Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: [1.0]

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
1/29/19	1.0	Dylan Brandtner	First version
1/30/2019	1.1	Dylan Brandtner	Updates from review

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 is more concrete and gets into the details of the item's technology such as sensors, control units, and actuators. Technical safety requirements are general hardware and software requirements but still without getting into specific details.

Inputs to the Technical Safety Concept

Functional Safety Requirements

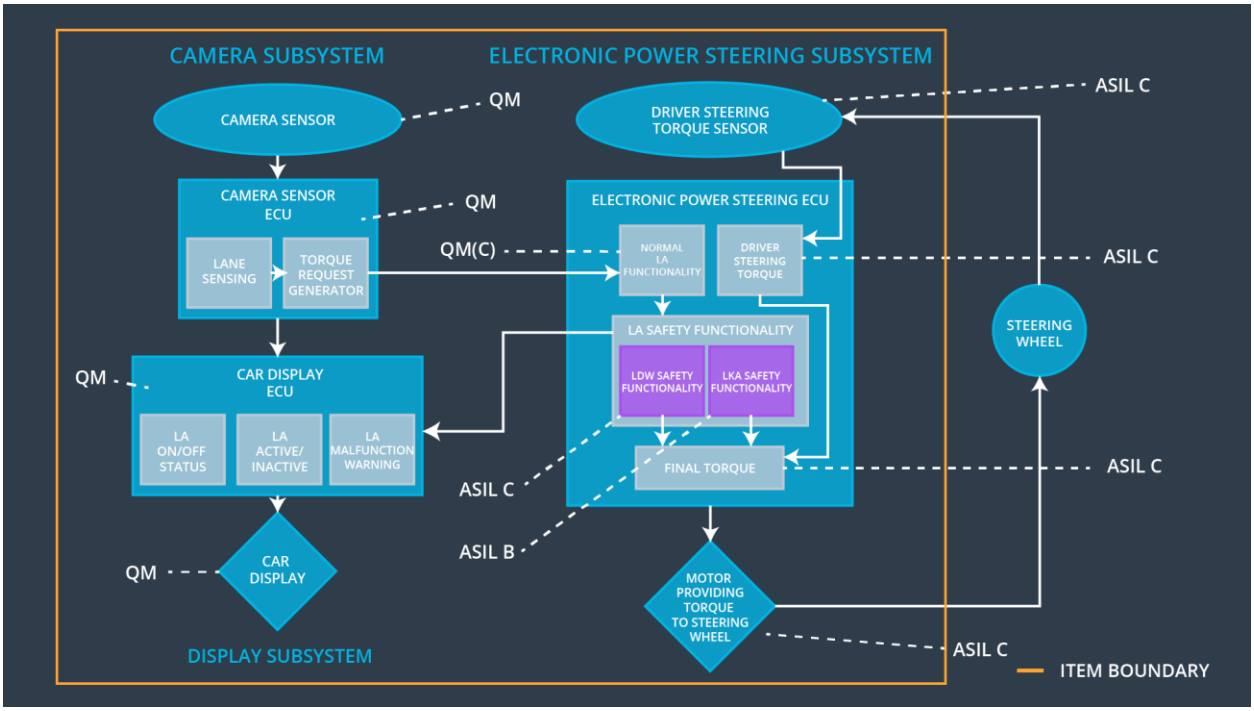
[Instructions: Provide the functional safety requirements derived in the functional safety concept]

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	Torque set 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	C	50ms	Torque set to 0
Functional Safety Requirement 01-03	The lane keeping item shall ensure that the lane departure oscillating torque is never applied while vehicle is not in Drive	QM	50ms	Torque set to 0
Functional Safety Requirement	Electronic power steering ECU shall ensure that the lane keeping assistance torque is	B	500	Torque set to 0

02-01	applied for only Max_Duration			

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	Reads in images from the road
Camera Sensor ECU - Lane Sensing	Senses lanes on road images
Camera Sensor ECU - Torque request generator	Requests a torque change when vehicle is outside the ego lane

Car Display	Displays information to the driver
Car Display ECU - Lane Assistance On/Off Status	Displays warning light indicating whether Lane Assistance system is on or off
Car Display ECU - Lane Assistant Active/Inactive	Displays warning light indicating whether Lane Assistance system is active
Car Display ECU - Lane Assistance malfunction warning	Displays warning light indicating whether Lane Assistance system is malfunctioning
Driver Steering Torque Sensor	Identifies amount of steering torque currently being applied to wheels
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Identifies amount of steering torque currently being applied to wheels
EPS ECU - Normal Lane Assistance Functionality	Determines the amount of steering torque to send to wheels to steer car back into ego lane and warn user of lane departure
EPS ECU - Lane Departure Warning Safety Functionality	Determines if amplitude and frequency of oscillating steering torque for Lane Departure warning exceeds limits and if so, it disables the LDA and warns the user
EPS ECU - Lane Keeping Assistant Safety Functionality	Determines if duration of steering torque for Lane Keeping Assistance exceeds limits and if so, it disables the LKA and warns the user
EPS ECU - Final Torque	Determines the final amount of steering torque to send to wheels to steer car back into ego lane after values have been validated by safety functionality
Motor	Provides steering torque to wheels

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 steering Torque' component is below 'Max_Torque_Amplitude.'	C	50ms	EPS ECU - Lane Departure Warning Safety Functionality	LDW will set 'LDW_Torque_Request' 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.	C	50ms	EPS ECU - Lane Departure Warning Safety Functionality	LDW deactivated
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'	C	50ms	EPS ECU - Lane Departure Warning Safety	LDW will set 'LDW_Torque_Request' amplitude to 0

	shall be set to zero.			Functionality	
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50ms	EPS ECU – 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	Memory Test	LDW will set 'LDW_Torque_Request' amplitude to 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 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	The LDW safety component shall	C	50ms	EPS ECU -	LDW

Safety Requirement 01	ensure that the frequency of the 'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Frequency.'			Lane Departure Warning Safety Functionality	will set 'LDW_Torque_Request' frequency 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	50ms	EPS ECU - Lane Departure Warning Safety Functionality	LDW deactivated
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	50ms	EPS ECU - Lane Departure Warning Safety Functionality	LDW will set 'LDW_Torque_Request' frequency to 0
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50ms	EPS ECU – 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	Memory Test	LDW will set 'LDW_Torque_Request' frequency to 0

Functional Safety Requirement 01-3 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 01-03	The lane keeping item shall ensure that the lane departure oscillating torque is never applied	X		

	while vehicle is not in Drive			

Technical Safety Requirements related to Functional Safety Requirement 01-03 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 a 'LDW_Torque_Request' is never sent to the 'Final electronic power steering Torque' component if the vehicle is not in Drive	QM	50ms	EPS ECU - Lane Departure Warning Safety Functionality	LDW will set 'LDW_Torque_Request' 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.	QM	50ms	EPS ECU - Lane Departure Warning Safety Functionality	LDW deactivated
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.	QM	50ms	EPS ECU - Lane Departure Warning Safety Functionality	LDW will set 'LDW_Torque_Request' to 0
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50ms	EPS ECU – 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	Memory Test	LDW will set 'LDW_Torque_Request' to 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 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 the duration of the 'LKA_Torque_Request' sent to the 'Final electronic power	B	500ms	EPS ECU - Lane Keeping Assistant Safety Functionality	LKA will set LKA_Torque_Request to 0

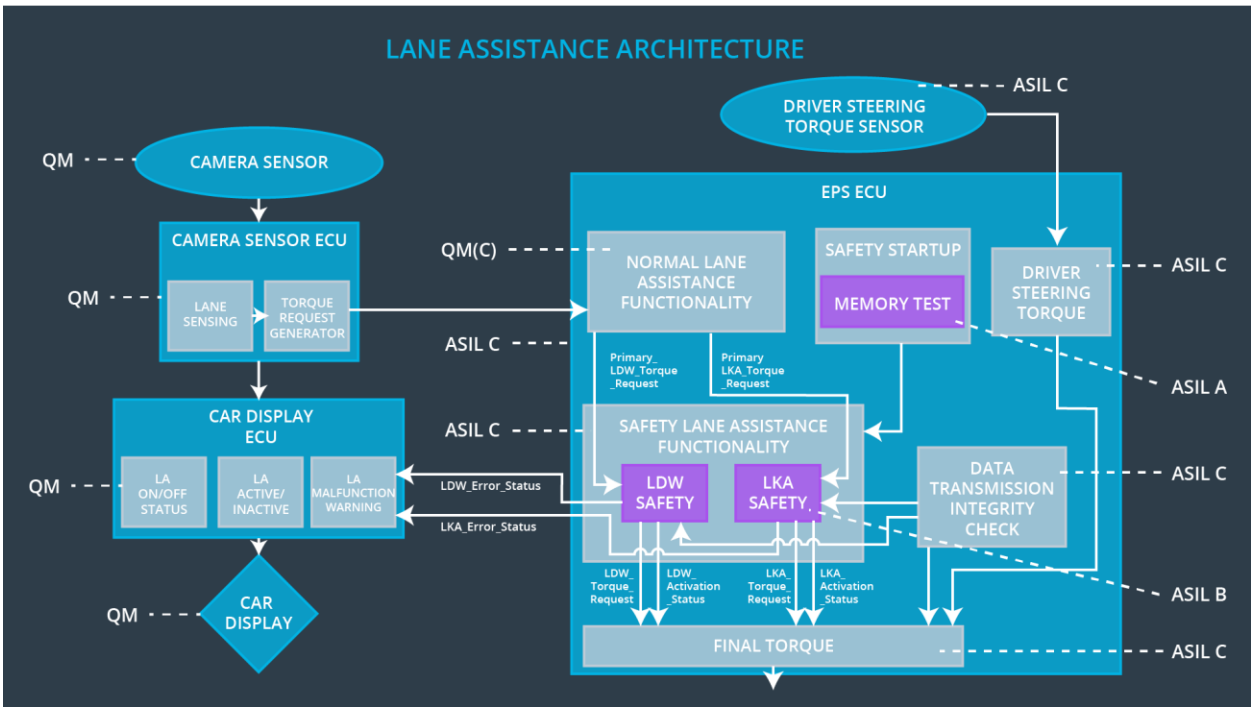
	steering Torque' component is shorter than ‘Max_Duration’				
Technical Safety Requirement 02	As soon as the LKA function deactivates the LKA feature, the ' LKA Safety' software block shall send a signal to the car display ECU to turn on a warning light.	B	500ms	EPS ECU - Lane Keeping Assistant Safety Functionality	LKA deactivated
Technical Safety Requirement 03	As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and the 'LKA_Torque_Request' shall be set to zero.	B	500ms	EPS ECU - Lane Keeping Assistant Safety Functionality	LKA will set 'LKA_Torque_Request' to 0
Technical Safety Requirement 04	The validity and integrity of the data transmission for ' LKA_Torque_Request' signal shall be ensured.	B	500ms	EPS ECU – 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	Memory Test	LKA will set 'LKA_Torque_Request' 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]

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.]

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off LDW functionality	Malfunction_01, Malfunction_02, Malfunction_04	Yes	Warning light on Car Display shows user LDW is turned off
WDC-02	Turn of LKA functionality	Malfunction_03	Yes	Warning light on Car Display shows user LKA is turned off