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
2018-12-01	1.0	Flash Yuan	Draft for the Technical Safety Concept for the Lane Assistance

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?]

Inputs to the Technical Safety Concept

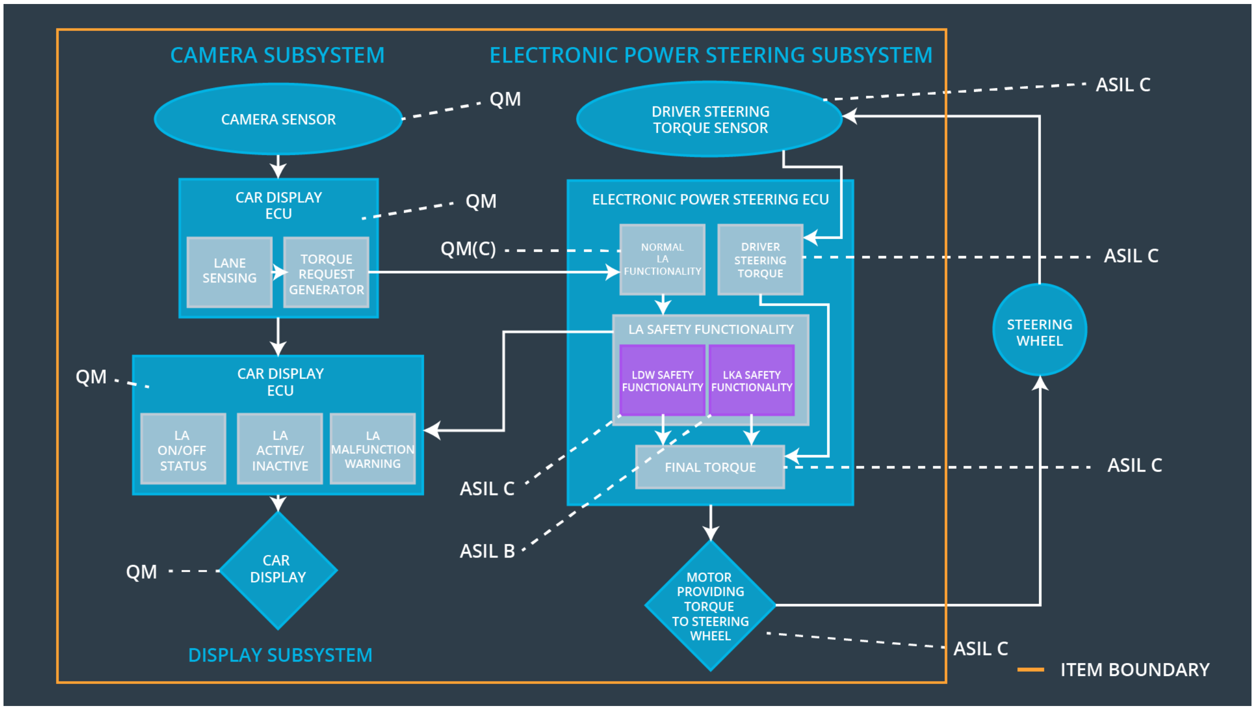
Functional Safety Requirements

[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 electronic power steering ECU shall ensure that the LDW torque oscillation amplitude is below Max_Torque_Amplitude	C	50ms	Off
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the LDW torque oscillation frequency is below Max_Torque_Frequency	C	50ms	Off
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the LKA torque is applied for only Max_Duration	B	500ms	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	The camera sensor reads the images on the road
Camera Sensor ECU - Lane Sensing	Process image for sensing the lane and passes information to the Torque Request Generator
Camera Sensor ECU - Torque request generator	Gets the data from Lane Sensing ECU and apply the torque to the Electronic power steering ECU to create haptic feedback or bring back the car in the center of lane,
Car Display	Takes the input from car display ECU and displays the warning on its display.
Car Display ECU - Lane Assistance On/Off Status	Shows light on and off depending on the information received from the Camera Sensor ECU.
Car Display ECU - Lane Assistant Active/Inactive	Shows light active and inactive depending on the information received from the Camera Sensor ECU.

Car Display ECU - Lane Assistance malfunction warning	Shows warning sign based on warning signal from LDW or LKA malfunction.
Driver Steering Torque Sensor	Measures the torque applied by the driver.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Receives input from Driver Steering Torque sensor and sends required torque to ECU Final torque.
EPS ECU - Normal Lane Assistance Functionality	Receives the input from Camera Sensor ECU – Torque Request Generator and calculates the vibrational torque request.
EPS ECU - Lane Departure Warning Safety Functionality	Receives vibrational torque request from the ‘Normal Lane Assistance’ and checks if the amplitude and frequency are under the limit. If there is malfunction it informs the ‘Car Display ECU’.
EPS ECU - Lane Keeping Assistant Safety Functionality	Receives torque request from the ‘Normal Lane Assistance’ Functionality and checks if torque steering assistance duration is no longer Max_Duration. If there is malfunction it informs the ‘Car Display ECU’.
EPS ECU - Final Torque	Receives request from the safety functionalities above and sends the final required torque value to the motor.
Motor	Takes the input from EPS ECU and applies the 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	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(input)	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	Off
Technical Safety Requirement 02(display)	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	Off
Technical Safety Requirement 03(output)	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	Off
Technical Safety Requirement 04(transmit)	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50ms	Data Transmission integrity check	Off

Technical Safety Requirement 05(menmory management)	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition cycle time	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	C	50ms	LDW Safety Functionality	Off

	'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	Off
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	Off
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	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 time	Safety startup	Off

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 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	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 Requireme	The validity and integrity of the data transmission for	B	500ms	Data Transmission Integrity check	Off

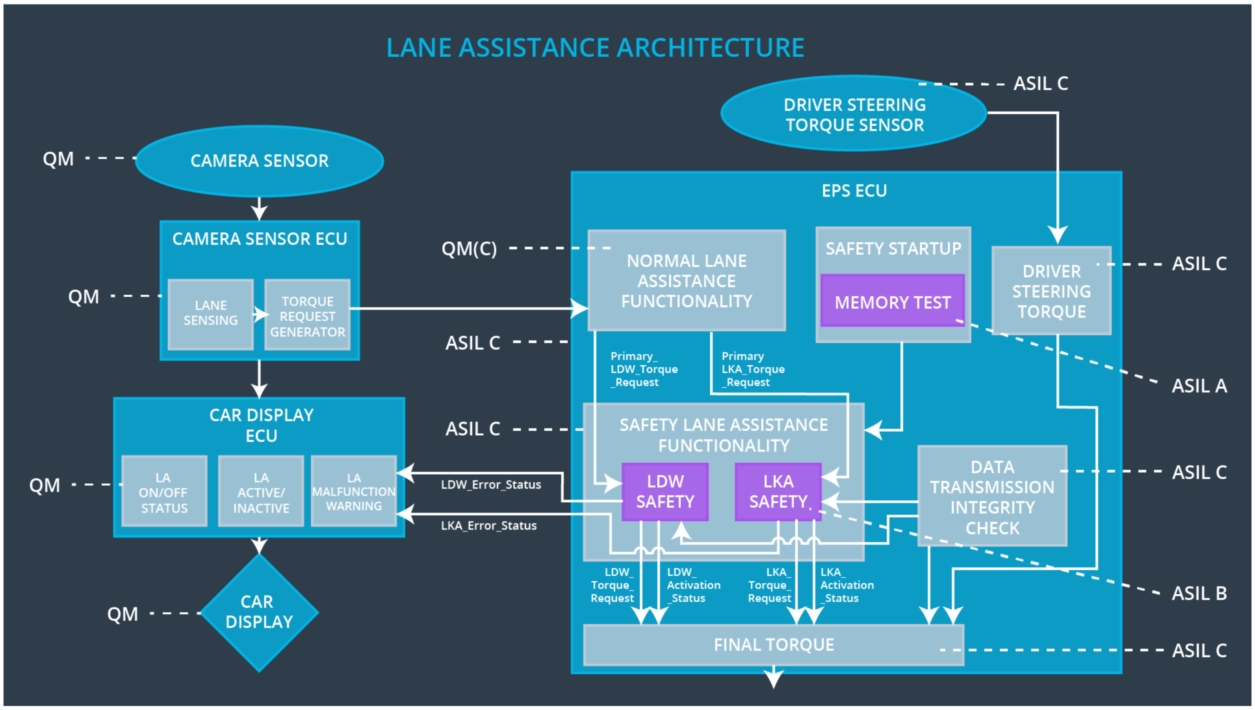
nt 04	'LDW_Torque_Request' signal shall be ensured.				
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition cycle time	Safety startup	Off

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]
For Lane Assistance system, all the requirements are allocated to LDW and LKA Safety Functionality, which overall is 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	Off	Torque amplitude exceeds Max_Torque_Amplitude OR Torque frequency exceeds Max_Torque_Frequency	Yes	Warning light on the car display
WDC-02	Off	LKA torque applied exceeds the duration greater than Max_Duration	Yes	Warning light on the car display