



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
06/08/2018	1.0	Banning Lyth	First edits

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]

[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

[Instructions: Answer what is the purpose of a technical safety concept?]

This document provides a system-level approach to the item. The functional safety requirements are refined as technical safety requirements. Functions are assigned to sub-level systems to conform to ISO 26262

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	A S I L	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_Amplitude.	C	50 ms	Vibration torque amplitude below Max_Torque_Amplitude.
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	C	50 ms	Vibration torque amplitude below Max_Torque_Frequency.
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the Lane Keeping Assistance torque is applied only Max_Assist_Time	B	500 ms	Assistance time is below Max_Assist_Time

Refined System Architecture from Functional Safety Concept

[Instructions: Provide the refined system architecture from the functional safety concept]

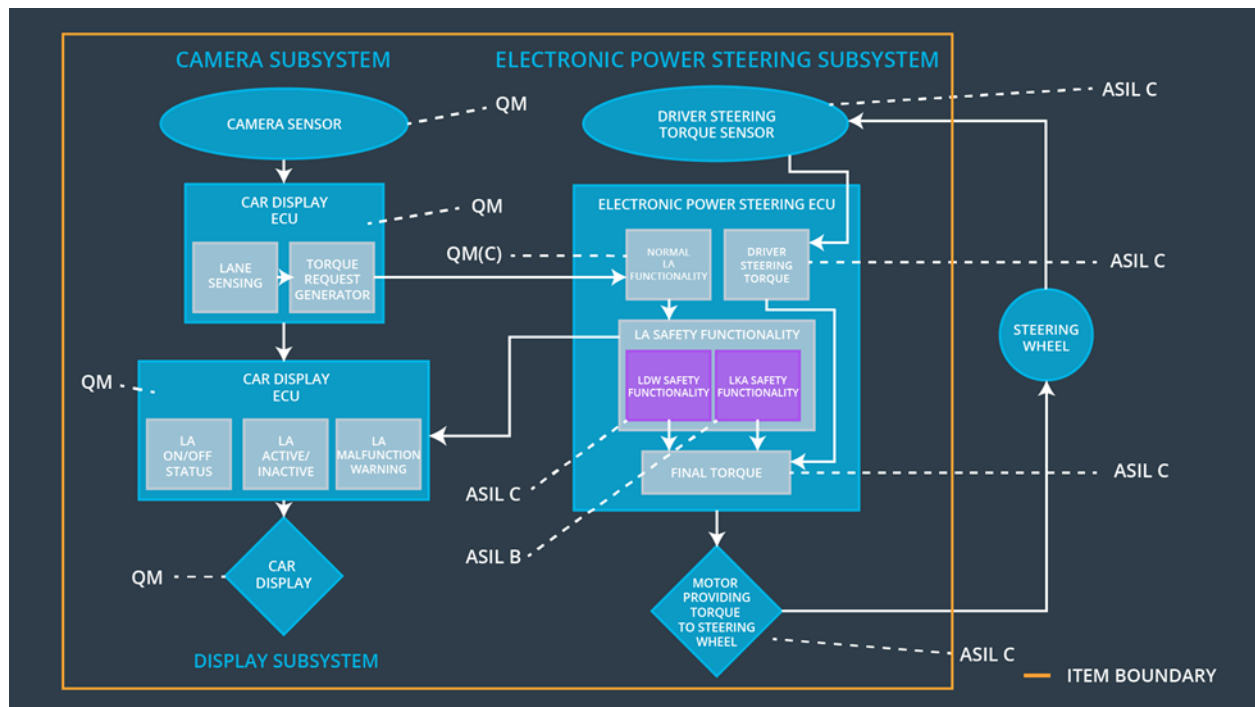


Image taken from Udacity lesson material

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	Capture images and send them to the Camera Sensor ECU
Camera Sensor ECU - Lane Sensing	Process Images to detect lane lines and calculate vehicle position with respect to the lane lines
Camera Sensor ECU - Torque request generator	Calculate the torque required to maintain vehicle in the lane
Car Display	Display the Lane Departure Warning and status of the Lane Assistance System

Car Display ECU - Lane Assistance On/Off Status	Identify the status of the Lane Assistance System (ON/OFF)
Car Display ECU - Lane Assistant Active/Inactive	Identify the status of the Lane Assistance System (Active/Inactive)
Car Display ECU - Lane Assistance malfunction warning	Identify Lane Assistance Malfunction
Driver Steering Torque Sensor	Measure the torque applied to the steering wheel by the driver
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Software module receiving the driver's torque request from the steering wheel
EPS ECU - Normal Lane Assistance Functionality	Software module receiving data from the Camera Sensor ECU torque request
EPS ECU - Lane Departure Warning Safety Functionality	Software module ensuring the torque amplitude is below Max_Torque_Amplitude and torque frequency is below Max_Torque_Frequency
EPS ECU - Lane Keeping Assistant Safety Functionality	Software module ensuring the Lane Keeping Assistance functionality application is not activate more than Max_Assist_Time time
EPS ECU - Final Torque	Combine the torque request from the Lane Keeping and Lane Departure Warning functionalities and sends them to the Motor
Motor	Applies the specified 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 01-01-01	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	Lane Departure Warning Torque Request Amplitude shall be set to zero.
Technical Safety Requirement 01-01-02	When the LDW 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 Request Amplitude shall be set to zero.
Technical Safety Requirement 01-01-03	When a failure is detected by the Lane Departure Warning functionality, it shall	C	50 ms	LDW Safety	Lane Departure Warning Torque

	deactivate the Lane Departure Warning feature and set 'LDW_Torque_Request' to zero.				Request Amplitude shall be set 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	Lane Departure Warning Torque Request Amplitude shall be set to zero.
Technical Safety Requirement 01-01-05	Memory test shall be conducted at startup of the EPS ECU to check for any memory problems	A	Ignition cycle	Memory Test	Lane Departure Warning Torque Request Amplitude shall be 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 01-01-01	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_Frequency.'	C	50 ms	LDW Safety	Lane Departure Warning Torque Request Frequency shall be set to zero.
Technical Safety Requirement 01-01-02	When the LDW 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 Request Frequency shall be set to zero.
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.	C	50 ms	LDW Safety	Lane Departure Warning Torque Request frequency shall be set 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	Lane Departure Warning Torque Request Frequency shall be set to zero.
Technical Safety Requirement 01-01-05	Memory test shall be conducted at startup of the EPS ECU to check	A	Ignition cycle	Memory Test	Lane Departure Warning Torque

	for any memory problems				Request Frequency shall be 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.]

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 02-01-01	The Lane Keeping Assistance safety component shall ensure the duration of the lane keeping	B	500 ms	LKA Safety	Lane Keeping Assistance Torque

	assistance torque is applied for less than Max_Duration				shall be set to zero.
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.	B	500 ms	LKA Safety	Lane Keeping Assistance Torque shall be set to zero.
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.	B	500 ms	LKA Safety	Lane Keeping Assistance Torque shall 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	Lane Keeping Assistance Torque shall be set to zero.
Technical Safety Requirement 02-01-05	Memory test shall be conducted at startup of the EPS ECU to check for any memory problems	A	Ignition cycle	Memory Test	Lane Keeping Assistance Torque shall be 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.]

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.]

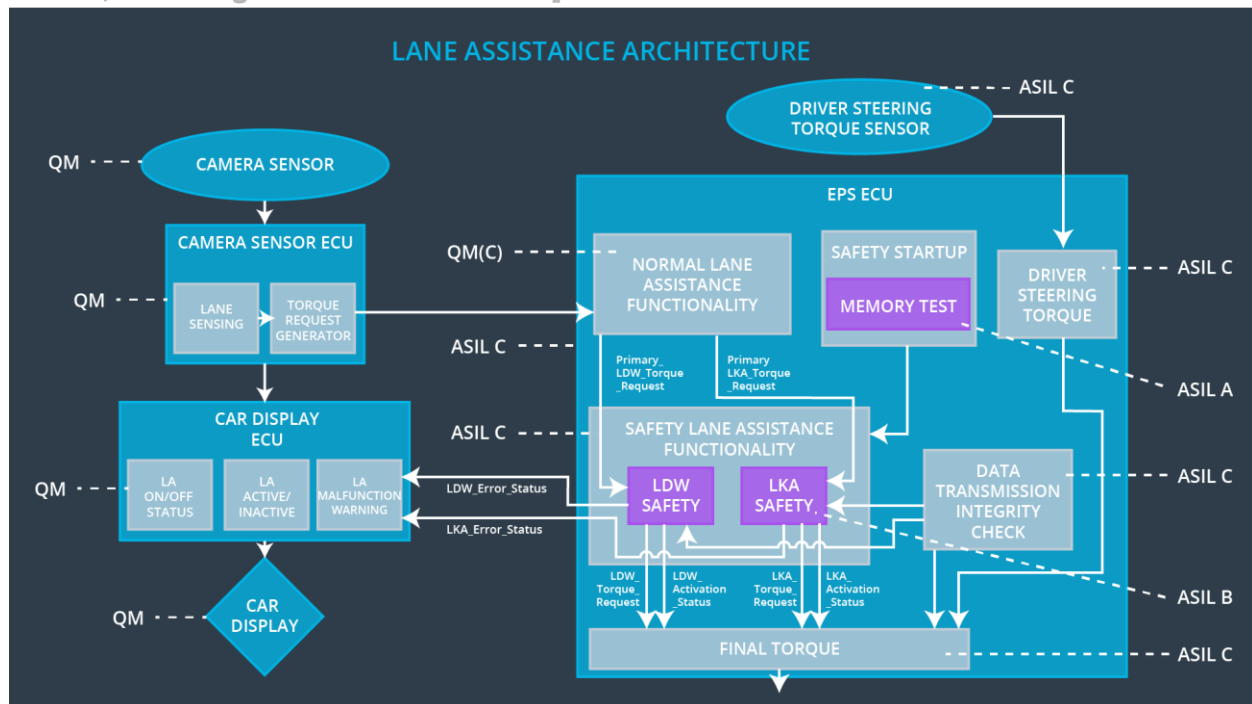


Image taken from Udacity lesson material

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]

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	When the Lane Departure Warning is deactivated, the	X		

01-01-02	'LDW Safety' software module shall send a signal to the Car Display ECU to turn on a warning signal.			
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 startup 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	X		

	'LKA_Torque_Request' shall be zero.			
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	X		

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 Lane Departure Warning functionality	Malfunction_01, Malfunction_02, Malfunction_05	Yes	Lane Departure Warning Malfunction Warning on Car Display
WDC-02	Turn off Lane Keeping Assistance functionality	Malfunction_03, Malfunction_04	Yes	Lane Keeping Assistance Malfunction Warning on Car Display