Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
12/12/17	1.0	Raz Nissim	Initial version

Table of Contents

Purpose of the Technical Safety Concept

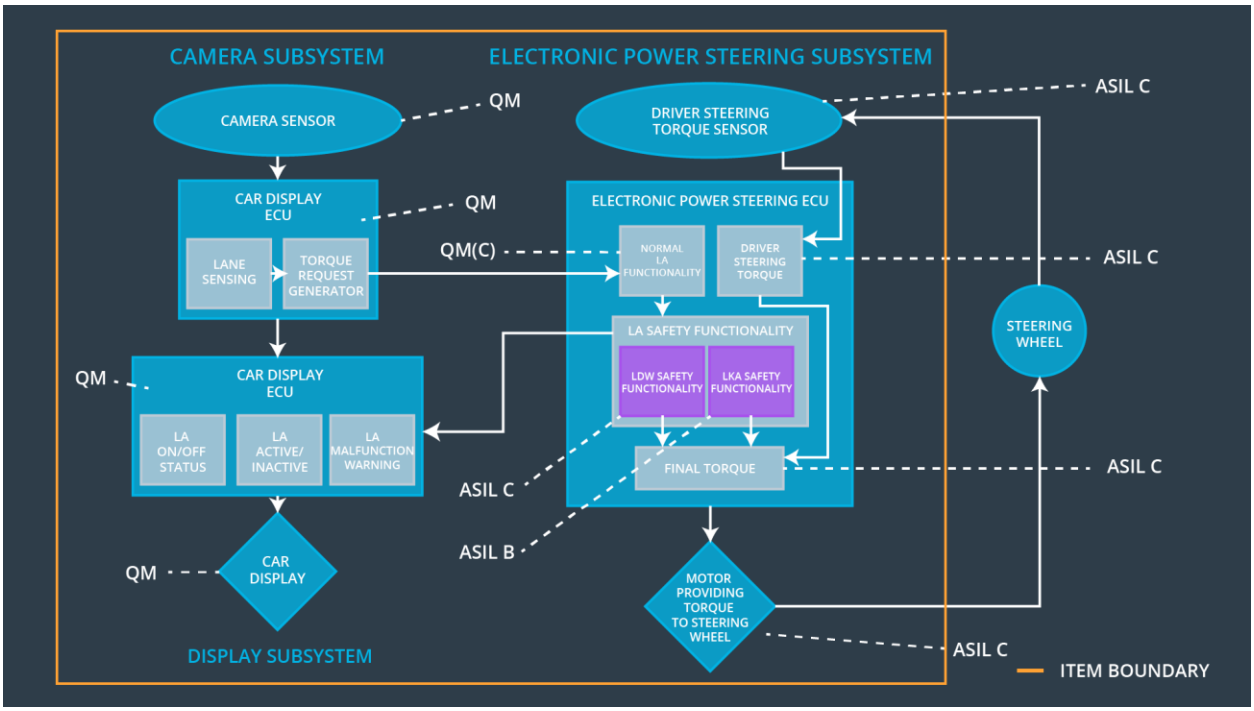
the technical safety concept involves turning functional safety requirements into technical safety requirements and allocating technical safety requirements to the system architecture.

Inputs to the Technical Safety Concept

Functional Safety Requirements

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	LDW oscillating torque amplitude shall be below MAX_TORQUE_AMPLITUDE	C	50ms	Set vibration torque amplitude to 0.
Functional Safety Requirement 01-02	LDW oscillating torque frequency shall be below MAX_TORQUE_FREQUENCY	C	50ms	Set vibration torque amplitude to 0.
Functional Safety Requirement 02-01	The Electronic Power Steering ECU shall ensure that the lane keeping assistance torque is only applied for MAX_DURATION	B	500	Set lane keeping assistance torque to 0

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Physical sensor responsible for detecting lane lines
Camera Sensor ECU - Lane Sensing	Software module which interprets sensor data and identifies lane markings in the image. Determines the position of the vehicle relative to the lane.
Camera Sensor ECU - Torque request generator	Software module in the camera sensor ECU which issues torque requests to the Electronic Power Steering ECU.
Car Display	Vehicle dashboard lights or display unit providing status feedback to the driver of vehicle systems.
Car Display ECU - Lane Assistance On/Off Status	A status light or LCD illustration on the car display which indicates the status of the Lane Assistance function as ON/OFF.
Car Display ECU - Lane Assistant Active/Inactive	A status light or LCD illustration on the car display which indicates the status of the Lane Assistance function as Active / Inactive.

Car Display ECU - Lane Assistance malfunction warning	A status light or LCD illustration on the car display which indicates warnings or fault of the Lane Assistance function
Driver Steering Torque Sensor	Physical sensor such as an encoder or strain gauge capable of measuring steering torque input on the steering wheel from the driver.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	A hardware / software module on the Power Steering ECU which measures the signal from the Torque sensor and provides a software value of the driver steering torque.
EPS ECU - Normal Lane Assistance Functionality	A non-safety verified software module which accepts torque requests from the camera sensor ECU and generates an output torque for the motor.
EPS ECU - Lane Departure Warning Safety Functionality	A safety verified software module which monitors and passes through the output of the Normal Lane Assistance Functionality for faults related to safety requirements of the LDW function. (Such as max torque amplitude and frequency)
EPS ECU - Lane Keeping Assistant Safety Functionality	A safety verified software module which monitors and passes through the output of the Normal Lane Assistance Functionality for faults related to safety requirements of the LKA function. (Such as MAX_DURATION for torque output)
EPS ECU - Final Torque	A software value of the final torque which should be output to the Electronic Power Steering Motor based on the Lane Assistance Function and the driver input measured torque.
Motor	The motor which applies torque to the steering column, accepts voltage / current control from the Power Steering ECU.

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 Functionalily (LDW Safety Block)	Turn off functionality
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 Safety Block)	Turn off functionality
Technical Safety Requirem	As soon as a failure is detected by the LDW function, it shall	C	50ms	EPS ECU - Lane Departure	Turn off functionality

ent 03	deactivate the LDW feature and the 'LDW_Torque_Request' shall be set to zero.			Warning Safety Functionality (LDW Safety Block)	
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50ms	EPS ECU - Lane Departure Warning Safety Functionality, EPS ECU - Final Torque (Data Integrity Check)	Turn off functionality
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 time	EPS ECU hardware	Turn off functionality

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	ASI	Fault Tolerant Time	Architecture Allocation	Safe State

		L	Interval		
Technical Safety Requirement 01	The LDW safety component shall ensure that the frequency of the 'LDW_Torque_Request_Rate' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Frequency.	C	50ms	EPS ECU - Lane Departure Warning Safety Functionality (LDW Safety Block)	Turn off function ality
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 Safety Block)	Turn off function ality
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_Requestt' shall be set to zero.	C	50ms	EPS ECU - Lane Departure Warning Safety Functionality (LDW Safety Block)	Turn off function ality
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50ms	EPS ECU - Lane Departure Warning Safety Functionality, EPS ECU - Final Torque (Data Integrity Check)	Turn off function ality
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 time	EPS ECU hardware	Turn off function ality

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:

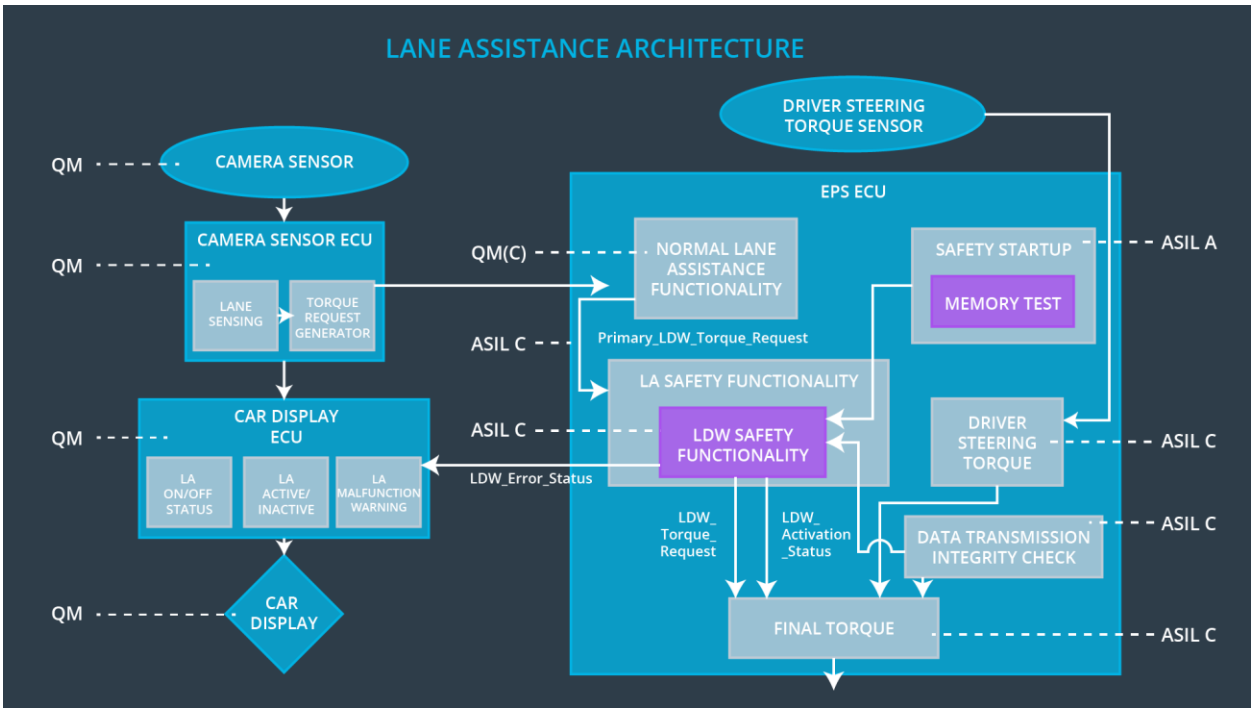
ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01	The LKA safety component shall ensure that the time of the 'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is below ‘Max_Duration’.	B	500ms	EPS ECU - Lane Keep Assistance Safety Module (LDW Safety Block)	Turn off functionality

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 Assistance Safety Functionality (LDW Safety Block)	Turn off functionality
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 Assistance Safety Functionality (LDW Safety Block)	Turn off functionality
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	B	500ms	EPS ECU - Lane Keeping Assistance Safety Functionality, EPS ECU - Final Torque (Data integrity Check)	Turn off functionality
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 time	EPS ECU Hardware	Turn off functionality

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



Allocation of Technical Safety Requirements to Architecture Elements

All technical safety requirements are allocated to the Power Steering ECU.

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	turn off the functionality	Malfunction_01/ 02	yes	Car display
WDC-02	turn off the functionality	Malfunction_03	yes	Car display