Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 1.2

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
06/23/19	1.0	Adam Gotlib	First draft
06/23/19	1.1	Adam Gotlib	
06/23/19	1.2	Adam Gotlib	Removed template-specific parts of the document

Table of Contents

Purpose of the Technical Safety Concept

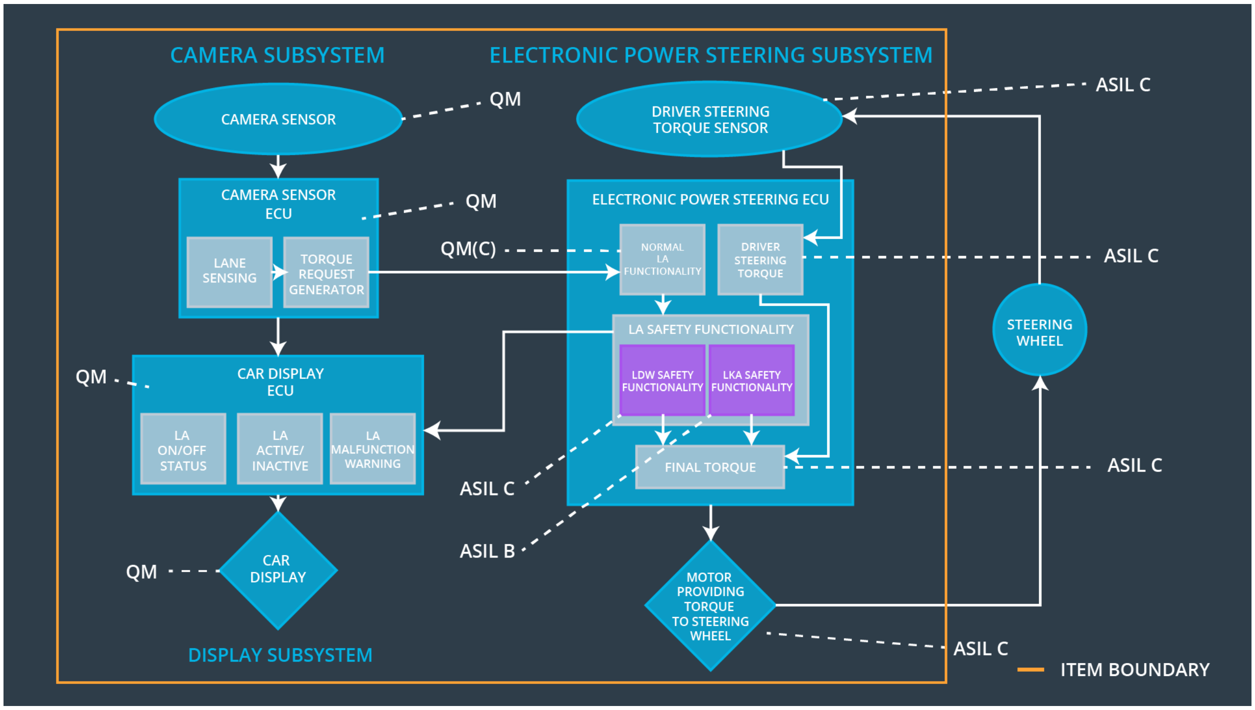
The Technical Safety Concept serves the purpose of deriving more detailed Technical Safety Requirements from the Functional Safety Requirements defined in the Functional Safety Concept.

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	The LDW function shall deactivate and display a visual warning to the driver.
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	The LDW function shall deactivate and display a visual warning to the driver.
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied only for Max_Duratoin.	B	500 ms	The LKA function shall deactivate and display a visual warning to the driver.

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Captures images in front of the vehicle.
Camera Sensor ECU - Lane Sensing	Analyses captured images and determines when the vehicle leaves the lane by mistake.
Camera Sensor ECU - Torque request generator	Generates lane keeping torque and lane departure oscillating torque request when the vehicle leaves the lane by mistake.
Car Display	Displays visual cues for the driver, informing them of functioning of the system.
Car Display ECU - Lane Assistance On/Off Status	Displays on/off status of the Lane Assistance item.
Car Display ECU - Lane Assistant Active/Inactive	Displays active/inactive status of LDW and LKA functions.
Car Display ECU - Lane Assistance malfunction warning	Informs the driver when LDW or LKA malfunction.
Driver Steering Torque Sensor	Measures the torque provided by the driver.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Reads the measured torque from the Driver Steering Torque Sensor.
EPS ECU - Normal Lane Assistance Functionality	Estimates the required amount of additional torque to be applied based on a lane assistance system torque request and the torque provided by the driver.
EPS ECU - Lane Departure Warning Safety Functionality	Ensures that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude and the lane departure oscillating torque frequency is below Max_Torque_Frequency.
EPS ECU - Lane Keeping Assistant Safety Functionality	Ensures that the lane keeping assistance torque is applied only for Max_Duratoin.
EPS ECU - Final Torque	Passes torque request to the Motor.
Motor	Applies additional 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 compontent 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 Functionality	The LDW function shall deactivate and display a visual warning to the driver.
Technical Safety Requirement 02	The validity and integrity of the data transmission for LDW_Torque_Request signal shall be ensured.	C	50 ms	LDW Safety Functionality	The LDW function shall deactivate and display a visual warning to the driver.
Technical Safety Requirement 03	As soon as a failure is detected by the LDW function, it shall deactiveate the LDW feature and the LDW_Torque_Request shall be set to zero.	C	50 ms	LDW Safety Functionality	The LDW function shall deactivate and display a visual warning to the driver.
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 Functionality	The LDW function shall deactivate and display a visual warning to the driver.
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	LDW Safety Functionality	The LDW function shall deactivate and display a visual warning to the driver.

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 compontent 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 Functionality	The LDW function shall deactivate and display a visual warning to the driver.
Technical Safety Requirement 02	The validity and integrity of the data transmission for LDW_Torque_Request signal shall be ensured.	C	50 ms	LDW Safety Functionality	The LDW function shall deactivate and display a visual warning to the driver.
Technical Safety Requirement 03	As soon as a failure is detected by the LDW function, it shall deactiveate the LDW feature and the LDW_Torque_Request shall be set to zero.	C	50 ms	LDW Safety Functionality	The LDW function shall deactivate and display a visual warning to the driver.
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 Functionality	The LDW function shall deactivate and display a visual warning

					to the driver.
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	LDW Safety Functionality	The LDW function shall deactivate and display a visual warning to the driver.

Lane Keeping Assistance (LKA) Requirements:

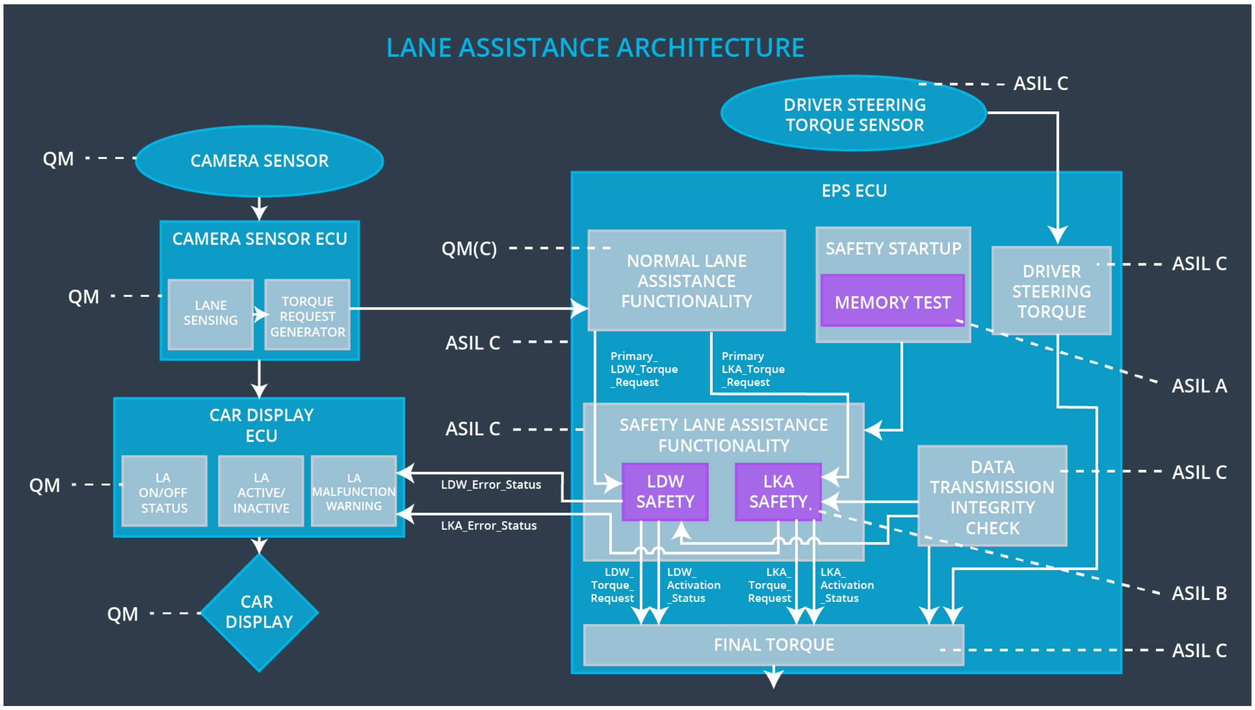
Functional Safety Requirement 02-1 with its associated system elements
(derived in the functional safety concept)

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 compontent shall ensure that the LKA_Torque_Request sent to the Final EPS Torque component has non-zero value for only Max_Duration.	B	500 ms	LKA Safety Functionality	The LKA function shall deactivate and display a visual warning to the driver.
Technical Safety Requirement 02	The validity and integrity of the data transmission for LKA_Torque_Request signal shall be ensured.	B	500 ms	LKA Safety Functionality	The LKA function shall deactivate and display a visual warning to the driver.
Technical Safety Requirement 03	As soon as a failure is detected by the LKA function, it shall deactiveate the LKA feature and the LKA_Torque_Request shall be set to zero.	B	500 ms	LKA Safety Functionality	The LKA function shall deactivate and display a visual warning to the driver.
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.	B	500 ms	LKA Safety Functionality	The LKA function shall deactivate and display a visual warning to the driver.
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	LKA Safety Functionality	The LKA function shall deactivate and display a visual warning to the driver.

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 EPS ECU component.

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Deactivate LDW function.	Malfunction_01 Malfunction_02	YES	Visual display
WDC-02	Deactivate LKA function.	Malfunction_03	YES	Visual display