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
01.03.2019	1.0	Hiep Truong Cong	First draft
08.03.2019	2.0	Hiep Truong Cong	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

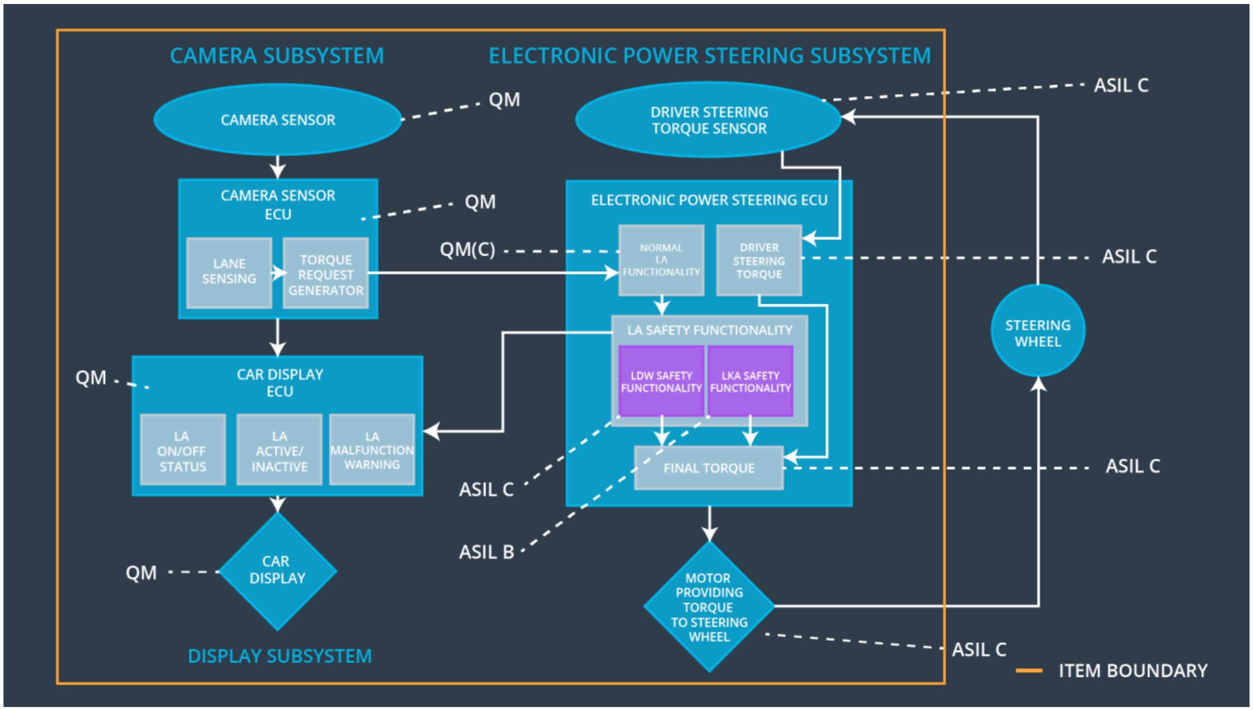
Purpose of a technical safety concept is to define new requirements and then allocating those requirements to system architecture in a low level. Technical Safety concept is looking at the safety requirements of sensors, control units and actuators.

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 electronic power steering ECU shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitue	C	50 ms	LDW will set the oscillating torque 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 will set the oscillating torque to 0.
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	500 ms	Lane Keeping Assistance torque is zero

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Take images from the road
Camera Sensor ECU - Lane Sensing	Detecting lane lines and determining when the vehicle leaves the lane
Camera Sensor ECU - Torque request generator	request electronic power steering ECU to generate a demand torque, send appropriate messages to the car display ECU
Car Display	Display warning messages and system states
Car Display ECU - Lane Assistance On/Off Status	Display status of Lane Assistance System, it the system is switched on or off
Car Display ECU - Lane Assistant Active/Inactive	Display if the lane Assistance in active or idle mode
Car Display ECU - Lane Assistance malfunction warning	Display warnings
Driver Steering Torque Sensor	Measure steering torque on the steering wheel,

	produced by the driver
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Monitoring steering torque applied by the driver
EPS ECU - Normal Lane Assistance Functionality	Realize normal functionalities of Lane Assistance Item, such as Lane Departure Warning and Land keeping assistance
EPS ECU - Lane Departure Warning Safety Functionality	Monitoring the oscillating torque amplitude and frequency
EPS ECU - Lane Keeping Assistant Safety Functionality	Monitoring the active duration of Lane Keeping Assistance
EPS ECU - Final Torque	Decide which torque will be applied to steering system.
Motor	Generate torque 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 eclectronic power steering Torque' component is below 'Max_Torque_Ampliture'	C	50 ms	LDW Safety functionality	LDW will set the oscillating torque to 0.
Technical Safety Requirement 01-01-02	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured	C	50 ms	Data Transmission integrity check	LDW will set the oscillating torque to 0.
Technical Safety Requirement 01-01-03	As soon as 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 will set the oscillating torque to 0.
Technical Safety Requirement 01-01-04	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 functioality	LDW will set the oscillating torque to 0.
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	B	Ignition cycle	Safety startup	LDW will set the oscillating torque to 0.

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 amplitude of the 'LDW_Torque_Request' sent to the 'Final eclectronic power steering Torque' component is below 'Max_Torque_Frequency'	C	50 ms	LDW Safety functionality	LDW will set the oscillating torque to 0.
Technical Safety Requirement 01-02-02	The validity and integrity of the data transmission for 'LDW_Torque_Frequency' signal shall be ensured	C	50 ms	Data Transmission integrity check	LDW will set the oscillating torque to 0.
Technical Safety Requirement 01-02-03	As soon as failure is detected by the LDW function, it shall deactivate the LDW feature and the 'LDW_Torque_Frequency' shall be set to zero	C	50 ms	LDW Safety functionality	LDW will set the oscillating torque to 0.
Technical Safety Requirement 01-02-04	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 functioality	LDW will set the oscillating torque to 0.
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	B	Ignition cycle	Safety startup	LDW will set the oscillating torque to 0.

Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria:

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Technical Safety Requirement 01-01-01	Validate the Max_Torque_Amplitude is high enough to warn the driver but not too high, so that the driver loses control	Verify that the the lane assistance output is set to zero with within the 50 ms fault tolerant time interval, when when the torque amplitude crosses the limit
Technical Safety Requirement 01-01-02	N.A.	Verify that LDW will set the oscillating torque to 0 when an invalid LDW_Torque_Request is detected
Technical Safety Requirement 01-01-03	N.A.	Verify that LDW_Torque_Request will be set to 0 when a failure is detected
Technical Safety Requirement 01-01-04	N.A.	Verify that the car display ECU turns on a warning light when the LDW function is deactivated
Technical Safety Requirement 01-01-05	N.A.	Verify that memory test is conducted and any memory faults will be detected
Technical Safety Requirement 01-02-01	Validate the Max_Torque_Frequency is high enough to be detected by the driver but not too high, so that the driver loses control	Verify that the the lane assistance output is set to zero with within the 50 ms fault tolerant time interval, when when the torque frequency crosses the limit
Technical Safety Requirement 01-02-02	LDW_Torque_Frequency	Verify that LDW will set the oscillating torque to 0 when an invalid LDW_Torque_Frequency is detected
Technical Safety Requirement 01-02-03	N.A.	Verify that LDW_Torque_Frequency will be set to 0 when a failure is detected
Technical Safety Requirement 01-02-04	N.A.	Verify that the car display ECU turns on a warning light when the LDW function is deactivated

Technical Safety Requirement 01-02-05	N.A.	Verify that memory test is conducted and any memory faults will be detected

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:

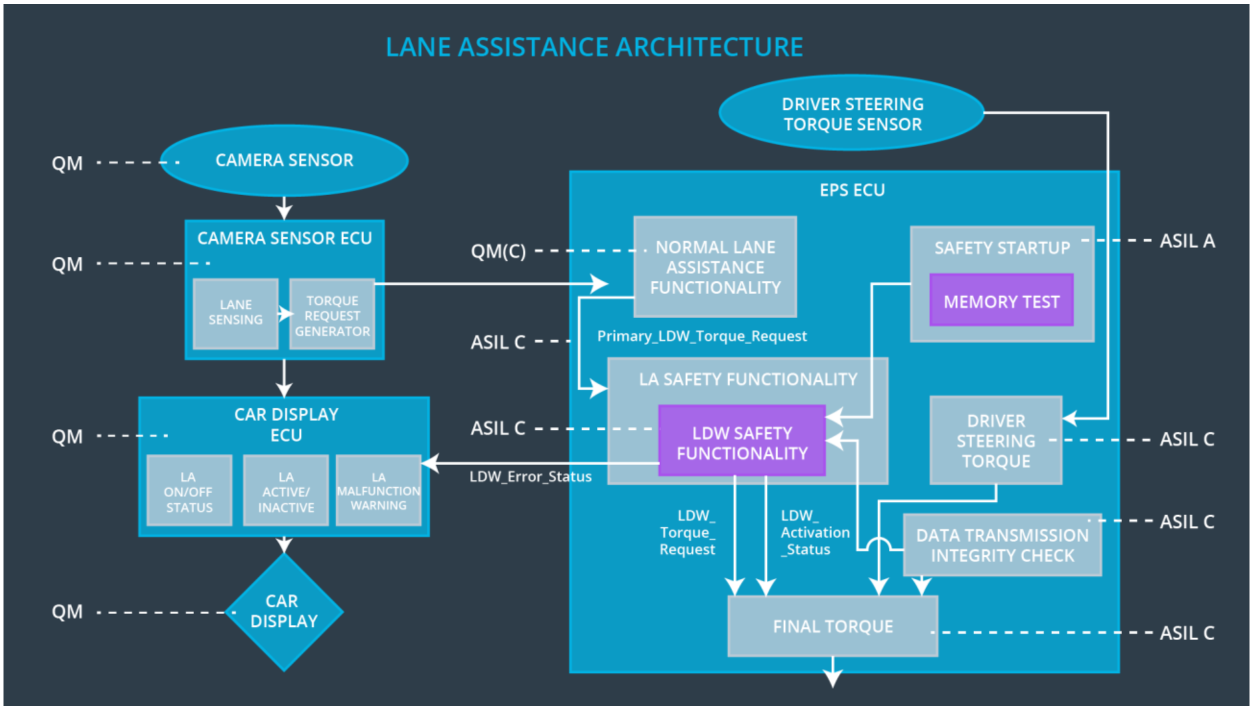
ID	**Technical Safety Requirement**	**ASIL**	**Fault Tolerant Time Interval**	**Allocation to Architecture**	**Safe State**
Technical Safety Requirement 02-01-01	The LKA safety component shall ensure the duration of the lane keeping assistance torque is applied for less than Max_Duration.	B	500 ms	LKA Safety	Lane Keeping Assistance torque is zero.
Technical Safety Requirement 02-01-02	The validity and integrity of the data transmission for ‚LKA_Torque_Request’ signal shall be ensured.	B	500 ms	LKA Safety	Lane Keeping Assistance torque is 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 be set to zero.	B	500 ms	LKA Safety	Lane Keeping Assistance torque is zero.

Technical Safety Requirement 02-01-04	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	Lane Keeping Assistance torque is 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	Safety startup	Lane Keeping Assistance torque is zero.

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

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Technical Safety Requirement 02-01-01	Validate the chosen Max_Duration not allow the driver to misuse the LKA as autonomous driving	Verify that the LKA will be deactivated if the active time exceeded Max_Duration
Technical Safety Requirement 02-01-02	N.A.	Verify that the LKA sets torque to 0 when errors are detected by Data Transmission Integrity Check
Technical Safety Requirement 02-01-03	N.A.	Verify that LKA will be deactivated and LKA_Torque_request is 0 after a failure was detected
Technical Safety Requirement 02-01-04	N.A	Verify if the car displays warning light when LKA function is deactivated.
Technical Safety Requirement 02-01-05	N.A	Verify that memory test is conducted and any memory faults will be detected

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Technical Safety Requirement 01-01-01	The LDW safety component shall ensure that the amplitude of the 'LDW_Torque_Request' sent to the 'Final eclectronic power steering Torque' component is below 'Max_Torque_Ampliture'	x		
Technical Safety Requirement 01-01-02	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured	x		
Technical Safety	As soon as failure is detected by the LDW function, it shall	x		

Requirement 01-01-03	deactivate the LDW feature and the ‘LDW_Torque_Request’ shall be set to zero			
Technical Safety Requirement 01-01-04	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	**x**		
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	**x**		
Technical Safety Requirement 01-02-01	The LDW safety component shall ensure that the amplitude of the ‘LDW_Torque_Request’ sent to the ‘Final eclectronic power steering Torque’ component is below ‘Max_Torque_Frequency’	**x**		
Technical Safety Requirement 01-02-02	The validity and integrity of the data transmission for ‘LDW_Torque_Frequency’ signal shall be ensured	**x**		
Technical Safety Requirement 01-02-03	As soon as failure is detected by the LDW function, it shall deactivate the LDW feature and the ‘LDW_Torque_Frequency’ shall be set to zero	**x**		
Technical Safety Requirement 01-02-04	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	**x**		
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	**x**		
Technical Safety Requirement	The LKA safety component shall ensure the duration of the lane	**x**		

02-01-01	keeping assistance torque is applied for less than Max_Duration.			
Technical Safety Requirement 02-01-02	The validity and integrity of the data transmission for ‚LKA_Torque_Request’ signal shall be ensured.	**x**		
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 be set to zero.	**x**		
Technical Safety Requirement 02-01-04	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.	**x**		
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.	**x**		

Warning and Degradation Concept

ID	**Degradation Mode**	**Trigger for Degradation Mode**	**Safe State invoked?**	**Driver Warning**
WDC-01	Lane departure warning shall be turned off	Malfunction_01 Malfunction_02	yes	Warning on car display
WDC-02	Lane keeping assistance shall be turned off	Malfunction_03	yes	Warning on car display