Technical Safety Concept 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
20/10/2018	1	Omar	First attempt

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]

Purpose of the Technical Safety Concept

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

the technical safety concept defines how the subsystem interact at the message level describes how the ECUs communicate with each other.

Inputs to the Technical Safety Concept

Functional Safety Requirements

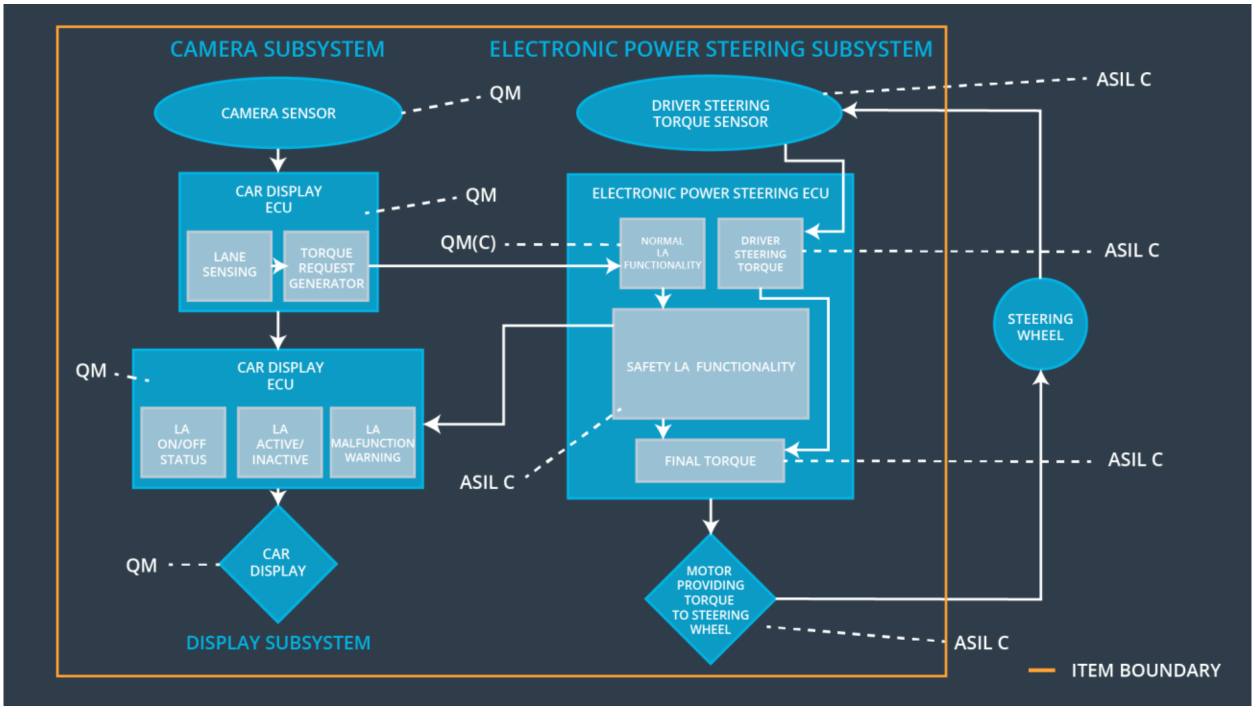
[Instructions: Provide the functional safety requirements derived in the functional safety concept]

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	Lane departure warning torque request amplitude shall be set 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	50 ms	Lane departure warning torque request amplitude shall be set to zero
Functional Safety Requirement 02-01	the electronic power steering ECU shall ensure that the lane keeping assistance torque is	B	500 ms	lane keeping assistance function shall be time

	applied for only Max_Duration			limited and the additional steering torque shall end after a given timer interval so that the driver can not misuse the system for autonomous driving

Refined System Architecture from Functional Safety Concept

[Instructions: Provide the refined system architecture from the 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	The camera sensor reads in images from the road
Camera Sensor ECU - Lane Sensing	Camera Sensor ECU - Lane Sensing it detect the lane and it give signal if there are any lane changing or the driver move out of your lane or not.
Camera Sensor ECU - Torque request generator	Camera Sensor ECU - Torque request generator If the Camera Sensor ECU - Lane Sensing detect any lane changing it will make activate torque request generator which will give signal EPS subsystem to normal lane assistance functionality and the system will check if it’s safe to make lane change or the driver move out of your lane or not
Car Display	Car Display contain three software blocks on controls a light that tells the driver If the lane

	keeping item is on or off and second one will Control a light telling the driver that the lane departure Warning is activated or in active.
Car Display ECU - Lane Assistance On/Off Status	Car Display ECU - Lane Assistance On/Off Status controls a light that tells the driver If the lane keeping item is on or off
Car Display ECU - Lane Assistant Active/Inactive	Car Display ECU - Lane Assistant Active/Inactive Control a light telling the driver that the lane departure Warning is activated or in active.
Car Display ECU - Lane Assistance malfunction warning	Car Display ECU - Lane Assistance malfunction warning work as follow as soon as the LDW function deactivates he LDW feature the LDW safety software block shall send a signal to the car display to turn on a warning light.
Driver Steering Torque Sensor	Driver Steering Torque Sensor will sense the applied steering of the diver on the steering wheels.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Electronic Power Steering ECU will sense how Much the driver is turning the steering wheel and t will receive the vibrational torque request from the camera Subsystem this is where we will limit the amplitude and The frequency to be low max torque amplitude and max torque frequency. the last thing Electronic Power Steering ECU do it will add these torque request together to output a final torque to the motor that moves the steering wheel.
EPS ECU - Normal Lane Assistance Functionality	EPS ECU - Normal Lane Assistance Functionality it control the normal steering as long as it's safe as it sent the data to LA functionaity
EPS ECU - Lane Departure Warning Safety Functionality	EPS ECU - Lane Departure Warning Safety Functionality it shall ensure that the amplitude of he LDW_Torque_Request sent to the Final electroics power steering Torque componet is below Max_Torque_Amplitude
EPS ECU - Lane Keeping Assistant Safety Functionality	the lane keeping assistance function shall be time limited and the additional steering torque shall end after a given timer interval so that the driver can not misuse the system for autonomous driving
EPS ECU - Final Torque	EPS ECU - Final Torque is the final torque that will be provided to the steering wheels
Motor	Motor will Providing torque to steering

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	The LDW safety component shall ensure that the amplitude of the	C	50 ms	LDW safety software componet	Lane departure warning torque request amplitude shall be set to zero

	'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Amplitude.				
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	50 ms	LDW safety software componet	Lane departure warning torque request amplitude shall be set to zero
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	50 ms	LDW safety software componet	Lane departure warning torque request amplitude shall be set to zero
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Reque	C	50 ms	data transmission integrity check	Lane departure warning torque request amplitude shall be set to

	st' signal shall be ensured.				zero
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	Safety Startup	Lane departure warning torque request amplitude shall be set 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	ASI	Fault Tolerant Time	Architecture Allocation	Safe State

		L	Interval		
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_Frequency .	C	50 ms	LDW safety software componet	Lane departure warning torque request amplitude shall be set to zero
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	50 ms	LDW safety software componet	Lane departure warning torque request amplitude shall be set to zero
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	50 ms	LDW safety software componet	Lane departure warning torque request amplitude shall be set to zero

Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50 ms	data transmission integrity check	Lane departure warning torque request amplitude shall be set to zero
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	Safety Startup	Lane departure warning torque request amplitude 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 01	The Lane keeping item shall ensure that the lane departure oscillating torque amplitude is below 'Max_Torque_Amplitude	B	500 ms	LDW safety software componet	lane keeping assistance function shall be time limited and the additional steering torque shall end after a given timer interval so that the driver

					can not misuse the system for autonomous driving
Technical Safety Requirement 02	As soon as The Lane keeping item deactivates the Lane keeping item feature, the The Lane keeping item Safety' software block shall send a signal to the car display ECU to turn on a warning light.	B	500 ms	LDW safety software componet	lane keeping assistance function shall be time limited and the additional steering torque shall end after a given timer interval so that the driver can not misuse the system for autonomous

					driving
Technical Safety Requirement 03	As soon as a failure is detected by The Lane keeping item, it shall deactivate The Lane keeping item and the 'LDW_Torque_Request' shall be set to zero.	B	500 ms	LDW safety software componet	lane keeping assistance function shall be time limited and the additional steering torque shall end after a given timer interval so that the driver can not misuse the system for autonomous driving
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request'	B	500 ms	data transmission integrity check	lane keeping assistance function

	signal shall be ensured.				shall be time limited and the additional steering torque shall end after a given timer interval so that the driver can not misuse the system for autonomous driving
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	Safety Startup	lane keeping assistance function shall be time limited and the additional steering

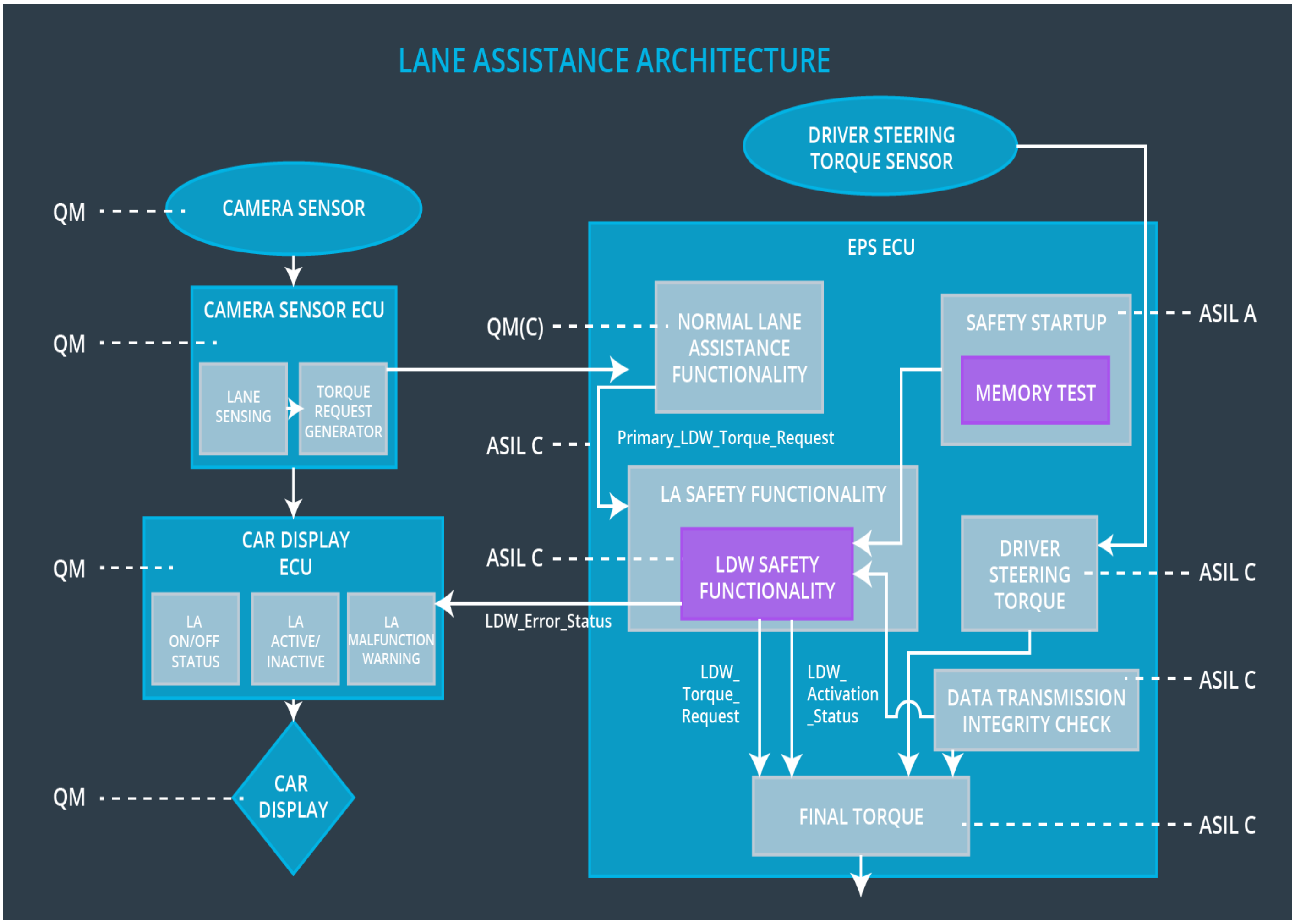
					torque shall end after a given timer interval so that the driver can not misuse the system for autonomous driving

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]

1- LDW safety software componet
2- data transmission integrity check
3- Safety Startup

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 off the functionality	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	Yes	There is no warning
WDC-02	turn off the functionality	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	Yes	the driver will see a warning light on the dashboard when the system malfunctions