Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 1.1

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
5 September 2017	1.0	Edward Venator	Initial submission
16 September 2017	1.1	Edward Venator	Correct allocation of TSR-01-01-05 Correct typo in TSR-01-02-01 Correct allocation of TSR-01-02-05 Correct typo in WDC-02 Correct ASIL level of FSR-02-01 Correct FTTI of all TSRs of FSR-02-01

Table of Contents

Purpose of the Technical Safety Concept

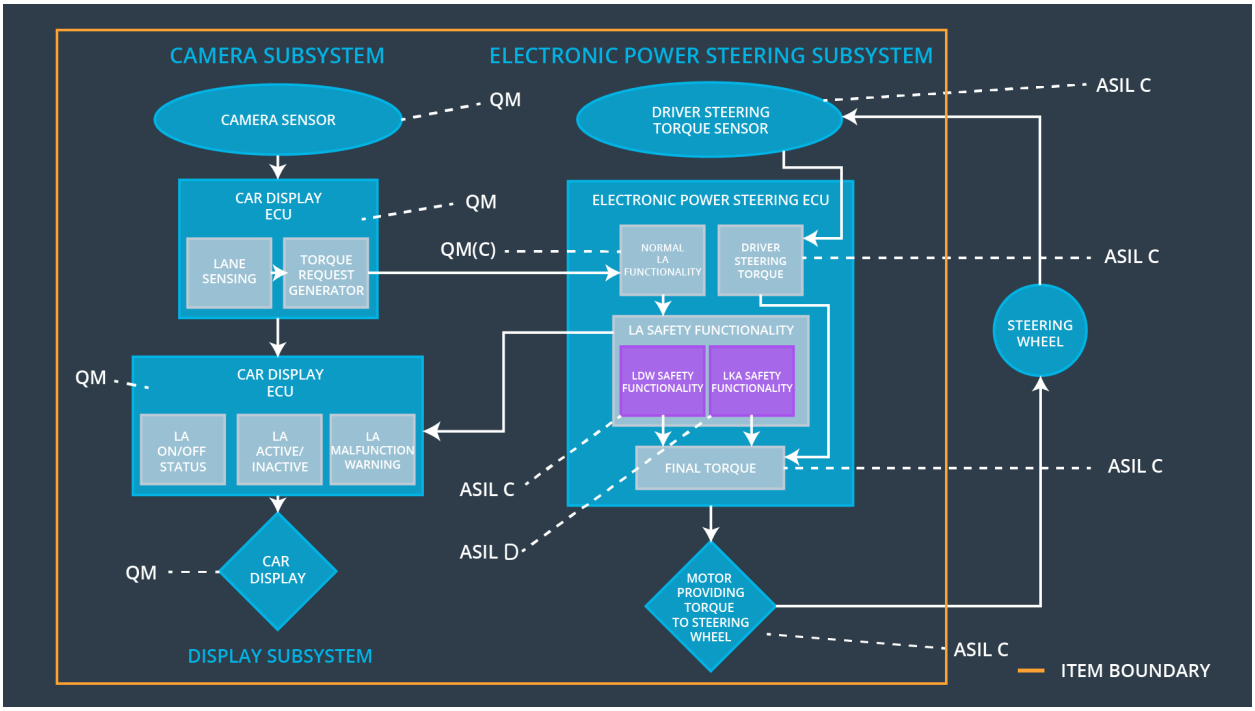
The purpose of the technical safety concept is to refine the functional safety concept to a level of detail that can be implemented.

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 is below Max_Torque_Ampliltude.	C	50ms	LDW disabled (output torque zero)
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque is below Max_Torque_Frequency.	C	50ms	LDW disabled (output torque zero)
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	LKA disabled (output torque zero)
Functional Safety Requirement 03-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is below Max_Torque_Magnitude.	D	50ms	LKA disabled (output torque zero)

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Captures imagery of the road in front of the car.
Camera Sensor ECU - Lane Sensing	Determines the position of the car in the ego lane based on imagery from the Camera Sensor.
Camera Sensor ECU - Torque request generator	Calculates required torque for LDW and LKA functions and sends torque requests to the Electronic Power Steering ECU.
Car Display	Displays the status of system functions using lights.
Car Display ECU - Lane Assistance On/Off Status	Keeps track of whether the Lane Assistance is on or off and controls an indicator on the Car Display.
Car Display ECU - Lane Assistant Active/Inactive	Keeps track of whether the Lane Assistant is Active or Inactive and controls an indicator on the Car Display.
Car Display ECU - Lane Assistance malfunction warning	In the event of any malfunction in the Lane Assistance system, illuminates an indicator light on the Car Display.

Driver Steering Torque Sensor	Measures the torque being applied to the steering wheel.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Processes measurements from the Driver Steering Torque Sensor.
EPS ECU - Normal Lane Assistance Functionality	Calculate torque to apply to the steering wheel to maintain the car's position in the lane.
EPS ECU - Lane Departure Warning Safety Functionality	Ensure that steering wheel torque does not exceed Max_Torque_Amplitude or Max_Torque_Frequency.
EPS ECU - Lane Keeping Assistant Safety Functionality	Ensure the LKA function is not active for longer than Max_Duration.
EPS ECU - Final Torque	Combine driver steering torque and lane assistance torque to get the final torque requires from the motor.
Motor	Provides torque to the steering wheel; controlled 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	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	LDW Safety	LDW disabled (output torque zero)
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	50ms	LDW Safety	LDW disabled (output torque zero)
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	50ms	LDW Safety	LDW disabled (output torque zero)
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50ms	Data Transmission Integrity Check	LDW disabled (output torque zero)
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	C	Ignition cycle	Separate External Block of Memory	LDW disabled (output torque 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	50ms	LDW Safety	LDW disabled (output torque zero)
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	50ms	LDW Safety	LDW disabled (output torque zero)
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	50ms	LDW Safety	LDW disabled (output torque zero)
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50ms	Data Transmission Integrity Check	LDW disabled (output torque 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	Separate External Block of Memory	LDW disabled (output torque 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 lane keeping assistance torque is applied for only Max_Duration.	B	500ms	LKA Safety	LKA disabled (output torque zero)
Technical Safety Requirement 02	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	50ms	LKA Safety	LKA disabled (output torque zero)
Technical Safety	As soon as the LKA function deactivates the LKA feature,	B	500ms	LKA Safety	LKA disabled

Requirement 03	the LKA Safety' software block shall send a signal to the car display ECU to turn on a warning light.				(output torque zero)
Technical Safety Requirement 04	The validity and integrity of the data transmission for LKA_Torque_Request' signal shall be ensured.	B	500ms	Data Transmission Integrity Check	LKA disabled (output torque 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	LKA disabled (output torque zero)

Functional Safety Requirement 03-1 with its associated system elements (derived in the functional safety concept)

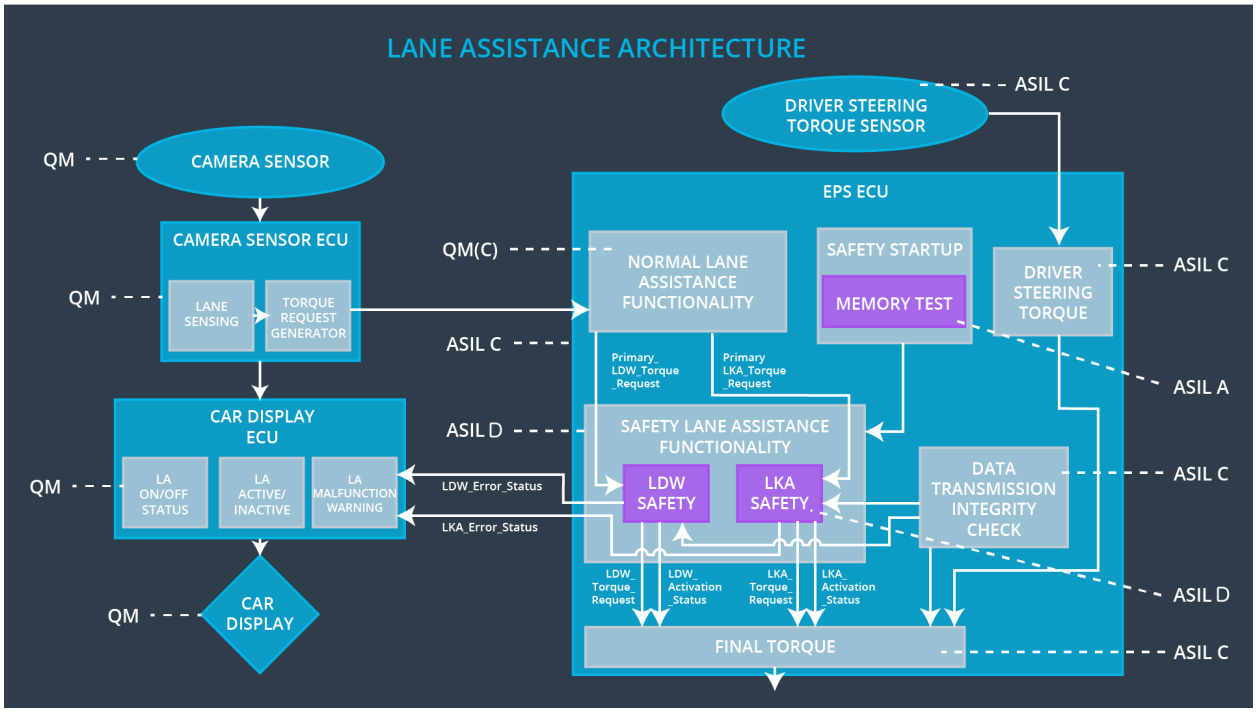
ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 03-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is below Max_Torque_Magnitude.	X		

Technical Safety Requirements related to Functional Safety Requirement 03-01 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 amplitude of the ‘LKA_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Magnitude.’	D	50ms	LKA Safety	LKA disabled (output torque zero)
Technical	As soon as a failure is detected	D	50ms	LKA Safety	LKA

Safety Requirement 02	by the LKA function, it shall deactivate the LKA feature and the LKA_Torque_Request' shall be set to zero.				disabled (output torque zero)
Technical Safety Requirement 03	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.	D	50ms	LKA Safety	LKA disabled (output torque zero)
Technical Safety Requirement 04	The validity and integrity of the data transmission for LKA_Torque_Request' signal shall be ensured.	D	50ms	Data Transmission Integrity Check	LKA disabled (output torque 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	LKA disabled (output torque zero)

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

All of the technical safety requirements are allocated the Electronic Power Steering ECU. Further detail is shown in the tables above.

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off LDW	The LDW applies an oscillating torque with very high amplitude (above limit).	Yes	Display shows warning light
WDC-02	Turn off LDW	The LDW applies an oscillating torque with very high frequency (above limit).	Yes	Display shows warning light
WDC-03	Turn off LKA	The LKA function is not time-limited, allowing its misuse as an autonomous driving function.	Yes	Display shows warning light