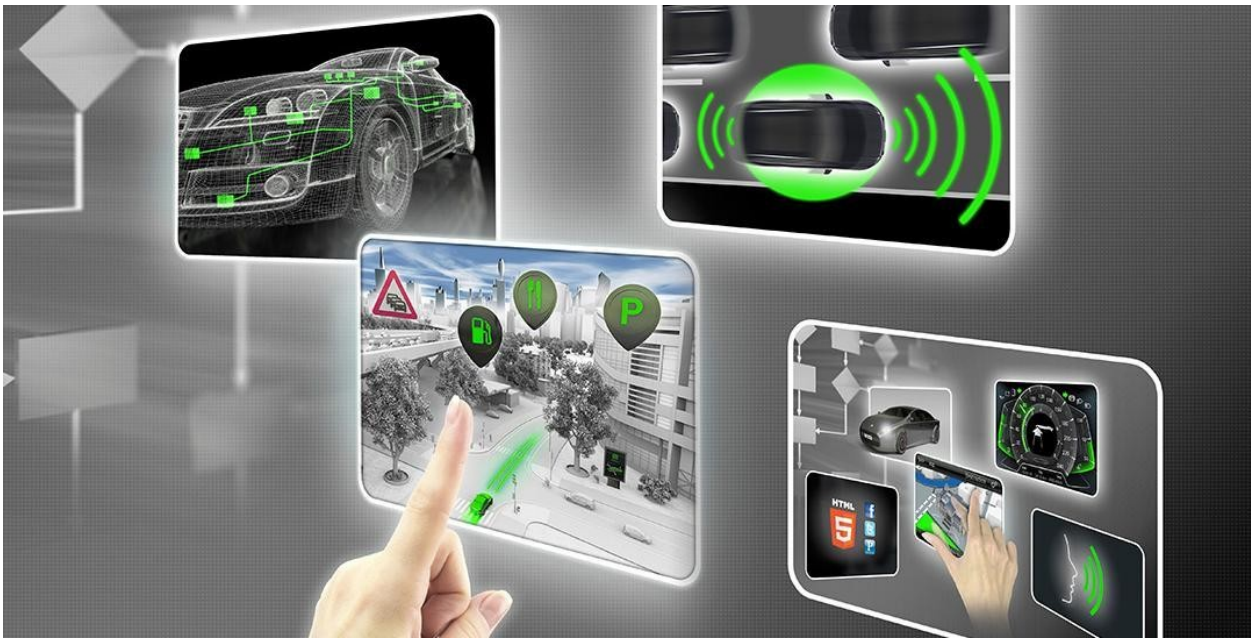
Elektrobit

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
12-27-18	1.0	Nick Fiege	
01-01-19	1.1	Nick Fiege	Changed Safe State for Functional Safety Requirement 01-01 and 01-02 after submission.

Table of Contents

Purpose of the Technical Safety Concept

The purpose of a technical safety concept is to:

- Define technical safety requirements
- Allocate these requirements to the system architecture

These steps are in essence the same as for the functional safety concept. However the functional safety concept defines requirements on a system and sub-system level. Whereas the technical safety concept is more concrete and will define and allocate requirements at sensor, control unit and actuator level and define the requirements on the interactions between them.

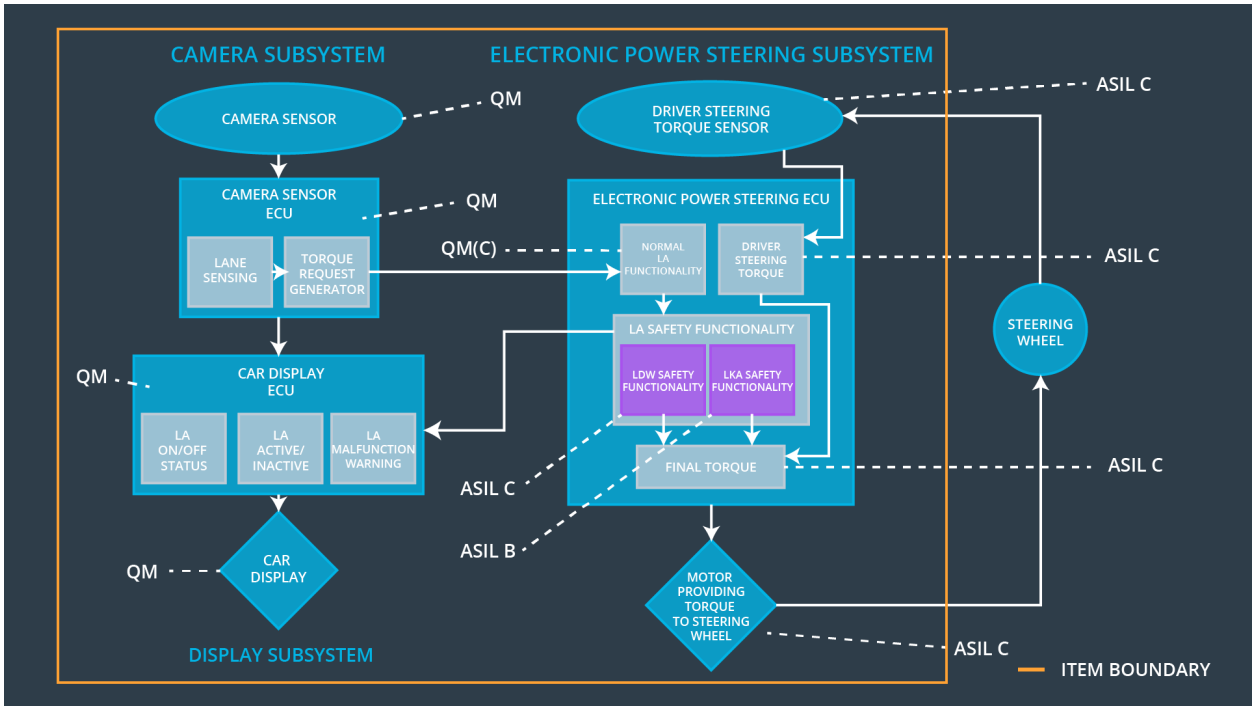
Inputs to the Technical Safety Concept

Functional Safety Requirements

[Instructions: Provide the functional safety requirements derived in the functional safety concept]

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 mas_torque_amplitude.	C	50 ms	Oscillating torque amplitude is set to zero.
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below max_torque_frequency.	C	50 ms	Oscillating torque frequency is set to zero.
Functional Safety Requirement 02-01	The Electronic Power Steering ECU shall ensure that the the applied torque used for maneuvering back to the center of the lane is applied for a maximum time defined by max_torque_duration.	B	500 ms	Torque is not applied anymore (set to zero).

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Provides images which can be processed for lane assistance.
Camera Sensor ECU - Lane Sensing	Processes given images to determine vehicle odometry and lane boundarys.
Camera Sensor ECU - Torque request generator	Calculates target torque requests with using ego vehicle odometry and lane information and sends these to the Electronic Power Steering ECU.
Car Display	Displays warnings and general information for the driver.
Car Display ECU - Lane Assistance On/Off Status	Processes and stores requests from the system to control the light indicating that the system is turned on/off.
Car Display ECU - Lane Assistant Active/Inactive	Processes and stores requests from the system to control the light indicating that the system is active/inactive.
Car Display ECU - Lane Assistance malfunction warning	Processes and stores requests from the system to control the light indicating that the system is malfunctioning.
Driver Steering Torque Sensor	Detects exterted torque to the steering wheel.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Processes and stores the torque exerted on the steering wheel by the driver to calculate the additional torque which has to be applied by the system in order to match the required torque from the Camera Sensor ECU - Torque request generator.
EPS ECU - Normal Lane Assistance Functionality	Processes and stores torque requests from the Camera Sensor ECU - Torque request generator for further processing in the EPS ECU.
EPS ECU - Lane Departure Warning Safety Functionality	Ensures that the torque amplitude stored is below max_torque_amplitude and the torque frequency stored is below max_torque_frequency.
EPS ECU - Lane Keeping Assistant Safety Functionality	Ensures that the operation time of the lane keeping assistance torque application remains below max_torque_duration.

EPS ECU - Final Torque	Uses resulting (safe) torque request which are applied to the motor.
Motor	Applies the torque requested from the Electronic Power Steering ECU to the steering wheel.

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	50 ms	LDW Safety	LDW sets torque request to zero.
Technical Safety Requirement 02	On deactivation of the LDW function, the LDW Safety shall send a signal to the display ECU to turn on a warning indicator.	C	50 ms	LDW safety	LDW sets torque request to zero.
Technical Safety Requirement 03	On error detection, the LDW safety shall deactivate the LDW function and the	C	50 ms	LDW safety	LDW sets torque request

	requested torque shall be set to zero.				to zero.
Technical Safety Requirement 04	The validity and integrity of the data transmission for torque request signals shall be ensured.	C	50 ms	LDW safety	LDW sets torque request to zero.
Technical Safety Requirement 05	A initialization memory test routine shall be conducted at start up of the EPS ECU to check for any faults in memory.	B	Initialization/Ignition cycle	Data transmission integrity check	LDW sets torque request 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 the 'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Frequency.	C	50 ms	LDW safety	LDW sets torque request to zero.
Technical Safety Requiremen 02	On deactivation of the LDW function, the LDW Safety shall send a signal to the display ECU to turn on a warning indicator.	C	50 ms	LDW safety	LDW sets torque request to zero.
Technical Safety Requirement 03	On error detection, the LDW safety shall deactivate the LDW function	C	50 ms	LDW safety	LDW sets torque

	and the requested torque shall be set to zero.				request to zero.
Technical Safety Requirement 04	The validity and integrity of the data transmission for torque request signals shall be ensured.	C	50 ms	LDW safety	LDW sets torque request to zero.
Technical Safety Requirement 05	A initialization memory test routine shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Initialization/Ignition cycle	Data transmission integrity check	LDW sets torque request to zero.

Lane Keeping Assistance (LKA) Requirements:
Functional Safety Requirement 02-1 with its associated system elements (derived in the functional safety concept)

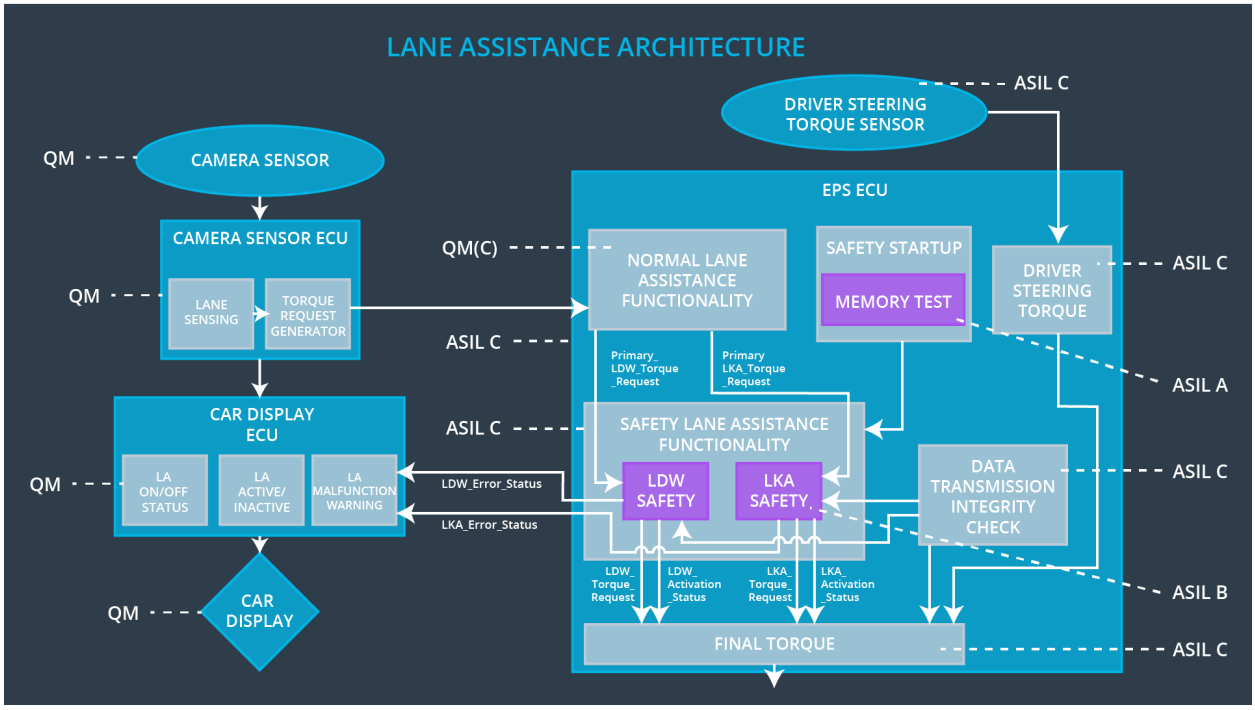
ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	X		

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 Electronic Power Steering ECU shall ensure that the the applied torque used for maneuvering back to the center of the lane is applied for a maximum time defined by max_torque_duration.	B	500 ms	LKA safety	LKA sets torque request to zero.
Technical Safety Requirement 02	On deactivation of the LDW function, the LDW Safety shall send a signal to the	B	500 s	LKA safety	LKA sets torque request to zero.

	display ECU to turn on a warning indicator.				
Technical Safety Requirement 03	On error detection, the LDW safety shall deactivate the LDW function and the requested torque shall be set to zero.	B	500 ms	LKA safety	LKA sets torque request to zero.
Technical Safety Requirement 04	The validity and integrity of the data transmission for torque request signals shall be ensured.	B	500 ms	LKA safety	LKA sets torque request to zero.
Technical Safety Requirement 05	A initialization memory test routine shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Initialization/Ignition cycle	Data transmission integrity check	LKA sets torque request to zero.

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

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 mas_torque_amplitude.	**x**		
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below max_torque_frequency.	**x**		
Functional Safety Requirement 02-01	The Electronic Power Steering ECU shall ensure that the the applied torque used for maneuvering back to the center of the lane is applied for a maximum time defined by max_torque_duration.	**x**		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Lane assistance system is turned off.	Malfunction_01 Malfunction_02 Malfunction_03 Malfunction_04	Yes	Dashboard warning light, Display warning