Online Testing of RFID Memories by Using March SS-BIST

1.P.Amani, 2.Dr.Gurunadha Babu,,Ph.D
1M.Tech Student In ECE Department At CMRIT,Hydearabad, amani.polumati@gmail.com, ,
2.HOD Of ECE Department At CMRIT,Hydearabad, ecehod.cmrit@gmail.com

Abstract—Radio Frequency Identification (RFID) devices depend on the correct operation of their memory for guaranteeing accurate identification and delivery of transponder's information. In this paper, a novel approach for online testing of RFIDs based on March-BIST techniques for EEPROMs is presented. Online test is achieved by modifying the transponder's operation and access protocol to exploit the waiting time that transponders waste before being accessed. The solution was described in VHDL, simulated and synthesized to obtain area and timing results. A novel access scheme supporting online test for RFIDs was presented. The novel scheme takes advantages of the idle state of transponders while waiting to be accessed by the interrogator to perform the test of their internal memory. The transponder finite state machine describing the access scheme was presented and the architecture of the transparent BIST circuit was described. March algorithms are widely used because March algorithms provides high faults coverage and easy to implement with these architectures. In this paper we discuss about implementation of March ss algorithm for memory .BIST architecture based on finite sate machine. Timing results present the maximum size of blocks that can be tested within one slot of the accessing scheme by considering two different march algorithms.

I.INTRODUCTION

The memory BIST approach is commonly used because it provides efficient, less costly and speed testing solution for memory. the Built-in self -test approach eliminates the need of external test equipment .the memory BIST provides several advantages such as high fault coverage ,high speed testing ,low area and low cost than other testing methods. There are several testing algorithms are used for memory testing but .the march algorithms are preferred over other test algorithms because march algorithms are easy to implement with BIST and better fault coverage .the FSM based memory BIST having advantage of speed testing small area and compact but less flexibility .

Radio frequency identification devices are the main devices are the main constituting actors in the internet of things paradigm where they are used to face the challenges of labeling physical objects to allow them to participate in the digital world such RFID devices rely on their memory to accomplish their function which range from the simple read-only transponder to the high end transponder with intelligent cryptological modules.

Read-only transponders represent the low-end, low-cost segment of the range of RFID data carriers. As soon as such transponder enters the interrogation zone of a reader, a scheme to access its identification number is deployed. The tag's unique identification number is hardwired into the transponder during chip manufacture; therefore, the user cannot alter this serial number, nor any data on the chip. Writable transponders can be written by the interrogator and their memory may have several kilobits. Write and read access to the transponder is often performed in blocks of, usually, 16 bits, as in the EPC Class 1 Generation 2 protocol (C1G2) [2]. Recent developments aim at increasing RFID data rate to 10 Mbps, which entails the possibility of incrementing memory capacity to 1 Mbyte or more [3]. Considering the trend to increase memory capacity in RFIDs, a new RFID architecture and access scheme is proposed that allows concurrent online tests of the transponder memory. A built-in self-test (BIST) controller with appropriate march-tests is carefully exploited to check for memory errors. The following of this paper is organized as follows. In Section II, the general operation of the Transponder and the typical organization of its memory are presented. Section III describes the regular accessing scheme of the transponder and the modifications proposed to allow the online test of the memory. Section IV. Description of the March algorithm utilized is shown and the BIST architecture is introduced. Section V.BIST implementation .VI. Simulation results

II. RELATED WORK

In the application layer, the transponder receives commands from the interrogator that are valid only when the tag has been singled out. These commands generally consist of writing, reading or locking the tag's internal memory. At this layer, an interrogator may be able to terminate indefinitely the tag's operation by issuing a password-protected command.

The communication layer allows an interrogator to manage tag populations while embracing an anti-collision protocol. A great number of tags may be controlled by supervising tag's data collisions. A regular scheme to avoid collisions employs a two-part scheme where an interrogator, first, selects a broad number of tags and, subsequently, forces them to randomly choose access slots. This access mechanism is employed within the EPC C1G2 protocol and is based in the Dynamic Framed Slotted ALOHA algorithm (DFSA) [4]. To support access from several interrogators, transponders provide session. Transponder memory is organized in agreement with different standards, but, commonly, it follows a division in banks according to the function of the memory portion as follows:

- Reserved memory, which includes passwords for accessing special tag functions.
- Product Identification memory, which is a code

used to identify the object containing the tag.

- Tag Identifier memory, which is the unique identification number of the tag.
- User memory, which is an application specific bank.

III CONCURRENT TEST STATE ACCESSSCHEME

A selection command issued by the interrogator impels a tag or group of tags to set or unset their internal flags according to a comparison mask. In this way, an interrogator is able to split in smallest sets a larger group of tags in order to access them easily. Typically, an interrogator starts a new inventory pointing towards a previously selected set of tags. Transponders matching the interrogator's flags selection must generate an internal random Queue Position Number (QPN) which represents its assigned slot in the DFSA algorithm. The maximum QPN available for the transponders is determined by the interrogator each time an inventory starts. In order to establish a direct link interrogator -transponder, the interrogator sends a command which is answered only by transponders which QPN is equal to zero. Meanwhile, the other transponders involved in the inventory should decrement their own QPN by one, until their turn to answer the interrogator comes. The success of the anti-collission scheme relies in the effectiveness of the interrogator to select an appropriate maximum value for the QPN which avoids picking the same time slot by more than one transponder. Selection Stage, Every transponder works in one of four sessions and has separate inventoried flag for each. These flags determine whether the transponder may respond to the interrogator or not within an inventory round. A Selected flag (SL) also exists which purpose is to ensure a greater accuracy during management of large transponder populations. The proposed scheme introduces a Test flag which can be asserted by the interrogator to force transponders to a testing state while being accessed.

Testing Stage Fig. 1 shows the proposed finite state machine (FSM) of the transponder access scheme. Once a transponder is within the range of an interrogator, it reaches the Ready state. The Ready state is a holding state for energized transponders that are not participating in an inventory round. A transponder that is in Ready state accepts Select commands from the interrogator that force it to set or unset session flags. The proposed testing approach includes a new state for testing, MemTest, which sends a signal to a BIST controller to start the test of a given memory block and keeps track of its result. To prevent unwanted behavior, a transponder ti in the MemTest state reacts only to the QueryRep command which forces the decrement of QPNi, i.e., changes to the next time slot. An extra 32-bit register is implemented in the transponder to be used as a memory block counter during the test process. The information regarding the memory block to test is sent through data lines towards the BIST.

When the test is finished, the transponder transits to the Arbitrate state to continue with the regular operation related to accessing its information. In order to inform the interrogator that an error has been detected, the transponder should transit to the Reply state while sending a temporary random identifier accompanied with an error code. The error code describes the nature of the error and the place where it has been detected as well. In case of no error detection or while in regular operation, the transponder should backscatter only the temporary identifier.

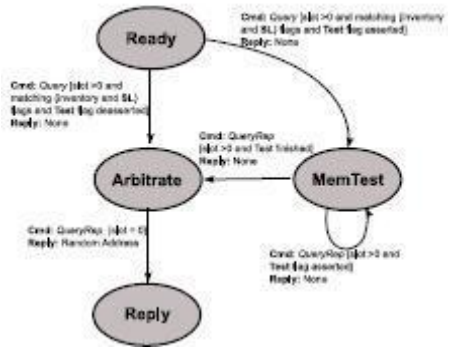


Figure 1. Proposed FSM Transponder access scheme with concurrent test state.

IV. MARCH TEST

A march test contains a sequence of march elements which is composed by a read/write operation that have to be performed into every cell of the memory. March tests are able to detect several fault models such as Stuck-at Faults (SAF), Address Faults (AF) and some Coupling Faults (CF). The operations that can be executed in the cells may be: write zero (w0), write one (w1), read zero (r0) and read one (r1). The read operation checks if the value inside the cell is the expected one. The order in which cells are considered can be ascending or descending. A typical march test used to test RAMs is MARCH c- which can be adapted to test also EEPROMs. The MARCH c- algorithm is described as follows

$$\uparrow w0\ \uparrow (r0, w1)\ \uparrow (r1,w0)\ \downarrow (r0, w1)\ \downarrow (r1,w0)\ \downarrow r0$$

word-oriented memories, such the ones found in an RFID, need a slightly different approach. By extending the 0 or 1 to 16 bits, march algorithm can be easily applied to RFID's word-oriented memories with a reduction on the coverage of CF.

The stuck–at 1 fault is detected by writing 0(w0) to memory location and then reading expected value o(R0);if it is not matched then it is known as stuck-at 1 fault. The stuck–at 0 fault is detected by writing 1(W1) to the memory location and reading expected value 1(R1);if it is not matched then it is known as stuck–at 0 fault

The faults that are covered in the MARCH C- Algorithm are Address Faults (AF), Stuck At Faults (SAF), Transition Faults (TF), Inversion Coupling Faults (CFin), Idempotent Coupling Faults (CFid), State Coupling Faults (CFst).

Some such newly defined fault models are Write Disturb Fault (WDF), Transition Coupling Fault (Cft), Deceptive Read Disturb Coupling Fault (Cfdrd). Another class of faults called Dynamic faults which require more than one operation to be performed sequentially in time in order to be sensitized have also been defined. These new faults cannot be easily detected by established tests like March C-, rendering it insufficient/ inadequate for today's and the future high speed memories. More appropriate test algorithms like March SS have been developed to deal with these new fault models. While March SS covers some of the new fault models like Deceptive Read Destructive fault (DRDF), Write disturb fault (WDF), etc.,

Symmetric Transparent Test

A Regular march test produces the erase of the contents in the memory. To prevent losing data a transparent approach is introduced. The transparent method avoids traditional comparison and, instead, uses a signature analysis mechanism based on a feedback shift register [6]. Well-known march tests can be easily extended to transparent versions by replacing values 0 and 1, in the read and write operations, by a and ac, respectively, where a refers to original content and ac to its complement. Besides this modification, the initialization part in the original march test should be removed. A symmetric transparent test poses a constraint on the symmetry of the march test, e.g., it should have the same number of reading for the original and the complement content, since the signature mechanism computes the signature when fed by the original content and computes the reciprocal signature when fed by the complementary content. By doing so, the initial state of the signature mechanism should be found at the end of the test when the memory is fault free. messages) in all the sessions. With Jetty as the underlying

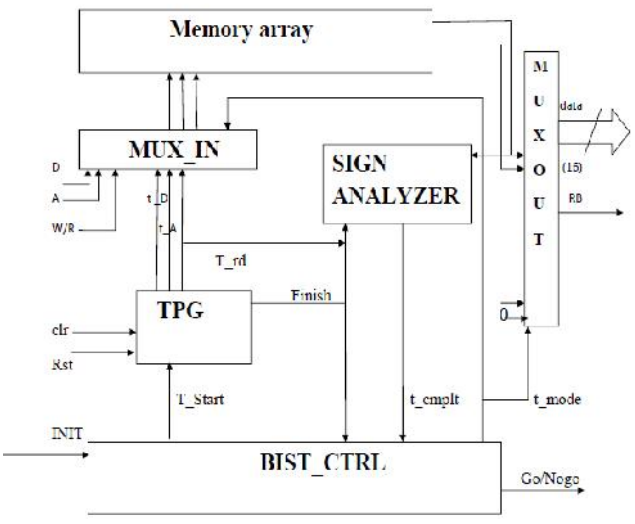


Figure 2. Architecture of thememory module with the BIST controller.

In the proposed FSM based Memory BIST, bist_en, clk, re-set, faultdetect and bist_end are basic signals. If bist_en sig-nal goes to high, then proposed BIST is come into the work mode. The clk signal implies the clock pulse applied to the circuit. The faultdetect signal indicates the detection of fault. The bist_end signal indicates completion of March algorithm. If bist_en signal set to 1, reset signal set to 0, clk signal is applied and March algorithm is selected then write or read operations are performed onto memory locations in either ascending or descending address order, depends upon March algorithm se-quence. The output of memory is compared with the expected data using comparator block, if it is not matched then it pro-duces faultdetect signal to high and else it produces faultdetect signal to low. After performing all operations of March algorithm the BIST circuit produces the bist_end signal to high.

V. BIST IMPLEMENTATION

Figure 2 shows the architecture of the BIST module composed by six entities: offset generator, memory input multiplexer, output multiplexer, BIST controller, signature analyzer and test pattern generator.

The function of the input multiplexer is to choose which signals input to the memory according to the BIST mode. The output multiplexer provides constant values and the ready/busy(RB) signal is set to zero throughout all the test period. The offset generator is a module that modifies incoming address depending on the bank selected for the memory during regular operation. The BIST controller captures the init signal from the transponder's FSM and starts the test procedure. The test pattern generator id responsible for generating the test vectors to be introduced to the memory .it contains the sequence and direction of the march test in a configuration array its implementation consists of a FSM which takes information from the complement of the data read from the memory is used as input when needed

The signature analyzer is a Multiple Input Shift Register (MISR) with a flow signal that sets its direction of propagation. This implementation avoids the use of two different shift registers for the signature and the reciprocal signature computation. To reduce the probability of error masking, an irreducible polynomial was selected for the MISR; it has the following form:

$$h(x) = 1 + x^7 + x^9 + x^{12} + x^{16}$$

Additional methods to avoid error masking involves hardware solutions, e.g., additional check parity, the use of hamming codes or larger MISRs, which are undesirable for the constrained RFID system due their overhead.

To evaluate the timing performance of the circuit two march tests were executed ;the march c- algorithm described before and the march ss algorithm .the march ss algorithm has a higher complexity than march c- and is described in the following in its transparent version ;

$$\uparrow (r_a^c) \uparrow (r_a, r_a, w_a, r_a, w_a^c) \uparrow (r_a^c, r_a^c, w_a^c, r_a^c, w_a) \downarrow (r_a, r_a, w_a, r_a, w_a^c) \downarrow (r_a^c, r_a^c, w_a^c, r_a^c, w_a) \downarrow (r_a)$$

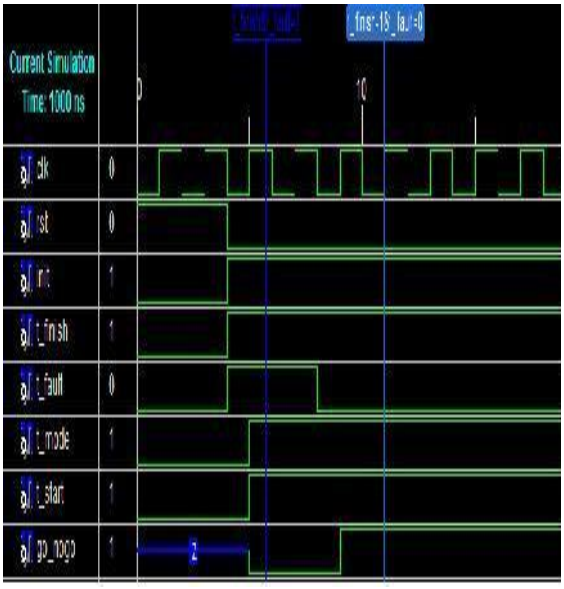
VI.SIMULATION RESULTS

The proposed scheme was synthesized and simulated in order to evaluate its performance regarding timing and area synthesized using a 0,65 _m technology. The BIST used the transponder's internal clock signal which is obtained from the interrogator carrier frequency, and was chosen equal to 1

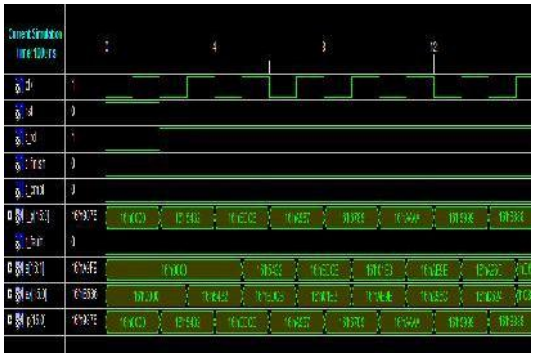
MHz. The evaluation of the area overhead was calculated considering the memory since it is the largest component of the transponder. A memory capacity of 1 kB was assumed, which is, in average, larger than the capacity of most of current passive transponders. The area overhead was computed as

AO = BIST Area /Memory Area * 100%. To obtain realistic values for the memory area, the data was extrapolated from [7]. To evaluate the timing performance of the circuit two march tests were executed: the march c- algorithm, described before, and the March ss algorithm. The March ss algorithm has a higher complexity than March c- .

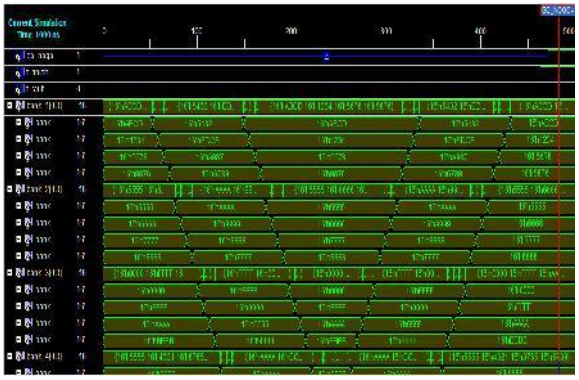
The simulations were performed varying the testing block sizes. Furthermore, the timing information of the basic approach is also presented to compare with the transparent approach. The 20 ms threshold is also highlighted for convenience. As can be seen in the simulations results, the absence of the initialization stage in the transparent approach provides an interesting reduction of test time. In average, the time is reduced by 20.5 % for the March C algorithm and 18% march-ss. These simulations show the maximum block size which can be tested within one single slot according to the algorithm utilized. Synthesis and simulation results show the feasibility of the proposed scheme. Area results show the negligible overhead of the BIST in terms of area compared with the memory size, i.e., about 0.1 %. Timing results present the maximum size of blocks that can be tested within one slot of the accessing scheme by considering two different march algorithms. Future work will include other testing approaches which provide a direct testing command to the interrogator and a larger list of supported march algorithms.



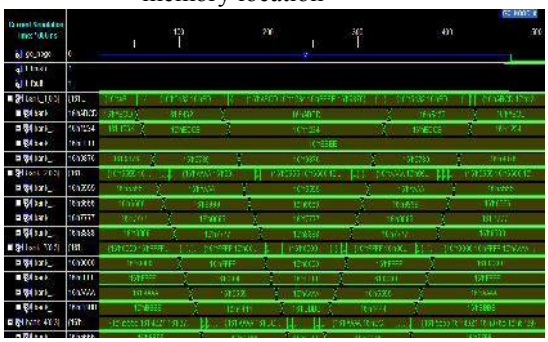
simulation waveform for the BIST_CTRL



simulation waveform for the MISR



: simulation waveform for the FSM without fault in the memory location



simulation waveform for the FSM with fault in the memory location

REFERENCE

[1] E. Welbourne, L. Battle, G. Cole, K. Gould, K. Rector, S. Raymer, M. Balazinska, and G. Borriello, "Building the internet of things using rfid: The rfid ecosystem experience," Internet Computing, IEEE, vol. 13, no. 3, pp. 48–55, may-june 2009.

[2] EPCGlobal, EPC radio-frequency identity protocols Class-1 Generation-2 UHF RFID air interface Version 1.2.0, Oct. 2008.

[3] J. McDonnell, J. Waters, H. Balinsky, R. Castle, F. Dickin, W. W. Loh,and K. Shepherd, "Memory spot: A labeling technology," Pervasive Computing, IEEE, vol. 9, no. 2, pp. 11–17, april-june 2010. [12] R. Schatz, S. Wagner, S. Egger, and N. Jordan, "Mobile TV becomes Social - Integrating Content with Communications," in Proc. of ITI, 2007.

[4] T. Cheng and L. Jin, "Analysis and simulation of rfid anti-collision algorithms,"in Advanced Communication Technology, The 9th International Conference on, vol. 1, 2007, pp. 697–701.

[5] M. L. Bushnell and V. D. Agrawal, Essentials of Electronic Testing for Digital, Memory and Mixed-Signal VLSI Circuits. Springer, 2000.

[6] S. Hellebrand, H.-J. Wunderlich, and V. Yarmolik, "Symmetric transparent bist for rams," Design, Automation and Test in Europe Conference and Exhibition, vol. 0, p. 702, 1999.

[7] D. R. Banerjee, S; Chowdhury, "Built-in self-test for flash memory embedded in soc," in Third IEEE International Workshop on Electronic Design, Test and Applications, DELTA 2006., January 2006.

[8] U. Karthaus and M. Fischer, "Fully integrated passive uhf rfid transponder ic with 16.7- mu;w minimum rf input power," Solid-State Circuits, IEEEJournal of, vol. 38, no. 10, pp. 1602 – 1608, 2003.