

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 |
| 10/15/2018 | 1.0 | John O’Shea | Initial Draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# 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 document is to document detailed software safety requirements using the technical safety requirments.

# 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 component shall ensure that the LDW\_Torque\_Request for lane departure warning is below Max\_Torque\_Amplitude. | C | 50 ms | LDW Safety | The LDW torque amplitude is set to 0. |
| Technical  Safety  Requirement  02 | When the LDW feature is deactivated, the LDW software component shall block any requests to activate a warning light to the car display ECU | C | 50 ms | LDW Safety | The LDW torque amplitude is set to 0. |
| Technical  Safety  Requirement  03 | Once a failure is detected the LDW feature is deactivated and a torque request shall not be sent. | C | 50 ms | LDW Safety | The LDW torque amplitude is set to 0. |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for LDW\_Torque\_Request shall be checked | C | 50 ms | Data Transmission Integrity check | The LDW torque amplitude is set to 0. |
| Technical  Safety  Requirement  05 | A memory test shall be conducted during the start up of the EPS ECU to check for any faults in memory. | A | Ignition Cycle | Memory Test | The LDW torque amplitude is set to 0. |

## 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 component shall ensure that the LDW\_Torque\_Request for lane departure warning is below Max\_Torque\_Amplitude. | C | 50 ms | LDW Safety | The LDW torque amplitude is set to 0. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Software Safety Requirement | ASIL | Allocation Software Elements | Safe State |
| Software  Safety  Requirement  01-01 | The input signal ‘Primary\_LDW\_Torque\_Request’ shall be read and pre-processed to determine the torque request coming from the ‘Basic/Main LANE Assistance Funtionality’ SW component. The signal ‘Processed\_LDW\_Torque\_Request’ shall be generated at the end of processing. | C | LDW\_SAFETY\_INPUT\_PROCESSING | N/A |
| Software Safety Requirement 01-02 | If ‘Processed\_LDW\_Torque\_Request’ has a value greater than ‘Max\_Torque\_Amplitude\_LDW’ , the torque signal ‘Limited\_LDW\_Torque\_Request’ shall be set to zero, else  ‘Limited\_LDW\_Torque\_Request’ shall take the value of the ‘Processed\_LDW\_Torque\_Request’ | C | TORQUE\_LIMITER | limited\_LDW\_Torque\_Request = 0 |
| Software Safety Requirement 01-03 | The ‘Limited\_LDW\_Torque\_Request’ shall be transformed into a signal ‘LDW\_Torque\_Request’ 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 torque amplitude set to 0 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| Technical  Safety  Requirement  02 | When the LDW feature is deactivated, the LDW software component shall block any requests to activate a warning light to the car display ECU | C | 50 ms | LDW Safety  Data Transmission Integrity check | The LDW torque amplitude is set to 0. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | **ASIL** | **Allocation Software Elements** | **Safe State** |
| Software Safety Requirement 02-01 | When the LDW function is deactivated (activation\_status=0), and further requests shall first check activation\_status before sending requests | C | All SW Elements | The LDW torque amplitude is set to 0. |
| Software Safety Requirement 02-02 | When the LDW function is deactivated (activation\_status=0), the activation\_status shall be sent to the Car Display ECU to enable the Car Display warning light | C | Car Display ECU, Car Display | activation\_status=0 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| Technical  Safety  Requirement  03 | Once a failure is detected the LDW feature is deactivated and a torque request shall not be sent. | C | 50 ms | LDW Safety | The LDW torque amplitude is set to 0. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | **ASIL** | **Allocation Software Elements** | **Safe State** |
| Software Safety Requirement03-01 | Each SW element detecting an error shall assert its error signal to indicate an error was detected. | C | All SW elements with error outputs | N/A |
| Software Safety Requirement03-02 | Each SW element shall check for errors asserted by other elements and if an error is detected it shall deactivate the LDW feature. (activation\_status=0) | C | LDW\_SAFETY\_ACTIVATION | N/A |
| Software Safety Requirement03-03 | Each SW element shall check for errors asserted by other elements and if an error is not detected it shall assert keep LDW feature activated. (activation\_status=1) | C | LDW\_SAFETY\_ACTIVATION | N/A |
| Software Safety Requirement03-04 | If an error is detected by any SW element the LDW\_Torque\_Request shall be set to 0 | C | All SW elements with error outputs | LDW\_Torque\_Request = 0 |
| Software Safety Requirement03-05 | If the LDW is deactivated, it shall stay deactivated until the vehicle is shut off and restarted | 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 | The validity and integrity of the data transmission for LDW\_Torque\_Request shall be checked | C | 50 ms | Data Transmission Integrity check | The LDW torque amplitude is set to 0. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | **ASIL** | **Allocation Software Elements** | **Safe State** |
| Software Safety Requirement 04-01 | All data transmitted outside of “LDW Safety” shall be protected with End2End(E2E) protection.  The E2E shall be activated for header/payload portions of each data packet | C | E2E Calculation | LDW\_Torque\_Request is set to 0 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| Technical  Safety  Requirement  05 | A memory test shall be conducted during the start up of the EPS ECU to check for any faults in memory. | A | Ignition Cycle | Memory Test | The LDW torque amplitude is set to 0. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | **ASIL** | **Allocation Software Elements** | **Safe State** |
| Software Safety Requirement 05-01 | A BIST memory test shall be run to test data and address busses using various patterns to validate the integtrity of the memory system | A | MEMORY\_TEST | activation\_status=0 |
| Software Safety Requirement 05-02 | A CRC shall be computed for SW requests packets between ECUs | A | MEMORY\_TEST | activation\_status=0 |
| Software Safety Requirement 05-03 | Any error detected by the MEMORY\_TEST shall be propogated to the LDW\_Safety\_ component | A | MEMORY\_TEST | activation\_status=0 |
| Software Safety Requirement 05-04 | Any error detected by the MEMORY\_TEST shall cause the LDW\_Safety\_Activation component to set activation\_status=0 | A | LDW\_SAFETY\_ACTIVATION | activation\_status=0 |

# 

# Refined Architecture Diagram

**[**