Software Safety Requirements and Architecture

Lane Assistance

Document Version: [Version] Template Version 1.0, Released on 2017-06-21

****

# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 26/08/2017 | 1.0 | Bide Huang | Initial 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

Inputs to the Software Requirements and Architecture Document Technical safety requirementsRefined Architecture Diagram from the Technical Safety Concept

Software Requirements

Refined Architecture Diagram

# Purpose

The purpose of 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 system as defined by ISO26262.

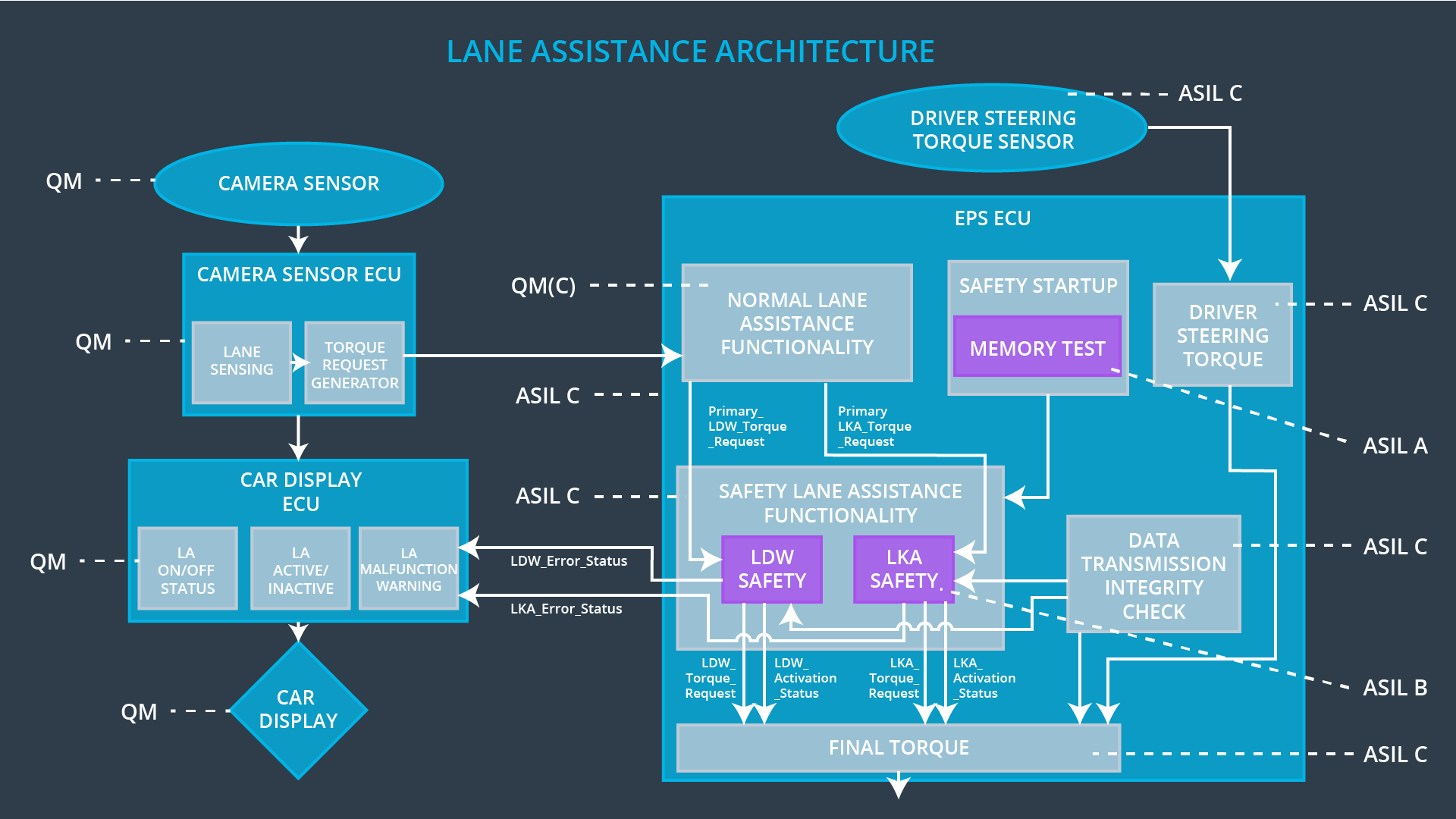
# Inputs to the Software Requirements and Architecture Document

## Technical safety requirements

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **A S I L** | **Fault Tolerant Time Interval** | **Architecture Allocation** | **Safe State** |
| Technical | The LDW safety components | C | 50ms | LDW Safety | LDW torque |
| Safety Requirement 01 | shall ensure that the amplitude of "LDW\_Torque\_Request" |  |  | Functionality | output is set to zero |
|  | send to the "Final electronic |  |  |  |  |
|  | power steering torque" |  |  |  |  |
|  | components is below |  |  |  |  |
|  | "Max\_Torque\_Amplitude" |  |  |  |  |
| Technical | The validity and integrity of | C | 50ms | Data | N/A |
| Safety | the data transmission for |  |  | Transmission |  |
| Requirement  02 | LDW\_Torque\_Request signal shall be ensured |  |  | integrity  check |  |
| Technical | As soon as a failure is | C | 50ms | LDW Safety | LDW torque |
| Safety Requirement 03 | detected by the LDW function, it shall deactivate the LDW feature and |  |  | Functionality | output is set to zero |
|  | "LDW\_Torque\_Request" |  |  |  |  |
|  | shall be set to zero. |  |  |  |  |
| Technical | As soon as the LDW function | C | 50ms | LDW Safety | LDW torque |
| Safety | deactivates the LDW feature, |  |  | Functionality | output is set |
| Requirement  04 | the "LDW Safety" software block shall send a signal to |  |  |  | to zero |
|  | the car display to turn a |  |  |  |  |
|  | warning light. |  |  |  |  |
| Technical | Memory test shall be | A | Ignition | Safety startup | LDW torque |
| Safety Requirement 05 | conducted at startup of the EPS ECU to check any faults in memory. |  | Cycle | memory test | output is set to zero |

## Refined Architecture Diagram from the Technical Safety Concept

****

# Software Requirements

Lane Departure Warning (LDW) Amplitude Malfunction Software Requirements:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **A** | **Fault** | **Allocation to** | **Safe State** |
|  |  | **S I L** | **Tolerant Time Interval** | **Architecture** |  |
| Technical | The LDW safety component | C | 50ms | LDW Safety | LDW torque |
| Safety Requirement 01 | shall ensure that the amplitude of the LDW\_Torque\_Request sent to the Final Electronic |  |  | Functionality | output is set to zero |
|  | Power Steering Torque |  |  |  |  |
|  | component is below |  |  |  |  |
|  | Max\_Torque\_Amplitude |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Software Safety Requirement | A S I L | Allocation Software Elements | Safe State |
| Software | The input signal | C | LDW\_SAFETY\_INPUT\_P | N/A |
| Safety | “Primary\_LDW\_Torq\_Req” shall |  | ROCESSING |  |
| Requirement | be read and pre-processed to |  |  |  |
| 01-01 | 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. |  |  |  |
| Software | In case the | C | TORQUE\_LIMITER | “limited\_LDW\_ |
| Safety | “processed\_LDW\_Torq\_Req” |  |  | Torq\_Req” = |
| Requirement | signal has a value greater |  |  | 0(Nm=Newton- |
| 01-02 | than“Max\_Torque\_Ampltide\_LD |  |  | meter) |
|  | 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”. |  |  |  |
| Software | The | C | LDW\_SAFETY\_OUTPUT\_ | LDW\_Torq\_Req |
| Safety | “limited\_LDW\_Torq\_Req”shall |  | GENERATOR | = 0 (Nm) |
| Requirement | be transformed into a signal |  |  |  |
| 01-03 | “LDW\_Torq\_Req” whichis |  |  |  |
|  | suitable to be transmitted |  |  |  |
|  | outside of the LDW Safety |  |  |  |
|  | component (“LDW Safety”) to the “Final EPS Torque”component. Also see SofSafReq02-01 andSofSafReq02-02 |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **A S I L** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| Technical | The validity and integrity of the | C | 50ms | Data | N/A |
| Safety | data transmission for |  |  | Transmission |  |
| Requirement  02 | LDW\_Torque\_Request signal shall be ensured |  |  | Integrity Check |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | **A S I L** | **Allocation Software Elements** | **Safe State** |
| Software | Any data to be transmitted | C | E2ECalc | LDW\_Torq\_Re |
| Safety | outside of the LDW Safety |  |  | q= 0 (Nm) |
| Requirement | component (“LDW Safety”) |  |  |  |
| 02-01 | including |  |  |  |
|  | "LDW\_Torque\_Req"and |  |  |  |
|  | “activation\_status” |  |  |  |
|  | (seeSofSafReq03-02) shall be |  |  |  |
|  | protected by an End2End(E2E) |  |  |  |
|  | protection mechanism |  |  |  |
| Software | The E2E protection protocol | C | E2ECalc | LDW\_Torq\_Req |
| Safety | shall contain and attach the |  |  | = 0 (Nm) |
| Requirement | control data: alive counter (SQC) |  |  |  |
| 02-02 | and CRC to the data to be |  |  |  |
|  | transmitted. |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **A S I L** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| Technical | As soon as a failure is detected | C | 50ms | LDW Safety | LDW torque |
| Safety | by the LDW function, it shall |  |  | Functionality | output is set |
| Requirement  03 | deactivate the LDW feature and the LDW\_Torque\_Request shall |  |  |  | to zero |
|  | be set to zero |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | **A S I L** | **Allocation Software Elements** | **Safe State** |
| Software | Each of the SW elements shall | C | All | N/A |
| Safety | output a signal to indicate any |  |  |  |
| Requirement | error which is detected by the |  |  |  |
| 03-01 | element. Error signal = |  |  |  |
|  | error\_status\_input(LDW\_SAFETY |  |  |  |
|  | \_INPUT\_PROCESSING), |  |  |  |
|  | error\_status\_torque\_limiter(TORQ |  |  |  |
|  | UE\_LIMITER), |  |  |  |
|  | error\_status\_output\_gen(LDW\_SA |  |  |  |
|  | FETY\_OUTPUT\_GENERATOR) |  |  |  |
| Software | A software element shall evaluate | C | LDW\_SAFETY\_A | Activation\_status = 0 |
| Safety | the error status of all the other |  | CTIVATION | (LDW function |
| Requirement | software elements and in case any |  |  | deactivated) |
| 03-02 | 1 of them indicates an error, it |  |  |  |
|  | shall deactivate the LDW |  |  |  |
|  | feature(“activation\_status”=0) |  |  |  |
| Software | In case of no errors from the | C | LDW\_SAFETY\_A | N/A |
| Safety | software elements, the status of |  | CTIVATION |  |
| Requirement | the LDW feature shall be set to |  |  |  |
| 03-03 | activated (“activation\_status”=1) |  |  |  |
| Software | In case an error is detected by any | C | All | LDW\_Torq\_Req = 0 |
| Safety | of the software elements, it shall |  |  |  |
| Requirement | set the value of its corresponding |  |  |  |
| 03-04 | torque to 0 so that |  |  |  |
|  | “LDW\_Torq\_Req” is set to 0 |  |  |  |
| Software | Once the LDW functionality has | C | LDW\_SAFETY\_A | Activation\_status = 0 |
| Safety Requirement 03-05 | been deactivated, it shall stay deactivated till the time the ignition is switched from off to on again. |  | CTIVATION | (LDW function deactivated) |

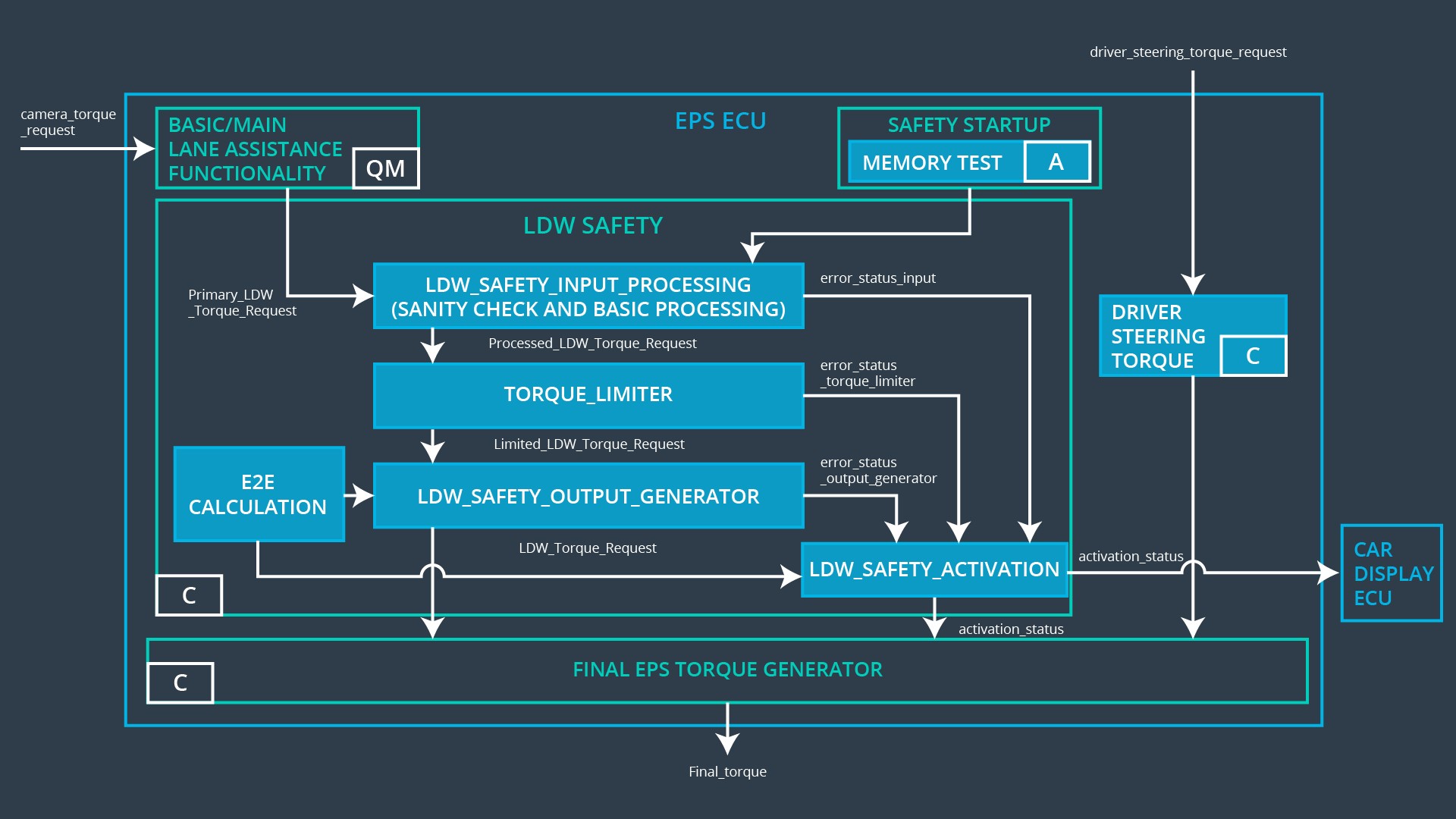
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **A S I L** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| Technical | As soon as the LDW function | C | 50ms | LDW Safety | LDW torque |
| Safety | deactivates the LDW feature, the |  |  | Functionality | output is set |
| Requirement  04 | LDW Safety software block shall send a signal to the car display |  |  |  | to zero |
|  | ECU to turn on a warning light |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | **A S I L** | **Allocation Software Elements** | **Safe State** |
| Software | When the LDW function is | C | LDW\_SAFET | N/A |
| Safety | deactivated (activation\_status |  | Y\_ACTIVATIO |  |
| Requirement | set to 0), the activation\_status |  | N, CarDisplay |  |
| 04-01 | shall be sent to the car |  | ECU |  |
|  | displayECU. |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **A S I L** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| Technical | Memory test shall be conducted | A | Ignition | Safety startup | LDW torque |
| Safety | at start up of the EPS ECU to |  | Cycle | memory test | output is set |
| Requirement  05 | check for any faults in memory |  |  |  | to zero |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | **A S I L** | **Allocation Software Elements** | **Safe State** |
| Software | A CRC verification check over the | A | MEMORYTES | Activation\_status = 0 |
| Safety | software code in the Flash |  | T |  |
| Requirement | memory shall be done every time |  |  |  |
| 05-01 | the ignition is switched from off to |  |  |  |
|  | on to check for any corruption of |  |  |  |
|  | content. |  |  |  |
| Software | Standard RAM tests to check the | A | MEMORYTES | Activation\_status = 0 |
| Safety | data bus, address bus and device |  | T |  |
| Requirement | integrity shall be done every time |  |  |  |
| 05-02 | the ignition is switched from off to |  |  |  |
|  | on (E.g.walking 1s test, RAM |  |  |  |
|  | pattern test. Refer RAM and |  |  |  |
|  | processor vendor |  |  |  |
|  | recommendations ) |  |  |  |
| Software | The test result of the RAM or | A | MEMORYTES | Activation\_status = 0 |
| Safety | Flash memory shall be indicated to |  | T |  |
| Requirement | the LDW\_Safety component via |  |  |  |
| 05-03 | the “test\_status” signal |  |  |  |
| Software | In case any fault is indicated via | A | MEMORYTES | Activation\_status = 0 |
| Safety | the “test\_status” signal the |  | T |  |
| Requirement | INPUT\_LDW\_PROCESSING shall |  |  |  |
| 05-04 | set an error on error\_status\_input |  |  |  |
|  | (=1) so that the LDW functionality |  |  |  |
|  | is deactivated and the LDW |  |  |  |
|  | Torque is set to 0 |  |  |  |

# Refined Architecture Diagram

****

Lane Departure Warning (LDW) Frequency Malfunction Software Requirements:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | | **Technical Safety Requirement** | | **A S I L** | | **Fault Tolerant Time Interval** | **Allocation to Architecture** | | **Safe State** |
| Technical | | The LDW safety component | | C | | 50ms | LDW Safety | | LDW torque |
| Safety | | shall ensure that the frequency | |  | |  | Functionality | | output is set |
| Requirement  01 | | of the LDW\_Torque\_Request sent to the Final Electronic | |  | |  |  | | to zero |
|  | | Power Steering Torque | |  | |  |  | |  |
|  | | component is below | |  | |  |  | |  |
|  | | Max\_Torque\_Frequency | |  | |  |  | |  |
| ID | Software Safety Requirement | | A S I L | | Allocation Software Elements | | | Safe State | |
| Software | The input signal | | C | | LDW\_SAFETY\_INPUT\_P | | | N/A | |
| Safety | “Primary\_LDW\_Torq\_Req” shall | |  | | ROCESSING | | |  | |
| Requirement | be read and pre-processed to | |  | |  | | |  | |
| 01-01 | 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. | |  | |  | | |  | |
| Software | In case the | | C | | TORQUE\_LIMITER | | | “limited\_LDW\_ | |
| Safety | “processed\_LDW\_Torq\_Req” | |  | |  | | | Torq\_Req” = | |
| Requirement | signal has a value greater | |  | |  | | | 0(Nm=Newton- | |
| 01-02 | than“Max\_Torque\_Frequency\_L | |  | |  | | | meter) | |
|  | 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”. | |  | |  | | |  | |
| Software | The | | C | | LDW\_SAFETY\_OUTPUT\_ | | | LDW\_Torq\_Req | |
| Safety | “limited\_LDW\_Torq\_Req”shall | |  | | GENERATOR | | | = 0 (Nm) | |
| Requirement | be transformed into a signal | |  | |  | | |  | |
| 01-03 | “LDW\_Torq\_Req” whichis | |  | |  | | |  | |
|  | suitable to be transmitted | |  | |  | | |  | |
|  | outside of the LDW Safety | |  | |  | | |  | |
|  | component (“LDW Safety”) to | |  | |  | | |  | |
|  | the “Final EPS | |  | |  | | |  | |
|  | Torque”component. Also see | |  | |  | | |  | |
|  | SofSafReq02-01 | |  | |  | | |  | |
|  | andSofSafReq02-02 | |  | |  | | |  | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **A S I L** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| Technical | The validity and integrity of the | C | 50ms | Data | N/A |
| Safety | data transmission for |  |  | Transmission |  |
| Requirement  02 | LDW\_Torque\_Request signal shall be ensured |  |  | Integrity Check |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | **A S I L** | **Allocation Software Elements** | **Safe State** |
| Software | Any data to be transmitted | C | E2ECalc | LDW\_Torq\_Re |
| Safety | outside of the LDW Safety |  |  | q= 0 (Nm) |
| Requirement | component (“LDW Safety”) |  |  |  |
| 02-01 | including |  |  |  |
|  | "LDW\_Torque\_Req"and |  |  |  |
|  | “activation\_status” |  |  |  |
|  | (seeSofSafReq03-02) shall be |  |  |  |
|  | protected by an End2End(E2E) |  |  |  |
|  | protection mechanism |  |  |  |
| Software | The E2E protection protocol | C | E2ECalc | LDW\_Torq\_Req |
| Safety | shall contain and attach the |  |  | = 0 (Nm) |
| Requirement | control data: alive counter (SQC) |  |  |  |
| 02-02 | and CRC to the data to be |  |  |  |
|  | transmitted. |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **A S I L** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| Technical | As soon as a failure is detected | C | 50ms | LDW Safety | LDW torque |
| Safety | by the LDW function, it shall |  |  | Functionality | output is set |
| Requirement  03 | deactivate the LDW feature and the LDW\_Torque\_Request shall |  |  |  | to zero |
|  | be set to zero |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | **A S I L** | **Allocation Software Elements** | **Safe State** |
| Software | Each of the SW elements shall | C | All | N/A |
| Safety | output a signal to indicate any |  |  |  |
| Requirement | error which is detected by the |  |  |  |
| 03-01 | element. Error signal = |  |  |  |
|  | error\_status\_input(LDW\_SAFETY |  |  |  |
|  | \_INPUT\_PROCESSING), |  |  |  |
|  | error\_status\_torque\_limiter(TORQ |  |  |  |
|  | UE\_LIMITER), |  |  |  |
|  | error\_status\_output\_gen(LDW\_SA |  |  |  |
|  | FETY\_OUTPUT\_GENERATOR) |  |  |  |
| Software | A software element shall evaluate | C | LDW\_SAFETY\_A | Activation\_status = 0 |
| Safety | the error status of all the other |  | CTIVATION | (LDW function |
| Requirement | software elements and in case any |  |  | deactivated) |
| 03-02 | 1 of them indicates an error, it |  |  |  |
|  | shall deactivate the LDW |  |  |  |
|  | feature(“activation\_status”=0) |  |  |  |
| Software | In case of no errors from the | C | LDW\_SAFETY\_A | N/A |
| Safety | software elements, the status of |  | CTIVATION |  |
| Requirement | the LDW feature shall be set to |  |  |  |
| 03-03 | activated (“activation\_status”=1) |  |  |  |
| Software | In case an error is detected by any | C | All | LDW\_Torq\_Req = 0 |
| Safety | of the software elements, it shall |  |  |  |
| Requirement | set the value of its corresponding |  |  |  |
| 03-04 | torque to 0 so that |  |  |  |
|  | “LDW\_Torq\_Req” is set to 0 |  |  |  |
| Software | Once the LDW functionality has | C | LDW\_SAFETY\_A | Activation\_status = 0 |
| Safety | been deactivated, it shall stay |  | CTIVATION | (LDW function |
| Requirement | deactivated till the time the ignition |  |  | deactivated) |
| 03-05 | is switched from off to on again. |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **A S I L** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| Technical | As soon as the LDW function | C | 50ms | LDW Safety | LDW torque |
| Safety | deactivates the LDW feature, the |  |  | Functionality | output is set |
| Requirement  04 | LDW Safety software block shall send a signal to the car display |  |  |  | to zero |
|  | ECU to turn on a warning light |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | | | **A S I L** | | **Allocation Software Elements** | | **Safe State** | |
| Software | When the LDW function is | | | C | | LDW\_SAFET | | N/A | |
| Safety | deactivated (activation\_status | | |  | | Y\_ACTIVATIO | |  | |
| Requirement | set to 0), the activation\_status | | |  | | N, CarDisplay | |  | |
| 04-01 | shall be sent to the car | | |  | | ECU | |  | |
|  | displayECU. | | |  | |  | |  | |
| **ID** | | **Technical Safety Requirement** | **A S I L** | | **Fault Tolerant Time Interval** | | **Allocation to Architecture** | | **Safe State** |
| Technical | | Memory test shall be conducted | A | | Ignition | | Safety startup | | LDW torque |
| Safety | | at start up of the EPS ECU to |  | | Cycle | | memory test | | output is set |
| Requirement  05 | | check for any faults in memory |  | |  | |  | | to zero |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | | **Software Safety Requirement** | | **A S I L** | | **Allocation Software Elements** | | **Safe State** | |
| Software | | A CRC verification check over the | | A | | MEMORYTES | | Activation\_status = 0 | |
| Safety | | software code in the Flash | |  | | T | |  | |
| Requirement | | memory shall be done every time | |  | |  | |  | |
| 05-01 | | the ignition is switched from off to | |  | |  | |  | |
|  | | on to check for any corruption of | |  | |  | |  | |
|  | | content. | |  | |  | |  | |
| Software | | Standard RAM tests to check the | | A | | MEMORYTES | | Activation\_status = 0 | |
| Safety | | data bus, address bus and device | |  | | T | |  | |
| Requirement | | integrity shall be done every time | |  | |  | |  | |
| 05-02 | | the ignition is switched from off to | |  | |  | |  | |
|  | | on (E.g.walking 1s test, RAM | |  | |  | |  | |
|  | | pattern test. Refer RAM and | |  | |  | |  | |
|  | | processor vendor | |  | |  | |  | |
|  | | recommendations ) | |  | |  | |  | |
| Software | | The test result of the RAM or | | A | | MEMORYTES | | Activation\_status = 0 | |
| Safety | | Flash memory shall be indicated to | |  | | T | |  | |
| Requirement | | the LDW\_Safety component via | |  | |  | |  | |
| 05-03 | | the “test\_status” signal | |  | |  | |  | |
| Software | | In case any fault is indicated via | | A | | MEMORYTES | | Activation\_status = 0 | |
| Safety | | the “test\_status” signal the | |  | | T | |  | |
| Requirement | | INPUT\_LDW\_PROCESSING shall | |  | |  | |  | |
| 05-04 | | set an error on error\_status\_input | |  | |  | |  | |
|  | | (=1) so that the LDW functionality | |  | |  | |  | |
|  | | is deactivated and the LDW | |  | |  | |  | |
|  | | Torque is set to 0 | |  | |  | |  | |
| **ID** | **Technical Safety Requirement** | | **A S I L** | | **Fault Tolerant Time Interval** | | **Allocation to Architecture** | | **Safe State** |
| Technical | The LKA safety component shall | | B | | 500ms | | LKA Safety | | LKA torque |
| Safety | ensure that the duration of | |  | |  | | Functionality | | output is set |
| Requirement 01 | "LKA\_Torque\_Request" send to the "Final electronic power steering torque" component is | |  | |  | |  | | to zero |
|  | below Max\_Duration. | |  | |  | |  | |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Software Safety Requirement | A S I L | Allocation Software Elements | Safe State |
| Software | The input signal | B | LKA\_SAFETY\_INPUT\_PR | N/A |
| Safety | “Primary\_LKA\_Torq\_Req” shall |  | OCESSING |  |
| Requirement | be read and pre-processed to |  |  |  |
| 01-01 | determine the torque request |  |  |  |
|  | coming from the “Basic/Main |  |  |  |
|  | LAFunctionality” SW |  |  |  |
|  | Component. |  |  |  |
|  | Signal“processed\_LKA\_Torq\_Re |  |  |  |
|  | q”shall be generated at the end |  |  |  |
|  | of the processing. |  |  |  |
| Software | In case the | B | TORQUE\_LIMITER | “limited\_LKA\_ |
| Safety | “processed\_LKA\_Torq\_Req” |  |  | Torq\_Req” = |
| Requirement | signal has a value greater |  |  | 0(Nm=Newton- |
| 01-02 | duration than“Max\_Duration |  |  | meter) |
|  | \_LKA”(maximum duration |  |  |  |
|  | allowed safe torque), 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”. |  |  |  |
| Software | The | B | LKA\_SAFETY\_OUTPUT\_G | LKA\_Torq\_Req |
| Safety | “limited\_LKA\_Torq\_Req”shall be |  | ENERATOR | = 0 (Nm) |
| Requirement | transformed into a signal |  |  |  |
| 01-03 | “LKA\_Torq\_Req” whichis |  |  |  |
|  | suitable to be transmitted |  |  |  |
|  | outside of the LKA Safety |  |  |  |
|  | component (“LKA Safety”) to the |  |  |  |
|  | “Final EPS Torque”component. Also see SofSafReq02-01 andSofSafReq02-02 |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **A S I L** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| Technical | The validity and integrity of the | B | 500ms | Data | N/A |
| Safety | data transmission for |  |  | Transmission |  |
| Requirement 02 | "LKA\_Torque\_Request" signal shall be ensured. |  |  | integrity check |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | **A S I L** | **Allocation Software Elements** | **Safe State** |
| Software | Any data to be transmitted | B | E2ECalc | LKA\_Torq\_Req |
| Safety | outside of the LKA Safety |  |  | = 0 (Nm) |
| Requirement | component (“LKA Safety”) |  |  |  |
| 02-01 | including "LKA\_Torque\_Req"and |  |  |  |
|  | “activation\_status” |  |  |  |
|  | (seeSofSafReq03-02) shall be |  |  |  |
|  | protected by an End2End(E2E) |  |  |  |
|  | protection mechanism |  |  |  |
| Software | The E2E protection protocol | B | E2ECalc | LKA\_Torq\_Req |
| Safety | shall contain and attach the |  |  | = 0 (Nm) |
| Requirement | control data: alive counter (SQC) |  |  |  |
| 02-02 | and CRC to the data to be |  |  |  |
|  | transmitted. |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **A S I L** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| Technical | As soon as a failure is detected | B | 500ms | LKA Safety | LKA torque |
| Safety Requireme nt  03 | by the LKA function, it shall deactivate the LKA feature and "LKA\_Torque\_Request" shall be set to zero. |  |  | Functionallity | output is set to zero |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | **A S I L** | **Allocation Software Elements** | **Safe State** |
| Software | Each of the SW elements shall | B | All | N/A |
| Safety | output a signal to indicate any |  |  |  |
| Requirement | error which is detected by the |  |  |  |
| 03-01 | element. Error signal = |  |  |  |
|  | error\_status\_input(LKA\_SAFETY\_ |  |  |  |
|  | INPUT\_PROCESSING), |  |  |  |
|  | error\_status\_torque\_limiter(TORQ |  |  |  |
|  | UE\_LIMITER), |  |  |  |
|  | error\_status\_output\_gen(LKA\_SA |  |  |  |
|  | FETY\_OUTPUT\_GENERATOR) |  |  |  |
| Software | A software element shall evaluate | B | LKA\_SAFETY\_A | Activation\_status = 0 |
| Safety | the error status of all the other |  | CTIVATION | (LKA function |
| Requirement | software elements and in case any |  |  | deactivated) |
| 03-02 | 1 of them indicates an error, it |  |  |  |
|  | shall deactivate the LKA |  |  |  |
|  | feature(“activation\_status”=0) |  |  |  |
| Software | In case of no errors from the | B | LKA\_SAFETY\_A | N/A |
| Safety | software elements, the status of |  | CTIVATION |  |
| Requirement | the LKA feature shall be set to |  |  |  |
| 03-03 | activated (“activation\_status”=1) |  |  |  |
| Software | In case an error is detected by any | B | All | LKA\_Torq\_Req = 0 |
| Safety | of the software elements, it shall |  |  |  |
| Requirement | set the value of its corresponding |  |  |  |
| 03-04 | torque to 0 so that |  |  |  |
|  | “LKA\_Torq\_Req” is set to 0 |  |  |  |
| Software | Once the LKA functionality has | B | LKA\_SAFETY\_A | Activation\_status = 0 |
| Safety | been deactivated, it shall stay |  | CTIVATION | (LKA function |
| Requirement | deactivated till the time the ignition |  |  | deactivated) |
| 03-05 | is switched from off to on again. |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **A S I L** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| Technical | As soon as the LKA function | B | 500ms | LKA Safety | LKA torque |
| Safety | deactivates the LKA feature, the |  |  | Functionallity | output is set |
| Requireme  nt 04 | "LKA Safety" software block shall send a signal to the car display to turn a warning light. |  |  |  | to zero |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | **A S I L** | **Allocation Software Elements** | **Safe State** |
| Software | When the LKA function is | B | LKA\_SAFETY | N/A |
| Safety | deactivated (activation\_status |  | \_ACTIVATION |  |
| Requirement | set to 0), the activation\_status |  | , CarDisplay |  |
| 04-01 | shall be sent to the car |  | ECU |  |
|  | displayECU. |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **A S I L** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| Technical | Memory test shall be conducted | A | Ignition | Safety startup | LKA torque |
| Safety | at startup of the EPS ECU to |  | Cycle | memory test | output is set |
| Requireme  nt | check any faults in memory. |  |  |  | to zero |
| 05 |  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | **A S I L** | **Allocation Software Elements** | **Safe State** |
| Software | A CRC verification check over the | A | MEMORYTES | Activation\_status = 0 |
| Safety | software code in the Flash |  | T |  |
| Requirement | memory shall be done every time |  |  |  |
| 05-01 | the ignition is switched from off to  on to check for any corruption of content. |  |  |  |
| Software | Standard RAM tests to check the | A | MEMORYTES | Activation\_status = 0 |
| Safety | data bus, address bus and device |  | T |  |
| Requirement | integrity shall be done every time |  |  |  |
| 05-02 | the ignition is switched from off to |  |  |  |
|  | on (E.g.walking 1s test, RAM |  |  |  |
|  | pattern test. Refer RAM and |  |  |  |
|  | processor vendor |  |  |  |
|  | recommendations ) |  |  |  |
| Software | The test result of the RAM or | A | MEMORYTES | Activation\_status = 0 |
| Safety | Flash memory shall be indicated to |  | T |  |
| Requirement | the LDW\_Safety component via |  |  |  |
| 05-03 | the “test\_status” signal |  |  |  |
| Software | In case any fault is indicated via | A | MEMORYTES | Activation\_status = 0 |
| Safety | the “test\_status” signal the |  | T |  |
| Requirement | INPUT\_LKA\_PROCESSING shall |  |  |  |
| 05-04 | set an error on error\_status\_input |  |  |  |
|  | (=1) so that the LKA functionality |  |  |  |
|  | is deactivated and the LKA Torque |  |  |  |
|  | is set to 0 |  |  |  |