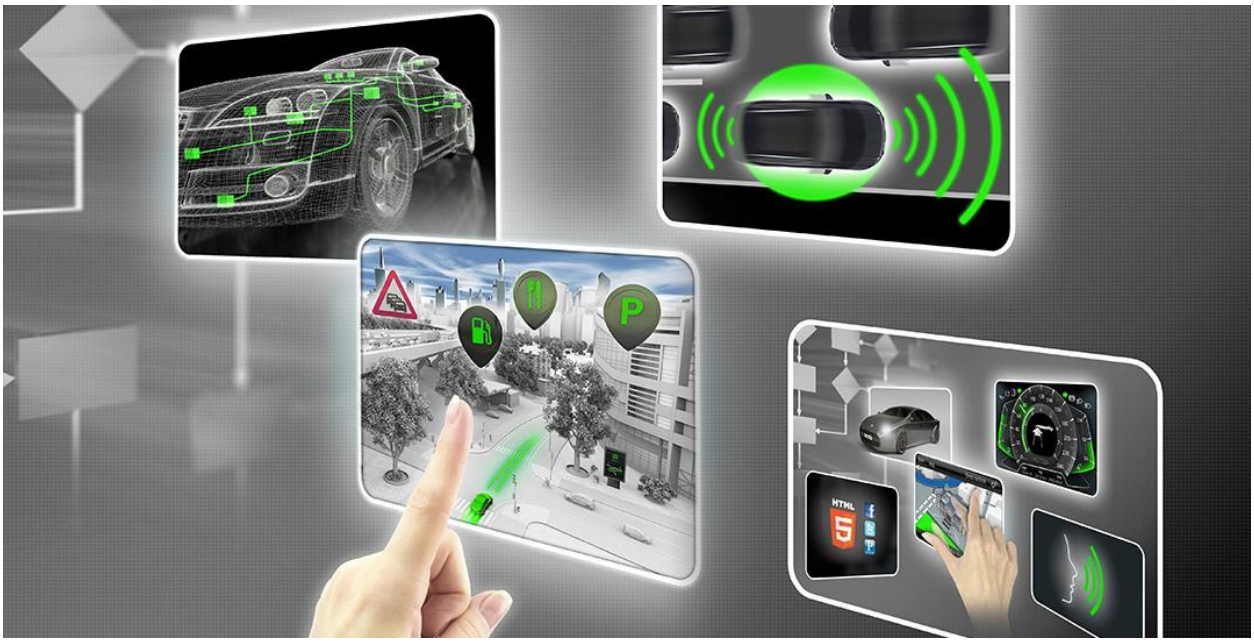
Elektrobit

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
2018-09-30	1.0	Rob Poyck	First setup

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

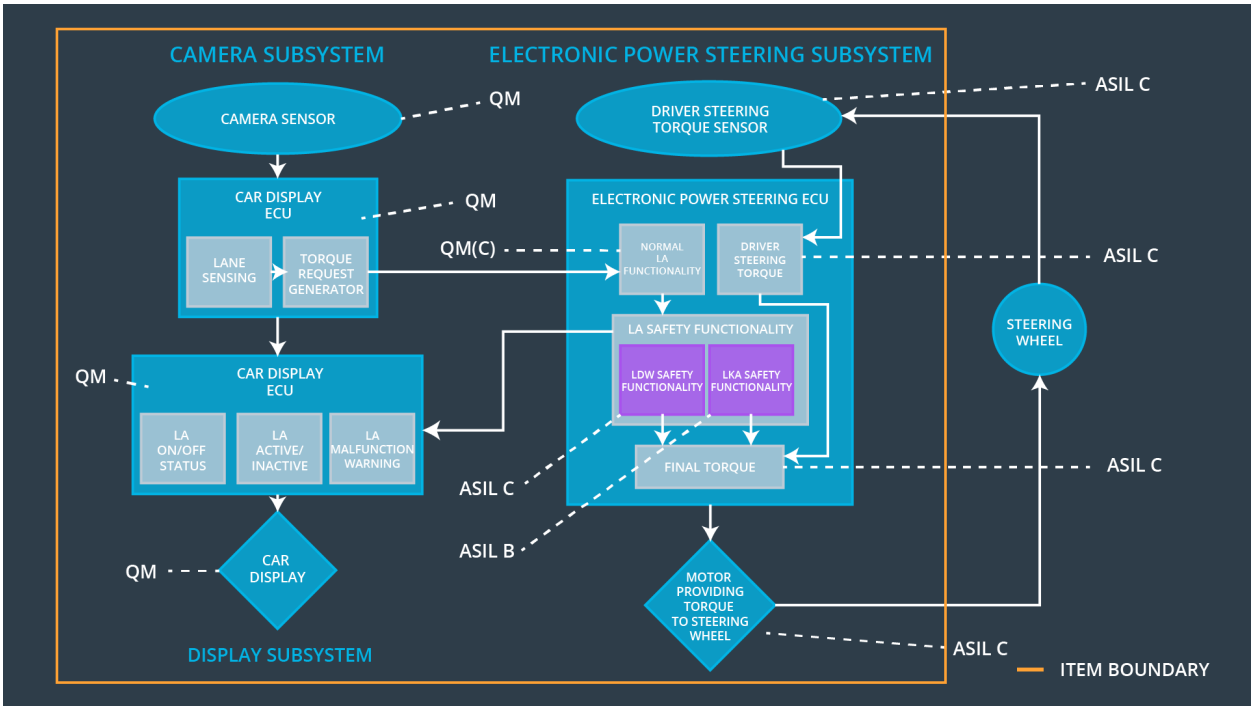
These steps are in essence the same as for the functional safety concept. However the functional safety concept defines requirements on a system and sub-system level. Whereas the technical safety concept is more concrete and will define and allocate requirements at sensor, control unit and actuator level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

Inputs to the Technical Safety Concept

Functional Safety Requirements

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]	Lane assistant system turned off.
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]	Lane assistant system turned off.
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	500 [ms]	Lane assistant system turned off.
Functional Safety Requirement 02-02	The system shall only be active when the torque exerted by the driver is propertly detected by the power steering system torque sensor.	D	50 [ms]	Lane assistant system turned off.

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Provides the camera images for analyses by the camera sensor ECU.
Camera Sensor ECU - Lane Sensing	Processes the images from the camera sensor in order to determine the position of the vehicle w.r.t. the lane lines.
Camera Sensor ECU - Torque request generator	Using the information from the Lane sensing, actuation requests might be sent to the power steering system when the vehicle leaves the lane unintendedly.
Car Display	Indicate information and warnings/errors to the driver.
Car Display ECU - Lane Assistance On/Off Status	Processes and stores the requests by the system to turn the light on that the system is turned on.
Car Display ECU - Lane Assistant Active/Inactive	Processes and stores the requests by the system to turn the light on that the system is active.
Car Display ECU - Lane Assistance malfunction warning	Processes and stores the requests by the system to turn the light on that the system has malfunctioned.
Driver Steering Torque Sensor	Detects the torque already exerted on the steering wheel by the driver.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Processes and stores the torque exerted on the steering wheel by the driver, in order to calculate the additional torque which has to be applied by the system in order to match the required torque from the torque request generator.
EPS ECU - Normal Lane Assistance Functionality	Processes and stores the torque requests by the camera ECU for further processing in the EPS ECU.
EPS ECU - Lane Departure Warning Safety Functionality	A functionality to ensure that the torque amplitude is below max_torque_amplitude and the torque frequency is below max_torque_frequency, before further processing in the EPS ECU.

EPS ECU - Lane Keeping Assistant Safety Functionality	Functionaly to ensure that the active time of the lane keeping assistance remains below the max_duration time.
EPS ECU - Final Torque	Generates the final additional torque request which has to be supplied by the system and sends it to the EPS motor.
Motor	Applies the torque requested from the EPS 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	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	50 [ms]	LDW safety	LDW sets torque request to zero.

Technical Safety Requirement 03	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	LDW sets torque request 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]	LDW safety	LDW sets torque request to 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	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 Requirement 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	50 [ms]	LDW safety	LDW sets torque request to zero.
Technical Safety Requirement 03	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	LDW sets torque request 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]	LDW safety	LDW sets torque request to 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	Data transmission integrity check	LDW sets torque request to zero.

Lane Keeping Assistance (LKA) Requirements:

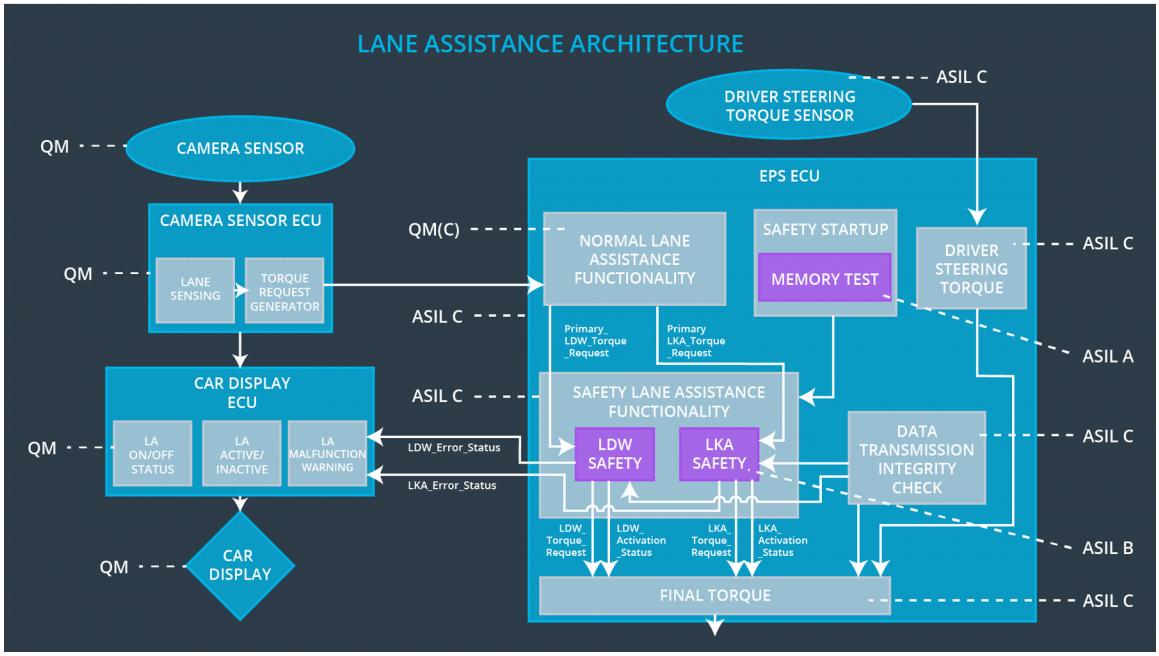
Functional Safety Requirement 02-1 with its associated system elements (derived in the functional safety concept)

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 Lane Keeping Assistant (LKA) safety component shall ensure that the 'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' for no more than max_duration.	B	500 [ms]	LKA safety	LKA sets torque request to zero.
Technical Safety Requirement 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.	B	500 [ms]	LKA safety	LKA sets torque request to zero.
Technical Safety Requirement 03	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.	B	500 [ms]	LKA safety	LKA sets torque request to zero.
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	B	500 [ms]	LKA safety	LKA sets torque request to 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	Data transmission integrity check	LKA sets torque request to zero.

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

For this item, the lane assistant item, all the above mentioned safety requirements are allocated to the electronic power steering ECU, as specified in the functional safety requirements above.

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Lane assistant system turned off.	Malfunction_01, Malfunction_02, Malfunction_03, Malfunction_04	Yes	A lane assistant system malfunction light on the dashboard