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
02.09.17	1.0	Klemens Esterle	Initial Version

Table of Contents

Purpose of the Technical Safety Concept

The purpose of the technical safety concept is to derive technical requirements from functional requirements.

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 warning oscilatting torque amplitude is below Max_Torque_Amplitude	C	50ms	System turned off
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure warning oscilatting torque frequency is below Max_Torque_Frequency	C	50ms	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	500ms	System turned off
Functional Safety Requirement 02-02	The camera sensor ECU shall ensure that the system is switched off if the detection uncertainty is below Min_Detection_Certainty	B	50ms	System turned off

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	Front camera sensor to film lane in front
Camera Sensor ECU - Lane Sensing	ECU using algorithms to extract lane information from camera video stream
Camera Sensor ECU - Torque request generator	ECU generating torque request and forwarding it to EPS ECU
Car Display	Interface to human showing current status of functionality (on, off)
Car Display ECU - Lane Assistance On/Off Status	ECU to process input from driver (switch on/off)
Car Display ECU - Lane Assistant Active/Inactive	ECU processing any system status for visualization to driver
Car Display ECU - Lane Assistance malfunction warning	ECU processing malfunction warning
Driver Steering Torque Sensor	Sensor to measure applied steering torque by driver to steering wheel
Electronic Power Steering (EPS) ECU - Driver Steering Torque	and sending necessary torque signal to motor
EPS ECU - Normal Lane Assistance Functionality	ECU forwarding torque request to safety lane assistance functionality
EPS ECU - Lane Departure Warning Safety Functionality	ECU generating lane departure warning and sending it to CAR Display ECU
EPS ECU - Lane Keeping Assistant Safety Functionality	ECU performing LDW safety check
EPS ECU - Final Torque	ECU to process request for returning to lane
Motor	Actuator applying torque to 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	50ms	LDW safety element	LDW torque request amplitude shall be set to zero
Technical Safety Requirement 02	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured	C	50ms	Data transmission ingegrity check item	LDW torque output is set to zero
Technical Safety Requirem	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and	C	50ms	LDW safety element	LDW torque output is set to zero

ent 03	the ‘LDW_Torque_Request’ shall be set to zero				
Technical Safety Requirement 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 light	C	50ms	LDW safety element	LDW torque output is set to zero
Technical Safety Requirement 05	Memory test shall be conducted at start of the EPS ECU to check for any faults in memory	A	Length of vehicle ignition cycle	Memory test item	LDW torque output 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 the ‘LDW_Torque_Request’ sent to the ‘Final electronic power steering Torque’ component is below ‘Max_Torque_Frequency’	C	50ms	LDW safety element	LDW torque request amplitude shall be set to zero

Technical Safety Requirement 02	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured	C	50ms	Data transmission ingegrity check item	LDW torque output is set 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	50ms	LDW safety element	LDW torque output is set to zero
Technical Safety Requirement 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 light	C	50ms	LDW safety element	LDW torque output is set to zero
Technical Safety Requirement 05	Memory test shall be conducted at start of the EPS ECU to check for any faults in memory	A	Length of vehicle ignition cycle	Memory test item	LDW torque output is set to zero

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

[OPTIONAL: For each technical safety requirement, identify both the verification and validation acceptance criteria. "Validation" asks whether or not you chose the appropriate parameters. "Verification" involves testing to make sure the vehicle behaves as expected when the parameter value is crossed. There is not necessarily one right answer. Look at your verification and validation acceptance criteria from the functional safety concept for inspiration.]

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	Camera	Car Display

		Power Steering ECU	ECU	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 safety component shall ensure that the duration of the 'LKA_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Duration'	B	500ms	LKA safety element	LKA torque request amplitude shall be set to zero
Technical Safety Requirement 02	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured	B	500ms	Data transmission ingegrity check item	N/A
Technical Safety Requirement 03	As soon as a failure is detected by the LKA function, it shall deactivate the LDW feature and the 'LKA_Torque_Request' shall be set to zero	B	500ms	LKA safety element	LKA torque output is set to zero
Technical Safety Requirement 04	As soon 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	500ms	LKA safety element	LKA torque output is set to zero
Technical Safety Requirement 05	Memory test shall be conducted at start of the EPS ECU to check for any faults in memory	A	Length of vehicle ignition cycle	Memory test item	LKA torque output is set to zero

Functional Safety Requirement 02-2 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 02-02	The camera sensor ECU shall ensure that the system is switched off if the detection uncertainty is below Min_Detection_Certainty	X	X	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 safety component shall ensure that the value of the 'LKA_Lane_Detection_Certainty' sent to the 'Final electronic power steering Torque' component is below 'Min_Detection_Certainty'	B	50ms	LKA safety element	LKA torque request amplitude shall be set to zero
Technical Safety Requirement 02	The validity and integrity of the data transmission for 'LKA_Lane_Detection_Certainty'' signal shall be ensured	B	50ms	Data transmission ingegrity check item	N/A
Technical Safety Requirement 03	As soon as a failure is detected by the LKA function, it shall deactivate the LDW feature and the 'LKA_Torque_Request' shall be set to zero	B	50ms	LKA safety element	LKA torque output is set to zero
Technical Safety Requirement 04	As soon 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	50ms	LKA safety element	LKA torque output is set to zero
Technical	Memory test shall be conducted	A	Length of	Memory test	LKA torque

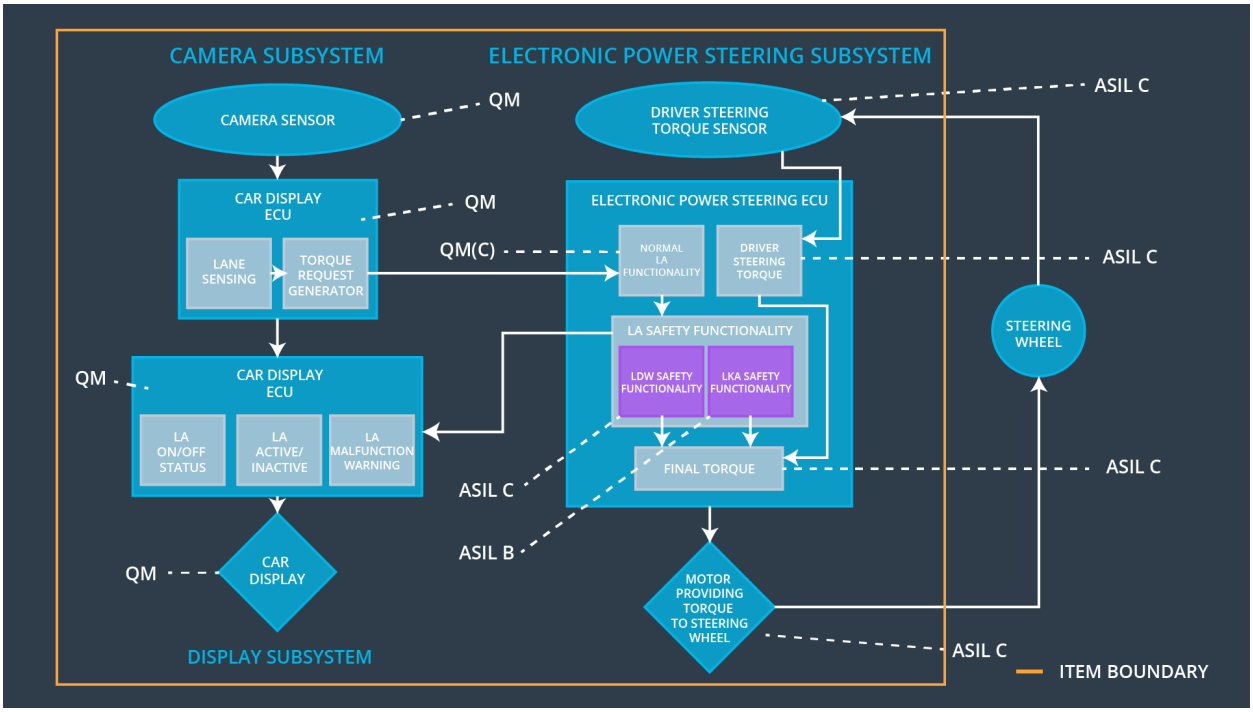
Safety Requirement 05	at start of the EPS ECU to check for any faults in memory		vehicle ignition cycle	item	output is set to zero

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

[OPTIONAL: For each technical safety requirement, identify both the verification and validation acceptance criteria. “Validation” asks whether or not you chose the appropriate parameters. “Verification” involves testing to make sure the vehicle behaves as expected when the parameter value is crossed. There is not necessarily one right answer. Look at your verification and validation acceptance criteria from the functional safety concept for inspiration.]

Refinement of the System Architecture

[Instructions: Include the refined system architecture. Hint: The refined system architecture should include the system architecture from the end of the technical safety lesson, including all of the ASIL labels.]



Allocation of Technical Safety Requirements to Architecture Elements

[Instructions: We already included the allocation as part of the technical requirement tables. Here you can state that for this particular item, all technical safety requirements are allocated to the Electronic Power Steering ECU]

Warning and Degradation Concept

[Instructions: We've already identified that for any system malfunction, the lane assistance functions will be turned off and the driver will receive a warning light indication. The technical safety requirements have not changed how functionality will be degraded or what the warning will be.

So in this case, the warning and degradation concept is the same for the technical safety requirements as for the functional safety requirements. You can copy the functional safety warning and degradation concept here.

Oftentimes, a technical safety analysis will lead to a more detailed warning and degradation concept.]

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off functionality	Malfunction_01, Malfunction_02	yes	warning light on the dashboard
WDC-02	Turn off functionality	Malfunction_03	yes	warning light on the dashboard, acoustic signal
WDC-03	Gradual degredation	Malfunction_04	yes	warning light on the dashboard, acoustic signal