

Software Safety Requirements and Architecture

Lane Assistance

**Document Version: [Version]**

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



# Document history

**[Instructions: Fill in the date, version and description fields. You can fill out the Editor field with your name if you want to do so. Keep track of your editing as if this were a real world project.**

**For example, if this were your first draft or first submission, you might say version 1.0. If this is a second submission attempt, then you'd add a second line with a new date and version 2.0]**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 21/06/2018 | 1 | Xue Fei | Home Work |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# Table of Contents

**[Instructions: We have provided a table of contents. If the table of contents is not showing up correctly in your word processor of choice, please update it. The table of contents should show each section of the document and page numbers or links. Most word processors can do this for you. In** [**Google Docs**](https://support.google.com/docs/answer/116338?co=GENIE.Platform%3DDesktop&hl=en)**, you can use headings for each section and then go to Insert > Table of Contents.** [**Microsoft Word**](https://support.microsoft.com/en-us/help/285059/how-to-create-a-table-of-contents-by-marking-text-in-word) **has similar capabilities]**

[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

**[Instructions: Answer what is the purpose of this document?]**

**The purpose of the Software Requirements and Architecture Document is to identify and verify software requirements and metrics for Lane Assistance item**

# Inputs to the Software Requirements and Architecture Document

**[Instructions:**

**REQUIRED:**

**You are only required to develop this document for the LDW (lane departure warning) amplitude malfunction. So here, provide the technical safety requirements for the LDW amplitude malfunction as well as the refined system architecture diagram from the technical safety concept.**

**OPTIONAL:**

**Expand this document to include software safety requirements for the LDW frequency malfunction as well. Go even further and document software safety requirements for the Lane Keeping Assistance (LKA) function as well.**

**]**

## Technical safety requirements

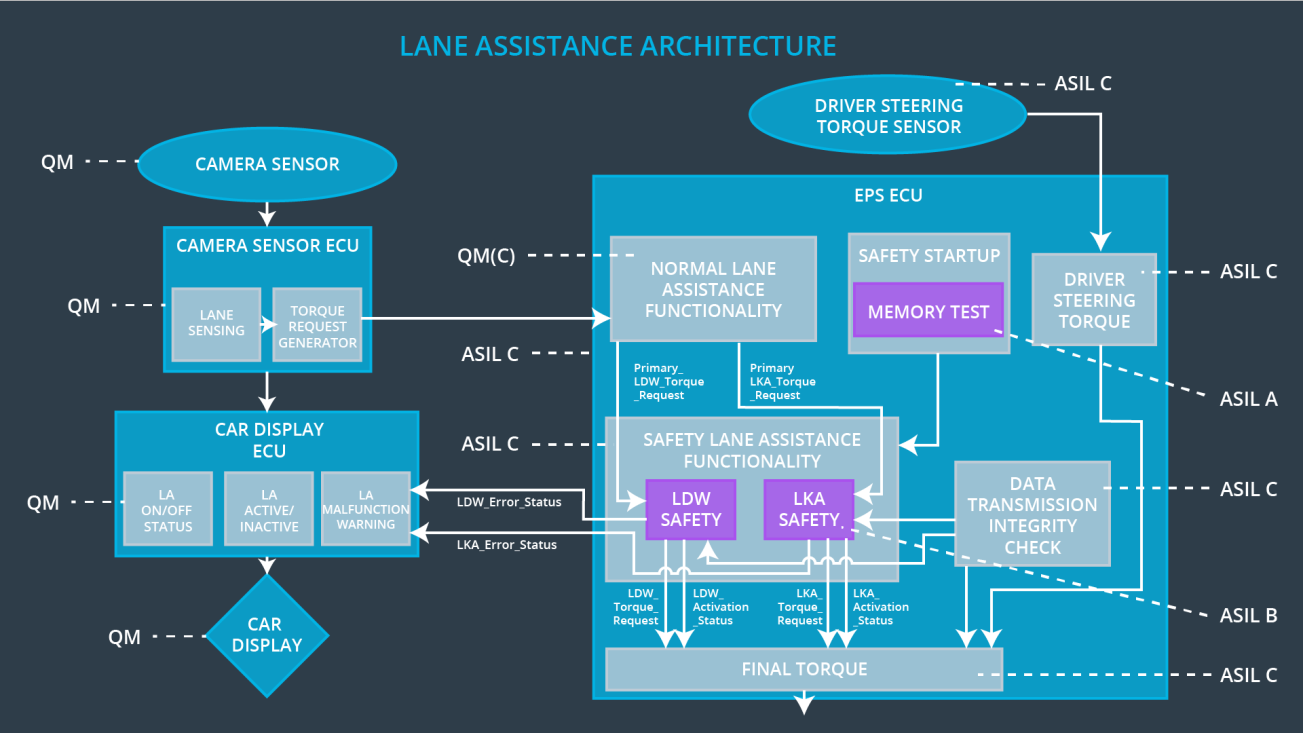
Technical Safety Requirements related to Functional Safety Requirement 01-01 are:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Architecture Allocation** | **Safe State** |
| Technical  Safety  Requirement  01 | The LDW safety component  shall make sure that the  amplitude of the  LDW\_Torque\_Request is less than Max\_Torque\_Amplitude | C | 50 ms | LDW Safety | LDW torque  output is set  to 0. |
| Technical  Safety  Requirement  02 | As soon as the LDW function  turns off the LDW feature,  the LDW Safety software  block shall notify the car display ECU to turn  on a warning light. | C | 50 ms | LDW Safety | LDW torque  output is set  to 0. |
| Technical  Safety  Requirement  03 | As soon as a failure is  detected by the LDW  function, it shall turn off  the LDW feature and the  LDW\_Torque\_Request shall  be set to 0. | C | 50 ms | LDW Safety | LDW torque  output is set  to 0. |
| Technical  Safety  Requirement  04 | The errors of the data transmission for  LDW\_Torque\_Request  signal shall be detected | C | 50 ms | LDW Safety | LDW torque  output is set  to 0. |
| Technical  Safety  Requirement  05 | Memory test shall be  conducted at the beginning of the EPS ECU to check for any faults in memory. | A | Ignition  cycle | Memory Test | LDW torque  output is set  to 0. |

## Refined Architecture Diagram from the Technical Safety Concept

**[Instructions:**

**REQUIRED: Provide the refined system architecture diagram from the technical safety concept**

**]**

# Software Requirements

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

**[Instructions: Fill in the software safety requirements for the LDW amplitude malfunction technical safety requirements. We have provided the associated technical safety requirements. Hint: The software safety requirements were discussed in the text from the software and hardware lesson.**

**OPTIONAL:**

**CHALLENGE ONE**

**Develop software safety requirements for the Lane Departure Warning (LDW) frequency function and modify the system architecture as needed.**

**CHALLENGE TWO**

**Develop software safety requirements for the Lane Keeping Assistance (LKA) function and modify the system architecture as needed.**

**]**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Technical Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Allocation to Architecture** | **Safe State** |
| Technical  Safety  Requirement  01 | The LDW safety component shall make sure that the amplitude of the LDW\_Torque\_Request is less than Max\_Torque\_Amplitude | C | 50 ms | LDW Safety | The torque  output from LDW is set  to 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\_P  ROCESSING | 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 0, else  “limited\_LDW\_Torq\_Req” shall  take the value of  “processed\_LDW\_Torq\_Req” | C | TORQUE\_LIMITER | “limited\_LDW\_T  orq\_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 of the LDW Safety  component (“LDW Safety”) to  the “Final EPS  Torque”component. Also see  SofSafReq02-01 and  SofSafReq02-02 | 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 | C | 50 ms | Data Transmission Intergrity Check | N.A. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | **ASIL** | **Allocation Software Elements** | **Safe State** |
| Software Safety Requirement 02-01 | Any data to be transmitted  outside of the LDW Safety  component (“LDW  Safety”)including  "LDW\_Torque\_Req"and  “activation\_status” (seeSofSafR  eq03-02) shall be protected by  an End2End(E2E)protection  mechanism | C | E2ECalc | LDW\_Torq\_Re  q = 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. |  | E2ECalc | LDW\_Torq\_Re  q = 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 | 50ms | LDW Safety | Off |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | **ASIL** | **Allocation Software Elements** | **Safe State** |
| Software Safety Requirement03-01 | Each of the SW elements shall  output a signal to indicate any  error which is detected by the  element. Error signal =  error\_status\_input(LDW\_SAFET  Y\_I NPUT\_PROCESSING),  error\_status\_torque\_limiter(TOR  QU E\_LIMITER),  error\_status\_output\_gen(LDW\_  SAF  ETY\_OUTPUT\_GENERATOR | C | All | N/A |
| Software Safety Requirement03-02 | A software element shall  evaluate the error status of all  \_A CTIVATION  the other software elements and  in case any 1 of them indicates  an error, it shall deactivate the  LDW  feature(“activation\_status”=0) | C | LDW\_SAFETY\_ACTIVATION | Activation\_status = 0  (LDW function  deactivated) |
| Software Safety Requirement03-03 | In case of no errors from the  software elements, the status of  \_A CTIVATION  the LDW 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 of its  corresponding torque to 0 so  that “LDW\_Torq\_Req” is set to 0 | C | All | LDW\_Torq\_Req = 0 |
| Software Safety Requirement03-05 | Once the LDW functionality has  been deactivated, it shall stay  deactivated until the time the  ignition is switched from off to  on again. | C | LDW\_SAFETY  \_A CTIVATION | Activation\_status = 0  (LDW function  deactivated) |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **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  Functionality | Off |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | **ASIL** | **Allocation Software Elements** | **Safe State** |
| Software Safety Requirement 04-01 | When the LDW function is  deactivated (activation\_status  set to 0), the activation\_status  shall be sent to the car display  ECU. | C | LDW\_SAFET  Y\_  ACTIVATION,  CarDisplay  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 | Memory test | Off |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Software Safety Requirement** | **ASIL** | **Allocation Software Elements** | **Safe State** |
| Software Safety Requirement 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 corruption of content. | A | MEMORY  TEST | activation\_status = 0 |
| Software Safety Requirement 05-02 | 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 | MEMORY  TEST | activation\_status = 0 |
| Software Safety Requirement 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 | MEMORY  TEST | activation\_status = 0 |
| Software Safety Requirement 05-04 | In case any fault is indicated via  the test\_status signal theINPUT\_LDW\_PROCESSING shall set an error on error\_status\_input (= 1) so that the LDW functionality is deactivated and the LDW torque  is set to 0. | A | MEMORY  TEST | activation\_status = 0 |

# 

# Refined Architecture Diagram

**[Instructions: Include the refined system architecture. Hint: The refined system architecture should include the system architecture from the end of the software and hardware lesson, including all of the ASIL labels.]**

