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
10/04/2017	1.0	Alessandro Gullì	First Submission

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 goal of technical safety is avoiding accidents by reducing risk to acceptable level, which provides a more deep insight compared to the general overview given by the functional safety concept

Inputs to the Technical Safety Concept

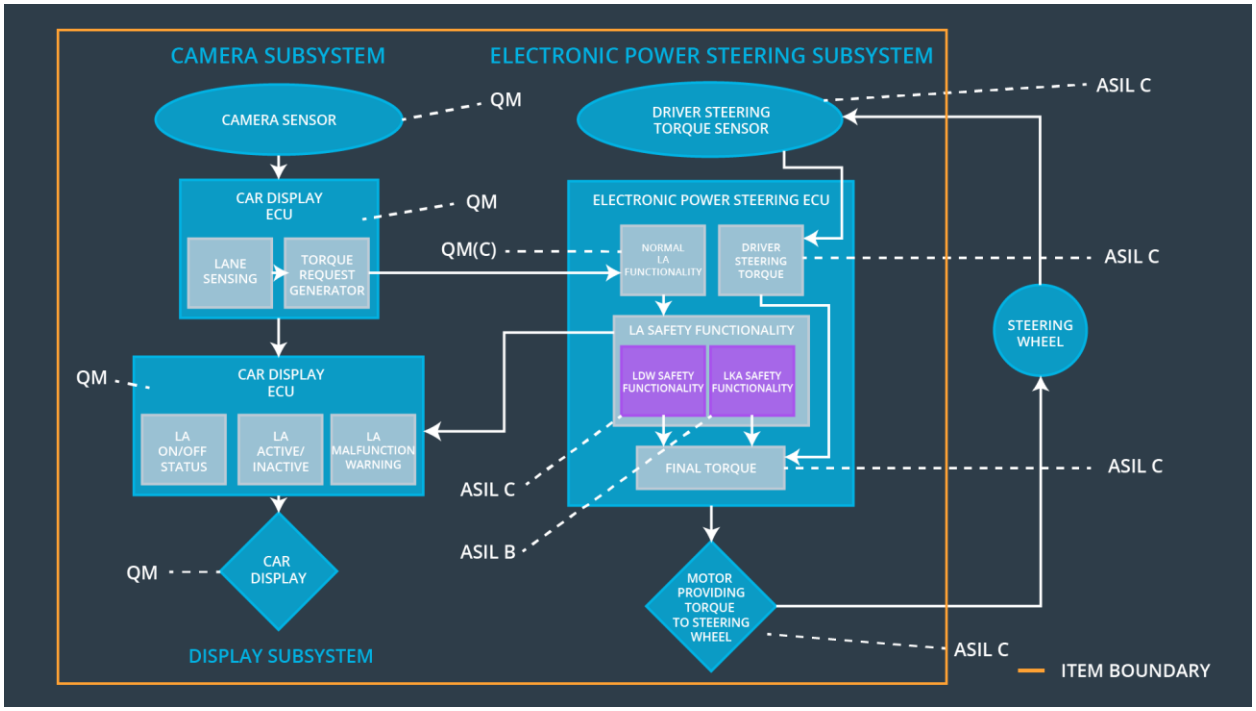
Functional Safety Requirements

[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	50 mS	LDW set the oscillating torque amplitude 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	50 mS	LDW set the oscillating torque frequency to 0
Functional Safety Requirement 02-01	The lane keeping assistance function shall be time limited and the additional steering torque shall end after a given time interval so that the driver cannot misuse the system for autonomous driving	B	500 mS	LKA set the intervention time 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	It reads in images from the road
Camera Sensor ECU - Lane Sensing	Detects lanes from the road and communicate with the Camera Sensor ECU - Torque request generator
Camera Sensor ECU - Torque request generator	Ensure torque request amplitude is below maximum
Car Display	The Car Display notifies that the lane has been

	departed and receives data from the Camera Sensor ECU regarding the Lane Assistance System functionality informing the driver about the situation
Car Display ECU - Lane Assistance On/Off Status	It controls a light that tells the driver if the lane keeping item is on or off
Car Display ECU - Lane Assistant Active/Inactive	It tells the driver that the lane departure warning is activated or not
Car Display ECU - Lane Assistance malfunction warning	It receives from the LA Safety Functionality a malfunctioning warning
Driver Steering Torque Sensor	Measures the steering torque of the driver and send information to the Electronic Power Steering ECU
Electronic Power Steering (EPS) ECU - Driver Steering Torque	The EPS ECU set the steering torque and ensure output is below maximum
EPS ECU - Normal Lane Assistance Functionality	It sends requests to the LA Safety
EPS ECU - Lane Departure Warning Safety Functionality	It receives the vibration torque functionality from the Camera Sensor ECU –Torque Request (Amplitude and Frequency)
EPS ECU - Lane Keeping Assistant Safety Functionality	It receives the vibration torque functionality from the Camera Sensor ECU –Torque Request (Duration)
EPS ECU - Final Torque	It outputs the final torque to the motor
Motor	The Motor provides 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 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	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 03	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the amplitude of the LDW_Torque_Request shall be set to zero	C	50 mS	LDW Safety Functionality	LDW torque output is set to zero
Technical Safety Requirement 04	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 05	Memory test shall be conducted at start-up of the EPS ECU to check for any faults in memory	A	Ignition cycle	Ignition Cycle	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]

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	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 03	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the frequency of the LDW_Torque_Request shall be set to zero	C	50 mS	LDW Safety	LDW torque output is set to zero
Technical Safety Requirement 04	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 05	Memory test shall be conducted at start-up of the EPS ECU to check for any faults in memory	C	50 mS	Ignition Cycle	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.]

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Technical Safety Requirement 01	Test and validate that the 'Max_Torque_Frequency' and the 'Max_Torque_Amplitude' chose really did dissuade drivers from taking their hands off the wheel	Verify that the system really does turn off if the lane keeping assistance every exceeded both 'Max_Torque_Frequency' and' Max_Torque_Amplitude'
Technical Safety Requirement 02	Test and validate that the warning light chose doesn't introduce items of distraction for the driver which can cause collisions	Verify that the light is well signaled and understandable from the driver
Technical Safety Requirement 03	Test and validate that the absence of torque shall be well perceived by the driver	Verify and measure that the torque is really set to zero
Technical Safety Requirement 04	Test and validate that the communications between nodes shall be effectively up and running	Verify the communication is guaranteed introducing mechanisms for errors detection, like the CRC
Technical Safety Requirement 05	Test and validate that the memory isn't affected by any faults at the startup	Verify through a safety check that the memory areas are correctly written or read

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 LKA_Torque_Request' sent to the 'Final electronic power steering Torque' component is below Max_Duration	B	500 mS	LKA Safety	LKA torque output is set to zero
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	LKA torque output is set to zero
Technical Safety Requirement 03	As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and LKA_Torque_Request shall be set to zero	B	500 mS	LKA Safety	LKA torque output is set to zero
Technical Safety Requirement 04	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 05	Memory test shall be conducted at start-up of the EPS ECU to check for any faults in memory	B	500 mS	Ignition Cycle	LKA torque output is set to zero

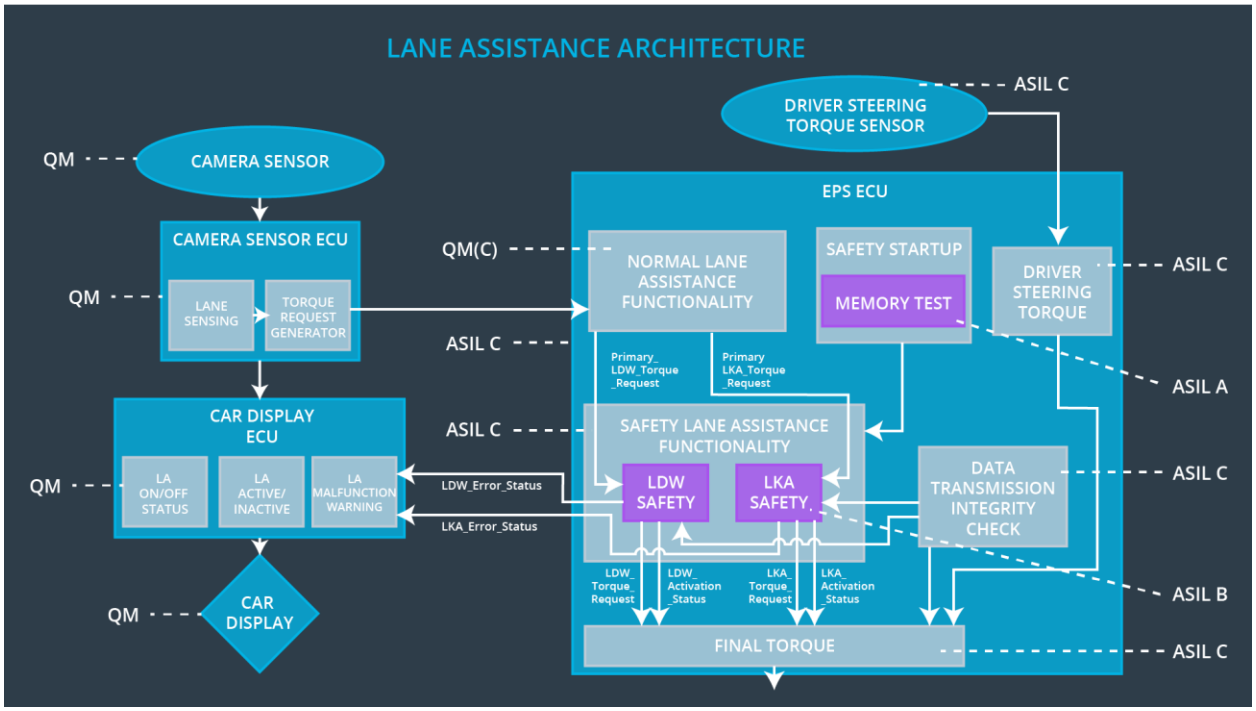
Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:

[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.]

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Technical Safety Requirement 01	Test and validate that the max_duration chose really did dissuade drivers from taking their hands off the wheel	Verify that the system really does turn off if the lane keeping assistance every exceeded max_duration
Technical Safety Requirement 02	Test and validate that the warning light chose doesn't introduce items of distraction for the driver which can cause collisions	Verify that the light is well signaled and understandable by the driver
Technical Safety Requirement 03	Test and validate that the absence of torque shall be well perceived by the driver	Verify and measure that the torque is really set to zero
Technical Safety Requirement 04	Test and validate that the communications between nodes shall be effectively up and running	Verify the communication is guaranteed introducing mechanisms for errors detection, like the CRC
Technical Safety Requirement 05	Test and validate that the memory isn't affected by any faults at the startup	Verify through a safety check that the memory areas are correctly written or read

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 the allocations for this particular requirement about technical requirements are allocated to the EPS ECU, divided mainly into four blocks or LDW Safety, LKA Safety, Data Transmission Check and Ignition Cycle.

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 functionality	Malfunction	YES	Through the Car Display, a warning light turns on
WDC-02	Turn off the functionality	Malfunction	YES	Through the Car Display, a warning light turns on