Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: [0.2]

Document history

[Instructions: Fill in the date, version and description fields. You can fill out the Editor field with your name if you want to do so. Keep track of your editing as if this were a real world project.

Date	Version	Editor	Description
25.8.2017	0.1	Aneeq Mahmood	Technical Safety Concept Lane Assistance
28.8.2017	0.2	Aneeq Mahmood	Fixed comments from reviewer

Table of Contents

Purpose of the Technical Safety Concept

[Instructions: Answer what is the purpose of a technical safety concept?]
Technical safety concept is an upgrade on functional safety concept (FSC); it takes the safety requirements devised in FSC and refines them so that they can be technically specified in terms of hardware and software changes, to be made inside the system architecture.

Inputs to the Technical Safety Concept

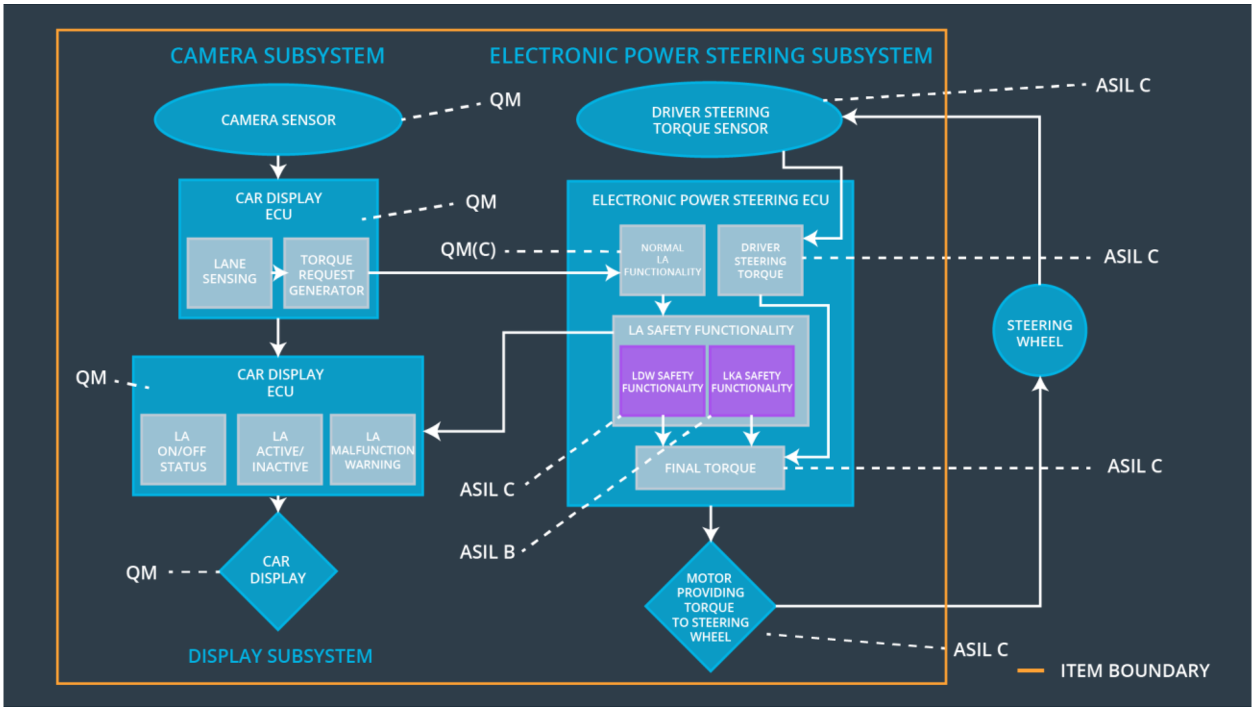
Functional Safety Requirements

[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 EPS ECU shall ensure that the oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	Off
Functional Safety Requirement 01-02	The EPS ECU shall ensure that the oscillating torque amplitude is below Max_Torque_Frequency	C	50 ms	Off
Functional Safety Requirement 02-01	The EPS ECU shall ensure that the LKA support is available for only Max_Duration	B	500 ms	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	Captures the road and sends the captured frames to the camera sensor ECU
Camera Sensor ECU - Lane Sensing	ECU for sensing if the vehicle is in lane or is drifting out mistakenly
Camera Sensor ECU - Torque request generator	ECU for requesting torque generation to bring the car in the lane center or create haptic feedback
Car Display	Takes the input from car display ECU to turn the LEDS Off or On, active/Inactive or malfunction state
Car Display ECU - Lane Assistance On/Off Status	Shows the On or Off state of lane assistance system
Car Display ECU - Lane Assistant Active/Inactive	Shows the Active or Inactive state of lane assistance system
Car Display ECU - Lane Assistance	Shows if Lane Assistance system is working

malfunction warning	correctly or not
Driver Steering Torque Sensor	Measures the torque coming from the driver
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Receives input from Driver Steering Torque Sensor and sends final required torque value to EPS ECU final torque
EPS ECU - Normal Lane Assistance Functionality	Receives the input from the Camera Sensor ECU and is responsible for generating requests for torques for LDW and LKA functionality
EPS ECU - Lane Departure Warning Safety Functionality	It is part of the Safety Lane Assistance Functionality. It gets Primary_LDW_Torque_Request from Normal Lane Assistance Functionality And eventually creates LDW_Torque_Request to generate final torque. Its also create LDW_Activation_Status. Lastly, it sends LDW_Error_Status to Car Display ECU
EPS ECU - Lane Keeping Assistant Safety Functionality	is part of the Safety Lane Assistance Functionality. It gets Primary_LKA_Torque_Request from Normal Lane Assistance Functionality And eventually creates LKA_Torque_Request to generate final torque. Its also create LKA_Activation_Status. Lastly, it sends LKA_Error_Status to Car Display ECU
EPS ECU - Final Torque	Sends the final required torque value to the motor
Motor	Takes its input from the EPS ECU and responsible for providing torque to the steering wheel and also

Technical Safety Concept

Technical Safety Requirements

[Instructions: Fill in the technical safety requirements for the lane departure warning first functional safety requirement. We have provided the associated functional safety

requirement in the first table below. Hint: The technical safety requirements were discussed in the lesson videos. The architecture allocation column should contain element names such as LDW Safety block, Data Transmission Integrity Check, etc. Allocating the technical safety requirements to the "EPS ECU" does not provide enough detail for a technical safety concept.]

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 Functionality	Off
Technical Safety Requirement 02	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 Functionality	Off
Technical Safety Requirement 03	As soon as the LDW function deactivates the LDW feature, the 'LDW Safety' software block shall	C	50 ms	LDW Safety Functionality	Off

	send a signal to the car display ECU to turn on a warning light.				
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50 ms	Data Transmission integrity check	Off
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	Safety startup	Off

[Instructions: Fill in the technical safety requirements for the lane departure warning second functional safety requirement. We have provided the associated functional safety requirement in the table below. Hint:. Most of the technical safety requirements will be the same. At least one technical safety requirement will have to be slightly modified because we are talking about frequency instead of amplitude. These requirements were not given in the lessons]

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 amplitude of the 'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Frequency	C	50 ms	LDW Safety Functionality	Off
Technical Safety Requirement 02	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 Functionality	Off
Technical Safety Requirement 03	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 Functionality	Off
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50 ms	Data Transmission integrity check	Off
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	Safety startup	Off

Lane Keeping Assistance (LKA) Requirements:

[Instructions: Fill in the technical safety requirements for the lane keeping assistance functional safety requirement 02-01. We have provided the associated functional safety requirement in the table below. Hint:. You can reuse the technical safety requirements from functional safety requirement 01-01. But you need to change the language because we are now looking at a different system. The ASIL and Fault Tolerant Time Interval are different as well.]

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 safety component shall ensure that the 'LKA_Torque_Request' sent to the ' Final electronic power steering Torque' component is applied for only Max_Duration	B	500 ms	LKA Safety Functionality	Off
Technical Safety Requirement 02	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	500 ms	LKA Safety Functionality	Off
Technical Safety Requirement 03	As soon as a failure is detected by the LKA f unction, it shall deactivate the LKA feature and the 'LKA_Torque_Request' shall be set to zero.	B	500 ms	LKA Safety Functionality	Off
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	B	500 ms	Data Transmission safety check	Off

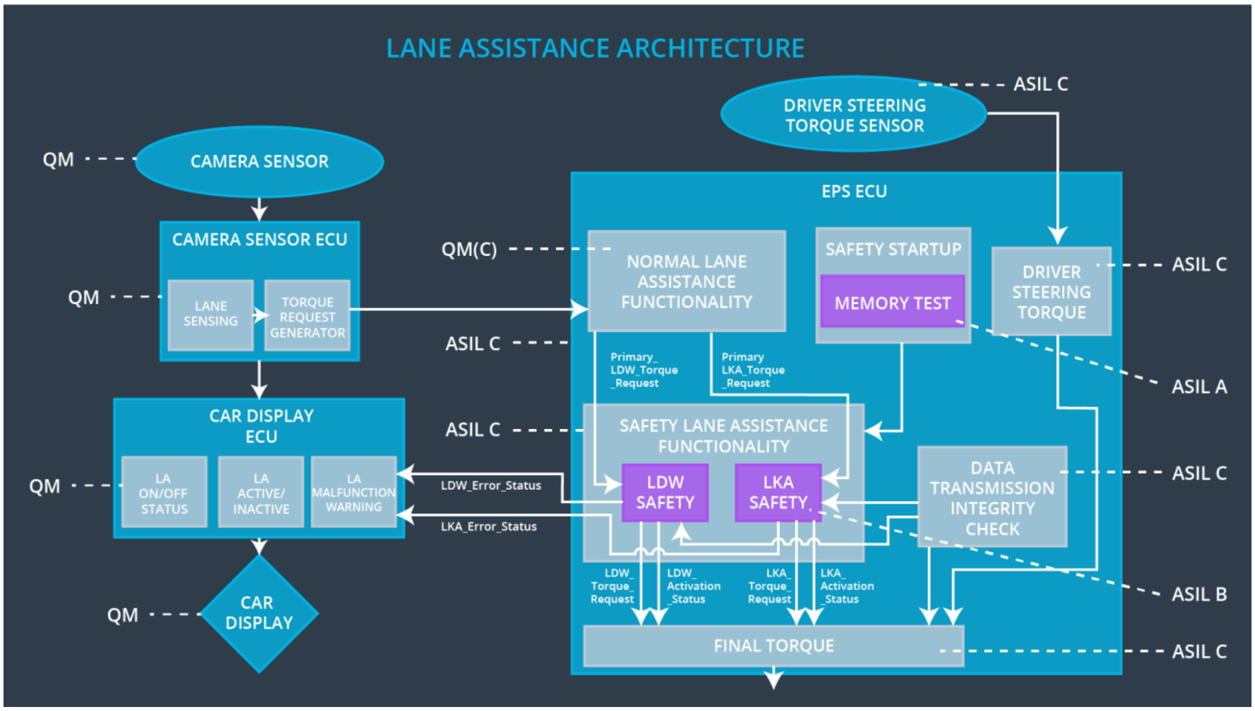
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Safety startup	Off

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]

For the entire lane assistance system being discussed in this document, all technical safety requirements are allocated to the Electronic Power Steering ECU

Warning and Degradation Concept

[Instructions: Fill in the warning and degradation concept. Same as functional safety concept in this case]

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Off	Torque frequency or amplitude exceeds its maximum threshold i.e., Max_Torque_Amplitude or Max_Torque_Frequency	Yes	LED on Car Display
WDC-02	Off	The LKA torque is being applied for more than max_duration	Yes	LED on Car Display