Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 1.0
2019-03-29

Document history

Date	Version	Editor	Description
2019-03-29	1.0	Sergey Morozov	Completed all document sections

Table of Contents

Purpose of the Technical Safety Concept

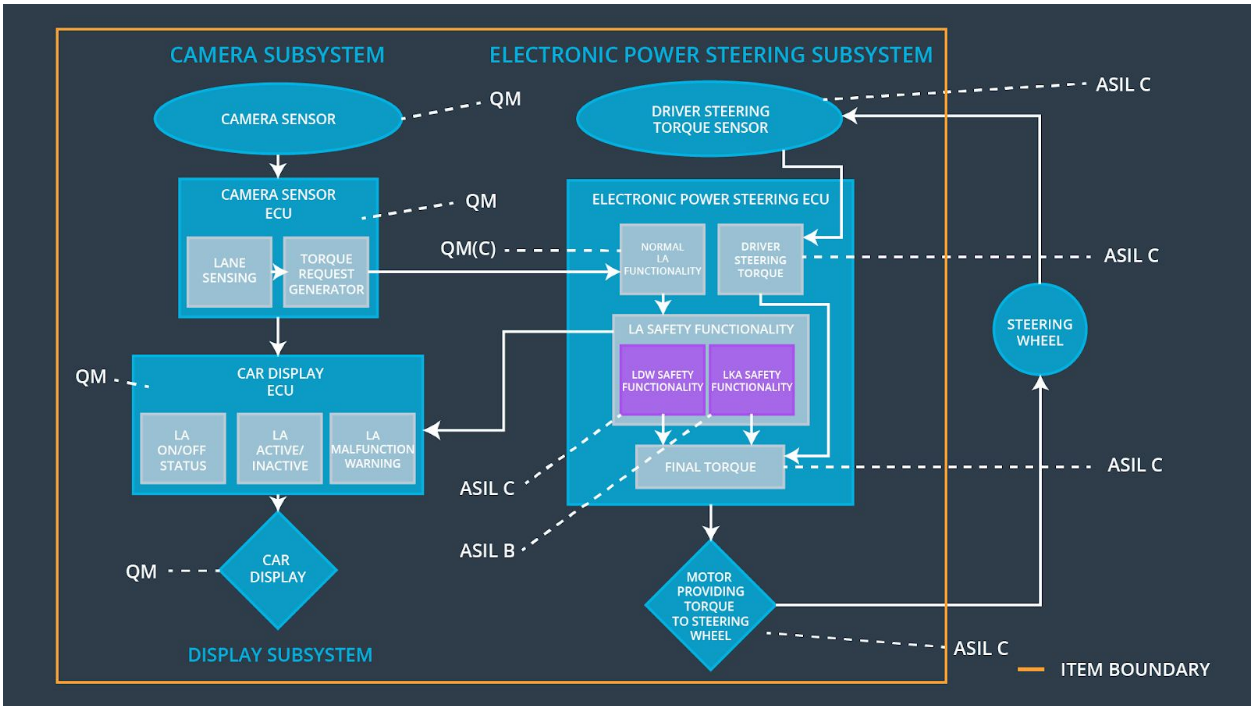
The Technical Safety Concept looks at the technical implementation of the Item. The purpose of the Technical Safety Concept is to turn functional safety requirements into technical safety requirements and allocate those technical safety requirements to the system architecture. The Technical Safety Concept considers the system at a more technical level, thinks about sensors, control units, and actuators. Technical safety requirements are general hardware and software requirements but without getting into specific details.

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 torque is zero. Warning displayed on the Car Display.
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 torque is zero. Warning displayed on the Car Display.
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration.	B	500 mS	The torque is zero. Warning displayed on the Car Display.

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Captures images of the road.
Camera Sensor ECU - Lane Sensing	Detects lane lines on the road based on the camera images.
Camera Sensor ECU - Torque request generator	Generate torque requests based on the information provided by the Camera Sensor ECU - Lane Sensing when identifies that the vehicle accidentally departed its lane.
Car Display	Provides the driver with visual notifications about the current state of the lane assistance item.
Car Display ECU - Lane Assistance On/Off Status	Controls the On/Off status of the lane assistance system on the Car Display.

Car Display ECU - Lane Assistant Active/Inactive	Controls the Active/Inactive status of the lane assistance system on the Car Display.
Car Display ECU - Lane Assistance malfunction warning	Controls the malfunction warning notification of the lane assistance system on the Car Display.
Driver Steering Torque Sensor	Measures the steering torque applied by the driver to the steering wheel.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Receives the steering torque measured by the Driver Steering Torque Sensor and applies the appropriate amplification.
EPS ECU - Normal Lane Assistance Functionality	Converts the torque request received from the Camera Sensor ECU - Torque request generator into the appropriate torque request while not applying safety thresholds identified during the functional safety process.
EPS ECU - Lane Departure Warning Safety Functionality	Converts the torque requests received from the EPS ECU - Normal Lane Assistance Functionality into the LDW torque requests that respect maximum torque amplitude and frequency identified during the functional safety process and reports errors to the Car Display ECU - Lane Assistance malfunction warning.
EPS ECU - Lane Keeping Assistant Safety Functionality	Converts the torque requests received from the EPS ECU - Normal Lane Assistance Functionality into the LKA torque requests that respect maximum torque duration identified during the functional safety process and reports errors to the Car Display ECU - Lane Assistance malfunction warning.
EPS ECU - Final Torque	Combines torque requests from the EPS ECU - Lane Departure Warning Safety Functionality, EPS ECU - Lane Keeping Assistant Safety Functionality, and Electronic Power Steering (EPS) ECU - Driver Steering Torque and sends the result to the Motor.
Motor	Applies the torque to the steering wheel as it was determined by the Electronic Power Steering ECU.

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 01-01-01	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	LDW is deactivated with appropriate notification on the Car Display. LDW_Torque_Request is set to zero.

Technical Safety Requirement 01-01-02	As soon as the LDW function deactivates the LDW feature, the 'LDW Safety' software block shall send a signal ‘LDW_Error_Status’ to the Car Display ECU to turn on a warning light.	C	50 mS	LDW Safety	LDW is deactivated with appropriate notification on the Car Display. LDW_Torque_Request is set to zero.
Technical Safety Requirement 01-01-03	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	LDW is deactivated with appropriate notification on the Car Display. LDW_Torque_Request is set to zero.
Technical Safety Requirement 01-01-04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50 mS	Data Transmission Integrity Check	LDW is deactivated with appropriate notification on the Car Display. LDW_Torque_Request is set to zero.
Technical Safety Requirement 01-01-05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Safety Startup (Memory Test)	LDW is deactivated with appropriate notification on the Car Display. LDW_Torque_Request is set to zero.

Functional Safety Requirement 01-02 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 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 01-02-01	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	LDW is deactivated with appropriate notification on the Car Display. LDW_Torque_Request is set to zero.
Technical Safety Requirement 01-02-02	As soon as the LDW function deactivates the LDW feature, the 'LDW Safety' software block shall send a signal ‘LDW_Error_Status’ to the Car Display ECU to turn on a warning light.	C	50 mS	LDW Safety	LDW is deactivated with appropriate notification on the Car Display. LDW_Torque_Request is set to zero.

Technical Safety Requirement 01-02-03	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	LDW is deactivated with appropriate notification on the Car Display. LDW_Torque_Request is set to zero.
Technical Safety Requirement 01-02-04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50 mS	Data Transmission Integrity Check	LDW is deactivated with appropriate notification on the Car Display. LDW_Torque_Request is set to zero.
Technical Safety Requirement 01-02-05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Safety Startup (Memory Test)	LDW is deactivated with appropriate notification on the Car Display. LDW_Torque_Request is set to zero.

Lane Keeping Assistance (LKA) Requirements:

Functional Safety Requirement 02-01 with its associated system elements (derived in the functional safety concept):

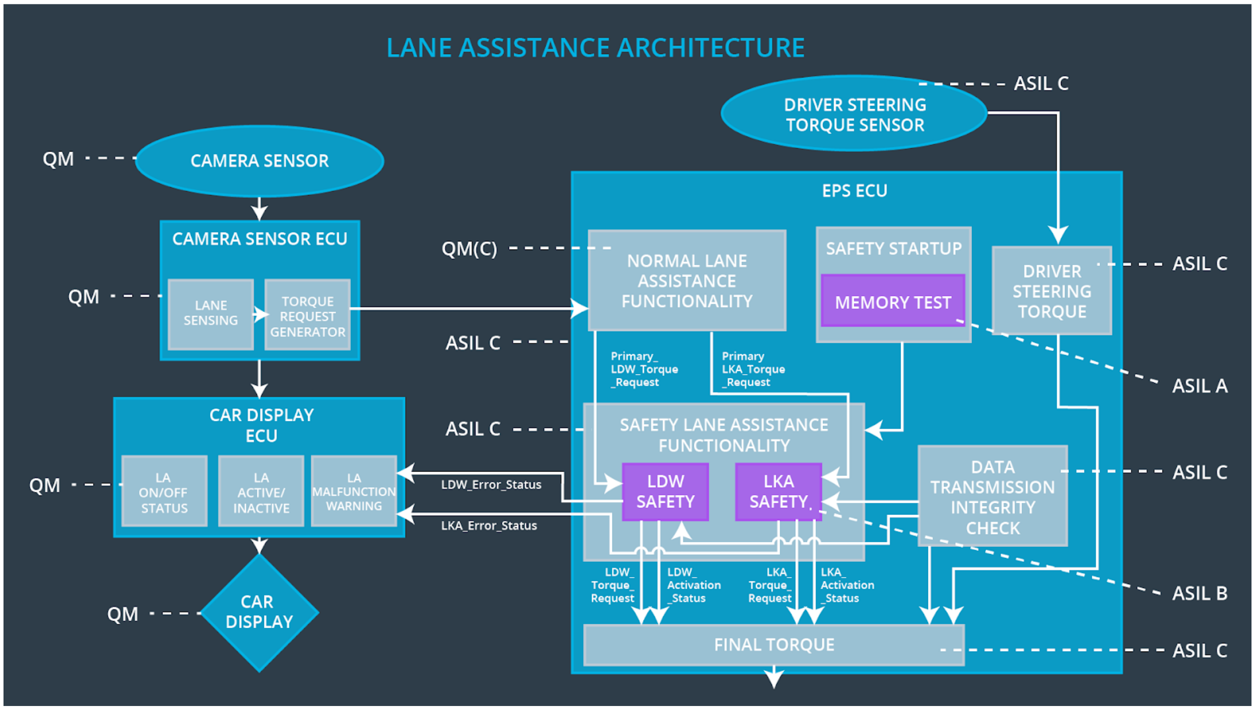
ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration.	X	-	-

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

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 02-01-01	The LKA safety component shall ensure that the duration of the 'LKA_Torque_Request' sent to the 'Final electronic power steering Torque' component is no longer than 'Max_Duration.'	B	500 mS	LKA Safety	LKA is deactivated with appropriate notification on the Car Display. LKA_Torque_Request is set to zero.

Technical Safety Requirement 02-01-02	As soon as the LKA function deactivates the LKA feature, the 'LKA Safety' software block shall send a signal ‘LKA_Error_Status’’ to the Car Display ECU to turn on a warning light.	B	500 mS	LKA Safety	LKA is deactivated with appropriate notification on the Car Display. LKA_Torque_Request is set to zero.
Technical Safety Requirement 02-01-03	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	LKA is deactivated with appropriate notification on the Car Display. LKA_Torque_Request is set to zero.
Technical Safety Requirement 02-01-04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	B	500 mS	Data Transmission Integrity Check	LKA is deactivated with appropriate notification on the Car Display. LKA_Torque_Request is set to zero.
Technical Safety Requirement 02-01-05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Safety Startup (Memory Test)	LKA is deactivated with appropriate notification on the Car Display. LKA_Torque_Request is 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 ECU.

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off LDW function.	Malfunction_01, Malfunction_02	Yes	Warning displayed on the Car Display
WDC-02	Turn off LKA function.	Malfunction_03	Yes	Warning displayed on the Car Display.