Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 1.0
Released on 2017-09-11

Document history

Date	Version	Editor	Description
09/11/2018	1.0	Vianney Monestel	First release

Table of Contents

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

The purpose of the technical safety concept is to derive technical safety requirements from the functional safety requirements. These new requirements are allocated to the system architecture and they go into more technical details of the system. Technical safety requirements are general hardware and software requirements but still without getting into specific details (they are related to parts like sensors, control units, ...).

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	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50ms	Vibration amplitude is below Max_Torque_Amplitude value
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	Vibration frequency is below Max_Torque_Frequency value
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	500ms	System is off

Refined System Architecture from Functional Safety Concept

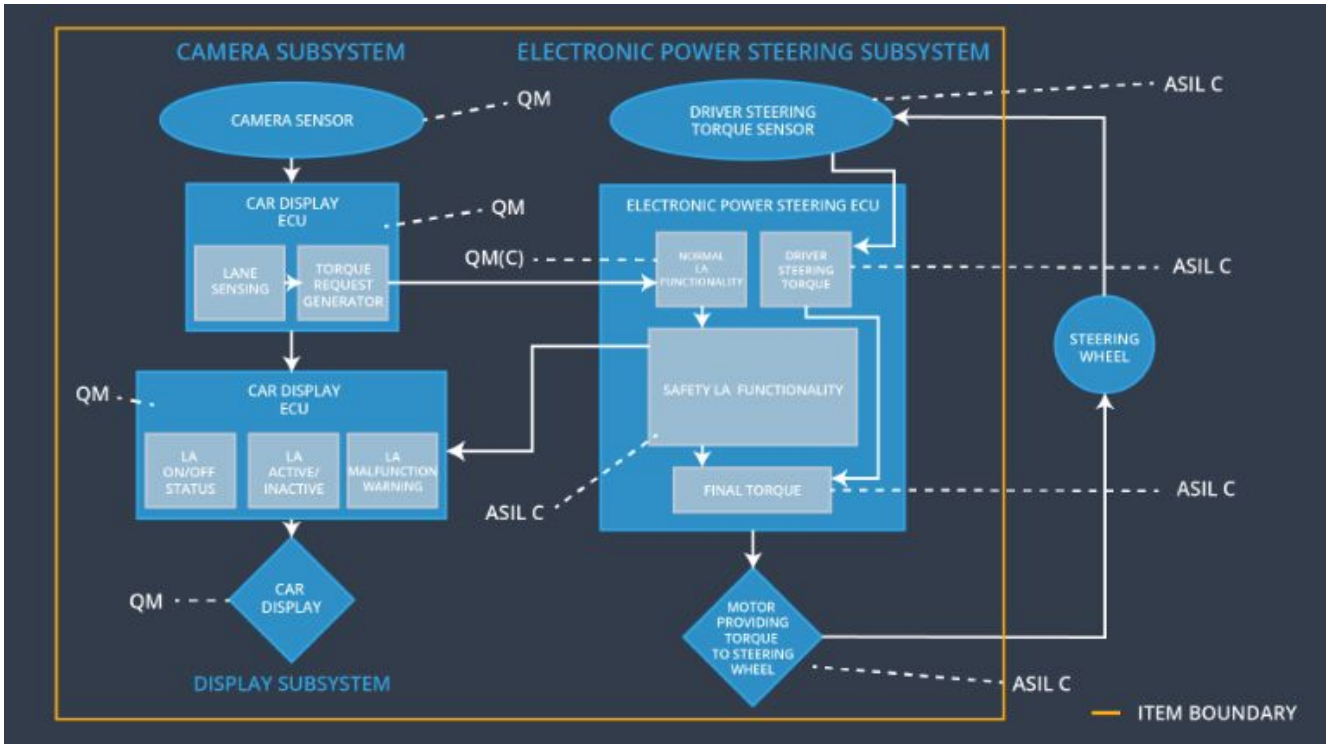

Figure 1. System Architecture with ASIL labels

Functional overview of architecture elements

Element	**Description**
Camera Sensor	Capture lane images and provide them to the Camera Sensor ECU.
Camera Sensor ECU - Lane Sensing	Determine the car position respect to its lane using the images provided by the camera sensor.
Camera Sensor ECU - Torque request generator	Request an amount of torque to the EPS based on the current car position.
Car Display	Show warnings on the car’s dashboard.

Car Display ECU - Lane Assistance On/Off Status	Show if the Lane Keeping Assistance is on or off.
Car Display ECU - Lane Assistant Active/Inactive	Indicate if the Lane Assistance has detected that the car is moving out of its lane and its active because of that
Car Display ECU - Lane Assistance malfunction warning	Show any malfunction in the Lane Assistance system.
Driver Steering Torque Sensor	Determine the current torque amount applied to the wheel by the driver.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Receive and process the input from the Driver Steering Torque Sensor
EPS ECU - Normal Lane Assistance Functionality	Process the input torque from the Camera Sensor - Torque request generator
EPS ECU - Lane Departure Warning Safety Functionality	Ensure that the requested torque amplitude is below Max_Torque_Amplitude and that the requested torque frequency is below Max_Torque_Frequency
EPS ECU - Lane Keeping Assistant Safety Functionality	Ensure that the lane keeping assistance torque is activated for only Max_Duration time, otherwise the system is turned off.
EPS ECU - Final Torque	Determines the final torque amount using the input from the Lane Keeping Assistance and the Lane Departure Warning.
Motor	Receive the final torque amount and applies it to the steering wheel.

Technical Safety Concept

Technical Safety Requirements

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 01-01-01	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 functionality	LDW torque is equal to zero.
Technical	As soon as the LDW function	C	50 ms	LDW safety	LDW torque

Safety Requirement 01-01-02	deactivates the LDW feature, the 'LDW Safety' software block shall send a signal to the car display ECU to turn on a warning light.			functionality	is equal to zero.
Technical Safety Requirement 01-01-03	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	50 ms	LDW safety functionality	LDW torque is equal to zero.
Technical Safety Requirement 01-01-04	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 is equal to zero.
Technical Safety Requirement 01-01-05	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 torque is equal to zero.

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 01-02-01	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 functionality	LDW torque is equal to zero.
Technical Safety Requirement 01-02-02	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 functionality	LDW torque is equal to zero.
Technical Safety Requirement 01-02-03	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	50 ms	LDW safety functionality	LDW torque is equal to zero.
Technical Safety Requirement 01-02-04	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 is equal to zero.
Technical Safety Requirement 01-02-05	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 torque is equal to zero.

Lane Keeping Assistance (LKA) Requirements:

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 02-01-01	The LKA safety component shall ensure that the lane keeping assistance torque is applied for only Max_Duration.	B	500 ms	LKA safety functionality	LKA torque is equal to zero.
Technical Safety Requirement 02-01-02	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 functionality	LKA torque is equal to zero.
Technical Safety Requirement 02-01-03	As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and the 'LKA_Torque_Request' shall	B	500 ms	LKA safety functionality	LKA torque is equal to zero.

	be set to zero.				
Technical Safety Requirement 02-01-04	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 is equal to zero.
Technical Safety Requirement 02-01-05	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 torque is equal to zero.

Refinement of the System Architecture

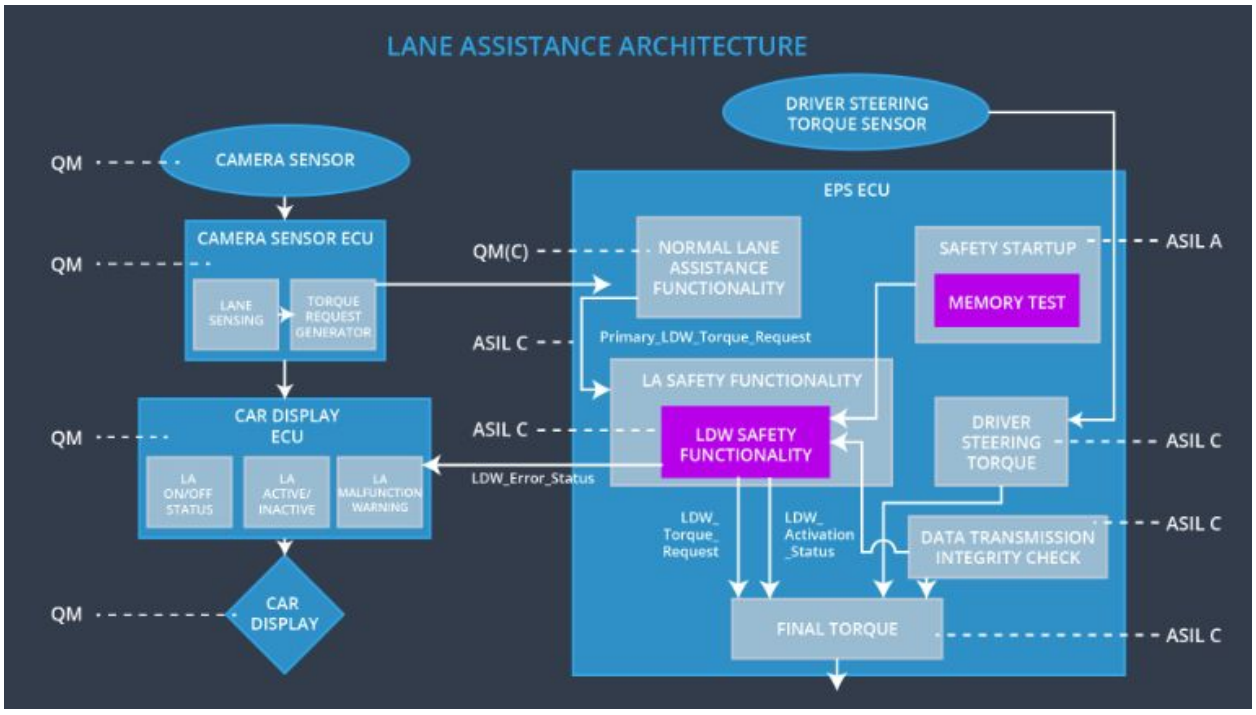

Figure 2. Architecture refinement with the allocation of technical safety concept

Allocation of Technical Safety Requirements to Architecture Elements

For this particular item, all the technical safety requirements are allocated to the Electronic Power Steering ECU and no other elements are involved.

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off the system	Malfunction_01 Malfunction_02	Yes	Lane Departure Malfunction warning displayed to the driver.
WDC-02	Turn off the system	Malfunction_03	Yes	Lane Keeping Assistance warning displayed to the driver.