

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 |
| 9/23/2017 | 1.0 | Martin Pfeifle | First version of SW Requirements and Architecture document |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

Contents

[Document history 2](#_Toc494214977)

[Table of Contents 2](#_Toc494214978)

[Purpose 2](#_Toc494214979)

[Inputs to the Software Requirements and Architecture Document 3](#_Toc494214980)

[Technical safety requirements 3](#_Toc494214981)

[Refined Architecture Diagram from the Technical Safety Concept 4](#_Toc494214982)

[Software Requirements 4](#_Toc494214983)

[Refined Architecture Diagram 11](#_Toc494214984)

# Purpose

The purpose of the software requirements and architecture document is to develop requirements and metrics against which the item can be verified, that will ensure its functional safety.

# 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 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 = 0 |
| Technical  Safety  Requirement  02 | 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 | Electronic Power Steering ECU - LDW Safety Functionality | LDW\_Torque\_Request = 0 |
| 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 | Electronic Power Steering ECU - LDW Safety Functionality | LDW\_Torque\_Request = 0 |
| Technical  Safety  Requirement  04 | The validity and integrity of the data transmission for 'LDW\_Torque\_Request' signal shall be ensured. | C | 50ms | Electronic Power Steering ECU – Data transmission integrity check | LDW\_Torque\_Request = 0 |
| 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 | Electronic Power Steering ECU – Safety Startup | LDW\_Torque\_Request = 0 |

## Refined Architecture Diagram from the Technical Safety Concept

# Macintosh HD:Users:Jimmy:Documents:Udacity:CarND-Functional-Safety-Project:Architecture_Diagrams:graphic_asset_4.pngSoftware 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 | Electronic Power Steering ECU - LDW Safety Functionality | LDW\_Torque\_Request = 0 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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\_SAFETY\_INPUT\_PROCESSING | N/A |
| Software Safety Requirement 01-02 | In case the “processed\_LDW\_Torq\_Req” signal has a value greater than“Max\_Torque\_Ampltide\_LDW”(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”. | 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” whichis suitable to be transmittedoutside of the LDW Safetycomponent (“LDW Safety”) to the “Final EPS Torque”component. Also see SofSafReq02-01 andSofSafReq02-02 | 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 |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | **ASIL** | **Allocation Software Elements** | **Safe State** |
| SoftwareSafetyRequirement02-01 | Any data to be transmittedoutside of the LDW Safetycomponent (“LDW Safety”)including "LDW\_Torque\_Req"and “activation\_status” (seeSofSafReq03-02) shall beprotected by an End2End(E2E)protection mechanism | C | E2ECalc | LDW\_Torq\_Req= 0 (Nm) |
| SoftwareSafetyRequirement02-02 | The E2E protection protocol shall contain and attach the control data: alive counter (SQC) and CRC to the data to be transmitted. | C | E2ECalc | LDW\_Torq\_Req= 0 (Nm) |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| TechnicalSafetyRequirement03 | 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 output is set to zero |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | **ASIL** | **Allocation Software Elements** | **Safe State** |
| SoftwareSafetyRequirement03-01 | Each of the SW elements shal loutput 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 |
| SoftwareSafetyRequirement03-02 | A software element shall evaluate the error status of all the other software elements and in case any 1 of them indicates an error, it shall deactivate theLDW feature(“activation\_status”=0) | C | LDW\_SAFETY\_ACTIVATION | Activation\_status = 0 (LDW function deactivated) |
| SoftwareSafetyRequirement03-03 | In case of no errors from the software elements, the status of the LDW feature shall be set to activated (“activation\_status”=1) | C | LDW\_SAFETY\_ACTIVATION | N/A |
| SoftwareSafetyRequirement03-04 | In case an error is detected by any of the software elements, it shall set the value of its corresponding torque to 0 so that “LDW\_Torq\_Req” is set to 0 | C | All | LDW\_Torq\_Req = 0 |
| SoftwareSafetyRequirement03-05 | Once the LDW functionality has been deactivated, it shall stay deactivated till the time the ignition is switched from off to on again. | C | LDW\_SAFETY\_ACTIVATION | Activation\_status = 0 (LDW function deactivated) |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| TechnicalSafetyRequirement04 | 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 | LDW torque output is set to zero |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | **ASIL** | **Allocation Software Elements** | **Safe State** |
| SoftwareSafetyRequirement04-01 | When the LDW function is deactivated (activation\_status set to 0), the activation\_status shall be sent to the car displayECU. | C | LDW\_SAFETY\_ACTIVATION, CarDisplay ECU | N/A |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| TechnicalSafetyRequirement05 | Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory | A | 50 ms | Ignition Cycle | LDW torque output is set to zero |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | **ASIL** | **Allocation Software Elements** | **Safe State** |
| SoftwareSafetyRequirement05-01 | 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 corruption of content. | A | MEMORYTEST | Activation\_status = 0 |
| SoftwareSafetyRequirement05-02 | Standard RAM tests 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 RAM and processor vendor recommendations ) | A | MEMORYTEST | Activation\_status = 0 |
| SoftwareSafetyRequirement05-03 | 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 |
| SoftwareSafetyRequirement05-04 | In case any fault is indicated via the “test\_status” signal the INPUT\_LDW\_PROCESSING shall set an error on error\_status\_input (=1) so that the LDW functionality is deactivated and the LDWTorque is set to 0 | A | LDW\_SAFETY\_INPUT\_PROCESSING | Activation\_status = 0 |

# 

# Refined Architecture Diagram

