

Technical Safety Concept Lane Assistance

**Document Version: 1.0**

**Template Version 2.0, Released on 2017-10-17**



Document History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Editor | Description |
| 2017-10-16 | 1.0 | Daniel Gattringer | Initial version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[Document History 2](#_Toc496900852)

[Table of Contents 2](#_Toc496900853)

[1. Purpose of the Technical Safety Concept 3](#_Toc496900854)

[2. Inputs to the Technical Safety Concept 3](#_Toc496900855)

[2.1. Functional Safety Requirements 3](#_Toc496900856)

[2.2. Refined System Architecture from Functional Safety Concept 4](#_Toc496900857)

[3. Technical Safety Concept 6](#_Toc496900858)

[3.1. Technical Safety Requirements 6](#_Toc496900859)

[3.2. Refinement of the System Architecture 10](#_Toc496900860)

[3.3. Allocation of Technical Safety Requirements to Architecture Elements 11](#_Toc496900861)

[3.4. Warning and Degradation Concept 11](#_Toc496900862)

# Purpose of the Technical Safety Concept

The creation of a technical safety concept is part of the safety process of ISO 26262 for the treatment of potential malfunctions in electrical and electronic systems.

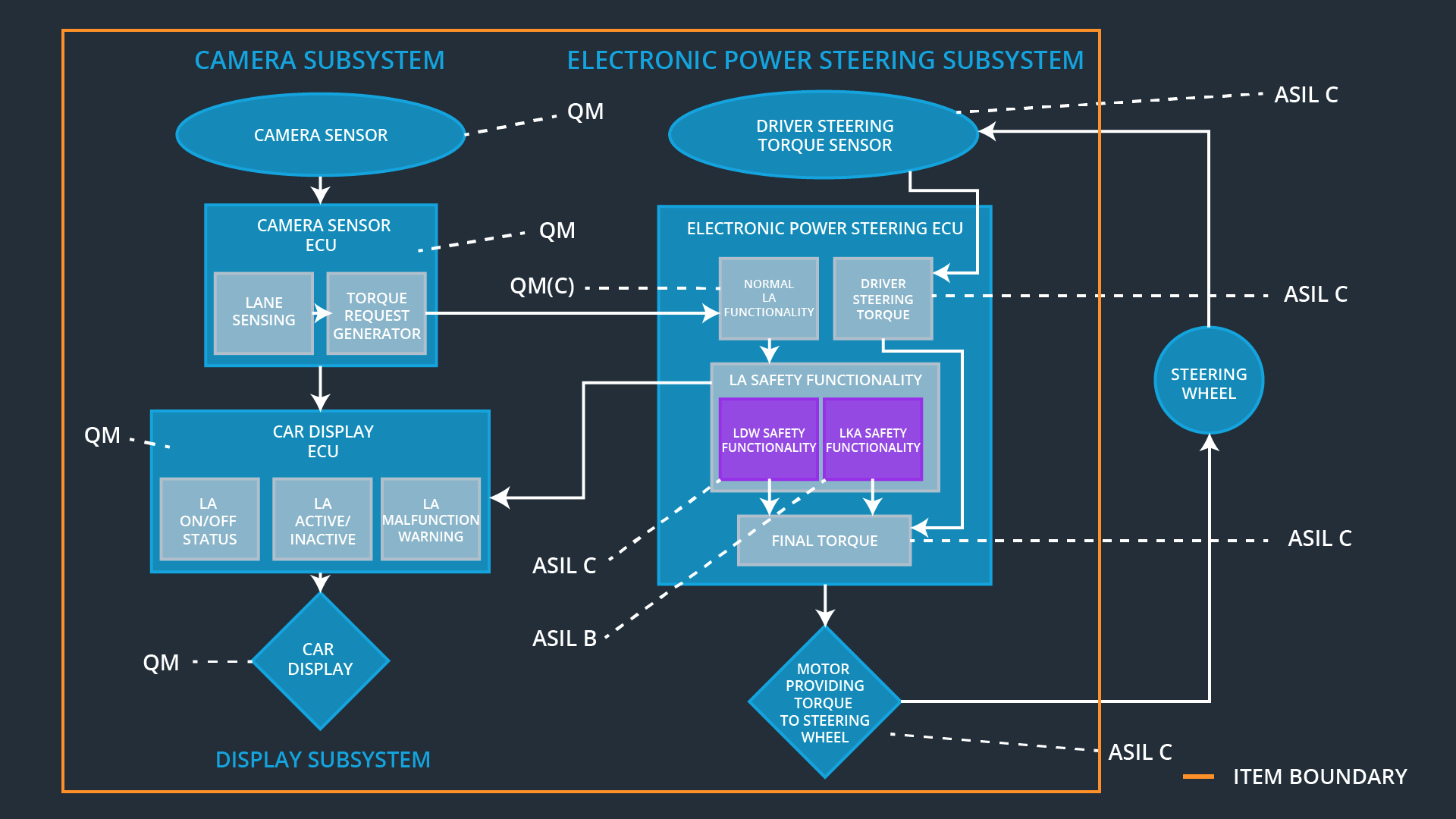
The purpose of the technical safety concept is to transform functional safety requirements to additional technical requirements and allocate these high-level hardware and software requirements to system diagrams of the lane assistance functional safety project.

# Inputs to the Technical Safety Concept

## Functional Safety Requirements

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **ASIL** | **Fault Tolerant Time Interval** | **Safe State** |
| Functional  Safety  Requirement  01-01 | The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max\_Torque\_Amplitude. | C | 50ms | Set the oscillating torque to zero. |
| Functional  Safety  Requirement  01-02 | The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max\_Torque\_Frequency. | C | 50ms | Set the oscillating torque to zero. |
| Functional  Safety  Requirement  02-01 | The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max\_Duration. | B | 500ms | Set the lane keeping add extra torque to zero. |
| Functional  Safety  Requirement  03-01 | The lane keeping item shall ensure that the lane departure warning by means of vibration of the steering wheel is only possible when LDW\_On is set. | A | 50ms | Set the oscillating torque to zero. |
| Functional  Safety  Requirement  04-01 | The electronic power steering ECU shall ensure that the lane keeping assistance torque is set to zero when the camera sensor ECU can’t reliably detect the lane boundaries. | A | 50ms | Set the lane keeping add extra torque to zero. |
| Functional  Safety  Requirement  04-02 | The electronic power steering ECU shall ensure that the lane keeping assistance functionality is deactivated and signalized on the car display when the camera sensor ECU can’t reliably detect the lane boundaries. | A | 50ms | Set the lane keeping add extra torque to zero. |

## Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

|  |  |
| --- | --- |
| **Element** | **Description** |
| Camera Sensor | Sensor for the optical detection of the front area of the vehicle, including detectable lane lines. |
| Camera Sensor ECU | Electronic Control Unit responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake. Responsible for triggering reactions to add extra torque for LDW and LKA functionality. |
| Camera Sensor ECU  Lane Sensing | Component within the camera sensor ECU responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake. |
| Camera Sensor ECU Torque Request Generator | Component within the camera sensor ECU responsible for calculating and sending an request for additional steering torque for the LDW and LKA functionality. |
| Car Display | Visual display which is, among other functionalities, responsible for displaying warning of lane departures and LKA and LDW activation-status. |
| Car Display ECU | Electronic control unit, which is responsible for creating and providing the data and information that the car display visualizes. |
| Car Display ECU  LA on/off status | Component within the car display ECU responsible for visualizing if the lane assistance functionality is switched on or off. |
| Car Display ECU  LA active/inactive | Component within the car display ECU responsible for visualizing if the lane assistance functionality is active at the moment. Active means the car is drifting away from the center of the lane and LKA is actively acting or the car is getting too narrow to a lane boundary and LDW is warning. |
| Car Display ECU  LA malfunction warning | Component within the car display ECU responsible for visualizing if there occurs any malfunction within the lane assistance system. |
| Driver Steering Torque Sensor | Sensor responsible for measuring the steering torque provided by the driver. |
| Electronic Power Steering (EPS) ECU | The electronic control unit is responsible for evaluating the torque provided by the driver and for adding an additional torque based on the torque request of the lane assist system (LKA). Initializes the vibration of the steering wheel when the driver inadvertently drifts away from the center of the lane (LDW). |
| EPS ECU  Normal Lane Assistance Functionality | Component within the electronic power steering ECU responsible for receiving extra torque request from the camera sensor ECU and doing different non-safety tasks. |
| EPS ECU  Driver Steering Torque | Component within the electronic power steering ECU responsible for receiving the steering torque with which the driver moves the steering wheel. |
| EPS ECU  LDW Safety Functionality | Component within the electronic power steering ECU responsible for keeping the lane departure warning action (oscillating torque) below Max\_Torque\_Amplitude and Max\_Torque\_Frequency.  This component is also responsible for ensuring that the lane departure warning by means of vibration of the steering wheel is only applicated when LDW\_On is set. |
| EPS ECU  LKA Safety Functionality | Component within the electronic power steering ECU responsible for ensuring that the lane keeping assistance is not forcing the car longer than Max\_Duration to the center of the lane.  This component is also responsible for ensuring that the lane keeping assistance by forcing the car to the center of the lane is only applicated when the lane boundaries can be detected reliably. |
| EPS ECU  Final Torque | Component within the electronic power steering ECU responsible for ensuring that the single torque values from LDW, LKA are combined with the drivers original steering torque and sent to the motor. |
| Motor | Mechatronic device which adds extra steering torque directly to the steering wheel. |

# Technical Safety Concept

## Technical Safety Requirements

**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 |  |  |

The following image shows the LDW safety component of the EPS ECU:



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 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 |  | Set the oscillating torque to zero. |
| Technical  Safety  Requirement  02 |  |  |  |  |  |
| Technical  Safety  Requirement  03 |  |  |  |  |  |
| Technical  Safety  Requirement  04 |  |  |  |  |  |
| Technical  Safety  Requirement  05 |  |  |  |  |  |

**[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 |  |  |

The following image shows the LDW safety component of the EPS ECU:



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 |  |  |  |  |  |
| Technical  Safety  Requirement  02 |  |  |  |  |  |
| Technical  Safety  Requirement  03 |  |  |  |  |  |
| Technical  Safety  Requirement  04 |  |  |  |  |  |
| Technical  Safety  Requirement  05 |  |  |  |  |  |

**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.]**

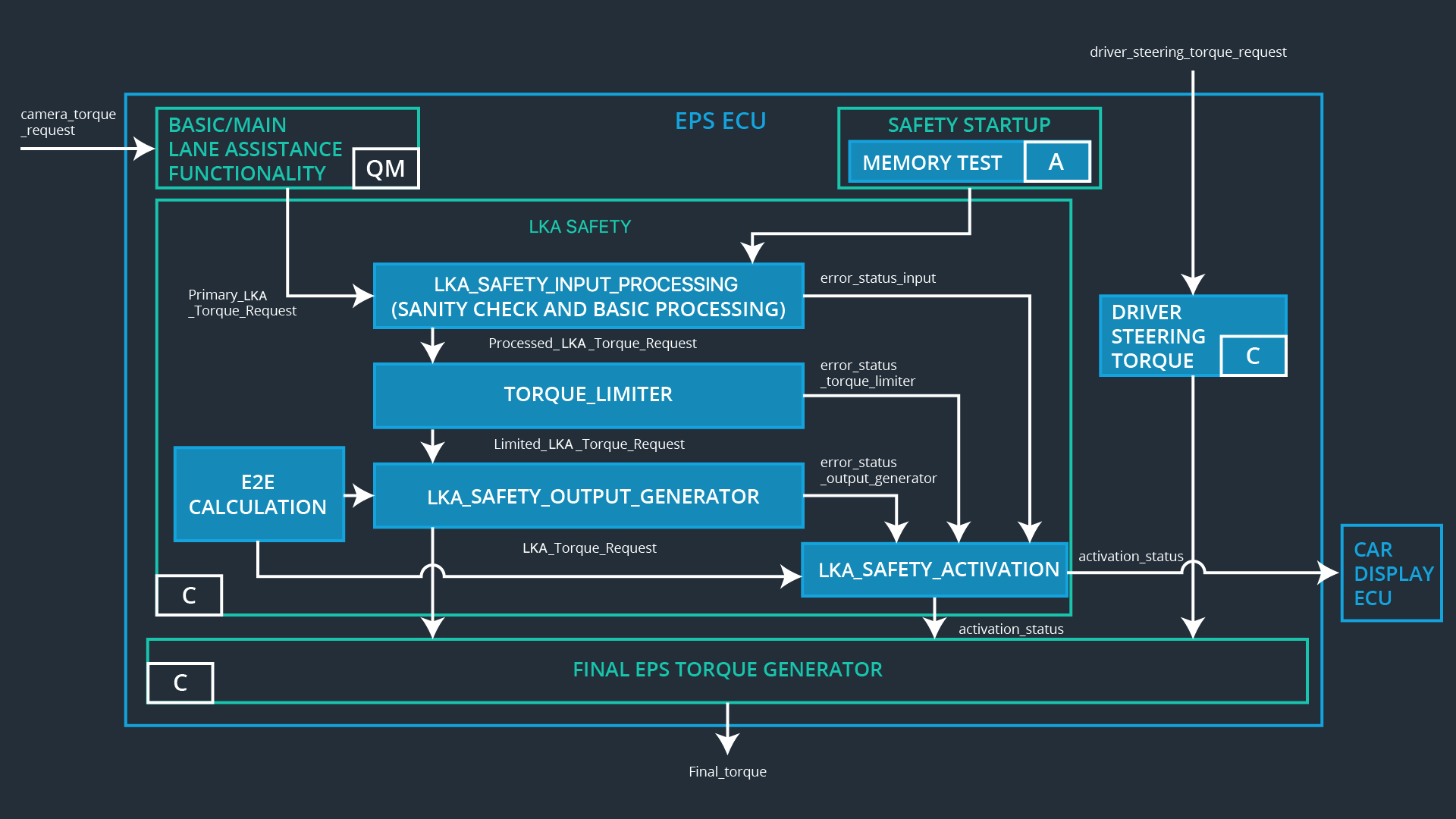
**Lane Keeping Assistance (LKA) Requirements:**

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 |  |  |

The following image shows the LKA safety component of the EPS ECU:



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 |  |  |  |  |  |
| Technical  Safety  Requirement  02 |  |  |  |  |  |
| Technical  Safety  Requirement  03 |  |  |  |  |  |
| Technical  Safety  Requirement  04 |  |  |  |  |  |
| Technical  Safety  Requirement  05 |  |  |  |  |  |

**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.]**

## 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.]**

## 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]**

## 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. ]**