Functional Safety Concept Lane Assistance

Document Version: 4.0
Released on 2017-10-31

Document history

Date	Version	Editor	Description
10-23-2017	1.0	Brian McHugh	Set up template
10-24-2017	2.0	Brian McHugh	Initial draft
10-27-2017	3.0	Brian McHugh	Complete up to FSR
10-28-2017	4.0	Brian McHugh	Finalize

Table of Contents

Purpose of the Functional Safety Concept

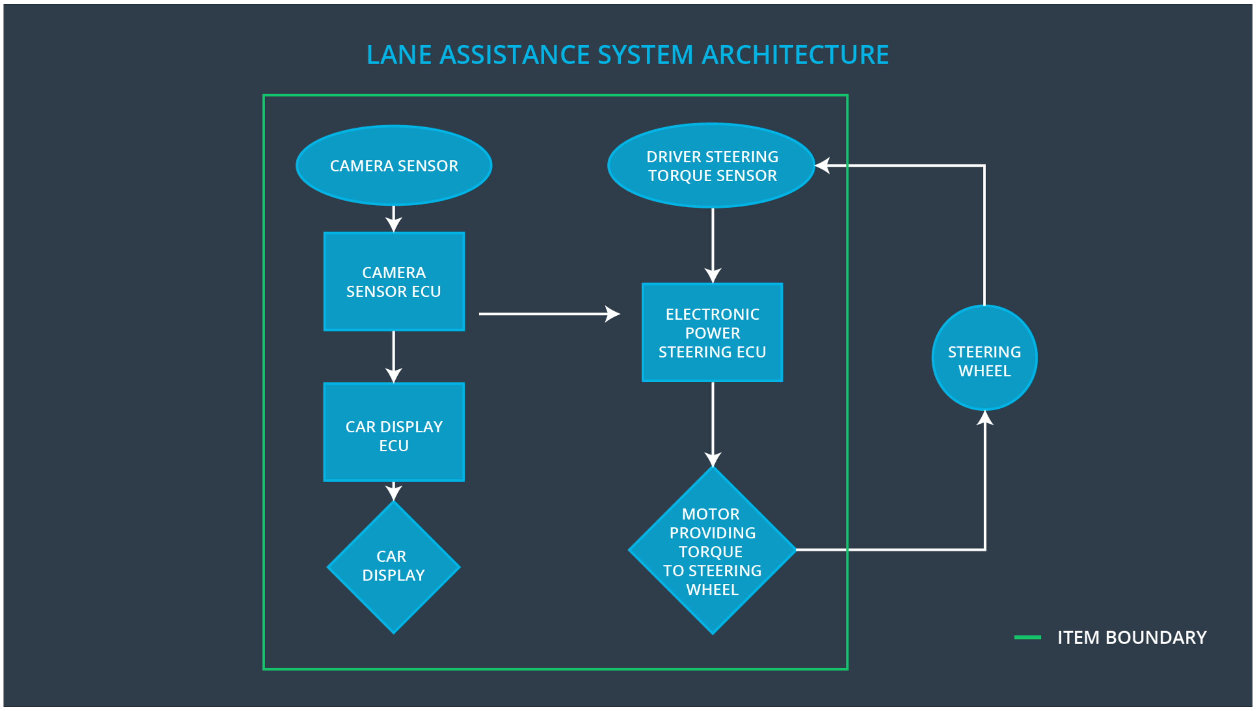
By reviewing the item's architectural design, we can figure out which subsystems and elements can be used to meet safety goals. The Functional Safety Concept will identify these subsystems and elements and further refine these high-level goals into Functional Safety Requirements. Each Functional Safety Requirement is then allocated to its appropriate place in the item's architecture.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	The oscillating steering torque from the Lane Departure Warning (LDW) function shall be limited
Safety_Goal_02	Total loss of the Lane Keeping Assistance (LKA) function shall be prevented
Safety_Goal_03	Continuous activation of the LDW function when lane markers are undetectable shall be prevented
Safety_Goal_04	The LKA function shall be time limited, and the additional steering torque shall end after a given time interval so that the driver cannot misuse the system for autonomous driving

Preliminary Architecture


LANE ASSISTANCE SYSTEM ARCHITECTURE
CAMERA SENSOR
DRIVER STEERING TORQUE SENSOR
CAMERA SENSOR ECU
ELECTRONIC POWER STEERING ECU
STEERING WHEEL
CAR DISPLAY ECU
CAR DISPLAY
MOTOR PROVIDING TORQUE TO STEERING WHEEL
ITEM BOUNDARY

Description of architectural elements

Element	Description
Camera Sensor	Captures images of the road ahead, as well as the front periphery of the vehicle and sends that data to the Camera Sensor ECU
Camera Sensor ECU	Processes images from the Camera Sensor and determines when the vehicle has unintentionally started to depart its lane and sends the appropriate messages to the Car Display ECU and the Electronic Power Steering ECU
Car Display	Receives input from the Car Display ECU and acts as a graphical user interface for the vehicle to communicate operational status to its operator
Car Display ECU	Processes data from the Camera Sensor ECU and transmits data to the Car Display
Driver Steering Torque Sensor	Receives input from the Steering Wheel and sends

	torque-level data to the Electronic Power Steering ECU
Electronic Power Steering ECU	Processes lane detection information received from the Camera Sensor ECU and torque-level readings from the Driver Steering Torque Sensor and outputs commands to/for the Steering Wheel Motor
Steering Wheel Motor	Acts as an actuator, applying torque and oscillations to the Steering Wheel when needed

Functional Safety Concept

The functional safety concept consists of:

- Functional safety analysis
- Functional safety requirements
- Functional safety architecture
- Warning and degradation concept

Functional Safety Analysis

Malfunction ID	**Main Function of the Item Related to Safety Goal Violations**	**Guidewords (NO, WRONG, EARLY, LATE, MORE, LESS)**	**Resulting Malfunction**
Malfunction_01	The LDW function shall apply an oscillating steering torque to provide haptic feedback	MORE	The LDW function applies an oscillating torque with very high torque amplitude (above limit)
Malfunction_02	The LDW function shall apply an oscillating steering torque to provide haptic feedback	MORE	The LDW function applies an oscillating torque with very high torque frequency (above limit)
Malfunction_03	The LKA function shall apply the steering torque when active in order to stay in ego lane	WRONG	The LKA function is engaged but fails to apply steering torque to maintain ego lane
Malfunction_04	The LDW function shall apply an	WRONG	The LDW function applies an oscillating

	oscillating steering torque to provide haptic feedback		torque continuously when lane markers are undetectable, even while vehicle is centered within ego lane
Malfunction_05	The LKA function shall apply the steering torque when active in order to stay in ego lane	NO	The LKA function is not limited in time of use, allowing the vehicle operator to misuse it for autonomous driving

Functional Safety Requirements

Lane Departure Warning (LDW) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	The lane assistance item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	OFF
Functional Safety Requirement 01-02	The lane assistance item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50 ms	OFF
Functional Safety Requirement 01-03	The lane assistance item shall ensure that the lane departure oscillating torque amplitude and oscillating torque frequency default to 0 (shut off) if the electronic power steering ECU exceeds Max_Torque_Duration	QM	50 ms	OFF

Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria:

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Functional Safety Requirement 01-01	Test how drivers react to different torque amplitudes to prove that we chose an appropriate value	When the torque amplitude crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval; conduct a software test inserting a fault into the system and log the results
Functional Safety Requirement 01-02	Test how drivers react to different torque frequencies to prove that we chose an appropriate value	When the torque frequency crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval; conduct a software test inserting a fault into the system and log the results
Functional Safety Requirement 01-03	Test and validate that the Max_Duration chosen terminates the LDW function soon enough for drivers to remain calm while operating the vehicle	When the torque duration crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval; conduct a software test inserting a fault into the system and log the results

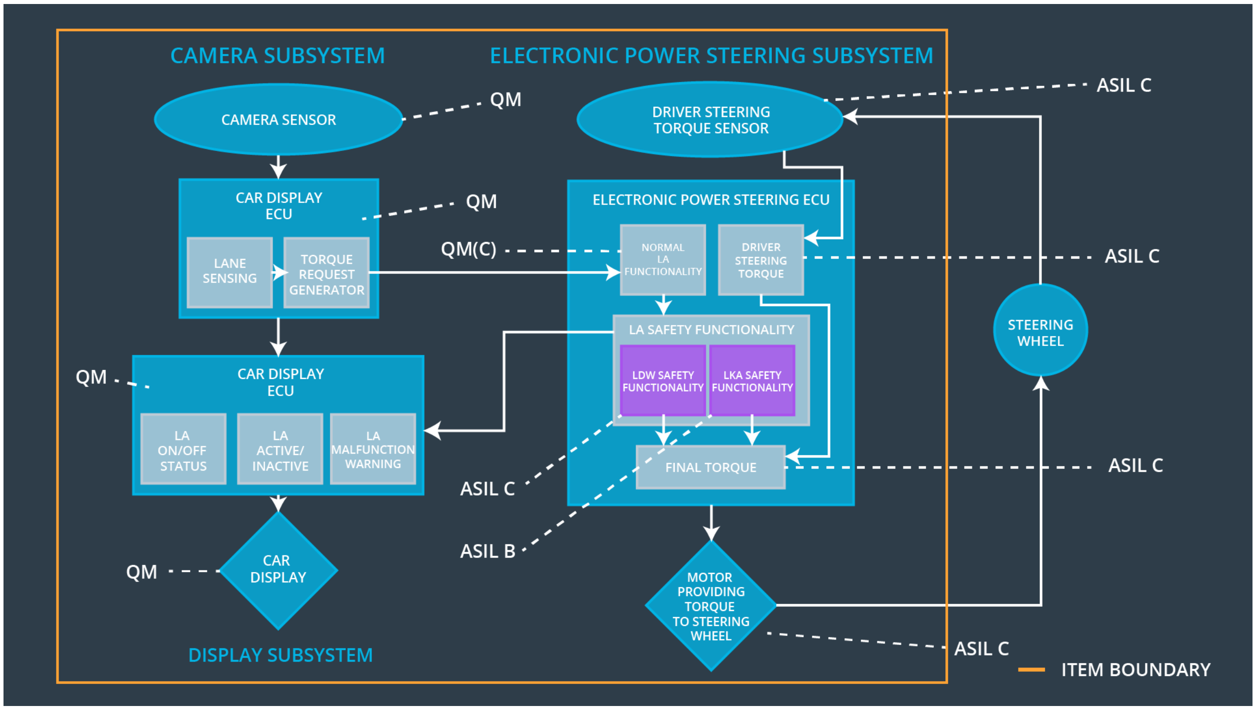
Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The lane assistance item shall ensure that the necessary redundancies are included in the system architecture to prevent total loss of the LKA function	A	500 ms	OFF
Functional Safety Requirement 02-02	The lane assistance item shall ensure that the electronic power steering ECU limits torque usage to Max_Duration	B	500 ms	OFF

Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Functional Safety Requirement 02-01	Test and validate redundant system options and choose the most efficient solution; make sure FTTI is reasonable for switch to redundant system and check that warning for complete failures is quick enough for test drivers	Conduct a software test inserting a fault into the primary system and verify that the redundant system kicks in; insert a fault in primary *and* redundant system to verify that malfunction message is sent to Car Display
Functional Safety Requirement 02-02	Test and validate that the Max_Duration timeframe chosen really does dissuade drivers from taking their hands off the wheel	Verify that the system really does turn off if the lane keeping assistance ever exceeds Max_Duration

Refinement of the System Architecture



The Car Display subsystem gains three additional software blocks:

1) Light indicator for Lane Assistance: on/off
2) Light indicator for Lane Assistance: active/inactive
3) Light indicator for Lane Assistance: malfunction warning

The Camera Sensor subsystem gains two additional software blocks:

1) Lane Sensing - detect ego lane and determine if vehicle is staying centered within lane markers
2) Torque Request Generator - send torque requests to Electronic Power Steering subsystem

The Electronic Power Steering subsystem gains four additional software blocks:

1) Normal Lane Assistance Functionality - receives the vibrational torque request from the Camera Sensor subsystem
2) Lane Assistance Safety Functionality - receives the vibrational torque request from the Normal Lane Assistance Functionality block; sets amplitude, frequency and duration limits on torque requests sent to the Final Torque block and sends operational information to the Car Display subsystem
3) Driver Steering Torque - detects how much the driver is turning the Steering Wheel
4) Final Torque - adds torque requests together to output a final torque request to the Steering Wheel Motor

Allocation of Functional Safety Requirements to Architecture Elements

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 01-01	The Electronic Power Steering ECU shall ensure that the lane departure oscillating torque amplitude does not exceed Max_Torque_Amplitude	X		
Functional Safety Requirement 01-02	The Electronic Power Steering ECU shall ensure that the lane departure oscillating torque frequency does not exceed Max_Torque_Frequency	X		
Functional Safety Requirement 01-03	The Electronic Power Steering ECU shall ensure that the lane departure oscillating torque amplitude and oscillating torque frequency default to 0 (shut off) if the electronic power steering ECU exceeds Max_Duration for torque	X		
Functional	The Electronic Power Steering			

Safety Requirement 02-01	ECU shall provide the necessary redundancies to prevent total loss of the LKA function	X		
Functional Safety Requirement 02-02	The Electronic Power Steering ECU shall ensure that the electronic power steering ECU limits torque to Max_Duration	X		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	OFF	Oscillating torque amplitude exceeds Max_Torque_Amplitude	YES	Car Display
WDC-02	OFF	Oscillating torque frequency exceeds Max_Torque_Frequency	YES	Car Display
WDC-03	OFF	LKA function is on and activated but fails to apply steering torque	YES	Car Display
WDC-04	OFF	Oscillating torque duration exceeds Max_Torque_Duration	YES	Car Display
WDC-05	OFF	LKA function usage exceeds Max_Duration	YES	Car Display