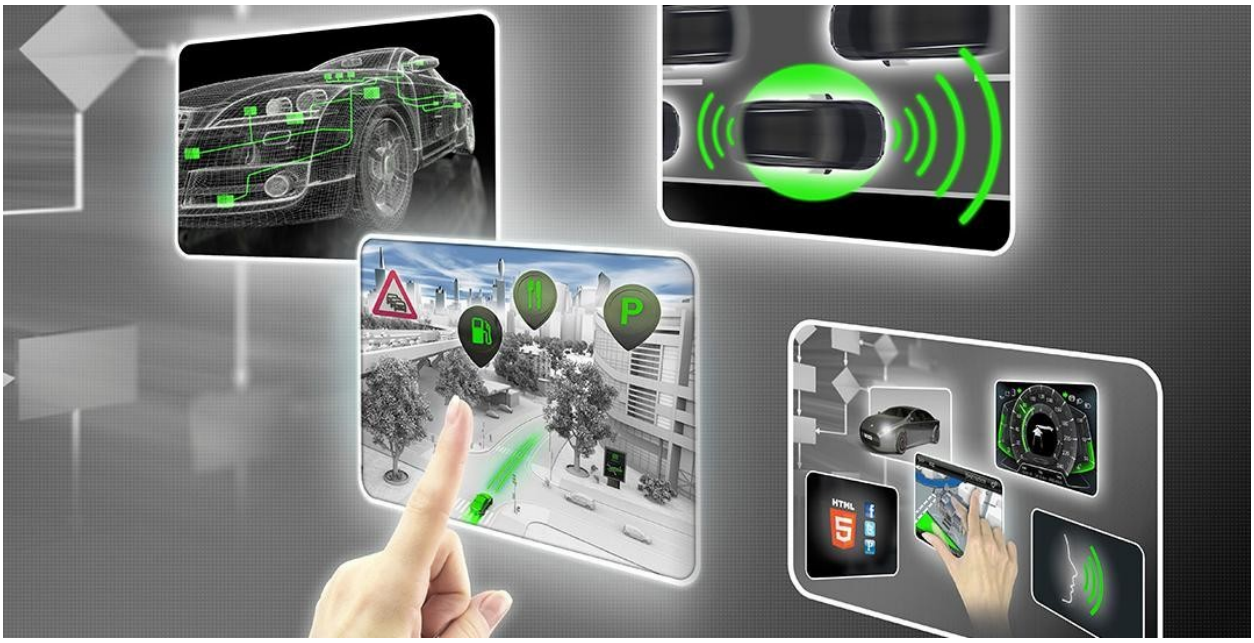
Elektrobit

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
25/12/2018	1.0	Ahmed Desoky	Technical Safety Concept for Lane Assistance system
26/12/2018	1.1	Ahmed Desoky	Fixing the safe state

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

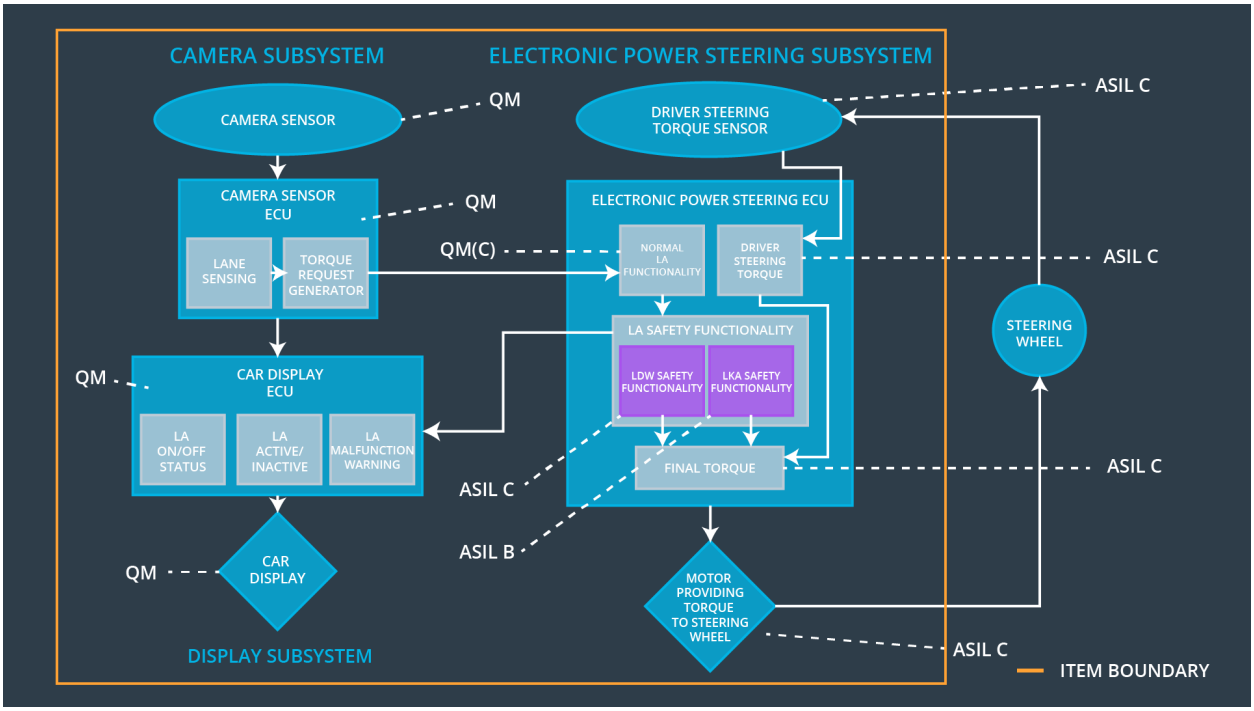
In this document, the function safety requirements set in the functional safety concept are set with more details. Here, requirements are more concrete and more detials for assigning each requirments to the system architecture as specified by ISO 26262.

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 departure warning (LDW) shall ensure that lane departure oscillating torque is below Max_Torque_Amplitude.	C	50 ms	Vibration torque amplitude below Max_Torque_Amplitude
Functional Safety Requirement 01-02	The lane departure warning (LDW) shall ensure that lane departure oscillating frequency is below Max_Torque_Frequency.	C	50 ms	Vibration torque amplitude below Max_Torque_Amplitude
Functional Safety Requirement 01-03	The lane departure warning (LDW) shall stop when the camera sensor stops working	C	10 ms	LDW function is deactivated
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that lane keeping assist (LKA) troque is applied for just Max_Duration	B	500 ms	Funcition is deactivated
Functional Safety Requirement 02-02	The lane keeping assist (LKA) shall stop when the camera sensor stops working	C	10 ms	Lane keeping assistance torque = zero

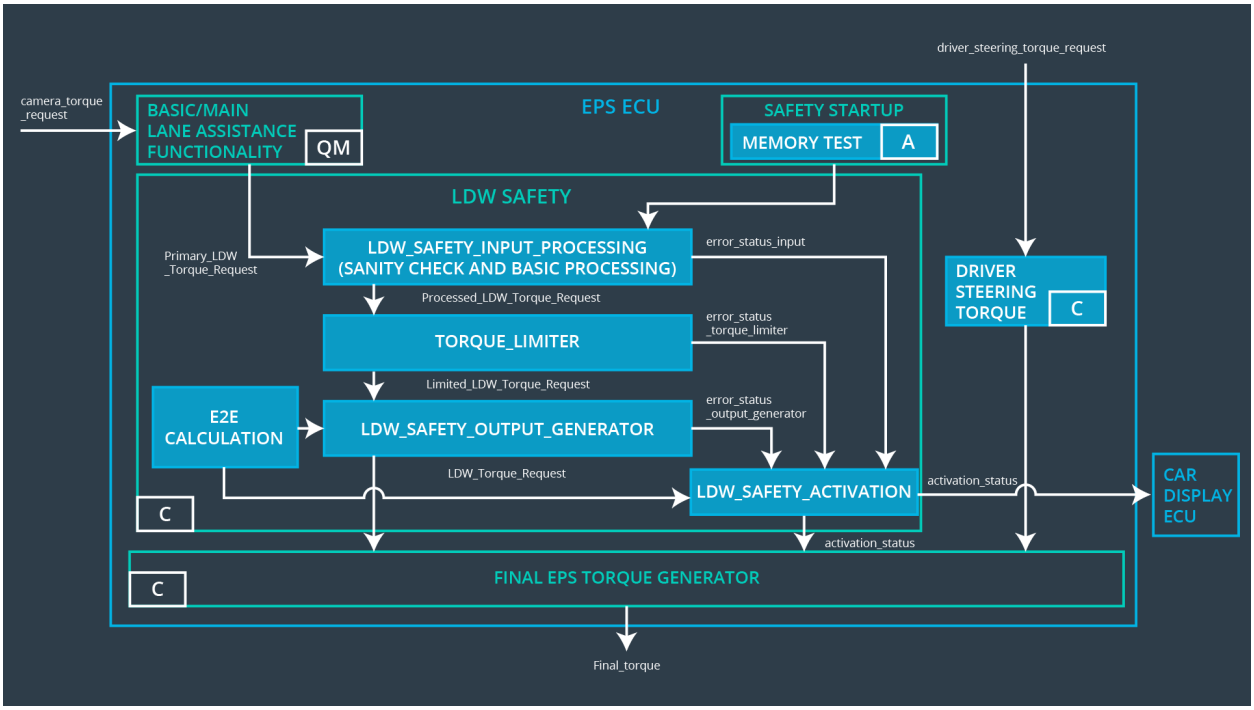
Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Captures images and provides them to the camera ECU
Camera Sensor ECU - Lane Sensing	Software unit that processes the camera images to detect the position of lane lines
Camera Sensor ECU - Torque request generator	Software unit that requests a defninte amout of torque to be applied based on the current drift of the ego vehicle
Car Display	Provides indicators for the driver to reflect the status of some systems
Car Display ECU - Lane Assistance On/Off Status	Provides indicators for lane assistance status (on/off)
Car Display ECU - Lane Assistant Active/Inactive	Provides indicators for lane assistance status (Active/Inactive)
Car Display ECU - Lane Assistance malfunction warning	Provides indicators for malfunctions in lane assistance systems
Driver Steering Torque Sensor	**Measures the toque applied to the steering wheel by the driver**
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Software module that receives the drivers steering from the steering sensor
EPS ECU - Normal Lane Assistance Functionality	Software modules that receives a torque request from the camera sub-system
EPS ECU - Lane Departure Warning Safety Functionality	Software module that ensures that the steering torque amplitude < Max_Torque_Amplitude. And steering troque frequency < Max_Torque_Frerquency
EPS ECU - Lane Keeping Assistant Safety Functionality	Software module that ensures that the steering torque duration < Max_Duration.
EPS ECU - Final Torque	Software modules that calculates the final torque to be sent to the motor
Motor	Applies the torque sent from the electrnic power steering ECU. This is the actuator

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 departure warning (LDW) shall ensure that lane departure oscillating torque 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 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	LDW torque = zero
Technical Safety Requirement 01-01-02	When the LDW is deactivated, the LDW safety SW module shall send a signal the car display ECU to activate the warning indicator	C	50 ms	LDW Safety	LDW torque = zero
Technical Safety Requirement 01-01-03	When a failure is detected by the LDW functionality, it shall deactivate the LDW feature by setting the “LDW_Torque_Request” by zero	C	50 ms	LDW Safety	LDW torque = zero
Technical Safety Requirement 01-01-04	The validity and integrity of data sent for “LDW_Torque_Request” shall be ensured	C	50 ms	LDW Safety	LDW torque = zero
Technical Safety Requirement 01-01-05	Memory test shall be done upon start-up of the EPS ECU to check any memory faults	C	Ignition cycle	Safety Startup	LDW function is deactivated

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 departure warning (LDW) shall ensure that lane departure oscillating 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 lane departure warning 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	LDW torque = 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:

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 electronic power steering ECU shall ensure that lane keeping assist (LKA) troque is applied for just Max_Duration	X		

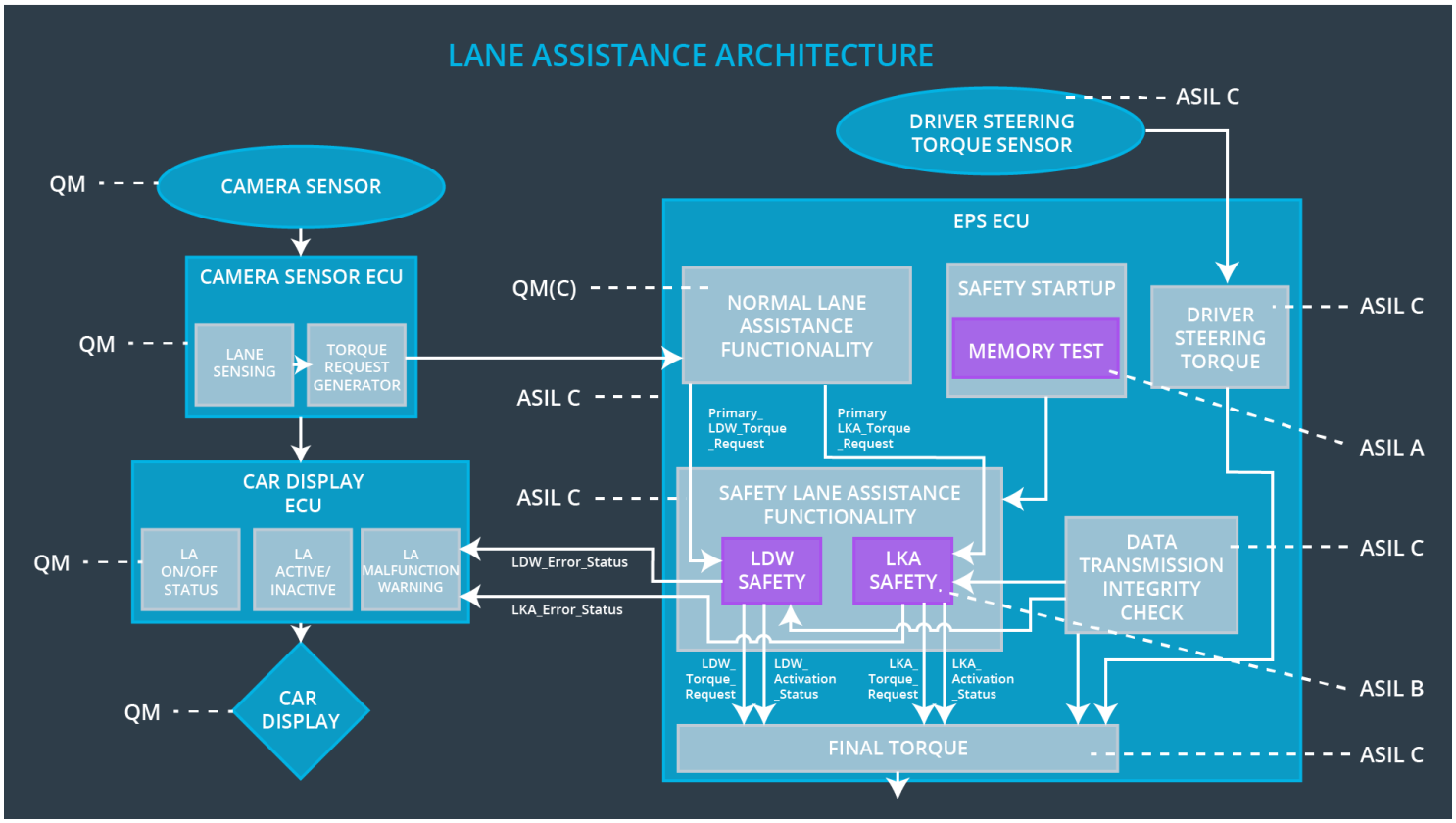
Technical Safety Requirements related to Functional Safety Requirement 02-01 are:

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 that the duration of the lane keeping assist torque applied is < Max_Duration	C	500 ms	LKA Safety	Lane keeping assistance torque = zero
Technical Safety Requirement 02-01-02	When the LKA is deactivated, the LKA safety SW module shall send a signal the car display ECU to activate the warning indicator	C	500 ms	LKA Safety	Lane keeping assistance torque = zero
Technical Safety Requirement 02-01-03	When a failure is detected by the LKA functionality, it shall deactivate the LKA feature by setting the “LKA_Torque_Request” by zero		500 ms	LKA Safety	Lane keeping assistance torque = zero
Technical Safety Requirement 02-01-04	The validity and integrity of data sent for “LKA_Torque_Request” shall be ensured	C	500 ms	LKA Safety	Lane keeping assistance torque = zero
Technical Safety Requirement 02-01-05	Memory test shall be done upon start-up of the EPS ECU to check any memory faults	C	Ignition Cycle	Safety Startup	LKA function is deactivated

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



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 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 LDW is deactivated, the LDW safety SW module shall send a signal the car display ECU to activate the warning indicator	**X**		
Technical Safety Requirement 01-01-03	When a failure is detected by the LDW functionality, it shall deactivate the LDW feature by setting the “LDW_Torque_Request” by zero	**x**		
Technical Safety Requirement 01-01-04	The validity and integrity of data sent for “LDW_Torque_Request” shall be ensured	**X**		
Technical Safety Requirement 01-01-05	Memory test shall be done upon start-up of the EPS ECU to check any memory faults	**x**		
Technical Safety Requirement 01-02-01	The lane departure warning 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	**X**		
Technical Safety Requirement 02-01-01	The lane keeping assistance safety component shall ensure that the duration of the lane keeping assist torque applied is < Max_Duration	**X**		

Technical Safety Requirement 02-01-02	When the LKA is deactivated, the LKA safety SW module shall send a signal the car display ECU to activate the warning indicator	**X**		
Technical Safety Requirement 02-01-03	When a failure is detected by the LKA functionality, it shall deactivate the LKA feature by setting the “LKA_Torque_Request” by zero	**X**		
Technical Safety Requirement 02-01-04	The validity and integrity of data sent for “LKA_Torque_Request” shall be ensured	**X**		
Technical Safety Requirement 02-01-05	Memory test shall be done upon start-up of the EPS ECU to check any memory faults	**X**		

Warning and Degradation Concept

ID	**Degradation Mode**	**Trigger for Degradation Mode**	**Safe State invoked?**	**Driver Warning**
WDC-01	Turn off the LDW	Malfunction_01, Malfunction_02, Malfunction_04	Yes	Warning indicator on the dashboard for malfunction
WDC-02	Turn off the LKA	Malfunction_03, Malfunction_05	Yes	Warning indicator on the dashboard for malfunction