Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
6/23/19	1.0	R.Crane	Initial draft version

Table of Contents

Purpose of the Technical Safety Concept

The Technical Safety Concept document turns functional safety requirements identified in the Functional Safety Concept into technical safety requirements that are determined during the system design. Technical safety requirement allocation to system architecture is identifed.

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	50ms	System turned off
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	System turned 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	500ms	System turned off

Refined System Architecture from Functional Safety Concept

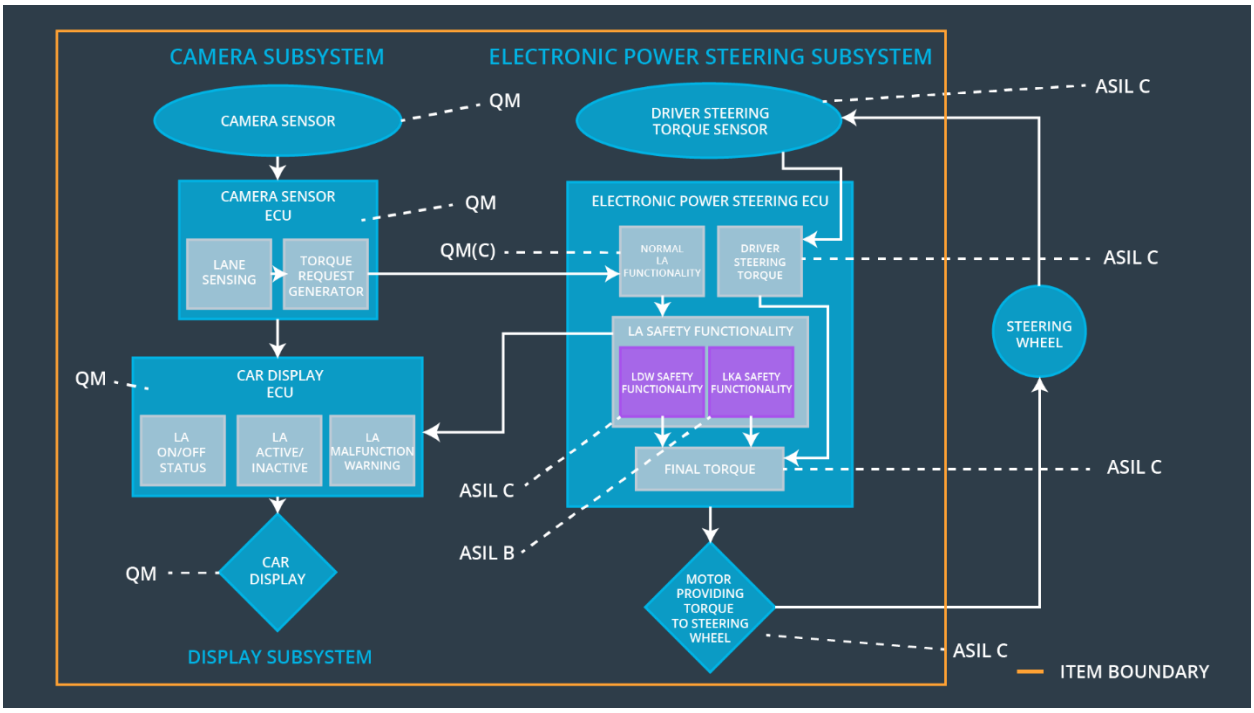


Figure 1. Refined System Architecture

The functional safety requirements for LKA and LDW are derived from ASIL B and C assigned safety goals. They are both allocated to the Power steering ECU. ASIL decomposition creates a single LA Safety Functionality module within the ECU in which two modules can assume the responsibility for meeting the functional safety requirements. These are assumed to be independent. If they were not independent, both would receive ASIL C ratings (the higher).

Functional overview of architecture elements

Element	Description
Camera Sensor	Creates and transmits imagery data of the road surface to an extent that lane lines are visible.
Camera Sensor ECU - Lane Sensing	Determine boundaries of lanes and vehicle position in lane from imagery data.
Camera Sensor ECU - Torque request generator	Generate a request for additional steering torque to move vehicle closer to center of lane.
Car Display	Display activation and enable states to user. Display warning and fault conditions.

Car Display ECU - Lane Assistance On/Off Status	Make requests to display to display state based on system inputs.
Car Display ECU - Lane Assistant Active/Inactive	Make requests to display to display state based on system inputs.
Car Display ECU - Lane Assistance malfunction warning	Make requests to display to display state based on system inputs.
Driver Steering Torque Sensor	Determine existing torque input to steering to compute appropriate amount to set.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	From driver steering torque sensor, provide final torque component with measurement of driver input.
EPS ECU - Normal Lane Assistance Functionality	From the Camera component input, generate normal torque requests for lane keeping assistance.
EPS ECU - Lane Departure Warning Safety Functionality	Validate the torque request meetings safety requirements before forwarding request to final torque component.
EPS ECU - Lane Keeping Assistant Safety Functionality	Validate that the system has been activated for less than the nominal value.
EPS ECU - Final Torque	Synthesize the requested torque values with the driver steering to generate appropriate signal to motor for steering actuation.
Motor	Provide actual torque values to steering system on request.

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	LDW Safety software	The departure warning torque request amplitude shall be set to 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	LDW Safety software	The departure warning torque request amplitude shall be set to zero.
Technical Safety	As soon as a failure is detected by the LDW function, it shall	C	50	LDW Safety software	The departure warning

Requirement 03	deactivate the LDW feature and the 'LDW_Torque_Request' shall be set to zero.				torque request amplitude shall be set to zero.
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50	Data Transmission Integrity Check Component	The departure warning 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.	A	Ignition Cycle	Safety Startup Component	The departure warning torque request amplitude shall be set to 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	The LDW safety component shall	C	50	LDW Safety	The

Safety Requirement 01	ensure that the frequency of the 'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Frequency.			software	departure warning torque request amplitude shall be set to 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	LDW Safety software	The departure warning torque request amplitude shall be set to 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	LDW Safety software	The departure warning torque request amplitude shall be set to zero.
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50	Data Transmission Integrity Check Component	The departure warning 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.	A	Ignition Cycle	Safety Startup Component	The departure warning torque request amplitud

					e shall be set to zero.

Lane Keeping Assistance (LKA) Requirements:

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

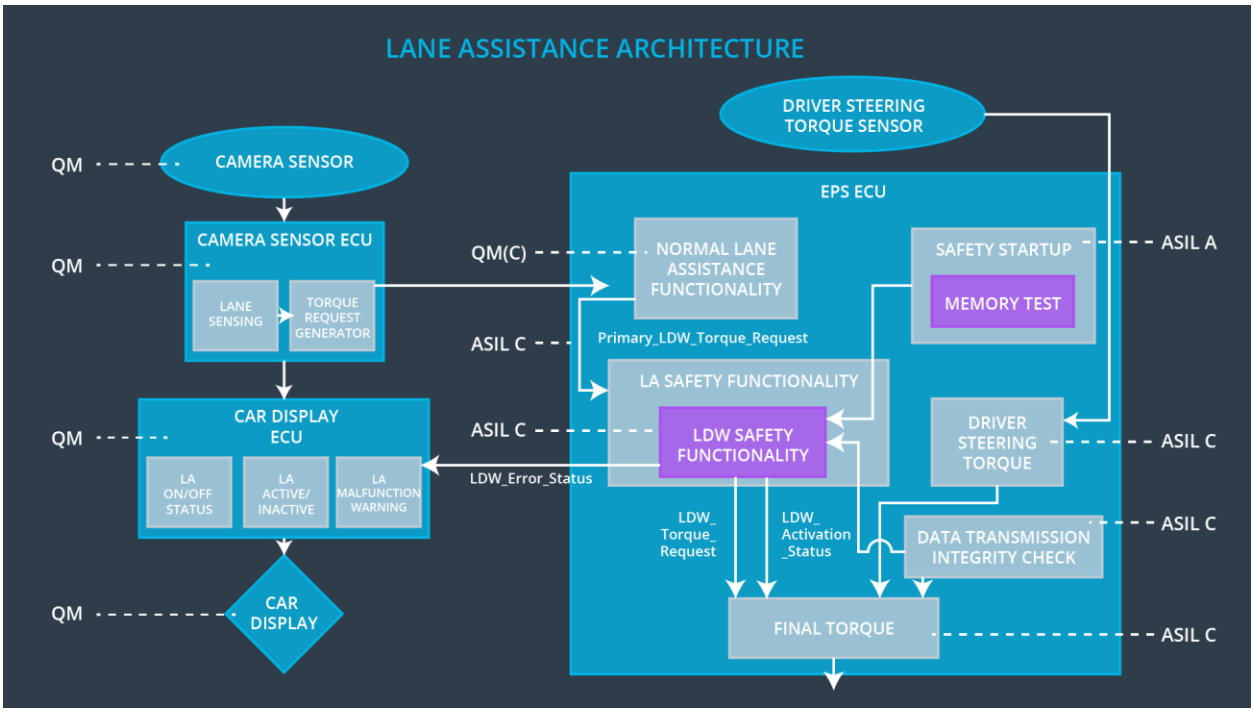
ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	X		

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 'LKA_Torque_Request' sent to the 'Final electronic power steering Torque' component is applied for no longer than MAX_DURATION.	B	500	LKA Safety software	The departure warning torque request amplitude shall be set to zero.
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	LKA Safety software	The departure warning torque request amplitude shall be set to zero.
Technical Safety Requirement	As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and	B	500	LKA Safety software	The departure warning torque

03	the ‘LKA_Torque_Request' shall be set to zero.				request amplitude shall be set to zero.
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	B	500	Data Transmission Integrity Check Component	The departure warning 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.	A	Ignition Cycle	Safety Startup Component	The departure warning torque request amplitude shall be set to zero.

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

All technical safety requirements are allocated to the Electronic Power Steering (EPS) ECU.

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off functionality	Violation of MAX_TORQUE_AMPLITUDE or MAX_TORQUE_FREQUENCY	Yes	Visual indication
WDC-02	Turn off functionality	Violation of MAX_DURATION	Yes	Visual indication