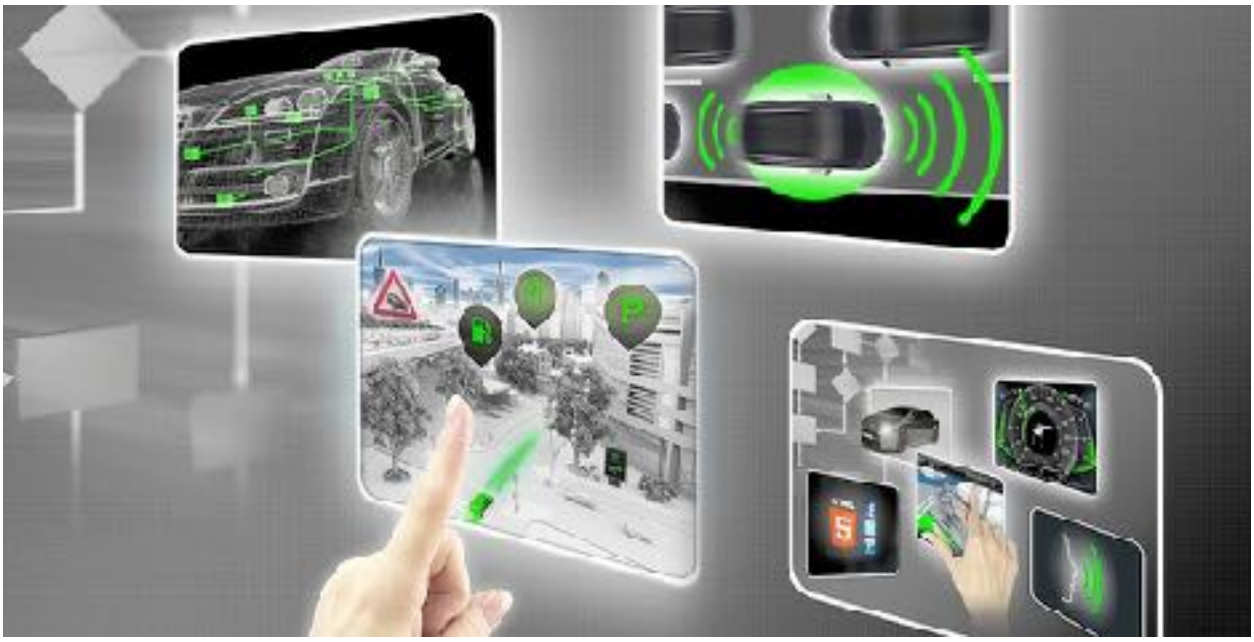
Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21



Document history

Date	Version	Editor	Description
2/24/2018	1.0	Huaping Gu	Original submission
3/4/2018	2.0	Huaping Gu	Add more materials leant from lesson

Table of Contents

Purpose of the Technical Safety Concept

This technical safety concept is part of the product development phase which is more concrete and gets into the details of the item's technology. The technical safety concept defines how the subsystems interact at the message level and describes how the ECUs communicate with each other.

Inputs to the Technical Safety Concept

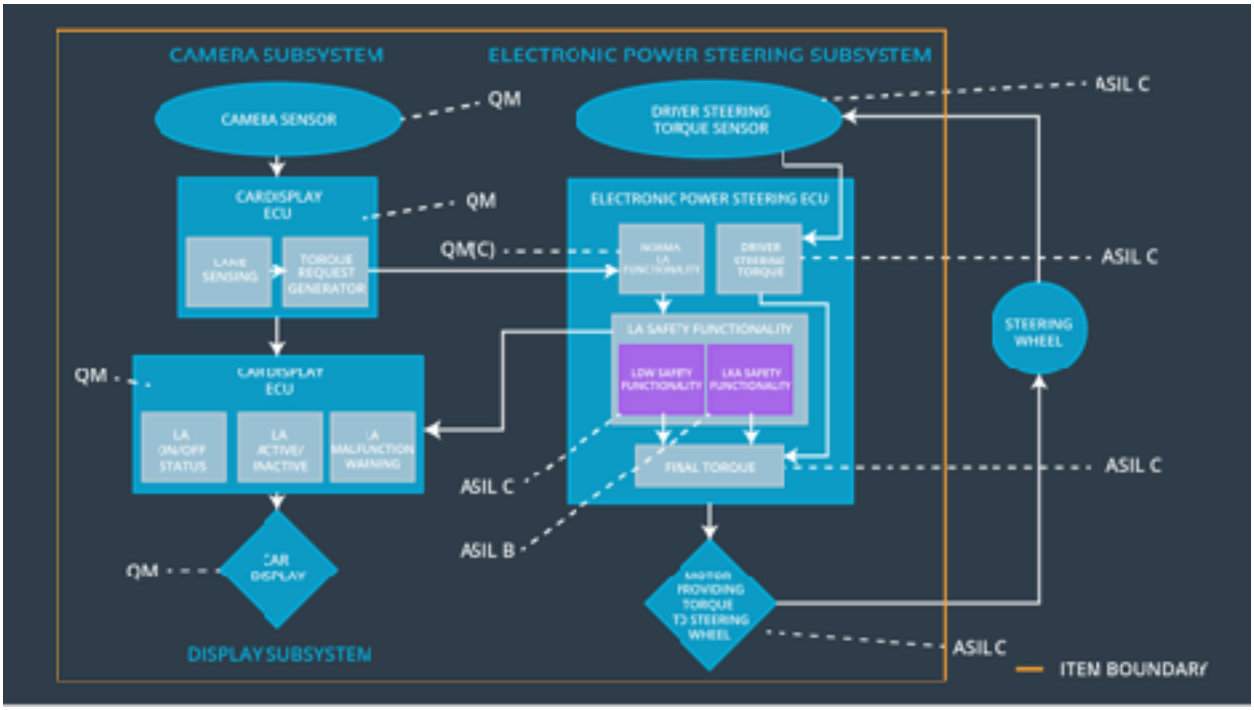
Functional Safety Requirements

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	The oscillating steering torque from the lane departure warning function shall ensure that the lane departure oscillating torque amplitude is bellow Max_Torque_**Amplitude**.	C	50ms	Torque amplitude is bellow Max_Torque_**Amplitude**.
Functional Safety Requirement 01-02	The oscillating steering torque from the lane departure warning function shall ensure that the lane departure oscillating torque frequency is bellow Max_Torque_**Frequency**.	C	50ms	Torque frequency is bellow Max_Torque_**Frequency**.
Functional Safety Requirement 02-01	The LKA shall ensure that the Lane Keeping Assistance torque is applied within Max_Duration.	B	50ms	The lane keeping assistance function is limited in time duration which prevents misuse as an autonomous driving function.
Functional Safety Requirement 03-01	The LKA shall automatically OFF when the camera ECU work incorrectly	A	50ms	LKA automatically OFF when it detects the camera ECU is not work.
Functional Safety Requirement 04-01	The LKA shall automatically OFF when the car is parked off road.	QM	500ms (Since vehicle is parked, no need to be shorter interval)	LKA automatically OFF when the car is parked off road.

Note: Because template and knowledge wise, Functional Safety Req 03-01 and 04-01 are similar to first 3, and also to align with the next

“SoftwareRequirementsAndArchitecture_LaneAssistance” document, here will only explain and expand the first 3 Functional Safety Requirements, aka 01-01, 01-02 and 02-01.

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	The component which can capture images of the road and around, then feed to the Camera Sensor ECU.
Camera Sensor ECU - Lane Sensing	Module which can do the lane line and vehicle position detection based on the Camera sensor’s image feeding.

Camera Sensor ECU - Torque request generator	Module which use some algorithms to generate the torque which can be used to send to the Electronic Power Steering ECU.
Car Display	Display screen which can be used to show messages/warnings to driver.
Car Display ECU - Lane Assistance On/ Off Status	One component of the Car Display ECU, which can tell Lane Assistance is On or Off
Car Display ECU - Lane Assistant Active/Inactive	One component of the Car Display EDU, which can tell Lane Assistant function is Active or Inactive.
Car Display ECU - Lane Assistance malfunction warning	One component of the Car Display EDU, which can display the Lane Assistance malfunction warnings.
Driver Steering Torque Sensor	The component which can measure the torque which is applied to the wheel by the driver
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Module which can receive the torque which is applied by the driver on the wheel.
EPS ECU - Normal Lane Assistance Functionality	Module receiving and fuse signals from Camera Sensor ECUTorque requesting.
EPS ECU - Lane Departure Warning Safety Functionality	The module ensuring the torque amplitude and frequency is within expected range.
EPS ECU - Lane Keeping Assistant Safety Functionality	The module ensuring the lane assistant duration is within expected range.
EPS ECU - Final Torque	Combine both the signals from the lane Departure Warning and Lane Keeping functionalities and feed to the Motor
Motor	The mechanic component which can generate and apply torque to the steering wheels based on signal from the EPS ECU’s final Torque.

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	50ms	LDW safety	Deactivate the LDW feature and the “LWD_Torque_Request” shall be set to zero.
Technical Safety Requirement 01-01-02	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	LDW safety	N/A
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	50ms	LDW safety	Deactivate the LDW feature and the “LWD_Torque_Request” 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	50ms	Data Transmission Integrity Check	Deactivate the LDW feature and the “LWD_Torque_Request” shall be set 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	Deactivate the LDW feature and the “LWD_Torque_Request” 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 01-02-01	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	50ms	LDW safety	Deactivate the LDW feature and the “LWD_Torque_Request” shall be set 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	50ms	LDW safety	N/A
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	50ms	LDW safety	Deactivate the LDW feature and the “LWD_Torque_Request” shall be set 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	50ms	Data Transmission Integrity Check	Deactivate the LDW feature and the “LWD_Torque_Request” shall be set 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	Deactivate the LDW feature and the “LWD_Torque_Request” 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.]

Intentionally skip here.

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:

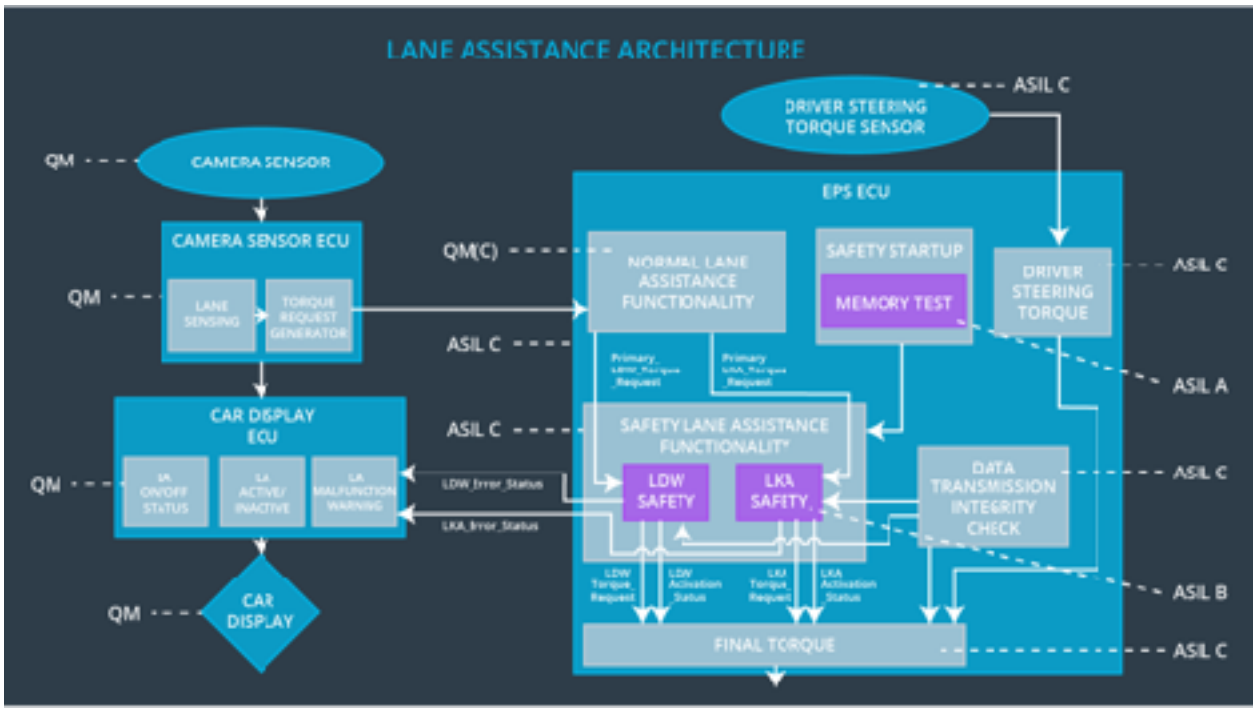
ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 02-01-01	The **LKA** safety component shall ensure that the lane keeping assistance **duration** of the 'LKA_Torque_Request' sent to the 'Final electronic power steering Torque' component is below ‘Max_Duration’	B	50ms	LKA safety	Deactivate the LKA feature and the “LKA_Torque_Request” shall be set 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	50ms	LKA safety	N/A
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	50ms	LKA safety	Deactivate the LKA feature and the “LKA_Torque_Request” 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	50ms	Data Transmission Integrity Check	Deactivate the LKA feature and the “LKA_Torque_Request” shall be set 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	Deactivate the LKA feature and the “LKA_Torque_Request” 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.]
Intentionally skip here.

Refinement of the System Architecture

Bellow is the refined System Architecture diagram withe technical safety components.



Allocation of Technical Safety Requirements to Architecture Elements

We already included the allocation as part of the technical requirement tables, all technical safety requirements except the MEMORY TEST, are allocated to the **Electronic Power Steering ECU**.

Warning and Degradation Concept

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.

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Lane Departure warning function will be OFF	Malfunction_01	Yes	Warning message of the lane Departure will be shown on the Vehicle Display screen
WDC-02	Lane keeping assistance function will be OFF	Malfunction_02 Malfunction_03 Malfunction_04	Yes	Warning message of the lane keeping assistance will be shown on the Vehicle Display screen