Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 1.0

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
3/21/18	1.0	David G	First draft

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]

Purpose of the Technical Safety Concept

A technical safety concept is a concrete evaluation of a system’s technology and specific technical safety requirements for that system. It also involves:

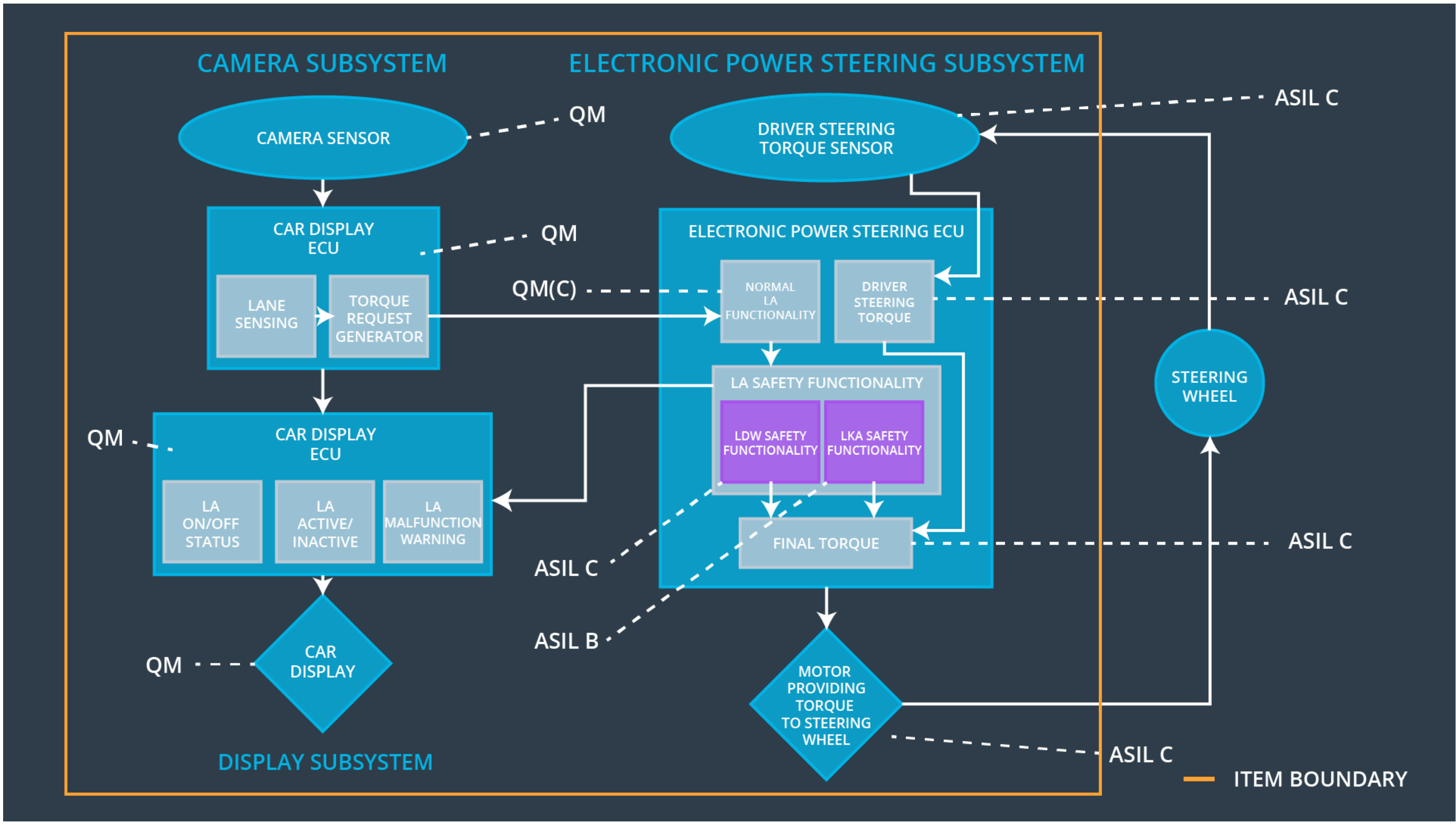
- Turning functional safety requirements into technical safety requirements
- Allocating technical safety requirements to the system architecture

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 keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	C	50 ms	LDW function turned off.
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	C	50 ms	LDW function turned off.
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	LKA function turned off.

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Visual observation of driving surface for lane detection. Signal sent to camera sensor ecu.
Camera Sensor ECU - Lane Sensing	Lane sensing functionality. Outputs data to torque request generator.
Camera Sensor ECU - Torque request generator	Sends torque request to electronic power steering ECU.
Car Display	Visual display to driver of LDW/LKA status recieved from car display ECU.
Car Display ECU - Lane Assistance On/Off Status	Determines if LA on/off. Sends to car display.

Car Display ECU - Lane Assistant Active/Inactive	Determines if LA active/inactive. Sends to car display.
Car Display ECU - Lane Assistance malfunction warning	Receives malfunction information from LA safety functionality. Sends to car display.
Driver Steering Torque Sensor	Measures driver torque input. Sends input to electronic power steering ECU driver toque element.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Recieves driver steering torque from torque sensor. Sends to final torque element in EPS ECU.
EPS ECU - Normal Lane Assistance Functionality	Standard LA functionality without safety implementations. Recieves driver torque request, sends to LA safety functionality.
EPS ECU - Lane Departure Warning Safety Functionality	Recieves torque request from normal LA functionality. Limits torque in regard to Functional Safety Requirement 01-01/01-02. Sends output to final torque.
EPS ECU - Lane Keeping Assistant Safety Functionality	Recieves torque request from normal LA functionality. Limits torque in regard to Functional Safety Requirement 02-01. Sends output to final torque.
EPS ECU - Final Torque	Recieves input from LA safety functionality and driver steering torque. Determines required torque to send to motor.
Motor	Receives required torque from final torque element and applies to steering wheel.

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	The lane keeping item shall	X		

Safety Requirement 01-01	ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude			

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 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 function turned off.
Technical Safety Requirement 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	50 ms	LDW Safety	LDW function turned off.
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	LDW function turned off.
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50 ms	Data Transmission Integrity Check	LDW function turned off.
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	Memory Test	LDW function turned off.

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 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 function turned off.
Technical Safety Requirement 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	50 ms	LDW Safety	LDW function turned off.
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	LDW function turned off.
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50 ms	Data Transmission Integrity Check	LDW function turned off.
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	Memory Test	LDW function turned off.

Lane Keeping Assistance (LKA) Requirements:

Functional Safety Requirement 02-1 with its associated system elements
(derived in the functional safety concept)

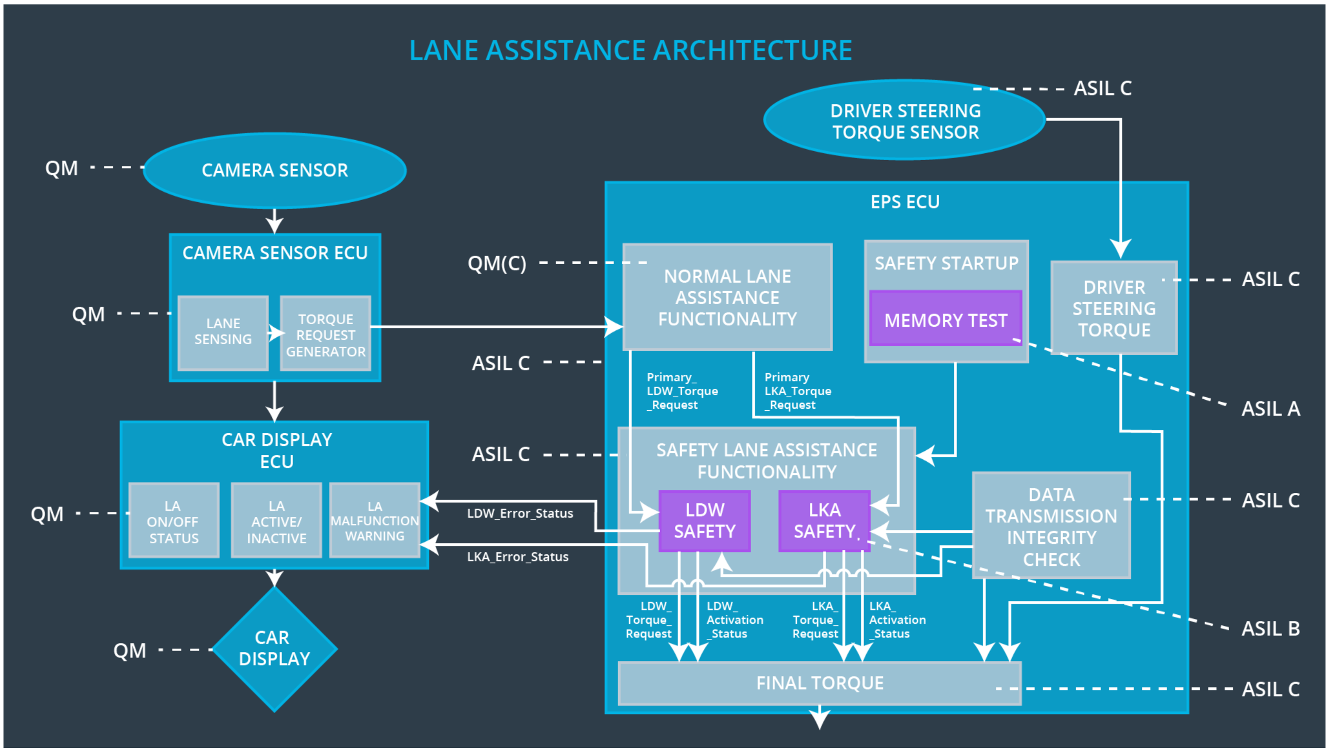
ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	X		

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_Request' sent to the 'Final electronic power steering Torque' component is below Max_Duration.	B	500 ms	LKA Safety	LKA function turned off.
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 function turned off.
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 function turned off.
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	B	500 ms	Data Transmission Integrity Check	LKA function turned off.
Technical Safety Requireme	Memory test shall be conducted at start up of the EPS ECU to	A	500 ms	Memory Test	LKA function turned off.

nt 05	check for any faults in memory.				

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

All technical safety requirements are allocated to the Electronic Power Steering ECU.

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off LDW function.	Malfunction_01 / Malfunction_02	Yes	Malfunction warning on Car Display.
WDC-02	Turn off LKA function.	Malfunction_03	Yes	Malfunction warning on Car Display.