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
01/23/2019	1.0	Rouzbeh Shirvani	First attempt
01/27/2019	1.1	Rouzbeh Shirvani	Second attempt

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 defines how the sub-systems interact at the system level and describes how the ECUs communicate with each other.

Inputs to the Technical Safety Concept

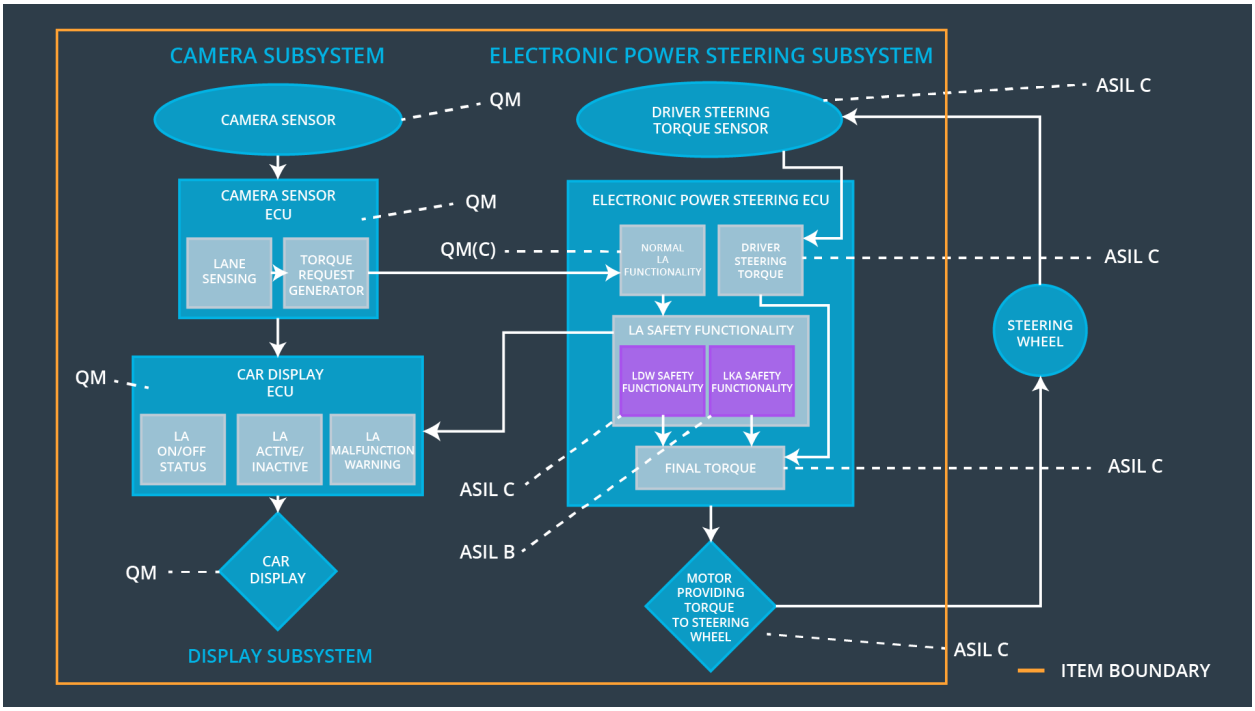
Functional Safety Requirements

[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 oscillating torque aplitude requested by the LDW function is below max_torque_amplitude	C	50 ms	LDW will set the oscillating torque amplitude to 0
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	B	50ms	LDW will set the oscillating frequency to 0
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	Safe state would be a state that the driver takes control of the wheel and does not rely on the system. Deactivating the system so that the driver takes control.

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 system reads images from the road
Camera Sensor ECU - Lane Sensing	The camera system ECU identifies when the vehicle accidentally departds its lane and sends the approprate messages to the car display ECU and the electronic power steering ECU
Camera Sensor ECU - Torque request	The camera system ECU checks whether

generator	appropriate torque request has been generated in order to steer the vehcile in the right direction
Car Display	Car Displays system visualizes information and provides feedback for driver about the Lane Assistance system among other display functionality
Car Display ECU - Lane Assistance On/Off Status	Car Display ECU checks whether the lane assitance system is on or off so that it can generate the right signal in order to show to the driver.
Car Display ECU - Lane Assistant Active/Inactive	Car Display ECU makes sure whether the driver is in charge or the lane assitance is active currently.
Car Display ECU - Lane Assistance malfunction warning	In case of malfunctioning Car Display ECU provides appropriate feedback for the driver in order to be aware of the situation.
Driver Steering Torque Sensor	Driver Steering Torque Sensor senses how much torque is applied to the steering wheel and sends it to the power steering ECU
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Electronic power Steering ECU senses the steering torque generated by the driver for further processes. For example making sure that the driver is providing right amount of steering power.
EPS ECU - Normal Lane Assistance Functionality	EPS ECU makes sure that the Lane Assistance system is working under normal situation and sends appropriate signal to the driver
EPS ECU - Lane Departure Warning Safety Functionality	EPS ECU makes sure that the Lane Departure torque amplitude and frequency are in the safe range and potentially set to zero in case of missuse
EPS ECU - Lane Keeping Assistant Safety Functionality	EPS ECU makes sure that lane keeping assitance has a time limit
EPS ECU - Final Torque	EPS ECU makes sure that enough torque is applied in order to keep the vehicle on the path
Motor	The motor provides required force in order to move the steering wheel in the appropriate direction.

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	C	50 ms	LDW Safety block	LDW will set the oscillating torque amplitude to 0

	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	50 ms	LDW safety block	LDW will set the oscillating torque amplitude to 0
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	50 ms	LDW safety block	LDW will set the oscillating torque amplitude to 0
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	N/A
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	Driver should be warned to stop the engine.

[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_Frequency_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_ Frequency _Amplitude.	B	50 ms	LDW Safety block	LDW will set the oscillating torque amplitude to 0
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.	B	50 ms	LDW safety block	LDW will set the oscillating torque amplitude to 0
Technical Safety Requirement 03	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the 'LDW_ Frequency _Request' shall be set to zero.	B	50 ms	LDW safety block	LDW will set the oscillating torque amplitud

					e to 0
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_ Frequency _Request' signal shall be ensured.	B	50 ms	Data Transmission integrity check	N/A
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	Driver should be warned to stop the engine.

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	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 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_Duration	C	50 ms	LDW Safety block	LDW will set the duration to 0
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	50 ms	LDW safety block	LDW will set the duration to 0
Technical Safety Requirement 03	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the Max_Duration shall be set to zero.	C	50 ms	LDW safety block	LDW will set the duration to 0
Technical Safety Requirement 04	The validity and integrity of the data transmission for Max_Duration signal shall be ensured.	C	50 ms	Data Transmission integrity check	N/A
Technical	Memory test shall be	A	ignition	Safety Startup	Driver

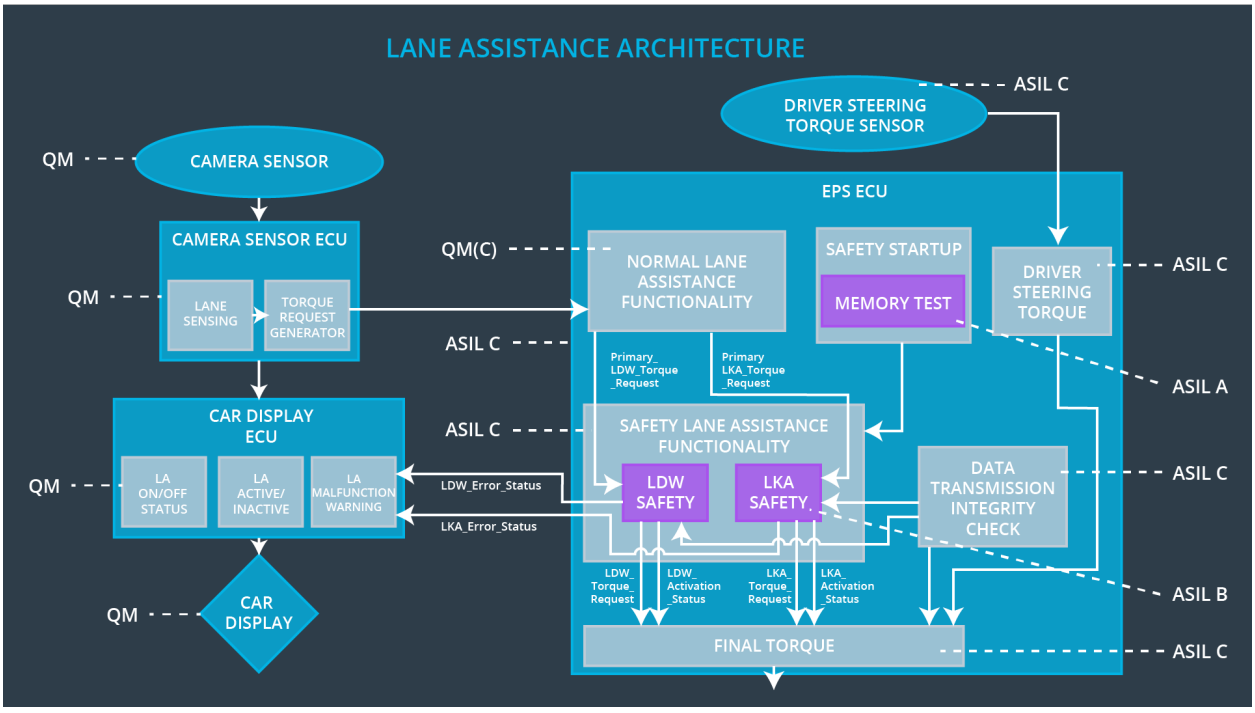
Safety Requirement 05	conducted at start up of the EPS ECU to check for any faults in memory.		cycle		should be warned to stop the engine.

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.]