# Technical Safety Concept Lane Assistance

**Document Version:** [Version]1.0

**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 |
|---|---|---|---|
| 06/08/2018 | 1.0 | Efraim Kropp | Initial version |
| | | | |
| | | | |
| | | | |
| | | | |

# 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, you can use headings for each section and then go to Insert > Table of Contents. Microsoft Word has similar capabilities]**

# 1. Purpose of the Technical Safety Concept

**[Instructions: Answer what is the purpose of a technical safety concept?]**
The purpose of the Technical Safety Concept is to turn functional safety requirements into technical safety requirements and to allocate the technical safety requirements to the system architecture

# 2. Inputs to the Technical Safety Concept

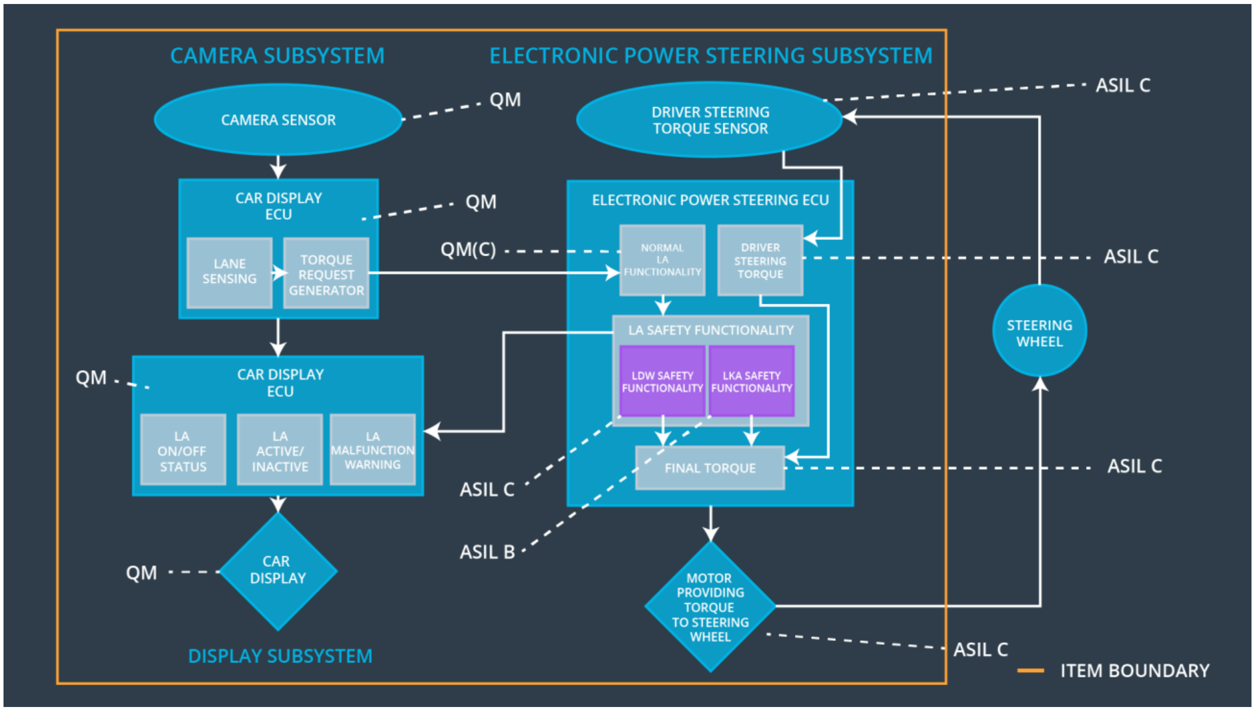
## 2.1. Functional Safety Requirements

**[Instructions: Provide the functional safety requirements derived in the functional safety concept ]**

| ID | Functional Safety Requirement | ASIL | Fault Tolerant Time Interval | Safe State |
|---|---|---|---|---|
| Functional Safety Requirement 01-01 | The Electronic Power Steering ECU shall ensure that Lane Departure Warning (LDW) oscillating torque amplitude is below Max_Torque_Amplitude | C | 50 ms | The LDW oscillating torque amplitude is set to 0 |
| Functional Safety Requirement 01-02 | The Electronic Power Steering ECU shall ensure that LDW oscillating torque amplitude is below Max_Torque_ Frequency | C | 50 ms | The LDW oscillating torque frequency is set to 0 |
| Functional Safety Requirement 02-01 | The Electronic Power Steering ECU shall ensure that the Lane Keeping Assistance (LKA) torque is applied for only Max_Duration | B | 500 ms | The LKA torque is set to 0 |

## 2.2. Refined System Architecture from Functional Safety Concept

**[Instructions: Provide the refined system architecture from the functional safety concept]**



### 2.2.1. Functional overview of architecture elements

**[Instructions: Provide a description for each functional safety element; what is each element's purpose in the lane assistance item?]**

| **Element** | **Description** |
|---|---|
| Camera Sensor | The Camera Sensor provides road images to the Camera Sensor ECU |
| Camera Sensor ECU - Lane Sensing | The Camera Sensor ECU detects when the vehicle accidentally departures its Lane |
| Camera Sensor ECU - Torque request generator | The Camera Sensor ECU generates Torque request to the Electronic Power Steering ECU |
| Car Display | The Car Display displays Lane Assistance warning and status lights on the dashboard |
| Car Display ECU - Lane Assistance On/Off Status | The Car Display ECU controls Lane Assistance On/Off Status signal to the Car Display |

| | |
|---|---|
| Car Display ECU - Lane Assistant Active/Inactive | The Car Display ECU controls Lane Assistance Active/Inactive signal to the Car Display |
| Car Display ECU - Lane Assistance malfunction warning | The Car Display ECU activates Lane Assistance malfunction warning signal on the Car Display |
| Driver Steering Torque Sensor | The Driver Steering Torque Sensor measures the torque provided by the driver |
| Electronic Power Steering (EPS) ECU - Driver Steering Torque | EPS ECU receives driver steering torque and provides to the Final Torque component |
| EPS ECU - Normal Lane Assistance Functionality | EPS ECU calculates an additional amount of steering torque for the motor |
| EPS ECU - Lane Departure Warning Safety Functionality | EPS ECU ensures that the amplitude of the “LDW_Torque_Request” is below “Max_Torque_Amplitude” value and the frequency of the “LDW_Torque_Request” is below “Max_Torque_Frequency” |
| EPS ECU - Lane Keeping Assistant Safety Functionality | EPS ECU ensures that duration of the “LKA_Torque_Request” is below “Max_Duration” value |
| EPS ECU - Final Torque | EPS_ECU provides “Final_Torque_Request” to the Motor |
| Motor | The Motor provides the final torque to the Steering Wheel |

# 3. Technical Safety Concept

## 3.1. Technical Safety Requirements

**[Instructions: Fill in the technical safety requirements for the lane departure warning first functional safety requirement. We have provided the associated functional safety requirement in the first table below. Hint: The technical safety requirements were discussed in the lesson videos. The architecture allocation column should contain element names such as LDW Safety block, Data Transmission Integrity Check, etc. Allocating the technical safety requirements to the "EPS ECU" does not provide enough detail for a technical safety concept.]**

### 3.1.1. Lane Departure Warning (LDW) Requirements:

Functional Safety Requirement 01-01 with its associated system elements
(derived in the functional safety concept)

| ID | Functional Safety Requirement | Electronic Power Steering ECU | Camera ECU | Car Display ECU |
|---|---|---|---|---|
| Functional Safety Requirement 01-01 | The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude | X | | |

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 LWD Safety component shall ensure that amplitude of the “LDW_Torque_Request” sent to the “Final Torque” component is below “Max_Torque_Amplitude” | C | 50 ms | EPS ECU | Deactivate the LDW feature and set LDW oscillating torque amplitude to 0 |
| Technical Safety Requirem | The LDW Safety block shall perform Data Transmission Integrity Check of the LDW | C | 50 ms | EPS ECU | Deactivate the LDW feature and |

| | | | | | |
|---|---|---|---|---|---|
| ent 02 | torque amplitude signal of the “LDW_Torque_Request” | | | | set LDW oscillating torque amplitude to 0 |
| Technical Safety Requirement 03 | If amplitude of the “LDW_Torque_Request” is above “Max_Torque_Amplitude” value, the LDW Safety block shall set “LDW_Activation_Status” signal to “Inactive” | C | 50 ms | EPS ECU | Deactivate the LDW feature and set LDW oscillating torque amplitude to 0 |
| Technical Safety Requirement 04 | As soon and “LDW_Activation_Status signal is set to “Inactive”, LDW Safety block shall provide “LDW_Error_Status” signal to the LA Malfunction Warning block of the Car Display ECU | C | 50 ms | EPS ECU | Deactivate the LDW feature and set LDW oscillating torque amplitude to 0 |
| Technical Safety Requirement 05 | Memory test shall be conducted at startup (power on reset/wakeup, ignition transition to Run) of the EPS ECU to check for any faults in memory partition associated with LDW function | A | “Max_Startup_Time” | EPS ECU | Disable the LDW feature and set LDW oscillating torque amplitude to 0 |

**[Instructions: Fill in the technical safety requirements for the lane departure warning second functional safety requirement. We have provided the associated functional safety requirement in the table below. Hint:. Most of the technical safety requirements will be the same. At least one technical safety requirement will have to be slightly modified because we are talking about frequency instead of amplitude. These requirements were not given in the lessons]**

Functional Safety Requirement 01-2 with its associated system elements
(derived in the functional safety concept)

| ID | Functional Safety Requirement | Electronic Power Steering ECU | Camera ECU | Car Display ECU |
|---|---|---|---|---|
| Functional Safety Requirement 01-02 | The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency | X | | |

Technical Safety Requirements related to Functional Safety Requirement 01-02 are:

| ID | Technical Safety Requirement | ASIL | Fault Tolerant Time Interval | Architecture Allocation | Safe State |
|---|---|---|---|---|---|
| Technical Safety Requirement 01 | The LWD Safety component shall ensure that frequency of the “LDW_Torque_Request” sent to the “Final Torque” component is below “Max_Torque_Frequency” | C | 50 ms | EPS ECU | Deactivate the LDW feature and set LDW oscillating torque frequency to 0 |
| Technical Safety Requirement 02 | The LDW Safety block shall perform Data Transmission Integrity Check of the LDW torque frequency signal of the “LDW_Torque_Request” | C | 50 ms | EPS ECU | Deactivate the LDW feature and set LDW oscillating torque frequency to 0 |
| Technical Safety Requirement 03 | If frequency of the “LDW_Torque_Request” is above “Max_Torque_Frequency” value, the LDW Safety block shall set | C | 50 ms | EPS ECU | Deactivate the LDW feature and set LDW |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
|  | “LDW_Activation_Status” signal to “Inactive” |  |  |  | oscillating torque frequency to 0 |
| Technical Safety Requirement 04 | As soon and “LDW_Activation_Status signal is set to “Inactive”, LDW Safety block shall provide “LDW_Error_Status” signal to the LA Malfunction Warning block of the Car Display ECU | C | 50 ms | EPS ECU | Deactivate the LDW feature and set LDW oscillating torque frequency to 0 |
| Technical Safety Requirement 05 | Memory test shall be conducted at startup (power on reset/wakeup, Ignition transition to Run) of the EPS ECU to check for any faults in memory partition associated with LDW function | A | “Max_Startup_Time” | EPS ECU | Disable the LDW feature and set LDW oscillating torque frequency to 0 |

### Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria:

**[OPTIONAL: For each technical safety requirement, identify both the verification and validation acceptance criteria. “Validation” asks whether or not you chose the appropriate parameters. “Verification” involves testing to make sure the vehicle behaves as expected when the parameter value is crossed. There is not necessarily one right answer. Look at your verification and validation acceptance criteria from the functional safety concept for inspiration.]**

### 3.1.2. Lane Keeping Assistance (LKA) Requirements:

**[Instructions: Fill in the technical safety requirements for the lane keeping assistance functional safety requirement 02-01. We have provided the associated functional safety requirement in the table below. Hint:. You can reuse the technical safety requirements from functional safety requirement 01-01. But you need to change the language because we are now looking at a different system. The ASIL and Fault Tolerant Time Interval are different as well.]**

Functional Safety Requirement 02-1 with its associated system elements
(derived in the functional safety concept)

| ID | Functional Safety Requirement | Electronic Power Steering ECU | Camera ECU | Car Display ECU |
|---|---|---|---|---|
| Functional Safety Requirement 02-01 | The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration | X | | |

Technical Safety Requirements related to Functional Safety Requirement 02-01 are:

| ID | Technical Safety Requirement | ASIL | Fault Tolerant Time Interval | Allocation to Architecture | Safe State |
|---|---|---|---|---|---|
| Technical Safety Requirement 01 | The Lane Keep Assistance (LKA) Safety component shall ensure that duration of the "LKA_Torque_Request" sent to the "Final Torque" component is below "Max_Duration" value | B | 500 ms | EPS ECU | Deactivate the LKA feature and set "LKA_Torque_Request" value to 0 |
| Technical Safety Requirement 02 | The LKA Safety block shall perform Data Transmission Integrity Check of the "LKA_Torque_Request" signal | B | 500 ms | EPS ECU | Deactivate the LKA feature and set "LKA_Torque_Request" value to 0 |
| Technical Safety | If duration of the "LKA_Torque_Request" is above | B | 500 ms | EPS ECU | Deactivate the LKA |

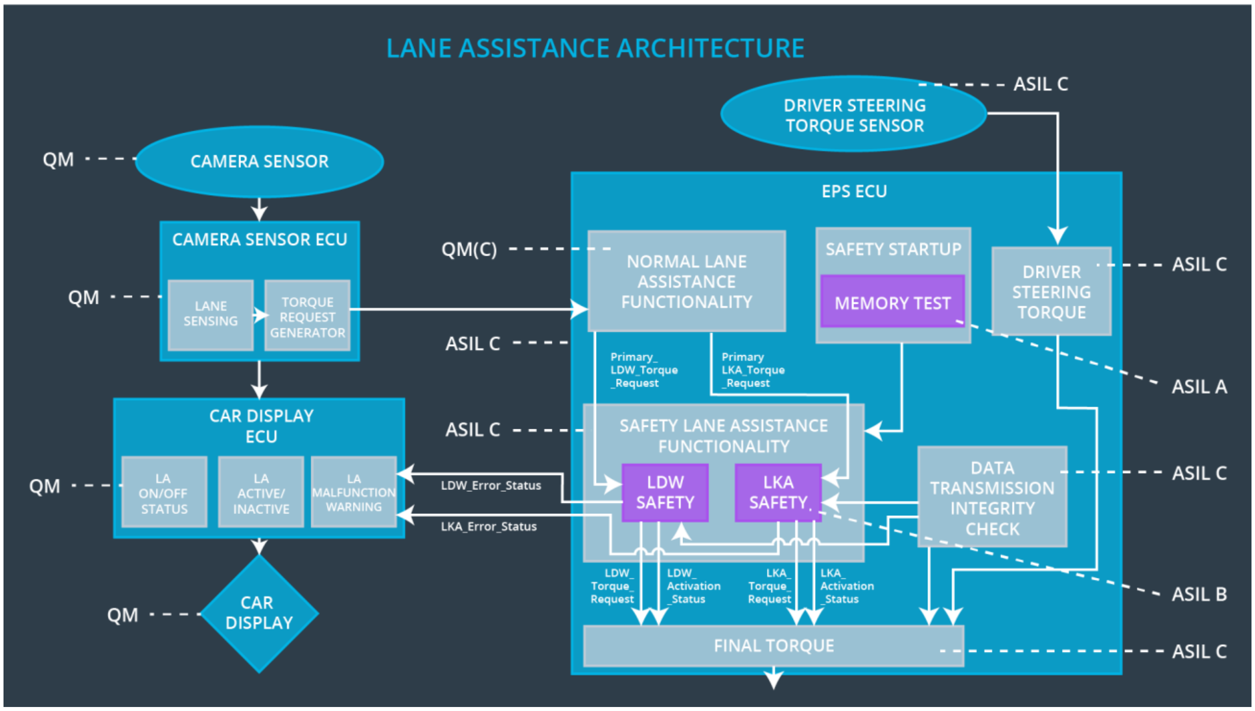
|  |  |  |  |  |  |
|---|---|---|---|---|---|
| Requirement 03 | “Max_Duration” value, the LKA Safety block shall set the“LKA_Activation_Status” signal to “Inactive” |  |  |  | feature and set “LKA_Torque_Request” value to 0 |
| Technical Safety Requirement 04 | As soon and “LKA_Activation_Status signal is set to “Inactive”, LDW Safety block shall provide “LKA_Error_Status” signal to the LA Malfunction Warning block of the Car Display ECU | B | 500 ms | EPS ECU | Deactivate the LKA feature and set “LKA_Torque_Request” value to 0 |
| Technical Safety Requirement 05 | Memory test shall be conducted at startup (power on reset/wakeup, Ignition transition to Run) of the EPS ECU to check for any faults in memory partition associated with LDW function | A | “Max_Startup_Time” | EPS ECU | Deactivate the LKA feature and set “LKA_Torque_Request” value to 0 |

### Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:

**[OPTIONAL: For each technical safety requirement, identify both the verification and validation acceptance criteria. “Validation” asks whether or not you chose the appropriate parameters. “Verification” involves testing to make sure the vehicle behaves as expected when the parameter value is crossed. There is not necessarily one right answer. Look at your verification and validation acceptance criteria from the functional safety concept for inspiration.]**

## 3.2. Refinement of the System Architecture

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



## 3.3. Allocation of Technical Safety Requirements to Architecture Elements

**[Instructions: We already included the allocation as part of the technical requirement tables. Here you can state that for this particular item, all technical safety requirements are allocated to the Electronic Power Steering ECU]**

All Technical Safety Requirements of the LDW Safety component are allocated to the EPS ECU.

All Technical Safety Requirements of the LKA Safety component are allocated to the EPS ECU.

## 3.4. Warning and Degradation Concept

**[Instructions: We've already identified that for any system malfunction, the lane assistance functions will be turned off and the driver will receive a warning light indication. The technical safety requirements have not changed how functionality will be degraded or what the warning will be.**

**So, in this case, the warning and degradation concept is the same for the technical safety requirements as for the functional safety requirements. You can copy the functional safety warning and degradation concept here.**

**Oftentimes, a technical safety analysis will lead to a more detailed warning and degradation concept.]**

The Warning and Degradation Concept is the same as for Functional Safety Requirements:

| **ID** | **Degradation Mode** | **Trigger for Degradation Mode** | **Safe State invoked?** | **Driver Warning** |
|---|---|---|---|---|
| WDC-01 | The LDW function is turned off | (1) The Lane Departure oscillating torque amplitude value is MORE than Max_Torque_Amplitude<br>OR<br>(2) The Lane Departure oscillating torque frequency value is MORE than Max_Torque_Frequency | Yes | The Lane Assist Malfunction Warning light is activated on the Car Display |
| WDC-02 | LKA function is turned off | Duration of the applied LKA torque is MORE than Max_Duration | Yes | The Lane Assist Malfunction Warning light is activated on the Car Display |