Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 1.0
Released on 2017-11-10

Document history

Date	Version	Editor	Description
November 10, 2017	1.0	Sampayo, Sebastián L.	First submission

Table of Contents

Purpose of the Technical Safety Concept

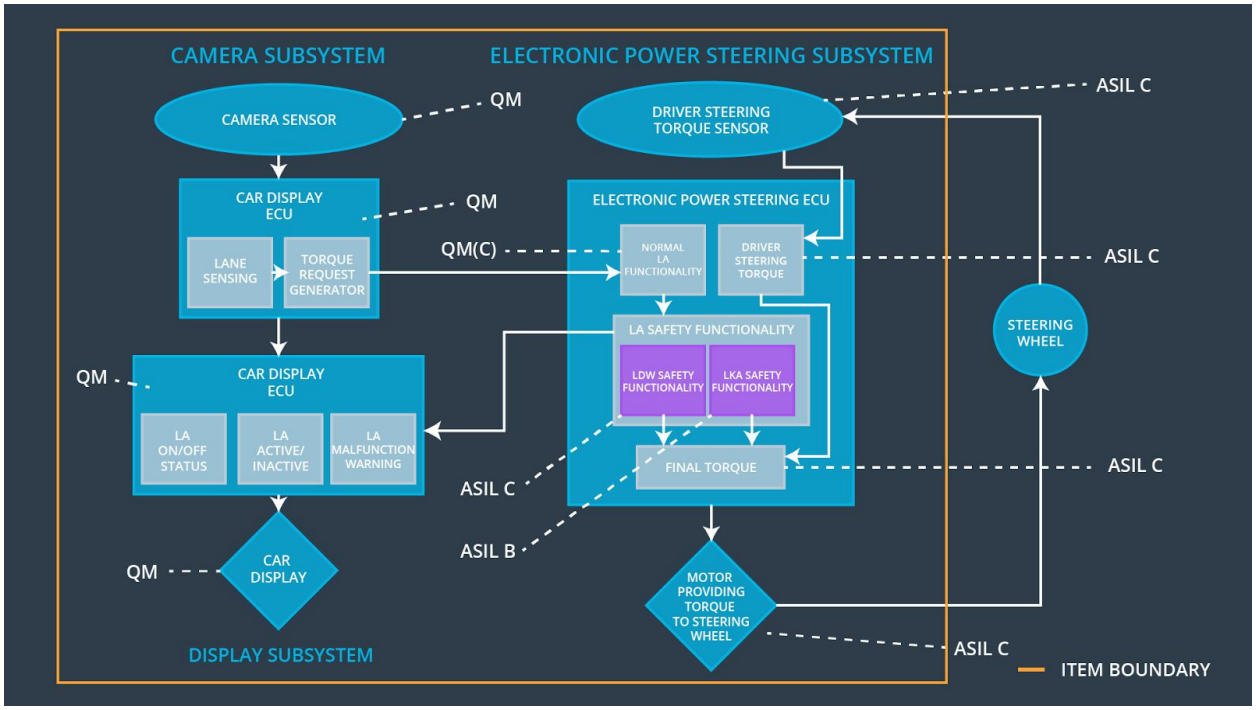
[What is the purpose of a technical safety concept?]
The purpose of a Technical Safety Concept is to define new technical requirements and allocate them to our system architecture. The difference with the Functional Safety Concept is that the latter, considers an item from a bird's eye view, while the Technical Safety Concept is more concrete.

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 Electronic Power Steering ECU shall ensure that the lane departure warning oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	LDW off
Functional Safety Requirement 01-02	The Electronic Power Steering ECU shall ensure that the lane departure warning oscillating torque frequency is below Max_Torque_Frequency	C	50 ms	LDW off
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	LKA off

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Provides raw images of the road and the environment ahead of the vehicle.
Camera Sensor ECU - Lane Sensing	Responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake.
Camera Sensor ECU - Torque request generator	Responsible for calculating the required torque to be applied to the steering wheel in order to stay on the center of the lane, based on the information from the Lane Sensing component, and sending it to the Electronic Power Steering ECU.
Car Display	Displays warning/alert messages and whether the subsystems are on/off.

Car Display ECU - Lane Assistance On/Off Status	Displays the current status (on/off) of the Lane Assistance item based on the signals received by the Electronic Power Steering ECU.
Car Display ECU - Lane Assistant Active/Inactive	Displays the current status (active/inactive) of the Lane Assistance item based on the signals received by the Electronic Power Steering ECU.
Car Display ECU - Lane Assistance malfunction warning	Displays a warning message and lights when the Lane Assistance item has a malfunction.
Driver Steering Torque Sensor	Responsible for measuring the torque provided to the steering wheel.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Responsible for adding the appropriate amount of torque based on a lane assistance system torque request.
EPS ECU - Normal Lane Assistance Functionality	Handles torque requests from the camera sensor ECU.
EPS ECU - Lane Departure Warning Safety Functionality	Handles torque requests from the camera subsystem and limits the amplitude and frequency to comply with the LDW safety requirements.
EPS ECU - Lane Keeping Assistant Safety Functionality	Handles torque requests from the camera subsystem and limits the amount of time turned on to comply with the LKA safety requirements.
EPS ECU - Final Torque	Calculates the final torque based on all the EPS components and torque requests.
Motor	The physical element that actually applies the torque to the steering wheel.

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	50 ms	LDW safety component	LDW output torque shall be set 0 (LDW off)
Technical Safety	As soon as the LDW function deactivates the LDW feature,	C	50 ms	LDW safety component	LDW output torque shall be set 0

Requirement 02	the 'LDW Safety' software block shall send a signal to the car display ECU to turn on a warning light.				(LDW off)
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 component	LDW output torque shall be set 0 (LDW off)
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 component	N/A
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	Memory Test of the Safety Startup component	LDW output torque shall be set 0 (LDW off)

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	50 ms	LDW safety component	LDW output torque shall be set 0 (LDW off)
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 component	LDW output torque shall be set 0 (LDW off)
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 component	LDW output torque shall be set 0 (LDW off)
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 component	N/A
Technical	Memory test shall be conducted	A	Ignition	Memory Test	LDW

Safety Requirement 05	at start up of the EPS ECU to check for any faults in memory.		cycle	of the Safety Startup component	output torque shall be set 0 (LDW off)

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 02-1 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		

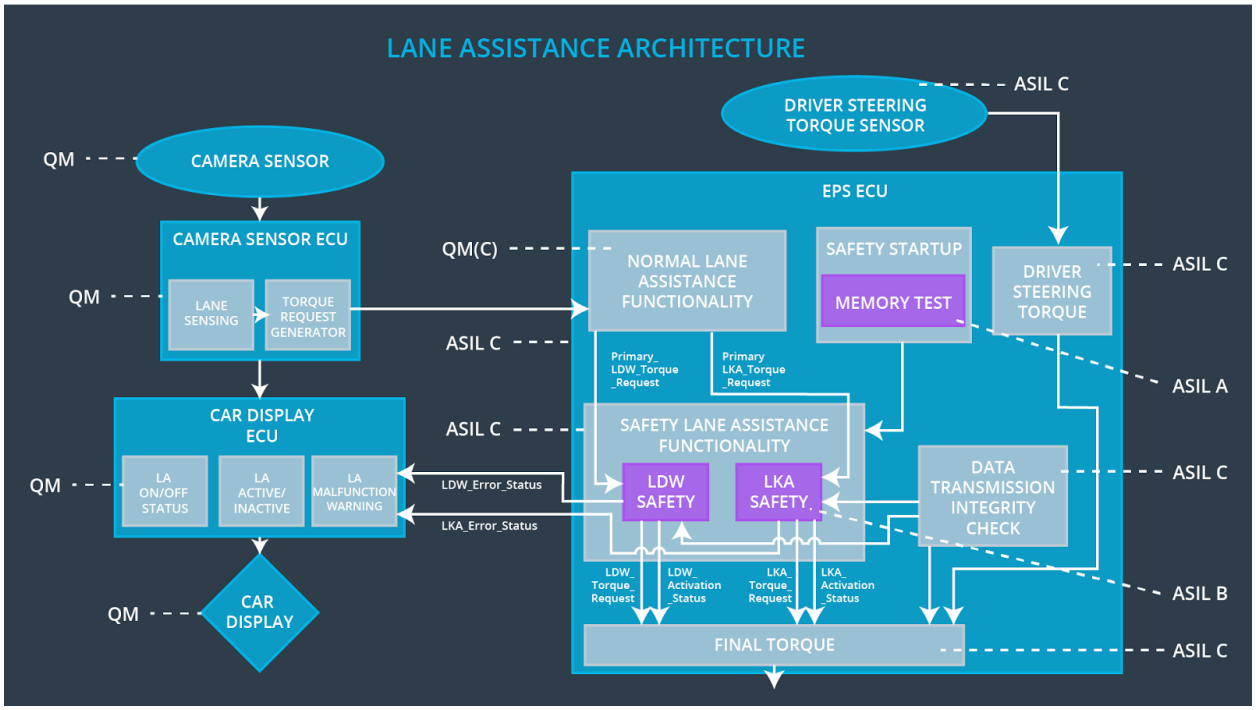
Technical Safety Requirements related to Functional Safety Requirement 02-01 are:

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 duration of the 'LKA_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Duration'.	B	500 ms	LKA safety component	LKA output torque shall be set 0 (LDW off)
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	500 ms	LKA safety component	LKA output torque shall be set 0 (LKA off)
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 component	LKA output torque shall be set 0 (LKA off)
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	B	500 ms	Data Transmission Integrity Check component	N/A
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	Memory Test of the Safety Startup component	LKA output torque shall be set 0 (LDW off)

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 Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off LDW functionality	Malfunction_01 Malfunction_02	Yes	Yellow light on the car display
WDC-02	Turn off LKA functionality	Malfunction_03	Yes	Yellow light on the car display