Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 1.1

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
Apr. 1, 2018	1.1	Yi-Ching Chung	First draft from the template.

Table of Contents

Purpose of the Technical Safety Concept

This document is to define and assign new requirements to the system architecture. These new requirements are more concrete and gets into details of the item's technology as specified by ISO 26262.

Inputs to the Technical Safety Concept

Functional Safety Requirements

This table provides the functional safety requirements derived in the functional safety concept.

Table 1 Functional safety requirements.

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	The Lane Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	C	50 ms	Vibration torque amplitude below Max_Torque_Amplitude.
Functional Safety Requirement 01-02	The Lane Departure Warning item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	C	50 ms	Vibration frequency is below Max_Torque_Frequency.
Functional Safety Requirement	The electronic power steering ECU shall ensure that the Lane Keeping Assistance torque is applied only	B	500 ms	Lane Keeping Assistance torque is zero.

02-01	Max_Duration.			

Refined System Architecture from Functional Safety Concept

The following figure includes the system architecture with the ASIL labels.

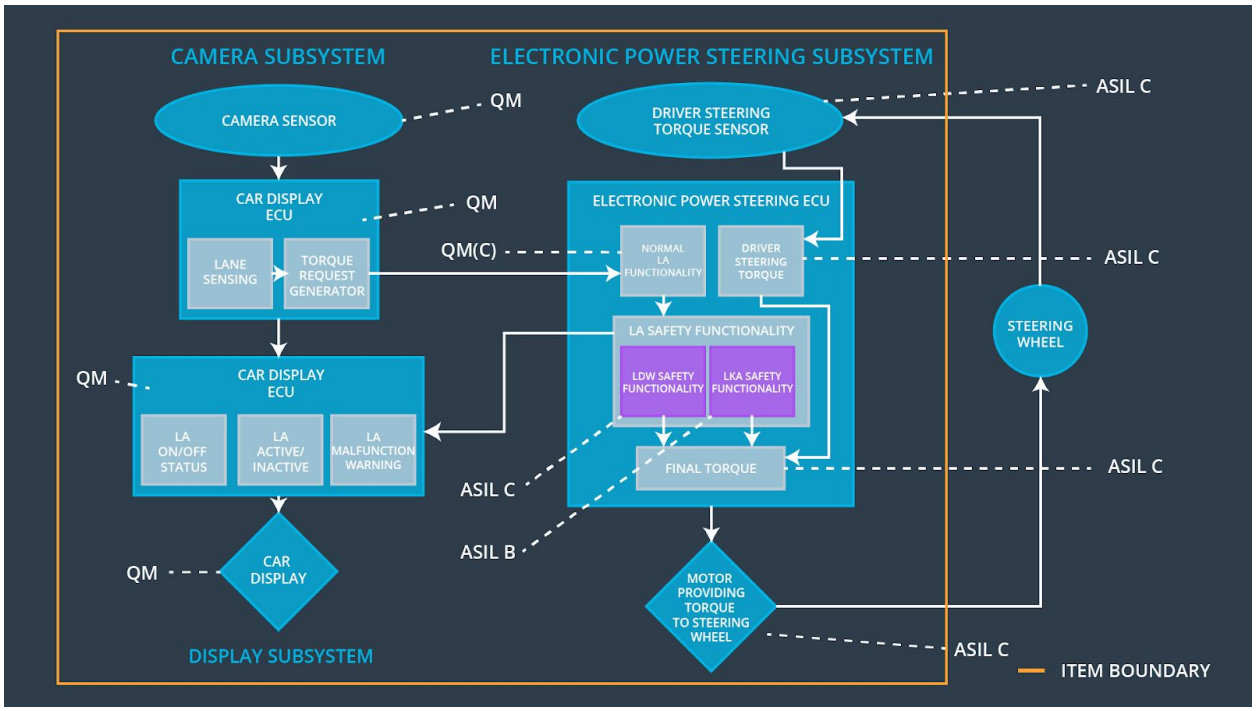

Fig 2 Refined system architecture (Udacity. *Functional Safety: Functional Safety Concept*. Retrieved from https://classroom.udacity.com/nanodegrees/nd013/parts).

Functional overview of architecture elements

This section provides a description for each functional safety element.

Table 2 Each element's purpose in the lane assistance item.

Element	**Description**
Camera Sensor	To capture road images and provide them to the Camera Sensor ECU.

Camera Sensor ECU - Lane Sensing	To detect the lane line positions from the Camera Sensor images.
Camera Sensor ECU - Torque request generator	To calculate the necessary torque to be requested to the Electronic Power Steering ECU.
Car Display	To display warning for the driver.
Car Display ECU - Lane Assistance On/Off Status	To Indicate the status of the Lane Assistance functionality (On/Off.)
Car Display ECU - Lane Assistant Active/Inactive	To indicate if the Lane Assistance functionality is properly functioning (Active/Inactive.)
Car Display ECU - Lane Assistance malfunction warning	To indicate a malfunction on the Lane Assistance functionality.
Driver Steering Torque Sensor	To measure the torque applied to the steering wheel by the driver.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	To receive the driver's torque request from the steering wheel.
EPS ECU - Normal Lane Assistance Functionality	To receive the Camera Sensor ECU torque request.
EPS ECU - Lane Departure Warning Safety Functionality	To ensure the torque amplitude is below Max_Torque_Amplitude and torque frequency is below Max_Torque_Frequency.
EPS ECU - Lane Keeping Assistant Safety Functionality	To ensure the Lane Keeping Assistance functionality application is not activate more than Max_duration time.
EPS ECU - Final Torque	To combine the torque request from the Lane Keeping and Lane Departure Warning functionalities and sends them to the Motor.
Motor	To apply the required torque to the steering

	wheels.

Technical Safety Concept

The following figure gives an overview (Fig. 3).

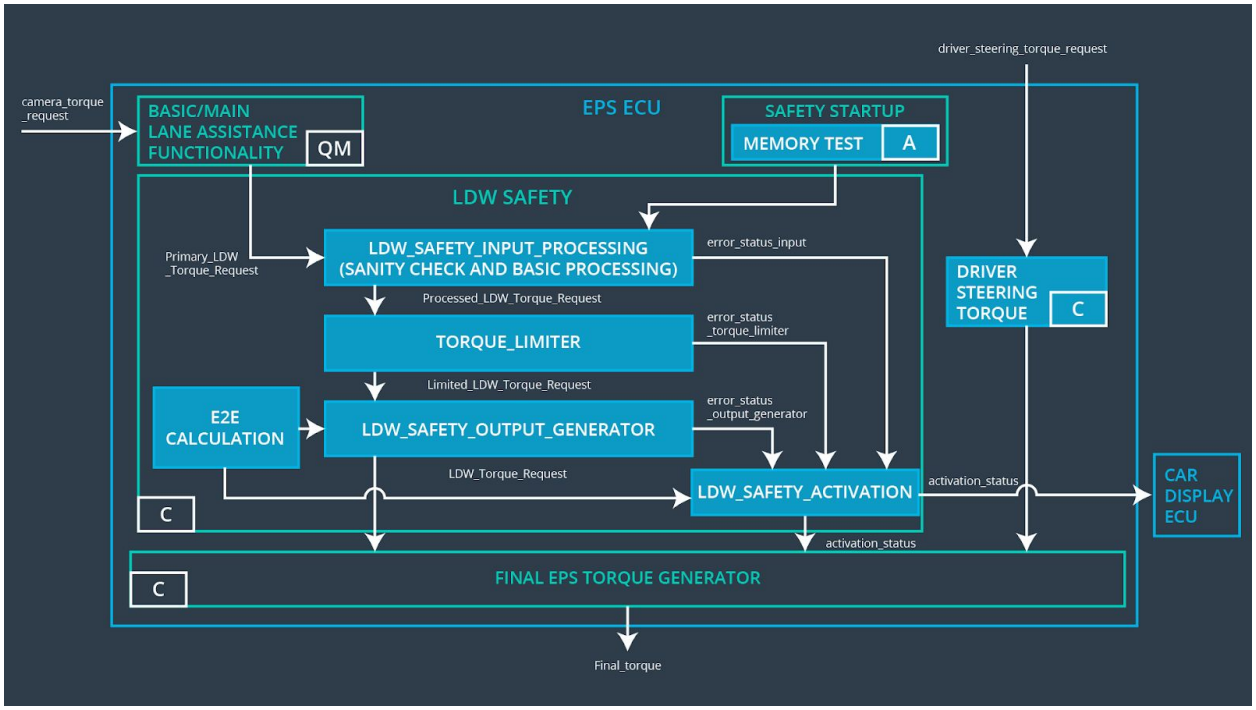

Fig. 3 Technical safety concept.

Technical Safety Requirements

The following table has provided the Lane Departure Warning (LDW) Requirements (derived in the functional safety concept).

Table 3 Functional Safety Requirement 01-01 with its associated system elements.

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety	The lane keeping item shall ensure that the lane departure	X		

Requirement 01-01	oscillating torque amplitude is below Max_Torque_Amplitude			

In Table 4, the architecture allocation column contains element names such as LDW Safety block, Data Transmission Integrity Check, etc.

Table 4 Technical Safety Requirements related to Functional Safety Requirement 01-01.

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 01	The Lane Departure Warning 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	Lane Departure Warning torque to zero.
Technical Safety Requirement 02	When the Lane Departure Warning is deactivated, the 'LDW Safety' software module shall send a signal to the Car Display ECU to turn on a warning signal.	C	50 ms	LDW Safety	Lane Departure Warning torque to zero.
Technical Safety Requirement 03	When a failure is detected by the Lane Departure Warning functionality, it shall deactivate the Lane	C	50 ms	LDW Safety	Lane Departure Warning torque to zero.

	Departure Warning feature and set 'LDW_Torque_Request' 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	LDW Safety	Lane Departure Warning torque to zero.
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any memory problems.	A	Ignition cycle	Data Transmission Integrity Check	Lane Departure Warning torque to zero.

Most of the technical safety requirements are similar. Here the frequency is discussed instead of amplitude (derived in the functional safety concept). Please see Table 5 and 6 for more details.

Table 5 Functional Safety Requirement 01-2 with its associated system elements.

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 in the following table.

Table 6 Technical safety requirements for the lane departure warning second functional safety requirement.

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 01	The Lane Departure Warning safety component shall ensure the frequency of the 'LDW_Torque_Reques' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Frequency.'	C	50 ms	LDW Safety	Lane Departure Warning torque to zero.

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

In Table 7, "Validation" refers to the process choosing the appropriate parameters. "Verification" involves testing to make sure the vehicle behaves as expected when the parameter value is crossed. Here the details are listed for the Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria.

Table 7 Verification and validation acceptance criteria.

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Technical Safety Requirement 01-01-01	To validate the Max_Torque_Amplitude is the chosen from the Lane Departure Warning Validation	To verify the Lane Departure Warning functionality is turned off.
Technical Safety Requirement 01-01-02	To validate if the 'TORQUE_LIMITER' sends the error_status_torque_limiter signal to the LDW_SAFETY_ACTIVATION.	To verify the Car Display ECU displays the Lane Departure Warning malfunction warning signal.
Technical	Validate if the	To verify the Final EPS Torque

Safety Requirement 01-01-03	'TORQUE_LIMITER' sends 'LDW_Torque_Request' with zero.	generator receives a LDW_Torque_Request of zero.
Technical Safety Requirement 01-01-04	To validate if the 'TORQUE_LIMITER' calculates and sends the correct cyclic redundancy check (CRC) and Alive counter for data transmission validity and integrity.	To verify if the functionality is turn off when there is a CRC or Alive counter discrepancy.
Technical Safety Requirement 01-01-05	To validate the Safety Startup Memory test to check memory faults catch memory faults.	To verify the Lane Departure Warning is turned off when the Safety Startup Memory fails.
Technical Safety Requirement 01-02-01	Validate the Max_Torque_Frequency set is the chosen from the Lane Departure Warning Acceptance Criteria.	To verify the functionality is turned off if the 'LDW_Torque_Request' frequency exceeds 01-02-01 chosen from the Lane Departure Warning Acceptance Criteria. Max_Torque_Request.

The Lane Keeping Assistance (LKA) Requirements is in Table 8 and the associated technical safety requirements from functional safety is in Table 9 (derived in the functional safety concept). Note that the ASIL and Fault Tolerant Time Interval are different as well.

Table 8 Functional Safety Requirement 02-1 with its associated system elements.

ID	**Functional Safety Requirement**	**Electronic Power Steering ECU**	**Camera ECU**	**Car Display ECU**
Functional	The lane keeping item shall	X		

Safety Requirement 02-01	ensure that the lane keeping assistance torque is applied for only Max_Duration			

Table 9 Technical Safety Requirements related to Functional Safety Requirement 02-01.

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01	The Lane Keeping Assistance safety component shall ensure the duration of the lane keeping assistance torque is applied for less than Max_Duration.	C	500 ms	LKA Safety	Lane Keeping Assistance torque to zero.
Technical Safety Requirement 02	When the Lane Keeping Assistance function deactivates, the 'LKA Safety' shall send a signal to the Car Display ECU to turn on a warning light.	C	500 ms	LKA Safety	Lane Keeping Assistance torque to zero.
Technical Safety Requirement 03	When a failure is detected, the Lane Keeping Assistance function shall deactivate and the 'LKA_Torque_Request' shall be zero.	C	500 ms	LKA Safety	Lane Keeping Assistance torque to zero.
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	C	500 ms	LKA Safety	Lane Keeping Assistance torque to zero.

Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any memory problems.	A	Ignition cycle	Data Transmission Integrity Check	Lane Departure Warning torque to zero.

Table 10 indicates the Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria.

Table 10 Verification and Validation Acceptance Criteria.

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Technical Safety Requirement 01-01-01	To validate the Max_Duration is set to the chosen value from LKA Validation Assistance Criteria	To verify the functionality is turned off after it is applied for Max_Duration.
Technical Safety Requirement 02-01-02	To Validate the 'TORQUE_LIMITER' sends the error_status_torque_limiter signal to the LKA_SAFETY_ACTIVATION.	To verify the Car Display ECU displays the Lane Keeping Assistance malfunction warning signal.
Technical Safety Requirement 02-01-03	To validate the TORQUE_LIMITER' sends 'LKA_Torque_Request' with zero.	To verify the Final EPS Torque generator receives a LKA_Torque_Request of zero.
Technical Safety Requirement 02-01-04	To validate the 'TORQUE_LIMITER' calculate and sends the correct cyclic redundancy check (CRC) and Alive counter for data transmission validity and integrity.	To verify the functionality is turn off if there is a CRC or Alive counter discrepancy.

Technical Safety Requirement 02-01-05	To validate the Safety Startup Memory test to check memory faults catch memory faults.	To verify the Lane Keeping Assistance is turned off when the Safety Startup Memory fails.

Refinement of the System Architecture

The following figure include the system architecture from the end of the technical safety lesson, including all of the ASIL labels.

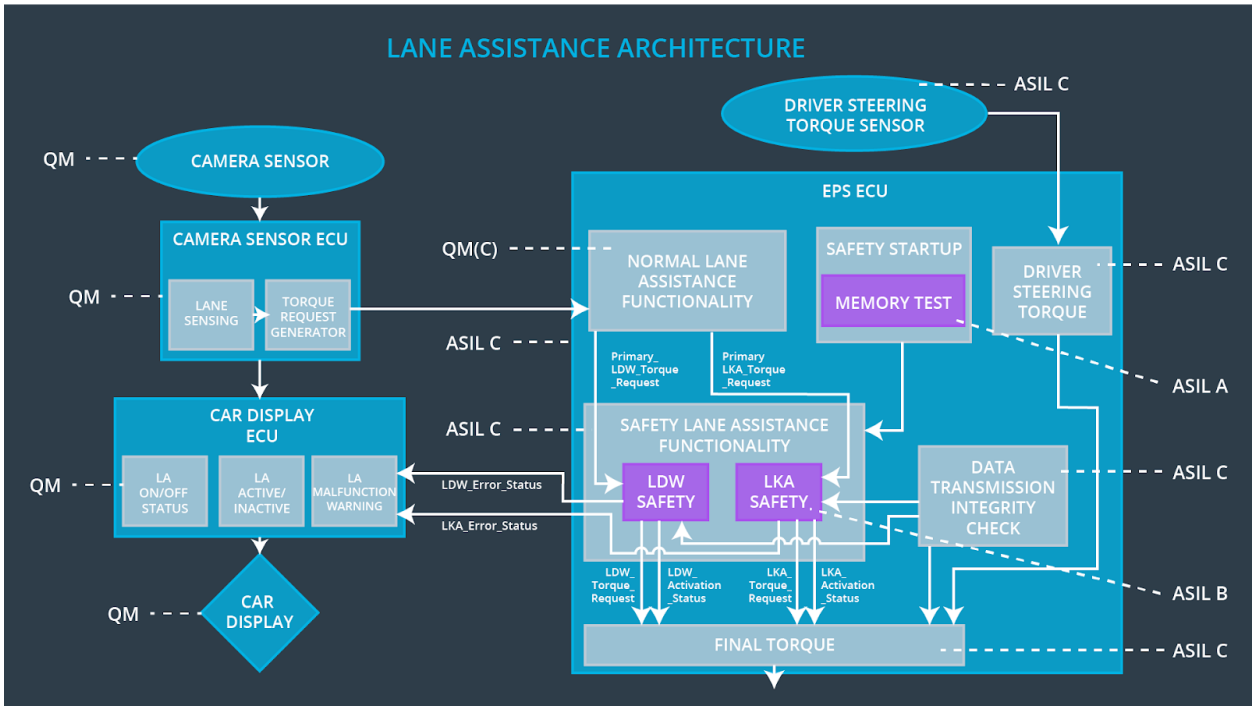

Fig. 3 Refined system architecture.

Allocation of Technical Safety Requirements to Architecture Elements

All technical safety requirements are allocated to the Electronic Power Steering ECU. Please see Table 11 for more details.

Table 11 Allocation of technical safety requirement..

ID	Technical Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Technical Safety Requirement 01-01-01	The Lane Departure Warning 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.’	**X**		
Technical Safety Requirement 01-01-02	When the Lane Departure Warning is deactivated, the ‘LDW Safety’ software module shall send a signal to the Car Display ECU to turn on a warning signal.	**X**		
Technical Safety Requirement 01-01-03	When a failure is detected by the Lane Departure Warning functionality, it shall deactivate the Lane Departure Warning feature and set ‘LDW_Torque_Request’ to zero.	**X**		
Technical Safety Requirement 01-01-04	The validity and integrity of the data transmission for ‘LDW_Torque_Request’ signal shall be ensured.	**X**		
Technical Safety Requirement 01-01-05	Memory test shall be conducted at start up of the EPS ECU to check for any memory problems	**X**		

Technical Safety Requirement 01-02-01	The Lane Departure Warning safety component shall ensure the frequency of the ‘LDW_Torque_Reques’ sent to the ‘Final electronic power steering Torque’ component is below ‘Max_Torque_Frequency.’	**X**		
Technical Safety Requirement 02-01-01	The Lane Keeping Assistance safety component shall ensure the duration of the lane keeping assistance torque is applied for less than Max_Duration	**X**		
Technical Safety Requirement 02-01-02	When the Lane Keeping Assistance function deactivates, the ‘LKA Safety’ shall send a signal to the Car Display ECU to turn on a warning light.	**X**		
Technical Safety Requirement 02-01-03	When a failure is detected, the Lane Keeping Assistance function shall deactivate and the ‘LKA_Torque_Request’ shall be zero.	**X**		
Technical Safety Requirement 02-01-04	The validity and integrity of the data transmission for ‘LKA_Torque_Request’ signal shall be ensured.	**X**		
Technical Safety Requirement 02-01-05	Memory test shall be conducted at start up of the EPS ECU to check for any memory problems			

Warning and Degradation Concept

The warning and degradation concept is the same for the technical safety requirements as for the functional safety requirements, seen in Table 12.

Table 12 Allocation of technical safety requirement.

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off Lane Departure Warning functionality	Malfunction_01, Malfunction_02, Malfunction_04	Yes	Lane Departure Warning Malfunction Warning on Car Display
WDC-02	Turn off Lane Keeping Assistance functionality	Malfunction_03, Malfunction_05	Yes	Lane Keeping Assistance Malfunction Warning on Car Display