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
23/May/2018	1.0	Shreya Srivastava	First Draft

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

1. Purpose of the Technical Safety Concept

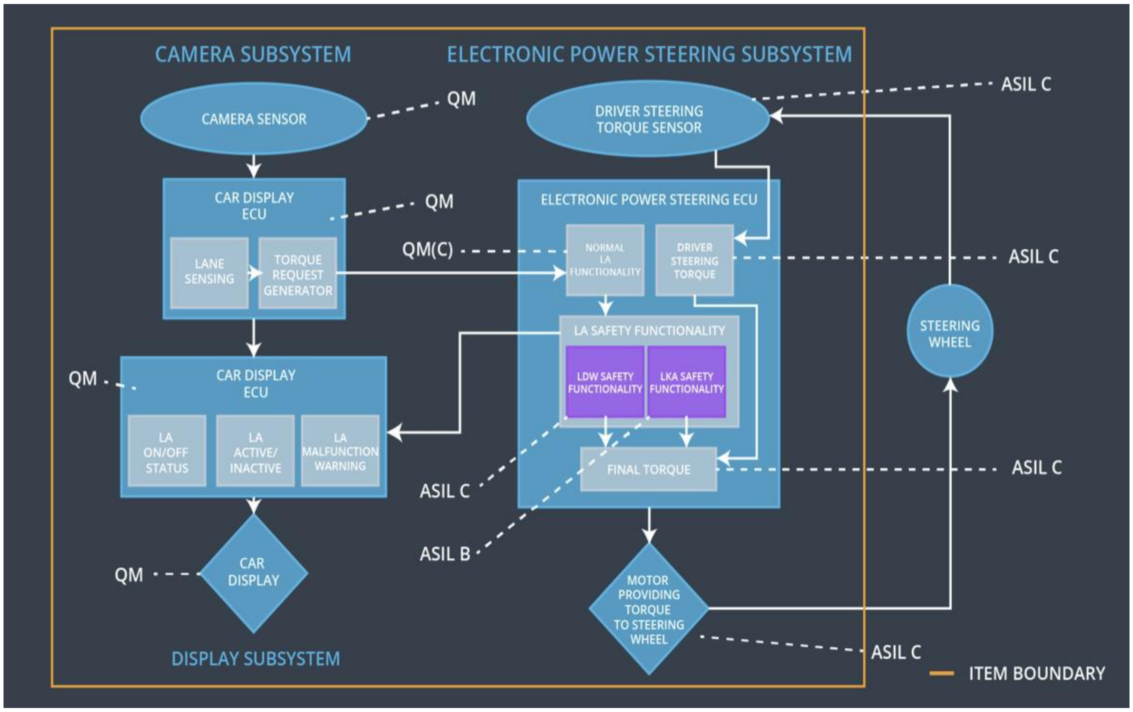
The purpose of the Technical safety concept is to get into the more concrete details of the items technology. The technical safety concept comes under the production phase of the safety lifecycle. It looks into the hardware and the software components in a grater detail.

2. Inputs to the Technical Safety Concept

2.1 Functional Safety Requirements

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	The lane keeping system shall ensure that the lane departure oscillating torque amplitude is below the Max_Torque_Amplitude.	C	50 ms	Vibration torque amplitude below Max_Torque_Amplitude.
Functional Safety Requirement 01-02	The lane Keeping shall ensure that the lane departure oscillating torque frequency is below the Max_Torque_Frquency.	C	50 ms	Vibration frequency is below Max_Torque_Frequency.
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

2.2 Refined System Architecture from Functional Safety Concept



Lane Assistance System Architecture

Functional overview of architecture elements

Element	Description
Camera Sensor	Capture the images of the lane and provide it to the Camera sensor ECU
Camera Sensor ECU - Lane Sensing	Sense the lane lines on the road calculate the position of the vehicle w.r.t the lanes
Camera Sensor ECU - Torque request generator	Generate the torque request for the Electronic Power system
Car Display	Display the warnings of the Lane departure and the lane keeping system
Car Display ECU - Lane Assistance On/Off Status	Display if the lane assistance system is on or off.
Car Display ECU - Lane Assistant Active/Inactive	Display if the lane assistance system is in active or inactive state if the system is switched on.

Car Display ECU - Lane Assistance malfunction warning	Displays a warning that some malfunction has occurred in the lane assistance system.
Driver Steering Torque Sensor	Sense the steering torque applied
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Calculate the steering torque applied by the driver
EPS ECU - Normal Lane Assistance Functionality	It takes input from Driver Steering Torque Sensor and camera ECU and passes it to the safety lane assistance functionality
EPS ECU - Lane Departure Warning Safety Functionality	Checks for any malfunction in the Lane Departure Warning function and take appropriate action. (deactivate if there is malfunction, pass the output torque to the final torque is there isn't any malfunction)
EPS ECU - Lane Keeping Assistant Safety Functionality	Checks for any malfunction in the Lane Keeping Assistance function and take appropriate action. (deactivate if there is malfunction, pass the output torque to the final torque is there isn't any malfunction)
EPS ECU - Final Torque	Combine the inputs from LDW and LKA and deliver the final torque request to the motor
Motor	The Motor is actuated by the input from Electronic Power Steering ECU. It applies the requisite torque to the steering wheel

3. Technical Safety Concept

3.1 Technical Safety Requirements

3.1.1 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	The LDW safety component shall ensure the 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	The lane departure warning torque request amplitude shall be set to zero.
Technical Safety Requirement 02	The validity and the integrity of the data transmission for “LDW_Torque_Request” shall be ensured.	C	50 ms	LDW Safety	The lane departure warning torque request amplitude shall be set to zero.
Technical Safety Requirement 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	50 ms	LDW Safety	The lane departure warning torque request amplitude shall be set to zero.
Technical	As soon as the LDW	C	50 ms	LDW Safety	The lane departure

Safety Requirement 04	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.				warning torque request amplitude shall be set to zero.
Technical Safety Requirement 05	Memory test shall be conducted at the start of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Data Transmission Integrity check	The lane departure warning torque request amplitude shall be set to zero.

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	The LDW safety component shall ensure the component shall ensure that the frequency of the	C	50 ms	LDW Safety	The lane departure warning torque request amplitude

	LDW_Torque_Request sent to the ‘Final electronic power steering torque’ component is below “Max_Torque_Frequency				shall be set to zero.
Technical Safety Requirement 02	The validity and the integrity of the data transmission for “LDW_Torque_Request” shall be ensured.	C	50 ms	LDW Safety	The lane departure warning torque request amplitude shall be set to zero.
Technical Safety Requirement 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	50 ms	LDW Safety	The lane departure warning torque request amplitude shall be set to zero.
Technical Safety Requirement 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	The lane departure warning torque request amplitude shall be set to zero.
Technical Safety Requirement 05	Memory test shall be conducted at the start of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Data Transmission Integrity check	The lane departure warning torque request amplitude 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.]

3.1.2 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:

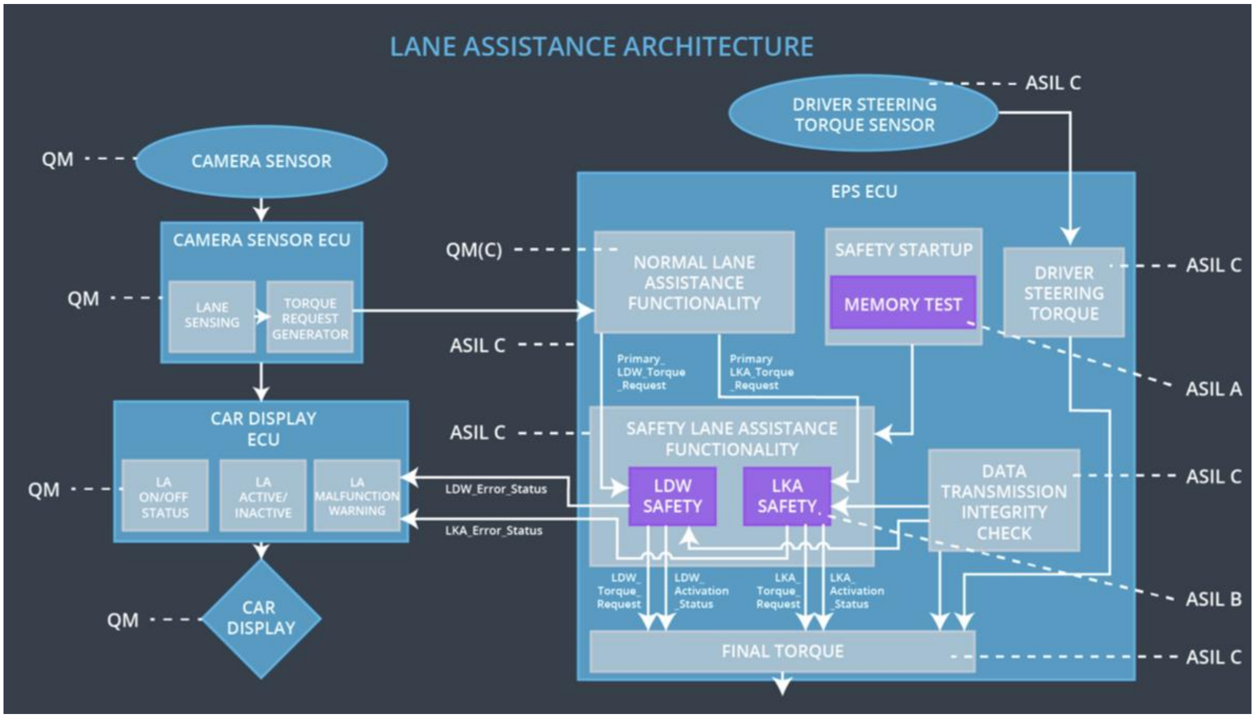
ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01	The LKA safety component shall ensure that the Duration of LKA Torque application is less than Max_Duration.	B	500 ms	LKA Safety	LKA feature and the LKA_Torque_Request' shall be set to zero

Technical Safety Requirement 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	500 ms	LKA Safety	LKA feature and the LKA_Torque_Request' shall be set to zero
Technical Safety Requirement 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	LKA feature and the LKA_Torque_Request' shall be set to zero
Technical Safety Requirement 04	The validity and integrity of the data transmission for LKA_Torque_Request' signal shall be ensured.	B	500 ms	LKA Safety	LKA feature and the LKA_Torque_Request' shall be set to zero
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition Cycle	Data Transmission Integrety Check	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.]

3.2 Refinement of the System Architecture



3.3 Allocation of Technical Safety Requirements to Architecture Elements

All the technical safety requirements are allocated to EPS ECU.

3.4 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	Yes	Lane Departure Warning Malfunction Warning on Car Display
WDC-02	Turn off Lane Keeping Assistance functionality	Malfunction_03	Yes	Lane Keeping Assistance Malfunction Warning on Car Display