

Software Safety Requirements and Architecture  
Lane Assistance

**Document Version: 1.0**

**Template Version 1.0, Released on 2017-06-21**



# Document history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 2018-06-04 | v0.9 | Csathó, Csaba | First draft |
| 2018-06-21 | v1.0 | Csathó, Csaba | Final version |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

Contents

[Document history 2](#_Toc517463942)

[Table of Contents 2](#_Toc517463943)

[Purpose 2](#_Toc517463944)

[Inputs to the Software Requirements and Architecture Document 3](#_Toc517463945)

[Technical safety requirements 3](#_Toc517463946)

[Refined Architecture Diagram from the Technical Safety Concept 4](#_Toc517463947)

[Software Requirements 5](#_Toc517463948)

[Refined Architecture Diagram 10](#_Toc517463949)

# Purpose

This document provides the detailed software safety requirements for the software components at a component level to identify potential complications on software design and architecture that may lead to a violation of safety goals. Specifications are provided for system state and signal paths, communication protocols and even naming conventions applied and to be used during the development of the software. The software modules architecture is refined based on the software safety requirements.

# Inputs to the Software Requirements and Architecture Document

## Technical safety requirements

Technical Safety Requirements related to Functional Safety Requirement **01-01** are …

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| T/S ID | Functional Safety Requirement | ASIL | F/Tol. Time Intv. | Safe State |
| **Requirement 01-01-01** | The *LDW safety component* shall ensure that the amplitude of the LDW\_Torque\_Request sent to the *Final Electronic Powersteering Torque Component* is below Max\_Torque\_Amplitude. | C | 50 ms | LDW torque is set to zero |
| **Requirement 01-01-02** | If and when the LDW is deactivated, the *LDW Safety Component* software module shall send a signal to the Car Display ECU to show a warning signal. | C | 50 ms | LDW torque is set to zero |
| **Requirement 01-01-03** | When 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 torque is set to zero |
| **Requirement 01-01-04** | The validity and integrity of the data transmission for LDW\_Torque\_Request signal shall be ensured. | C | 50 ms | LDW torque is set to zero |
| **Requirement 01-01-05** | Memory test shall be conducted at startup of the EPS ECU in order to rule out any faults in the memory module. | A | Ignition cycle timespan | LDW torque is set to zero |

## Refined Architecture Diagram from the Technical Safety Concept

*Refined System Architecture*

****

# Software Requirements

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| T/S ID | Functional Safety Requirement | ASIL | F/T T/I | Alloc. to Arch. | Safe State |
| **Requirement 01-01-01** | The *LDW safety component* shall ensure that the amplitude of the LDW\_Torque\_Request sent to the *Final Electronic Powersteering Torque Component* is below Max\_Torque\_Amplitude. | C | 50 ms | LDW Safety | LDW torque is set to zero |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| S/S ID | Software Safety Requirement | ASIL | Alloc. SW Elem. | Safe State |
| **Requirement 01-01-01-01** | 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 |
| **Requirement 01-01-01-02** | 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’ | C | TORQUE\_LIMITER | ‘limited\_LDW\_Torq\_Req’ = 0 (Nm=Newton-meter) |
| **Requirement 01-01-01-03** | 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) |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| T/S ID | Functional Safety Requirement | ASIL | F/T T/I | Alloc. to Arch. | Safe State |
| **Requirement 01-01-02** | If and when the LDW is deactivated, the *LDW Safety Component* software module shall send a signal to the Car Display ECU to show a warning signal. | C | 50 ms | LDW Safety | LDW torque is set to zero |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| S/S ID | Software Safety Requirement | ASIL | Alloc. SW Elem. | Safe State |
| **Requirement 01-01-02-01** | When the LDW function is deactivated (‘activation\_status’ set to 0), the activation\_status shall be sent to the Car Display ECU. | C | LDW\_SAFETY\_ACTIVATION, Car Display ECU | N/A |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| T/S ID | Functional Safety Requirement | ASIL | F/T T/I | Alloc. to Arch. | Safe State |
| **Requirement 01-01-03** | When 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 is set to zero |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| S/S ID | Software Safety Requirement | ASIL | Alloc. SW Elem. | Safe State |
| **Requirement 01-01-03-01** | 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 |
| **Requirement 01-01-03-02** | 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). |
| **Requirement 01-01-03-03** | 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 |
| **Requirement 01-01-03-04** | 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 0 | C | All | LDW\_Torq\_Req = 0 |
| **Requirement 01-01-03-05** | 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). |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| T/S ID | Functional Safety Requirement | ASIL | F/T T/I | Alloc. to Arch. | Safe State |
| **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 | LDW torque is set to zero |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| S/S ID | Software Safety Requirement | ASIL | Alloc. SW Elem. | Safe State |
| **Requirement 01-01-04-01** | 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) |
| **Requirement 01-01-04-02** | 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) |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| T/S ID | Functional Safety Requirement | ASIL | F/T T/I | Alloc. to Arch. | Safe State |
| **Requirement 01-01-05** | Memory test shall be conducted at startup of the EPS ECU in order to rule out any faults in the memory module. | A | Ignition cycle timespan | Data Transmission Integrity Check | LDW torque is set to zero |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| S/S ID | Software Safety Requirement | ASIL | Alloc. SW Elem. | Safe State |
| **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 |
| **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 |
| **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 |
| **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

*Refined System Architecture Diagram*

