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
22-5-2018	1.0	Atul Singh	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]

Document history

Table of Contents

Purpose of the Technical Safety Concept

Inputs to the Technical Safety Concept

- Functional Safety Requirements
- Refined System Architecture from Functional Safety Concept
  - Functional overview of architecture elements

Technical Safety Concept
- Technical Safety Requirements
- Refinement of the System Architecture
- Allocation of Technical Safety Requirements to Architecture Elements
- Warning and Degradation Concept

Purpose of the Technical Safety Concept

[Instructions: Answer what is the purpose of a technical safety concept?]
From the functional safety concept, we got a bird's eye view of the system. The purpose of the technical safety concept is to go into the technical details of these systems i.e to identify new requirements and allocate the hardware and software requirements to the system diagrams.

Inputs to the Technical Safety Concept

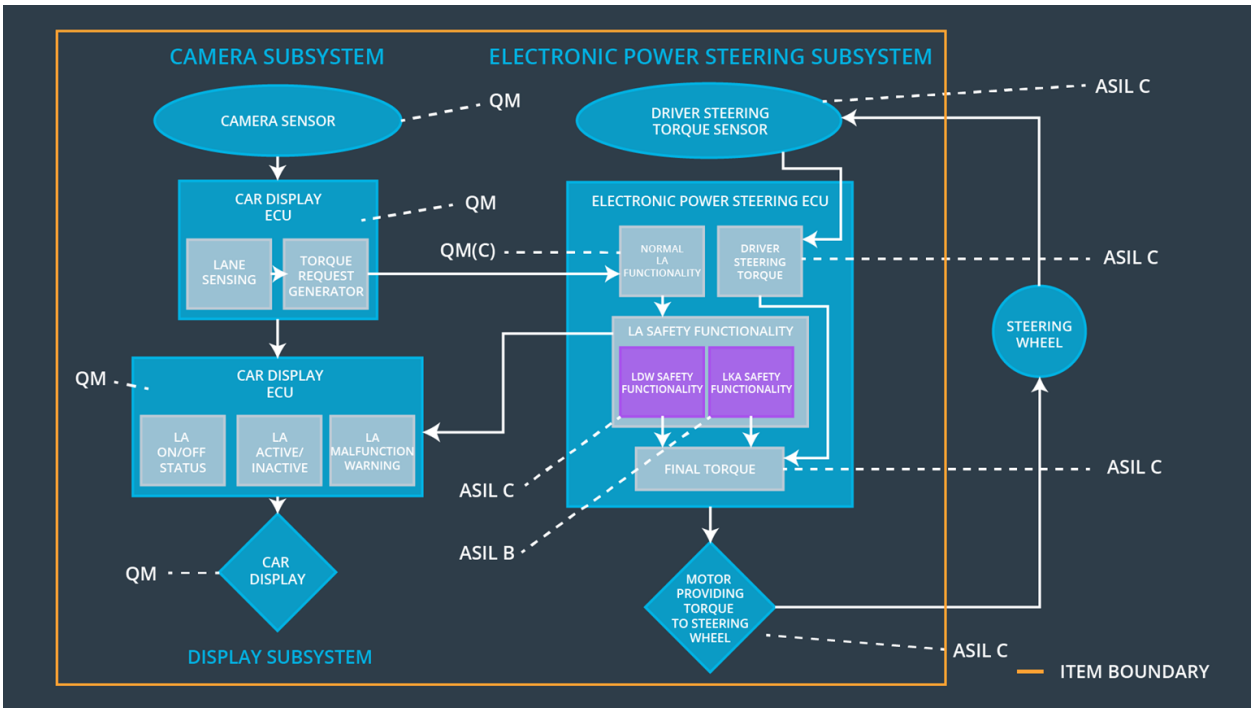
Functional Safety Requirements

[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 ECU should ensure that the lane departure oscillating torque amplitude is below the MAX_Torque_Amplitude	C	50 ms	Turn off the lane departure warning system
Functional Safety Requirement 01-02	The ECU should ensure that the lane departure oscillating torque frequency is below the MAX_Torque_Frequency	C	50 ms	Turn off the lane departure warning system
Functional Safety Requirement 02-01	The ECU should ensure that the lane departure oscillating torque duration should not exceed MAX_Duration	B	500 ms	Turn off the lane departure warning system

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	Provides lane images to the Camera Sensor ECU
Camera Sensor ECU - Lane Sensing	Checks whether the car is leaving the lane or is in the lane by going through the image provided by the camera sensor.
Camera Sensor ECU - Torque request generator	Its functionality is to send the required torque to the power steering ECU

Car Display	It is uses to display warnings to the driver
Car Display ECU - Lane Assistance On/Off Status	It receives the status of the LDW from the power steering ECU in form of signals and conveys the same to the car display system.
Car Display ECU - Lane Assistant Active/Inactive	It receives the status of the lane assistant function from the power steering ECU in form of signals and conveys the same to the car display system.
Car Display ECU - Lane Assistance malfunction warning	It receives the status of the lane assistant function from the power steering ECU in form of signals and if there is any malfunction in the signal it conveys the same to the car display system.
Driver Steering Torque Sensor	Measure the torque applied by the driver on the steering wheel by the driver.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	It receives and process the data from the camera sensor ECU and torque sensor
EPS ECU - Normal Lane Assistance Functionality	It receives the data from the driver steering torque sensor .
EPS ECU - Lane Departure Warning Safety Functionality	It ensure the LDW safety functionality
EPS ECU - Lane Keeping Assistant Safety Functionality	It receives the request from the camera subsystem and conveys it to the steering wheel through the motor.
EPS ECU - Final Torque	Calculates the final torque that is needed to be applied on the steering wheel by considering the torque applied by the driver and the torque requested by the camera subsystem.
Motor	Receives the torque from the ECU and applies it 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	LDW safety component should ensure the amplitude of `LDW_Torque_Requesr` is below 'Max_Torque_Amplitude'	C	50 ms	LDW safety	LDW torque request should be 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.	N/A
Technical Safety Requirement 03	If a failure is detected by the LDW function it shall deactivate the LDW feature and set the torque to zero	C	50 ms	LDW safety	LDW torque request should be zero
Technical Safety Requirem	As soon as the LDW feature is deactivated by the LDW function the car display ECU	C	50 ms	LDW safety	LDW torque request should be

ent 04	should show a warning light.				zero
Technical Safety Requirement 05	Memory test should be done at start of the EPS ECU to check for any faults in memory	A	ignition cycle	LDW safety	LDW torque request should be 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	LDW safety component should ensure the Frequency of `LDW_Torque_Request ` is below	C	50 ms	LDW safety	LDW torque frequency

	‘Max_Torque_Frequency				request should be zero
Technical Safety Requirement 02	The validity and integrity of the data transmission for Max_Torque_Frequency signal shall be ensured.	C	50 ms	Data Transmission integrity check.	N/A
Technical Safety Requirement 03	If a failure is detected by the LDW function it shall deactivate the LDW feature and set the ‘Max_Torque_Frequency to zero	C	50 ms	LDW safety	LDW torque frequency request should be zero
Technical Safety Requirement 04	As soon as the LDW feature is deactivated by the LDW function the car display ECU should show a warning light.	C	50 ms	LDW safety	LDW torque frequency request should be zero
Technical Safety Requirement 05	Memory test should be done at start of the EPS ECU to check for any faults in memory	A	ignition cycle	LDW safety	LDW torque frequency request should be 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	LKA safety component should ensure the amplitude of `LKA_Torque_Requesr` is below ‘Max_Torque_Amplitude’	B	500 ms	LKA safety	LKA torque request should be 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.	N/A
Technical Safety Requirement 03	If a failure is detected by the LKA function it shall deactivate the LKA feature and set the torque to zero	B	500 ms	LKA safety	LKA torque request should be zero

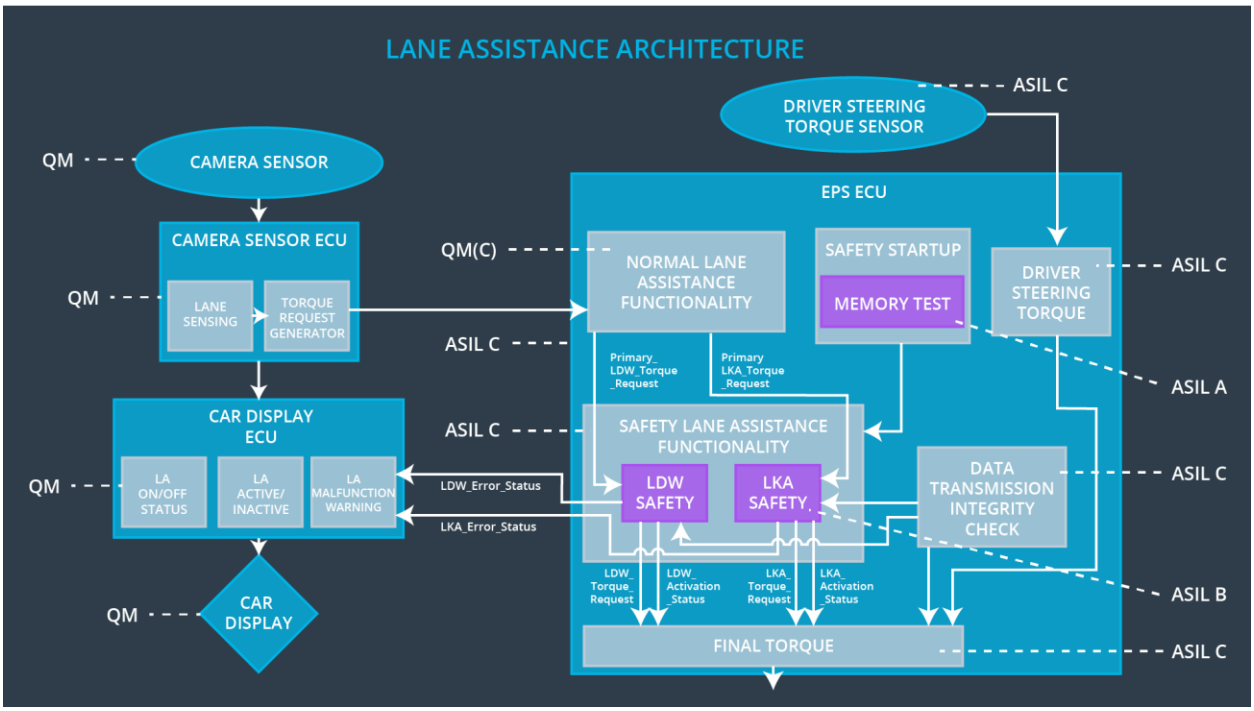
Technical Safety Requirement 04	As soon as the LKA feature is deactivated by the LKA function the car display ECU should show a warning light.	B	500 ms	LKA safety	LKA torque request should be zero
Technical Safety Requirement 05	Memory test should be done at start of the EPS ECU to check for any faults in memory	A	ignition cycle	LKA safety	LKA torque request should be 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]

All technical safety requirements are allocated to the electronic power steering ECU. For exact allocation with EPS ECU compare the technical requirement table above.

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 the lane assistance functionality	Malfucntion_01 Malfucntion_02	Yes	Turn on warning light on car display
WDC-02	Turn off the lane assistance functionality	Malfucntion_03	Yes	Turn on warning light on car display