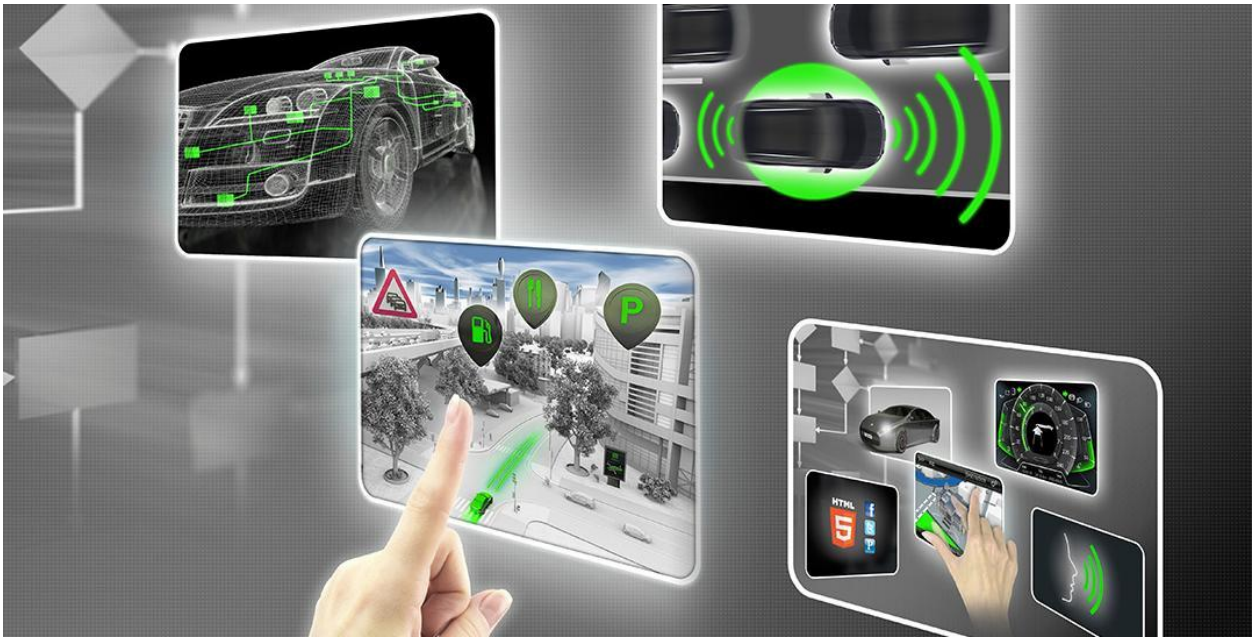
Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 2.0

Template Version 1.0, Released on 2017-06-21



Document history

Date	Version	Editor	Description
10/21/2018	1.0	Chunfeng Yang	Initial version.
10/31/2018	2.0	Chunfeng Yang	Updated these sections: Purpose of the Technical Safety Concept, Functional Safety Requirements, Refinement of System Architecture, Technical Safety Requirements.

Table of Contents

Purpose of the Technical Safety Concept

The purpose of the technical safety concept is to refine the functional safety requirements established in the Functional Safety Concept into technical safety requirements. As part of product development technical safety concept involves:

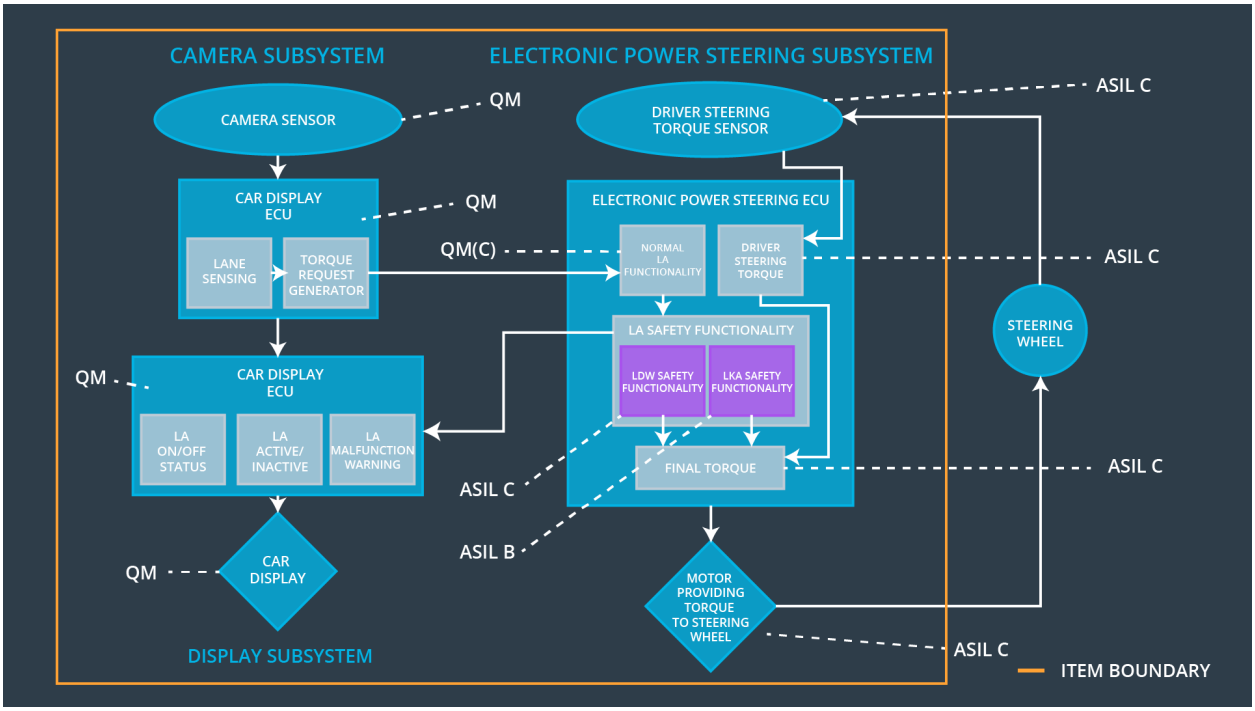
- Turning functional safety requirements into technical safety requirements
- Allocating technical safety requirements to the system architecture

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 oscillating torque amplitude requested by the LDW function is below Max_Torque_Amplitude.	C	50 ms	LDW torque request amplitude is set to zero.
Functional Safety Requirement 01-02	The Electronic Power Steering ECU shall ensure that the oscillating torque frequency requested by the LDW function is below Max_Torque_Frequency.	C	50 ms	LDW torque request frequency is set to zero.
Functional Safety Requirement 02-01	The Electronic Power Steering ECU shall ensure that the Lane Keeping Assistance torque is applied only Max_Duration.	B	500 ms	Lane Keeping Assistance torque is zero.

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Capture road images and provide them to the Camera Sensor ECU.
Camera Sensor ECU - Lane Sensing	Software module detecting the lane line positions from the Camera Sensor images.
Camera Sensor ECU - Torque request generator	Software module calculating the necessary torque to be requested to the Electronic Power Steering ECU.
Car Display	Display warning for the driver.
Car Display ECU - Lane Assistance On/Off Status	Indicate the status of the Lane Assistance functionality (On/Off).
Car Display ECU - Lane Assistant Active/Inactive	Indicate if the Lane Assistance functionality is properly functioning (Active/Inactive).

Car Display ECU - Lane Assistance malfunction warning	Indicate a malfunction on the Lane Assistance functionality.
Driver Steering Torque Sensor	Measure the torque applied to the steering wheel by the driver.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Software module receiving the driver's torque request from the steering wheel.
EPS ECU - Normal Lane Assistance Functionality	Software module receiving the Camera Sensor ECU torque request.
EPS ECU - Lane Departure Warning Safety Functionality	Software module ensuring the torque amplitude is below Max_Torque_Amplitude and torque frequency is below Max_Torque_Frequency.
EPS ECU - Lane Keeping Assistant Safety Functionality	Software module ensuring the Lane Keeping Assistance functionality application is not active more than Max_Duration time.
EPS ECU - Final Torque	Combine the torque request from the Lne Keeping and Lane Departure Warning functionalities and sends them to the Motor.
Motor	Applies the required torque to the steering wheels.

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	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is	X		

01-01	below Max_Torque_Amplitude			

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 Lane Departure Warning 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	Lane Departure Warning torque request amplitude is set to zero.
Technical Safety Requirement 02	When the Lane Departure Warning is deactivated, the 'LDW Safety' software module shall send a signal to the Car Display ECU to turn on a warning signal.	C	50 ms	LDW Safety	Lane Departure Warning torque request amplitude is set to zero.
Technical Safety Requirement 03	When a failure is detected by the Lane Departure Warning functionality, it shall deactivate the Lane Departure Warning feature and set 'LDW_Torque_Request' to zero.	C	50 ms	LDW Safety	Lane Departure Warning torque request amplitude is set to zero.
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal	C	50 ms	Data Transmission Integrity Check	Lane Departure Warning torque request

	shall be ensured.				amplitude is set to zero.
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any memory problems	A	Ignition cycle	Memory Test	Lane Departure Warning torque request amplitude is 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 Safety Requirement 01	The LDW safety component shall ensure that the *frequency* of 'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is	C	50 ms	LDW Safety	Lane Departure Warning torque request frequency is set to zero.

	below ‘Max_Torque_Frequency’.				
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	Lane Departure Warning torque request frequency is set to zero.
Technical Safety Requirement 03	As soons 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	Lane Departure Warning torque request frequency is 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 ms	Data Transmission Integrity Check	Lane Departure Warning torque request frequency is set to zero.
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	Memory Test	Lane Departure Warning torque request frequency is set to zero.

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

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Technical	Validate the Max_Duration is set to	Verify the functionality is turned off

Safety Requirement 02-01-01	the chosen value from LKA Validation Assistance Criteria	after it is applied for Max_Duration.
Technical Safety Requirement 02-01-02	Validate the 'TORQUE_LIMITER' sends the error_status_torque_limiter signal to the LKA_SAFETY_ACTIVATION.	Verify the Car Display ECU displays the Lane Keeping Assistance malfunction warning signal.
Technical Safety Requirement 02-01-03	Validate the 'TORQUE_LIMITER' sends 'LKA_Torque_Request' with zero.	Verify the Final EPS Torque generator receives a LKA_Torque_Request of zero.
Technical Safety Requirement 02-01-04	Validate the 'TORQUE_LIMITER' calculate and sends the correct cyclic redundancy check (CRC) and Alive counter for data transmission validity and integrity.	Verify the functionality is turn off if there is a CRC or Alive counter discrepancy.
Technical Safety Requirement 02-01-05	Validate the Safety Startup Memory test to check memory faults catch memory faults.	Verify the Lane Keeping Assistance is turned off when the Safety Startup Memory fails.

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	The lane keeping item shall	X		

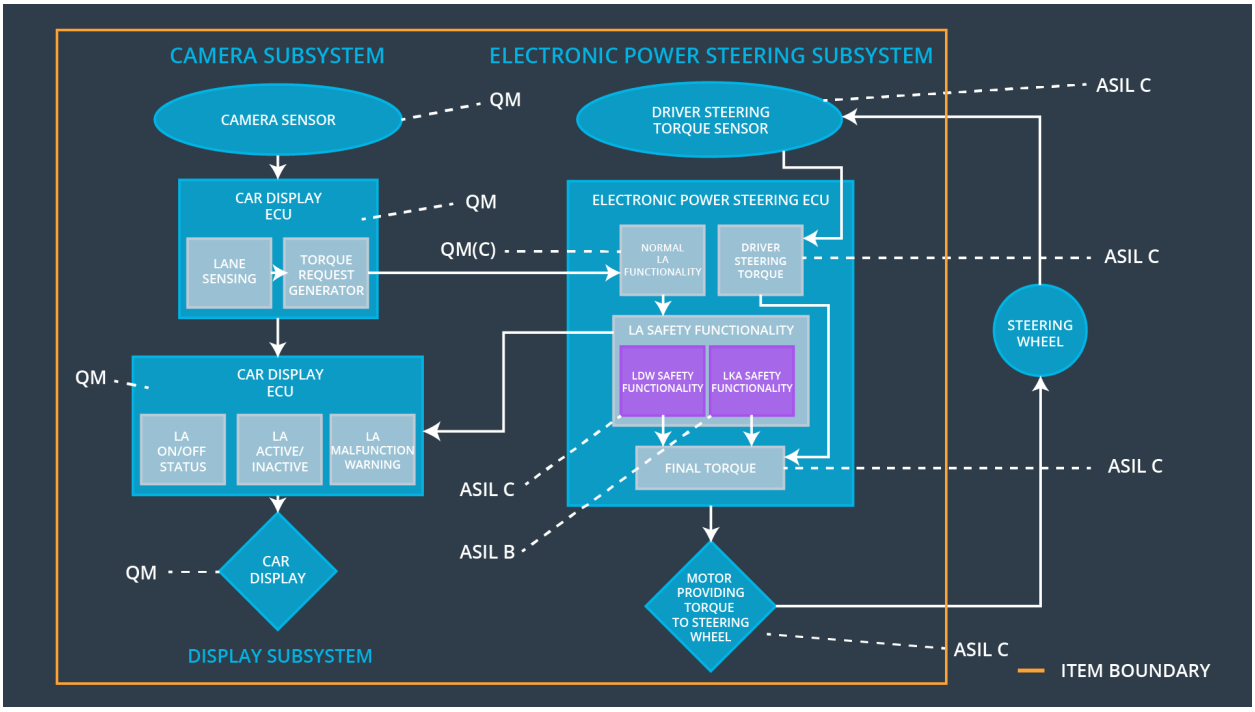
Safety Requirement 02-01	ensure that the lane keeping assistance torque is applied for only Max_Duration			

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 'LKA_Torque_Request' is sent to the 'Final electronic power steering Torque' component for only 'Max_Duration'.	B	500 ms	LKA Safety	Lane Keeping Assistance activation status to 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	500 ms	LKA Safety	Lane Keeping Assistance activation status to zero.
Technical Safety Requirement 03	As soons 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	Lane Keeping Assistance activation status to zero.
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	Lane Keeping Assistance activation status to zero.
Technical Safety Requirement	Memory test shall be conducted at startup of the EPS ECU to	A	Ignition cycle	Memory Test	Lane Keeping Assistance activation

05	check for any faults in mermory.				status to zero.

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

ID	Technical Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Technical Safety Requirement 01-01	The Lane Departure Warning safety component shall ensure that the amplitude of the ‘LDW_Torque_Request’ sent to	X		

	the ‘Final electronic power steering Torque’ component is below ‘Max_Torque_Amplitude.’			
Technical Safety Requirement 01-02	When the Lane Departure Warning is deactivated, the ‘LDW Safety’ software module shall send a signal to the Car Display ECU to turn on a warning signal.	X		
Technical Safety Requirement 01-03	When a failure is detected by the Lane Departure Warning functionality, it shall deactivate the Lane Departure Warning feature and set ‘LDW_Torque_Request’ to zero.	X		
Technical Safety Requirement 01-04	The validity and integrity of the data transmission for ‘LDW_Torque_Request’ signal shall be ensured.	X		
Technical Safety Requirement 01-05	Memory test shall be conducted at startup of the EPS ECU to check for any memory problems	X		
Technical Safety Requirement 02-01	The Lane Departure Warning safety component shall ensure the frequency of the ‘LDW_Torque_Reques’ sent to the ‘Final electronic power steering Torque’ component is below ‘Max_Torque_Frequency.’	X		

Technical Safety Requirement 02-02	The Lane Keeping Assistance safety component shall ensure the duration of the lane keeping assistance torque is applied for less than Max_Duration	X		
Technical Safety Requirement 02-03	When the Lane Keeping Assistance function deactivates, the ‘LKA Safety’ shall send a signal to the Car Display ECU to turn on a warning light.	X		
Technical Safety Requirement 02-04	When a failure is detected, the Lane Keeping Assistance function shall deactivate and the ‘LKA_Torque_Request’ shall be zero.	X		
Technical Safety Requirement 02-05	The validity and integrity of the data transmission for ‘LKA_Torque_Request’ signal shall be ensured.	X		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State Invoked?	Driver Warning
WDC-01	Turn off Lane Departure Warning functionality	Malfunction_01, Malfunction_02, Malfunction_04	Yes	Lane Departure Warning Malfunction Warning on Car

				Display
WDC-02	Turn off Lane Keeping Assistance functionality	Malfunction_03, Malfunction_05	Yes	Lane Keeping Assistance Malfunction Warning on Car Display