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
Sept 12 2017	0.1	RE	First Draft
Sept 13 2017	1.0	RE	INITIAL RELEASE

Table of Contents

Purpose of the Technical Safety Concept

The technical safety concept describes the technical implementation of the details and design parameters of the system as technical requirements. These are used to implement the functional safety requirements outlined in the functional safety concept. Technical safety requirements are generated based on the functional safety requirements. These are then allocated to the system architecture. Validation and verification tests are provided for the technical requirements

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	turn off functionality
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50ms	turn off functionality
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	turn off functionality

Refined System Architecture from Functional Safety Concept

The refined system architecture is presented in Figure 1. Note that the Camera Sensor ECU is mistakenly labbelled as a Car Display ECU.

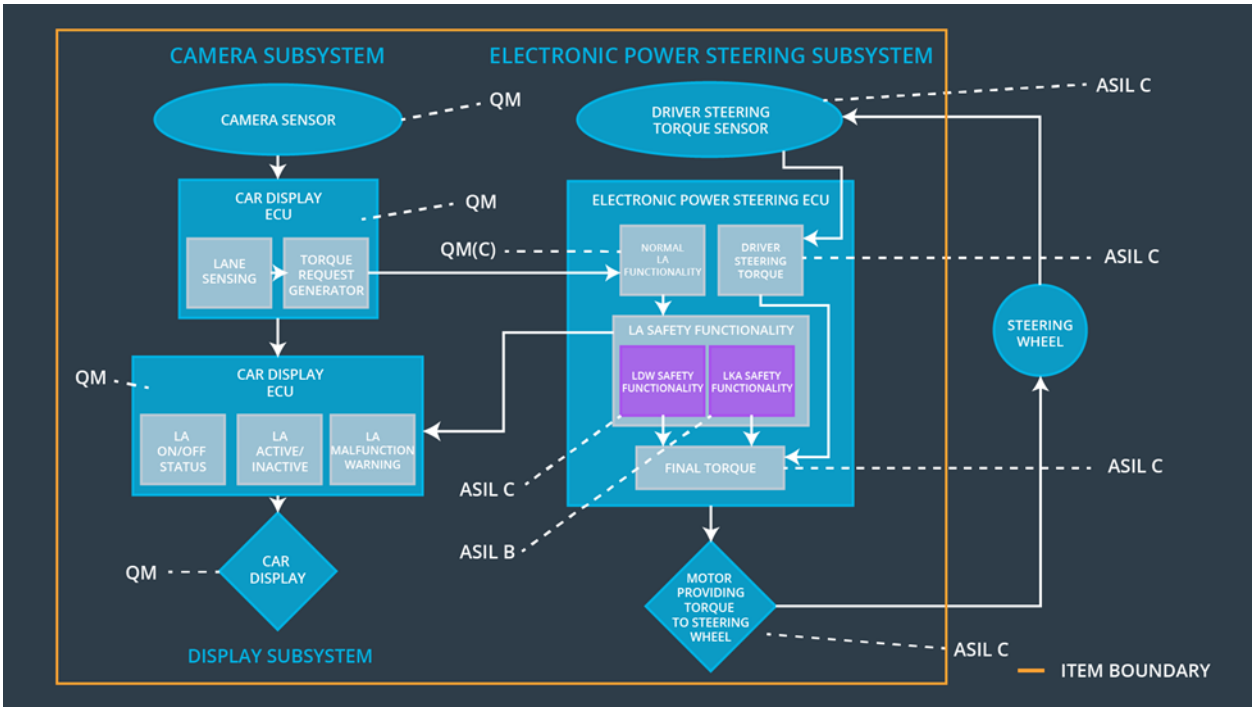

Figure 1: Refined System Architecture with ASIL labels

Functional overview of architecture elements

Element	Description
Camera Sensor	Physical sensor responsible for detecting lane lines
Camera Sensor ECU - Lane Sensing	Software module which interprets sensor data and identifies lane markings in the image. Determines the position of the vehicle relative to the lane.
Camera Sensor ECU - Torque request generator	Software module in the camera sensor ECU which carrys out lane positioning control of the vehicle by issuing torque requests to the Electronic Power Steering ECU.
Car Display	Vehicle dashboard lights or display / screen unit providing status feedback to the driver of vehicle systems.
Car Display ECU - Lane Assistance On/Off Status	A status light or LCD illustration on the car display which indicates the status of the Lane Assistance function as ON/OFF.

Car Display ECU - Lane Assistant Active/Inactive	A status light or LCD illustration on the car display which indicates the status of the Lane Assistance function as Active / Inactive.
Car Display ECU - Lane Assistance malfunction warning	A status light or LCD illustration on the car display which indicates warnings or fault of the Lane Assistance function
Driver Steering Torque Sensor	Physical sensor such as an encoder or strain gauge capable of measuring steering torque input on the steering wheel from the driver.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	A hardware / software module on the Power Steering ECU which measures the signal from the Torque sensor and provides a software value of the driver steering torque.
EPS ECU - Normal Lane Assistance Functionality	A non-safety verified software module which accepts torque requests from the camera sensor ECU and generates an output torque for the motor.
EPS ECU - Lane Departure Warning Safety Functionality	A safety verified software module which monitors and passes through the output of the Normal Lane Assistance Functionality for faults related to safety requirements of the LDW function. (Such as max torque amplitude and frequency)
EPS ECU - Lane Keeping Assistant Safety Functionality	A safety verified software module which monitors and passes through the output of the Normal Lane Assistance Functionality for faults related to safety requirements of the LKA function. (Such as max_duration for torque output)
EPS ECU - Final Torque	A software value of the final torque which should be output to the Electronic Power Steering Motor based on the Lane Assistance Function and the driver input measured torque.
Motor	The motor which applies torque to the steering column, accepts voltage / current control from the 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	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	50ms	EPS ECU - Lane Departure Warning Safety Functionalily (LDW Safety Block)	Turn off functionality
Technical Safety Requirement 01-02	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	50ms	EPS ECU - Lane Departure Warning Safety Functionality (LDW Safety Block)	Turn off functionality
Technical Safety Requirement 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	C	50ms	EPS ECU - Lane Departure Warning Safety Functionality (LDW Safety	Turn off functionality

	be set to zero.			Block)	
Technical Safety Requirement 01-04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50ms	EPS ECU - Lane Departure Warning Safety Functionality, EPS ECU - Final Torque (Data Integrity Check)	Turn off functionality
Technical Safety Requirement 01-05	Memory test shall be conducted at start-up of the EPS ECU to check for any faults in memory.	A	Ignition cycle time	EPS ECU hardware	Turn off functionality

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	The LDW safety component shall ensure that the frequency of the 'LDW_Torque_Request_Rate'	C	50ms	EPS ECU - Lane Departure	Turn off functionality

02-01	sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Frequency.			Warning Safety Functionality (LDW Safety Block)	
Technical Safety Requirement 02-02	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	50ms	EPS ECU - Lane Departure Warning Safety Functionality (LDW Safety Block)	Turn off functionality
Technical Safety Requirement 02-03	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the 'LDW_Torque_Requestt' shall be set to zero.	C	50ms	EPS ECU - Lane Departure Warning Safety Functionality (LDW Safety Block)	Turn off functionality
Technical Safety Requirement 02-04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50ms	EPS ECU - Lane Departure Warning Safety Functionality, EPS ECU - Final Torque (Data Integrity Check)	Turn off functionality
Technical Safety Requirement 02-05	Memory test shall be conducted at start-up of the EPS ECU to check for any faults in memory.	A	Ignition cycle time	EPS ECU hardware	Turn off functionality

Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria:

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Technical Safety Requirement 01-01	Driver testing indicates that most drivers can resume control of the vehicle if high-amplitude vibration is stopped within 50ms	Software testing introduces a high amplitude oscillation, precision timing checks that safety module detects and stops vibration within 50ms
Technical Safety Requirement 01-02	Driver testing indicates that a driver should know the state of the LDW system, the car display is adequate feedback	Software testing introduces a high amplitude oscillation. User verifies car display status is updated when safety module deactivates LDW
Technical Safety Requirement 01-03	Ensure that LDW_Torque_Request is the valid parameter to control the EPS output.	Software testing introduces a high amplitude oscillation. Communications are monitored to verify 'LDW_Torque_Request' is set to zero
Technical Safety Requirement 01-04	Communications integrity checks of safety systems are standard practice	Software testing is used to send an LDW_Torque_Request with a faulty checksum and separately with stale timing data. EPS detects faulty and repeat messages and sets torque to zero, shuts of system.
Technical Safety Requirement 01-05	Memory tests of start-up of safety systems are standard practice	Memory tests on faulty memory detect results
Technical Safety Requirement 02-01	Driver testing indicates that most drivers can resume control of the vehicle if high-frequency vibration is stopped within 50ms	Software testing introduces a high frequency oscillation, precision timing checks that safety module detects and stops vibration within 50ms
Technical Safety Requirement 02-02	Driver testing indicates that a driver should know the state of the LDW system, the car display is adequate feedback	Software testing introduces a high frequency oscillation. User verifies car display status is updated when safety module deactivates LDW
Technical Safety Requirement 02-03	Ensure that LDW_Torque_Request is the valid parameter to control the EPS output.	Software testing introduces a high frequency oscillation. Communications are monitored to verify 'LDW_Torque_Request' is set to zero

Technical Safety Requirement 02-04	Communications integrity checks of safety systems are standard practice	Software testing is used to send an LDW_Torque_Request with a faulty checksum and separately with stale data. EPS detects faulty and repeat messages and sets torque to zero, shuts off system.
Technical Safety Requirement 02-05	Memory tests of start-up of safety systems are standard practice	Memory tests on faulty memory detect results

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 03-01	The LKA safety component shall ensure that the integral time of the 'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is below ‘Max_Duration’.	B	500ms	EPS ECU - Lane Keep Assistance Safety Module (LDW Safety Block)	Turn off functionality
Technical Safety	As soon as the LKA function deactivates the LKA feature, the	B	500ms	EPS ECU - Lane Keeping	Turn off functionality

Requirement 03-02	LKA Safety' software block shall send a signal to the car display ECU to turn on a warning light			Assistance Safety Functionality (LDW Safety Block)	
Technical Safety Requirement 03-03	As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and the 'LKA_Torque_Requestt' shall be set to zero.	B	500ms	EPS ECU - Lane Keeping Assistance Safety Functionality (LDW Safety Block)	Turn off functionality
Technical Safety Requirement 03-04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	B	500ms	EPS ECU - Lane Keeping Assistance Safety Functionality, EPS ECU - Final Torque (Data integrity Check)	Turn off functionality
Technical Safety Requirement 03-05	Memory test shall be conducted at start-up of the EPS ECU to check for any faults in memory.	A	Ignition cycle time	EPS ECU Hardware	Turn off functionality

Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Technical Safety Requirement 03-01	Driver testing indicates that deactivation of the LKA after max_duration is effective at preventing use as an autonomous system	Timing is used to verify there is no measurable torque output after max_duration
Technical Safety Requirement 03-02	Driver testing indicates that a driver should know the state of the LKA system, the car display is adequate feedback	User verification that the car display indicates LKA status after max_duration
Technical Safety Requirement	Ensure that LKA_Torque_Request is the valid parameter to control the EPS	Communications are monitored to verify ‘LKA_Torque_Request’ is set to zero after max_duration

03-03	output.	
Technical Safety Requirement 03-04	Communications integrity checks of safety systems are standard practice	Software testing is used to send an LKA_Torque_Request with a faulty checksum and separately with stale timing data. EPS detects faulty and repeat messages and sets torque to zero, shuts off system
Technical Safety Requirement 03-05	Memory tests of start-up of safety systems are standard practice	Memory tests on faulty memory detect results

Refinement of the System Architecture

The system architecture diagram has been refined based on technical safety requirements presented above. The diagram with ASIL labels is given in Figure 2.

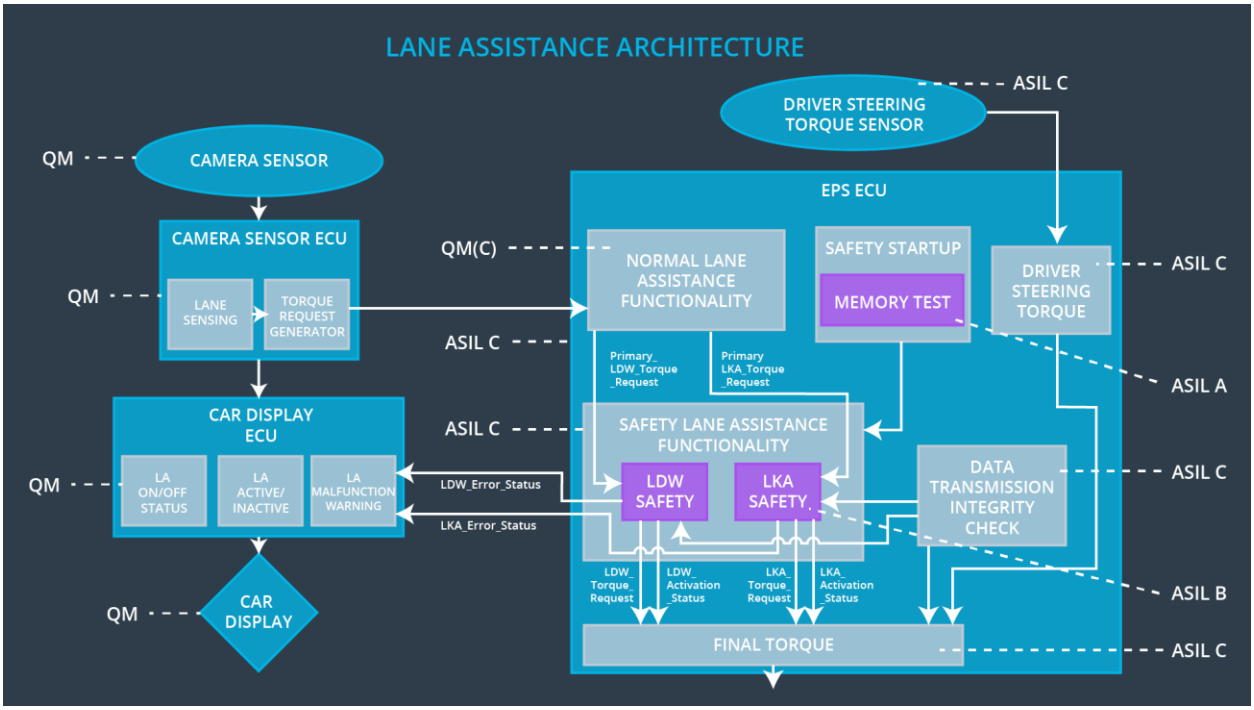

Figure 2: Refined System Architecture from Technical Safety Requirements

Allocation of Technical Safety Requirements to Architecture Elements

All technical safety requirements for TSR-01,02,03 are allocated to the Power Steering ECU. This is identical to the allocation of the corresponding functional safety requirement.

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	turn off the functionality	Malfunction_01/ 02	yes	Car display
WDC-02	turn off the functionality	Malfunction_03	yes	Car display