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
2017/12/31	1.0	MIURA Yasuyuki	First 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 subsystems interact at the message level and describes how the ECUs communicate with each other.

Inputs to the Technical Safety Concept

Functional Safety Requirements

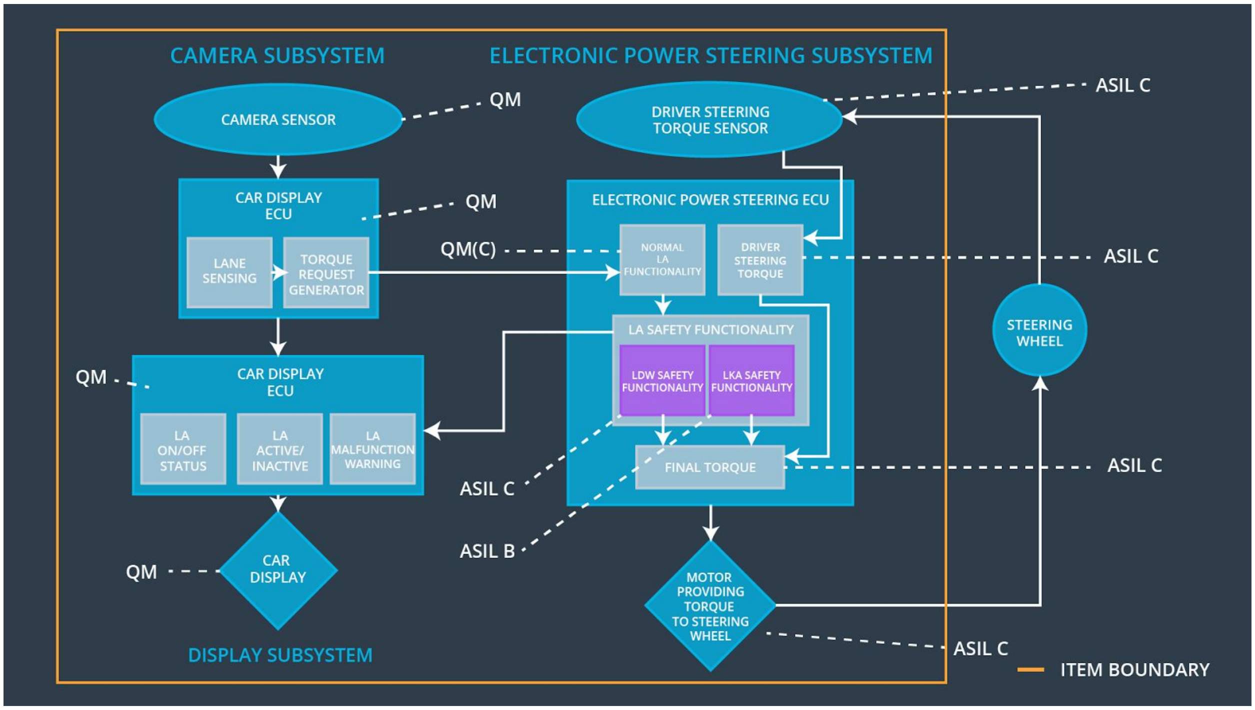
[Instructions: Provide the functional safety requirements derived in the functional safety concept]

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 amplitude requested by the LDW function is below Max_Torque_Amplitude.	C	50 ms	LDW will set the ocsillating torque amplitude to 0.
Functional Safety Requirement	The Electronic Power Steering ECU shall ensure that the oscillating torque frequency requested by the LDW function is below	C	50 ms	LDW will set the ocsillating torque frequency to 0.

01-02	Max_Torque_Frequency.			
Functional Safety Requiremen t 02-01	The Electronic Power Steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration.	B	500 ms	LKA will set the ocsillating torque duration to 0.

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 in images from the road.
Camera Sensor ECU - Lane Sensing	The Camera Sensor ECU - Lane Sensing identifies when the vehicle has accidentally departed its lane, and sends the appropriate messages to the Car Display ECU.
Camera Sensor ECU - Torque request generator	Camera Sensor ECU - Torque request generator sends the appropriate messages to the Electronic Power Steering ECU.
Car Display	The Car Display controls a light that tells the driver if the lane keeping item is on or off, and will control a light telling the driver that the lane departure warning is activated.
Car Display ECU - Lane Assistance On/Off Status	Car Display ECU - Lane Assistance On/Off Status receives the message and display Lane Assistance On/Off Status on the display.
Car Display ECU - Lane Assistant Active/Inactive	Car Display ECU - Lane Assistant Active/Inactive receives the message and display Lane Assistant Active/Inactive on the display.
Car Display ECU - Lane Assistance malfunction warning	Car Display ECU - Lane Assistance malfunction warning receives the message and display Lane Assistance malfunction warning on the display.
Driver Steering Torque Sensor	The Driver Steering Torque Sensor will sense how much the driver is turning the steering wheel.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	The EPS ECU - Driver Steering Torque will receive the vibrational torque from the Driver Steering Torque Sensor, and will send the vibrational torque to The EPS ECU - Final Torque.
EPS ECU - Normal Lane Assistance Functionality	The Electronic Power Steering ECU will receive the vibrational torque request from the Camera ECU, and will send the vibrational

	torque request to EPS ECU - Lane Departure Warning Safety Functionality and EPS ECU - Lane Keeping Assistant Safety Functionality.
EPS ECU - Lane Departure Warning Safety Functionality	The EPS ECU - Lane Departure Warning Safety Functionality will receive the vibrational torque from the Driver Steering Torque Sensor and the vibrational torque from the The EPS ECU - Driver Steering Torque, and will determine whether or not a Lane Departure Warning is necessary. Then, It send the judgment result to the EPS ECU - Final Torque and Car Display ECU.
EPS ECU - Lane Keeping Assistant Safety Functionality	The EPS ECU - Lane Keeping Assistant Safety Functionality will receive the vibrational torque from the Driver Steering Torque Sensor and the vibrational torque from the The EPS ECU - Driver Steering Torque, and will determine whether or not a Lane Keeping Assistant is necessary. Then, It send the judgment result to the EPS ECU - Final Torque and Car Display ECU.
EPS ECU - Final Torque	The EPS ECU - Final Torque will add these torque requests together to output a final torque to the Motor.
Motor	The Motor moves 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 Electronic Power Steering ECU shall ensure that the oscillating torque amplitude requested by the LDW function 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	LDW Torque Request Amplitude shall be set to the 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	C	50 ms	LDW Safety Functionality	LDW Torque Request Amplitude shall be set to the 0.

	on a warning light.				
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	Lane Assistance Malfunction Warning / LDW Safety Functionality	LDW Torque Request Amplitude shall be set to the 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 Trans-mission Integrity Check	LDW Torque Request Amplitude shall be set to the 0.
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	Memory Test	LDW Torque Request Amplitude shall be set to the 0.

[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 Requiremen	The Electronic Power Steering ECU shall ensure that the oscillating torque frequency	X		

t 01-02	requested by the LDW function is below Max_Torque_Frequency.			

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	50 ms	LDW Safety	LDW Torque Request Frequency shall be set to the 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 Functionality	LDW Torque Request Frequency shall be set to the 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	Lane Assistance Malfunction Warning / LDW Safety Functionality	LDW Torque Request Frequency shall be set to

					the 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 Trans-mission Integrity Check	LDW Torque Request Frequency shall be set to the 0.
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	Memory Test	LDW Torque Request Frequency shall be set to the 0.

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 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 frequency of the 'LKA_Torque_Request' sent to the 'Final electronic power steering Torque' component is below ‘Max_Duration’.	B	500 ms	LKA Safety	LKA will set the ocsillating torque duration to 0.
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	LKA will set the ocsillating torque duration to 0.
Technical Safety	As soon as a failure is detected by the LKA function, it	B	500 ms	Lane Assistance	LKA will set the

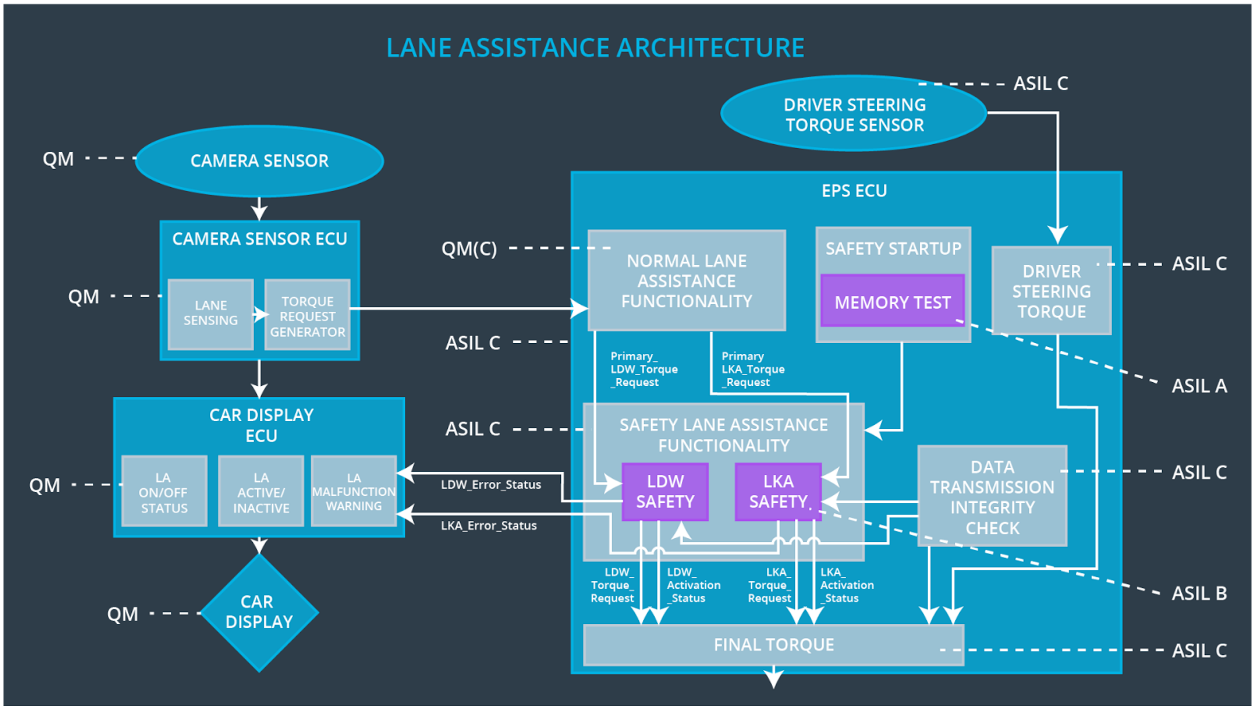
Requirement 03	shall deactivate the LKA feature and the 'LKA_Torque_Request' shall be set to zero.			Malfunction Warning / LKA Safety Functionality	ocsillating torque duration to 0.
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	B	500 ms	Data Trans-mission Integrity Check	LKA will set the ocsillating torque duration to 0.
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	Memory Test	LKA will set the ocsillating torque duration to 0.

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]

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 01-01	The Electronic Power Steering ECU shall ensure that the oscillating torque amplitude requested by the LDW function is below Max_Torque_Amplitude.	X		X
Functional Safety	The Electronic Power Steering ECU shall ensure that the	X		X

Requirement 01-02	oscillating torque frequency requested by the LDW function is below Max_Torque_Frequency.			
Functional Safety Requirement 02-01	The Electronic Power Steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration.	X		

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	we will display a warning on the driver dashboard.	when the steering wheel ECU receives a vibrational torque request beyond the allowed maximum	Yes	Beyond the lane.
WDC-02	we will display	when the	Yes	Driver please

	a warning on the driver dashboard.	steering wheel ECU receives a vibrational torque request beyond the allowed maximum		drive.