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
12/Sep/2017	0.1	Andrew Wilkie	Updating while following T3.M2.E2.L18 videos

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]

Document history 2

Table of Contents 2

Purpose of the Technical Safety Concept 3

Inputs to the Technical Safety Concept 3

Functional Safety Requirements 3

Refined System Architecture from Functional Safety Concept 4

Diagram 1 : Refinement of the System Architecture From Functional Safety Concept 5

Functional overview of architecture elements 5

Technical Safety Concept 7

Technical Safety Requirements 7

Refinement of the System Architecture 13

Diagram 2 : Refinement of the System Architecture 14

Allocation of Technical Safety Requirements to Architecture Elements 14
Warning and Degradation Concept 14

Purpose of the Technical Safety Concept

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

The purpose of the Technical Safety Concept (aka document) is to turn the Functional Safety requirements into lower level technical safety requirements. These technical safety requirements will be allocated to the system architecture.

Inputs to the Technical Safety Concept

Functional Safety Requirements

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

Lane Departure Warning (LDW) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	The electronic power steering ECU shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	B	50 ms	Turn off by setting torque request to 0.

Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	B	50 ms	Turn off by setting torque request to 0.

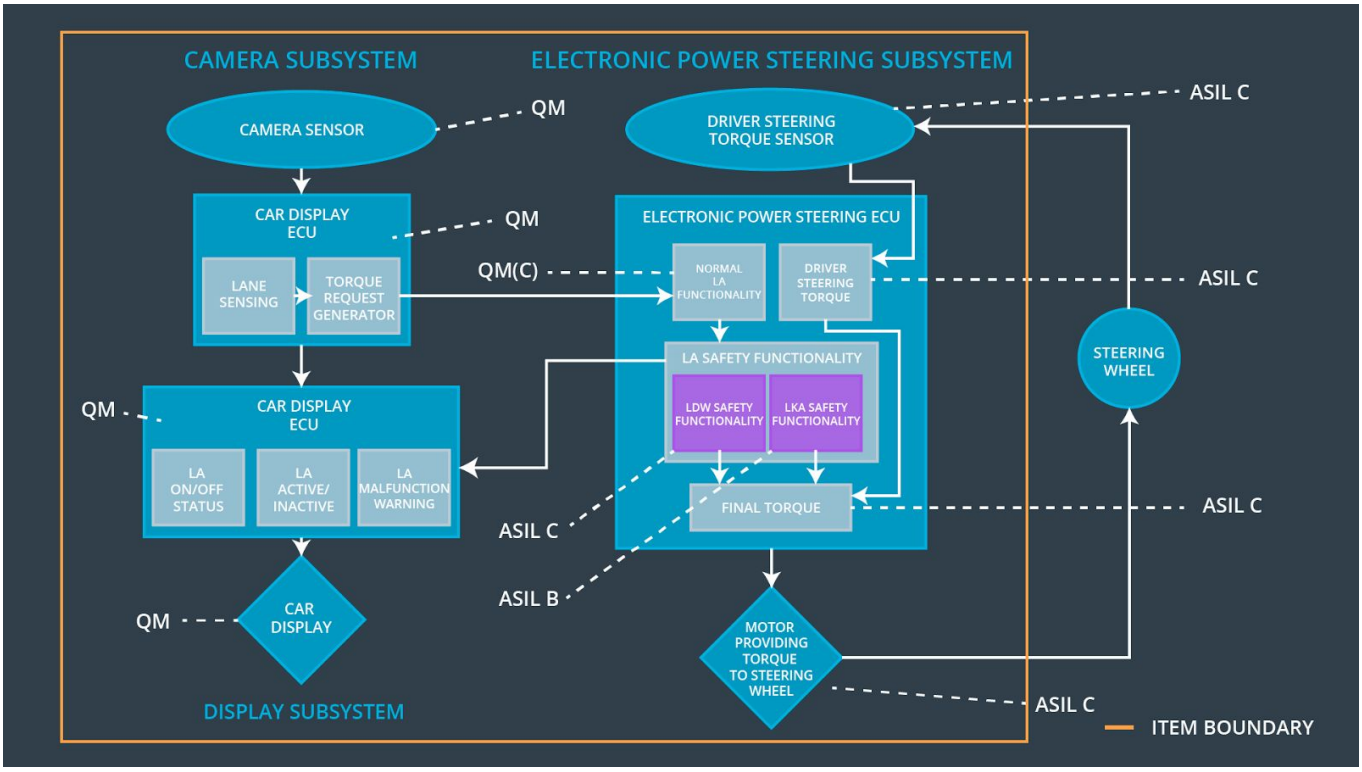
Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration.	C	500 ms	Turn off function.

Refined System Architecture from Functional Safety Concept

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

Diagram 1 : [Refinement of the 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	Captures images within its field of view.
Camera Sensor ECU - Lane Sensing	Takes image input from the Camera Sensor to perform road lane detection and pass this information to both the Car Display ECU and the Camera Sensor ECU - Torque request generator.
Camera Sensor ECU - Torque request generator	Takes road lane detection / position information as input and passes these as parameters to the EPS ECU - Normal Lane Assistance

	Functionality.
Car Display	Takes data input from Car Display ECU to display status and warning information to the driver.
Car Display ECU - Lane Assistance On/Off Status	The LKA Status displays On / Off when the steering assistance function is activated / deactivated.
Car Display ECU - Lane Assistant Active/Inactive	The LDW displays Active / Inactive when the steering wheel vibration function is activated / deactivated.
Car Display ECU - Lane Assistance malfunction warning	Warning display is activated / deactivated by the EPS ECU - LDW Safety Functionality and EPS ECU - LKA Safety Functionality.
Driver Steering Torque Sensor	Takes Steering Wheel data input and outputs to the EPS ECU - Driver Steering Torque.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Takes Steering Wheel movement information and outputs torque information representing the Driver's force applied to the Steering Wheel.
EPS ECU - Normal Lane Assistance Functionality	Processes Torque Requests sent from the Camera Sensor ECU - Torque request generator and sends new torque values to the EPS ECU - LDW Safety Functionality and EPS ECU - LKA Safety Functionality.
EPS ECU - Lane Departure Warning Safety Functionality	Assess if the Max_Torque_Amplitude and / or the Max_Torque_Frequency limits have been exceeded. If limit is breached appropriate values are then sent to : 1. EPS ECU - Final Torque function 2. Car Display ECU - Lane Assistant Active/Inactive 3. Car Display ECU - Lane Assistance malfunction warning
EPS ECU - Lane Keeping Assistant Safety Functionality	Assess if the Max_Duration limit has been exceeded and passes appropriate value to the EPS ECU - Final Torque function.

	If limit is breached appropriate values are then sent to : 1. EPS ECU - Final Torque function 2. Car Display ECU - Lane Assistance On/Off Status 3. Car Display ECU - Lane Assistance malfunction warning
EPS ECU - Final Torque	Fuses torque values from the EPS ECU - Driver Steering Torque, EPS ECU - Lane Departure Warning Safety Functionality and the EPS ECU - Lane Keeping Assistant Safety Functionality and outputs final torque value to be the Motor.
Motor	Motor is an actuator that applies final torque value provided by the EPS ECU - Final 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	LDW Safety block	

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 electronic power steering Torque’ component is below ‘Max_Torque_Amplitude.	C	50 ms	LDW Safety block	LDW torque request amplitude 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	LDW torque request amplitude shall be set to zero.
Technical Safety Requirement 03	As soon as a failure is detected, the LDW Safety module shall deactivate the LDW feature and the ‘LDW_Torque_Request’ shall be set to zero.	C	50 ms	LDW Safety block	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 ECU to turn on a warning light.	C	50 ms	LDW Safety block, LA Malfunction Warning block	LDW 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. Note : The functional safety standard ISO 26262 only requires avoiding latent faults for items labeled ASIL C or D.	A	Length of vehicle ignition cycle	Safety Startup block	N/A

[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 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 block	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	LDW torque request frequency shall be set to zero.
Technical Safety Requirement 03	As soon as a failure is detected, the LDW Safety module shall deactivate the LDW feature and the 'LDW_Torque_Request' shall be set to zero.	C	50 ms	LDW Safety block	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 ECU to turn on a warning light.	C	50 ms	LDW Safety block, LA Malfunction Warning block	LDW torque request frequency 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. Note : The functional safety standard ISO 26262 only requires avoiding latent faults for items labeled ASIL C or D.	A	Length of vehicle ignition cycle	Safety Startup block	N/A

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 'LKA_Torque_Request' sent to the 'Final electronic power steering Torque' component is applied for a time span below 'Max_Duration.	C	50 ms	LKA Safety block	LKA torque request duration shall be set to zero.
Technical Safety Requirement 02	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	C	50 ms	Data Transmission Integrity Check	LKA torque request duration shall be set to zero.
Technical Safety Requirement 03	As soon as a failure is detected, the LKA Safety module shall deactivate the LKA feature and the 'LKA_Torque_Request' shall be set to zero.	C	50 ms	LKA Safety block	LKA torque request duration shall be set to zero.
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 ECU to turn on a warning light.	C	50 ms	LKA Safety block, LA Malfunction Warning block	LKA torque request duration 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. Note : The functional safety standard ISO 26262 only requires avoiding latent faults for items labeled ASIL C or D.	A	Length of vehicle ignition cycle	Safety Startup block	N/A

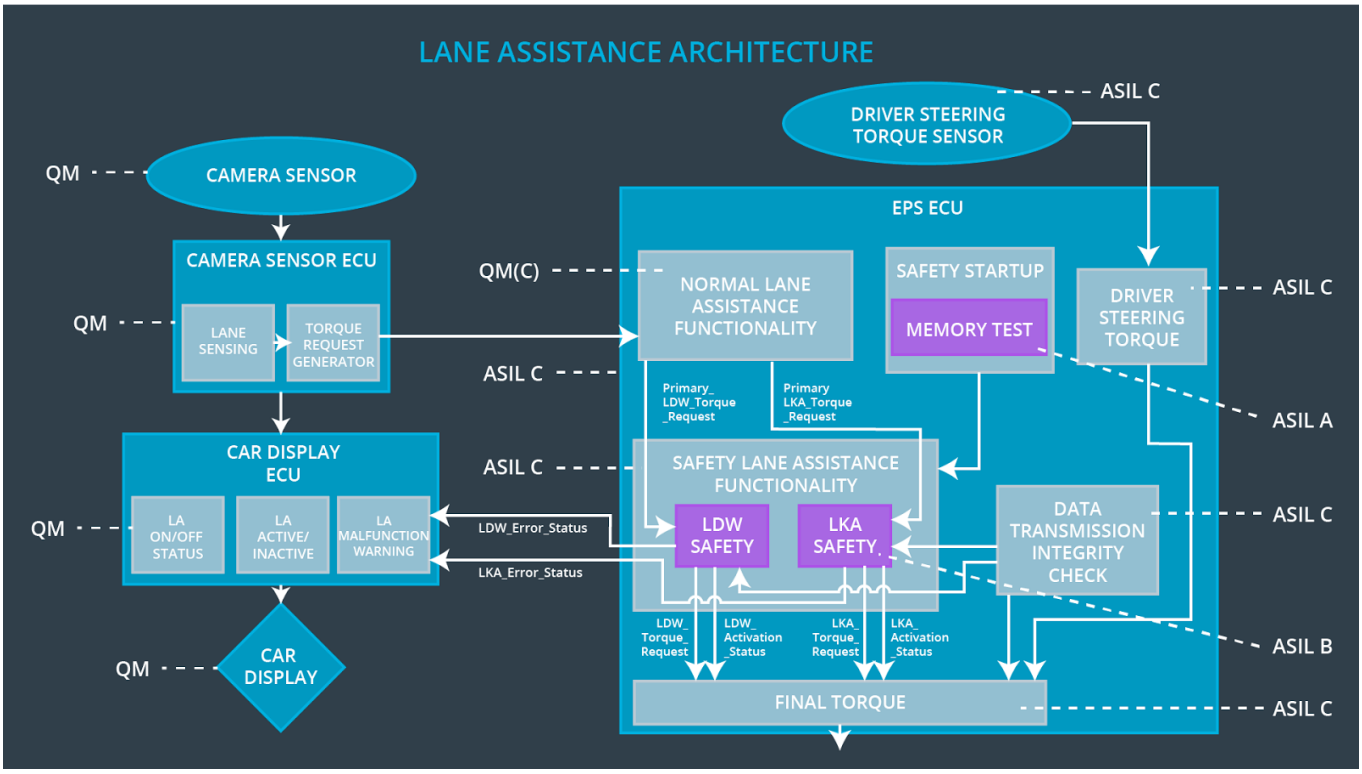
Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:

[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.]

Diagram 2 : [Refinement of the System Architecture]



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]

For the Lane Assistance 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.]

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01-01	Turn off function.	Steering oscillation torque amplitude is above Max_Torque_Amplitude.	Yes.	LDW Active / Inactive display indicates Inactive. LA Malfunction Warning display light is On.
WDC-01-02	Turn off function.	Steering oscillation torque amplitude is above Max_Torque_Frequency.	Yes.	LDW Active / Inactive display indicates Inactive. LA Malfunction Warning display light is On.
WDC-02-01	Turn off function.	Lane keeping assistance torque applied time length is above Max_Duration.	Yes.	LKA On / Off Status display indicates Off. LA Malfunction Warning display light is On.