Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: [V1.1]

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
24-01-2019	V1.1	Liping S	First version with all required content

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?]

ISO 26262 places the technical safety concept as part of the product development phase. Before developing hardware or software, the technical safety requirements need to be determined for each of these systems.
The technical safety concept involves:

- Turning functional safety requirements into technical safety requirements
- Allocating technical safety requirements to the system architecture

This will set us up for drilling down into software and hardware implementation in the next step.

Inputs to the Technical Safety Concept

Functional Safety Requirements

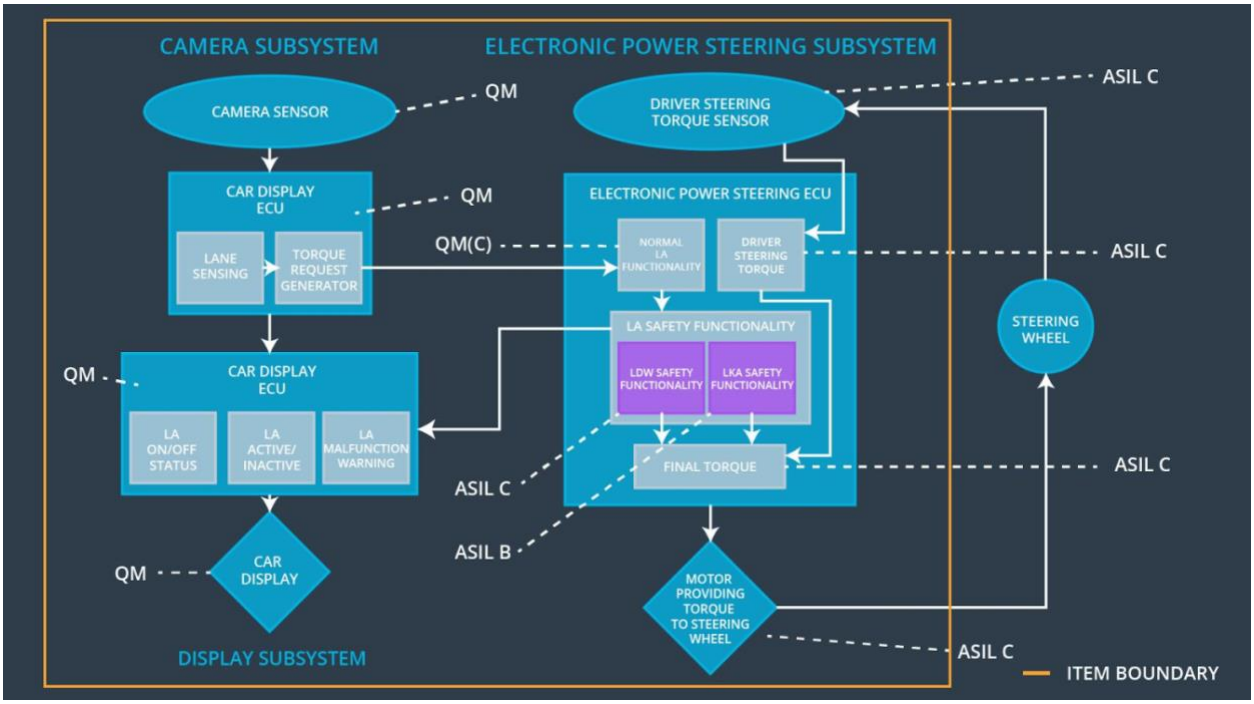
[Instructions: Provide the functional safety requirements derived in the functional safety concept]

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50ms	Function is deactivated
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50ms	Function is deactivated

Functional Safety Requirement 02-01	The steering ECU shall ensure that the wheel steering torque only be applied in the Max_Duration	B	500ms	Lane Keeping Assistance torque is zero.

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	Provide visual signal to camera sensor ECU
Camera Sensor ECU - Lane Sensing	Detect lane line

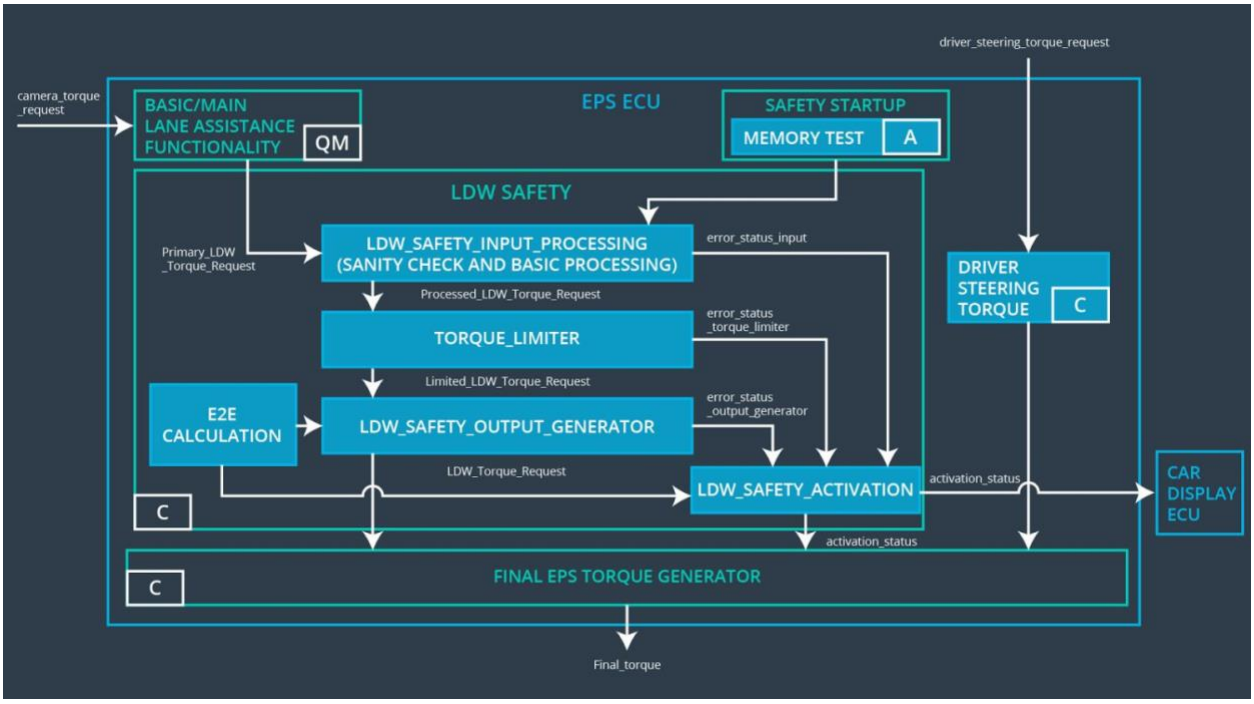
Camera Sensor ECU - Torque request generator	Calculate the torque to be requested to the Electronic Power Steering ECU.
Car Display	Provide user interface to the driver and show the info of the system
Car Display ECU - Lane Assistance On/Off Status	Indicate the status of the Lane Assistance functionality (On/Off.)
Car Display ECU - Lane Assistant Active/Inactive	Indicate if the Lane Assistance functionality is properly functioning (Active/Inactive.)
Car Display ECU - Lane Assistance malfunction warning	Indicate a malfunction on the Lane Assistance functionality
Driver Steering Torque Sensor	Measure the torque applied to the steering wheel
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Receive driver torque request from the steering wheel
EPS ECU - Normal Lane Assistance Functionality	Receive Camera ECU torques request
EPS ECU - Lane Departure Warning Safety Functionality	Ensure the torque is below Max_Torque_Amplitude and Max_Torque_Frequency.
EPS ECU - Lane Keeping Assistant Safety Functionality	Ensure the Lane Keeping Assistance functionality is not activated more than Max_duration
EPS ECU - Final Torque	Receive and process torque request from the Lane Keeping and Lane Departure Warning and send the final torque decision to the Motor
Motor	Apply the required 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	The LDW safety component shall ensure that amplitude of 'LDW_Torque_Request' sent to the 'Final electronic power steering torque' is below 'Max_Torque_Amplitude'	C	50ms	LDW Safety	LDW activation status to zero
Technical Safety Requirement 02	The LDW safety component shall send warning signal to Car Display ECU for display when LDW is deactivated.	C	50ms	LDW Safety	LDW activation status to zero
Technical Safety Requirement 03	When a failure is detected by the LDW, it shall deactivate the LDW and set 'LDW_Torque_Request' to zero.	C	50ms	LDW Safety	LDW activation status to zero
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' shall be ensured	C	50ms	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 memory problems	A	Ignition cycle	Memory Test	LDW activation status to 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 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 frequency of 'LDW_Torque_Request' sent to the 'Final electronic power steering torque' is below 'Max_Torque_Frequency	C	50ms	LDW Safety	LDW activation status to zero
Technical Safety Requirement 02	The LDW safety component shall send warning signal to Car Display ECU for display when LDW is deactivated.	C	50ms	LDW Safety	LDW activation status to zero
Technical Safety Requirement 03	When a failure is detected by the LDW, it shall deactivate the LDW and set 'LDW_Torque_Request' to zero.	C	50ms	LDW Safety	LDW activation status to zero
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' shall be ensured	C	50ms	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 memory problems	A	Ignition cycle	Memory Test	LDW activation status to zero

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:

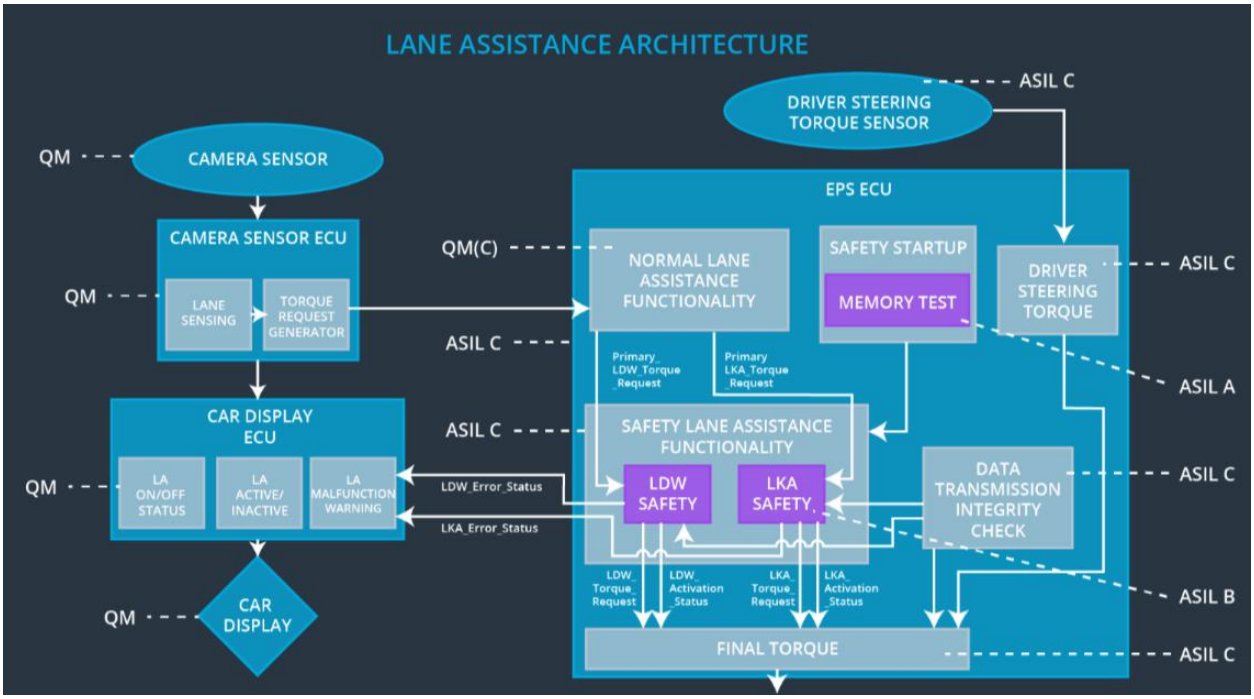
ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01	The LKA safety component shall ensure that 'LKA_Torque_Request' is sent to 'Final electronic power steering torque' in limited period of time(Max_Duration)	B	500ms	LKA Safety	LKA activation status to zero
Technical Safety Requirement 02	The LKA safety component shall send warning signal to Car Display ECU for display when LKA is deactivated.	B	500ms	LKA Safety	LKA activation status to zero
Technical Safety Requirement 03	When a failure is detected by the LKA, it shall deactivate the LKA and set 'LKA_Torque_Request' to zero.	B	500ms	LKA Safety	LKA activation status to zero
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' shall be ensured	B	500ms	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 memory problems	A	Ignition cycle	Memory test	LKA activation status to zero

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 item, all technical safety requirements were 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	Turn off Lane Assistant functionality	Malfunction_01	Yes	Lane assistance malfunction warning on car display
WDC-02	Turn off Lane Assistant functionality	Malfunction_02	Yes	Lane assistance malfunction warning on car display
WDC-03	Turn off Lane Assistant functionality	Malfunction_03	Yes	Lane assistance malfunction warning on car display