Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

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.

For example, if this were your first draft or first submission, you might say version 1.0. If this is a second submission attempt, then you'd add a second line with a new date and version 2.0]

Date	Version	Editor	Description
01/05/19	1.0	C.Wong	Initial Version

Table of Contents

[Instructions: We have provided a table of contents. If the table of contents is not showing up correctly in your word processor of choice, please update it. The table of contents should show each section of the document and page numbers or links. Most word processors can do this for you. In Google Docs, you can use headings for each section and then go to Insert > Table of Contents. Microsoft Word has similar capabilities]

Purpose of the Technical Safety Concept

[Instructions: Answer what is the purpose of a technical safety concept?]

The technical safety concept is derived from the functional safety concept. It is a meta-model element(s) describing the system design from a technical component view. While the functional safety concept defines safety measures, activities and high level solutions, the technical concept defines the safety mechanisms and associated technical safety requirements. Those requirements can be traced to item architecture.

Inputs to the Technical Safety Concept

Functional Safety Requirements

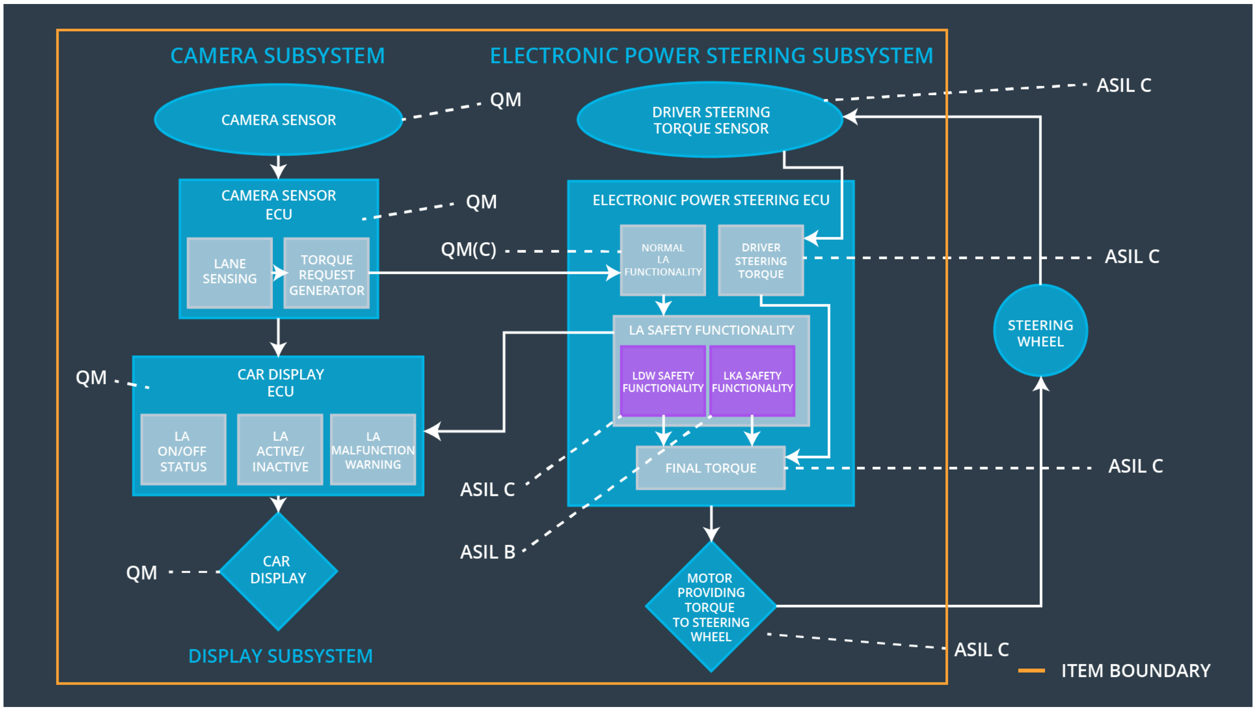
[Instructions: Provide the functional safety requirements derived in the functional safety concept]

ID	**Functional Safety Requirement**	**ASIL**	**Fault Tolerant Time Interval**	**Safe State**
Functional Safety Requirement 01-01	(**LDW**) The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	Vibration/ oscillating torque amplitude is set to zero.
Functional Safety Requirement 01-02	(**LDW**) The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50 ms	Vibration/ oscillating torque frequency is set to zero
Functional Safety Requirement 02-01	(**LKA**) The electronic power steering ECU shall ensure that the LKA torque is applied for only Max_Duration	C	500 ms	LKA torque is set to zero.
Functional Safety Requirement 02-02	(**LKA**) The electronic power steering ECU shall ensure that the LKA torque is always zero while the vehicle is in reverse (moving	B	500 ms	Function deactivated.

	backwards)			

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 image and converts to pixel data sent to Camera Sensor ECU
Camera Sensor ECU - Lane Sensing	Processes images from camera sensor to identify lanes in image. Passes lane locations to Torque request generator.
Camera Sensor ECU - Torque request generator	Uses lane information from the lane sensing subsystem and deteremines the torque request

	values to create haptic feedback torque and steering torque to steer the vehicle back to ego center. The torque values are sent to the power steering subsystem.
Car Display	Displays a warning or status when it receives car display ECU data.
Car Display ECU - Lane Assistance On/ Off Status	Uses the LKA and LDW error status from the EPS ECU and sends to the car display the active or inactive status of the Lane Asisstance Function.
Car Display ECU - Lane Assistant Active/Inactive	Uses the LKA and LDW error status from the EPS ECU and sends to the car display the active or inactive status of the Lane Asisstance Function.
Car Display ECU - Lane Assistance malfunction warning	Sends a malfunction warning to the car display ECU based on the values of the LDW and LKA statuses
Driver Steering Torque Sensor	Measures the torque applied by the driver and sends to the driver sterring torque subsystem
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Uses data from the driver steering torque sensor and sends the current torque to EPS ECU - Final Torque
EPS ECU - Normal Lane Assistance Functionality	Receives the input from Camera Sensor ECU - Torque request generator and calculates a LDW torque request, e.g. vibration torque request, for haptic feedback.
EPS ECU - Lane Departure Warning Safety Functionality	Receives a vibration torque request from the Normal Lane Assistance Functionality and check if the requested amplitude and frequency are under limits. If it cannot check the limits or the values are beyond range, a malfunction is generated and sent to the Car Display ECU.
EPS ECU - Lane Keeping Assistant Safety Functionality	Receives the current steering torque request from the Normal Lane Assistance Functionality and determines if the request has a duration no longer than max_duration. If it cannot determine duration, a malfunction message is sent to the Car display ECU
EPS ECU - Final Torque	Receives torque requests from Driver Steering Torque, Normal Lane Assistance Functionality , Lane Departure Warning Safety Functionality, Lane Keeping Assistant Safety Functionality and generates the final torque for the motor. Send the

	torque command to the motor.
Motor	Receives commands from the Electronic Power Steering ECU and applies torque to the steering wheel.

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	(**LDW**) The electronic power steering ECU 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 Requirem ent	The LDW safety component shall ensure that the amplitude of the 'LDW_Torque_Request'	C	50ms	LDW Safety Functionality	Lane Departure

01	sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Amplitude.				
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	50ms	LDW Safety Functionality	LDW Torque is 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 Functionality	LDW Torque is zero
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50ms	Data Transmission Integrity Check	LDW Torque is 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	At ignition cycle time	Safety Startup	LDW Torque is zero

[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 electronic power steering ECU 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 Functionality	
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	50ms	LDW Safety Functionality	
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 Functionality	
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50ms	Data Transmission integrity check	
Technical Safety Requirement	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	At Ignition cycle	Safety startup	

05			time		

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:

[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 electronic power steering ECU shall ensure that the LKA torque is applied for only for Max_Duration	X		

Technical Safety Requirements related to Functional Safety Requirement 02-01 are:

ID	Technical Safety Requirement	ASI	Fault Tolerant Time	Allocation to Architecture	Safe State

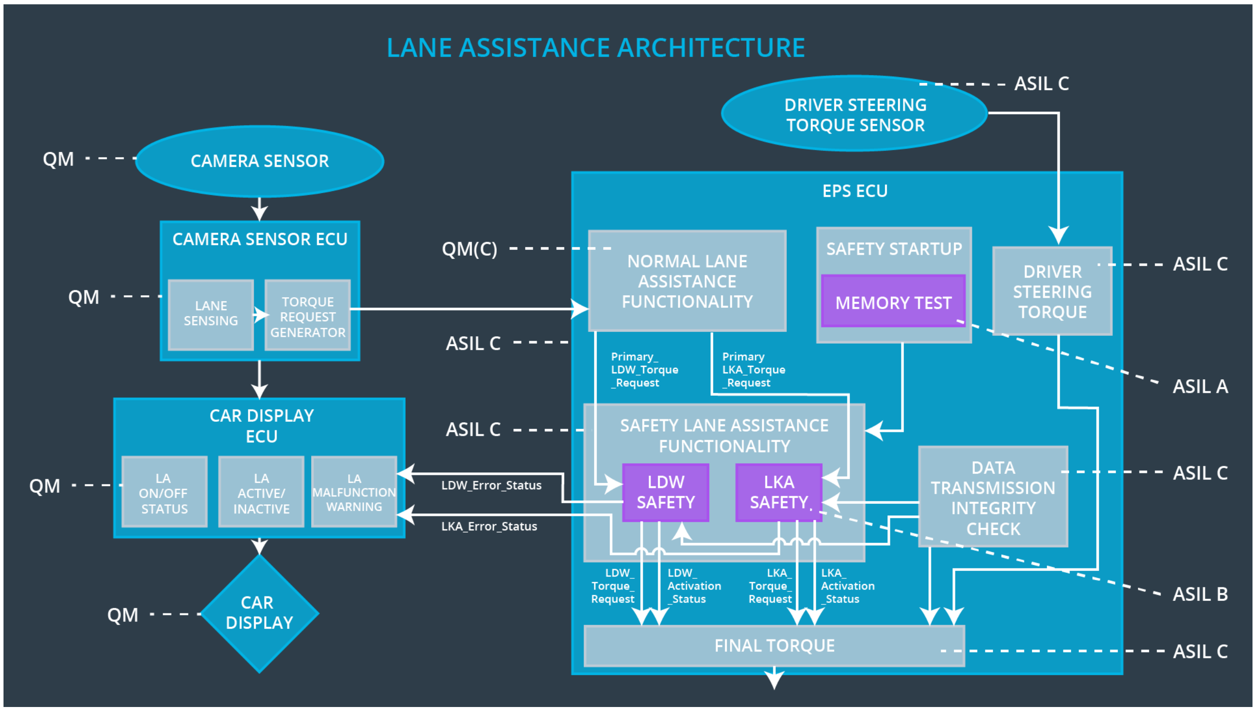
		L	Interval		
Technical Safety Requirement 01	The LKA safety component shall ensure that the frequency of the 'LKA_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Duration'.	B	500ms	LKA Safety Functionality	Off
Technical Safety Requirement 02	As soon as the 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	500ms	LKA Safety Functionality	Off
Technical Safety Requirement 03	As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and the 'LKA_Torque_Request' shall be set to zero.	B	500ms	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	500ms	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	At Ignition cycle time	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]

Lane Assistance system has all the requirements allocated to LDW and LKA Safety Functionality, and is allocated to the Electronic Power Steering ECU at the highest level.

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	Off	If LDW Torque oscillation amplitude exceeds Max_Torque_Amplitude OR Torque oscillation frequency exceeds Max_Torque_Frequency	Yes	Warning light on the Car Display
WDC-02	Off	If LKA torque applied for the duration longer than the Max_Duration	Yes	Warning light on the Car Display
WDC-03	Off	If vehicle transmission set to reverse, then Reverse_Mode_Torque is TRUE	Yes	Warning light on the Car Display