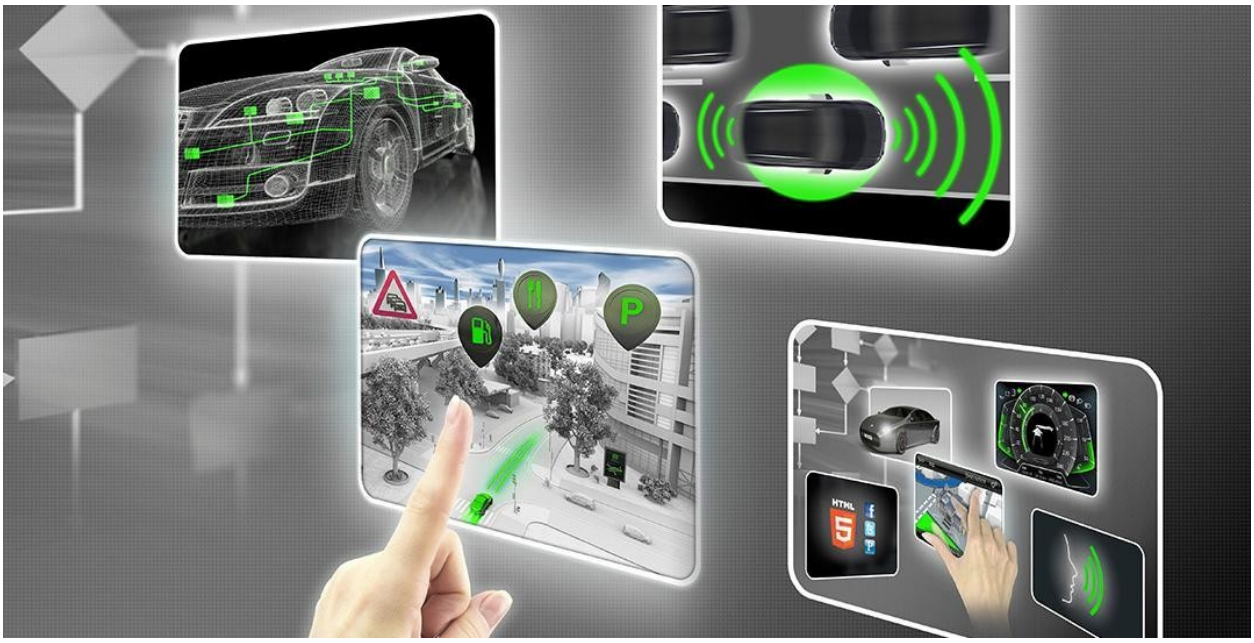
Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21



Document history

Date	Version	Editor	Description
10/9/2018	1.0	John O'Shea	Initial Draft
11/27/2018	1.1	John O'Shea	Corrected architecture allocation block for LKA Technical Safety Req 2,3

Table of Contents

Purpose of the Technical Safety Concept

The technical safety concept involves:

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

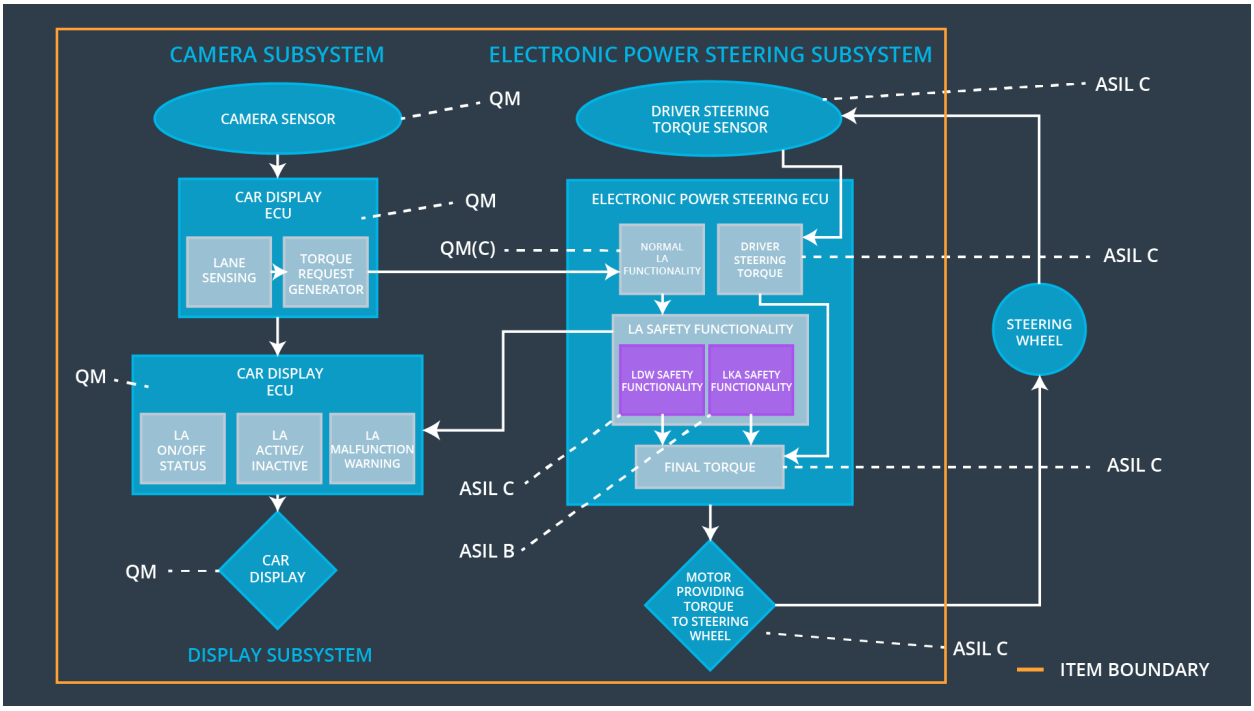
Inputs to the Technical Safety Concept

Functional Safety Requirements

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	The Lane Departure Warning (LDW) item shall ensure that the lane departure oscillating torque is below Max_Torque_Amplitude.	C	50 ms	The torque amplitude is below Max_Torque_Amplitude
Functional Safety Requirement 01-02	The Lane Departure Warning (LDW) item shall ensure that the lane departure oscillating torque is below Max_Torque_Frequency.	C	50 ms	The torque frequency is below Max_Torque_Frequency.
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the Lane Keeping Asssistance (LKA) torque is applied only for Max_Duration.	B	500 ms	The torque applied by the power steering ECU after Max_Duration is 0Nm.

Refined System Architecture from Functional Safety Concept

Functional overview of architecture elements



Element	Description
Camera Sensor	Captures images of the road surface and sends them to the Camera Sensor ECU.
Camera Sensor ECU - Lane Sensing	Processes a valid image to look for lane lines
Camera Sensor ECU - Torque request generator	• Makes a determination of a lane line violation • Alerts Driver Steering Torque Sensor with “Lane Departure Alert” Torque request message
Car Display	Provides a visual indication to the driver if a “Lane Departure Alert ” was detected.
Car Display ECU - Lane Assistance On/Off Status	Processes status packets from Camera Sensor ECU. Detects “Lane Departure Alert” message packet and sets the Car Display warning “ON” indicator. Detects “In Lane” message packet and sets the Car Display by turning off warning “OFF” indicator
Car Display ECU - Lane Assistant Active/Inactive	Processes Car Display input requests from the driver. If “Activate” function is received from the driver the Car Display ECU will first check that the Lane Assistance item is functioning correctly, and will then proceed to send a “Lane Active” message packet to set Car Display indicator to “ACTIVE” If “Deactivate” function is received from the driver the Car Display ECU send a “Lane Inactive” message packet to set Car Display indicator to “INACTIVE”
Car Display ECU - Lane Assistance malfunction warning	Processes data packets from Camera Sensor ECU. If the camera ECU detects bad packets(CRC or other error code) from the camera sensor than an error message packet is sent to the Car Display ECU to set the Car Display warning “MALFUNCTION” indicator.
Driver Steering Torque Sensor	Measures the torque applied to the power steering unit.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	• Processes status packets from Drivier Steering Torque Sensor ECU. • Detects “Lane Departure Alert” message

	packet and sends a command to the motor to apply an oscillating torque to the drive power steering unit. • Detects “In Lane” message packet and send a reset command to disable the oscillating torque if enabled.
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 and torque frequency is below Max_Torque_Ampllitude and Max_Torque_Frequency respectively.
EPS ECU - Lane Keeping Assistant Safety Functionality	Software module ensuring the Lane Keeping Assistance (LKA) module is not activated for longer than Max_Duration in time.
EPS ECU - Final Torque	Process the the safe steering torque requests by the LKA and the LDA and send to EPS ECU
Motor	Process the requested torque request and apply it to the steering wheel motor.

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 component shall ensure that the LDW_Torque_Request for lane departure warning is below Max_Torque_Amplitude.	C	50 ms	LDW Safety	The LDW torque amplitude is set to 0.
Technical Safety Requirement 02	When the LDW feature is deactivated, the LDW software component shall block any requests to activate a warning light to the car display ECU	C	50 ms	LDW Safety	The LDW torque amplitude is set to 0.
Technical Safety Requirement 03	Once a failure is detected the LDW feature is deactivated and a torque request shall not be sent.	C	50 ms	LDW Safety	The LDW torque amplitude is set to 0.
Technical Safety Requirement 04	The validity and integrity of the data transmission for LDW_Torque_Request shall be checked	C	50 ms	Data Transmission Integrity check	The LDW torque amplitude is set to 0.
Technical Safety Requirement 05	A memory test shall be conducted during the start up of the EPS ECU to check for any faults in memory.	A	Ignition Cycle	Memory Test	The LDW torque amplitude is set to 0.

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 component shall ensure that the LDW_Torque_Request frequency is below Max_Torque_Frequency.	C	50 ms	LDW Safety	The LDW torque frequency is set to 0.
Technical Safety Requirement 02	When the LDW feature is deactivated, the LDW software component shall block any requests to activate a warning light to the car display ECU	C	50 ms	LDW Safety	The LDW torque frequency is set to 0.
Technical Safety Requirement 03	Once a failure is detected the LDW feature is deactivated and a torque request shall not be sent.	C	50 ms	LDW Safety	The LDW torque frequency is set to 0.
Technical Safety Requirement 04	The validity and integrity of the data transmission for LDW_Torque_Request shall be checked	C	50 ms	Data Transmission Integrity check	The LDW torque frequency is set to 0.
Technical Safety Requirement 05	A memory test shall be conducted at start up of the EPS ECU to check for any faults in memory	A	Ignition Cycle	Memory Test	The LDW torque frequency is set to 0.

Lane Keeping Assistance (LKA) Requirements:

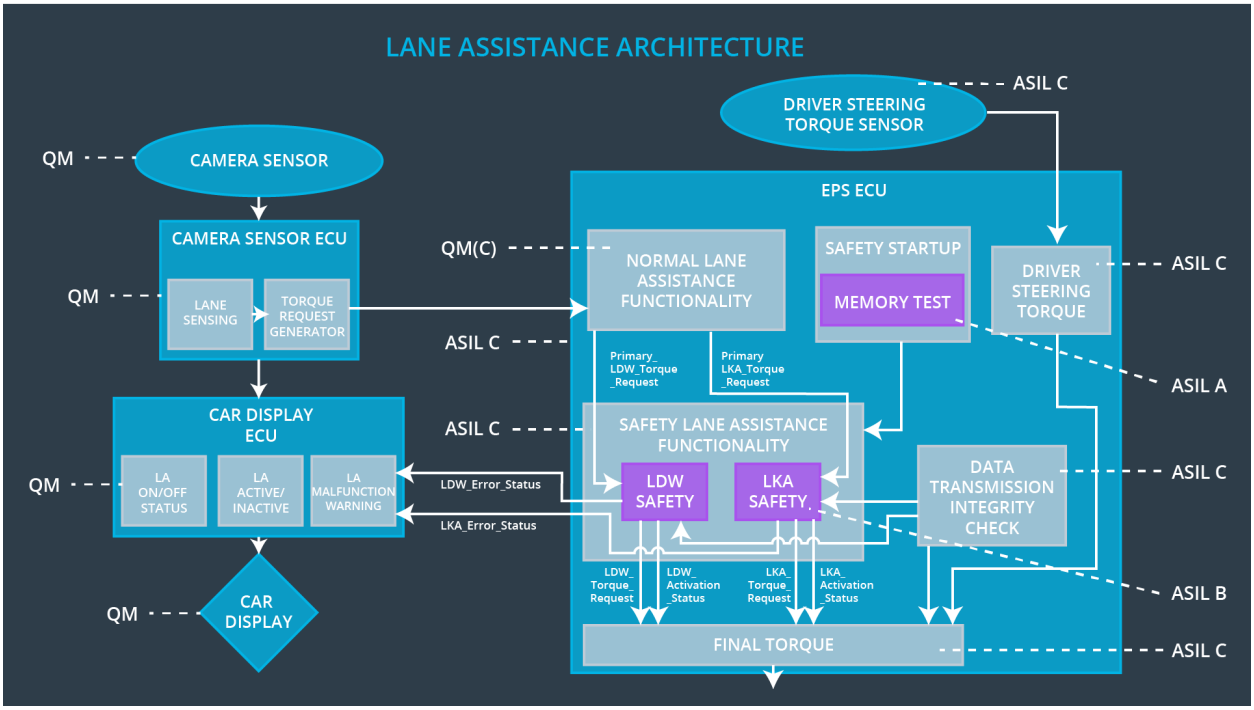
Functional Safety Requirement 02-1 with its associated system elements (derived in the functional safety concept)

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 component shall ensure that the LKA_Torque_Request sent does not exceed Max_Duration	B	500ms	LKA Safety	The LKA Torque Request is set to 0.
Technical Safety Requirement 02	When the LKA feature is deactivated, the LKA software component shall block any requests to activate a warning light to the car display ECU	B	500 ms	LKA Safety	The LKA Torque Request is set to 0.
Technical Safety Requirement 03	When a failure is detected by the LKA, it shall deactivate the LKA feature, and the LKA_Torque_Request shall be set to 0.	B	500 ms	LKA Safety	The LKA function is turned off.
Technical Safety Requirement 04	The validity and integrity of the data transmission for LDW_Torque_Request shall be checked	B	500 ms	Data Transmission Integrity check	The LKA Torque Request is set to 0.
Technical Safety Requirement 05	A memory test shall be conducted at start up of the EPS ECU to check for any faults in memory	A	Ignition Cycle	Memory Test	The LKA Torque Request is set to 0.

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	LDW is disabled	Malfunction_01, Malfunction_02,	Yes	Car Display provides visual indication that LDW is disabled
WDC-02	LKA is disabled	Malfunction_03	Yes	Car Display provides visual indication that LKA is disabled