A HF Radio Frequency Identification Digital Controller Architecture

T.K.Cuong, N.P.Quoc, N.H.Quan
IC Design Research and Education Center
Vietnam National University-Ho Chi Minh City
Ho Chi Minh City, Vietnam

***Abstract*—A HF Radio Frequency Identification Digital Controller is designed as the central unit of the HF RFID Tag. It is compatible with the ISO/IEC 18000-3, the ISO/IEC 15693 and is successfully silicon proven. This design combines the analog module and the antenna module to form the complete tag. Our design supports most of the normal HF RFID Tag functions. Moreover, it has an error self-correction for the transmission and a special authentication method to improve the system security.**

***Keywords*—Tag, Radio Frequency Identification, HF.**

I. INTRODUCTION

The Radio-frequency identification (RFID) is the wireless contactless. The tag contains electronically stored information and uses the radio frequency electromagnetic fields to transfer data. RFID tags can be passive, active or battery assisted passive. Tags may either be read-only, or read/write, or write-once, read-multiple.

RFID tag contains an analog module, a digital controller module, a memory and an antenna module. The digital controller is the central control part of the tag.

Our tag design supports most of features described in ISO/IEC 18000-3. Besides, it has four additionally authenticate commands to divide the memory into many security levels. To do that, an authenticate flow and a security handling are inserted; they are what different make our products with other devices.

The overview of the HF Tag is shown on Figure 1.

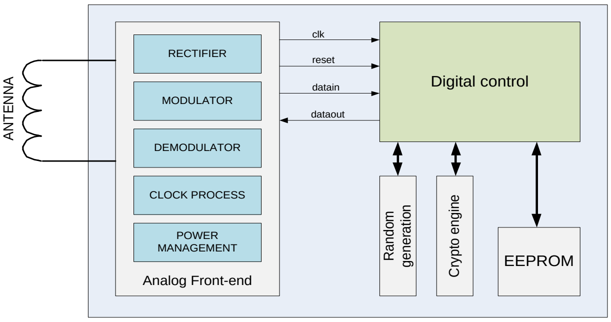

Fig. 1. HF RFID Tag overview

II. ARCHITECTURE

A. *Features*

- Compatible with ISO/IEC 18000-3 and ISO/IEC 15693.
- 13.56 MHz carrier frequency.
- Uplink:
    - 100% ASK modulation.
    - 1/4 pulse position coding (26 Kbit/s).
    - 1/256 pulse position coding (1.6 Kbit/s).
- Downlink:
    - Manchester coding with 423 kHz and 484 kHz subcarrier in Fast data rate (26 Kbit/s) and Low data rate (6.6 Kbit/s).
- 2K bit EEPROM with Lock Block features.
- 64-bit unique identifier.
- EAS (electronic article surveillance) features.
- READ block and WRITE block (32-bit blocks).

B. *Block Diagram*

The digital controller is the central unit of the tag. It receives the command from the reader, handles the request and data response to the reader. There are three main modules: the data process module, the data flow module and the memory controller module.

The data process module handles the receiving data command, gives the arranged data to the data flow module; it doesn’t care the content of the data. However, it modulates the output data and sends them to the analog modulation.

The data flow module analyzes the receiving command and gives the way to handle this command. It can either delete the corrupted command, or ignore, or respond to the reader. The data flow uses some functions such as: collision management, random generation, function calculation, and authentication to access the request from reader.

The memory controller manages the access of the EEPROM. Besides, the clock generator module divides and manages the system clock of the design and the reset generator manages the reset signal when full power received.

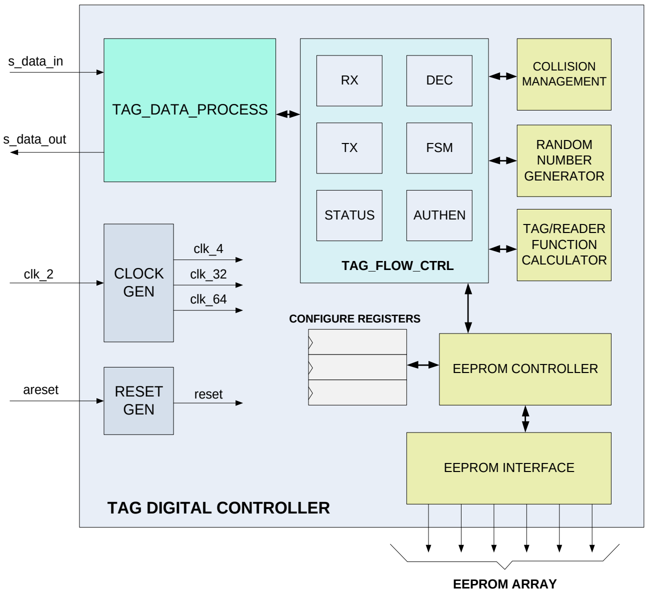

Fig. 2. Digital controller module

C. Commands

Our design supports most of the command described on the ISO/IEC 18000-3. The structure of normal command is shown on the figure 3.

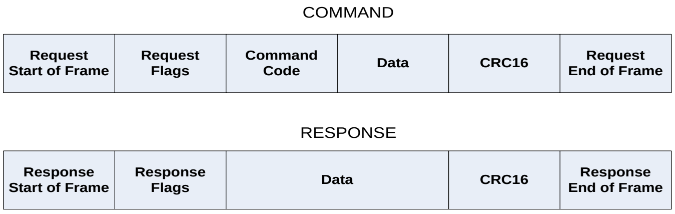

Fig. 3. Command and Response structure

One command fails if receiving timing failure, or CRC failure, or not supported command. All commands below are supported in our design:

TABLE I. TAG COMMANDS

Command	Command code
Inventory	0x01
Stay quiet	0x02
Select	0x25
Reset to ready	0x26
Write block	0x21
Lock block	0x22
Read multi block	0x23
Write AFI	0x27
Set EAS (based AFI)	0x27
Reset EAS (based AFI)	0x27
EAS Alarm Inventory	0x01
Authentication1	0xF0
Authentication2	0xF1
Write secure	0xF2
Read multi secure	0xF3

Four commands: The Authentication1, the Authentication2, the Write secure and the Read-multi secure are special commands that only in our design. These commands are designed for user’s private purpose. Their detail is described in the following.

III. ANALYSIS

A. Data Detection and Modulation

The Tag can detect data from reader in two data modes: 1/256 and 1/4. The base clock is divided by 4 to generate the sample clock. The lower clock increases the error rate but it saves the power consumption. The clock divisor ratio is chosen highest possible depending on the limit data error ratio.

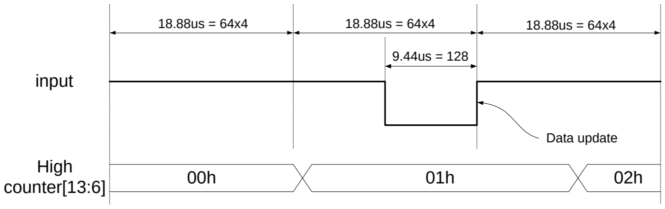

Fig. 4. Data detection in 1/256 mode (example data 0x01h)

The detection counter is 14 bits wide. This number is enough to the longest timing (4.833 ms). We separate the counter into two parts: the unit part with 5 bits and the half-data part with 9 bits. The unit part detects in one modulation time (9.44 us).

The operation of the detection counter is described on Figure 4 (1/256 mode) and Figure 5 (1/4 mode). The valid data are temporarily saved in the data buffer at the rising edge modulation and loaded at the end of the detection period time (4.833 ms in 1/256 mode or 75.52 ms in 1/4 mode).

At the modulation time, there is no clock, because of the lost power. The counter doesn’t count in 9.44 us, so the total counter steps calculated with sample clock is 16288 (64*255-32) or 224 (64*4-32).

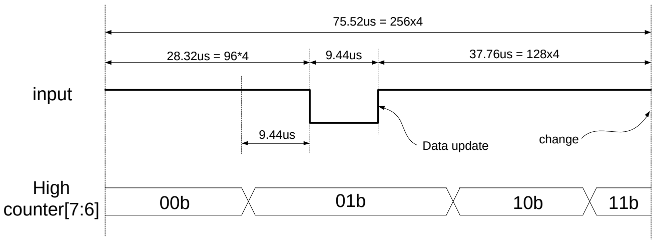

Fig. 5. Data detection in 1/4 mode (example data 0x01b)

B. Error correction

When detecting sequential data packet, the counter may accumulate the remaining time of the previous packets. The remaining time causes the error if it is higher than 9.44 us. In some cases, one detection period is shorter than the standard, because of noise or other reason.

The remaining time of previous packet occurs because of the analog error modulation in falling/rising edge of the input line. It makes 8 times for falling edge and 6 times for rising edge. At the result, the maximum error cycle for each modulation is 14 clock cycles (10.9 %).

The reset time and reset value of the unit counter is the key of self-correction method. The unit counter is reset/set at the end of each detection period time (not reset/set at the rising edge of the input data). Depending on the remaining number in the unit counter at the reset/set time, the unit counter maybe reset to 0x00h or set to 0x1Eh. The error time can be corrected is maximum 4.72 us.

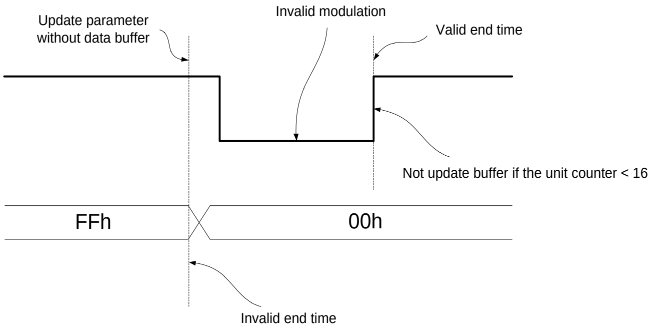
Update parameter without data buffer
Invalid modulation
Valid end time
Not update buffer if the unit counter < 16
FFh
00h
Invalid end time

Fig. 6. Error in the last phase

One special case occurs in detecting 0xFFh value (1/256 mode) or 0x11b (1/4 mode) with lacked timing (Figure 6), the data buffer isn't updated with the truth value even when finishing data frame and the modulation falls in the next frame (two modulations in one data frame). We use one status bit to determine the 0xFFh value (or 0x11b) and the remaining counter number time at the 0x00h data frame to remove the invalid modulation.

C. Authentication and security

The authentication and security method is used to limit the access right to the EEPROM memory. Normal user only accesses the simple task such as: read UID, read/write free user space. To access to other spaces, the user must authenticate by master key, or super key or normal key. In some cases, one space memory is written only one time and never written again.

For the secure command, signed-CRC is the enciphered CRC which is combined from normal CRC and a secure key (Master key, Super Key, User key 0, User key 1 or User Key 2). Signed-CRC is used into write secure, read multi secure, master authentication 1, master authentication 2, master authentication 3 and master authentication 4 command.

D. Tag access

The Tag memory is separated from many part, each part has the different access. All tag access levels relate to the secure bit and the recent status of the tag. There are two main access levels:

- The master access rights: the hide and secret mode and designed for manufacture. These accesses are authenticated with two 96-bit master keys by special protocol.
- The user access rights: the public mode and has three levels: the supper user access, the normal-user access and the free-user access.

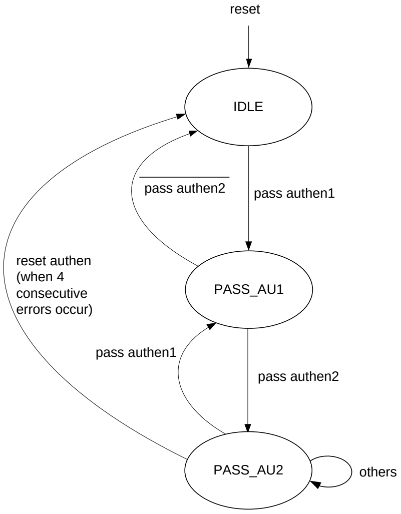

Fig. 7. User authentication process

Super key authenticate policy

Super key is used in the super user access mode. This mode can access all parts in the memory, while the user key is only used for the corresponding memory part. Super key is used to authenticate as following policy:

- The reader sends the authentication command to the tag and specifies which secure key is used.
- The tag generates a 48-bit random number and sends it to the reader.
- The reader generates another 48-bit random number and calculates the functions TF (TRN, RRN, Key) and RF (TRN, RRN, Key) and then, responds to the tag by transmitting R and TF (TRN, RRN, Key).
- The tag compares TF (TRN, RRN, Key) transmitted by the reader and TF' (TRN, RRN, Key) that it has calculated. If TF=TF', the tag calculates the functions RF' (TRN, RRN, Key) and sends it to the reader.
- The reader compares RF' (TRN, RRN, key) and RF (TRN, RRN, Key) calculated before. If RF=RF' then the reader confirmed.

E. Memory Controller

Our design contains 2KB EEPROM that be controlled through the EEPROM Interface and EEPROM Controller. The Figure 8 describes the basic diagram and connection signals between the tag and the EEPROM components.

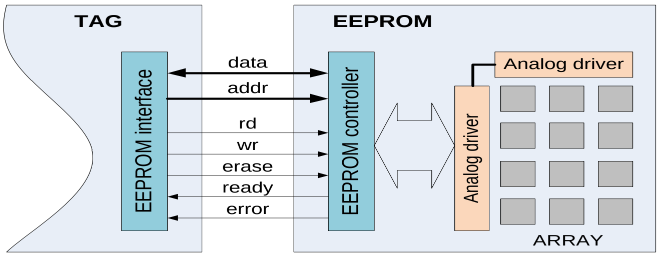

Fig. 8. EEPROM Digital Components

EEPROM interface is used to access (erase/read/write) EEPROM. All its signals are connected to EEPROM controller of EEPROM memory.

EEPROM controller is the digital controller of EEPROM, which implements the access mechanism of EEPROM. It is connected to the analog driver which drives directional the EEPROM array.

IV. Conclusion

This paper introduces the architecture of the central control of the HF RFID Tag that runs well on FPGA and is successfully silicon proven. In addition to the conventional features, our design possesses some enhanced methods to improve system security and flexible usage.

The design, with more sophisticated tools similar to LEDA, VCS… of Synopsys, will be used for a complete test of the design before manufacturing.

V. Acknowledgement

We are indebted to Prof. Dr. Dang Luong Mo, advisor of VNU-HCM and ICDREC, for taking his time to thoroughly read our manuscript, help rewording it and finally reshaping it into the present form.

We would like to thank the Verification team, the Physical team and the Analog team of ICDREC for engineering support in the implementation of our design.

References

[1] ISO/IEC 18000, Part 3, Information Technology AIDC Techniques – RFID for Item Management – Air Interface, Part 3 – “Parameters for Air Interface Communications at 13.56 MHz”.

[2] ISO/IEC CD 15693-3, Identification Card – Contactless integrated circuit(s) cards – Vicinity cards – Part 3: “Anti-collision and transmission protocol”.

[3] STMicroelectronic Inc, “ISO 15693 standard compliant, 13.56 MHz, 512 bit, high-endurance EEPROM TAG IC with EAS”, November 2007.