

AN EXPOSURE TOWARDS FAULT TOLERANT MEMORY SYSTEM



K.Subbareddy

Email: subbu.177@gmail.com

K.Satish

Email:ksatishd09@gmail.com

ABSTRACT:

There has been a rising demand for well-organized and reliable digital storage as well as transmission systems in the recent years. Only memory cells were vulnerable to faults of transient in addition to the supporting circuitry around the memory however due to the enhance in the rate of soft error in logic circuits, the decoder circuitry and encoder around the memory blocks have also turn out to be susceptible to soft errors and have to be protected. A novel approach which is competent of tolerating errors not simply in the memory bits but also in the supporting logic was introduced. Architecture of fault tolerant memory which put up with transient faults both in storage unit and in the supporting logic was introduced. The unit of Fault Secure Detector is used to make sure the output vector of the decoder circuitry and the encoder. A class of Error Correcting Codes whose redundancy formulates the design of Fault Secure Detector easy is introduced and this type of error correcting codes known as fault secure detector capable ECC. The codes of Euclidean Geometry Low Density Parity Check have the fault secure detector ability and by means of the small codes of Euclidean Geometry Low Density Parity Check (15, 7, 5) up to 2 errors can be acceptable and correct codeword can be re-written subsequent to correcting it. The organization can correct together the errors at same time in single clock by means of the parallel architecture of the corrector in which all 15 corrector circuits function at similar time.

Keywords: *Memory cells, Fault tolerant memory, Error Correcting Codes, Fault Secure Detector.*

1. INTRODUCTION:

Memory cells have been secluded from soft errors due to the enhance in the rate of soft error in logic circuits, the decoder circuitry around the memory blocks and encoder have turn out to be susceptible to soft errors and have to also be secluded. A novel approach is introduced to intend fault-secure encoder and decoder circuitry intended for designs of memory. Hamming codes are frequently used in the present day's memory systems to accurate

single error and become aware of double errors in any memory word. In these architectures of memory, only errors in the memory words are accepted and there is no training to tolerate errors in the sustaining logic. Combinational logic has by now started performing susceptibility to soft errors, and as a result the encoder and the units of corrector will no longer be protected from the transient faults. Consequently, defending the memory systems support logic implementation is additionally significant. A system of fault tolerant memory is introduced that tolerates numerous errors in each memory word in addition to numerous errors in the encoder and the units of corrector [4]. Error detection and correction or error control is method that enables consistent delivery of digital data over undependable communication channels. Error detection is the discovery of errors caused by means of noise or other impairments throughout transmission from the transmitter towards the receiver. Error correction is the discovery of errors in addition to reconstruction of the innovative, error-free information. Error Correction Codes (ECC) is a method that is used to distinguish and correct errors which are introduced throughout storage or transmission of information [8]. Various kinds of RAM chips within a computer put into practice this system to accurate the data errors and known as ECC Memory. The chips of ECC Memory are mainly used in servers rather than in computers of client. A class of error-correcting codes is recognized that assures the existence of a simple designs of fault-tolerant detector. This class convinces a novel, restricted explanation for ECCs which assures that the codeword of ECC has a suitable redundancy organization such that it can notice numerous errors occurring in both the accumulated codeword in memory and the nearby circuitries [1]. This type of codes of error-correcting are known to be fault-secure detector capable ECCs. The parity-check Matrix of a fault-secure detector capable ECCs has a meticulous organization that the decoder circuit, created from

matrix of parity-check, is Fault-Secure.

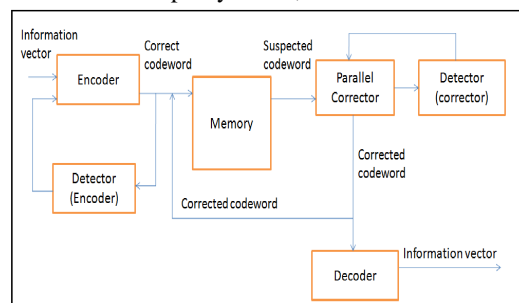


Fig1: An overview of architecture of fault-tolerant memory system.

2. METHODOLOGY:

The design of memory system that can put up with errors in any part of the system is summarized, including the storage unit, encoder in addition to corrector circuits using the detector of fault-secure [3]. Design is practicable when the subsequent two basic properties are fulfilled such as: Any single error within the corrector circuitry or encoder can at most corrupt a single bit of codeword; there is a fault protected detector that can notice any combination of errors in the codeword which was received all along with errors within the detector circuit. This detector of fault-secure can confirm the accuracy of the encoder and corrector process. The initial property is effortlessly satisfied by means of preventing logic sharing among the circuits producing each bit of codeword or bit of information within the encoder and the corrector correspondingly [9]. An outline of the proposed system of reliable memory is revealed in fig1. The bits of information are fed into the encoder to instruct the information vector; in addition the fault secure detector of the encoder confirms the validity of the vector encoded. If the detector notices any error, the operation of encoding has to be redone to produce the accurate codeword. The codeword is subsequently stored in the memory. During the operation of memory access, the code words that are stored will be accessed from the unit of memory. Code words are vulnerable to faults of transient while they are accumulated in the memory; consequently a corrector unit is considered to accurate the errors of potential in the retrieved code words [7]. All the memory words pass all the way through the corrector and any potential error within the memory words will be approved. Comparable to the unit of encoder, a fault-secure detector examines the corrector unit operation. In the encoder an n-bit codeword (c) is created by means of multiplying the k-bit information vector (i) by bit generator matrix (G). $c = i \cdot G$; $G = [I_k | P]$. Where I = Identity Matrix (k x k); P = Parity Check Bits (k x (n-k)). The codeword

of n bit consists of “k” information bits followed by means of “(n-k)” parity bits. The codes of Euclidean Geometry are known as EG-LDPC codes which are based on the information that they are the codes of low-density parity-check containing a limited number of 1’s in every row as well as column of the matrix; this bound guarantees restricted complexity in their connected detectors and correctors building them quick and light weight [2]. In the fault secure detector: the core of the detector process is to create the syndrome vector, which is principally implementing the subsequent vector-matrix multiplication scheduled the received encoded vector C and parity-check matrix H : $S = C \cdot H^T$; $H = [I_{n-k} | P^T]$

If $S = 0$, No Error; If $S = 1$, Error present

If a detector notices an error, the encoder has to repeat the process to create the accurate codeword. The codeword is subsequently stored within the memory. Codewords are vulnerable to transient faults while they are accumulated in the memory; hence a unit of corrector is intended to accurate potential errors within the retrieved code words [5]. One-step majority-logic correction is a quick and moderately compact error-correcting method which is the process that identifies the accurate value of every bit in the codeword openly from the codeword received; this is in disparity to the common strategy of message-passing error correction which may possibly demand multiple iterations of error analysis in addition to trial improvement. This method contains generating a detailed set of linear sums of the bits of received vector in addition to finding the best value of the computed linear sums [6]. A fault secure detector comparable to the circuit that is placed subsequent to the encoder is used to make sure the rightness of the output of the corrector. Occasionally the corrector circuit may perhaps be upset or be unsuccessful; consequently to make sure the accuracy of the corrector a fault-secure detector observes the process of the corrector unit. The codeword which is obtained is multiplied with the Parity check matrix H. If the achieved output is “0”, the codeword is accurate or else the corrector has to start again the process. A simple decoder is used to get hold of the information vector. Once the accurate codeword is obtained, the bits 1 to 7 are in use which is the unique information vector.

3. RESULTS:

ModelSim Actel 6.6d is used to confirm the performance of the verilog code which is made by means of giving various inputs and examination of the outputs. Tests are performed where at both times inputs are similar but dissimilar errors are set up to check the performance of the circuit. The waveform given I the figure explains that the circuit has approved the 2 errors as well as the

data_in value is re-written its accurate value after the parallel corrector approved it. The structure approved both the errors at similar time in single clock. This is due to the parallel construction of the corrector in which all 15 corrector circuits function at similar time.

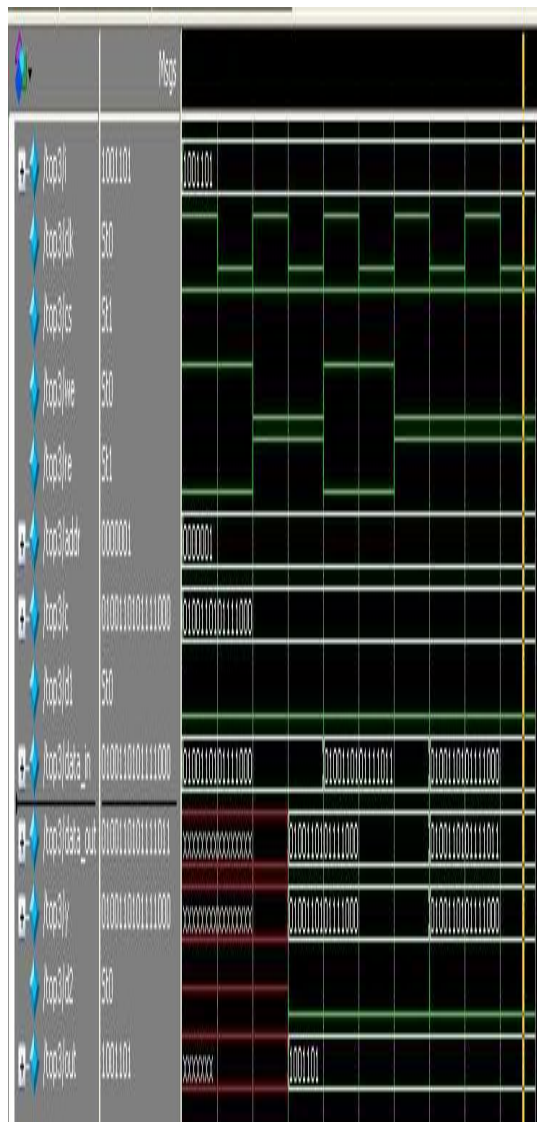


Fig2: An overview of the wave form.

4. CONCLUSION:

The architecture of Fault tolerant memory is presented which put up with transient faults both in the unit of storage and in the supporting logic. The structure can accurate both the errors at similar time in single clock which is appropriate to the parallel construction of the corrector in which all 15 corrector circuits function at similar time. When

3 or additional errors take place the parallel corrector cannot approve them and the detector intended for parallel corrector identifies the output of parallel corrector erroneous and positions its signal high demonstrating that the output of the parallel corrector is incorrect.

REFERENCES:

- [1] H. Naeimi and A. DeHon, "Fault secure encoder and decoder for memory applications," in *Proc. IEEE Int. Symp. Defect Fault Tolerance VLSI Syst.*, Sep. 2007, pp. 409–417.
- [2] H. Naeimi, "Reliable integration of terascale designs with nanoscale devices," Ph.D. dissertation, Dept. Comput. Sci., California Inst. Technol., Pasadena, CA, Sep. 2007.
- [3] Shu Lin and Daniel J. Costello, *Error Control Coding*. Prentice Hall, second edition, 2004
- [4] Peter Sweeney "ERROR CONTROL CODING From Theory to Practice", *University of Surrey, Guildford, UK JOHN WILEY & SONS, LTD.*
- [5] Claude laferriere "Error correcting capability of 1- step majority logic decoding", Thesis submitted to the school of graduate studies, university of Ottawa, June 1977.
- [6] H. Naeimi and A. DeHon, "Fault-tolerant nano-memory with fault secure encoder and decoder," presented at the Int. Conf. Nano-Netw., Catania, Sicily, Italy, Sep. 2007.
- [7] Samir palnitkar "Verilog HDL" 2nd Edition, Pearson Education.
- [8] R. G. Gallager, *Low-Density Parity-Check Codes*. Cambridge, MA: MIT Press, 1963.
- [9] R. J. McEliece, *The Theory of Information and Coding*. Cambridge, U.K.:Cambridge University Press, 2002.

Authors:

Subbareddy.k, M.tech from JNTUH presently working as an asst. Professor in MRIET, Hyderabad, AP ,India.

Satish.k, M.tech from jntuh, presently working as an Associate Professor in AEC, Hyderabad, AP ,India