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
2018.05.26	1.0	A. Fuchs	Initial revision

Table of Contents

Document history

Table of Contents

Purpose of the Technical Safety Concept

Inputs to the Technical Safety Concept
- Functional Safety Requirements
- Refined System Architecture from Functional Safety Concept
  - Functional overview of architecture elements

Technical Safety Concept
- Technical Safety Requirements
- Refinement of the System Architecture
- Allocation of Technical Safety Requirements to Architecture Elements
- Warning and Degradation Concept

Purpose of the Technical Safety Concept

[Instructions: Answer what is the purpose of a technical safety concept?]
The purpose of the technical safety concept is to turn functional safety requirements into technical safety requirements. It is part of the product development phase of the V-Model and looks at the technical implementation of the item.
It allocates the technical safety requirements to the system architecture and describes in detail what the system shall do when a malfunction violates a safety goal.

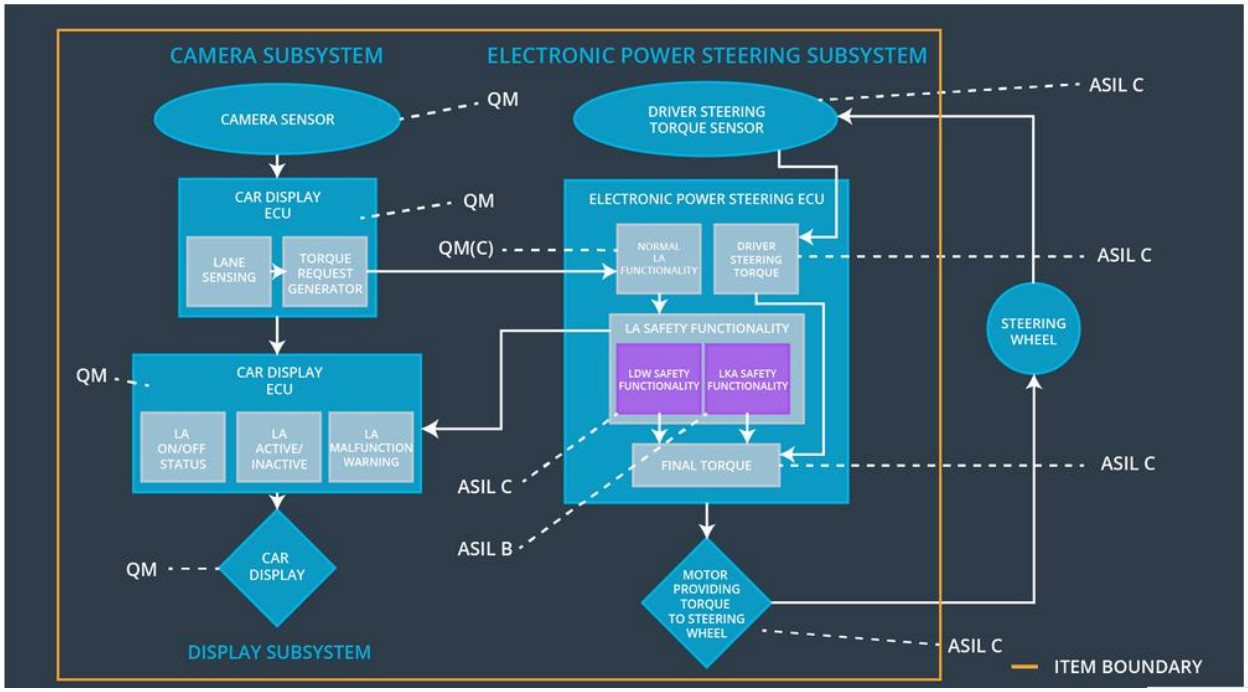
Inputs to the Technical Safety Concept

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 lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	C	50ms	Turn off LDW function.
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50ms	Turn off LDW function.
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	Turn of the LKA function.

Refined System Architecture from Functional Safety Concept

[Instructions: Provide the refined system architecture from the functional safety concept]



Functional overview of architecture elements

[Instructions: Provide a description for each functional safety element; what is each element's purpose in the lane assistance item?]

Element	Description
Camera Sensor	Provide the raw input (images) for the Camera Sensor ECU.
Camera Sensor ECU - Lane Sensing	Process the raw images and detect the lane lines and if the vehicle stays in the lane.
Camera Sensor ECU - Torque request generator	As an unintentionally drifting from the ego lane is detected the Camera Sensor ECU generates a Torque request (for LDW and LKF).

Car Display	Give visual outputs to the driver to inform or warn him of current system states.
Car Display ECU - Lane Assistance On/Off Status	Provide a visual indicator whether the lane assistance function is on or off.
Car Display ECU - Lane Assistant Active/Inactive	Provide a visual indicator whether the lane assistance function is active or inactive.
Car Display ECU - Lane Assistance malfunction warning	Provide a visual indicator (warning lamp) if the system has detected a malfunction and is turned off to transition into a safe state.
Driver Steering Torque Sensor	Measuring of the steering torque of the steering wheel.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Processes the generated Torque Request by the Camera Sensor ECU and outputs a Torque Request to the motor that applies steering torque to the steering wheel.
EPS ECU - Normal Lane Assistance Functionality	Processes the generated Torque Request by the Camera Sensor ECU and forwards it to the LA Safety Functionality.
EPS ECU - Lane Departure Warning Safety Functionality	Processes the Torque Request in terms of safety checks. Checks if the Technical Safety Requirements for the LDW function are fulfilled. Checks the data transmission for validity and integrity and evaluates the safety startup memory check to prevent latent faults.
EPS ECU - Lane Keeping Assistant Safety Functionality	Processes the Torque Request in terms of safety checks. Checks if the Technical Safety Requirements for the LKA function are fulfilled. Checks the data transmission for validity and integrity and evaluates the safety startup memory check to prevent latent faults.
EPS ECU - Final Torque	Final torque output that is sent to the e-motor to apply additional torque to the steering wheel.
Motor	Generates output torque for additional steering torque applied 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 01-01-01	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 Functionality block	Turn off. Set oscillating torque to zero.
Technical Safety Requirement 01-01-02	The LDW safety component shall ensure that the validity and integrity of the data transmission for 'LDW_Torque_Request' signal	C	50ms	Data Transmission Integrity Check	Turn off. Set oscillating torque to zero.

	shall be ensured.				
Technical Safety Requirement 01-01-03	As soon as a failure is detected by the LDW function, it shall deactivate the LDC feature and the ‘LDW_Torque_Request’ shall be set to zero.	C	50ms	LDW Safety Functionality block	Turn off. Set oscillating torque to zero.
Technical Safety Requirement 01-01-04	As soon as the LDW function deactivates the LDC feature the LDW safety software block shall send a signal to the car display ECU to turn on a warning lamp.	C	50ms	LDW Safety Functionality block	Turn off. Set oscillating torque to zero.
Technical Safety Requirement 01-01-05	Memory test shall be conducted at start of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Memory Test Block	Turn off. Set oscillating torque 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 01-02-01	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 Functionality block	Turn off. Set oscillating torque to zero.
Technical Safety Requirement 01-02-02	The LDW safety component shall ensure that the validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50ms	Data Transmission Integrity Check	Turn off. Set oscillating torque to zero.
Technical Safety Requirement 01-02-03	As soon as a failure is detected by the LDW function, it shall deactivate the LDC feature and the 'LDW_Torque_Request' shall be set to zero.	C	50ms	LDW Safety Functionality block	Turn off. Set oscillating torque to zero.
Technical Safety Requirement 01-02-04	As soon as the LDW function deactivates the LDC feature the LDW safety software block shall send a signal to the car display ECU to turn on a warning lamp.	C	50ms	LDW Safety Functionality block	Turn off. Set oscillating torque to zero.
Technical Safety Requirement 01-02-05	Memory test shall be conducted at start of the EPS ECU to check for any faults in memory.	A	Ignition cyle	Memory Test Block	Turn off. Set oscillating torque to zero.

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

ID	Technical Safety Requirement	ASIL	Validation Acceptance Criteria	Verification Criteria
Technical Safety Requirement 01-01-01	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	Test if the value for Max_Torque_Amplitude is chosen appropriate by testing different drivers' reaction to different torque amplitudes.	Software test by inserting a fault into the system and test if the torque output is 0Nm within the 50ms FTTI.
Technical Safety Requirement 01-01-02	The LDW safety component shall ensure that the validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	Test if the signal implemented validity and integrity test detects potentially corrupted data transmission in a robust manner.	Software test with artificial corrupted data transmission.. HW test with artificially created malfunctions in the hardware components e.g. short-circuit. Check if corrupted data transmission is detected within the 50ms FTTI.
Technical Safety Requirement 01-01-03	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	Test if the 'LDW_Torque_Request' is set to zero .	SW test with artificial created faults and measure if time of safe state transition is within the defined FTTI..
Technical Safety Requirement 01-01-04	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 lamp.	C	Test if the warning lamp is an appropriate visual indicator by testing different drivers time to notice the warning lamp.	SW test by inserting a fault into the system and test if a warning is issued in terms of a warning lamp within the 50ms FTTI.
Technical Safety Requirement	Memory test shall be conducted at start of the EPS ECU to check for any faults in memory.	A	Test if the determined FTTI (ignition cycle) is	Software test of the detection time with artificial created

01-01-05			appropriate to detect possible memory errors.	memory errors and check if the memory fault is detected within the defined ignition cycle FTTI.
Technical Safety Requirement 01-02-01	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	Test if the value for Max_Torque_Frequency is chosen appropriate by testing different drivers' reaction to different torque frequencies.	Software test by inserting a fault into the system and test if the torque output is 0Nm within the 50ms FTTI.

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 02-01-01	The LDW safety component shall ensure that the time interval for assistance torque application sent to the 'Final Electronic Power	B	500ms	LDW Safety Functionality block	Turn off. (Set 'LDW_Torque_Request' to zero.

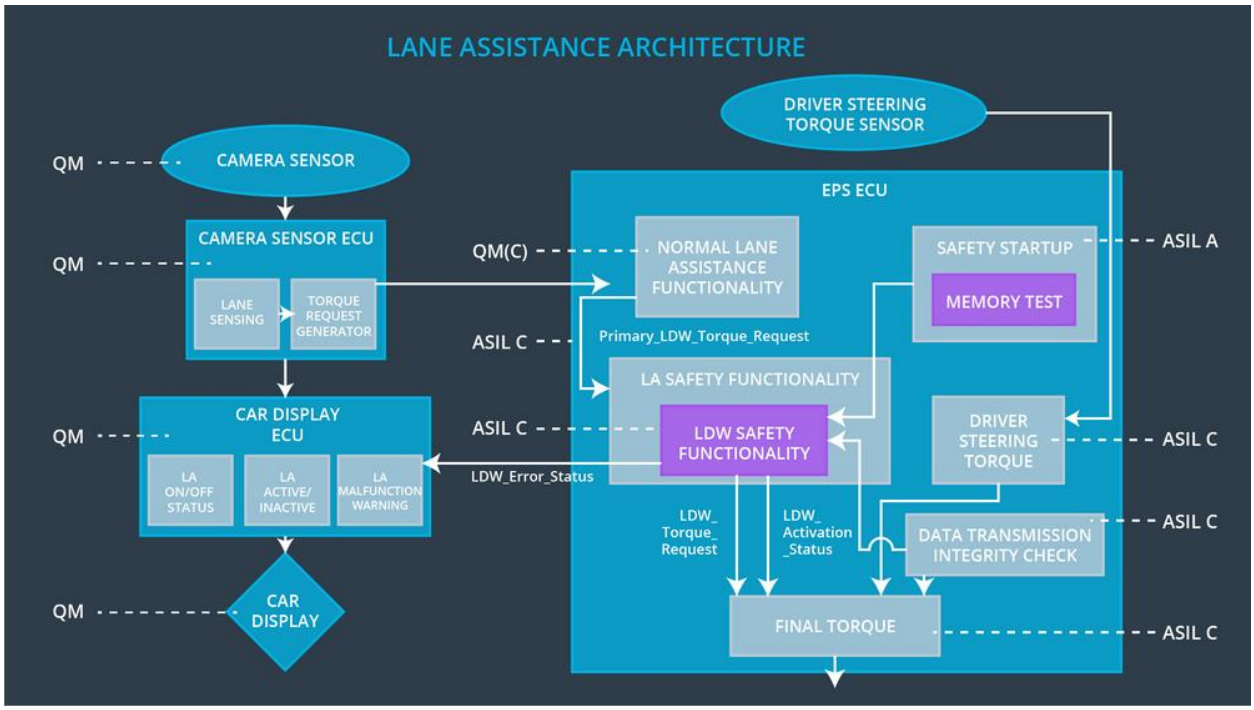
	Steering Torque' component is below 'Max_Duration'.				
Technical Safety Requirement 02-01-02	The LDW safety component shall ensure that the validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	B	500ms	Data Transmission Integrity Check	Turn off. (Set 'LDW_Torque_Request' to zero.
Technical Safety Requirement 02-01-03	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	500ms	LDW Safety Functionality block	Turn off. (Set 'LDW_Torque_Request' to zero.
Technical Safety Requirement 02-01-04	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 lamp.	B	500ms	LDW Safety Functionality block	Turn off. (Set 'LDW_Torque_Request' to zero.
Technical Safety Requirement 02-01-05	Memory test shall be conducted at start of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Memory Test Block	Turn off. (Set 'LDW_Torque_Request' to zero.

Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:

ID	Technical Safety Requirement	ASIL	Validation Acceptance Criteria	Verification Criteria
Technical Safety Requirement 02-01-01	The LDW safety component shall ensure that the time interval for assistance torque application sent to the 'Final Electronic Power Steering Torque' component is below 'Max_Duration'.	B	Test if the value for Max_Duration dissuades drivers from taking their hands off the wheel.	Test if the system turns off if the lane keeping assistance exceeds Max_Duration.
Technical Safety Requirement 02-01-02	The LDW safety component shall ensure that the validity and integrity of the data transmission for	B	Test if the signal implemented validity and integrity test	Software test with artificial corrupted data transmission.. HW test with

	‘LDW_Torque_Request’ signal shall be ensured.		detects potentially corrupted data transmission in a robust manner.	artificially created malfunctions in the hardware components e.g. short-circuit. Check if corrupted data transmission is detected within the 50ms FTTI.
Technical Safety Requirement 02-01-03	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	Test if the ‘LDW_Torque_Request’ is set to zero .	SW test with artificial created faults and measure if time of safe state transition is within the defined FTTI..
Technical Safety Requirement 02-01-04	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 lamp.	B	Test if the warning lamp is an appropriate visual indicator by testing different drivers time to notice the warning lamp.	SW test by inserting a fault into the system and test if a warning is issued in terms of a warning lamp within the 50ms FTTI.
Technical Safety Requirement 02-01-05	Memory test shall be conducted at start of the EPS ECU to check for any faults in memory.	A	Test if the determined FTTI (ignition cycle) is appropriate to detect possible memory errors.	Software test of the detection time with artificial created memory errors and check if the memory fault is detected within the defined ignition cycle FTTI.

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

For this particular item 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	Turn off the system.	Torque amplitude is higher than Max_Torque_Amplitude	Yes	Warning lamp at the vehicle dashboard.
WDC-02	Turn off the system.	Torque frequency is higher than Max_Torque_Fr	Yes	Warning lamp at the vehicle dashboard.

		equency		
WDC-03	Turn off the system.	Duration of torque application is higher than ‘Max_Duration’	Yes	Warning lamp at the vehicle dashboard.