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
2017-10-24	0.1	Wilhelm Nagel	Initial Version

Table of Contents

Purpose of the Technical Safety Concept

The Technical Safety Concept details the high-level requirements from the Functional Safety Concept. It describes how the desired functionality will be achieved on a technical level by defining requirements for sensors, control units and actuators. The Technical Safety Concept defines which component is responsible for a function, the electronic signals that are exchanged between ECUs and how the ECUs will behave on the reception of the signals. Technical Safety Concepts are often divided in System Level Technical Concepts and Sub System Level Technical Concepts.

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	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	Off
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 cannot misuse the system for autonomous driving	B	500 ms	Off

Refined System Architecture from Functional Safety Concept

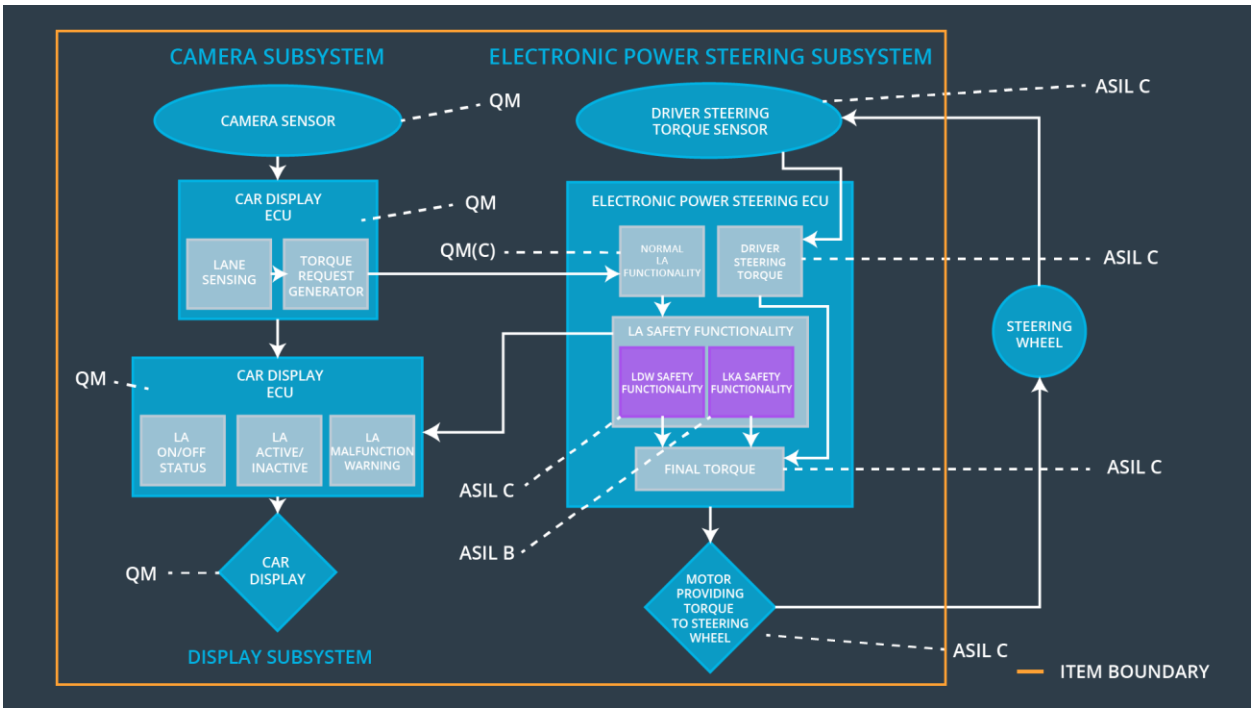

Figure 1: Refined System Architecture for Lane Assistance System

Functional overview of architecture elements

Element	Description
Camera Sensor	Capture images of the road and provide them to the Camera Sensor ECU
Camera Sensor ECU - Lane Sensing	Process the received images to detect drifts from the center of the lane and signal necessity for corrective action to Torque request generator
Camera Sensor ECU - Torque request generator	Translate the received corrective action into signals for the Electronic Power Steering ECU
Car Display	Display the state information provided by the Car Display ECU, e.g. activation of assistance function, warnings or malfunctions
Car Display ECU - Lane Assistance On/Off Status	Displays state of Lane Assistance, i.e. on or off
Car Display ECU - Lane Assistant Active/Inactive	Displays if the Lane Assistance function is performing corrective actions, e.g. steering towards lane center

Car Display ECU - Lane Assistance malfunction warning	Displays a warning if an error has been detected in the Lane Assistance function
Driver Steering Torque Sensor	Senses the torque at the steering wheel that is applied by the driver
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Processes signals from Driver Steering Torque Sensor and calculates required torque for EPS ECU
EPS ECU - Normal Lane Assistance Functionality	Process signals from Camera Sensor ECU and generate torque requests for LDW and LKA
EPS ECU - Lane Departure Warning Safety Functionality	Check that torque amplitude and oscillation are below the thresholds Max_Torque_Amplitude and Max_Torque_Frequency
EPS ECU - Lane Keeping Assistant Safety Functionality	Check that duration in which torque is applied does not exceed the threshold of Max_Duration
EPS ECU - Final Torque	Sends required torque value to motor
Motor	Receives input from EPS ECU and applies torque to steering wheel

Technical Safety Concept

Technical Safety Requirements

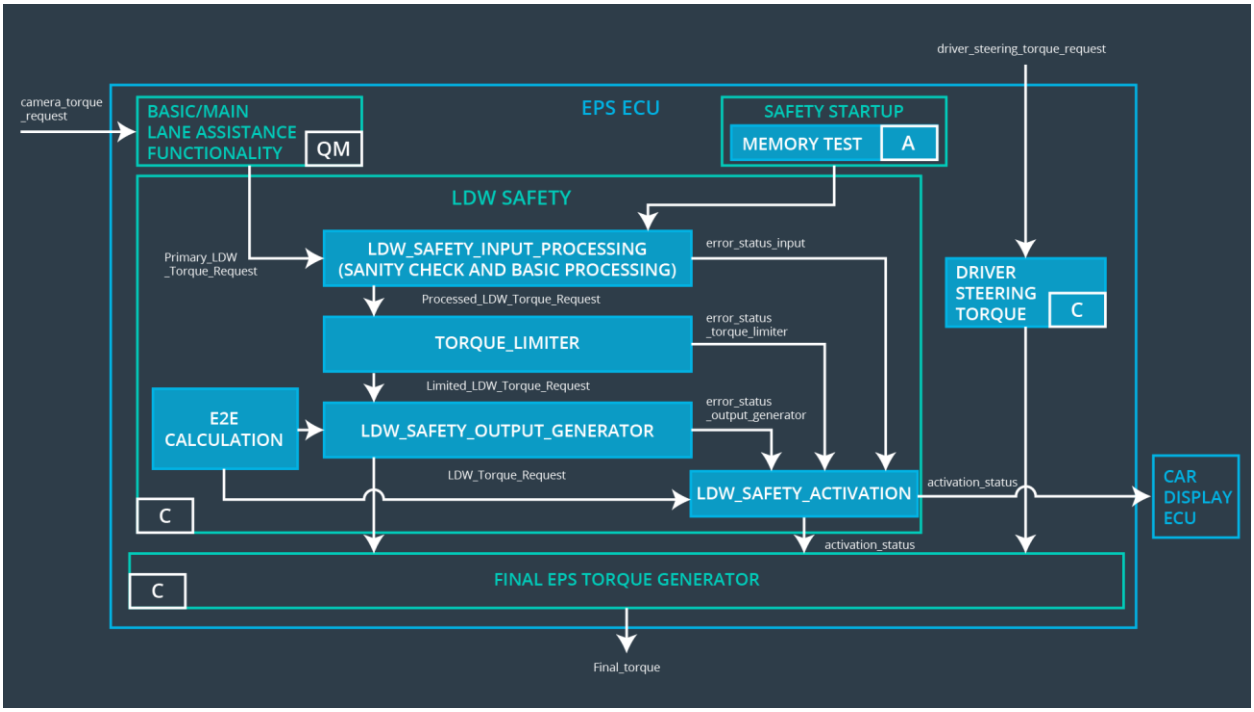

Figure 2: Lane Departure Warning component of the EPS ECU

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 Functionality	Off
Technical Safety Requirement 02	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 Functionality	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 Functionality	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	Off
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	ignition cycle	Safety startup	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 amplitude of the LDW_Torque_Request sent to the 'final electronic power steering Torque' component is below Max_Torque_Frequency	C	50 ms	LDW Safety Functionality	Off
Technical Safety Requirement 02	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 Functionality	Off
Technical Safety Requirement 03	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	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	Off
Technical Safety Requirement 05	Memory test shall be conducted at start up of EPS ECU to check for any faults in memory	A	Ignition cycle	Safety startup	Off

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 only Max_Duration	B	500 ms	LKA Safety Functionality	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 Functionality	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 Functionality	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	Off
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	Off

Refinement of the System Architecture

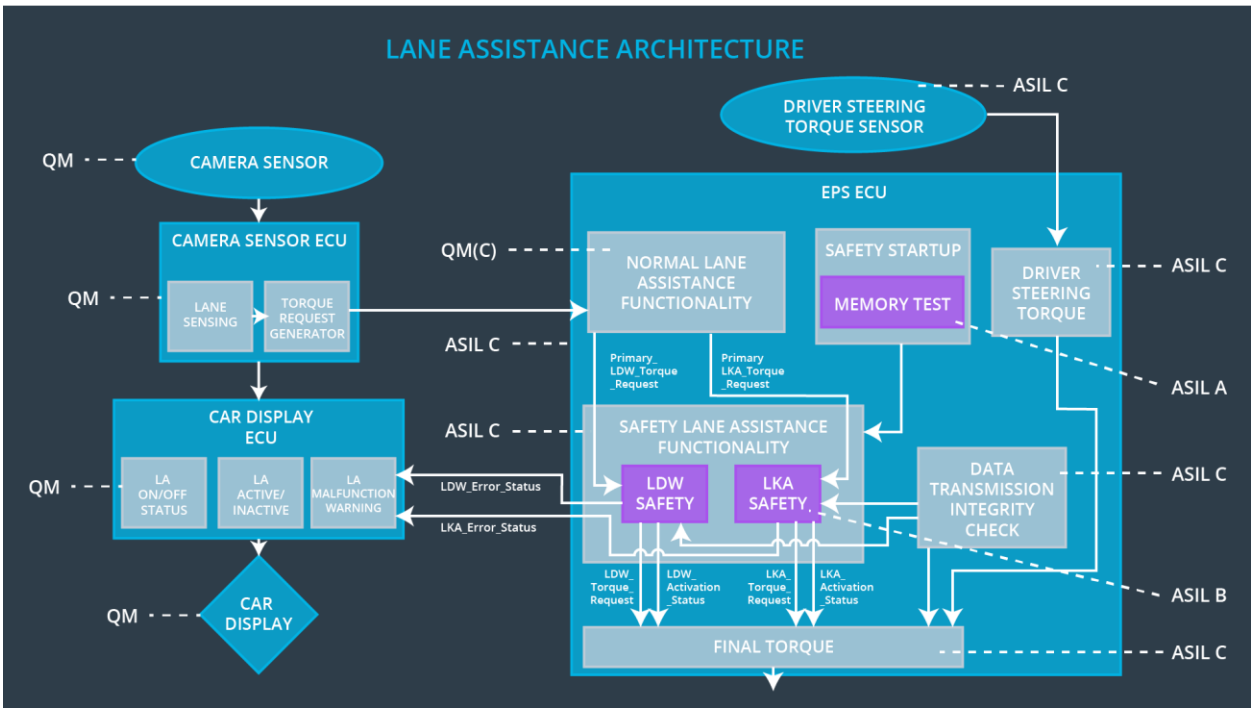

Figure 3: Refined System Architecture of Lane Assistance

Allocation of Technical Safety Requirements to Architecture Elements

All technical safety requirements of the Lane Assistance system 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	Off	LDW torque or frequency exceeds defined maximum values for Max_Torque_Amplitude or Max_Torque_Frequency	Yes	Visual warning in Car Display, e.g. by a flashing LED
WDC-02	Off	LKA torque is applied longer than Max_Duration	Yes	Visual warning in Car Display, e.g. by a flashing LED