

# Design and Implementation of a SEC-DED-DAEC-STECC Error Control Code for Reliable Memory System

Rathinavel Pandian A.<sup>1</sup>, Rasvica Sweety M.<sup>2</sup>, Nandhini S.<sup>3</sup>,  
Negha C.<sup>4</sup>, Sowmiya J.<sup>5</sup>

<sup>1</sup>Professor, <sup>2,3,4,5</sup>Student, Department of Electronics and Communication Engineering, V V College of Engineering, Thoothukudi, India.

**E-mail:** <sup>1</sup>rathinavel2727@gmail.com, <sup>2</sup>rasvicasweety013@gmail.com, <sup>3</sup>sundaramnandhini4@gmail.com,  
<sup>4</sup>neghachithiraikumar@gmail.com, <sup>5</sup>sowmiyajeyaraj365@gmail.com

## Abstract

Modern memory systems are vulnerable to soft errors caused by radiation effects, electrical noise, and process variations, leading to single-bit and multi-bit upsets. The conventional error correction techniques like Hamming and SEC-DED codes have very few defenses against multi-bit complex fault models. In this paper, a (14,8) SEC-DED-DAEC-STECC code is proposed with capabilities of Single Error Correction (SEC), Double Error Detection (DED), Double Adjacent Errors Correction (DAEC) along with selective Triple Bit error pattern corrections. The proposed scheme uses six parity bits with syndrome lookup technique to correct the fault patterns. It is based on parity check matrix and syndrome based localization to increase the fault tolerance with moderate hardware cost. The Encoder/Decoder design has been developed using Verilog HDL and validated through Xilinx ISE environment. The experiment results prove successful correction of single bit, adjacent double bit and selective triple bit fault patterns whereas the uncorrectable faults are detected and flagged properly. The synthesis results of FPGA technology prove the maximum frequency and critical path delay as 182 MHz and 5.48 ns respectively.

**Keywords:** Selected Triple-Bit Error Pattern Correction (STECC), Triple Error Detection (TED), Advanced Error Correction Codes (ECC), Multi-Bit Upset Mitigation, Reliable SRAM

Architecture, Syndrome-Based Error Localization, Fault-Tolerant VLSI Systems, Hardware Reliability Enhancement.

## 1. Introduction

The consistent development of semiconductor technology has led to the creation of high density memory systems with better storage capacity and performance. Nevertheless, the shrinkage of devices makes memory cells more sensitive to soft errors that include radiation effect, electrical noises, and process variations. Such factors can lead to Single-Bit Upset (SBU), Double-Bit Upset (DBU), and Multiple-Bit Upset (MBU) of memory cells.

Error Correcting Codes (ECCs) are used to ensure fault tolerance in memory systems. Standard Hamming codes support Single Error Correction (SEC), whereas SEC-DED codes allow not only for correction but also for detection of Double Error (DED). Such error detecting and correcting schemes are efficient in case of single-bit faults. Still, they do not provide reliable protection against adjacent double-bit errors and further multi-bit errors.

In order to enhance fault coverage, this paper presents a (14,8) SEC-DED-DAEC-TEC code scheme that is able to detect and correct Single Errors (SE), Double Errors (DE), Double Adjacent Errors (DAE) as well as Selected Triple-Bit Error Patterns (STE). The suggested implementation uses six parity bits, a design based on a parity check matrix and error location using a syndrome table. The encoder and decoder modules were designed using Verilog HDL and the results have been verified in the Xilinx ISE environment. FPGA synthesis was done to analyze the hardware requirements.

The major contributions of this work are summarized as follows:

- Development of a (14,8) SEC-DED-DAEC-TEC coding scheme for effective memory protection.
- Design of the parity check matrix and syndrome look up table for multiple error correction.
- Ability to correct single bit, adjacent double bit, and triple bit errors.
- Implementation in Verilog HDL, functionality and performance evaluation using FPGA.

- Improved fault coverage than standard SEC-DED schemes without any significant increase in hardware complexity.

This research paper is organized in the following manner. The review of the related literature on memory error correction techniques is given in Section 2. The basics of error correcting codes and memory protection are described in Section 3. Section 4 describes the (14,8) SEC-DED-DAEC-TEC coding scheme with the details of H-matrix, encoder, and decoder. The simulation results are provided in Section 5. Finally, Section 6 concludes the research work.

## 2. Literature Review

In the research carried out by Parrini et al., [1], the possibility of using error detection and correction codes for in-memory computing safety was investigated. The researchers developed new ECC methods that can be used for providing reliable memory computing through the application of ECCs that protect data integrity during the process of computation in memory. In the research conducted by Zhong et al. [2], a technique for correcting errors in quantum key distribution through the use of Hamming code techniques was proposed. The researchers used adaptive error correction in order to increase the efficiency of quantum key distribution in the presence of noise in the channel of communication. Nair et al. [3] recommended the use of XED which is an error correction framework that can be applied in improving memory reliability through the use of error detection on die. Unlike previous techniques where ECCs were used only, this technique utilizes the information gained from error detection and correction on die.

Pontarelli et al. [4] developed an error detection and correction algorithm based on Bloom filters used for content addressable memory. These techniques employed efficient data structures and fault detection algorithms to improve the performance of memory. The algorithm is capable of eliminating errors from the memory with least compromise on efficiency during hardware realization. Satyanarayana et al. [5] developed and implemented an error detection and correction scheme for the application of semiconductor memory. The main emphasis of the researchers was on designing an efficient ECC that can improve the performance of memory by correcting errors in the memory resulting from soft failure errors. Tambatkar et al. [6] proposed a 3-dimensional parity check with Hamming code for semiconductor memory application. It is based on generation of parity bits along rows, columns and diagonals.

The idea of HVPDH code was introduced by Raha et al. [7]. They utilized horizontal parity with the use of vertical parity and diagonal Hamming code in order to increase the fault tolerance capability. Experimental results indicated that there is an ability to correct multiple-bit errors while maintaining lower encoding overhead. Ge et al. [8] presented memory architecture design for improving memory reliability and security through algebraic manipulation detection codes and error correction mechanisms. In their research work, they have stressed upon the need to detect memory data corruption and protect it from any kind of attacks that can modify memory data without intention.

Memory reliability analysis via SEC codes has been conducted by Maestro and Reviriego et al. [9]. In their study, they found out that SEC codes offer effective protection against single-bit errors, but their performance becomes ineffective when the probability of multi-bit errors becomes high. The study validated the significance of developing efficient methods for correcting multi-bit errors. Park et al. [10] have proposed a novel approach for detecting and correcting errors through a reliable Ex-Logic gate structure in in-memory computing. The study pointed out the growing problem of reliability in in-memory computing and revealed how a customized fault tolerance logic can increase the detection and correction of errors without compromising on efficiency.

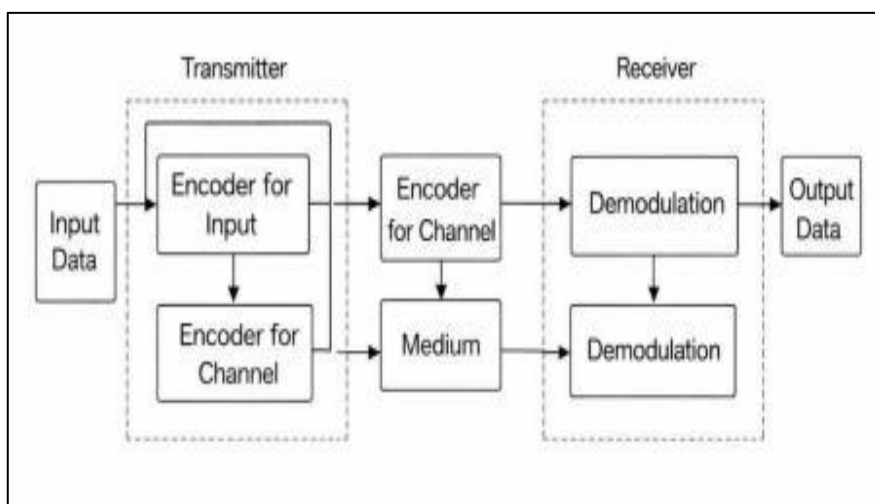
From the existing literature, one can clearly conclude that, while traditional Hamming codes and SEC schemes provide adequate protection against single-bit failures, they do not have any substantial capability to address problems arising from multi-bit upsets. This problem has forced researchers to look into alternative approaches, which include advanced parity codes, multi-dimensional codewords, and ECC schemes. Extending previous research in this area, the present study introduces an innovative SEC-DED-DAEC-TEC scheme, which provides capabilities of SEC, DED, DAEC, and TEC, respectively.

### **3. Error Correcting Codes in Memories**

Error Correcting Codes (ECCs) play a vital role in ensuring reliable data storage and transmission in modern digital systems. Through adding some redundancy in the form of coding in the data originally present, ECC helps in detecting and correcting any errors that may arise in the course of communications and memory processing. ECC basics are well explained by communications channel models.

### 3.1 Communication Channel

In a normal communication process, the information is carried from a source point to a destination point via a communication channel (Medium). In preparation for sending the information, the information at the source point goes through encoding in order to produce some redundancy in form of parity and to produce a protected code word.



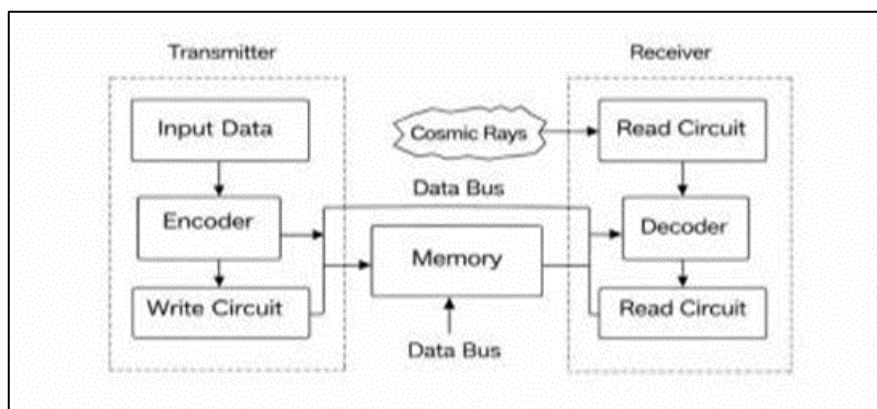
**Figure 1.** Block Diagram of Communication Channel

At the receiver end, a decoder detects and corrects the errors using the encoded parity bits in the received code word. The decoded data is then retrieved and forwarded to its destination. As seen from the communication channel model in Figure 1, error correction coding represents the core concept underlying the reliable digital communication systems. Hamming code, BCH code, Reed-Solomon codes, and multi-bit error correction codes, among others, are commonly used error correction methods employed in the communication systems to ensure reliable communications.

### 3.2 Memory System

The principles of error correction coding can also be applied to memory systems. Instead of transmitting information through a communication channel, data are stored in memory cells for a certain period and retrieved when required by the system. During the write operation, the input data are processed by the ECC encoder, which generates the required parity bits and forms the encoded codeword before it is stored in memory. While the encoded data reside in memory, they may be affected by transient faults such as radiation-induced soft errors, electrical noise, and process variations, which can alter one or more bits of the stored data.

As part of the read process, the codeword stored in memory is accessed and fed to the ECC decoder circuit. The syndrome bits are generated by the decoder, error location and correction are performed, and the data is provided at the system output.



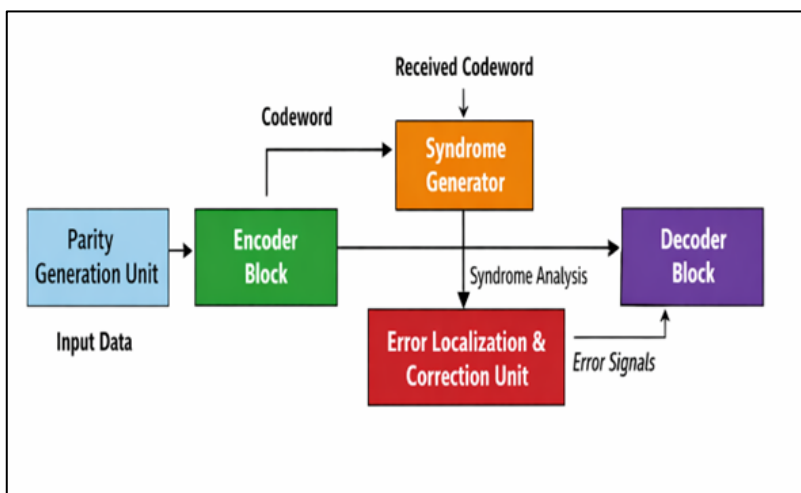
**Figure 2.** Block Diagram of Memory System

The memory protection scheme is depicted in Figure 2. Use of ECC techniques greatly enhances the reliability of memories due to their ability to withstand the effect of transient faults and multiple-bit upsets. Therefore, ECC-enabled memory designs find broad applications in present-day computing, communication, storage, and embedded systems.

#### 4. Proposed SEC-DED-DAEC-TEC Code Technique

In order to increase memory reliability for multiple bit upsets, we suggest a (14,8) SEC-DED-DAEC-TEC code that can carry out single error correction (SEC), double error detection (DED), double adjacent error correction (DAEC) as well as selected triple-bit error pattern correction (STECC). While SEC-DED codes offer only error correction for single bit fault conditions, the suggested architecture increases the number of errors for which fault tolerance is available through parity relationships and error localization using syndrome computations.

The proposed architecture has three main functional blocks, including parity generation block, syndrome generation block and error localization/correction block, which are illustrated in Figure 3. The process of encoding involves generating six parity bits from eight information bits resulting in a 14-bit protected codeword. In the process of decoding, the incoming codeword is checked by syndrome computation and lookup error localization in order to correct single bit, adjacent double bit and predefined triple-bit error patterns.



**Figure 3.** Proposed SEC-DED-DAEC-TEC Architecture

The proposed SEC-DED-DAEC-TEC system ensures improved fault tolerance with minimal hardware cost. Thus, it is applicable to dependable memory systems employed in safety critical and dependable applications. The structural properties and error correction ability of the suggested coding scheme are given in Table 1. The H-matrix design, encoder circuit, decoder circuit and correction based on syndromes are illustrated in the next subsections.

**Table 1.** Parameters of the Proposed SEC-DED-DAEC-TEC Code

Parameter	Value
Information Bits (k)	8
Parity Bits (r)	6
Codeword Length (n)	14
Single Error Correction (SEC)	Supported
Double Error Detection (DED)	Supported
Double Adjacent Error Correction (DAEC)	Supported
Selected Triple-Bit Error Pattern Correction (STEC)	Supported

The proposed coding scheme increases the fault tolerance of conventional SEC-DED coding scheme by offering improved tolerance to adjacent double faults and selected triple bit fault patterns using syndrome based decoding technique.

#### 4.1 H-Matrix Construction and Syndrome Derivation

The parity check matrix  $H$  has an important part to play in establishing the ability of the proposed (14,8) SEC-DED-DAEC-TECC code in detecting and correcting errors. This is because the matrix is such that each column denotes a distinct syndrome for a particular codeword bit.

The parity-check matrix is defined as:

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

For the received codeword

$$r = c + e \quad (2)$$

the syndrome vector is computed as

$$S = Hr^T \quad (3)$$

Substituting  $r = c + e$ ,

$$\begin{aligned} S &= H(c + e)^T \\ S &= Hc^T + He^T \end{aligned} \quad (4)$$

Since every valid codeword satisfies

$$Hc^T = 0 \quad (5)$$

the syndrome becomes

$$S = He^T \quad (6)$$

For a single-bit error occurring at location  $i$ ,

$$e = e_i \quad (7)$$

therefore

$$S = He_i^T = h_i \quad (8)$$

Where  $h_i$  is the  $i^{\text{th}}$  column of  $H$ . Thus each single-bit error generates a unique syndrome. For double adjacent errors:

$$S = h_i \oplus h_{i+1} \quad (9)$$

For triple errors,

$$S = h_i \oplus h_j \oplus h_k \quad (10)$$

All valid syndromes of the SEC syndromes, DAEC syndromes, and selected triple-bit error syndromes are precomputed and stored in the syndrome lookup table of the decoder. Only syndrome patterns having unique error localization capabilities are present in the correction table. The parity-check matrix was constructed in such a way that it can produce unique syndrome patterns for single bit error cases, double bit error cases for adjacent bits and some predefined triple-bit error cases considered in this study.

The capability of the proposed design in correcting error is verified using syndrome-based error localization technique and functional verification of the lookup table implementation. Coding theoretic proof of the minimum Hamming distance derivation, completeness of syndrome uniqueness analysis, and exhaustive enumeration of all multi-bit error cases is out of scope for the current study. Hence, the proposed design is a syndrome-lookup-based error correction scheme rather than a universal linear block code with triple error correction capability.

## 4.2 SEC-DED-DAEC-TEC Encoder

The primary function of the SEC-DED-DAEC-TEC encoder is to generate an encoded codeword by appending parity bits to the original data bits. The coding technique utilizes an 8-bit data sequence  $(d_1, d_2, \dots, d_8)$  to produce a codeword of 14 bits by addition of 6 parity bits. The parity bits are computed based on the parity check matrix guidelines, which allow achieving the functions of SEC, DED, DAEC, and STEC. At the encoding stage, the data bits enter the parity generation network, consisting of XOR logic gates. Each parity bit is calculated on the basis of a certain combination of the data bits.

The parity equations are expressed as

$$p_1 = d_8 \oplus d_6 \oplus d_3 \oplus d_2$$

$$p_2 = d_7 \oplus d_6 \oplus d_5 \oplus d_4 \oplus d_2$$

$$p_3 = d_8 \oplus d_7 \oplus d_4 \oplus d_2 \oplus d_1$$

$$p_4 = d_8 \oplus d_5 \oplus d_3 \oplus d_1$$

$$p_5 = d_7 \oplus d_5$$

$$p_6 = d_6 \oplus d_4 \oplus d_3 \oplus d_1$$

where  $\oplus$  denotes the modulo-2 XOR operation. After generating the parity bits, the encoder forms the complete 14-bit codeword as  $C = \{d_1, d_2, d_3, d_4, d_5, d_6, d_7, d_8, p_1, p_2, p_3, p_4, p_5, p_6\}$ . The generated codeword is subsequently stored in memory or transmitted through a communication channel.

### 4.3 SEC-DED-DAEC-TEC Decoder

Error detection, error classification, and error correction are conducted using the decoder on the received 14-bit codeword. At the time of reading from memory or receiving data, the codeword may be corrupted due to soft errors that may be introduced during the operation because of radiation-induced upsets, noise, manufacturing defects, or transient faults. For reconstructing the codeword, the syndrome-based method is used by the decoder. The received codeword is initially fed into the syndrome generator, where syndromes ( $s_1, s_2, \dots, s_6$ ) are generated.

$$s_1 = \text{encode}_{14} \oplus \text{encode}_{12} \oplus \text{encode}_9 \oplus \text{encode}_8 \oplus \text{encode}_6$$

$$s_2 = \text{encode}_{13} \oplus \text{encode}_{12} \oplus \text{encode}_{11} \oplus \text{encode}_{10} \oplus \text{encode}_8 \oplus \text{encode}_5$$

$$s_3 = \text{encode}_{14} \oplus \text{encode}_{13} \oplus \text{encode}_{10} \oplus \text{encode}_8 \oplus \text{encode}_7 \oplus \text{encode}_4$$

$$s_4 = \text{encode}_{14} \oplus \text{encode}_{11} \oplus \text{encode}_9 \oplus \text{encode}_7 \oplus \text{encode}_3$$

$$s_5 = \text{encode}_{13} \oplus \text{encode}_{11} \oplus \text{encode}_2$$

$$s_6 = \text{encode}_{12} \oplus \text{encode}_{10} \oplus \text{encode}_9 \oplus \text{encode}_7 \oplus \text{encode}_1$$

The syndrome vector thus obtained is decoded using the Error Localization and Correction Unit. If all bits of the syndrome are zero, the incoming codeword is assumed to have no errors. In case of a non-zero syndrome, this implies the existence of one or more errors. The

syndrome pattern is decoded by comparing it with a predefined set of syndrome patterns stored in a lookup table. The faulty pattern is thereby classified based on the syndrome decoding result, as one of the following:

- SE (Single Error): One erroneous bit is identified and corrected.
- DE (Double Error): Two non-adjacent bit errors are detected.
- DAE (Double Adjacent Error): Two consecutive erroneous bits are identified and corrected.
- TE (Triple Error): Three erroneous bits are localized and corrected.
- UE (Uncorrectable Error): Error patterns beyond the correction capability of the code.

After determination of the pattern, a correction vector is calculated and XORed with the incoming codeword, and the operation will bring the distorted bits back to their original state. After that, the decoded codeword is sent to the data extractor stage, from which the initial 8-bit information word will be extracted and sent as an output of the system. After generation of the syndrome vector, a comparison with a predetermined syndrome lookup table residing inside the decoder is carried out. Each specific pattern is associated with a particular error occurrence or a combination of errors. Depending on the matched syndrome, a correction vector is calculated by the decoder to correct the original codeword. Table 2 shows the syndrome lookup table used for error location.

**Table 2.** Syndrome Lookup Table for Error Localization of Single-Bit Errors, Adjacent Double-Bit Errors, and Selected Triple-Bit Error Patterns

Syndrome Pattern	Error Condition	Error Type	Correction Action
000000	No Error	NE	No Correction
000001	Bit-1 Error	SE	Flip Bit-1
000010	Bit-2 Error	SE	Flip Bit-2
000100	Bit-3 Error	SE	Flip Bit-3
001000	Bit-4 Error	SE	Flip Bit-4
010000	Bit-5 Error	SE	Flip Bit-5
100000	Bit-6 Error	SE	Flip Bit-6

000011	Adjacent Bits (1,2)	DAE	Flip Bits 1 and 2
000110	Adjacent Bits (2,3)	DAE	Flip Bits 2 and 3
001100	Adjacent Bits (3,4)	DAE	Flip Bits 3 and 4
011000	Adjacent Bits (4,5)	DAE	Flip Bits 4 and 5
110000	Adjacent Bits (5,6)	DAE	Flip Bits 5 and 6
101011	Bits (1,4,7)	TE	Flip Bits 1, 4, and 7
110101	Bits (2,5,8)	TE	Flip Bits 2, 5, and 8
111001	Bits (1,3,6)	TE	Flip Bits 1, 3, and 6
Invalid Syndrome	Four or More Errors	UE	Generate Error Flag

The syndrome table consists of representative cases for single bit, adjacent double bit, and some triple bit error cases. For the proposed codeword of 14-bits, a total of  $C(14,3) = 364$  triple bit error combinations are possible. Nevertheless, the proposed decoding scheme is not capable of correcting all kinds of triple bit error cases. The correction is only performed on specific triple bit error cases whose syndromes are unique and recorded in the table. Those triple bit error cases which are not included in the syndrome table are treated as uncorrectable and an error flag is generated for those cases.

### 5. Simulation Results and Performance Analysis

The designed SEC-DED-DAEC-TEC scheme was modeled using Verilog HDL and validated using the Xilinx ISE platform. Functional testing was conducted through the introduction of different faulty conditions to the encoded data stream to test the ability of the proposed system in detecting and correcting the errors. Moreover, FPGA synthesis was done to study the hardware requirements, frequency of operation, and decoding latency.

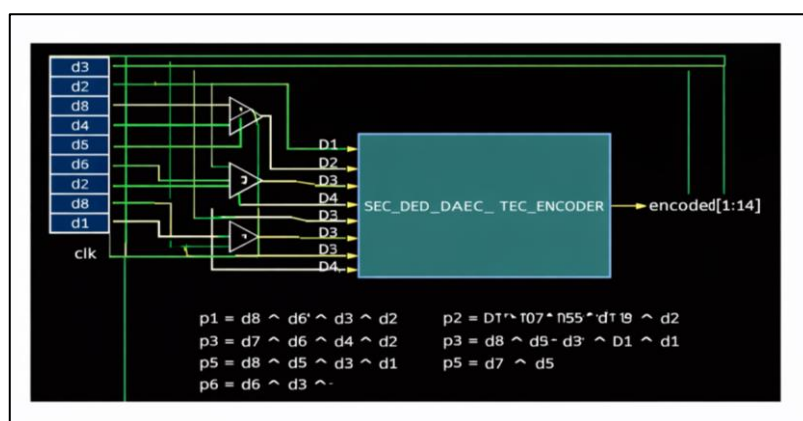
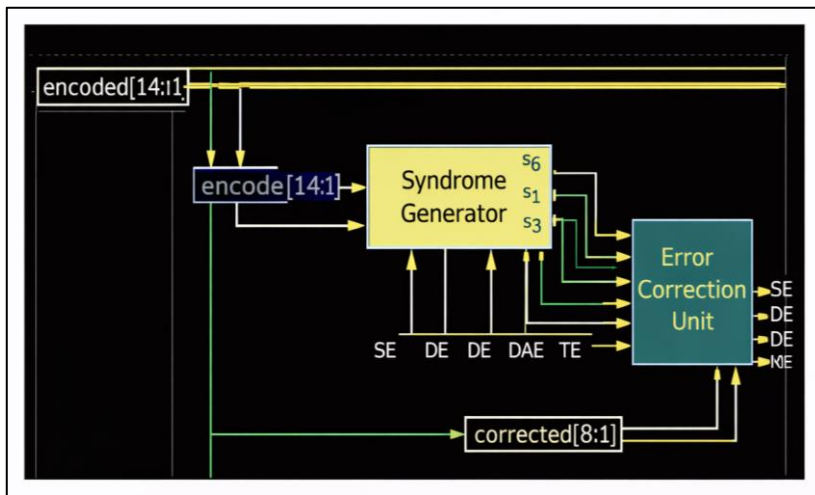


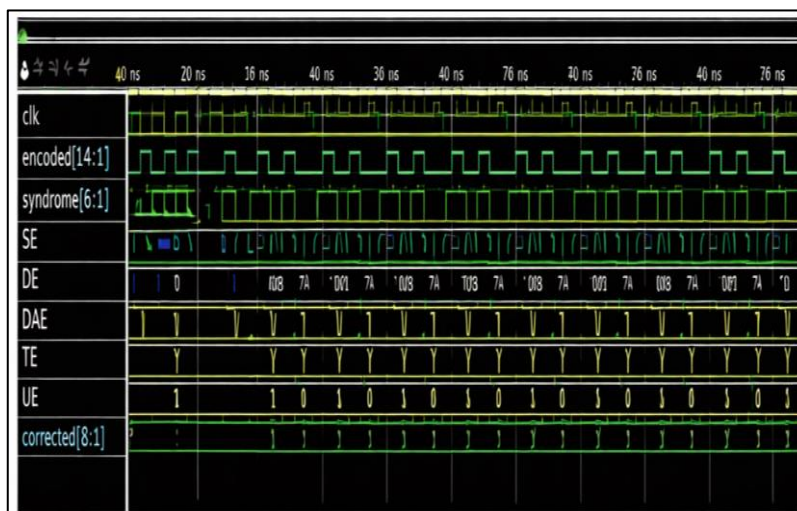
Figure 4. Encoder Simulation Result

The encoder simulation waveforms for different data patterns have been provided in Figure 4. The findings indicate that the six parity bits are generated correctly, and 14-bit codeword is formed correctly.



**Figure 5.** Decoder Simulation Result

Figure 5 shows the decoder simulation waveform. Generated syndromes are able to detect error free, single bit, adjacent double bit, and triple bit fault scenarios, allowing for precise localization and correction.



**Figure 6.** Error Corrections Result

Figure 6 shows the fault pattern correction operation. The decoder is able to decode the data correctly for correctable errors and generate the error signal for uncorrectable error conditions.

**Table 3.** Functional Verification Results

Error Type	Injected Errors	Detection	Correction
No Error	0	Yes	Not Required
Single Error	1	Yes	Yes
Double Error	2 Non-Adjacent	Yes	Detection Only
Double Adjacent Error	2 Adjacent	Yes	Yes
Triple-Bit Error Pattern	Selected 3-Bit Pattern	Yes	Yes
Four Bit Error	4	Yes	Uncorrectable

Table 3 shows the results of functional verifications for various fault conditions. The proposed decoder successfully handles single bit, adjacent double bit, and triple bit errors, but faults of higher order are detected and reported as uncorrectable.

**Table 4.** Hardware Complexity Comparison

Parameter	Hamming Code [6]	SEC-DED [9]	DAEC [7]	Proposed
Data Bits	8	8	8	8
Parity Bits	4	5	5	6
Single Error Correction	Yes	Yes	Yes	Yes
Double Error Detection	No	Yes	Yes	Yes
Double Adjacent Error Correction	No	No	Yes	Yes
Selected Triple-Bit Error Pattern Correction	No	No	No	Yes
Syndrome Bits	4	5	5	6
Fault Coverage	Low	Medium	High	Very High
Hardware Complexity	Low	Medium	Medium	Moderate

The comparison between the proposed SEC-DED-DAEC-TEC method and the existing ECC methods is provided in Table 4. The proposed method uses just an additional parity bit and syndrome bit in comparison with the traditional SEC-DED scheme; however, the correction ability is increased from single-bit errors to adjacent double-bit and triple-bit errors.

It should be noted that the proposed scheme demonstrates high fault coverage at a relatively low hardware cost.

The characteristics of the proposed decoder are presented in Table 5. Throughput of the decoder is computed based on the synthesizing frequency of operation and the correction time of the architecture, which is described further. Throughput of the proposed decoder is determined by the following expression:

$$\text{Throughput} = \frac{\text{Codeword Length} \times \text{Clock Frequency}}{\text{Correction Latency}} \quad (11)$$

For the proposed architecture:

$$\begin{aligned} \text{Codeword Length} &= 14 \text{ bits} \\ \text{Clock Frequency} &= 182 \text{ MHz} \\ \text{Correction Latency} &= 2 \text{ clock cycles} \end{aligned}$$

Substituting these values,

$$\begin{aligned} \text{Throughput} &= \frac{14 \times 182 \times 10^6}{2} \\ &= 1.274 \times 10^9 \text{ bits/s} \\ &= 1.27 \text{ Gbps} \end{aligned}$$

**Table 5.** Decoder Performance Metrics

Parameter	Proposed Architecture
Clock Frequency	182 MHz
Decoder Delay	5.48 ns
Correction Latency	2 Clock Cycles
Throughput	1.27 Gbps
Error Detection Time	1 Clock Cycle
Error Correction Time	2 Clock Cycles

Therefore, the proposed decoder realizes an efficient throughput rate of approximately 1.27 Gbps while correcting single errors, double adjacent errors, and certain three-bit errors. This architecture is capable of achieving a very low decoding delay of 5.48 ns, two cycle delay correction capability, and throughput rates of gigabit speed, thus making it suitable for use in reliable SRAM and embedded memories.

**Table 6.** FPGA Resource Utilization

Resource	Utilization
Slice Registers	118
Slice LUTs	162
Bonded IOBs	28
Occupied Slices	95
Maximum Frequency	182 MHz
Total Power	92 mW
Dynamic Power	31 mW
Static Power	61 mW
Critical Delay	5.48 ns

FPGA synthesis results have been presented in Table 6. The design uses 118 slice registers and 162 look-up tables while consuming very little power and timing. From the results above, it is evident that the architecture designed has improved fault-tolerance and efficient hardware resource usage.

## 6. Conclusion

In this paper, an error correction architecture for modern memory systems based on (14,8) SEC-DED-DAEC-TEC was introduced. Compared with conventional SEC-DED techniques, the proposed method is capable of performing single error correction (SEC), double error detection (DED), double adjacent error correction (DAEC), and correction of predefined triple-bit errors. In this study, the (14,8) SEC-DED-DAEC-TEC coding scheme was implemented in Verilog HDL and verified using functional simulation in Xilinx ISE. Simulation results demonstrated successful correction of the single-bit, adjacent double-bit and triple-bit errors as well as detection of higher fault conditions as uncorrectable. FPGA synthesis results confirmed efficient hardware realization of the designed decoder with relatively low resource consumption, decoding delay and high operational frequency. The proposed architecture provides significantly higher fault coverage with only a modest increase in hardware overhead. Therefore, the proposed SEC-DED-DAEC-TEC scheme is an efficient solution for enhancing the reliability of SRAM systems and embedded platforms.

## References

- [1] Parrini, Luca, Taha Soliman, Benjamin Hettwer, Jan Micha Borrmann, Simranjeet Singh, Ankit Bende, Vikas Rana, Farhad Merchant, and Norbert Wehn. "Error Detection and Correction Codes for Safe In-Memory Computations." arXiv preprint arXiv:2404.09818 (2024).
- [2] Zhong, Xiaodong, and Ge Jin. "Application of Hamming Code Based Error Correction Algorithm in Quantum Key Distribution System." 3rd International Conference on Electronics Technology (ICET) 2020, 857-861.
- [3] Nair, Prashant J., Vilas Sridharan, and Moinuddin K. Qureshi. "XED: Exposing on-Die Error Detection Information for Strong Memory Reliability." ACM SIGARCH Computer Architecture News 2016, vol. 44, no. 3, 341-353.
- [4] Pontarelli, Salvatore, and Marco Ottavi. "Error Detection and Correction in Content Addressable Memories by Using Bloom Filters." IEEE Transactions on Computers 2012, vol. 62, no. 6, 1111-1126.
- [5] Satyanarayana, Telugu, Vaseen Ahmed Qureshi, and G. Divya. "Design and Implementation of Error Detection and Correction System for Semiconductor Memory Applications." In 7th International Conference on Computing in Engineering & Technology (ICCET 2022), 325-330.
- [6] Tambatkar, Shivani, Siddharth Narayana Menon, V. Sudarshan, M. Vinodhini, and N. S. Murty. "Error Detection and Correction in Semiconductor Memories Using 3D Parity Check Code with Hamming Code." International Conference on Communication and Signal Processing (ICCSP) 2017, 0974-0978.
- [7] Raha, Paromita, M. Vinodhini, and N. S. Murty. "Horizontal-Vertical Parity and Diagonal Hamming Based Soft Error Detection and Correction for Memories." International Conference on Computer Communication and Informatics (ICCCI) 2017, 1-5.
- [8] Ge, Shizun, Zhen Wang, P. Luo, and M. Karpovsky. "Reliable and Secure Memories Based on Algebraic Manipulation Detection Codes and Robust Error Correction." In Proc. Int. Depend Symp. 2013.

- [9] Maestro, Juan Antonio, and Pedro Reviriego. "Reliability of Single-Error Correction Protected Memories." *IEEE Transactions on Reliability* 2008, vol. 58, no. 1, 193-201.
- [10] Park, Taegyun, Yeong Rok Kim, Dong Hoon Shin, Byeol Jun Lee, and Cheol Seong Hwang. "Efficient Method for Error Detection and Correction in In-Memory Computing Based on Reliable Ex-Logic Gates." *Advanced Intelligent Systems* 2023, vol. 5, no. 5, 2200341.