Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
02/03/2018	0.1	Michael Scharf	Initial attempt
02/03/2018	0.2	Michael Scharf	Fill out the sheet
02/03/2018	1.0	Michael Scharf	Internal Review and smaller fixes.
02/04/2018	2.0	Michael Scharf	Correct review findings after submission.

Table of Contents

Purpose of the Technical Safety Concept

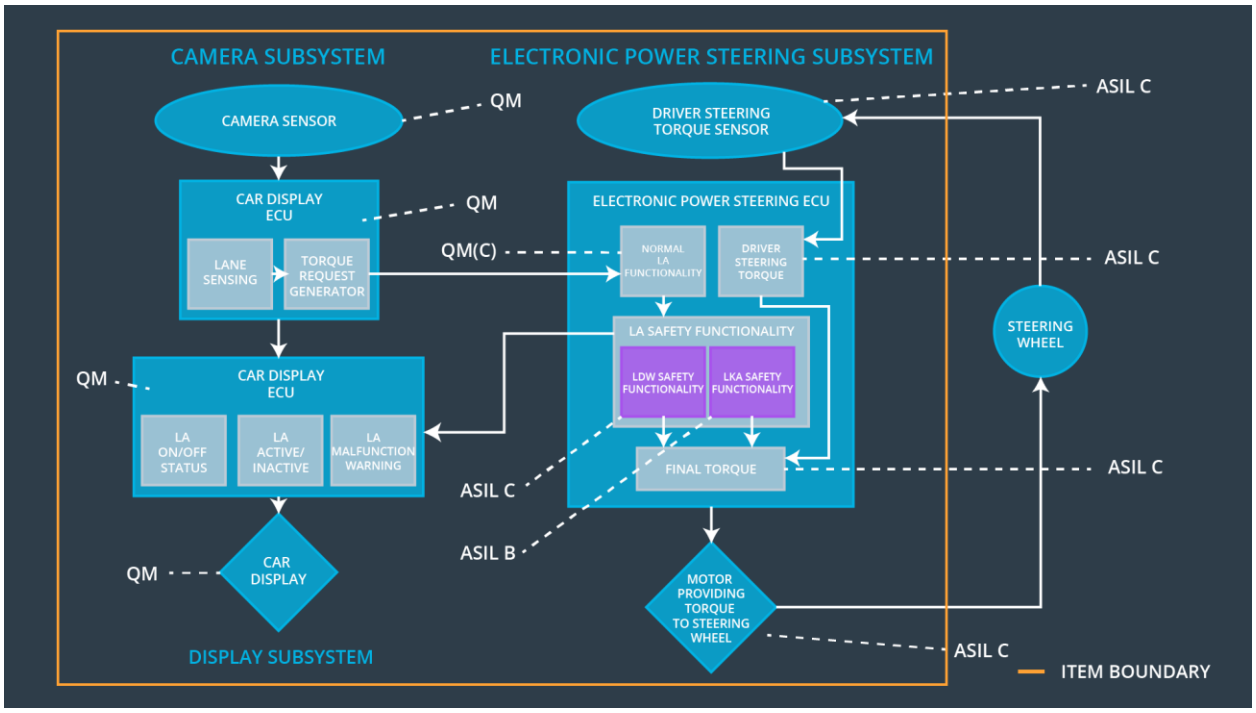
The Technical Safety Concept defines how the subsystems interact at the message level and describes how the ECUs communicate with each other.

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 oscillating torque amplitude requested by the LDW function is below Max_Torque_Amplitude	C	50 ms	LDW will set the oscillating torque amplitude to 0.
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 will set the oscillating torque frequency to 0.
Functional Safety Requirement 02-01	the lane keeping assistance function shall be time limited and the additional steering torque shall end after a given timer interval so that the driver can not misuse the system for autonomous driving	B	500 mS	LKA will set torque to 0.

Refined System Architecture from Functional Safety Concept



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

Functional overview of architecture elements

Element	Description
Camera Sensor	Grab images for further processing in the Camera Sensor ECU.
Camera Sensor ECU - Lane Sensing	Identify the ego lane in images.
Camera Sensor ECU - Torque request generator	Depending on the car position in the ego lane, generate a torque request signal for the EPS ECU.
Car Display	User interface allows to indicate different states/ signals
Car Display ECU - Lane Assistance On/Off Status	Identifies the state of the Lane Assistance. Depending on the state, the On or Off indication is triggered on the car display

Car Display ECU - Lane Assistant Active/Inactive	Identifies the state of the Lane Assistance. Depending on the state, the Active or Inactive indication is triggered on the car display
Car Display ECU - Lane Assistance malfunction warning	Warning indication is triggered on Car Display in case that the ECU receives the signal for a malfunction.
Driver Steering Torque Sensor	Measure the drivers steering torque
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Identification of the drivers steering wheel torque and conversion into the EPS ECU torque range
EPS ECU - Normal Lane Assistance Functionality	Generate a torque amplitude and torque frequency in given borders to generate a LDW.
EPS ECU - Lane Departure Warning Safety Functionality	Insures that the final electronic power steering torque amplitude is below the Max_Torque_Amplitude. If not, the error signal is sent to the Car Display ECU.
EPS ECU - Lane Keeping Assistant Safety Functionality	Insures that the max activation time of the Lane keeping function isn't exceeded.
EPS ECU - Final Torque	Combine the EPS ECU torque and the ECU driver steering torque to a final electronic power steering torque.
Motor	Convert the final electronic power steering torque into a mechanic movement.

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	Camera ECU	Car Display ECU

		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	Resulting torque amplitude is zero
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	Resulting torque amplitude is 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 Component	Resulting torque amplitude is zero
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 (SW)	Resulting torque amplitude is zero
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 (SW)	Resulting torque amplitude is zero

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	Resulting torque amplitude is zero
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	Resulting torque amplitude is 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 Component	Resulting torque amplitude is zero

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 (SW)	Resulting torque amplitude is zero
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 (SW)	Resulting torque amplitude is 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:

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:

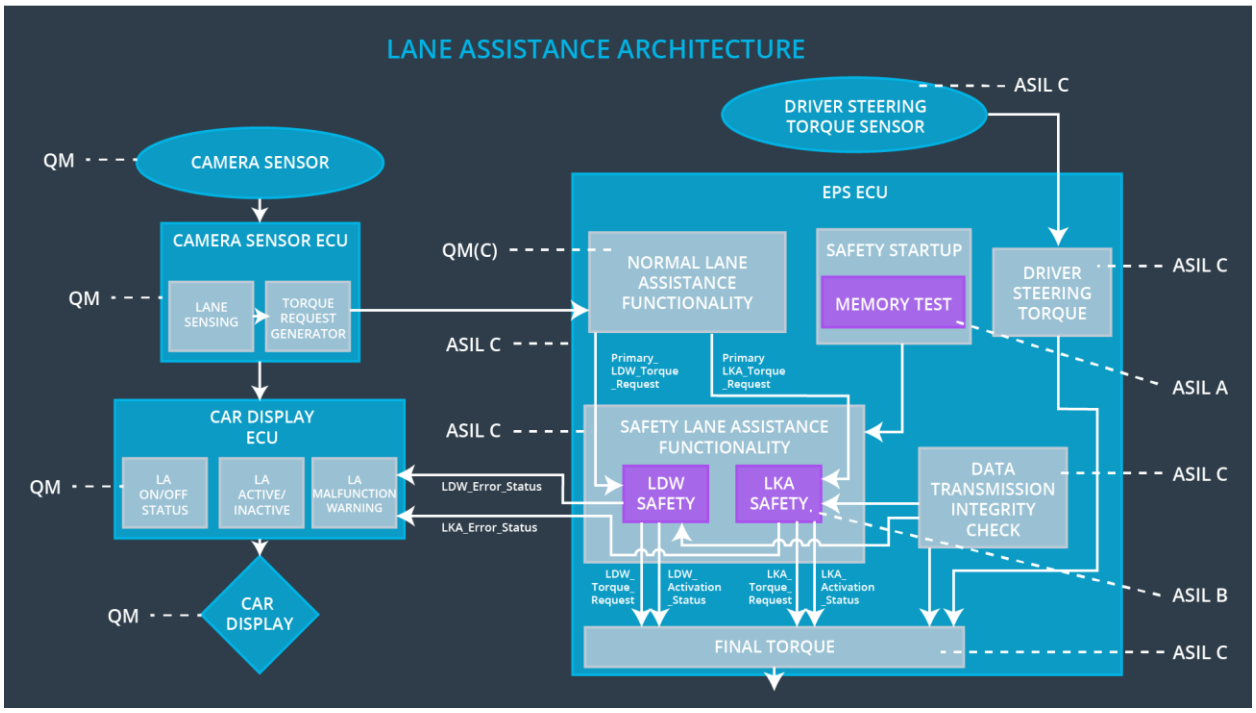
ID	Technical Safety Requirement	A	Fault	Allocation to	Safe State

		SIL	Tolerant Time Interval	Architecture	
Technical Safety Requirement 01	The LKA shall ensure that the ‘lane keeping assistance torque’ sent to the ‘Final electronic power steering Torque’ component is applied only ‘Max_Duration’	B	500 mS	LKA Safety Component	Resulting LKA torque is set to 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	500 mS	LKA Safety Component	Resulting LKA torque is set to 0.
Technical Safety Requirement 03	As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature.	B	500 mS	LKA Safety Component	Resulting LKA torque is set to 0.
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 (SW)	Resulting LKA torque is set to 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	Memory Test (SW)	Resulting LKA torque is 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

The technical safety requirements will be completely full filled inside the EPS ECU.
The LDW Safety Component is in charge to detect a malfunction in LDW and triggers the transition into safe mode.
The LKA Safety Component is in charge to detect a malfunction in LKA and triggers the transition into safe mode.
Data Transmission Integrity Check SW is ensuring the validity and integrity of data transmission for LKA as well as LDW.
The Memory Test SW is checking any faults in memory during start up for LKA as well as LDW.

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off functionality	ECU receives a vibrational	yes	Indication of malfunction via

		torque request beyond the allowed maximum		driver dashboard
WDC-02	Turn off functionality	ECU recognizes timeout of drivers interaction for lane keeping	yes	No automatic lane keeping. Eventually warning notification in drivers dashboard or hint in the manual that driver maintains responsibility for safe operation of the vehicle.