VOL. 14, NO. 16, AUGUST2019 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

DESIGN OF NOC ROUTER WITH 3PE, DOUBLE AND TRIPLE ERROR DETECTION BY USING IMPROVED HAMMING CODE

M. Senthil Kumar and Md. Javeed
Department of Electronics and Communication Engineering, Sree Dattha Institute of Engineering and Science, Hyderabad, India
E-Mail: professor.msk@gmail.com

ABSTRACT

Network on Chip (NoC) router is mainly used in system on chip (SoC) application. Millions of transistor integrated into a single chip is called as very large scale integration (VLSI) to design a single integrated circuit (IC). Also, millions of IC is integrated into single chip is called as SoC. Hence, the routing is very difficult in SoC. To avoid this kind of problem, the NoC router is incorporated into SoC board. NoC router is mainly used to transmit data from source to destination based on request. To set the priority, Priority arbiter is used for which data will come first from multiple request at the time. Lot of priority arbiter is available such as regular round robin arbiter, distributive round robin arbiter, matrix arbiter… etc. FIFO or buffer is used for temporary storage. Finite state machine (FSM) acts as controller of NoC router to control entire module. Network interconnect is used for linking. Multiplexing and de-multiplexing operation is carried out by Crossbar switch. The existing NoC router is designed with two programmable elements (2-PE) & single error correction with double error detection method by using hamming code. But the probability of error detection is low and speed is very less. To overcome this problem, the proposed NoC router is designed with three programmable elements (3-PE) and triple error detection is performed with less number of parity bit by using improved hamming code. Comparison between the existing and proposed router is carried out to analyze the various parameters. From the obtained results, it is illustrated that the proposed NoC router offers high speed, Low area and the highest probability of error detection than the existing NoC router. ModelSim and Xilinx ISE tools are used for simulation and synthesis process. Verilog HDL is used to design a different type of NoC router.

Keywords: NoC router, 3-PE, improved hamming code, double error detection, verilog HDL and triple error detection.

1. INTRODUCTION

The obligations of higher levels of data integrity and system trustworthiness in communication systems have been raised by using many Error Correcting Codes (ECC's). Hamming codes were offered that can correct single error per word are generally used to care for the soft errors which arise while a radiation particle hits the device and alters the valid values [9]. The decoding and encoding latency for Hamming directly affect the memory access time. Single error correction codes have a least hamming distance of three and so double error can be wrong for a single error incorrectly corrected. For Memory purpose these topics can be corrected by SEC-DED, these codes have a smallest hamming distance as four [8]. A Single Error Correction and Double Error Detection code can makes by improving a Hamming code with a parity bit covering every bit [1].

Hamming Codes are a kind of linear block error-correcting codes that simplify the rate codes discovered by Richard Hamming in 1950 [2]. Hamming codes are wonderful codes, they attain highest possible rate for codes with their minimum distance and block length. Hamming Codes can identify up to three-bit errors also correct one error.

In exactly hamming codes are characterized for m≥3 by the tracking parameters [3]:

$$n = 2^m - 1 \quad (1)$$

$$k = n - m \quad (2)$$

$$d\_min = 3 \quad (3)$$

Where k is the Number of information Bits, n is the block size, m is the parity check bits and d_min is the minimum distance of the code. For a SEC, the smallest number of hamming distance is three that denotes three parity bits are utilized to correct and detect single bit error. For a SEC-DED, the smallest number of hamming distance is four that means one extra parity bit is used to recognize double bit error however can incorrect the double bit error [4].

An Algorithm to produce hamming secret code's from data bits is as follows a) Number the every places of bits beginning from 1 to n, where n is the last place of the bit. b) Each and every one positions are written in their binary type as 1, 10, 11, 100, 101, 110 etc. C) All bit places that are powers of two are thinked as parity bits.

Place 1: test 1 bit and skip 1 bit steps are chased such as 1, 3, 5, 7, 9....
Place 2: test 2 bits and skip 2 bits steps are chased such as 2, 3, 6, 7, 10, 11....
Place 3: test out 4 bits and skip 4 bits steps are pursued such as 4, 5, 6, 7, 12, 13, 14, 15.....
Place 4: check 8 bits and omit 8 bits steps are pursued such as 8-15, 24-31, 40-47.....

Finally, set a parity bit to 1 if the total number of ones in the places is odd. Put a parity bit to 0 if the total number of ones in the places is even. In this method we obtain the password by using hamming. We can identify the single bit error by using syndrome values. The result of parity matrix and code of the present values are called as a

Syndrome. If the value of syndrome is null vector, after that the current value of the word is an actual code word and in any more cases there are offering error in that password. Parity bits are computed as follows [4]:

$$c1 = c3 + c5 + c7 \text{ or } p1 = d1 + d2 + d4 \quad (4)$$

$$c2 = c3 + c6 + c7 \text{ or } p2 = d1 + d3 + d4 \quad (5)$$

$$c4 = c5 + c6 + c7 \text{ or } p3 = d2 + d3 + d4 \quad (6)$$

So as to check the codeword or password, the parity bits are re-computed again from the data bits and compared to unique set of parity bit. If they match, then no error was identified, if not an error is detected and the non-identical parity bits can offer us with the data of bit that was flipped in order that the error can be corrected. For instances, parity check matrices for (7, 4) is [5]:

$$H = \begin{vmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{vmatrix} \quad (7)$$

This H matrix is called the same as a lexicographic check matrix. If produced password is 1011010, then the multiplication of Parity check matrix H and resulted password is 000, called as a Syndrome vector. It is a Null vector value provides the result of actual code that means no error has been produced, and hence, the present value of the word is an actual code word. If created password is (1011011), then the multiplication of Parity check matrix H and resulted password is (111). Hence, it can make value 7, that mean error can create in a seventh bit [6]. Like this we can straightforwardly identify and correct single bit error. But this technique is not appropriate for double bit error. For identifying double bit error, we require one more parity bit and hence least hamming distance become as four. But we cannot correct the identifying double bit error and could get a incorrect the word into a dissimilar valid one making Silent Data Corruption (SDC). We will notice SEC-DED techniques briefly in subsequently section [7].

Single event upset is occurred due to not correction the error in the input data. The main aim of the project is to reduce the multiple cells upset by reducing single event upset. To reduce the SEU, an efficient error detection and correction mechanism is followed in order to achieve low MPU and make error free router design [11]. In the existing technique, RKT switching technique is used for single error correction and detection. In the proposed technique, the enhanced decimal matrix codes (EDMC) is mainly used for single and double error detection. This method correct only one bit and detect 16bit error. But the number of parity bit is very high. Hence the computation time is high [12]. It has been found out in the study that both the permanent and temporary faults that may occur in the Network Interface (NI) can lead to incidences of unfavorable behavior that create unrecoverable conditions of the NoC. This condition may be deadlock or live lock. The power consumption and area utilization is higher than the existing method due to adding more number of parity bits [13].

These double and error detection technique is incorporated into NoC (network on chip) router with 3 programmable elements (PE). The main aim of this work is to design a fault free NoC router by using 3-PE, improved double and triple error detection scheme in order to reduce the bit error rate (BER) and create a reliable routing technique. In this article, to maximize the probability for correct a single error and identify the triple adjacent error Bit Placement algorithm is used. As well as, the existing single error correction and triple adjacent error detections (SEC-TAED) using Hamming Codes are also presented by using bit placement algorithm. For the existing Triple Adjacent Error Detection Codes, a new parity bit is needed than Double Adjacent Error Detection. In this proposed NoC router, triple adjacent error is identified without need of a new parity bit and offers 90% detection efficiency than the existing Triple Adjacent Error Detection method. The proposed scheme does not need some extra circuitry.

The rest of the article systematized as pursues section 2 presents NOC router design with an improved double error identification and single error corrections are discussed in detail. The proposed SEC-TAED with elevated detection effectiveness and less computational time is presented in section 3. In section 4 examine the simulation outputs and at last conclusion is offered in Section 5.

2. DESIGN OF NOC ROUTER WITH IMPROVED DOUBLE ERROR DETECTION

Syndrome calculation is used for single error detection. Syndrome calculation is nothing but product of hexa-graphic matrix (H-matrix) and transpose of codeword. Error detection and correction mechanism is very important in network on chip to avoid the data losses in order to make fault free router. Complexity is high in the existing NOC router design with existing data encoding method. Very difficult to implement in the integrated circuits. It will detect the error but not correct more than one bit error occurred. To overcome this problem bit replacement technique is introduced in the proposed technique. Very difficult to perform selective bit replacement technique [10]. It takes more amount of time to detect double and triple error detection in the NoC Router. But the number of parity bit is low when compared to all other state of art technique. The performance of the error detection of hamming code is very low due to long process. In the previous technique, single and double adjustment error detection is performed by using hamming code. It requires more number of parity bit to detect single and double error detection. In the proposed system, the improved hamming code is used to maximize the probability detection mechanism as shown in Table-1. But the complexity is high than the existing double error detection method.

The circuit diagram of 3x3 mesh topology based NOC router [14] with improved hamming code (IHC) is shown in Figure-1. An improved hamming code for SEC-

DAED and SEC-TAED is used in between two routers in NoC router based switch design.

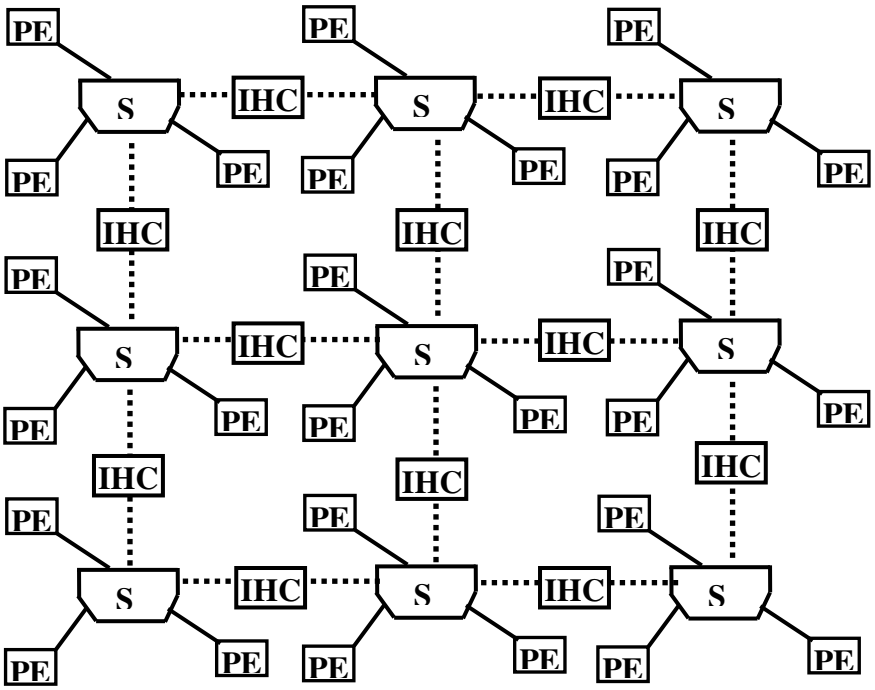

Figure-1. Circuit diagram of 3X3 NoC router with improved hamming code based on mesh topology.

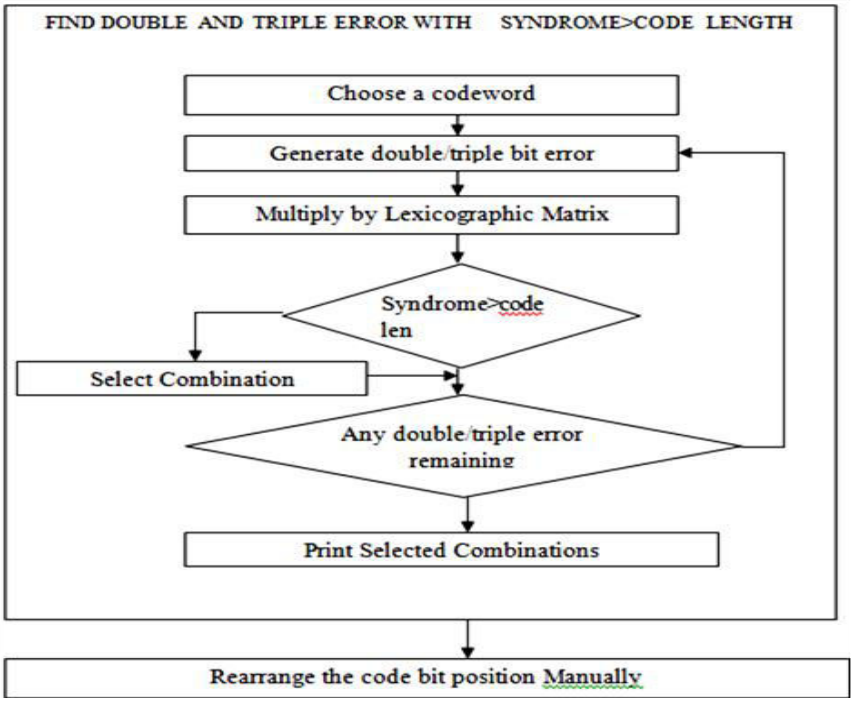

Figure-2. Flow diagram of bit replacement technique

So as to keep away from a miscorrection in an improved hamming code and maximize the probability of the adjacency of particular combinations rearranging the password or choosy bit pattern are introduced in fig.2. All the double error and triple error combinations which produces a syndrome that does not matched with any of the ones caused by a single error and then illustrates the finding of three bit adjacent error, after reordering all bits with one more parity bit. New parity bits are denoted as 'p'. When using a usual order of 12 bit code with an additional parity bit, (10-11-12) groupings only correct the triple adjacent error.

These groupings do not cause a miscorrection in the improved Hamming (13, 8) code. Consequently, improved Hamming of (13, 8) ensuing in 9 out of 11 contiguous errors are identified and not corrected. Simply 2-4-p, p-10-12 couples are detects the incorrect error. However, one more parity bit is consumed extra computational time.

Table-1. Proposed NoC router with improved double adjacent error detection for hamming (12, 8).

Bit Replacement													Detection	
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**p**	**3/11**	**27%**
1	12	2	3	4	9	6	8	7	10	5	11	p	9/11	90%

The proposed NoC router with 3x3 mesh topology is designed and applied double & triple error detection mechanism with single error correction based on hamming code. The block diagram of 3x3 mesh topology based NoC router with hamming code is shown in Figure-1. From the Figure-1, the hamming code is incorporated in between two routers. This configuration is followed to avoid unwanted data losses due to multiple cell upset problem. Similarly, triple error detection scheme is applied between two routers in the next section.

3. PROPOSED NOC ROUTER WITH IMPROVED SINGLE ERROR CORRECTION AND TRIPLE ERROR DETECTION

In earlier sections, the existing Single Error Correction and Double Error Detection scheme by using Hamming code is elucidated. In Bit Placement algorithm, rearranging the place of code bits is used to identify the double and triple adjacent error detection. The 15 arrangements are established for two bit error. In existing lexicographic matrix (8) for single error correction, 7-8 arrangement only correctly identifies the error. So as to maximize the probability for identifying the double adjacent error, rearranging the place of code bits is presented in 3. This algorithm incorrect the values with a various one for identifying the triple adjacent error. Likewise, the 51 arrangements are founded for three bit error. However, in usual order of code bits, only 10-11-12 arrangements only correctly identify the error.

Table-2 demonstrates that maximize the probability for identifying triple adjacent error with one more parity bit. This consequence in 9 out of 11 arrangements is correctly identifying the triple adjacent error with 82% efficiency. However this needs more computational time for identifying the error. In our proposed method, the triple adjacent bit error is identified by bit replacement algorithm without insert a one more parity bit is presented. Among this data a new order is planned in Table-3. The maximizations of the probability that can identify triple adjacent error is presented in our proposed method 8% more efficiency than the existing SEC-TAED Hamming codes with extra number of parity bits. In Table-2 demonstrate the detection of all adjacent bits matches the error arrangements apart from 2-4-p and p-10-12. Another parity bit consequences in high computational time and more difficult to identify the error. These two types of hamming code for triple error detection are applied in the network on chip router for on chip communication purpose.

Table-2. Existing triple adjacent error detection for hamming (13, 8).

Bit Replacement													Detection	
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**p**	**1/11**	**9%**
6	8	1	7	11	3	5	9	2	4	p	10	12	9/11	82%

Table-3. Proposed NoC router with improved triple adjacent error detection for hamming (12, 8).

Bit Replacement												Detection	
12	**11**	**10**	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**1/10**	**10%**
12	9	5	3	8	4	1	10	6	2	11	7	9/10	90%

In our proposed scheme, the required probability should be enhanced for identifying triple adjacent error exclusive of one more parity bit. All the contiguous bits in Table II match the particular fault arrangements apart from 12-9-5. This offers more efficient when compared to the triple adjacent detection for hamming (13, 8). In our proposed method, two benefits are comprised when compared to the conventional system. (1) With fewer number of parity bits, Single Error is corrected in addition to Triple Adjacent Error also identified. (2) Rising the number of likelihood identification and efficiency when compared to the conventional method. The results for the

Hamming (12, 8) codes illustrate the selective bit placement tactic can enhance the chance of detection the triple adjacent errors in Hamming Codes. The improved triple adjacent error detection with single error correction scheme is applied in the NoC router to make a fault free routing mechanism in system on chip (SoC) applications. Simulation results of proposed technique will be presented in next section.

4. RESULTS AND DISCUSSIONS

In proposed NoC router with single error correction and triple error detection Codes, maximum number of likelihood that can identify triple adjacent error is presented with less number of parity bit than the existing single error correction and triple error detection with an extra parity bit.

The proposed single error correction and triple error detection process offers 8% more efficiency than the conventional scheme. When single error is arising, the resulted put backed code bit offers syndrome is used to identify and correct the error. Hence, single error is identified and corrected as shown in Figure-3.

As triple bit error is happen, the status specified as "TED" but not corrected. For example, (2-11-7) bits modified, and then the substituted codeword offers syndrome which is equivalent to the binary representation. It cannot be corrected as it does not match a suitable code bit location. The outcome for detecting triple bit adjacent error is shown in Figure-4.

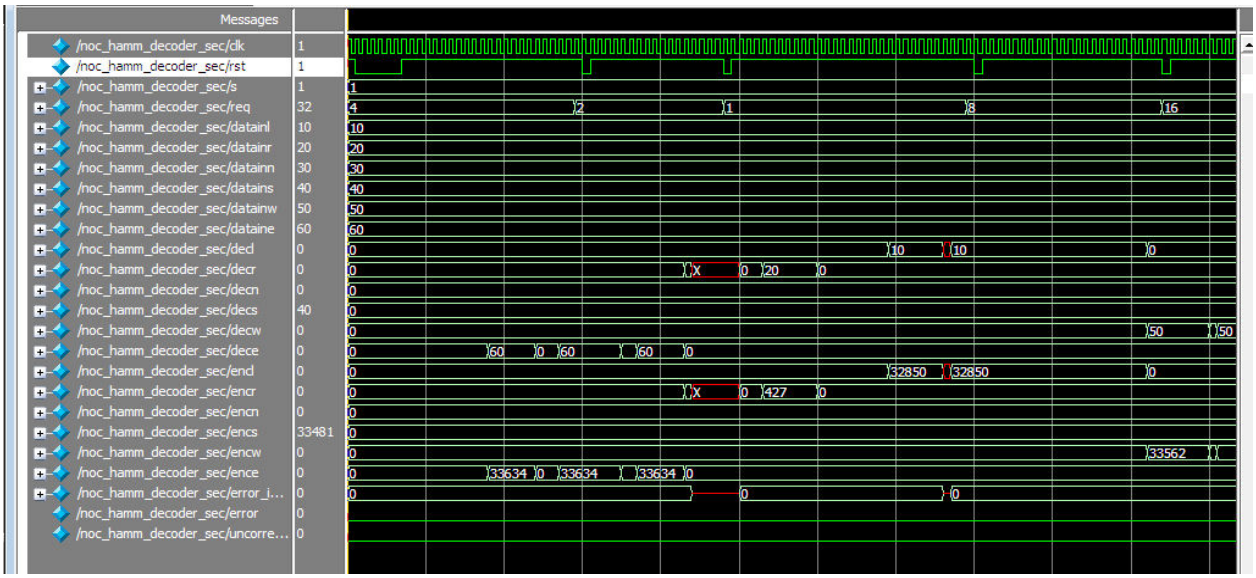

Figure-3. Simulation output of NOC router using improved hamming code for Single error detection & correction.

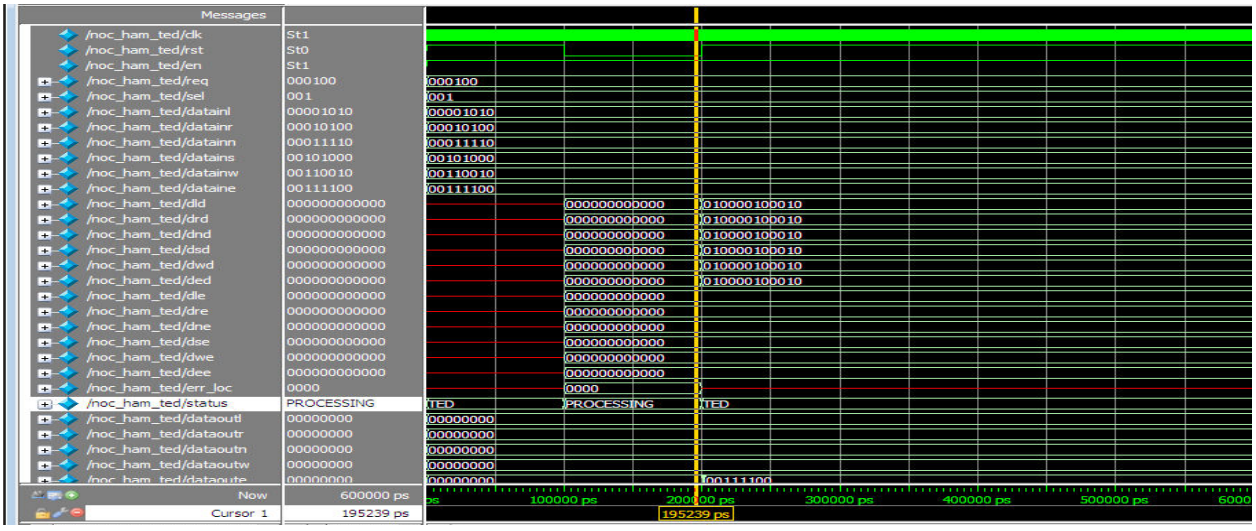

Figure-4. Simulation output of NoC router with single error correction and triple adjacent error detection using improved hamming code.

Table-4. Comparison of different NoC router using improved hamming code for SEC-DED and SED-TED.

Types	Slices (area)	LUT	Delay (ns)	Power (mW)
NoC router with SEC-DED	1486/10752	2883/21504	3.793	3897
NoC router with SEC-TED	1509/10752	1310/21504	5.059	3739

From the obtained results as given in Table-4, it is shows that the proposed NoC router with improved single error correction and double adjacent error detection (SEC-DAED) offers high speed. But the area and power consumption is very low than the single error correction and triple adjacent error detection method (SEC-TAED). Also the functionality of NoC router with double and triple bit error detection of improved hamming code is verified through simulation process.

CONCLUSIONS

In this work, a scheme used to maximize the likelihood of identifying the Triple Adjacent Errors using Hamming Code has been demonstrated for NoC router design. The improved detection is attained by applying the Bit Placement technique in SEC-DED Codes. This technique not only used to correct the single error, it is also used to increase the chance of identifying the Triple Adjacent Error with fewer number of parity bit. After that, an improved hamming code with single error correction and double and triple error detection is incorporated into network on chip router design. The proposed NoC router with Sec-DAED and SEC-TAED Codes provides high efficiency when compared to existing SEC-DED and SEC-TED. The proposed SEC-DAED Codes employ less amount of time for identifying error when compared to the existing SEC-DED with another parity bit. Also area and power consumption is very low for proposed NoC router with SEC-TAED method than the SEC-DAED due to less number of parity bit than the conventional methods. In future, the proposed scheme will be improved further to decrease the number of parity bits for identifying double and triple error in the NoC router.

REFERENCES

[1] Sanguhn Cha and Hongil Yoon. 2012. Efficient Implementation of Single Error Corrction and Doule Error Science Detection Code with Check Bit Pre-Computation for Memories. Journal of Semiconductor Technology. 12(4).

[2] Alfono Sanchez - Macian, Pedro Reviriego and Jaun Antonio Maestro. 2012. Enhanced Detection of Double and Triple Adjacent Errors in Hamming Codes Through Selective Bit Placement. IEEE Transaction. On Material and Rel. 12(2).

[3] Yuanyuan Cui, Mian Lou, Jianqing Xiao, Xunying Zhang, Senmao Shi, Pengwei Lu. 2014. Research and implementation of SEC-DED Hamming code algorithm. IEEE Trans. on Microelectronics. Vol. 31.

[4] A. Dutta and N. A. Touba. 2007. Multiple bit upset tolerant memory using a selective cycle avoidance based SEC-DED-DAEC code. IEEE VLSI Test Symp. pp. 349-354.

[5] A.L. Chen and M. Y. Hsiao. 1984. Error-correcting codes for semiconductor memory applications: A state-of-the-art review. IBM J. Res. Develop. 28(2): 124-134.

[6] R. W. Hamming. 1950. Error Detecting and Error Correcting Codes. Bell Syst. tech. J. 29(2): 147-160.

[7] M. Nicolaidis. 2005. Design for Soft Error Mitigation. IEEE Trans. on Device and Materials Reliability. 5(3): 405- 418.

[8] K. Manidurai and G.R. Mahendra Babu. 2014. Error-correcting codes for semiconductor memory applications: A state-of-the- art review. IJET Computer Science and Engineering. Vol. 1.

[9] R. Xu, Z. Gu and J. Luo. 2010. Design of radiation hardened error detection and correction circuit. IEEE Trans. on Microelectronics. 40: 547-550.

[10] Alfonso Sanchez - Macian, Pedro Reviriego and Jaun Antonio Maestro. 2014. Hamming SEC-DAED and Extended Hamming SEC-DED-TAED Codes through Selective Shortening and Bit Placement. IEEE Transaction: Device and Material Rel. 14(1).

[11] Reed K. Lawrence and Andrew T. Kelly. 2008. Single Event Effect Induced Multiple-Cell Upsets in a Commercial 90 nm CMOS Digital Technology. IEEE transactions on nuclear science. 55(6).

[12] Krithika Anand and Mukthi S L. 2016. An Efficient Error Correction Code for a Smart Reliable Network on Chip. International Journal for Scientific Research & Development. 4(03).

[13] Maurizio Palesi, Giuseppe Ascia, Fabrizio Fazzino and Vincenzo Catania. 2011. Data Encoding Schemes in Networks on Chip. IEEE transactions on computer-aided design of integrated circuits and systems. 30(5).

[14] Rohit Kumar and Ann Gordon-Ross. 2016. MACS: A Highly Customizable Low-Latency Communication Architecture. IEEE transactions on parallel and distributed systems. 27(1).