Technical Safety Concept Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
11/2/17	1.0	Nicholas Moellers	First Draft

Table of Contents

Purpose of the Technical Safety Concept

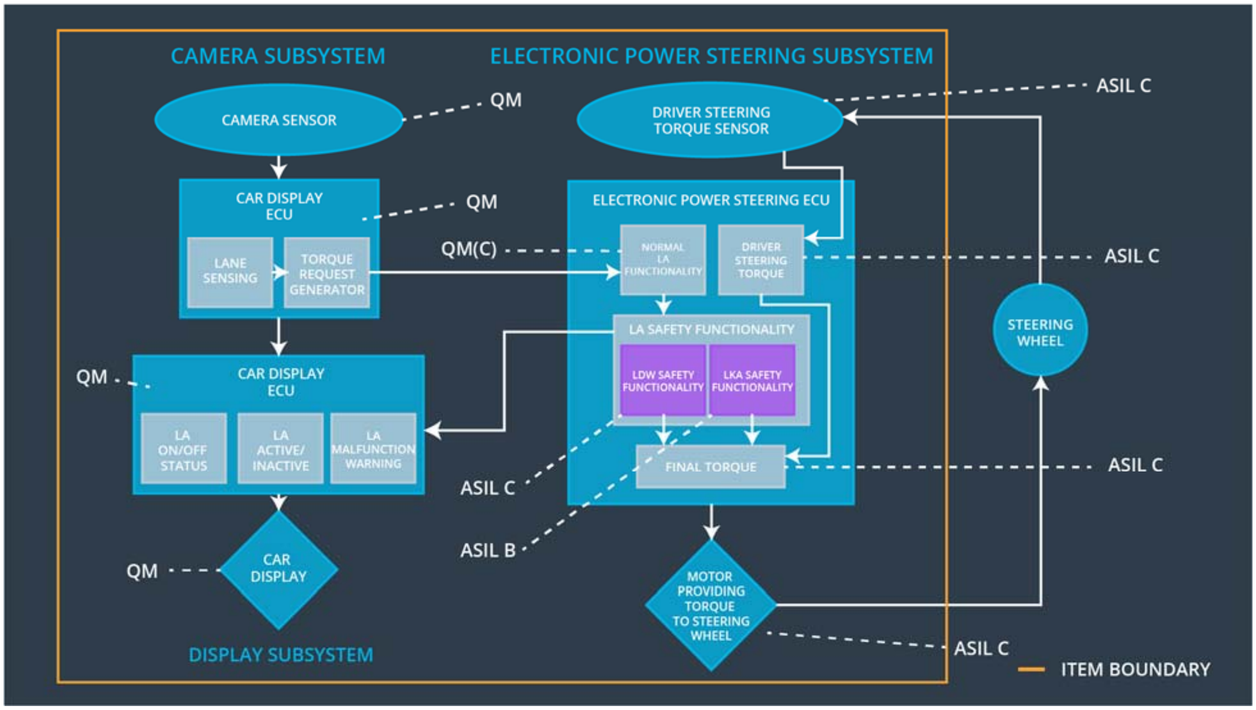
[Instructions: Answer what is the purpose of a technical safety concept?]
The Technical Safety Concept is more concrete than the Function Safety concept and gets into the details of the item's technology. In this document, the functional safety requirements will be translated into technical safety requirements and allocated to the system architecture.

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	Set vibration 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	50 mS	Set vibration torque to zero
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	B	500 mS	Lane keeping item is disabled

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	Provide image data of roads to camera sensor ECU
Camera Sensor ECU - Lane Sensing	Detect lane lines in camera sensor data
Camera Sensor ECU - Torque request generator	Calculate torque to apply to steering wheel
Car Display	Display lane assistance information to driver
Car Display ECU - Lane Assistance On/Off Status	Calculate the on/off status of the lane assistance feature
Car Display ECU - Lane Assistant Active/Inactive	Calculate the active/inactive status of the lane assistance feature
Car Display ECU - Lane Assistance malfunction warning	Determine if the driver needs to be warned of malfunction in the lane detection warning and lane keeping systems
Driver Steering Torque Sensor	Detect torque input and send to EPS ECU
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Calculate torque input being applied by driver
EPS ECU - Normal Lane Assistance Functionality	Send lane departure warnings and lane keeping torque request to safe lane assistance functionality
EPS ECU - Lane Departure Warning Safety Functionality	Ensure that the lane departure warnings are safe and controllable by driver
EPS ECU - Lane Keeping Assistant Safety Functionality	Ensure that the lane keeping assistance feature is not abused by the drive
EPS ECU - Final Torque	Send the torque application request to the steering wheel
Motor	Apply 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	The LDW safety component shall ensure that the amplitude of the ‘LDW_Torque_Request’ sent to the ‘Final EPS Torque’ component is below ‘Max_Torque_Amplitude’	C	50 ms	LDW Safety	The “LDW_Torque_Request” Amplitude shall be set to zero
Technical Safety	The validity and integrity of the data transmission for	C	50 ms	Data Transmission	The “LDW_Torque

Requirement 02	‘LDW_Torque Request’ signal shall be ensured”			Integrity Check	_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	The “LDW_Torque_Request” Amplitude shall be set to zero
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 ECO to turn on a warning light.	C	50 ms	LDW Safety	The “LDW_Torque_Request” Amplitude shall be set to zero
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Memory Test	The “LDW_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	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 01	The LDW safety component shall ensure that the frequency of the 'LDW_Torque_Request' sent to the 'Final EPS Torque' component is below 'Max_Torque_Frequency'	C	50 ms	LDW Safety	The "LDW_Torque_Request" Frequency shall be set to zero
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 Integrity Check	The "LDW_Torque_Request" Frequency 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	The "LDW_Torque_Request" Frequency shall be set to zero
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 ECO to turn on a warning light.	C	50 ms	LDW Safety	The "LDW_Torque_Request" Frequency shall be set to zero
Technical	Memory test shall be conducted at	A	Ignition	Memory Test	The

Safety Requirement 05	startup of the EPS ECU to check for any faults in memory.		cycle		“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:

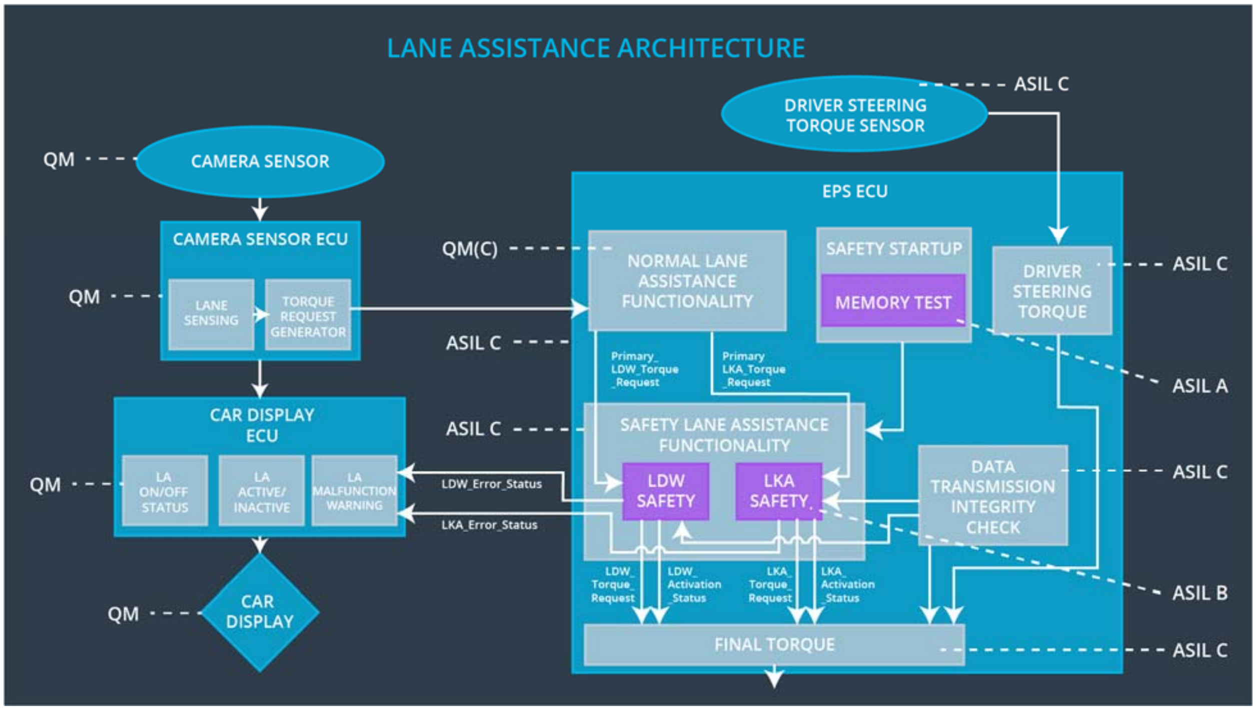
ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01	The LKA safety component shall ensure that the active duration of the ‘LKA_Torque_Request’ sent to the ‘Final EPS Torque’ component is less than ‘Max_Duration’	B	500 ms	LKA Safety	The LKA_Activation_Satus and LKA_Torque_Request shall be set to 0
Technical Safety Requirement 02	The validity and integrity of the data transmission for ‘LKA_Torque_Request’ signal shall be ensured”	B	500 ms	Data Transmission Integrity Check	The LKA_Activation_Satus and LKA_Torque_Request shall be set to 0
Technical Safety Requirement 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	The LKA_Activation_Satus and LKA_Torque_Request shall be set to 0
Technical Safety Requirement 04	As soon as the LKA function deactivates the LKA feature, the ‘LKA Safety’ software block shall send a signal to the car display ECO to turn on a warning light.	B	500 ms	LKA Safety	The LKA_Activation_Satus and LKA_Torque_Request shall be set to 0
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	QM	Ignition cycle	Memory Test	The LKA_Activation_Satus and LKA_Torque_Request shall be set

					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.]

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

For this particular item, all technical safety requirements are allocated to the Electronic Power Steering ECU.

Warning and Degradation Concept

ID	Degradation	Trigger for	Safe State	Driver Warning

	Mode	Degradation Mode	invoked?	
WDC-01	Lane keeping assistance mode is disabled	Lane keeping assistance torque has been applied for some time greater than Max_Duration	Yes	Lane keeping mode has been disabled because the functionality is not meant for autonomous driving, and the driver maintains responsibility for the safe operation of the vehicle.
WDC-02	Lane departure warning mode is disabled	The departure warning vibrations have exceeded either Max_Torque_Amplitude or Max_Torque_Frequency	Yes	Lane departure warning mode is disabled to ensure that the driver can maintain control of the vehicle