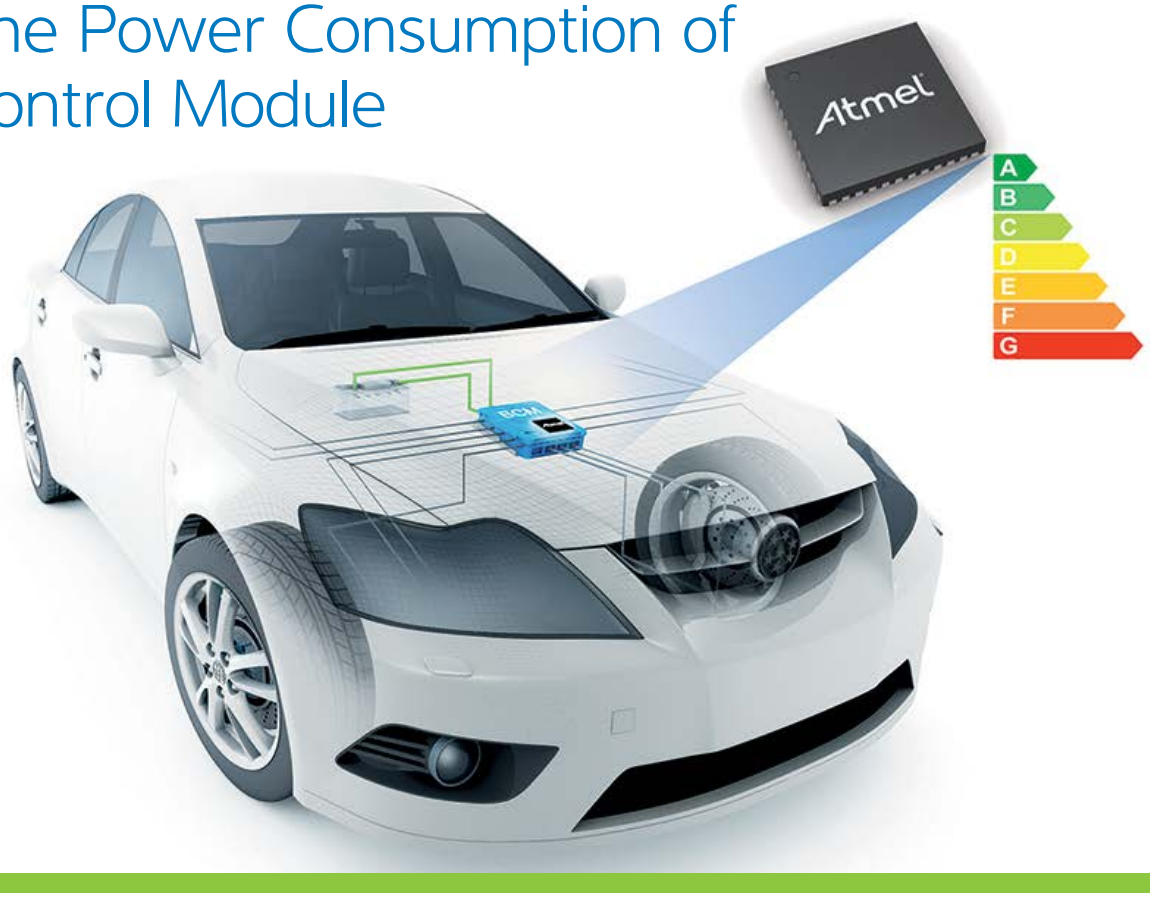
How Smart UHF Receivers Help to Reduce the Power Consumption of a Body Control Module

Dr. Peter Sauer



Overview

The Atmel® families of ATA578x UHF receiver (reference 1) and ATA583x UHF transceiver devices (reference 2) use an integrated 8-bit AVR® microcontroller to perform the UHF front-end control and the data processing during reception and transmission. These receiver and transceiver families include derivatives which have an embedded user-programmable Flash memory enabling the development of individual applications with the built-in ROM (read-only memory) firmware. All devices are configured with settings stored in an internal EEPROM (electrically erasable programmable read-only memory).

The main automotive application areas for these devices are:

1. Key fob applications with standalone operation using an internal Flash application
2. Receiver applications within or attached to a body control module (BCM)

This article focuses on the second application area where the receiver is part of or connected to a BCM. The CPU which controls the BCM application is typically a 32-bit microcontroller (MCU) with embedded memory. In this BCM application the UHF receiver is always powered on and is scanning (i.e., polling) for an RF signal from an associated key fob. This application, known as remote keyless entry (RKE), will unlock the vehicle doors when a valid key signal is detected. In addition the UHF receiver will search for data telegrams sent out by a tire pressure monitor system (TPMS). Figure 1 shows a BCM with typical functionality and interfaces to other car modules using CAN and/or LIN buses. The UHF receiver is directly connected to the MCU to activate the MCU in case of a detected key signal.

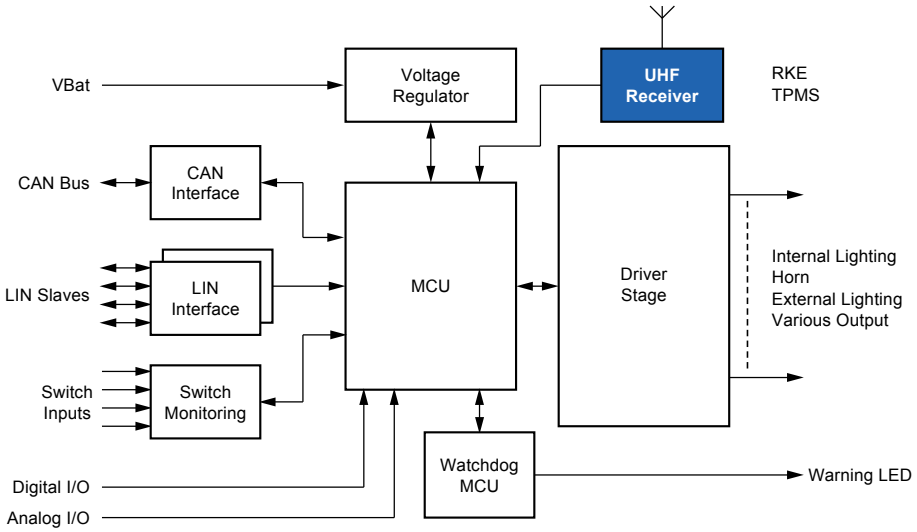


Figure 1. BCM with Integrated UHF Receiver for RKE and TPMS Signals

BCM Power Requirements During UHF Polling Mode

In the BCM example as shown in figure 1 the UHF receiver will receive two signals:

a) RKE: remote keyless entry signal to open the vehicle doors

b) TPMS: tire pressure monitoring system signal to receive the pressure values from the four vehicle tires

In the case of RKE, the signal is sent out from a key fob when the driver requests to unlock the car. In TPMS applications the signal is received at regular intervals where the interval time depends on the vehicle status. If the vehicle is moving, the TPMS signals are sent out more frequently than if parked. The TPMS signal is sent out as a burst sequence of data packets to ensure that the BCM will receive at least some of the data telegrams to validate the status of the tire pressure.

The critical parameter during the polling activity of the UHF receiver is the power consumption of the overall BCM system. When the car is locked and parked the BCM is in power-down mode where only the UHF receiver is polling for an RF signal. Once an RF signal with the correct data rate and data modulation scheme is detected in the expected RF channel, the BCM is switched into active mode to analyze the received data telegram. If a valid data telegram has been found the BCM unlocks the doors, otherwise it will return to power-down mode. The detection of false telegrams increases the overall power consumption which has to be avoided to save battery lifetime. The amount of detected false telegrams depends on the RF activity in the environment of the parked car. It will increase, for example, if the car is parked in the parking lot of a supermarket or at the car dealer.

The following example (see figure 2) details the power consumption over time with the following real-case data:

- UHF receiver:
  - Current consumption in active mode: Ia_{UHF} = 10mA
  - Polling cycle time: T_{poll} = 20ms
- BCM:
  - Current consumption in active mode: Ia_{BCM} = 150mA
  - Current consumption in power-down mode (including UHF receiver): Is_{BCM} = 2mA

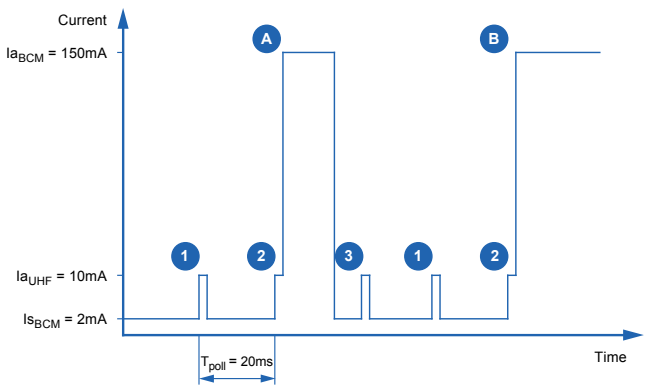


Figure 2. Current Consumption with Standard UHF Receiver Using BCM MCU for Data Processing

While the BCM is in power-down mode the UHF receiver operates in polling mode—"1", "2" and "3"—where the receiver is switched between standby mode and active mode every 20ms. Depending on the UHF receiver configuration, it will scan one or more UHF channels for a valid data telegram. The example in figure 2 shows the scanning of three channels "1", "2" and "3". This configuration is mainly defining the polling current, the mean current consumption of the UHF receiver. When the receiver detects a data telegram that fits the configuration with a correct RF channel, coding scheme, and data rate settings, the MCU switches to active mode ("A" and then "B") to analyze the data packet. If the data packet is not valid, the BCM will return to power-down mode "A", and the polling continues after this false wake-up. In case of a valid data packet "B" the MCU remains in active mode to open the doors and to activate the other car modules via the CAN and LIN buses.

BCM Power Improvement Using a Smart UHF Receiver

Car manufacturers define one main BCM requirement as low power consumption during power-down mode. To meet this requirement, BCM wake-ups caused by false telegrams need to be avoided. One way is by transferring the data validation task to the smart UHF receiver device. The current consumption of the active UHF receiver device is about 10-15 times less than that of the active BCM.

The smart UHF receiver includes an 8-bit Atmel AVR microcontroller with programmable Flash memory. The device is capable of carrying out the data pre-processing and analysis of the received data telegrams when you add or extend the integrated Flash application-specific software.

The following tasks can be performed by the UHF receiver device:

- Extend the ROM firmware with further control functionalities for the UHF front end; this will allow to implement enhanced data protocols
- Carry out data pre- or post-processing (AES data encryption and decryption)
- Perform control function, such as waking the BCM host up once the received data has been collected and validated
- Perform additional control functions for external devices such as using the GPIO (general purpose input/output) signals of the UHF receiver
- Add software-controlled data protocols such as the TWI protocol for external devices

The power consumption is improved if the smart UHF receiver takes over the data validation task from the BCM (figure 3) as compared to figure 2.

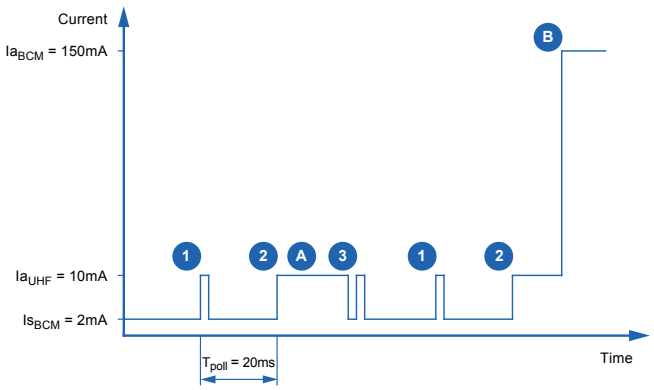


Figure 3. Current Consumption with Smart UHF Receiver Performing the Data Preprocessing

In this example, the smart UHF receiver checks the data packets "A" and "B". In case of an invalid data packet "A" the UHF receiver returns to polling mode without activating the MCU. If a valid data packet "B" has been detected, the MCU is activated to open the doors and to wake-up the other modules attached to the CAN and LIN buses.

Data Decryption Using a Smart UHF Receiver

The exchanged data is encrypted to ensure that the door locking and unlocking is only performed for a valid key fob. The validation of the data packets requires some additional computation effort to decrypt the data telegrams. With the Atmel open protocol an AES 128-bit encryption scheme is used to validate the key fob message (reference 3). The decryption of such a message takes about 18ms computation time that is performed by the 8-bit AVR MCU within the UHF receiver device. Compared to the BCM's MCU, which typically has a 32-bit CPU, the decoding takes longer but the activation of the 32-bit MCU would take even more time due to PLL initializations and RTOS activation tasks. Using data encryption within the UHF receiver, the overall current consumption can be reduced by a factor of 5 to 10.

The additional memory consumption for the AES decryption function is

- 1.5 kByte of Flash memory for the AES program code
- 100 bytes of additional SRAM data memory

The overall memory usage for the Flash application using the internal ROM functions is

- 2.6 kByte of Flash memory for program code
- 250 byte for SRAM data memory

The basic principle of such an encryption scheme (see figure 4) uses a data message that includes a message authentication code (MAC) which is generated by the 128bit AES encryption to validate the message data. This requires a secret key which is stored both in the UHF receiver and in the key fob's EEPROM. The AES-128 encryption is explained more detailed in the application note (see reference 3).

Data Frame Collection and Validation Using a Smart UHF Receiver

The typical data protocol used for RKE and TPMS functions defines the reception of multiple data frames for the validation of the data content. This increases the reliability of the data transfer in case of external disturbers or weak UHF signals.

An RKE data protocol operates on the UHF channels "B" and "C" (figure 5). A valid data reception is defined when the three data packets "a", "b", and "c" have been received. This requires the detection and reception of data packets on different UHF channels with the correct parameter settings. The smart UHF receiver collects the data frames in the expected sequence "a" to "c". Only if this data sequence is valid the BCM's MCU will be activated to unlock the doors.

A TPMS signal also works on the UHF channel "A" (see figure 5). A valid data reception requires the detection of a minimum number of data telegrams within a TPMS sensor's data packet burst "1" to "7". Once the minimum required number of data packets has been received and validated (data packets "2", "3" and "4" in this example), the MCU of the BCM will be activated to check the tire pressure data.

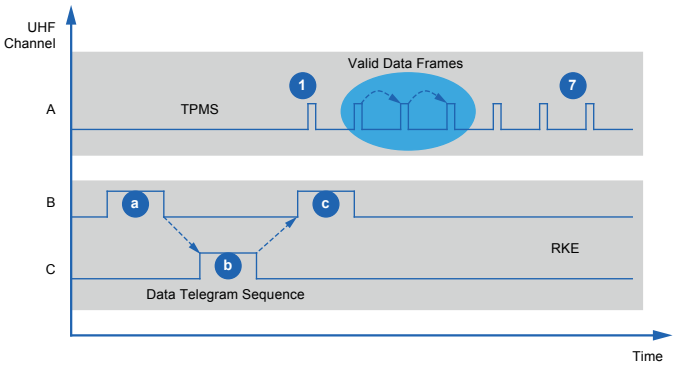


Figure 5. Collection of Data Frame Sequences for the Validation of RKE and TPMS Data

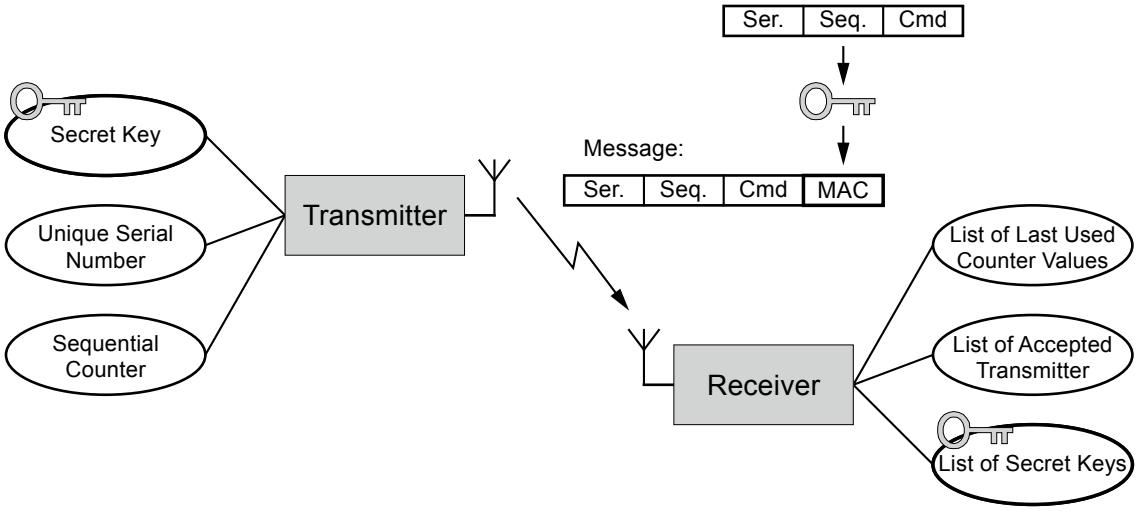


Figure 4. Basic Principle for an AES RKE Encryption Scheme (Reference 3)

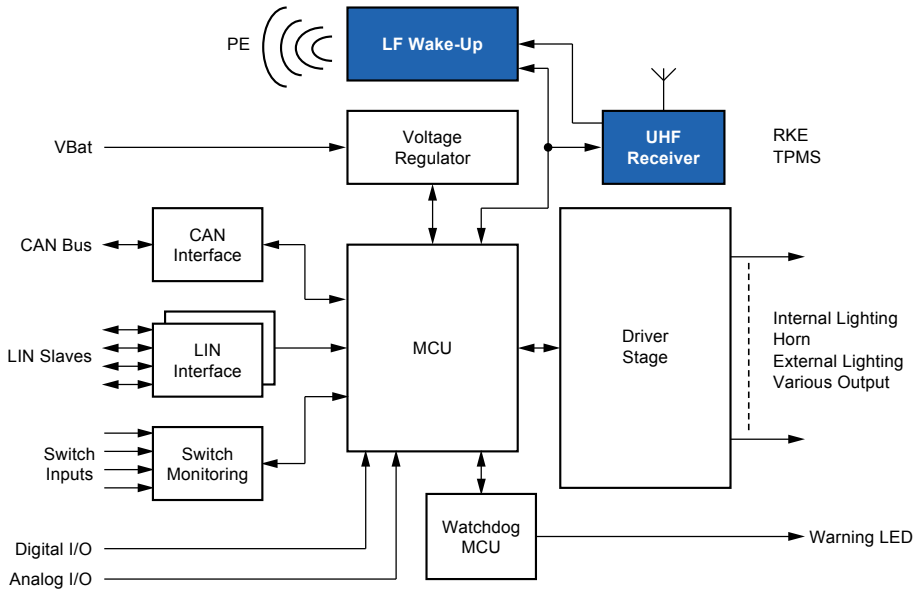


Figure 6. Passive Entry (PE) Functionality with the Smart UHF Receiver Concept as Shown in Figure 1

Passive Entry Systems Using a Smart UHF Receiver with LF Wake-Up

Future automotive passive entry systems may use the LF field to detect the approach of the driver carrying the key fob within a range of 2 to 3 meters. This requires an LF polling scheme to detect the approaching key fob. A typical LF data telegram will draw a current of up to 1A during LF field transmission. Such an architecture requires an even more sophisticated solution to keep the power consumption low.

Using the smart UHF receiver enables to initiate the LF polling sequence without the involvement of the BCM's MCU. An advanced LF driver circuit is needed that supports the automatic transmission of such LF data packets. The smart UHF receiver initiates the LF polling scheme by activating the LF driver device to send out the LF data telegram, and monitors the RF channels for a valid key-fob response. The smart UHF receiver and the LF driver device repeat this procedure autonomously in regular intervals without the activation of the MCU. For this scheme the LF driver device is connected to the smart UHF receiver (figure 6).

Summary

The smart UHF receiver and transceiver devices with their embedded microcontroller allow the implementation of application-specific programs in the user Flash memory. You can assign data transfer initiation and the validation of received data frames to these UHF devices. They perform pre-and post-processing at 10 to 15 times lower power consumption compared to handling these tasks in the BCM's MCU. Even in the case of upcoming car access applications such as using an LF wake-up, the Atmel UHF receiver/transmitter ICs combined with Atmel's smart LF devices will further reduce the power consumption.

References

(1) Datasheet ATA5781/2/3 family (http://www.atmel.com/Images/Atmel-9285s-Car-Access-ATA5831-ATA5832-ATA5833_Datasheet.pdf)

(2) Datasheet ATA5831/2/3 family (http://www.atmel.com/Images/Atmel-9285s-Car-Access-ATA5831-ATA5832-ATA5833_Datasheet.pdf)

(3) Application Note AVR411: Secure Rolling Code Algorithm for Wireless Link (http://www.atmel.com/Images/Atmel-2600-AVR411-Secure-Rolling-Code-Algorithm-for-Wireless-Link_Application-Note.pdf)