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
28/Oct/2017	v1.0	Atif Hussain	Initial draft on Safety
8/Nov/2017	v2.0	Atif Hussain	Review Comments applied
25/Nov/2017	V3.0	Atif Hussain	Updated LKA technical requirements

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]

Table of Contents

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 how the ECUs communicate with each other.

Inputs to the Technical Safety Concept

Functional Safety Requirements

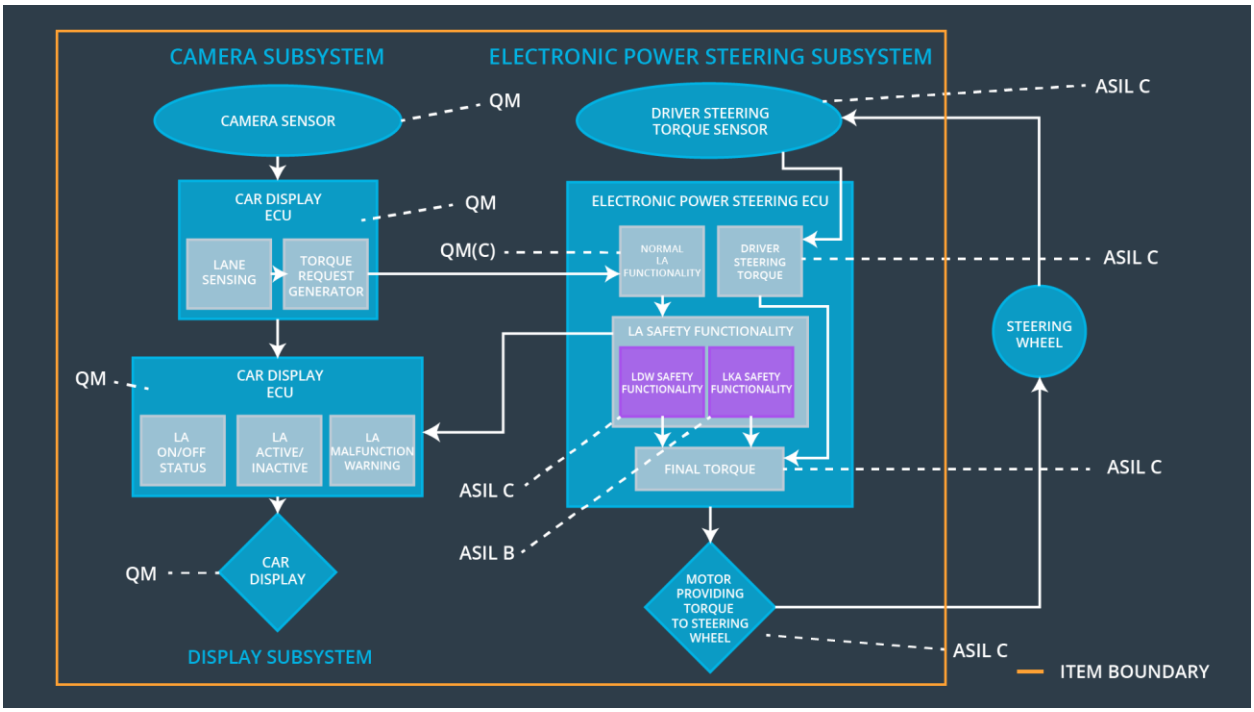
[Instructions: Provide the functional safety requirements derived in the functional safety concept]

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	The EPS ECU shall ensure that the lane departure warning torque amplitude is below Max_Torque_Amplitude	C	50 ms	LDW will set the oscillating torque amplitude and frequency to 0.
Functional Safety Requirement 01-02	The EPS ECU shall ensure that the lane departure warning torque frequency is below Max_Torque_Frequency	C	50 ms	LDW will set the oscillating torque amplitude and 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	500 ms	LKA torque output is set to 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	Captures lane marking images
Camera Sensor ECU - Lane Sensing	Localizes car within lane boundaries, and detects lane departure

Camera Sensor ECU - Torque request generator	Generates torque to be applied to fix lane departure
Car Display	ADAS Display within the car
Car Display ECU - Lane Assistance On/Off Status	Display whether Lane Assistance is manually set to On/Off status
Car Display ECU - Lane Assistant Active/Inactive	Display whether Lane Assistance has turned inactive due to any of the fault triggers
Car Display ECU - Lane Assistance malfunction warning	Display whether Lane Assistance function generated a malfunction warning
Driver Steering Torque Sensor	Sensor to detect the amount of torque applied by the driver
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Processes the amount of torque applied by the driver
EPS ECU - Normal Lane Assistance Functionality	Computes the additional torque to apply to the steering wheel to keep the vehicle in lane; and Detects the event of lane departure of the car, to provide haptic feedback to the driver
EPS ECU - Lane Departure Warning Safety Functionality	If LDW_torque requested is > max (either amplitude or frequency), then set to 0 (disable)
EPS ECU - Lane Keeping Assistant Safety Functionality	If LKA_torque is requested for > max duration, disable LKA function, to prevent autonomous driving
EPS ECU - Final Torque	Compute the final torque to apply to car steering wheel, based on current torque, and additional delta being requested.
Motor	Applies the extra 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.]

1. LDW Amplitude Malfunction (in Lane Departure Warning) – 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 Steering Torque component is below 'Max_Torque_Amplitude'	C	50 ms	LDW Safety	LDW torque output is set to zero
Technical Safety Requirement 02	The validity and integrity of the data transmission for LDW_Torque_Request signal shall be ensured	C	50 ms	Data Transmission Integrity Check	LDW torque output is set to zero
Technical Safety Requirement	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and	C	50 ms	LDW Safety	LDW torque output is set to zero

03	the LDW_Torque_Request shall be set to zero				
Technical Safety Requirement 04	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	LDW torque output is set to 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	Ignition Cycle	Safety startup –Memory test	LDW torque output is set 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]

2. LDW Frequency Malfunction (in Lane Departure Warning) – Requirement – 2

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 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 output is set to zero
Technical Safety Requirement 02	The validity and integrity of the data transmission for LDW_Torque_Request signal shall be ensured	C	50 ms	Data Transmission Integrity Check	LDW torque output is set to 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	C	50 ms	LDW Safety	LDW torque output is set to

	to zero				zero
Technical Safety Requirement 04	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	LDW torque output is set to 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	Ignition Cycle	Safety setup – memory test	LDW torque output is set 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.]

3. LKA Time Malfunction (in Lane Keeping Assistance) – 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 duration of the 'LKA_Torque_Request' sent to the 'Final Electronic Power Steering Torque' component is no more than Max_LKA_Duration	B	500 ms	LKA Safety block	LKA torque output is set to zero
Technical Safety Requirement 02	The validity and integrity of the data transmission for LKA_Torque_Request signal shall be ensured	B	500 ms	Data Transmission Integrity Check	LKA torque output is set to zero
Technical Safety	As soon as a failure is detected by the LKA function, it shall	B	500 ms	LKA Safety block	LKA torque output is set

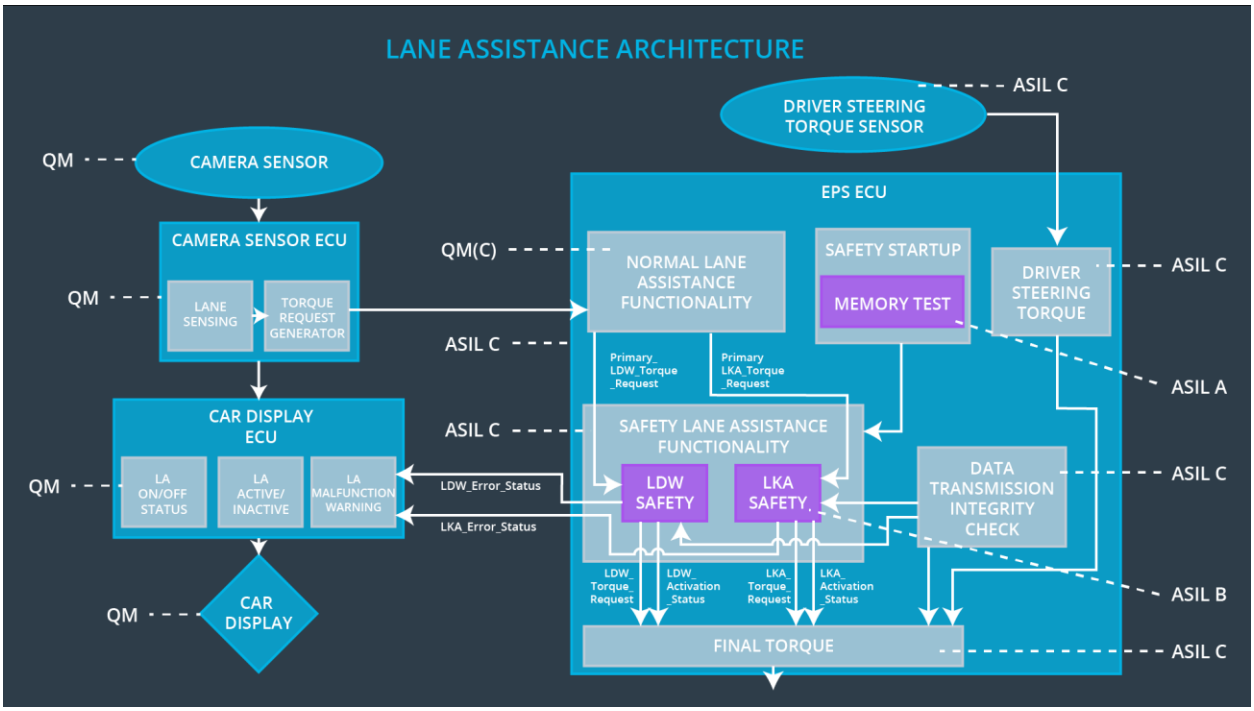
Requirement 03	deactivate the LKA feature and the LKA_Torque_Request shall be set to zero				to zero
Technical Safety Requirement 04	Re-activate the LKA torque request when vehicle falls back into the lane (so LKA is working again)	B	500 ms	LKA Safety block	LKA torque output is set to zero
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory	A	Ignition Cycle	Safety setup – memory test	LKA torque output is set 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 this Lane Assistance 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.]

A lane departure warning system is not critical for driving a vehicle. So if the system has a malfunction, we can shut the system down; on the other hand, a functioning motor is necessary for driving a vehicle. Degrading the motor system to a safer, but functioning, state would help the driver avoid getting stranded.

What will trigger the degradation mode? The malfunctions that you have already learned about.

Is the safe state invoked? Yes.

The driver warning makes the driver warned about the malfunction.