IOSR Journal of VLSI and Signal Processing (IOSR-JVSP)
Volume 5, Issue 3, Ver. I (May - Jun. 2015), PP 33-44
e-ISSN: 2319 – 4200, p-ISSN No. : 2319 – 4197
www.iosrjournals.org

Fault Tolerance in Network-on-Chip by Using Single Error Correction and Double Error Detection

Geeta A Sannakki[1,] & Maltesh Bajantri[2.]
[1,]*PG Student, M-Tech ,* [2,]*Assistant Professor*
[1,2,] *VLSI Design and Embedded Systems, Shridevi Institute of Engineering and Technology Tumkur, India.*

Abstract: *The emerging technique for communication with in a large VLSI system is a network on chip. The fast scaling of technique there has been susceptible faults in the component of the network on chip, thus there is a requirement for technique to maintain circuit reliability. A fault-tolerant NOC (Network-on-chip) should be having the capacity to detect a fault and recover the system to correctly operate and work according to the mapped application. The work performed here emphasizes on the learning and assessing of methods for growing flexibility of system interfaces with NOC based multi-processor system on chip (MPSOC) design. In between communication infrastructure and the IP cores, NIs (Network interface) acts as junction. The flawed action of one of the interface could affect or harm the overall system.*

I. Introducation

The favorite topics of research in the field of information technology is parallel processing which involves computer networks and network interfaces. In 2000, the field of NoC or Networks-on-Chip was designed because of the advent of the multi-core computer processing unit (CPU) and due to the predicted computing growth towards extremely incorporated architectures with interconnected networks [11] .Several surveys have been conducted about NoC and have been published. One of the leading topics that involve NoC is the fault-tolerant design which is well-known in terms of its significance and interest of the experts in technology and computer system.

It is therefore the purpose of this paper, to examine the extent of NoC in the field of computing and how it has affected the technology users. Moreover, the paper gives a general idea of all the aspects of network-on- chip fault tolerance including, determination of failure mechanisms, fault models, diagnosis and configuration strategies. In order to offer the significant context in understanding the system of NoC, this paper discusses the basic concepts of fault tolerance, defines and discusses the terminologies, and offers the comprehensive review of the physical processes involve in the NoC fault. Several sections are also allotted on the investigation of the methods utilized for fault-tolerance in the foundation of the Network-on-chip system giving emphasis on the data network and transport layers which are the important terms in creating and providing reliable transmission of data[7].

The continuous evolution of new application has become the reason of the invention of some new processor, memory and accelerator cores [1]. Moreover, the fast development and improvement of computation and the complexity of communication have caused the invention of the scalability-centered paradigms. These are the reasons why network-on-Chip (NoC) is designed in order to be an alternative in providing high-performing communication system in the field of Systems-on-Chip (SoCs) with several cores incorporated in one silicon die[6].

The Netwok-on-Chip is an effective architecture in the communication system under the System-on-Chip. It permits the incorporation of hefty quantity of computational blocks in a single circuit [1]. NoC allows the reutilization of blocks which results to the provision of high degree parallelism and performance of the system in higher level. Accordingly, the rising demand for NoC is a result of the requirement to achieve higher bandwidth if the field of communication. As stipulated in Moors law, the integration of the transistor can be doubled within the approximate eighteen months, however, challenges and the competition of the physical connection in Integrated Circuit (ICs) has caused severity in the delay of connections among the global wires [10]. The traditional method of connection namely, end-to-end, bus-based and other are not good solution to the problem regarding the wire delay in integrating IP cores with System-on-Chips because they do not scale well if there are more mechanism that are supplied into the system [7] .Moreover, there is the ad hoc solution that is of varying buses, crossbar and wiring that can attain mainly advantageous performance especially for specific application. However, the system cannot be recycled and it requires great costs for its development and verification [3].

This is where NoC comes in because it has the potential of providing short circuits and can thereby reduce the delays in wire. The utilization of NoC replaces the traditional methods of interconnection and it has several advantages in terms of its performance and modularity [5] .Furthermore, it was observed that the utilization of NoC among electrical properties have optimized, while it has reduced the power consumption ten folds and increased the speed three times as compared with the system that utilizes the bus-based connection [8].

- **Problem Statement**

It has been observed that relative to the failure of the CMOS technology into the deep-submicron domain, and interconnection of complex designs are prone to system malfunctions and failures which are difficult to calculate and to prevent especially with its new design and methodologies. The same is right among entrenched systems which are made up of various intellectual property (IP) cores and are connected through NoCs. The need of developing new approaches to fault-tolerance of NoCs through designing new methodologies and architectural solutions as primary solutions to deal with the failures in complex systems.

- **Methodology**

The goal of the proposed work is to deal with both the permanent and temporary fault by providing a new architecture to NI components FIFOs and Look Up Table which are sensitive to faults. The fault free NI which assumes a particular relevance in the design of a reliable MPSoC.

The network connection of IP in the infrastructure and system of communication is primarily influenced by the network interfaces. It presents vital points in the NoC fault-tolerance designs and methodologies. As a matter of fact the NI can directly cause fault and malfunction that can affect the accuracy of the data transmission and the control of information which are hard to detect and recuperate especially without the proper support Furthermore, an erroneous NI can isolate a not defective core from the rest of the system thereby causing an enormous fault area. Experts therefore suggest that intensive consideration must be given to the design of the fault-tolerance networks of NI.

The method for implementing of reconfiguration policies of LUT as software routines of NoC on the processor .Interrupt request is created by network interface at the error detection. SECDED architecture makes use of Hsiao code for correcting and detecting errors, without loss of architectural redundancy.

- **Existing Techniques and Its Effects**

In order to uphold protection of the NoC infrastructure, some researchers have recommended fault tolerant solutions that made use of familiar approaches such as the Triple Modular Redundancy (TMR), Time Redundancy or TM in order to secure the NoC from the faulty mechanism. Most of the common hardware which is fault-tolerant which have sensitive components has utilized the TMR with three copies of similar machinery performing the same operation in which result is obtained by voting mechanism [3].

However, one weakness observed in TMR is its cost in terms of assets and power, specifically in the entrenched systems which its intensive mechanism exclusively uses hardware redundancy which is relatively expensive. This is really true for NIs which has a significant role in the modern era of communication system. However, most of the communications that make use of the hardware redundancy severely progress specifically on power consumption in protecting the NoC router due to the fact that when a system is capable of triplication the hardware its power consumption also triplicates [5]. On the contrary, the Time Redundancy reduces the performance of NoC because the needed information must be retransmitted first hence causing an interruption in the processing of data.

The very known in fault tolerance technique is redundancy [2] and [9]. ECC or error correction code must be used to in order to adapt to this weakness of NoC. When the data source is from a neighboring router, the router selects the most efficient ECC mechanism to transmit data through connections. Nevertheless, it is necessary that the technician knows that in the fault-tolerance technique, only the link is secured hence it is protected from a disturbing sound called interference [10] .Between two methods, there is no mechanism that protects the routers.

In order to guarantee protection of the NoC link, the most common techniques is changing the routing algorithm. As compared with the TMR, the latency of the routing algorithm technique is lesser than the process of retransmission and is cheaper. Hence, it is recommended that a series of routing mechanisms in using NOC systems must be applied with partially erroneous connection [5].

- **Overview of the NI reference Architecture**

The fundamental composition of NoC structure is composed of routers, links and network interfaces [4] .The primary function of the router is to direct the data through the connections; the network interfaces are responsible for the adaption of both the incoming and outgoing data in the core of the connection.

The layout of the networks is called topology and it is the algorithms routing which is responsible for the selection of path to be taken between the source and the destination. The figure below demonstrates the 3x3

grid NoC which is composed of the accumulator, memory, floating point unit, CPU, and the blocks for output and input.

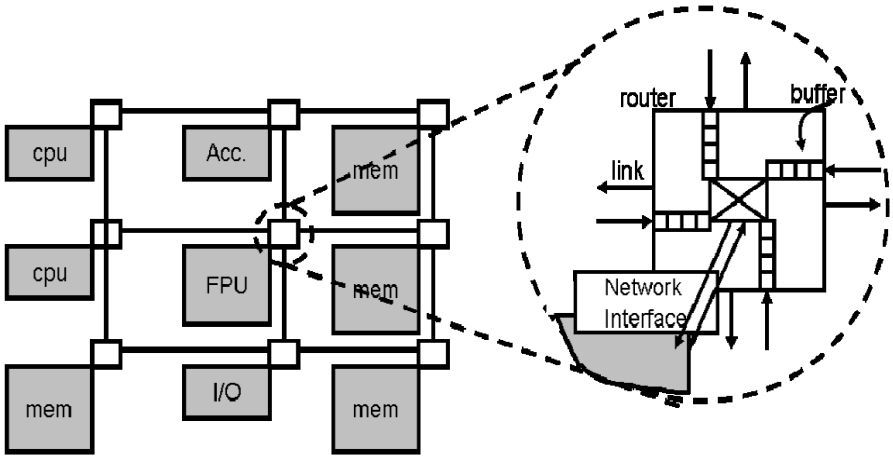

Fig.1: NoC 3x3 2-D Grid with 9 routers.

Advancement in technology has caused enhancement in the quantity of interconnections and on the other hand resulted to decrease in the transistor dimension [10]. In terms of the advent of NoC it gains the possibility of having increasing number of faults in the networks and the logic especially during the time of its manufacture or while it is being utilized in the system.

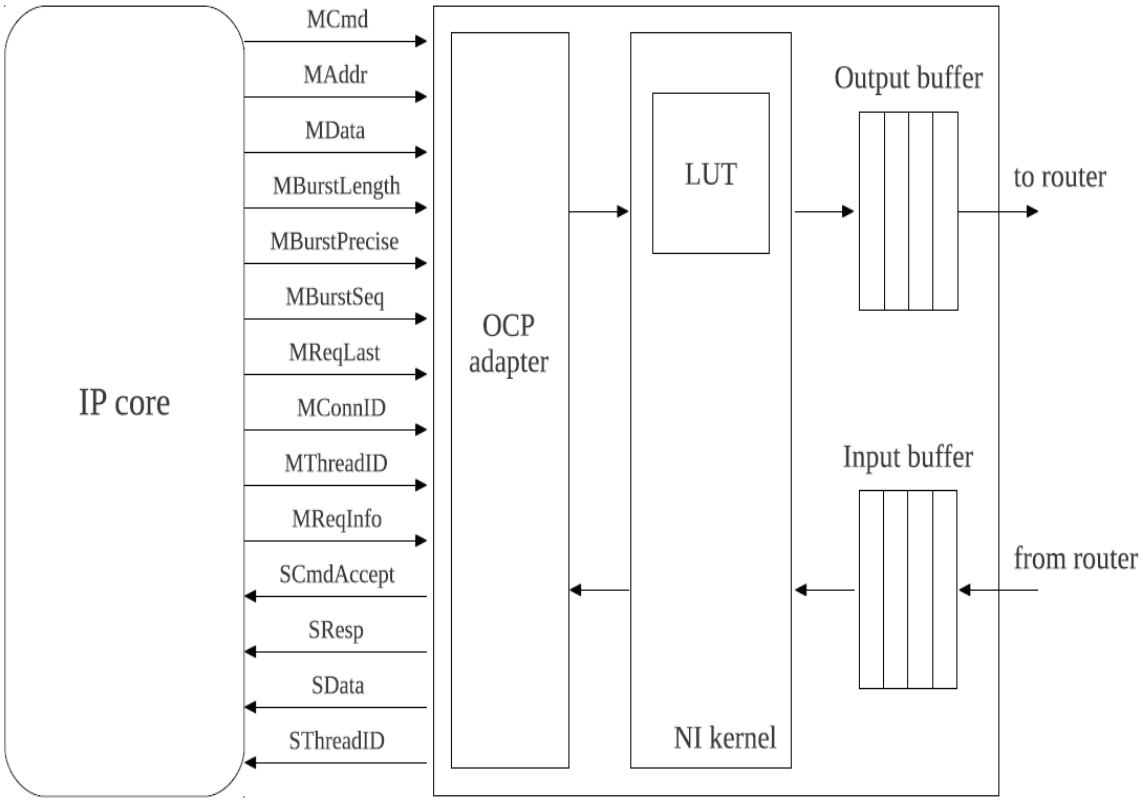

Fig.2: Overview of the reference NI architecture considered in the experiments.

INTEL [10] has projected that within a decade, there will be 100 billion transistor chips that will be created, however, an approximate of 20 billion of those transistors will not pass the quality standard upon its manufacture, and the other 10 billion will malfunction during the first year of its utilization [2] .This means a fault rate of 20-30% in the System-on-Chip, thus resulting to permanence, intermittence and transience of the faults in the system.

The figure above (Fig.2) illustrates the fundamental well-designed blocks of the NI which taken as basis of the evaluation conducted. There are various substitutes available in implementing the NI basic service, especially in the packetization phase. Part of the components of NI that are categorized as the most fault-resilient are the Lookup table (LUT), FIFOs or buffer and the Finite State Machines (FSMs). It is therefore considered in this study that NI can be a reliable block that is found between the core and the communication network. Among the primary devices of the NI system are the following:

- Open Core Protocol (OCP) adapter – which is in charge of the OCP implementation. When it is in the core functioning as initiators it employs as a slave interface, and as a Master interface when at the target core.
- NI kernel- responsible in programming and embedding data into the packets and FIFO buffer and transmit the information from the adapter.
- Output FIFO buffer- functions as the storage of packets when embedded in the NoC system; and input FIFO buffer that receives and keeps the incoming packets.

Network interfaces (NI) function in the implementation of transaction-based communication through the abstraction of the shared-memory in which the components of the NoC are mapped through memory [6] .Another function of the NI is the implementation of the wormhole flow-control and on the routing policy based on the source. In case of new transactions through the processing element, the NI traces and locates the address through memory mapping of the OCP. During the process, the programmable LUT in the NI kernel is utilized. Lookup table (LUT) is composed of minimal bits that direct the circuit implementation through packetization travels to the nodes of the entire systems of NoC. The transmitted information is embedded in the packet header. Its quantity and quality are basically dependent on the dimension and the topology of the NoC. In every router, in which the data may pass through, few bits of the sequence are used up before it reaches its targeted port of output[1] .After the transport and the process are completed, the used up bits are disposed and the packet header is being restructured. One of the advantageous characteristics of LUT is it is programmable, which means that the recorded data can be copied in support run-time modifications of the course-plotting paths, thereby increasing the possibility of the faulty links within the system of NoC.

- **The NI fault models**

The recommended NI model for functional fault is considered separately with the blocks that make up the system.

Among the identified faults are the following:

1) **Corrupt data fault** – This error may occur in protocol adapters and within the FIFO. This is characterized by the corruption of data during the application of the NI and when the faulty information is transmitted in the communication networks.
2) **Corruption Protocol Conversion Fault** – this mainly occurs in the protocol adapters of the NI. This error is caused when corruption of the node that initiates, transacts, and controls the signal is corrupted. This may result to the NI kernel's production of wrong routing and controlling of data in the packet header. When the corruption of code happens in the target node, this may result to disruption of the operation due to the erroneous connection and processing of communication transmission.
3) **Routing Path Fault** – Fault in the LUT and FIFOs. Errors in the insertion of the routing links in packet header may result to common communication errors namely; misdirection, deadlock or livelock.
4) **Multiple Copies-in-Time Fault** – this type of error usually happens in the FIFOs and protocol adapters. This may be due to the accumulation of minor faults that are then transmitted to the output and input packets. Since FIFOs are responsible in controlling the signals, this fault can cause disruption of the data altering the information being sent.

Table 1: Percentage of measured faults for each component of the NI and the router, calculated with respect to the total number of faults injected into the node

Component	Fault location	Fault percentage (%)
NIs	LUT	23.64
	Buffers	21.78
	FSMs	1.39
	Other	1.26
Routers	Buffers	32.98
	Crossbar	10.59
	Switch allocator	8.23
	Other	0.13

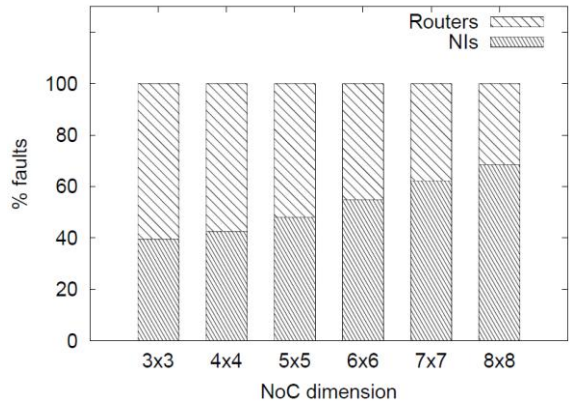

Fig. 3: Total faults in NIs and routers when varying the number of nodes in the NoC.

Whenever there are varying codes in the NoC system, a change in the permanent fault and error transmission happened [1]. The figure above showed the case of mesh topology and how it has affected the NIs as well as the routers with the changing value of n. Moreover, as illustrated in Figure 3, when the dimension of the NI increases, it becomes more sensitive to faults. The area of routers is directly proportional to the number of the nodes present in the topology, this is the reason why the prevalence of faults in the NI is affected by the size of area of the circuit involved. However, in LUT it increases with n^2. Consequently, this will result to higher possibility that NI will have faults as the quantity of the nodes are increased and eventually result to errors in the system. It is therefore suggested by the researchers that a fault-tolerant design should be created in order to address the fault occurrences in NI components.

- **Lookup table Architecture Overview**

In the application of NI, the LUT is utilized mainly for collecting the routing path which incorporated with specific address for data processing. It was found out that, faults of stored information and data, originate mainly from the routing path errors[6].

Basing on the network design, the researchers considered LUT in the utilization of either the programmable CAM (Content-Addressable Memory), RAM or the set of registers as indicated in figure 4. Furthermore, the register-based method is employed in this project. In the NoC system, the CAM is made up of the address boundaries that contain hard-code within the cores of the NoC along with the memory-mapped IPs. In the initiation of new connections, MSBs or most significant bits of the address [3] are compared with the values of the code along the path of the CAM. Aligning the lines of CAM with the input address is utilized in choosing the register which is used as storage lookup operation output. An example of this is the circuit in which the node is mapped in order to transmit the data to its destination input address .Information through the connection is automatically stored in the registers of the LUT during or after the conduct of the reconfigurations of topology.

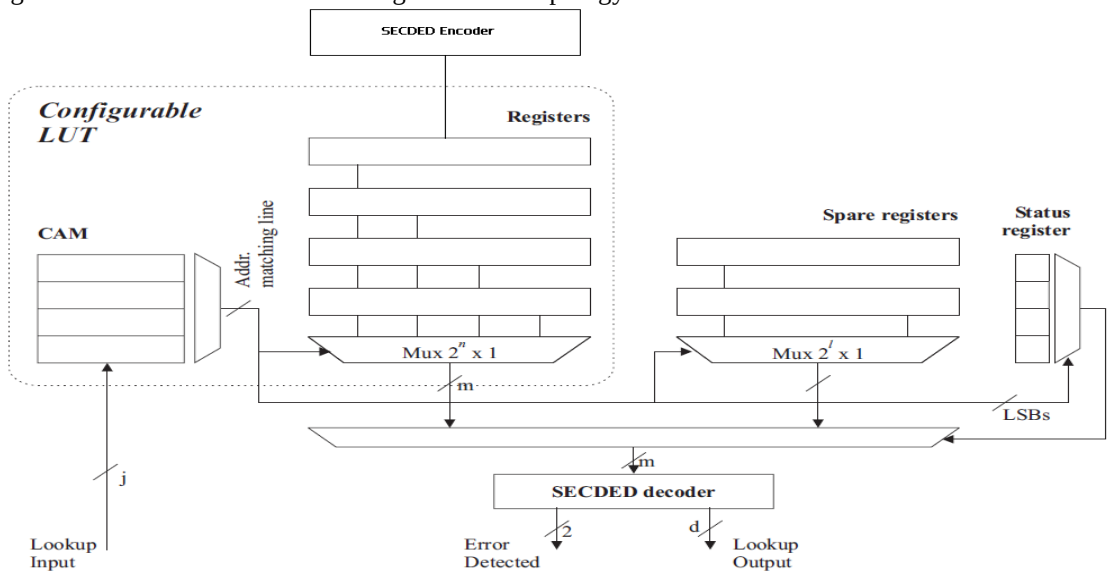

Fig. 4: Overview of the proposed LUT architecture.

It is shown in Fig. 4, the proposed design which allows increased way of recognizing codes and limiting the occurrences of design redundancy therefore, allowing the researchers to work on faults in the LUT system. On the other hand, the data circuit is saved though the application of the Single Error Correcting and Double Error Detecting (SECDED) Hsiao code which are capable of automatically correcting the error [1] .Moreover, it can also detect up to two connection faults in every LUT system. The researchers chose the Hsiao code due to its ability of allowing a uniform and equal allocation of the XORs during the encoding and decoding process [10]. As a result, it can reduce the quantity of logic ports and can diminish the overall delay of the circuit .

The main function of the ECC (Error Correcting Code) is to correct single-bit errors, whether it is temporary or permanent faults. Nonetheless, when a defective cell is utilized in the system, this can trigger multiple recurrences of permanent faults. When the defects of the cells and frequency of the fault accumulates, there is a great possibility that the device/ gadget cannot be used anymore. Therefore, in limiting the redundancy of the interface design, the researchers recommended that a spare register will be used. This is necessary because it controls the occurrence of errors in LUT register which cause failure of the entire core to reach its target destination in the NI system. The important role played by the bit in the status register, is that it specifies the functional and the faulty LUT through the selection of either the regular or the spare register [7].The least significant bits (LSBs) addressed the spare registers by addressing the signal. Hence, the utilization of the TMR has helped in the implementation of the status register and the control logic. The spare registers can be used as an alternative for the erroneous LUT registers which have been detected during the testing- both on the post manufacturing or on run-time.

- **Error Detection and reconfiguration policies**
- **Hamming code data and parity bits.**

The Hamming is a network of codes that allows correction of single-bit data. This assumption was that information to be transmitted is made up of number of data bits u, to this quantity he added the number of check bits p in a way that if the block received the data with error not exceeding 1 bit, then the p can recognize the error. He then used variable k which represents the data bits and m for the number of utilized check bits. Since m, check bits have to recognize information bits, the p value as interpreted by integers must have a range of 0 to m+k, which is m+k+1 distinct values. Moreover, since m bits can distinguish 2^m cases, we must have

$$2^m \geq m + k + 1.$$

The equation is known as the Hamming rule. It is applicable for the checking of all forms of information, specifically on SEC (single error correcting) and codes of binary blocks. Arranging the check bits in a position of power-of-two (1,2,4,8….) provides an advantage in making the path to function independently. Thus, the data sender can encode p0 independently of p1, p2 and so on; thus it enables computing of each check independent from other data.

- **A SEC-DED code**

In the conversion of Hamming code into a SEC-DED code, a single chick bit particularly the parity bit must be added to all bits in the words encrypted in SEC code. This is called the extended Hamming code which is not apparent that it is a SEC-DED. In order to check that it is, refer to Table 2 and it can be observed that the overall parity and syndrome can uniquely determine whether a 0,1 or 2 type of fault has happened. For 1-types error, the receiver cannot recognize the location of the error as to whether one of the errors occurred in the SEC part or both happened in the SEC portion.

Table 2: Adding a Parity bit to make a SEC-DED code

Possibilities			Receiver Conclusion
Errors	Overall Parity	Syndrome	
0	even	0	No error
1	odd	0	Overall parity bit is in error
		≠0	Syndrome indicates the bit in error
2	even	≠0	Double error (not correctable)

The column at the center illustrates the negligible solution to the inequality for the k values. While on the rightmost column the required bit for SECDED code is indicated.

- **Procedure for detecting errors in the LUT**

Fig. 5 presents the procedure applied when detecting errors in the LUT. In the flow working when one permanent fault has been detected in it: the register can still be used for providing a corrected routing information to the packet, thanks to the error correcting capabilities of the Hsiao decoder. In the case where a double error is detected in the considered generic i register, and no working spare registers are available, the whole LUT is considered to have failed, since the NI is not longer able to provide correct routing information for the packet directed to the NoC node associated with the doubly erroneous register. Therefore, the NI should be put offline, or the node memory-mapped to the address associated with the failed register should no longer be addressed by the NI communications.

As shown in Fig. 5, if a single error is detected during the lookup of a LUT register considered as working, the system reacts by performing a check to determine if the error was caused by a permanent fault. The check consists in copying the information read from the LUT"s i register, corrected by the SECDED decoder, into the same LUT register.

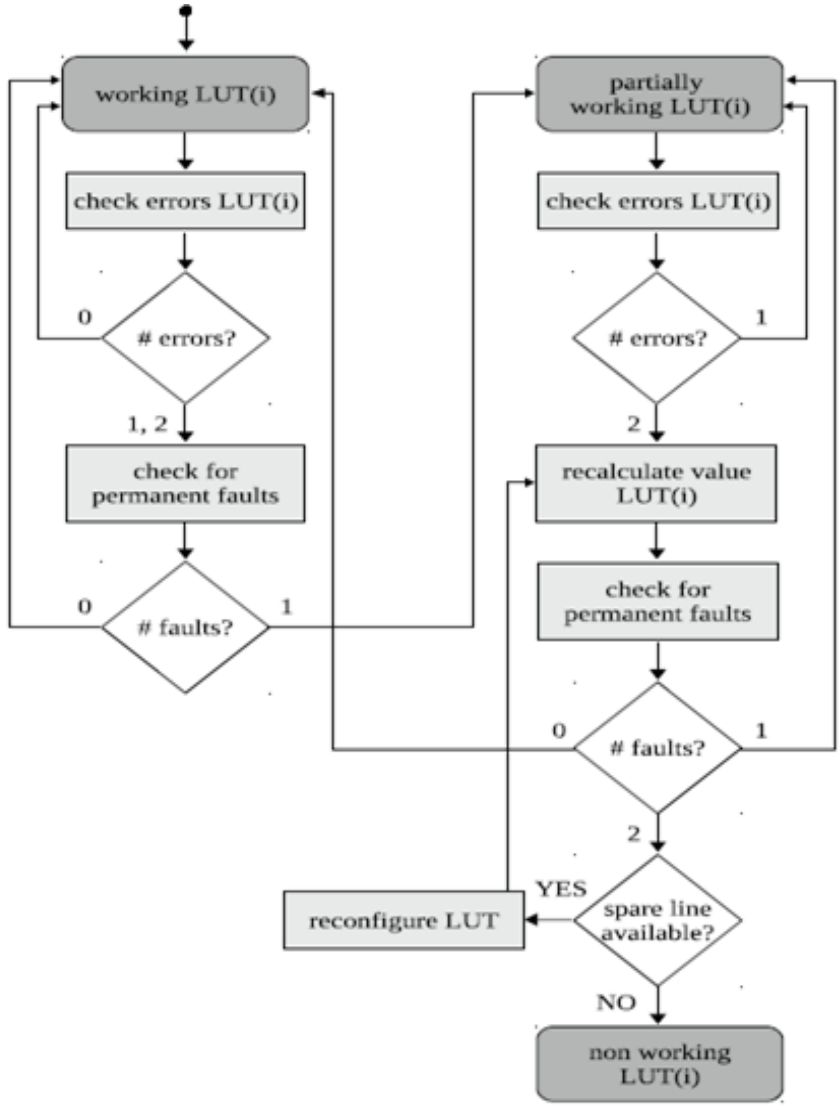

Fig. 5: Diagram describing the reconfiguration policy applied when detecting errors in the LUTs.

After this operation, if the register still presents a single error, the fault is considered as permanent, and the LUT register as partially working. The detection of a double error in a partially working register requires recalculation of the routing path associated with it. The recalculation of the routing path is performed by running a software routine that applies the rules of the routing algorithm implemented into the NoC for finding the path to the destination. Without loss of generality, we can assume this routine to be implemented in a fault-tolerant NoC, being in fact needed for dealing with permanent faults in links and router components.

After the recalculation, the information is copied in the register and checked again for errors. If working spare elements are still available, the LUT is reconfigured by enabling the use of the associated spare register, and still considered as working. Otherwise, it is considered as not working.

- **System Implementation**
- **Flow of system implementation**

In Fig. 4, the proposed design which allows increased way of recognizing codes and limiting the occurrences of design redundancy therefore, allowing the researchers to work on faults in the LUT system. On the other hand, the data circuit is saved though the application of the Single Error Correcting and Double Error Detecting (SECDED) Hsiao code [11] which are capable of automatically correcting the error .Moreover, it can also detect up to two connection faults in every LUT system. The researchers chose the Hsiao code due to its ability of allowing a uniform and equal allocation of the XORs during the encoding and decoding process. As a result, it can reduce the quantity of logic ports and can diminish the overall delay of the circuit [11].

- The main function of the **ECC (Error Correcting Code)** is to correct single-bit errors, whether it is temporary or permanent faults.
- It has been emphasized that the popular row or column substitution technique can be used in addressing permanent faults in RAM.
- **Content Addressable Memory (CAM)** assists in the implementation of the lookup table to function efficiently in one clock cycle by utilizing the comparison circuitry. CAMs have gained popularity in the communication network system, especially in forwarding of packets as well as on classification. However, it is advantageous in several other applications that needs high speed LUT.
- One error-correcting code may be considered ineffective; however, it is capable of accepting all the blocks that are directed towards it. One important feature of **single error correction double error detection (SECDED)** code is it is safer and it is mostly used in the correction and detection of faults in memories of computer .It also used the famous Hamming code which can be transformed to a SECDED code through adding one check bit to the SEC code words, making it unrecognizable that it is actually Hamming code.
- The researchers involved design of **spare registers** in order to supply redundancy mechanism to the **LUT**. An alternative to the LUT registers are used for that path with more than one fault which is not anymore capable of storing transmitted information within the circuit.
- The **Hamming** is a network of codes that allows correction of single-bit data. This assumption was that information to be transmitted is made up of number of data bits u, to this quantity he added the number of check bits p in a way that if the block received the data with error not exceeding 1 bit, then the p can recognize the error.
- In the conversion of Hamming code into a **SEC-DED code**, a single chick bit particularly the parity bit must be added to all bits in the words encrypted in SEC code. This is called the extended Hamming code which is not apparent that it is a **SEC-DED.**

II. Testing And Results

- **Synthesized and Simulation results**
- **SECDED Encoder**

Table 3 shows the bit positions for data bit and parity bits

Bit Position	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
Bit Number	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Data/Parity Bit	P5	D 15	D 14	D 13	D 12	D 11	P4	D 10	D9	D8	D7	D6	D5	D4	P3	D3	D2	D1	P2	D0	P1	P0

The parity bits P0-P4 are created for single error detection and correction and are created as follows:

- P0=D15⊕D13⊕D11⊕D10⊕D8⊕D6⊕D4⊕D3⊕D1⊕D0
- P1=D13⊕D12⊕D10⊕D9⊕D6⊕D5⊕D3⊕D2⊕D0
- P2=D15⊕D14⊕D10⊕D9⊕D8⊕D7⊕D3⊕D2⊕D1
- P3= D10⊕D9⊕D8⊕D7⊕D6⊕D5⊕D4
- P4= D15⊕D14⊕D13⊕D12⊕D11

Table 4: Error Detection

Syndrome	Overall Parity (P5)	Error Type	Notes
0	0	No Error	
/=0	1	Single Error	Correctable. Syndrome holds incorrect bit position.
/=0	0	Double Error	Not correctable.
0	1	Parity Error	Overall parity, P5 is in error and can be corrected.

➢ **Synthesis Report of SECDED encoder**

- **SECDED Encoder Simulation output**

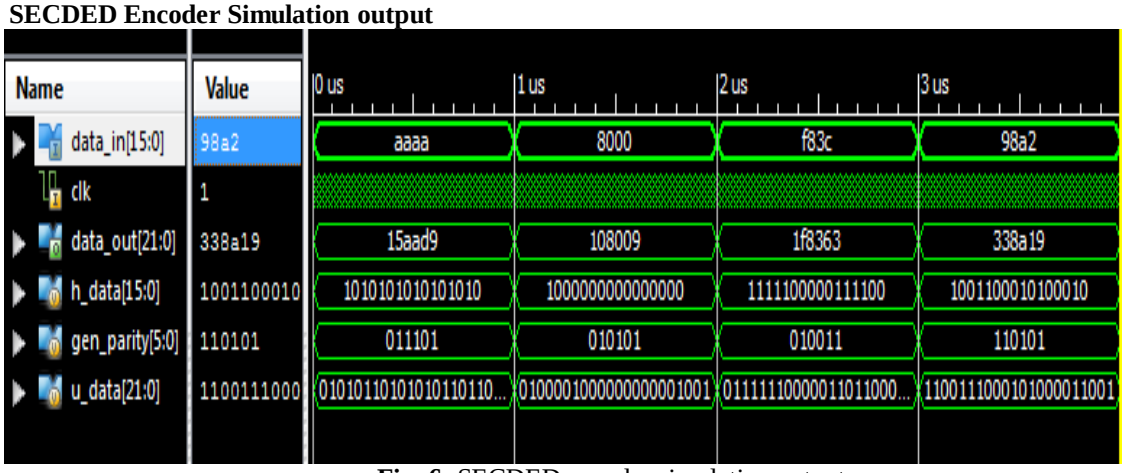

Fig. 6: SECDED encoder simulation output

➢ **SECDED Decoder**

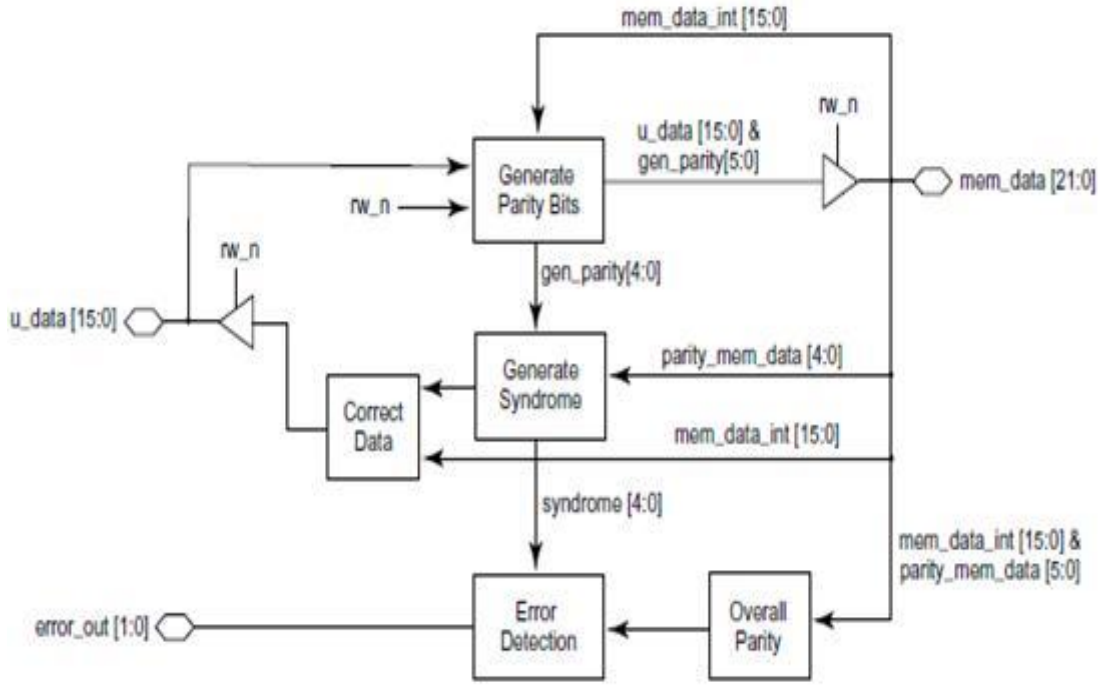

Fig. 7: Block diagram of SECDED decoder

Fig. 7 shows block diagram for Single error correction and Double error Detection. The input to SECDED encoder is 16 bit data, and encoder generates parity bit of P0-P5. The input to SECDED decoder is 22 bit patter declared as mem_data[21:0] in verilog code which is compared with decoder generated parity bits i.e gen_parity[4:0]. Suppose a code word is transmitted to a receiver

- Let, **u** denote the information bits received,

p denote the check bits received, and **s** (for syndrome) denote the exclusive or of p and the check bits calculated from u by the receiver. Then examination of Table 4 reveals that s will be set as shown in Table 3 for zero or one errors in the code word.

- **Synthesis Report of SECDED Decoder**
- **SECDED Decoder Simulation output**

As shown in Fig. 8. The output simulation for SECDED decoder it decodes incoming 22bit data pattern. The data out is represented as data_out[15:0] in verilog code and error out is considered as follows,

If error_out is 00 – No error.
If error_out is 01 – Single error, correctable syndrome holds incorrect bit position.
If error_out is 10 – Double error. Not correctable.
If error_out is 11 – Parity Error, Overall parity, P5 is in error and can be orrected.

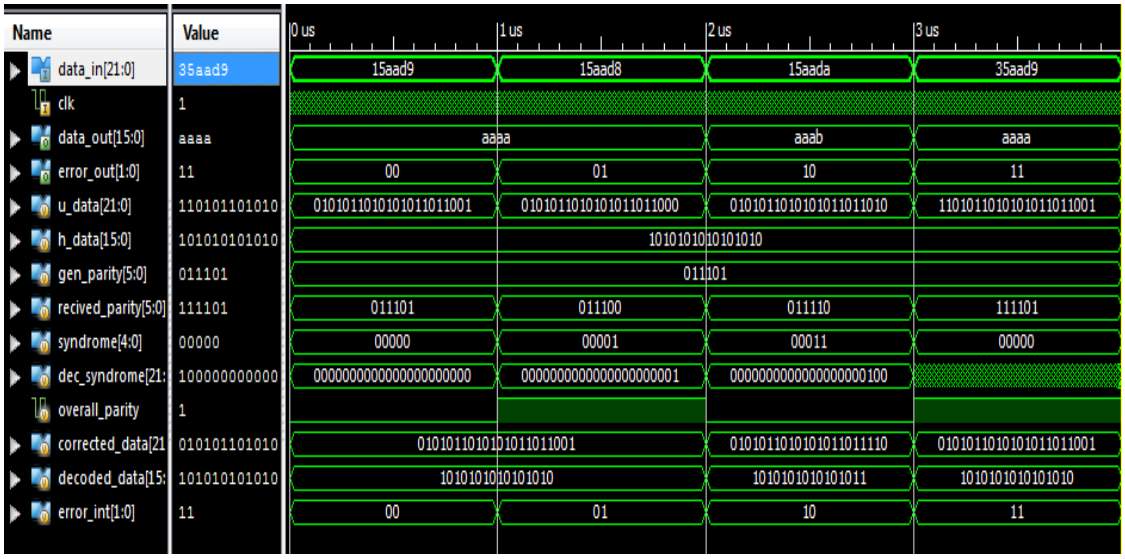

Fig. 8: SECDED decoder simulation output

- **Configurable LUT**

The look-up table (LUT) is by far the most versatile circuit to create a configurable logic function. In order to provide architectural redundancy to the LUT, we included in the design a certain number of spare registers that are meant to substitute LUT registers in which the number of faults is higher than one, and that cannot therefore be anymore employed for storing correctly the routing information. These spare registers are of critical importance because a defective LUT register will cause an entire core not to be reachable from that Network Interface.

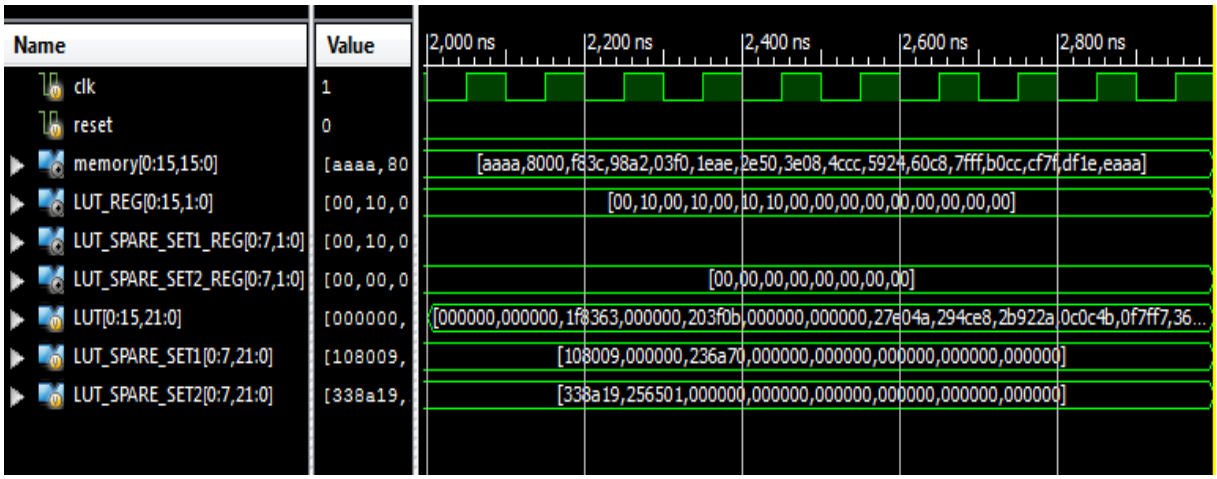

Fig. 9: LUT encoder decoder simulation output

If error is 00 – No error, (No need of using spare register)
If error is 01 – One error error, (No need of using spare register)
If error is 10 – More than one error, (Need to use spare register)

➢ **Simulation result of LUT encoder decoder with fault injection along with CAM operation**

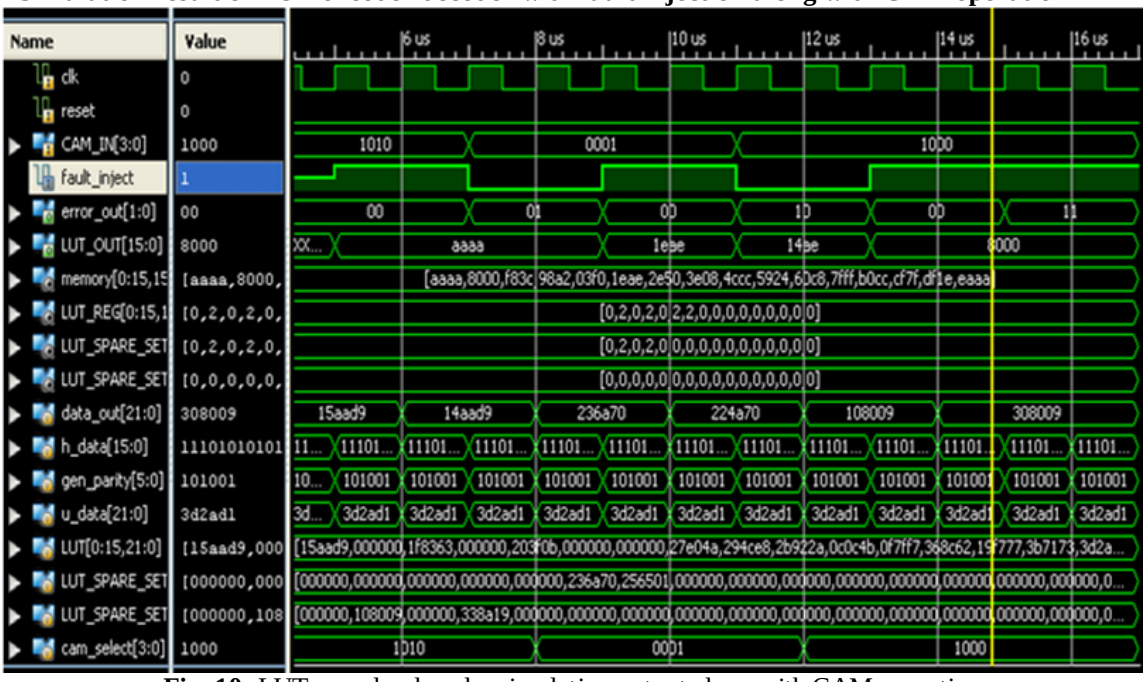

Fig. 10: LUT encoder decoder simulation output along with CAM operation

➢ **Triple Modular Redundancy (TMR) and Proposed SECDED**

- **Triple Module Redundancy (TMR)**

The most common example of TMR is a d-type flip-flop that has been triplicated and to which a voter has been added on its output. In computing, triple modular redundancy, sometimes called triple-mode redundancy, (TMR) is a fault-tolerant form of N-modular redundancy, in which three systems perform a process and that result is processed by a majority-voting system to produce a single output. If any one of the three systems fails, the other two systems can correct and mask the fault [13].

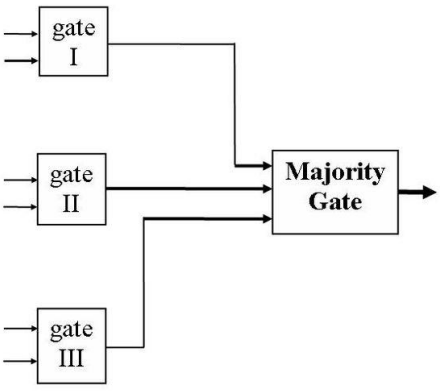

Fig. 11 : Triple Module Redundancy Model

In TMR, three identical logic circuits (logic gates) are used to compute the same set of specified Boolean function. If there are no circuit failures, the outputs of the three circuits are identical. But due to circuit failures, the outputs of the three circuits may be different. A majority gate is used to decide which of the circuits" outputs is correct. The majority gate output is 1 if two or more of the inputs of the majority gate are 1; output is 0 if two or more of the majority gate"s inputs are 0. The majority gate is a simple AND–OR circuit: if the inputs to the majority gate are denoted by x, y and z, then the output of the majority gate is

$$xy \vee yz \vee xz$$

Thus, the majority gate is the carry output of a full adder, i.e., the majority gate is a voting machines.

- **Hamming code with additional parity (SECDED)**

Hamming codes have a minimum distance of 3, which means that the decoder can detect and correct a single error, but it cannot distinguish a double bit error of some codeword from a single bit error of a different codeword. Thus, they can detect double-bit errors only if correction is not attempted [12].

- **Synthesis Report**

Table 5 : Devise Utilization and Synthesis Summary(TMR and SECDED)

Specifications	Design	
	TMR Based	Proposed SECDED Based
Number of 4 input LUTs:	87	59
Number of Flip-Flops:	36	13
Maximum Frequency (in MHz)	750	127.33
Net Read Latency (ns)	1.1860	1.9225
Net Write Latency (ns)	1.0000	2.6053

III. Conclusion

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 livelock [3]. Moreover, the study showed how NI could become a primary source of error in the system of NoC specially when there is an increase in the quantity of node. The suggested and recommended fault model in the study was the result of the analysis of the behavior of the NI which is driven by the main components of the system like the look up table (LUT). The suggested architectural solutions, on the other hand, were based on the observations done in correcting error and detecting codes from limited redundancy. Moreover, the discussed policies indispensable for the reconfiguration of the components should be implemented during the occurrence of error and the detecting of its cause.

The synthesis and placement of route results demonstrate the increase of performance upon the utilization of on-chip system. During the investigation, the implementation of SECDED showed a positive outcome, especially in the area utilization and also in the improvement of the response time to the system to the standard hardware which is used as a substitute for the TMR hardware.

Bibliography

[1]. Chen, S.J., Lan, Y.C., Tsai, W.C, & Hu, Y. "Fault Tolerance in BiNoC". Springer. 2012. 157-171.

[2]. Collet, J.H., Louri, A., Tulsidas, V. & Poluri, P. "ROBUST: A new Self-healing Fault-Tolerant NoC Router". University of Arizona. 5-17.

[3]. Grecu, C., Anghel, L., Pande, P., Ivanov, A. & Saleh, R. "Essential Fault-Tolerance Metrics for NoC Infrastructures". International Online Testing Symposium. 2007. 1-6.

[4]. Koupaei, F.K., Khademsadeh, A. & Janidarmian, M. "Fault-Tolerant Application-Specific Network-on-Chip". Proceedings of the World Congress on Engineering and Computer Science. 2011. 1-5.

[5]. Lehtonen, P. Liljeberg, T, & Plosila,J. "Online reconfigurable self-timed links for Fault-tolerant NoC." VLSI Design. 2007. 1-13.

[6]. Meloni, P., Tuveri, G., Raffo, L., Cannella, E., Stefanov, T. Derin, O., Fiorin, L. & Sami, M. "System Adaptivity and Fault-tolerance in NoC-based MPSoCs: the MADNESS Project Approach". Euromicro Conference on Digital System. 2012. 517-524.

[7]. Murali, T. Theocharides,. N. Vijaykrishnan, M. J. Irwin, L. Benini, G. De Micheli, "Analysis of error recovery schemes for networks on chips", IEEE Design and Test of Computers, Sept.-Oct. 2005. 434-442.

[8]. Radetzki, M., Feng, C., Zhao, X & Jantsch, A. "Methods for Fault Tolerance in Networks-on-Chip". ACM Computing Surveys. 2013. 46 (1). 1-38.

[9]. Ren, Y., Liu, L., Yin, S., Han, J., Wu, Q, & Wei, S. " A fault tolerant NoC architecture using quad spare mesh topology and dynamic reconfiguration.Journal of Systems Architecture. 2013. 59 (7): 482-491.

[10]. Sharma, T. & Braun, C. "Fault Tolerant Network on chips Topologies". Institut für Technische Informatik. 2009. 1-25.

[11]. M. Y. Hsiao, "A Class of Optimal Minimum Odd-weight-column SEC-DED Codes,"BM Journal of Research and Development, vol. 14, no. 4, pp. 395 –401, july 1970

[12]. Riaz Naseer, Rashed Zafar Bhatti, Jeff Draper, "Analysis of Soft Error Mitigation Techniques for Register Files in IBM Cu-08 90nm Technology," Circuits and Systems, MWSCAS '06. 49th IEEE International Midwest Symposium,2006

[13]. Anup Das, Akash Kumar, Bharadwaj Veeravalli "Fault-Tolerant Network Interface for Spatial Division Multiplexing Based Network-on-Chip," Reconfigurable Communication-centric Systems-on-Chip (ReCoSoC), 7th International Workshop,2012.