Elektrobit

UDACITY

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
28AUG17	1.0	Jim Reynolds	First version

Table of Contents

Table of Contents

Purpose of the Technical Safety Concept

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

Inputs to the Technical Safety Concept

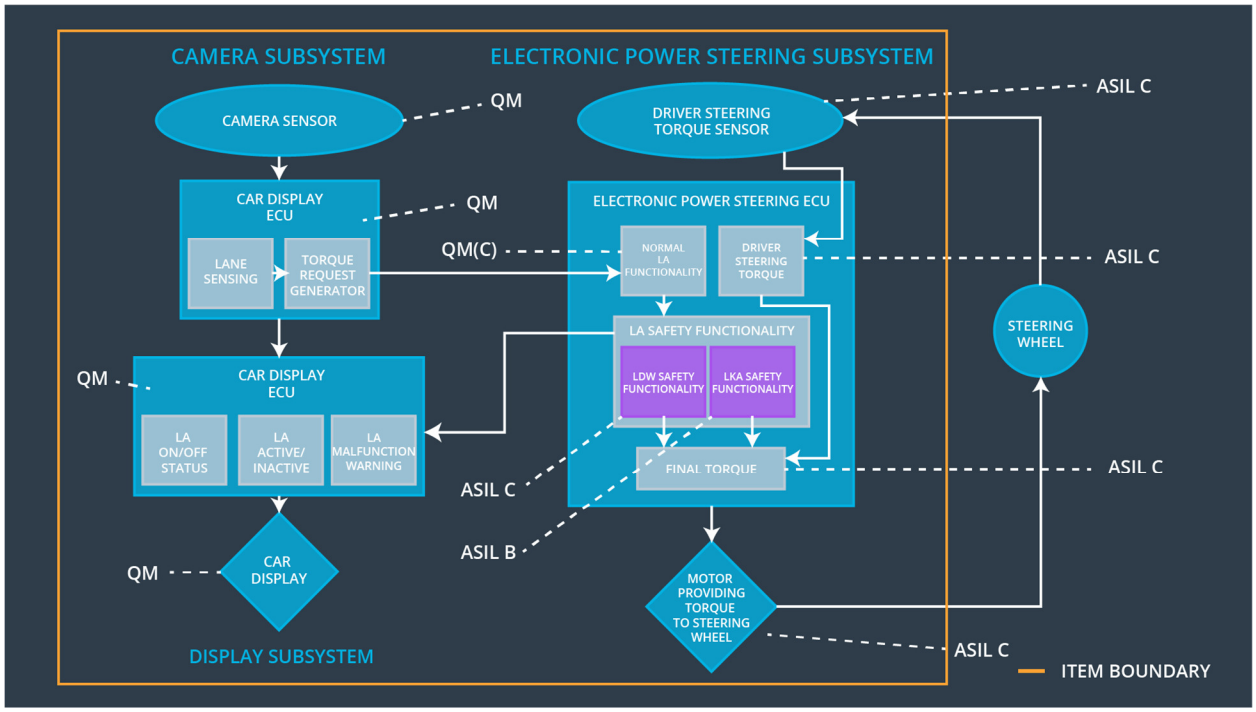
Functional Safety Requirements

[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	50ms	Lane keeping item output torque = 0
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Frequency	C	50ms	Lane keeping item output torque = 0
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	Lane keeping item output torque = 0
Functional Safety Requirement 02-02	The lane keeping item shall ensure that the total absolute steering angle does not exceed Max_Steering_Angle(Vehicle_Speed)	C	50ms	Lane keeping item output torque = 0
Functional Safety Requirement	The lane keeping item shall ensure that the rate-of-change of steering angle does not	C	50ms	Lane keeping item output torque = 0

02-03	exceed Max_Steering_Rate(Vehicle_Speed)			

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	A sensor that outputs an image of the scene in front of the vehicle
Camera Sensor ECU - Lane Sensing	A control module software feature that processes an image and identifies the lanes lines for the current lane, with respect to the position of the vehicle
Camera Sensor ECU - Torque request generator	A control module software feature that processes the vehicles position and trajectory with respect to the position and trajectory of the, and issues a torque request to alert the driver or correct the vehicle trajectory

Car Display	An actuator that displays information and messages to the driver via warning lamps or LCD display
Car Display ECU - Lane Assistance On/Off Status	A control module feature that displays whether the lane assistance feature is currently on or off (on means determining the lane position and whether to provide torque)
Car Display ECU - Lane Assistant Active/Inactive	A control module feature that displays whether the lane assistance feature is currently active or inactive (active means currently applying a nonzero torque)
Car Display ECU - Lane Assistance malfunction warning	An control module feature that displays a warning message if the lane assistance feature has experienced a malfunction
Driver Steering Torque Sensor	A sensor that outputs the torque that the driver is applying to the steering wheel
Electronic Power Steering (EPS) ECU - Driver Steering Torque	A control module feature that calculates the amount of steering torque being applied by the driver via the steering wheel
EPS ECU - Normal Lane Assistance Functionality	A control module feature that calculates the nominal amount of torque to apply, based on the driver steering torque and torque request from the camera sensor ECU
EPS ECU - Lane Departure Warning Safety Functionality	A control module feature that monitors the frequency and amplitude of the torque request for the LDW feature and limits both to a maximum; moreover, the feature will indicate a malfunction if the limits are exceeded
EPS ECU - Lane Keeping Assistant Safety Functionality	A control module feature that monitors the duration of the torque request for the LKA feature and limitsit to a maximum; moreover, the feature will indicate a malfunction if the limit is exceeded
EPS ECU - Final Torque	A control module feature that applies the arbitrated final torque, after both safety features, to the motor
Motor	An actuator that adds torque to the steering system in either direction (clockwise or counterclockwise)

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		

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	50ms	Electronic Power Steering ECU - LDW Safety Functionality	LDW_Torque_Request = 0
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	50ms	Electronic Power Steering ECU - LDW Safety Functionality	LDW_Torque_Request = 0
Technical Safety Requirement	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the 'LDW_Torque_Request'	C	50ms	Electronic Power Steering ECU - LDW Safety	LDW_Torque_Request = 0

03	shall be set to zero.			Functionality	
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50ms	Electronic Power Steering ECU - LDW Safety Functionality	LDW_Torque_Request = 0
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	Electronic Power Steering ECU – Safety Startup	LDW_Torque_Request = 0

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 electronic power steering Torque' component is below 'Max_Torque_Frequency.	C	50ms	Electronic Power Steering ECU - LDW Safety Functionality	LDW_Torque_Request = 0
Technical Safety Requirement	As soon as the LDW function deactivates the LDW feature, the	C	50ms	Electronic Power Steering ECU	LDW_Torque_Request

02	'LDW Safety' software block shall send a signal to the car display ECU to turn on a warning light.			- LDW Safety Functionality	= 0
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	50ms	Electronic Power Steering ECU - LDW Safety Functionality	LDW_Torque_Request = 0
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50ms	Electronic Power Steering ECU - LDW Safety Functionality	LDW_Torque_Request = 0
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	Electronic Power Steering ECU – Safety Startup	LDW_Torque_Request = 0

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 02-01 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 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 greater than 0 for no more than 'Max_Duration.	B	500ms	Electronic Power Steering ECU - LKA Safety Functionality	LKA_Torque_Request = 0
Technical Safety Requirement 02	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	500ms	Electronic Power Steering ECU - LKA Safety Functionality	LKA_Torque_Request = 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	500ms	Electronic Power Steering ECU - LKA Safety Functionality	LKA_Torque_Request = 0
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	B	500ms	Electronic Power Steering ECU - LKA Safety Functionality	LKA_Torque_Request = 0
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	Electronic Power Steering ECU – Safety Startup	LKA_Torque_Request = 0

Functional Safety Requirement 02-02 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 02-02	The lane keeping item shall ensure that the total absolute steering angle does not exceed Max_Steering_Angle(Vehicle_Speed)	X		

Technical Safety Requirements related to Functional Safety Requirement 02-02 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' is less than a torque resulting in Max_Steering_Angle(Vehicle_Speed).	C	50ms	Electronic Power Steering ECU - LKA Safety Functionality	LKA_Torque_Request = 0
Technical Safety Requirement 02	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	50ms	Electronic Power Steering ECU - LKA Safety Functionality	LKA_Torque_Request = 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.	C	50ms	Electronic Power Steering ECU - LKA Safety Functionality	LKA_Torque_Request = 0
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	C	50ms	Electronic Power Steering ECU - LKA Safety Functionality	LKA_Torque_Request = 0
Technical Safety Requirement 05	The validity and integrity of the data transmission for Steering_Angle signal shall be ensured.	C	50ms	Electronic Power Steering ECU - LKA Safety Functionality	LKA_Torque_Request = 0
Technical	The validity and integrity of the	C	50ms	Electronic	LKA_Torqu

Safety Requirement 05	data transmission for Vehicle_Speed signal shall be ensured.			Power Steering ECU - LKA Safety Functionality	e_Request = 0
Technical Safety Requirement 07	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Electronic Power Steering ECU – Safety Startup	LKA_Torque_Request = 0

Functional Safety Requirement 02-03 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 02-03	The lane keeping item shall ensure that the rate-of-change of steering angle does not exceed Max_Steering_Rate(Vehicle_Speed)	X		

Technical Safety Requirements related to Functional Safety Requirement 02-03 are:

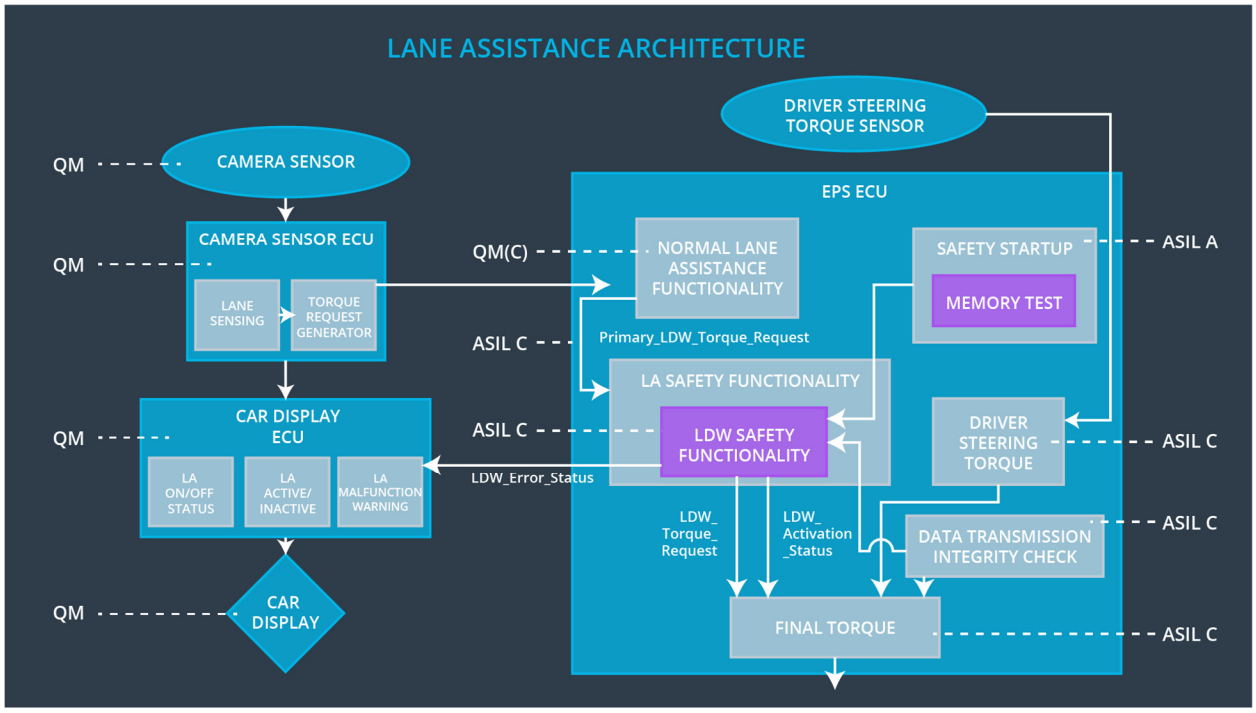
ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01	The LKA safety component shall ensure that the 'LKA_Torque_Request' sent to the 'Final electronic power steering Torque' is less than a torque resulting in Max_Steering_Rate(Vehicle_Speed).	C	50ms	Electronic Power Steering ECU - LKA Safety Functionality	LKA_Torque_Request = 0
Technical Safety Requirement 02	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	50ms	Electronic Power Steering ECU - LKA Safety Functionality	LKA_Torque_Request = 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.	C	50ms	Electronic Power Steering ECU - LKA Safety Functionality	LKA_Torque_Request = 0
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	C	50ms	Electronic Power Steering ECU - LKA Safety Functionality	LKA_Torque_Request = 0
Technical Safety Requirement 05	The validity and integrity of the data transmission for Steering_Angle signal shall be ensured.	C	50ms	Electronic Power Steering ECU - LKA Safety Functionality	LKA_Torque_Request = 0
Technical Safety Requirement 05	The validity and integrity of the data transmission for Vehicle_Speed signal shall be ensured.	C	50ms	Electronic Power Steering ECU - LKA Safety Functionality	LKA_Torque_Request = 0
Technical Safety Requirement 07	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Electronic Power Steering ECU – Safety Startup	LKA_Torque_Request = 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

All technical safety requirements are allocated to the Electronic Power Steering ECU, as noted in the tables above.

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	System disabled until module reset	Malfunction_01	Yes, immediately	1. Audible Chime 2. Pop-up message on instrument cluster
WDC-02	System disabled until module reset	Malfunction_02	Yes, immediately	1. Audible Chime 2. Pop-up message on

				instrument cluster
WDC-03	System disabled until module reset	Malfunction_03	Yes, immediately	1. Audible Chime 2. Pop-up message on instrument cluster
WDC-04	System disabled until module reset	Malfunction_04	Yes, immediately	1. Audible Chime 2. Pop-up message on instrument cluster
WDC-05	System disabled until module reset	Malfunction_05	Yes, immediately	1. Audible Chime 2. Pop-up message on instrument cluster