

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 |
| 10/28/2018 | v-1.0 | Yan Cui | First draft. |
| 11/01/2018 | v-1.1 | Yan Cui | Revision for submission |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# 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 includes new requirements for software components at component level, to identify potential problems on software design and architecture. These requirements are more detailled than technical safety concept requirement.

# 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  01-01-01 | The Lane Departure Warning safety component needs to ensure the amplitude of the LDW torque request being sent to Electronic Power Steering torque is below Max\_Torque\_Amplitude. | C | 50ms | LDW Safety | LDW torque at zero |
| Technical  Safety  Requirement  01-01-02 | When the Lane Departure Warning is deactivated, the LDW Safety module must send a signal message to Car Display ECU indicating the warning. | C | 50ms | LDW Safety | LDW torque at zero |
| Technical  Safety  Requirement  01-01-03 | When failure of Lane Departure Warning function is detected, it must deactivate the LDW feature and reset torque request to zero. | C | 50ms | LDW Safety | LDW torque at zero |
| Technical  Safety  Requirement  01-01-04 | The validity and integrity of data transmission of LDW torque request needs to be ensured. | C | 50ms | Data transmission integrity check | LDW torque at zero |
| Technical  Safety  Requirement  01-01-05 | Memory test needs to be conducted at starting of EPS ECU to check any memory issue. | A | Ignition cycle | Safety startup - Memory test | LDW torque at 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 | 50ms | LDW Safety | Lane Departure Warning torque at zero |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Software Safety Requirement | ASIL | Allocation Software Elements | Safe State |
| Software  Safety  Requirement  01-01 | The input signal, Primary\_LDW\_Torque\_Request must be read and processed to determing the torque request from the Normal Lane Assistance Functionality. | C | LDW\_SAFETY\_INPUT\_PROCESSING | N/A |
| Software Safety Requirement 01-02 | If the processed LDW\_Torque\_Request is greater than Max\_Torque\_Amplitude\_LDW, the signal limited\_LDW\_Torque\_Request must be reset to zero. Otherwise, limited\_LDW\_Torque\_Request takes value of processed LDW\_Torque\_Request. | C | TORQUE\_LIMITER | Limited\_LDW\_Torque\_Request set to zero |
| Software Safety Requirement 01-03 | The limited\_LDW\_Torque\_Request must be transformed to LDW\_Torque\_Request, which must be then transmitted out of LDW Safety Component to Final Torque EPS. | C | LDW\_SAFETY\_OUTPUT\_GENERATOR | LDW\_Torq\_Request set to zero |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **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 | 50ms | LDW Safety | Lane Departure Warning torque at zero |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | **ASIL** | **Allocation Software Elements** | **Safe State** |
| Software Safety Requirement 02-01 | Data transmitted out, LDW\_Torque\_Request and Activation\_status must be protected by an End-2-End protection mechanism | C | E2C Calc | LDW\_Torque\_Request at zero |
| Software Safety Requirement 02-02 | The End-2-End protection protocol must contain and attach the control data (SQC, CRC) to data that being transmitted | C | E2E Calc | LDW\_Torque\_Request at zero |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **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 | 50ms | LDW Safety | Lane Departure Warning torque at zero |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | **ASIL** | **Allocation Software Elements** | **Safe State** |
| Software Safety Requirement03-01 | Each software element must output a signal to indicate corresponding error | C | ALL | N/A |
| Software Safety Requirement03-02 | A software element shall evaluate the error status from other elements. If any of them shows error, this element shall deactivate the Lane Departure Warning, reset activation\_status to zero | C | LDW\_SAFETY\_ACTIVATION | Activation\_status = 0 |
| Software Safety Requirement03-03 | While no error from software elements, the Lane Departure Warning function shall be activated, activation\_status to 1 | C | LDW\_SAFETY\_ACTIVATION | N/A |
| Software Safety Requirement03-04 | If any error is detected by software elements, this shall reset the LDW\_Torque\_Request to zero | C | ALL | LDW\_Torque\_Request = 0 |
| Software Safety Requirement03-05 | Once the Lane Departure Warning functionality is deactivated, it shall remain at that status until the next ignition switched on | C | LDW\_SAFETY\_ACTIVATION | 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 | 50ms | LDW Safety | Lane Departure Warning torque at zero |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | **ASIL** | **Allocation Software Elements** | **Safe State** |
| Software Safety Requirement 04-01 | When the Lane Departure Warning is deactivated the activation\_status shall be sent to 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 at zero |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | **ASIL** | **Allocation Software Elements** | **Safe State** |
| Software Safety Requirement 05-01 | CRC checksum over the software in Flash memory must be done everytime ignition is switched on | A | MEMORYTEST | Activation\_status = 0 |
| Software Safety Requirement 05-02 | Standard RAM test to check the data bus, address bus and device integrity must be done everytime ignition is switched on | A | MEMORYTEST | Activation\_status = 0 |
| Software Safety Requirement 05-03 | The test result of RAM or Flash memory shall be indicated to LDW\_Safety component through test\_status signal | A | MEMORYTEST | Activation\_status = 0 |
| Software Safety Requirement 05-04 | If any error is indicated through test\_status signal, the INPUT\_LDW\_PROCESSING shall raise error flag and set error\_status\_input = 1, and consequently, LDW\_Torque\_Request reset to zero | A | LDW\_SAFETY\_INPUT\_PROCESSING | Activation\_status = 0 |

# 

# Refined Architecture Diagram

