirement 05-03 | The  “limited\_LKA\_Torq\_Req”shall be  transformed into a signal  “LKA\_Torq\_Req” whichis  suitable to be transmitted  outside of the LKA  Safetycomponent (“ LKA Safety”)  to the “Final EPS  Torque”component. | B | LKA\_SAFETY\_OUTPUT\_  GENERATOR | LKA\_Torq\_Req=  0 (Nm) |

Refined Architecture Diagram

