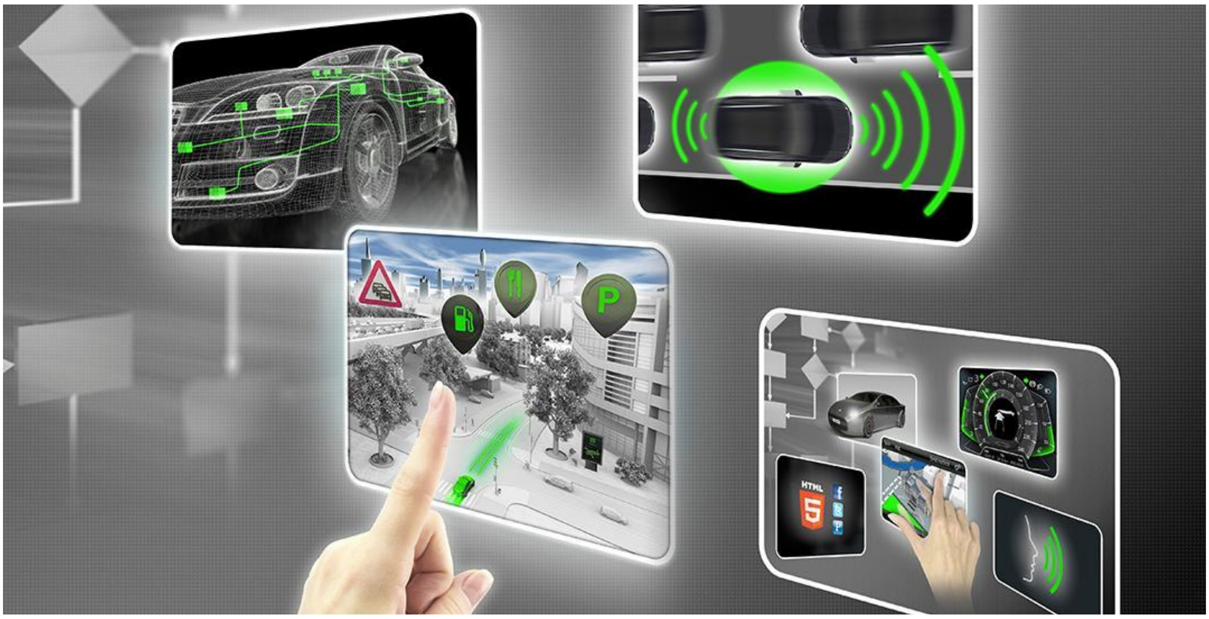
Software Safety Requirements and Architecture

Lane Assistance

Document Version: 0.1

Template Version 1.0, Released on 2017-06-21



Document history

Date	Version	Editor	Description
2017-09-10	**0.1**	**Olli Vertanen**	**Initial version**

Table of Contents

Purpose

The purpose of this document is to specify software safety requirements. These are derived from the technical safety requirements (see. Technical Safety Concept). Also, this document develops a software architectural design that realizes the software safety requirements. The software safety requirements are allocated to architectural components.

Inputs to the Software Requirements and Architecture Document

Technical safety requirements

Technical Safety Requirements for the Lane Assistance Item are stated in the Functional Safety Concept.

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

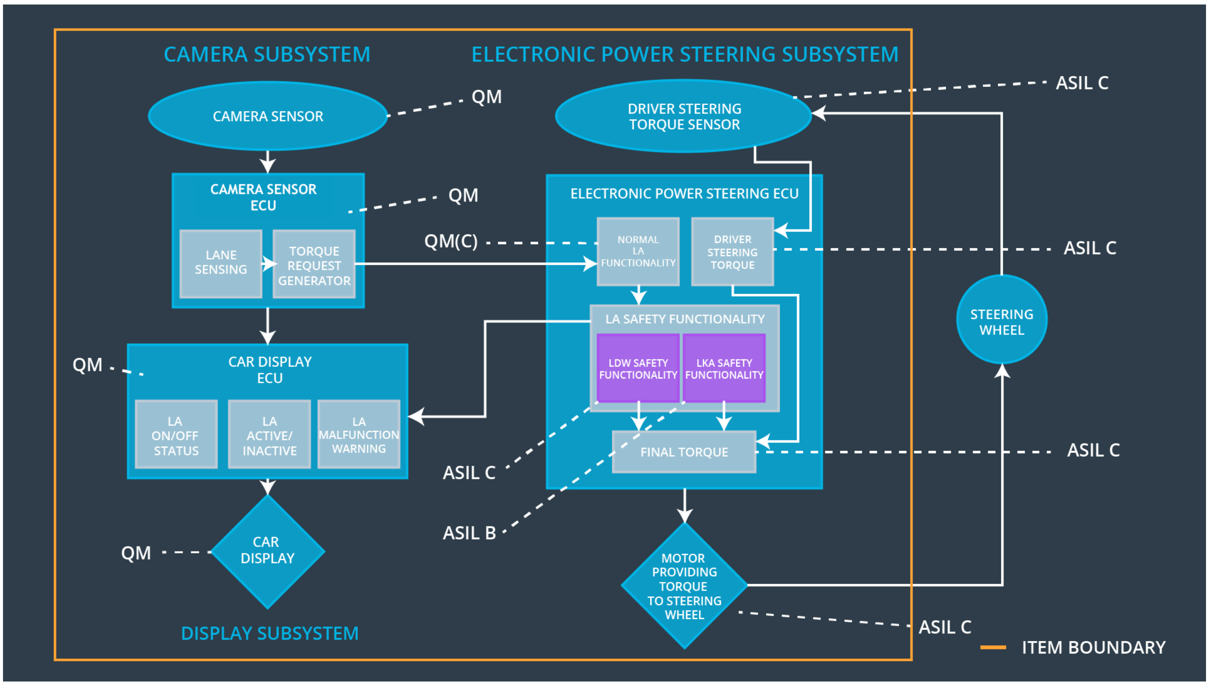
ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 01	The LDW Safety component shall ensure that the amplitude of LDW_Torque_Request sent to the Final Torque component is below Max_Torque_Amplitude.	C	50 ms	LDW Safety	LDW_Torque_Request == 0
Technical Safety Requirement 02	The validity and integrity of LDW_Torque_Request signal shall be ensured.	C	50 ms	Data Transmission Integrity Check	N/A
Technical Safety Requirement 03	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and LDW_Torque_Request shall be set to zero.	C	50 ms	LDW Safety	LDW_Torque_Request == 0

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	LDW_Torque_Request == 0
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	ignition cycle	Memory Test	LDW_Torque_Request == 0

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 LDW_Torque_Request sent to the Final Torque component is below Max_Torque_Frequency.	C	50 ms	LDW Safety	LDW_Torque_Request == 0
Technical Safety Requirement 02	The validity and integrity of LDW_Torque_Request signal shall be ensured.	C	50 ms	Data Transmission Integrity Check	N/A
Technical Safety Requirement 03	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and LDW_Torque_Request shall be set to zero.	C	50 ms	LDW Safety	LDW_Torque_Request == 0
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	LDW_Torque_Request == 0
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	ignition cycle	Memory Test	LDW_Torque_Request == 0, Warning light ON

Refined Architecture Diagram from the Technical Safety Concept



Software Requirements

Lane Departure Warning (LDW) Amplitude Malfunction Software Requirements

(for Functional Safety Requirement 01-01)

ID	**Technical Safety Requirement**	**ASIL**	**Fault Tolerant Time Interval**	**Allocation to Architecture**	**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	LDW_Torque_Request == 0

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01/01-01	The input signal “Primary_LDW_Torque_Request” shall be read and pre-processed to determine the torque amplitude request coming from the “Normal LA Functionality” SW Component. Signal “processed_LDW_Torque_Request” shall be generated at the end of the processing.	C	LDW_SAFETY_INPUT_PROCESSING	N/A

Software Safety Requirement 01-01/01-02	In case the “processed_LDW_Torque_Request ” signal has a value greater than “Max_Torque_Amplitude_LDW” (maximum allowed safe torque amplitude), the torque signal “limited_LDW_Torque_Request” shall be set to 0, else “limited_LDW_Torque_Request” shall take the value of “processed_LDW_Torque_Request”.	C	TORQUE_LIMITER	“limited_LDW_Torque_Request” = 0(Nm=Newton-meter)
Software Safety Requirement 01-01/01-03	The “limited_LDW_Torque_Request” shall be transformed into a signal “LDW_Torque_Request” which is suitable to be transmitted outside of the LDW Safety component (“LDW Safety”) to the “Final EPS Torque” component. Also see SofSafReq01-01/02-01 and SofSafReq01-01/02-02	C	LDW_SAFETY_OUTPUT_GENERATOR	LDW_Torque_Request= 0 (Nm)

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01-01/02	The validity and integrity of the data transmission for LDW_Torque_Request signal shall be ensured	C	50 ms	Data Transmission Integrity Check	N/A

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01/02-01	Any data to be transmitted outside of the LDW Safety component (“LDW Safety”) including “LDW_Torque_Request “ and “activation_status” (see SofSafReq01-01/03-02) shall be protected by an End2End (E2E) protection mechanism.	C	E2E CALCULATION	N/A
Software Safety Requirement 01-01/02-02	The E2E protection protocol shall contain and attach the control data: alive counter (SQC) and CRC to the data to be transmitted.		E2E CALCULATION	N/A

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
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	50 ms	LDW Safety	LDW_Torque_Request == 0

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement01-01/03-01	Each of the SW elements shall output a signal to indicate any error, which is detected by the element. Error signal = error_status_input(LDW_SAFETY_INPUT_PROCESSING), error_status_torque_limiter(TORQUE_LIMITER), error_status_output_gen(LDW_SAFETY_OUTPUT_GENERATOR)	C	All	N/A
Software Safety Requirement01-01/03-02	A software element shall evaluate the error status of all the other software elements and in case any of them indicates an error, it shall deactivate the LDW feature (“activation_status”=0)	C	LDW_SAFETY_ACTIVATION	activation_status == 0 (LA deactivated)
Software Safety Requirement01-01/03-03	In case of no errors from the software elements, the status of the LDW feature shall be set to activated (“activation_status”=1)	C	LDW_SAFETY_ACTIVATION	N/A
Software Safety Requirement01-01/03-04	In case an error is detected by any of the software elements, it shall set the value of its corresponding torque to 0 so that “LDW_Torque_Request” is set to 0	C	All	LDW_Torque_Request == 0
Software Safety Requirement01-01/03-05	Once the LDW functionality has been deactivated, it shall stay deactivated till the time the ignition is switched from off to on again.	C	LDW_SAFETY_ACTIVATION	activation_status == 0

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01-01/04	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	LDW_Torque_Request == 0

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01/04-01	When the LDW function is deactivated (activation_status set to 0), the activation_status shall be sent to the Car Display ECU.	C	LDW_SAFETY_ ACTIVATION Car Display ECU	N/A

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
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	C	50 ms	LDW_SAFETY	LDW_Torque_Request == 0

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-01/05-01	A CRC verification check over the software code in the Flash memory shall be done every time the ignition is switched from off to on to check for any corruption of content.	A	MEMORY_TEST	activation_status == 0
Software Safety Requirement 01-01/05-02	Standard RAM tests to check the data bus, address bus and device integrity shall be done every time the ignition is switched from off to on (E.g.walking 1s test, RAM pattern test. Refer RAM and processor vendor recommendations).	A	MEMORY_TEST	activation_status == 0
Software Safety Requirement 01-01/05-03	The test result of the RAM or Flash memory shall be indicated to the LDW Safety component via the “test_status” signal.	A	MEMORY_TEST	activation_status == 0
Software Safety Requirement 01-01/05-04	In case any fault is indicated via the “test_status” signal, the LDW_SAFERY_INPUT_PROCESSING shall set an error on error_status_input (=1) so that the LDW functionality is deactivated and the LDWTorque is set to 0.	A	LDW_SAFETY_INPUT_PROCESSING	activation_status == 0

Lane Departure Warning (LDW) Frequency Malfunction Software Requirements

(for Functional Safety Requirement 01-02)

Technical requirements for LDW frequency are mostly same and implemented by same SW blocks than requirements for LDW amplitude. Amplitude and frequency are both attributes of LDW_Torque_Request.

ID	**Technical Safety Requirement**	**ASIL**	**Fault Tolerant Time Interval**	**Allocation to Architecture**	**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	50 ms	LDW Safety	LDW_Torque_Request == 0

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-02/01-01	See SoftSafReq 01-01/01-01	C	LDW_SAFETY_INPUT_PROCESSING	N/A
Software Safety Requirement 01-02/01-02	In case the “processed_LDW_Torque_Request ” signal has a value greater than “Max_Torque_Frequency_LDW” (maximum allowed safe torque frequency), the torque signal “limited_LDW_Torque_Request” shall be set to 0, else “limited_LDW_Torque_Request” shall take the value of “processed_LDW_Torque_Request”.	C	TORQUE_LIMITER	“limited_LDW_Torque_Request” == 0 Nm
Software Safety Requirement 01-02/01-03	See 01-01/01-03	C	LDW_SAFETY_OUTPUT_GENERATOR	LDW_Torque_Request= 0 Nm

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01-02/02	The validity and integrity of the data transmission for LDW_Torque_Request signal shall be ensured.	C	50 ms	Data Transmission Integrity Check	N/A

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-02/02-01	See SofSafReq01-01/02-01.	C	E2E CALCULATION	N/A
Software Safety Requirement 01-02/02-02	See SofSafReq01-01/02-02.		E2E CALCULATION	N/A

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
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	50 ms	LDW Safety	LDW_Torque_Request == 0

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement01-02/03-01	See SoftSafReq 01-01/03-01	C	All	N/A

Software Safety Requirement01-02/03-02	See SoftSafReq 01-01/03-02	C	LDW_SAFETY_ACTIVATION	activation_status == 0 (LA deactivated)
Software Safety Requirement01-02/03-03	See SoftSafReq 01-01/03-03	C	LDW_SAFETY_ACTIVATION	N/A
Software Safety Requirement01-02/03-04	See SoftSafReq 01-01/03-05	C	All	LDW_Torque_Request == 0 Nm
Software Safety Requirement01-02/03-05	See SoftSafReq 01-01/03-05	C	LDW_SAFETY_ACTIVATION	activation_status == 0

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01-02/04	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	LDW_Torque_Request == 0

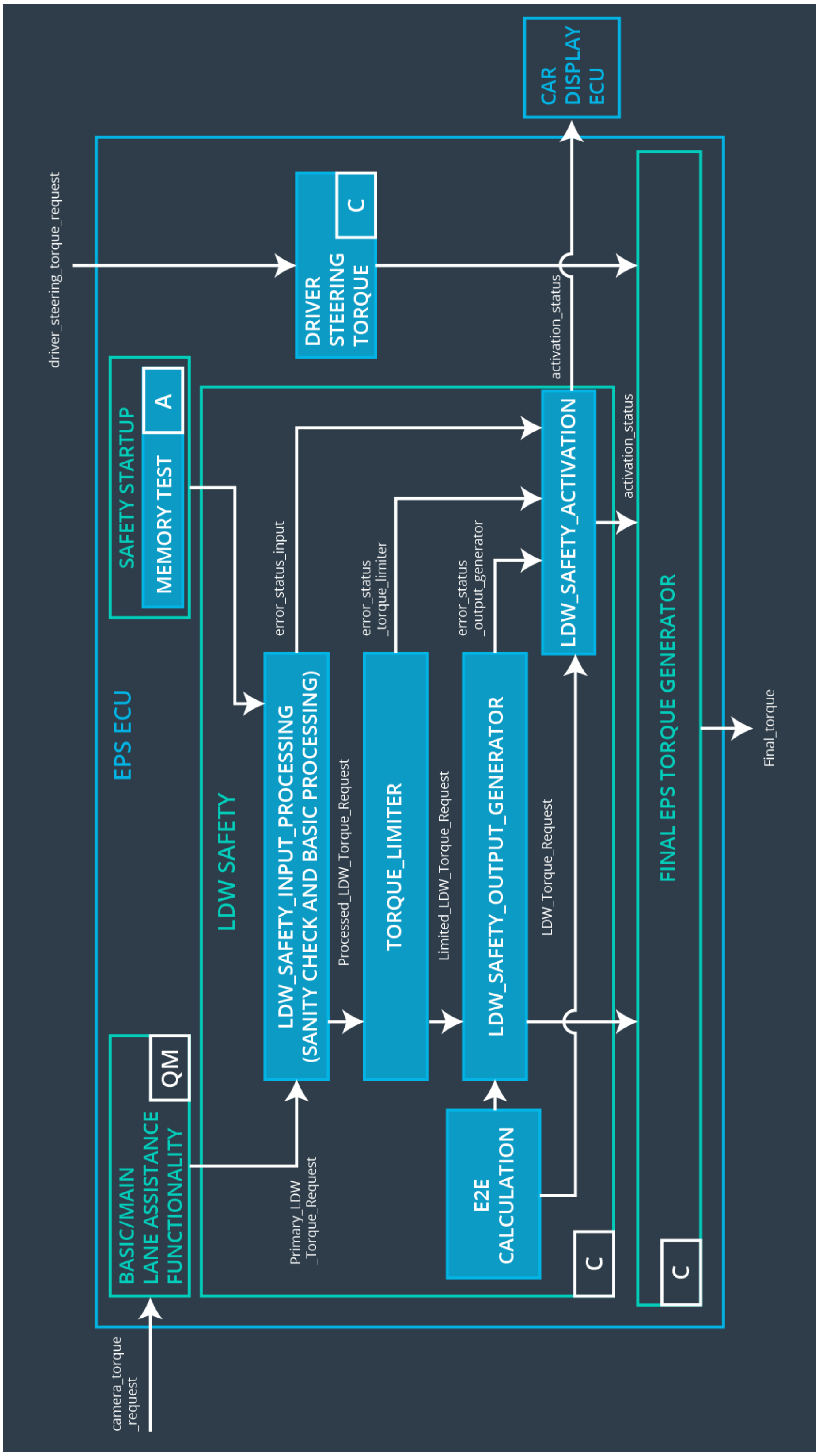
ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-02/04-01	See SoftSafReq 01-01/04-01	C	LDW_SAFETY_ACTIVATION Car Display ECU	N/A

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State

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	C	50 ms	LDW_SAFETY	LDW_Torque_Request == 0

ID	Software Safety Requirement	ASIL	Allocation Software Elements	Safe State
Software Safety Requirement 01-02/05-01	Same as SoftSafReq 01-01/05-01	A	MEMORY_TEST	activation_status == 0
Software Safety Requirement 01-02/05-02	Same as SoftSafReq 01-01/05-02	A	MEMORY_TEST	activation_status == 0
Software Safety Requirement 01-02/05-03	Same as SoftSafReq 01-01/05-03	A	MEMORY_TEST	activation_status == 0
Software Safety Requirement 01-02/05-04	Same as SoftSafReq 01-01/05-04	A	LDW_SAFETY_INPUT_PROCESSING	activation_status == 0

Refined Architecture Diagram


EPS ECU
CAR DISPLAY ECU
driver_steering_torque_request
DRIVER STEERING TORQUE
C
activation_status
SAFETY STARTUP
MEMORY TEST
A
LDW SAFETY
error_status_input
error_status _torque_limiter
error_status _output_generator
LDW_SAFETY_ACTIVATION
activation_status
LDW_SAFETY_INPUT_PROCESSING (SANITY CHECK AND BASIC PROCESSING)
Processed_LDW_Torque_Request
TORQUE_LIMITER
Limited_LDW_Torque_Request
LDW_SAFETY_OUTPUT_GENERATOR
LDW_Torque_Request
FINAL EPS TORQUE GENERATOR
Final_torque
BASIC/MAIN LANE ASSISTANCE FUNCTIONALITY
QM
Primary_LDW _Torque_Request
E2E CALCULATION
C
C
camera_torque _request