Intelligence Light Beam Controller For Vehicles

Gugan N[1], Guru Prasad V[2], Sai Jagatheeswaran S[3], Surya R[4], Dinesh Babu K[4]
[1, 2, 3, 4] SRI SHAKTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY

Abstract- *The Automatic High Beam Light Controller (AHBLC) is a cutting-edge technology designed to enhance vehicle safety and driving convenience. This system integrates advanced sensors, real-time data processing and intelligent algorithms to automatically control a vehicles high beam headlights based on the surrounding environment, traffic conditions and driver preferences.*

Keywords- Functional Safety Management, ISO 26262, MCU, Body Control Module.

I. INTRODUCTION

Nowadays, safety is one of the most important issues of the automobile development. With the advancement in the automotive industry, more and more safety related electronically controlled units (ECU) are integrated into vehicle that now consists of larger system architecture with complex interaction and interfaces. The development and integration of these ECUs will strengthen the need for safe system development processes and the need to provide evidence that all reasonable product safety objectives are satisfied. On the other hand, with the trend of increasing technological complexity, software and hardware implementation, there are increasing risks from both systematic failures and random hardware failures. All these aspects pushed the automotive industry to develop functional safety standards as guidelines to keep risk emanated from the system functions at an acceptance level in any condition. ISO 26262 [1], introduced in 2011, provides guidance to reduce these risks by failures avoidance and control by appropriate requirements and processes.

By having certification of ISO 26262, automotive manufactures promote high confidence for customers to purchase automobiles in which prevention of accidents and the reduction of risks is at an acceptable level [2].

ISO 26262 consists of ten parts, as shown in Figure 1. It starts by describing the vocabulary and management of functional safety. Then, it covers from concept phase to the different level of product development which includes system, hardware and software. Automotive Safety Integrity Level (ASIL) decomposition, analysis of dependent failures and safety analyses are explained in part 9.

In the concept phase, hazard analysis and risk assessment (HARA) is performed to determine the safety goals and their ASIL for the system function by a systematic evaluation of hazardous events. Based on severity, probability of exposure and controllability, ASIL is classified into five different levels (QM, A, B, C and D) where level D constitutes the highest level of safety integrity and level A the lowest. QM (quality managed) level corresponds to not safety relevant events. Table 1 contains examples of ASIL classification for some systems [3].

For the development phase, the standard provides requirements to be applied to avoid unreasonable residual risks and, also, requirements for validation and confirmation measures to ensure a sufficient and acceptable level of safety.
In case of safety relevant systems, the additional actions which are needed to reduce the risk to an accepted level are performed to avoid the systematic faults and, also, to control of random hardware faults and systematic faults. The actions for avoidance of systematic faults are implemented by safety management, processes and supporting processes. The control of random and systematic faults is realized by technical requirements within a safety concept which contains safety measures, including the safety mechanisms, to comply with the safety goals.

ISO 26262	
Part 1: Vocabulary	Part 6: Product Development Software Level
Part 2: Management of Safety Function	
	Part 7: Production and Operation
Part 3: Concept Phase	Part 8: Production and Operation
Part 4: Product Development System Level	Part 9: ASIL-oriented and Safety-oriented analysis
Part 5: Product Development Hardware Level	Part 10: Guideline on ISO

Figure 1. Parts involved in ISO 26262

TABLE I. EXAMPLES OF ASIL CLASSIFICATION

System	Hazards	Safety Goal	ASIL
Window Lifter	Pinching limit	Avoid unintended closing	A
Low Beam	Loss of road illumination	Maintain sufficient road illumination	B
Electronic Stability Program (ESP)	Activation of faulty break	Avoid unintended breaking	C
Electronic Steering Column Lock	Activation of faulty locks while driving	Avoid unintended locking	D

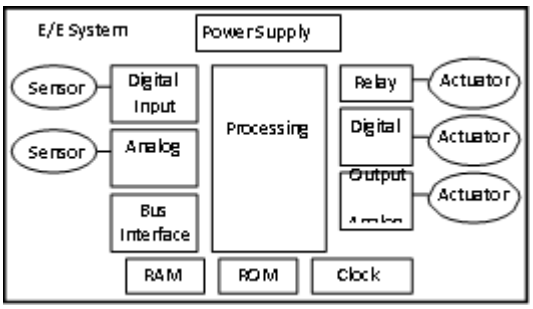

Figure 2. Generic hardware of an electronic control system

At first, functional safety requirements are derived and are allocated to elements based on preliminary architectural assumption of the items. Afterwards, technical safety requirements are refined into software and hardware level requirements.

Starting from guidelines and requirements from automotive safety standard ISO26262, in this paper safety concepts for power window and low beam functionalities are proposed. After a briefly presentation of the Body Control Module (BCM) in Section II, the proposed safety concepts for Power window and Low beam functions are presented in Section III and IV, respectively. Remarks and conclusions are provided in Section V.

II. BODY CONTROL MODULE

Modern cars have more than 30-50 Electronic Computer Units (ECU) to provide numerous functionalities, grouped in four areas [4]: body functionalities (e.g., access, lightning), chassis functionalities (e.g., braking, steering), powertrain functionalities (e.g., ignition, traction control), and infotainment and connectivity (e.g., navigation).

For body functionalities, Body Control Module (BCM) is the central ECU, communicating with many sensors and actuators through tens of input/output interface lines, and with other ECUs through Controller Area Network (CAN), Local Interconnect Network (LIN), FlexRay, and/or Ethernet [5]. BCM can provide many functions like: door lock, power window, exterior lighting, interior lighting, wiper, heating ventilation and air conditioning (HVAC) (see Figure 1). Functions like power window, wiper, and headlamp control for exterior lighting can pose hazards to people if these functions malfunction. In the next two sections, safety mechanisms defining the safety concepts for power window and low beam control functions are proposed.

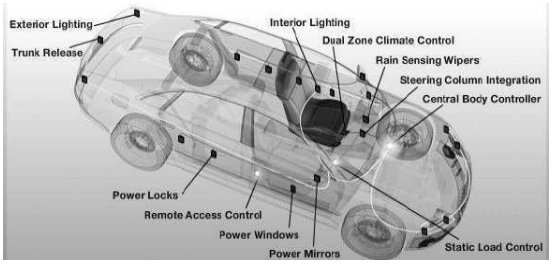

Figure 3. Functionalities provided by BCM [5]

III. POWER WINDOW SAFETY CONCEPT

This section considers power window functionality as a case study in analyzing and developing safety mechanisms and safety strategies.

Power window represents a standard functionality on every car, functionality which permits a user to move window in the car up or down automatically or manually. The request to move window can come from an analog switch or through a Controller Area Network (CAN) message. Based on the analog switch position or on CAN message, a control module actuates an H-bridge controlled motor to move window up or down. Due to a potential malfunction in the actuation system, a hazard can happen by closing the window unintendedly while parts of a human are outside through the window. In [6], power window was analyzed by performing hazard analysis and risk assessment, and it resulted that power window is a safety functionality with ASIL A level, and with safety goal "avoid unintended closing". To prevent closing situations leading to injuries, safety mechanisms and safety strategies need to be implemented in window functionality.

In Figure 4, a block diagram of a possible power window implementation is proposed. The technical implementation is split into four areas: input, processing system, output, and monitoring system. Starting from Figure 2 Generic hardware of an electronic control system, and from

guidelines presented in Annex D from ISO 26262 FE Part 5, safety mechanisms and safety strategies for power window are proposed.

Input area contains input signals which can request power window movements, i.e., analog switch signal, and window CAN messages. One of the common faults of switches is represented by stuck-at faults (e.g. short to Ground, short to Power supply), faults which can lead to an unintended closing of window.

A safety mechanism to detect stuck faults is to use coded resistive switches which provide different voltage ranges when the switch is pressed, pulled, or released. Using this type of safety mechanism, a diagnostic coverage of 90% can be obtained.

An unintended actuation of power window can result from erroneous CAN messages containing actuation requests. CAN messages can be affected by different faults (e.g. repetition, deletion, insertion, corruption, etc) [7], faults which can lead to closing window unintendedly. To protect from such faults, the window CAN requests must be protected by a Cyclic Redundant Check (CRC) and a counter message.

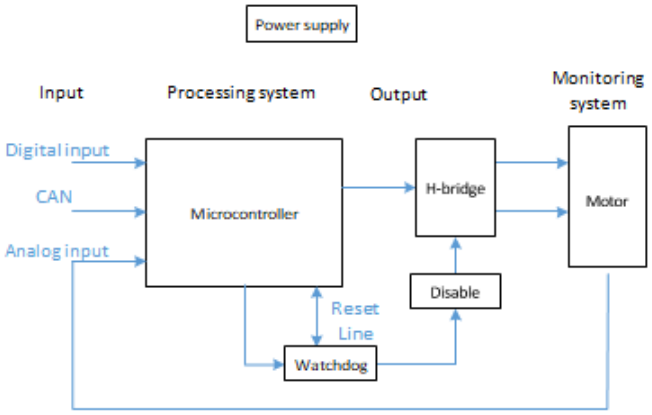

Figure 4. Power window block diagram

CRC represents a code added to data which is used to detect corruption of data during transmission. The counter message protects against repetition, deletion, and insertion faults. These safety mechanisms lead to a diagnostic coverage of 99%.

Processing or controlling system is formed by microcontroller which need to verify that the input signals are not damaged, to actuate H-bridge, and to detect and to react to pinch situations. A pinch situation occurs when during an upwards movement, the window exerts to an obstacle a force higher than a permissible threshold. ISO 26262 FE [1] presents the following failures which could affect the SW running in microcontroller: wrong coding, wrong or no execution, execution out of order, execution too fast or too slow, stack overflow/underflow. In case of these failures, it is possible that microcontroller could not detect pinch situations or could not react to pinch situations. Thus, an external watchdog monitors the correctness execution of program sequence, and in case of faults it resets microcontroller and concurrently, disables the H-bridge, stopping any window movement. Moreover, the external watchdog has a separate time reference than the microcontroller, and thus watchdog could detect faults in microcontroller clock like incorrect frequency, or period jitter.

The output area is represented by the microcontroller signals which control H-bridge, by H- bridge and by motor. To check that the output area is working correctly, the monitoring system provides information to microcontroller related to the motor rotation, the rotation direction, and if the torque force is increasing, as it happens in a pinch situation. The monitoring system can be implemented using hall sensors, for example.

The monitored information is provided to the microcontroller through analog digital converters, which can be tested during window rest phases with a reference signal to detect static failures (stuck-at failures) and cross-talk.

Using this safety mechanism (i.e., Test pattern Table D.7 — Analogue and digital I/O [1]), a diagnostic coverage of 90% for detecting failures in ADC convertors can be obtained. Moreover, because the digital conversion depends on the reference voltage signal, microcontroller needs to monitor the reference signal for over voltage and under voltage situations.

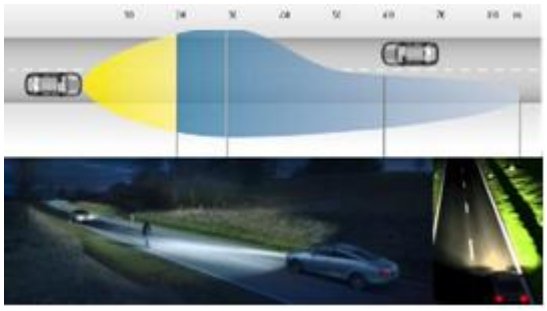

Figure 5. Road illumination by Low Beam

V. LOW BEAM LIGHTING SAFETY CONCEPT

One of the main classes of BCM functions is the control of exterior front lighting. Within this class, from safety point of view, we propose an analysis of the low beam

lighting. The low beam lighting is ensured by the two, left and right, headlights. The low beams provide a light distribution to give adequate forward and lateral illumination without dazzling the oncoming traffic, as depicted in Figure 5. The low beams remain switched on when activated in order to provide illumination of the road for at least 50 meters such that to be able to drive safely even under critical (high speed in the dark) environmental conditions [8]. The activation can be performed manually by the driver through a switch or automatically, in case the car provides this functionality.

Out of the Hazard Analysis and Risk Assessment [9], a typical Safety Goal says that "while driving, loss of sufficient illumination level of the road shall be prevented" with ASIL B. A typical Safe State is "At least one low beam is ON". As emergency operation, it is required to inform the driver whenever possible via the Instrument Cluster. From this point on, the design of a Safety Concept is an open topic that we address in the followings.

Starting from [10] and [11] our proposed block diagram for the implementation of the low beam functionality is given in Figure 6. The Safety Concept includes a safety strategy to ensure the intended functionality and prevent violation of the safety goal, as well as a set of safety mechanisms to detect and control potential failures that could lead to the violation of the safety goal. Using guidelines presented in Annex D from ISO 26262 FE Part 5 [1], we propose for each block appropriate safety mechanisms.

For low beam control, the power supply is redundant in the sense that there are more than one physical input supply lines from the car battery. At the same time, to detect faults like *drift and oscillation*, *under and over voltage*, *power spikes*, safety mechanisms like *D.2.8. Voltage or current control* [1] shall be used for the supply chain to ensure proper functionality of the component blocks, especially the microcontroller and the output driver.

As the triggers for turning the two low beams (left and right) are the light switch and the ignition switch, the inputs coming from these switches have to be checked for *consistency*, *integrity* or *stuck condition*, by measures like *filtering*, *debouncing* and *pattern testing* according to measure set *D.2.6* [1].

Left & Right Headlamps

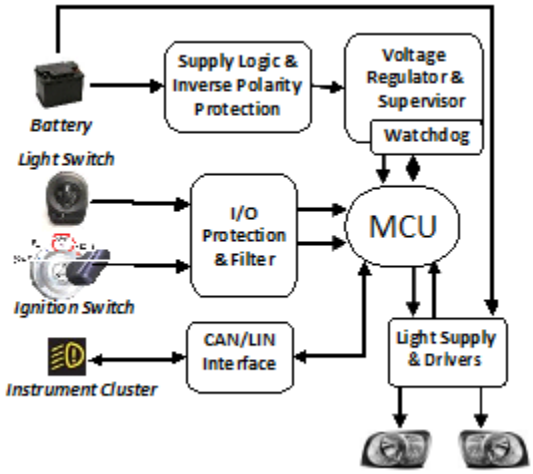

Figure 6. Low Beam control system architecture

The communication protocols, be it CAN, LIN or SPI, have to include mechanisms to cope with situations like *failures of communication peer*, *message delay*, *corruption* or *loss*, *unintended message repetition* or *insertion* [7]. The mechanisms shall include the so called end-2-end (E2E) protection by combining *D.2.7.6. Information redundancy*, *D.2.7.7. Frame counter*, and *D.2.7.8. Timeout monitoring* [1]. For the execution of the designed algorithms, the units that have to be monitored for possible failures are *D.4. Processing unit, D.10 Clock, D.5. ROM, D.6. RAM*. For the first two, the safety mechanisms proposed from section *D.2.9* of ISO 26262 Part 5 [1] are the *watchdog with separate time base* and the *logical monitoring of the program sequence*. For the memory related failures, several mechanisms have to be selected from sections *D.2.4* and *D.2.5*, e.g., *error- detection-correction codes, checksum, parity bit, block replication, double-inverted storage, RAM pattern/ march test*.

The blocks that are actually responsible for actuating the low beams are the ones related to voltage supply and output drivers, one set for each side, left and right. Moreover, with modern technologies, like LED or laser lighting, and increased complexity of the lighting functions, many manufacturers design separate ECUs especially for driving each of the headlamps. Although there are two such units, we state that ASIL decomposition is not feasible in general due to the fact that the units are similar, i.e., same design, same development. This situation falls into the category of the so-called homogeneous redundancy.

No matter they are separate units or blocks within same ECU, the light drivers have to satisfy same safety requirements. As such, the communication with the light drivers has to be reliable, the processing unit of the drivers has to also be reliable and they have to perform *diagnosis of the outputs* to insure proper command response. Thus,

mechanisms for communication, supply and processing similar to those previously described have to be implemented.

In addition, monitoring and feedback mechanisms have to be necessarily involved to detect possible failures like *open load*, *short circuits*, *voltage level*, *insufficient current intensity*.

VI. CONCLUSIONS

In this paper we determined what measures should be implemented within a Body Control Module to ensure the functional safety of the window lifter and low beam automotive functionalities. While a repository of general requirements is given within the ISO26262 standard, which measure is appropriate for a specific function is a difficult engineering topic that we tackled within this paper.

VII. ACKNOWLEDGMENT

Part of this work was supported by Continental Automotive Romania.

REFERENCES

[1] International Standards. (2011). *ISO 26262 Functional safety for road vehicles*. Geneva, Switzerland.

[2] A. Ismail, L. Qiang, “ISO 26262 automotive functional safety: issues and challenges”, International Journal of Reliability and Applications, vol. 15, no. 2, pp. 151-164, 2014

[3] J. Schwarz, J. Buechl, “Preparing the Future for Functional Safety of Automotive E/E-Systems”, 21st (ESV) International Technical Conference on the Enhanced Safety of Vehicles, pp. 1–3., 2009.

[4] B. Groza, H.E. Gurban, and M. Pal-Stefan, "Designing security for in-vehicle networks: a Body Control Module (BCM) centered viewpoint," on the 46th Annual IEEE/IFIP International Conference on *Dependable Systems and Networks Workshop*, 2016.

[5] T. Martinez, “Body Control Module,” Freescale, 2009, accessed 2018.04.01, https://www.nxp.com/files-static/training_pdf/WBNR_LA_AUTO_BCM_SPANISH.pdf

[6] Schwarz, J., “Functional Safety and Automotive Software – Introduction ISO 26262 Daimler”, 10th Workshop of Critical Software System, Tokyo, pp. 27-28, September 2012.

[7] J. Hedberg, A. Söderberg, T. Malm, M. Kivipuro, and H. Sivencrona, “Methods for Verification & Validation of time- triggered embedded systems,” Technical report NT TR 600, December 2005.

[8] Valeo, *Lighting Systems. From light to advanced vision technologies*, accessed 2018.04.01, https://static.valeoservice.systems/sites/default/files/catalog/lighting_systems_from_light_to_advanced_vision_technologies_technical_handbook_valeoscope_en_998542_web.pdf

[9] Autosar Standard, *Safety Use Case Example AUTOSAR CP Release 4.3.1*, accesed 2018.04.01, https://www.autosar.org/fileadmin/user_upload/standards/classic/4-3/ AUTOSAR_EXP_SafetyUseCase.pdf

[10] Texas Instruments, *Body Control Module. Reference Design*, accessed 2018.04.01, http://www.ti.com/solution/automotive_central_body_controller

[11] Renesas, *Body Control Module (BCM) / LED Head Light Unit*, accessed 2018.04.01, https://www.renesas.com/en-eu/solutions/automotive/body/body-control.html