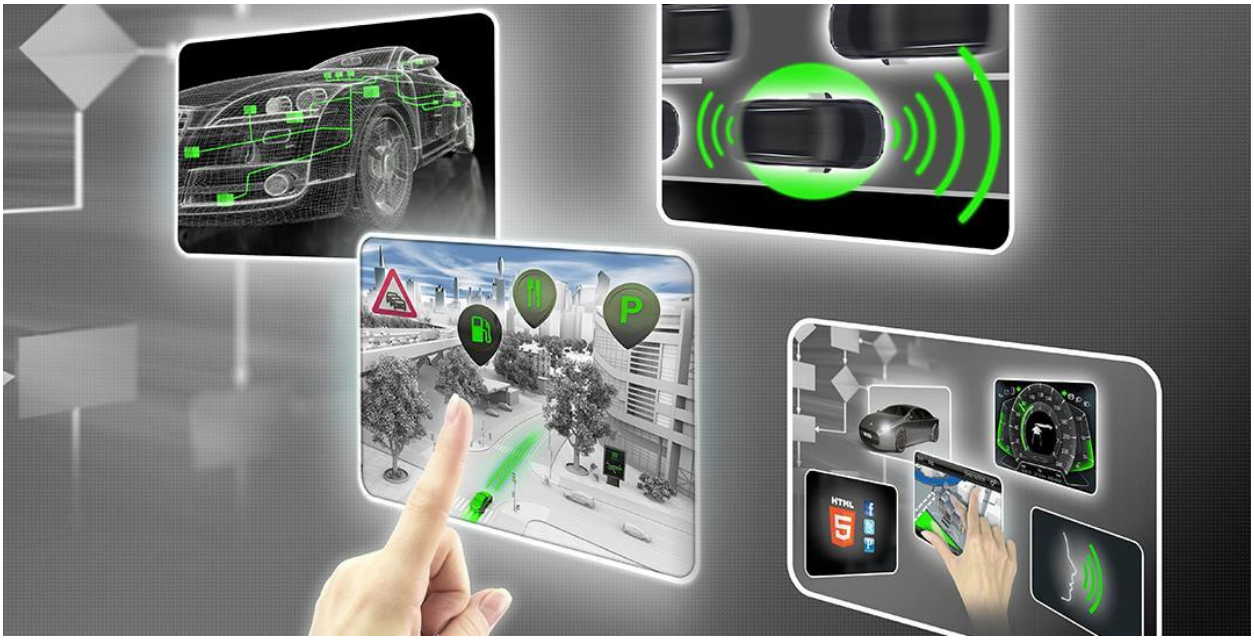
Elektrobit

UDACITY

Software Safety Requirements and Architecture
Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-06-21



Document history

Date	Version	Editor	Description
2018-06-04	v0.9	Csathó, Csaba	First draft
2018-06-21	v1.0	Csathó, Csaba	Final version

Table of Contents

Contents

Purpose

This document provides the detailed software safety requirements for the software components at a component level to identify potential complications on software design and architecture that may lead to a violation of safety goals. Specifications are provided for system state and signal paths, communication protocols and even naming conventions applied and to be used during the development of the software. The software modules architecture is refined based on the software safety requirements.

Inputs to the Software Requirements and Architecture Document

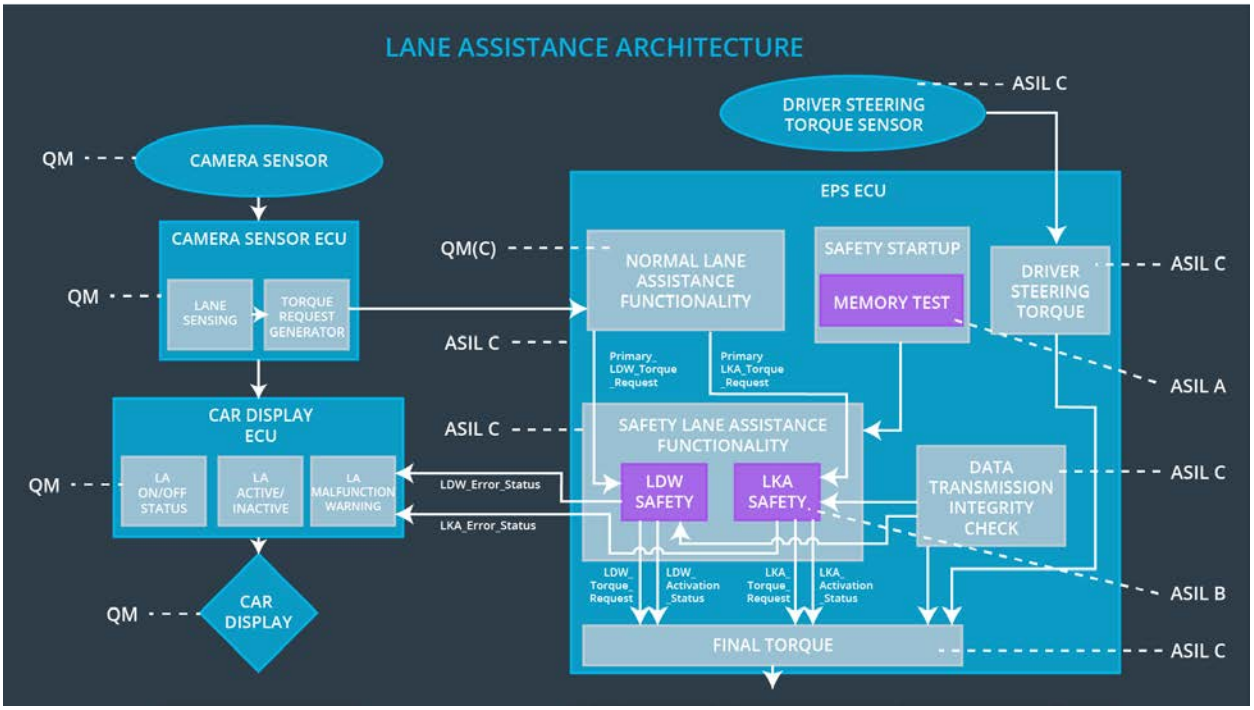
Technical safety requirements

Technical Safety Requirements related to Functional Safety Requirement **01-01** are …

T/S ID	Functional Safety Requirement	ASIL	F/Tol. Time Intv.	Safe State
Requirement 01-01-01	The *LDW safety component* shall ensure that the amplitude of the `LDW_Torque_Request` sent to the *Final Electronic Powersteering Torque Component* is below `Max_Torque_Amplitude`.	C	50 ms	LDW torque is set to zero
Requirement 01-01-02	If and when the LDW is deactivated, the *LDW Safety Component* software module shall send a signal to the Car Display ECU to show a warning signal.	C	50 ms	LDW torque is set to zero
Requirement 01-01-03	When 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 torque is set to zero
Requirement 01-01-04	The validity and integrity of the data transmission for `LDW_Torque_Request` signal shall be ensured.	C	50 ms	LDW torque is set to zero
Requirement 01-01-05	Memory test shall be conducted at startup of the EPS ECU in order to rule out any faults in the memory module.	A	Ignition cycle timespan	LDW torque is set to zero

Refined Architecture Diagram from the Technical Safety Concept

Refined System Architecture



Software Requirements

Lane Departure Warning (LDW) Amplitude Malfunction Software Requirements:

T/S ID	Functional Safety Requirement	ASIL	F/T T/I	Alloc. to Arch.	Safe State
Requirement 01-01-01	The *LDW safety component* shall ensure that the amplitude of the `LDW_Torque_Request` sent to the *Final Electronic Powersteering Torque Component* is below `Max_Torque_Amplitude`.	C	50 ms	LDW Safety	LDW torque is set to zero

S/S ID	Software Safety Requirement	ASIL	Alloc. SW Elem.	Safe State
Requirement 01-01-01-01	The input signal 'Primary_LDW_Torq_Req' shall be read and pre-processed to determine the torque request coming from the 'Basic/Main LAFunctionality' SW Component. Signal 'processed_LDW_Torq_Req' shall be generated at the end of the processing.	C	LDW_SAGETY_INPUT_PROCESSING	N/A
Requirement 01-01-01-02	In case the 'processed_LDW_Torq_Req' signal has a value greater than 'Max_Torque_Amplitude_LDW' (maximum allowed safe torque), the torque signal 'limited_LDW_Torq_Req'	C	TORQUE_LIMITER	'limited_LDW_Torq_Req' = 0 (Nm=Newton-meter)
Requirement 01-01-01-03	The 'limited_LDW_Torq_Req' shall be transformed into a signal 'LDW_Torq_Req' which is suitable to be transmitted outside the LDW Safety component ('LDW Safety') to the 'Final EPS Torque' component.	C	LDW_SAFETY_OUTPUT_GENERATOR	LDW_Torq_Req = 0 (Nm)

T/S ID	Functional Safety Requirement	ASIL	F/T T/I	Alloc. to Arch.	Safe State
Requirement 01-01-02	If and when the LDW is deactivated, the *LDW Safety Component* software module shall send a signal to the Car Display ECU to show a warning signal.	C	50 ms	LDW Safety	LDW torque is set to zero

S/S ID	Software Safety Requirement	ASIL	Alloc. SW Elem.	Safe State
Requirement 01-01-02-01	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

T/S ID	Functional Safety Requirement	ASIL	F/T T/I	Alloc. to Arch.	Safe State
Requirement 01-01-03	When 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 is set to zero

S/S ID	Software Safety Requirement	ASIL	Alloc. SW Elem.	Safe State
Requirement 01-01-03-01	Each Software element 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
Requirement 01-01-03-02	A software element shall evaluate the error status of all other software elements and in case any one of them indicates an error, it shall deactivate the Lane Departure Warning feature ('activation_status' = 0)	C	LDW_SAFETY_ACTIVATION	Lane Departure Warning function deactivated ('activation_status' =0).
Requirement 01-01-03-03	In case of a no error from the software elements, the status of the Lane Departure Warning feature shall be set to activated ('activation_status' = 1).	C	LDW_SAFETY_ACTIVATION	N/A
Requirement 01-01-03-04	In case an error is detected by any of the software elements, it shall set the value to its corresponding torque to zero so that 'LDW_Torq_Req' is set to 0	C	All	LDW_Torq_Req = 0
Requirement 01-01-03-05	Once the Lane Departure Warning functionality has been deactivated, it shall stay deactivating until the time the ignition is switched from off to on again.	C	LDW_SAFETY_ACTIVATION	Lane Departure Warning function deactivated ('activation_status' =0).

T/S ID	Functional Safety Requirement	ASIL	F/T T/I	Alloc. to Arch.	Safe State
Requirement 01-01-04	The validity and integrity of the data transmission for `LDW_Torque_Request` signal shall be ensured.	C	50 ms	LDW Safety	LDW torque is set to zero

S/S ID	Software Safety Requirement	ASIL	Alloc. SW Elem.	Safe State
Requirement 01-01-04-01	Any data to be transmitted outside the LDQ Safety component ('LDW Safety') including 'LDW_Torque_Req' and 'activation_status' shall be protected by an End-2-End protection mechanism.	C	E2C Calc	LDW_Torq _Req = 0 (Nm)
Requirement 01-01-04-02	The E2E protection protocol shall contain and attach the control data (alive counter (SQC) and CRC) to the data to be transmitted.	C	E2C Calc	LDW_Torq _Req = 0 (Nm)

T/S ID	Functional Safety Requirement	ASIL	F/T T/I	Alloc. to Arch.	Safe State
Requirement 01-01-05	Memory test shall be conducted at startup of the EPS ECU in order to rule out any faults in the memory module.	A	Ignition cycle timespan	Data Transmission Integrity Check	LDW torque is set to zero

S/S ID	Software Safety Requirement	ASIL	Alloc. SW Elem.	Safe State
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 content corruption.	A	MEMORYTEST	Activation_ status = 0
Requirement 01-01-05-02	Standard RAM test 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 to RAM and processor vendor recommendations)	A	MEMORYTEST	Activation_ status = 0
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	MEMORYTEST	Activation_ status = 0
Requirement 01-01-05-04	In case any fault is indicated via the 'test_status' signal the INPUT_LDW_PROCESSING shall set an error on the error_status_input (=1) so that the Lane Departure Warning functionality is deactivated and the LDW_Torque_Req is set to zero.	A	LDW_SFETY_INPUT_PROCESSING	Activation_ status = 0

Refined Architecture Diagram

Refined System Architecture Diagram