Technical Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
1-3-2018	0.1	majing	first draft
1-5-2018	1.0	majing	submission

Table of Contents

Purpose of the Technical Safety Concept

In this document new requirements are defined and assigned to the system architecture. These requirements are more concrete and gets into details of the item's technology as specified by ISO 26262.

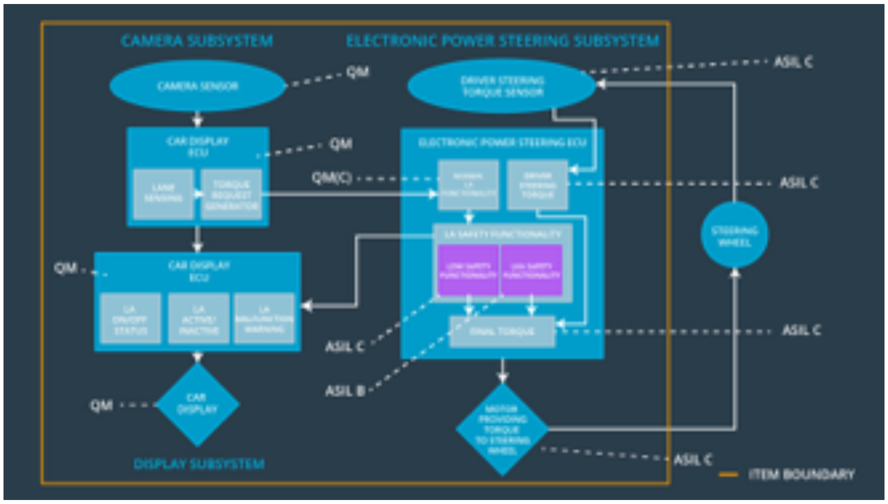
[Instructions: Answer what is the purpose of a technical safety concept?]

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	50 mS	The vibrational oscillating torque's amplitude is below Max_Torque_Amplitude.
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	C	50 mS	The vibrational oscillating torque's frequency is below Max_Torque_ Frequency.
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	500 mS	The torque applied by the power steering ECU after Max_Duration is 0.

Refined System Architecture from Functional Safety Concept



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	Capture road images and provide them to the Camera Sensor ECU.
Camera Sensor ECU - Lane Sensing	Software module detecting the lane line positions from the Camera Sensor images.
Camera Sensor ECU - Torque request generator	Software module calculating the necessary torque to be requested to the Electronic Power Steering ECU.
Car Display	Displays warning for the driver.
Car Display ECU - Lane Assistance On/ Off Status	Indicate the status of the Lane Assistance functionality.
Car Display ECU - Lane Assistant Active/Inactive	Indicates if the Lyne Assistance functionality is properly functioning (Active/Inactive).
Car Display ECU - Lane Assistance malfunction warning	Indicate a malfunction on the Lane Assistance functionality.
Driver Steering Torque Sensor	Measure the torque applied to the steering wheel by the driver.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Software module receiving the driver’s torque request from the steering wheel.
EPS ECU - Normal Lane Assistance Functionality	Software module receiving the Camera Sensor ECU torque request.
EPS ECU - Lane Departure Warning Safety Functionality	Software module ensuring the torque amplitude is below Max_Torque_Amplitude and torque frequency is below Max_Torque_Frequency.
EPS ECU - Lane Keeping Assistant Safety Functionality	Software module ensuring the Lane Keeping Assistance functionality application is not activate more than Max_duration time.
EPS ECU - Final Torque	Combine the torque request from the Lane Keeping and Lane Departure Warning functionalities and sends them to the motor.
Motor	Apples the required torque to the steering wheel.

Technical Safety Concept

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.]

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 01-01-01	The Lane Departure Warning 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	Lane Departure Warning torque to zero.

Technical Safety Requirement 01-01-02	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50 mS	LDW Safety	Lane Departure Warning torque to zero.
Technical Safety Requirement 01-01-03	When a failure is detected by the Lane Departure Warning functionality, it shall deactivate the Lane Departure Warning feature and set 'LDW_Torque_Request' to zero.	C	50 mS	LDW Safety	Lane Departure Warning torque to zero.
Technical Safety Requirement 01-01-04	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	50 mS	LDW Safety	Lane Departure Warning torque to zero.
Technical Safety Requirement 01-01-05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Data Transmission Integrity Check	Lane Departure Warning torque to zero.

[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 01-02-01	The LDW safety component shall ensure that the frequency of the 'LDW_Torque_Request‘ sent to the ‘Final electronically power steering Torque‘ component is below 'Max_Torque_Frequency’.	C	50 mS	LDW Safety	LDW Torque Request Frequency shall be set to zero.
Technical Safety Requirement 01-02-02	The validity and integrity of the data transmission for 'Max_Torque_Frequency’ signal shall be ensured.	C	50 mS	LDW Safety	LDW Torque Request Frequency shall be set to zero.
Technical Safety Requirement 01-02-03	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the 'Max_Torque_Frequency‘ shall be set to zero.	C	50 mS	LDW Safety	LDW Torque Request Frequency shall be set to zero.
Technical Safety Requirement 01-02-04	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	50 mS	LDW Safety	LDW Torque Request Frequency shall be set to zero.
Technical Safety Requirement 01-02-05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Data Transmission Integrity Check	LDW Torque Request Frequency shall be set to zero.

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:

[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 02-01-01	The LKA safety component shall ensure the duration of the lane keeping assistance torque is applied for less than Max_Duration.	B	500 mS	LKA Safety	Lane Keeping Assistance torque is zero.

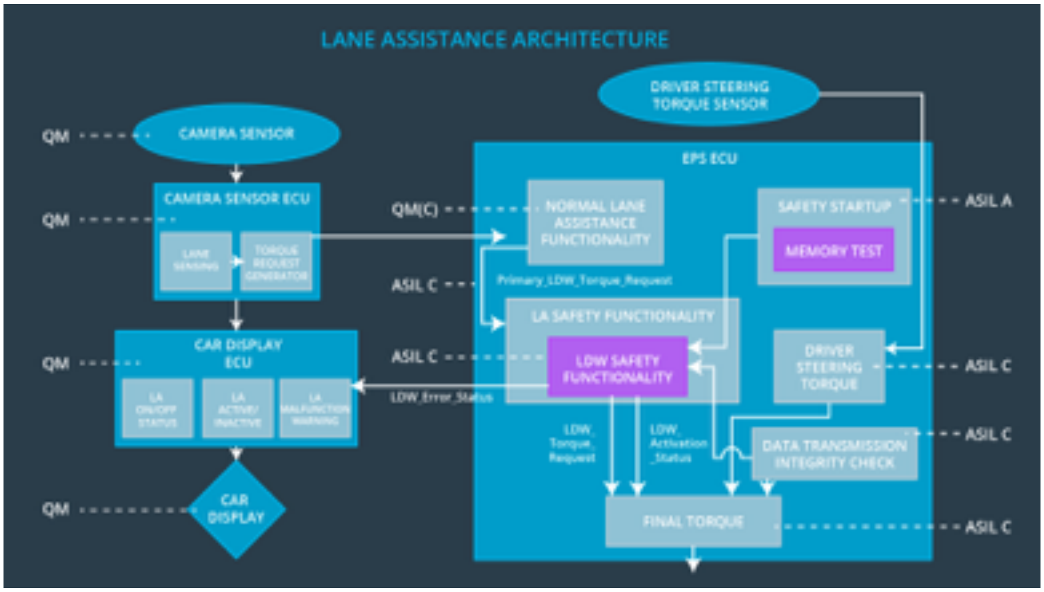
Technical Safety Requirement 02-01-02	The validity and integrity of the data transmission for ‚LKA_Torque_Request’ signal shall be ensured.	B	500 mS	LKA Safety	Lane Keeping Assistance torque is zero.
Technical Safety Requirement 02-01-03	As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and the 'LKA_Torque_Request‘ shall be set to zero.	B	500 mS	LKA Safety	Lane Keeping Assistance torque is zero.
Technical Safety Requirement 02-01-04	As soon as the LKA function deactivates the LKA feature, the LKA Safety software block shall send a signal to the car display ECU to turn on a warning light.	B	500 mS	LKA Safety	Lane Keeping Assistance torque is zero.
Technical Safety Requirement 02-01-05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Data Transmission Integrity Check	Lane Keeping Assistance torque is zero.

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]

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Technical Safety Requirement 01-01-01	The LDW safety component shall ensure that the amplitude of the 'LDW_Torque_Request‘ sent to the ‘Final electronically power steering Torque‘ component is below 'Max_Torque_Amplitude’.	X		
Technical Safety Requirement 01-01-02	The validity and integrity of the data transmission for 'LDW_Torque_Request’ signal shall be ensured.	X		
Technical Safety Requirement 01-01-03	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.	X		

Technical Safety Requirement 01-01-04	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.	X		
Technical Safety Requirement 01-01-05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	X		
Technical Safety Requirement 01-02-01	The LDW safety component shall ensure that the frequency of the 'LDW_Torque_Request‘ sent to the ‘Final electronically power steering Torque‘ component is below 'Max_Torque_Frequency’.	X		
Technical Safety Requirement 01-02-02	The validity and integrity of the data transmission for 'Max_Torque_Frequency’ signal shall be ensured.	X		
Technical Safety Requirement 01-02-03	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the 'Max_Torque_Frequency‘ shall be set to zero.	X		
Technical Safety Requirement 01-02-04	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.	X		
Technical Safety Requirement 01-02-05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	X		
Technical Safety Requirement 02-01-01	The LKA safety component shall ensure the duration of the lane keeping assistance torque is applied for less than Max_Duration.	X		
Technical Safety Requirement 02-01-02	The validity and integrity of the data transmission for ‚LKA_Torque_Request’ signal shall be ensured.	X		

Technical Safety Requirement 02-01-03	As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and the 'LKA_Torque_Request‘ shall be set to zero.	X		
Technical Safety Requirement 02-01-04	As soon as the LKA function deactivates the LKA feature, the LKA Safety software block shall send a signal to the car display ECU to turn on a warning light.	X		
Technical Safety Requirement 02-01-05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	X		

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.]

ID	**Degradation Mode**	**Trigger for Degradation Mode**	**Safe State invoked?**	**Driver Warning**
WDC-01	Turn system off.	Malfunction_01 Malfunction_02	Yes	Warning light on the dashboard
WDC-02	Turn system off.	Malfunction_03	Yes	Warning light on the dashboard