Functional Safety Concept (Example)

Front Lights Manager

Functional safety architecture

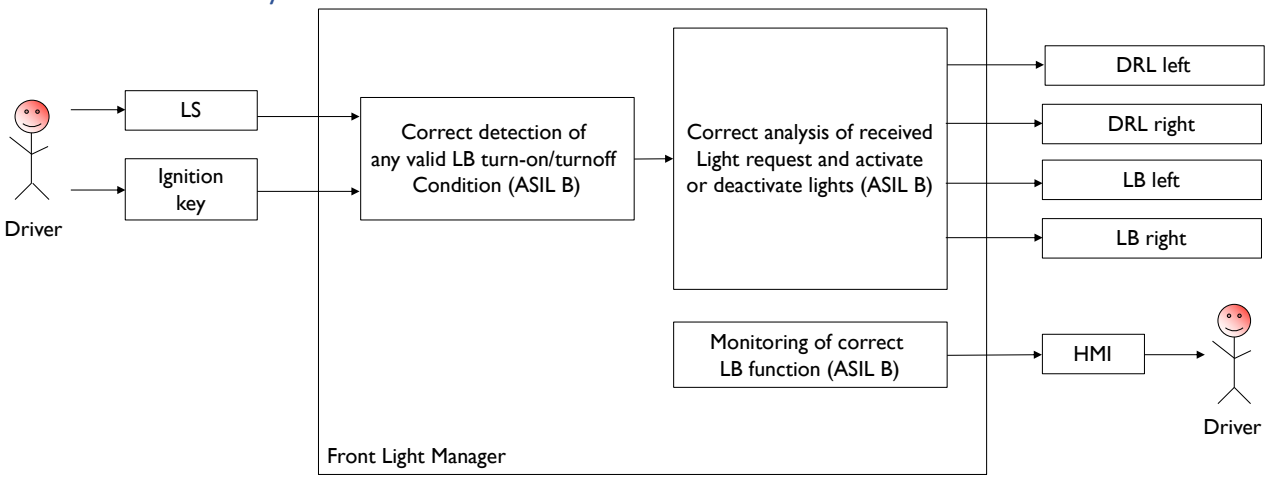


Figure 1 Functional safety architecture (from the safety concept)

Attributes of the safety goals

Fill in the attribute/parameters of the safety goal

Safety goal	**Attributes/Parameters of the safety goal**				
	Integrity	Safe state	Fault tolerance time	Warning concept	Degradation concept
SG1	B	Low beam on	500 ms	The driver must be notified if one of the low beam lights fails.	In case of failure of one low beam lights, turn on the DRL to make the car more visible to other drivers.

To avoid SG1 violation, in case of doubt on the position of LS or KL15, low beam shall be turned on.

Functional safety requirements and allocation

		Define functional safety requirements		Allocation of requirements on systems and elements	
		Safety requirements	**Remark**	**If applicable, allocate the safety requirements to other Items / Systems**	**If applicable, allocate the safety requirements to equipment other technologies to minimize risk. That could be e.g. hydraulic, mechanical equipment**
Safety goal	**Light should not switch off unintended while driving**	SR1 Any failure which causes that both low beam lamps are off shall be detected and the system shall switch on both lamps "ON" in continuous lighting within 500 ms	no	no	no
		SR2 If only one low beam lamp fails, the driver should get an information	Not safety relevant (maybe law), driver detection possible	Warning lamp in the Cockpit-Display	no
		SR3 The low beam shall be switch on continuous until a valid command is interpreted for turn off	no	no	no
		SR4 Both low beam lamps shall be provided and protected independent from each other	no	no	no

ONLY FOR EXAMPLE PURPOSES

ASIL preliminary architecture

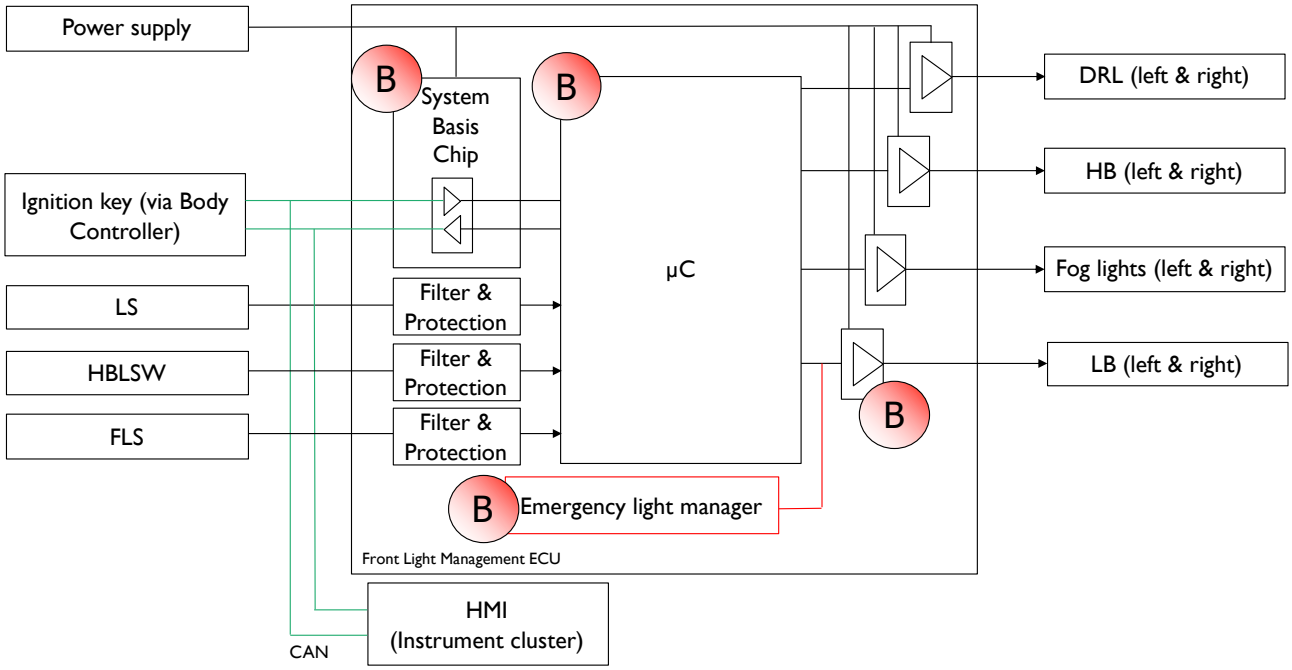


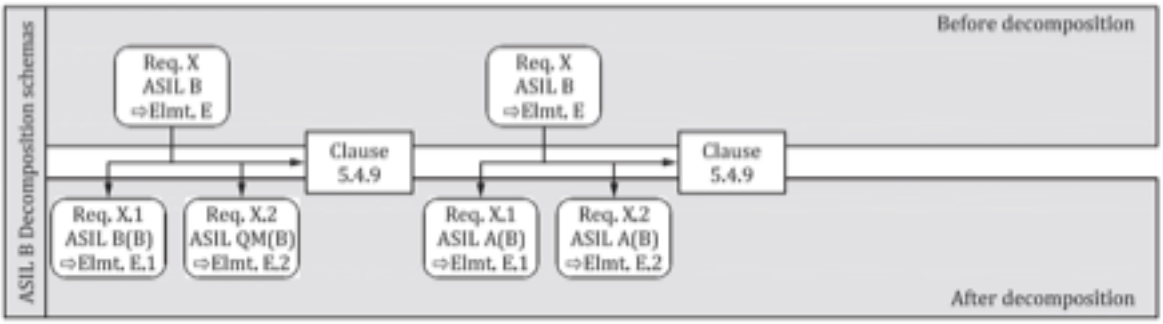
Figure 2 Preliminary architecture without ASIL decomposition

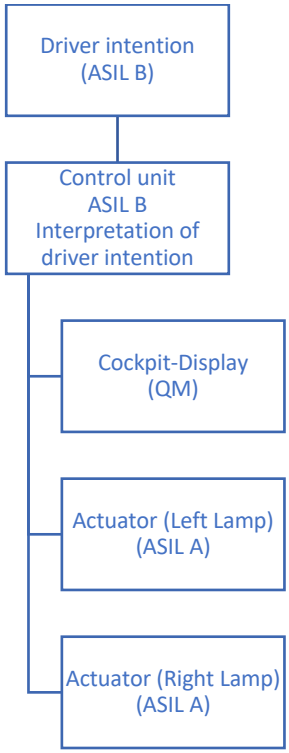
ONLY FOR EXAMPLE PURPOSES

ASIL preliminary architecture (with ASIL Decomposition)

Draw a preliminary functional architecture (with ASIL Decomposition)

Considering only the Low Beam (ASIL B) function, we propose the following ASIL decomposition, applying the rule on the right of the following figure:





ONLY FOR EXAMPLE PURPOSES

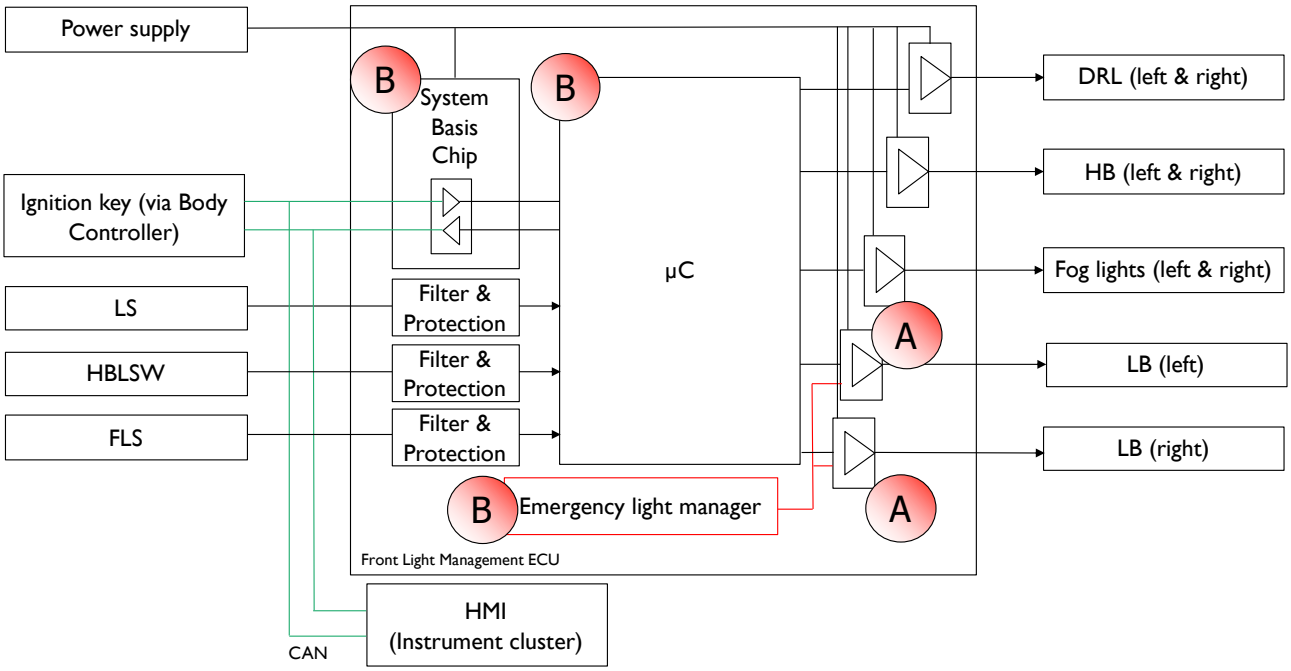


Figure 3 Preliminary architecture with ASIL decomposition. LBs drivers are able to measure the current flowing on the lamps

Functional redundancies

The µC can be replaced, in case of failure, by a simpler circuit, called Emergency Light Manager, that drives the Low Beams drivers to turn on the low beams.
The low beam lamps are drove by different drivers.

Independence of the individual blocks

The emergency light manager shall have a power supply different from the system basis chip.
The low beam drivers (left and right) are completely independent of each other, to avoid that a malfunction of one of them causes a single point of failure.

ONLY FOR EXAMPLE PURPOSES