

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 |
| 5/23/2018 | 1.0 | Gireek Bansal | First Attempt |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# 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

This document focuses on software required for achieving safety goals derived from technical safety requirements. These requirements are more detail oriented than the technical safety concept requirements and specify variable names, signal paths and various protocols.

# 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 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 | LDW\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  02 | On failure detection by LDW it shall be deactivated and LDW\_torque\_request reset to zero. | C | 50 ms | LDW\_safety | LDW\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  03 | When the LDW has been deactivated ‘LDW safety’ shall send a signal to car display ECU to turn on warning for the driver. | C | 50 ms | LDW\_safety | LDW\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  04 | Memory tests shall be conducted at start of EPS ECU for checking memory faults. | A | Ignition cycle | Safety start up | LDW\_Torque\_Request is set to zero. |
| Technical  Safety  Requirement  05 | The integrity of data transmission for LDW\_Torque\_Request signal shall be ensured. | C | 50 ms | Data transmission integrity check | LDW\_Torque\_Request 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** | **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 | 50 ms | LDW\_safety | LDW\_Torque\_Request is set 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\_Req’ shall be generated at the end of the processing. | C | LDW\_SAGETY\_INPUT\_PROCESSING | N/A |
| Software Safety Requirement 01-02 | In case the ‘processed\_LDW\_Torq\_Req’ signal has a value greater than ‘Max\_Torque\_Amplitude\_LDW’ (maximum allowed safe torque), the torque signal ‘limited\_LDW\_Torq\_Req’ shall be set to zero, else ‘limited\_LDW\_Torq\_Req’ shall take the value of ‘processed\_LDW\_Torq\_Req’ | C | TORQUE\_LIMITER | ‘limited\_LDW\_Torq\_Req’ = 0 (Nm=Newton-meter) |
| 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 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 | The validity and integrity of the data transmission for LDW\_Torque\_Request signal shall be ensured | C | 50 ms | Data Transmission Integrity check | LDW\_Torque\_Request is set to zero |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | **ASIL** | **Allocation Software Elements** | **Safe State** |
| Software Safety Requirement 02-01 | Any data to be transmitted outside the LDQ Safety component (‘LDW Safety’) including ‘LDW\_Torque\_Req’ and ‘activation\_status’ shall be protected by an End-2-End protection mechanism. | C | E2C Calc | LDW\_Torq\_Req = 0 (Nm) |
| Software Safety Requirement 02-02 | The E2E protection protocol shall contain and attach the control data (alive counter (SQC) and CRC) to the data to be transmitted. | C | E2C Calc | LDW\_Torq\_Req = 0 (Nm) |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| 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 | 50 ms | LDW\_safety | LDW\_Torque\_Request is set to zero |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | **ASIL** | **Allocation Software Elements** | **Safe State** |
| Software Safety Requirement03-01 | Each Software element shall output a signal to indicate any error which is detected by the element. Error signal = error\_status\_input (LDW\_SAFETY\_INPUT\_PROCESSING), error\_status\_torque\_limiter(TORQUE\_LIMITER), error\_status\_output\_gen(LDW\_SAFETY\_OUTPUT\_GENERATOR) | C | All | N/A |
| Software Safety Requirement03-02 | A software element shall evaluate the error status of all other software elements and in case any one of them indicates an error, it shall deactivate the Lane Departure Warning feature (‘activation\_status’=0) | C | LDW\_SAFETY\_ACTIVATION | Lane Departure Warning function deactivated (‘activation\_status’ =0). |
| Software Safety Requirement03-03 | In case of a no error from the software elements, the status of the Lane Departure Warning feature shall be set to activated (‘activation\_status’=1). | C | LDW\_SAFETY\_ACTIVATION | N/A |
| Software Safety Requirement03-04 | In case an error is detected by any of the software elements, it shall set the value to its corresponding torque to zero so that ‘LDW\_Torq\_Req’ is set to zero | C | All | LDW\_Torq\_Req = 0 |
| Software Safety Requirement03-05 | Once the Lane Departure Warning functionality has been deactivated, it shall stay deactivating until the time the ignition is switched from off to on again. | C | LDW\_SAFETY\_ACTIVATION | Lane Departure Warning function deactivated (‘activation\_status’ =0). |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **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 | 50 ms | LDW Safety | Lane Departure Warning torque to zero. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | **ASIL** | **Allocation Software Elements** | **Safe State** |
| Software Safety Requirement 04-01 | When the Lane Departure Warning function is deactivated (‘activation\_status’ set to zero), the activation\_status shall be sent to the Car Display ECU. | C | LDW\_SAFETY\_ACTIVATION, Car Display ECU | N/A |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| 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 | Data Transmission Integrity Check | Lane Departure Warning torque to zero. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | **ASIL** | **Allocation Software Elements** | **Safe State** |
| Software Safety Requirement 01-01-05-01 | 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 content corruption. | A | MEMORYTEST | Activation\_status = 0 |
| Software Safety Requirement 01-01-05-02 | Standard RAM test to check the data bus, address bus and device integrity shall be done every time the ignition is switched from off to on (e. G. walking 1s test, RAM pattern test, Refer to RAM and processor vendor recommendations) | A | MEMORYTEST | Activation\_status = 0 |
| Software Safety Requirement 01-01-05-03 | 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 01-01-05-04 | In case any fault is indicated via the ‘test\_status’ signal the INPUT\_LDW\_PROCESSING shall set an error on the error\_status\_input(=1) so that the Lane Departure Warning functionality is deactivated and the LDW\_Torque\_Req is set to zero. | A | LDW\_SFETY\_INPUT\_PROCESSING | Activation\_status = 0 |

# Refined Architecture Diagram

****