

Design and analysis of fault-tolerant sequential logic circuits for safety-critical applications

Shawkat Sabah Khairullah, Farah Natiq Qassabbashi, Jumana Abdullah Kareem

Department of Computer, College of Engineering, University of Mosul, Mosul, Iraq

Article Info

Article history:

Received Jan 6, 2023

Revised Apr 24, 2023

Accepted May 3, 2023

Keywords:

Dependability

Fault

Realization

Reliability

Safety-critical

Sequential

System

ABSTRACT

Safety-critical systems used in applications that demand high levels of dependability, efficiency, and fault-tolerance often use sequential logic circuits in its design and implementation. The safety-critical digital system typically uses latches, flip-flops, and other memory elements, which are prone to the effects of natural faults and single event upsets (SEUs) caused by radiation-induced effects. The faults can lead to subsystem failures due to the continuous advancement in the realization of the small size transistor. To design a reliable digital-based system, it is essential to develop new fault-tolerance approaches that are integrated into the design of sequential logic circuits. This work proposes a novel fault-tolerant approach based on the redundancy of sequential logic circuit, which consists of a variety of design components, D flip-flop storage elements linked to a fault injection unit, a duplicate modular redundancy, and data monitoring units with a switching circuit. The experimental simulation results using a five-state Markov chain analysis model prove that the proposed fault-tolerant system can achieve 0.99999998 for reliability of the fault detection coverage (C) which equal to 0.99999. Finally, we believe that using this new approach of fault-tolerance and redundancy would improve the dependability and reliability of next generation safety-critical applications.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Shawkat Sabah Khairullah

Department of Computer, College of Engineering, University of Mosul

Mosul, Ninawa, Iraq

Email: shawkat.sabah@uomosul.edu.iq

1. INTRODUCTION

Fault-tolerance and reliability analysis plays an essential role in the design and implementation of highly reliable and robust digital control systems [1]–[3]. Safety critical control applications that use these types of electronic digital circuits like avionics, space, and industrial control applications have become more vulnerable to the effects of faults stemming from different natural resources. Examples of these faults are intermittent faults, permanent single faults, transient single faults, multiple bit upsets (MBUs) or common cause faults (CCFs). All these faults may result from different factors like ionizing radiation, harsh environment and electromagnetic interference that can undermine and defeat the traditional fault-tolerant techniques even at the ground level [4]. Faults may affect digital control systems in a different way based on the level of severity of the environment in which the control system is operating. Different fault tolerant digital control systems were developed in the literature works to quickly identify the presence of a digital subsystem failure in the control system and diagnose its causes in terms of type. However, most of the developed digital systems caused low levels of dependability and reliability because of the limited capability of the developed fault tolerance mechanism and the inclusion of additional hardware components that are not necessary to the control system operation. Although there are some traditional fault tolerant techniques based on the hardware redundancy or

the reconfiguration strategies used to mask or correct the event of faults, there is a low fault coverage (C) of meeting high degrees of dependability and reliability in these critical control systems. An example of computer architecture, the field programmable gate array (FPGA) architecture consists of a two-dimensional array of logic blocks and flip-flops connected by the interconnection routing blocks. The logic blocks can perform combinational and sequential logic functions using the look up tables (LUTs) and the memory elements utilized to realize state machine control units. Combinational components like LUTs and routing resources are vulnerable to be affected by permanent faults. These faults can be corrected either by reloading the bitstream file or by resetting the FPGA chip. However, the sequential components like memory flip-flops are vulnerable to transient faults that can be corrected by the next load of configuration bit stream [5].

There are some challenges that stem from applying traditional fault-tolerant techniques in building reliable digital control systems. Firstly, the number of tolerated faults is limited to the number of redundant components available in the digital control system before the whole system fails. Secondly, the failure of redundancy management unit, which monitors the operation of the digital system, coordinates the redundancy of the components, and detects if there is a defect in the working element, may cause a whole system failure even if there are no actual defects in the working system [6]. The major contribution of this research work is overcoming and avoiding these architectural challenges by designing a novel fault-tolerant methodology that includes both static and dynamic redundant fault-tolerant systems. This approach consists of sequential logic circuit, D flip-flop storage elements linked to a fault injection unit, a duplicate modular redundancy, and data monitoring units. The experimental simulation work is presented, and the results prove that the approach achieves a robust fault-tolerant digital control system that can be used as a hardware platform for ultra-dependable and safety-critical control applications.

2. PREVIOUS WORKS

A brief presentation of research works focusing on the topic of fault tolerant digital systems and error detection methods is presented in this section. Different methods were used to create different types of the fault-tolerant digital embedded system as it is shown in Figure 1. All these presented methods are discussed in this section.

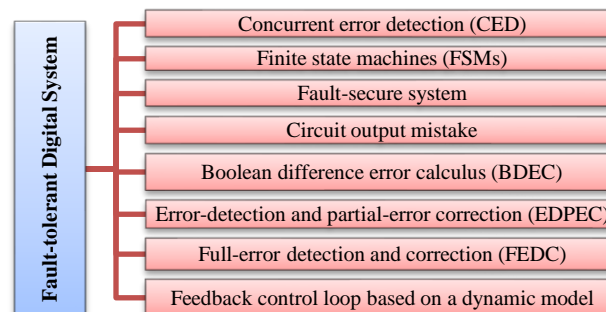


Figure 1. The different methods that were used for creating fault tolerant digital systems, from the literature

Almukhaizim and Makris [7] explained a methodology for creating fault-tolerant digital circuits that was built based on an expansion of the concurrent error detection (CED) method. They used the CED method to accomplish mistake detection as well as to provide error diagnosis and remedy capabilities. A fault tolerance method for sequential logic circuits based on the concept of sequential finite state machines (FSMs) [8], [9]. The suggested method was relied on the addition of redundant comparable states to safeguard a small number of states with a high likelihood of recurrence. All single errors occurring in the state variables of highly occurring states or in their combinational logic were guaranteed to be tolerated by the redundant states. Their method required little space because just a few states require protection as well as improved the fault tolerance of synthesized sequential circuits. Ostanin *et al.* [10] presented a fault-tolerant, low-overhead, and synchronous sequential circuit design. Their approach was based on a fault-secure system. Their method consisted of only one fault-secure sequential circuit, one regular (unprotected), one checker, and one rather straightforward exclusive OR (XOR) circuit. The recommended scheme's dependability was demonstrated for both single stuck-at failures at gate poles and transient, intermittent route delay faults. Each subsequent flaw was said to manifest itself after the preceding one has vanished. Ban and Junior [11]

established a trade-off between reliability and hardware area overhead by applying hardening methods to the arithmetic circuits. Their work also suggested several fault-tolerant strategies in which important component gates in mathematical circuits were identified and rated based on the consequences of a circuit output mistake. Regarding the area limitation of the design requirements, these crucial gates were toughened first. In fact, output bits that were deemed essential to a system were given greater protection priorities, which lowered the likelihood of catastrophic mistakes. The researcher selected the boolean difference error calculus (BDEC) method that was previously suggested in the literature and expanded it in two ways: first, to account for the impact of reliability-enhancement strategies like redundancy, and second, to encompass sequential circuit parts [12]. Dug *et al.* [13] constructed and examined two techniques for creating fault-tolerant pipelined sequential and combinational circuits on a FPGA board. Error-detection and partial error correction (EDPEC), and full-error detection and correction (FEDC) were considered as evaluated approaches. Shalini *et al.* [14] presented a selective triple modular redundancy (STMR) technique, where fault tolerance in digital circuits; hardware redundancy was a suitable approach. To enhance the timing behavior of synchronous sequential circuits, by disregarding the delay, the output was precisely determined. The selection criteria for STMR included latency and failure likelihood. It was demonstrated through simulation that the suggested approach decreased hardware failure by utilizing TMR technique only when necessary. The researchers developed a new a feedback control loop connected to a digital pipeline hardware system with an appropriate dynamic model to lessen the impact of errors and faults effects on the output [15]. The digital blocks whose executed operation was rewinded were selected as data-path registers for the correction loops of a robotic industrial arm which have applied correction factors. They evaluated the cost and reliability of the suggested technique and compared them to the standard TMR approach. In comparison with the triple approach, their method employed 30% fewer slices for FPGA technology. The architectural design of a hybrid and fault-tolerant processing core that is using concepts of error detection and correction against radiation faults is presented, analyzed, and simulated [16]. The error correction codes were embedded among five stages of pipeline processing to identify the run-time faults and operational errors. The experimental timing simulation results indicate that the proposed fault-tolerant method is efficient in consuming digital hardware resources and its software operation is continuously monitored by intelligent fault-tolerant techniques.

3. THE PROPOSED RESEARCH METHOD

The proposed fault-tolerant sequential logic system is created to achieve high standards of dependability in relation to several fault models, including transient, intermittent, and permanent faults. In the proposed fault-tolerant sequential logic system shown in Figure 2, three types of fault tolerance techniques are designed against different types of faults. The basic sequential circuit component that is investigated in this paper is a D flip flop (F-F) memory element, which has two fixed states and can save one bit at one time. In addition, a D flip flop is a bi-stable memory component that can store either a "1" or a "0" bit at a single time. Once the storage memory element reads the D input signal, a checking operation is executed in the circuit to monitor the status of the synchronous clocking signal whether it is high or low, during which point the input signal propagates to the output signal with the rising edge of each synchronous clocking pulse. Furthermore, the complementary of the output signal Q is called Q bar as it is shown in Table 1.

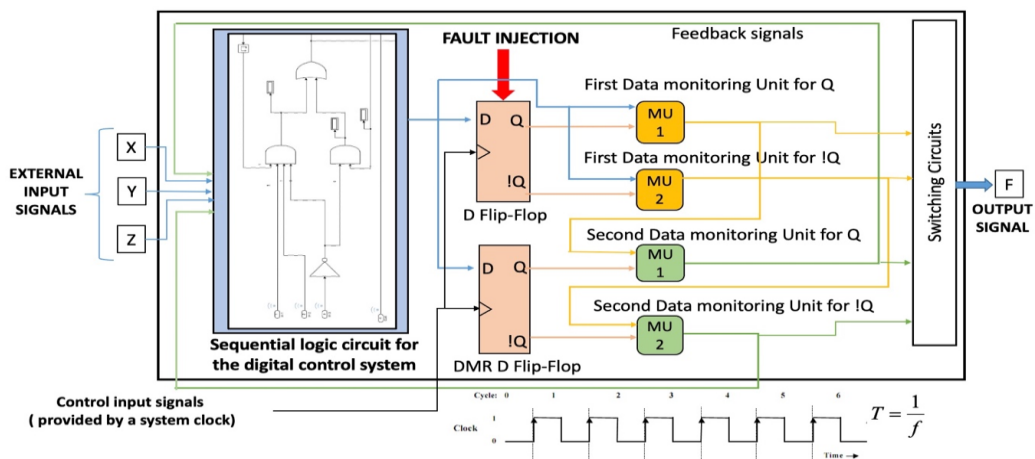


Figure 2. The proposed fault-tolerant sequential logic system

Table 1. D flip flop excitation

| D in | Clocking pulse | Current state Q | Next state Q |
|------|----------------|-----------------|--------------|
| X | 0 | 0 | 0 |
| X | 0 | 1 | 1 |
| 0 | 1 | 0 | 0 |
| 0 | 1 | 1 | 0 |
| 1 | 1 | 0 | 1 |
| 1 | 1 | 1 | 1 |

To design a highly robust sequential fault-tolerant system which can be resilient to the effects of various attacks of natural faults and single upsets, two types of fault tolerance techniques and data monitoring units for the two output signals Q and !Q were architected and embedded in the proposed system. For the first logic circuit, a exclusive-NOR (XNOR) gate called first data monitoring unit for Q which compare the input of D F-F with the next state Q was built, if the output of XNOR is high and equal to 1 that indicates the D F-F work normally and no fault appear, at the opposite of the (0) appearance that indicate an error appearance. For this purpose, a controlled switch depending on XNOR output was embedded, if the input of this switch is equal to 1 the output of Q will flow, and when its input equals to (0) the inverted value of Q will flow. Furthermore, a XOR gate called first data monitoring unit for !Q which compare the input of D F-F with the next state !Q was built, when its output equal (1) that indicates that the D F-F is working normally and when its output equal (0) indicates a fault appearance, so a controlled switch depending of XOR output was embedded, when its input equals to (1). The output of !Q will flow, and when its input equals to (0) the inverted value of !Q will flow. Consequently, these two types of intelligent fault tolerance techniques can be used to tolerate unlimited number of transient and intermittent faults efficiently. Furthermore, two additional Data monitoring Units for the output signals Q and !Q of another memory device were proposed. These two units use the concept of double modular redundancy (DMR) [17]–[19] with two XNOR gates and another two controlled switches that are responsible of detecting and correcting the effects of artificial and natural permanent faults. The idea is using an additional spare (D flip-flop), XNOR gates compares the output of a switch that follow the first XNOR with the output of the spare D flip flop, if its output equals (1) that indicates that no error is observed, and the switch will allow the output of a switch that follow the first XNOR to flow. However, when the output equals (0) that indicates that an error is observed, and the switch will allow the output of a spare D flip flop to flow. In addition, to make the execution of the proposed design deterministic and synchronous, all the digital switches that are used are controlled by a trigger signal which led to that the comparison of all the outputs will be at the same time. Represents the excitation equation of the proposed digital circuit shown in (1):

$$F = [X \text{ AND } Y \text{ AND } \sim Z \text{ AND } !Q(t + 1)] \text{ OR } [\sim Z \text{ AND } Q(t + 1)] \tag{1}$$

Figure 3(a) presents the first monitory unit (MU1) timing diagram in its Normal State operation when no fault appears by using MATLAB Simulink [20]. The input signals ‘X’, ‘Y’, and ‘Z’ are equal to the value 1,1,0 respectively and the data input of the D F-F is equal to 1, in this state the MU1 will compare the status of input signal with the resulted output signal by using the XNOR1 gate. Additionally, the D flip-flop input is checked with the complemented output by using the XOR gate, if both outputs of the XNOR and the XOR gates are equal to ‘1’ value, that indicates no fault appearance. Furthermore, Figure 3(b) presents the MU1 timing diagram when the ‘Q’ output signal of the D F-F is defected with a simulated fault. In this scenario, the output data of the XNOR gate will be equal to ‘0’ value and the MU1 will correct this false value and replace it with a right value using a programmable digital switch.

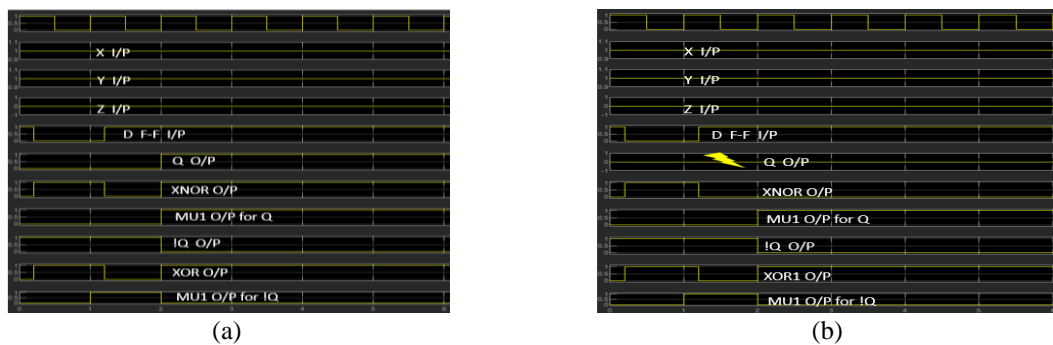


Figure 3. Timing diagram (a) MU1 in normal NO fault injection and (b) MU1 at first fault injection

4. RESULTS AND DISCUSSION

To evaluate the dependable and resilient behavior of the proposed fault-tolerant sequential logic circuit and calculate how much it is reliable and secure, a Markov chain diagram comprised of five descriptive states was modeled as it is shown in Figure 4 and Table 2 [21]. Three operating states were embedded in the reliability model, one state for failing in a safe mode, and one state for failing in an unsafe mode. The status of the system is in one of the five states: totally operational, first failing-operational, second failing-operational, failing in a safe mode, or failing in an unsafe mode.

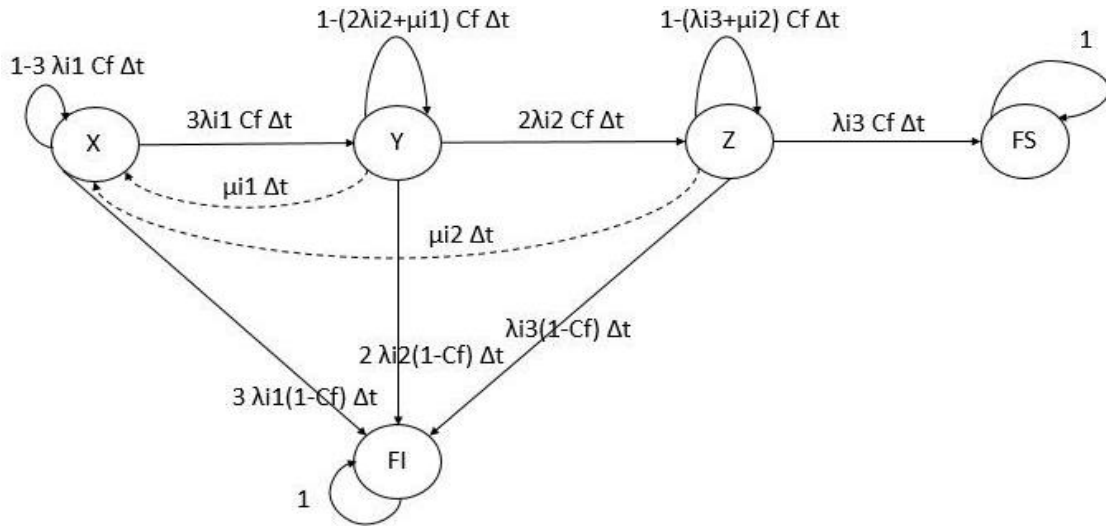


Figure 4. Discrete-time Markov chain for the proposed fault-tolerant sequential logic system

Table 2. The events describing the various states of the discrete-time Markov chain

| Event | Characterization |
|-------|---|
| X | Totally operational (the system's D Flip-Flop is fully operational, and one spare is available) |
| Y | First failing - operational (Q or !Q output of the D Flip-Flop is effected by transient fault or permanent or intermittent fault and discovered by XNOR gate, so the switch that follow XNOR or XOR is used for repair) |
| Z | Second failing-operational (Q or !Q output of the D Flip-Flop are effected by transient fault or intermittent fault or permanent then is effected by another fault and discovered by one of the two XOR gates, so one or two of the switches that follow XOR is used for repair by replacing them by the output signal of the spare D memory element) |
| FS | Failing in a safe mode Operational (Q or !Q output of the spare D Flip-Flop are effected by transient fault or intermittent fault or permanent fault but it cannot be repaired) |
| FI | Failing in an unsafe mode (output signal of the D memory or the spare flip-flop are failed without any detection) |

To analyze the reliable behavior of the designed sequential fault-tolerant system using Markov chain models, it can be assumed that each sequential memory element obeys the exponential failure rule and has a constant failure rate of λ [22]. The probability equation $P(t+\Delta t)$ that a fault-tolerant digital sequential circuit will fail in future at some time $(t+\Delta t)$ can be calculated and written as in the following relationship:

$$P(t + \Delta t) = 1 - e^{-\lambda \Delta t} \approx \lambda \Delta t \tag{2}$$

where, λ is the failure rate, and $P(t + \Delta t)$: probability that a fault-tolerant digital sequential circuit will fail at some time $(t + \Delta t)$.

$$PX(t + \Delta t) = (1 - 3\lambda i1 Cf \Delta t) PX(t) + \mu i1 \Delta t PY(t) + \mu i2 \Delta t PZ(t)$$

$$PY(t + \Delta t) = [1 - (\lambda i2 + \mu i1)Cf \Delta t]PY(t)$$

$$PZ(t + \Delta t) = [1 - (\lambda i3 + \mu i2)Cf \Delta t]PZ(t)$$

$$PFS(t + \Delta t) = \lambda i3 Cf \Delta t PZ(t) + PFS(t)$$

$$PFI(t + \Delta t) = 3\lambda_1(1 - Cf)\Delta t PX(t) + 2\lambda_2(1 - Cf)\Delta t PY(t) + \lambda_3(1 - Cf)\Delta t PZ(t) + PFI(t)$$

The reliability can be computed from (3):

$$R(t) = 1 - PFS(t) - PFI(t) = PX(t) PY(t) + PZ(t) \quad (3)$$

where,

$$\frac{PX(t + \Delta t) - PX(t)}{\Delta t} = -3\lambda_1 Cf PX(t) + \mu_1 PY(t) + \mu_2 PZ(t)$$

$$\frac{PY(t + \Delta t) - PY(t)}{\Delta t} = -(2\lambda_2 + \mu_1)Cf PY(t)$$

$$\frac{PZ(t + \Delta t) - PD(t)}{\Delta t} = -(\lambda_3 + \mu_2) Cf PZ(t)$$

$$\frac{PFS(t + \Delta t) - PFS(t)}{\Delta t} = \lambda_3 Cf PZ(t)$$

$$\frac{PFI(t + \Delta t) - PFI(t)}{\Delta t} = 3\lambda_1(1 - Cf)PX(t) + 2\lambda_2(1 - Cf)PY(t) + \lambda_3(1 - Cf)PZ(t)$$

$$P - \text{system}(t + \Delta t) = \begin{matrix} PX((t + \Delta t) \\ PY((t + \Delta t) \\ PZ((t + \Delta t) \\ PFS((t + \Delta t) \\ PFI((t + \Delta t) \end{matrix}, P - \text{system}(t) = \begin{matrix} PX(t) \\ PY(t) \\ PZ(t) \\ PFS(t) \\ PFI(t) \end{matrix}$$

The two-dimensional state transition matrix of a Markov model would resemble:

$$P - \text{system}(t + \Delta t) = \begin{matrix} & -3\lambda_1 Cf & \mu_1 & \mu_2 & 0 & 0 \\ & 0 & -(2\lambda_2 + \mu_1) Cf & 0 & 0 & 0 \\ & 0 & 0 & -(\lambda_3 + \mu_2) Cf & 0 & 0 \\ & 0 & 0 & \lambda_3 Cf & 0 & 0 \\ & 3\lambda_1(1 - Cf) & 2\lambda_2(1 - Cf) & \lambda_3(1 - Cf) & 0 & 0 \end{matrix}$$

Using algebraic manipulation to let the temporal interval t decrease to zero, the following differential equations are produced:

$$\frac{dPX(t)}{dt} = -3\lambda_1 Cf PX(t) + \mu_1 PY(t) + \mu_2 PZ(t)$$

$$\frac{dPY(t)}{dt} = -(2\lambda_2 + \mu_1)Cf PY(t)$$

$$\frac{dPZ(t)}{dt} = -(\lambda_3 + \mu_2) Cf PZ(t)$$

$$\frac{dPFS(t)}{dt} = \lambda_3 Cf PZ(t)$$

$$\frac{dPFI(t)}{dt} = 3\lambda_1(1 - Cf)PX(t) + 2\lambda_2(1 - Cf)PY(t) + \lambda_3(1 - Cf)PZ(t)$$

The following equations have been constructed using the Laplace transform:

$$S PX(S) - PX(0) = -3\lambda_1 Cf PX(S) + \mu_1 PY(S) + \mu_2 PZ(S)$$

$$S_{PY}(S) - PY(0) = -(2\lambda_2 + \mu_1)C_f PY(S)$$

$$S_{PZ}(S) - PZ(0) = -(\lambda_3 + \mu_2)C_f PZ(S)$$

$$S_{PFS}(S) - PFS(0) = \lambda_3 C_f PZ(S)$$

$$S_{PFI}(S) - PFI(0) = 3\lambda_1(1 - C_f) PX(S) + 2\lambda_2(1 - C_f) PY(S) + \lambda_3(1 - C_f) PZ(S)$$

System reliability $R(t)$ is typically defined as the probability that a logic circuit operate without going to failure during the period $[0, t]$. In addition, reliability is considered as an evaluation metric for measuring that the predicted service is reached to customer [23] and [24]. In (4) represents reliability and how it is calculated. On the other hand, the safety is an extened concept of the reliability. The safety of a logic circuit $S(t)$ is defined as the probability of a circuit to execute its predicted function completely or transition to operate in a failing in a safe mode in the period $[0, t]$. Hence, (5) represents the safety and how it is calculated.

$$R(t) = PX(t) + PY(t) + PZ(t) \tag{4}$$

$$S(t) = PX(t) + PY(t) + PZ(t) + PFS(t) \tag{5}$$

The stratix IV FPGA fabric which has been assumed to be a target realization platform has 38.1 FIT failure rate. Where FIT refers to failure in time which is a unit that represents how many failures can be occur every 10^9 hours in time. $FIT = hours * 10^{-9}$ So, $hours = 38.1 * 10^{-9}$ failure/hour. Altera's stratix IV FPGA chip has the same frequency as 50 MHz. Thus, the mean time to repair (MTTR) for one clock is 20 ns. In Table 3, it can be observed that we compare the probability state values of different fault detection coverage values which represents the probability of being in different states in Figure 4. Additionally, the WINSTEM SURE analysis program [25] was used to model the reconfigurable behaviour of the proposed system. The SURE program is a reliability analysis simulation tool that is developed by the National Aeronautics and Space Administration (NASA) agency to calculate the probabilities of failure rate. Table 4 demonstrates reliability and safety at different fault detection coverage values and in Figure 5, we can observe the fault detection coverage versus reliability.

Table 3. Probabilities for different states with different fault detection coverage values

| Coverage (C) | State X probability | State Y probability | State Z probability | State (FS) probability | State (FIS) probability |
|--------------|---------------------|---------------------|---------------------|------------------------|-------------------------|
| 0.8 | 9.99002728523E-0001 | 7.96851758717E-0004 | 2.12798315173E-0007 | 1.89632981572E-0011 | 2.00206901247E-0004 |
| 0.85 | 9.99002947007E-0001 | 8.46655055530E-0004 | 2.40229356768E-0007 | 2.27457729220E-0011 | 1.50157684996E-0004 |
| 0.9 | 9.99003165494E-0001 | 8.96458359624E-0004 | 2.69322887327E-0007 | 2.70004784426E-0011 | 1.00106796057E-0004 |
| 0.99 | 9.99003558777E-0001 | 9.86104325345E-0004 | 3.25880715104E-0007 | 3.59376382250E-0011 | 1.00109807011E-0005 |
| 0.999 | 9.99003598106E-0001 | 9.95068923215E-0004 | 3.31832753489E-0007 | 3.69266929356E-0011 | 1.00110108110E-0006 |
| 0.9999 | 9.99003602039E-0001 | 9.95965383015E-0004 | 3.32430919884E-0007 | 3.70265847616E-0011 | 1.00110138220E-0007 |
| 0.99999 | 9.99003602432E-0001 | 9.96055028995E-0004 | 3.32490766149E-0007 | 3.70365838407E-0011 | 1.00110141230E-0008 |

Table 4. Reliability and safety with different fault detection coverage values

| Coverage (C) | Reliability results | Safety results |
|--------------|-----------------------|-------------------------|
| 0.8 | 0.999849619985586768 | 0.999849620005 |
| 0.85 | 0.999849842291886768 | 0.999849842315 |
| 0.9 | 0.9998998931765113227 | 0.999899893204 |
| 0.99 | 0.999989988983060 | 0.999989989019 |
| 0.999 | 0.999998998861968489 | 0.99999899889518193560 |
| 0.9999 | 0.99999899852934884 | 0.999998998899614687616 |
| 0.99999 | 0.99999899951761149 | 0.99999899887977328407 |

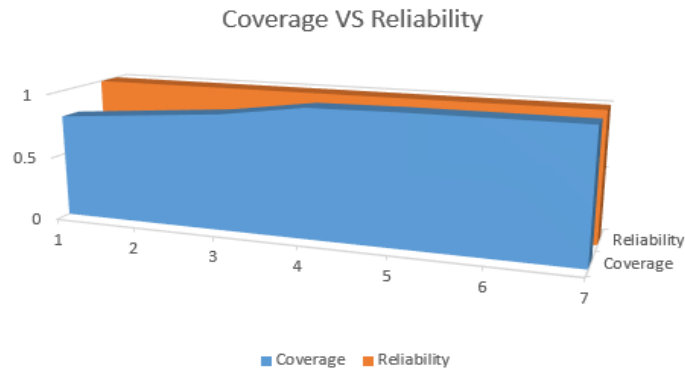


Figure 5. Fault detection coverage versus reliability

5. CONCLUSION AND FUTURE WORK

In this paper, we presented an architectural design and reliability analysis of a novel fault-tolerant sequential logic circuit for safety-critical digital applications. The primary objective is overcoming the deficiencies and faults can attack the operation of latches and D flip-flops embedded in safety-critical sequential circuits. The advantage of the approach is that it tolerates an unlimited number of intermittent and transient faults. We demonstrated the experimental results of achieving high levels of reliability by simulating the fault injection campaigns into the output signals of memory storage elements. The results prove that the proposed system can achieve 0.9998 reliability and safety for the fault detection coverage which is equal to 0.8 and achieve 0.99999998 reliability for the coverage equals to 0.99999. For the future work, it is planned to focus on using the mathematical verification concepts that could be utilized to validate the operational execution of the data monitoring models. Furthermore, the proposed circuit can operate in critical environments that generate potential CCFs by adding a hybrid fault-tolerant mechanism with spare sequential components. Finally, generating the hardware description language (HDL) code using the MathWorks Simulink-based HDL coder and synthesizing the proposed circuit in real-time is one of the future works.

ACKNOWLEDGEMENTS

The authors would like to thank Mosul University, College of Engineering, Department of Computer, for the financial support given during implementing this work.




REFERENCES

- [1] Z. Zhang, Y. Wang, S. Yang, R. Yao, and J. Cui, "The research of self-repairing digital circuit based on embryonic cellular array," *Neural Computing and Applications*, vol. 17, no. 2, pp. 145–151, Mar. 2008, doi: 10.1007/s00521-007-0095-9.
- [2] S. S. Khairullah and C. R. Elks, "A Bio-Inspired, Self-Healing, Resilient Architecture for Digital Instrumentation and Control Systems and Embedded Devices," *Nuclear Technology*, vol. 202, no. 2–3, pp. 141–152, Apr. 2018, doi: 10.1080/00295450.2018.1450014.
- [3] S. S. Khairullah and C. R. Elks, "Self-repairing hardware architecture for safety-critical cyber-physical-systems," *IET Cyber-Physical Systems: Theory and Applications*, vol. 5, no. 1, pp. 92–99, Nov. 2019, doi: 10.1049/iet-cps.2019.0022.
- [4] F. N. Kassab Bashi, S. S. Khairullah, and C. R. Elks, "Realization of Dependable Digital Systems for Safety-Critical Computer Systems using FPGAs," *IOP Conference Series: Materials Science and Engineering*, vol. 1152, no. 1, p. 012020, May 2021, doi: 10.1088/1757-899x/1152/1/012020.
- [5] S. S. Khairullah, "Realization of a 16-bit MIPS RISC pipeline processor," in *2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, IEEE, Jun. 2022, doi: 10.1109/hora5278.2022.9799944.
- [6] E. Dubrova, "Fault-Tolerant Design," in *Fault-Tolerant Design*, E. Dubrova, Ed., New York, NY: Springer, 2013, pp. 1–185, doi: 10.1007/978-1-4614-2113-9_1.
- [7] S. Almukhaizim and Y. Makris, "Fault tolerant design of combinational and sequential logic based on a parity check code," in *Proceedings 18th IEEE Symposium on Defect and Fault Tolerance in VLSI Systems*, Boston, MA, USA, Nov. 2003, pp. 563–570, doi: 10.1109/DFTVS.2003.1250156.
- [8] A. H. El-Maleh and A. S. Al-Qahtani, "A finite state machine based fault tolerance technique for sequential circuits," *Microelectronics Reliability*, vol. 54, no. 3, pp. 654–661, Mar. 2014, doi: 10.1016/j.microrel.2013.10.022.
- [9] A. H. El-Maleh, "A sequential circuit fault tolerance technique with enhanced area and power," in *2015 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT)*, IEEE, Dec. 2015, doi: 10.1109/isspit.2015.7394348.
- [10] S. Ostanin, A. Matrosova, N. Butorina, and V. Lavrov, "A fault-tolerant sequential circuit design for soft errors based on fault-secure circuit," in *2016 IEEE East-West Design and Test Symposium (EWDTS)*, IEEE, Oct. 2016, doi: 10.1109/ewdts.2016.7807676.
- [11] T. Ban and G. G. S. Junior, "Critical Gates Identification for Fault-Tolerant Design in Math Circuits," *Journal of Electrical and Computer Engineering*, vol. 2017, pp. 1–7, 2017, doi: 10.1155/2017/5684902.




- [12] J. Anwer and M. Platzner, "Evaluating fault-tolerance of redundant FPGA structures using Boolean difference calculus," *Microprocessors and Microsystems*, vol. 52, pp. 160–172, Jul. 2017, doi: 10.1016/j.micpro.2017.06.002.
- [13] M. Dug, M. Krstic, and D. Jokic, "Implementation and Analysis of Methods for Error Detection and Correction on FPGA," *IFAC-PapersOnLine*, vol. 51, no. 6, pp. 348–353, 2018, doi: 10.1016/j.ifacol.2018.07.178.
- [14] S. Shalini, M. Saravanan, and T. Ananth Kumar, "Design of fault tolerant sequential circuits using selective triple modular redundancy algorithm," *International Journal of Pure and Applied Mathematics*, vol. 119, no. 14, pp. 1045–1049, Jan. 2018.
- [15] O. Boncalo, A. Amaricai, and Z. Lendek, "Fault Tolerant Digital Data-Path Design via Control Feedback Loops," *Electronics*, vol. 9, no. 10, p. 1721, Oct. 2020, doi: 10.3390/electronics9101721.
- [16] J. Li, S. Zhang, and C. Bao, "DuckCore: A Fault-Tolerant Processor Core Architecture Based on the RISC-V ISA," *Electronics*, vol. 11, no. 1, p. 122, Dec. 2021, doi: 10.3390/electronics11010122.
- [17] M. Zheng, Z. Wang, and L. Li, "DAO: Dual module redundancy with AND/OR logic voter for FPGA hardening," in *2015 First International Conference on Reliability Systems Engineering (ICRSE)*, IEEE, Oct. 2015, doi: 10.1109/icrse.2015.7366414.
- [18] M. Zheng, Z. Wang, and L. Li, "A Fault Masking Dual Module Redundancy Method for FPGA," *CASIA OpenIR*, May 2016.
- [19] M. S. Farias, N. Nedjah, and P. V. R. de Caravhlo, "Active Redundant Hardware Architecture for Increased Reliability in FPGA-Based Nuclear Reactors Critical Systems," in *2020 23rd Euromicro Conference on Digital System Design (DSD)*, IEEE, Aug. 2020, doi: 10.1109/dsd51259.2020.00100.
- [20] Y. P. Siwakoti and G. E. Town, "Design of FPGA-controlled power electronics and drives using MATLAB Simulink," in *2013 IEEE ECCE Asia Downunder*, IEEE, Jun. 2013, doi: 10.1109/ecce-asia.2013.6579155.
- [21] R. W. Butler and S. C. Johnson, "Techniques for modeling the reliability of fault-tolerant systems with the Markov state-space approach," *National Aeronautics and Space Administration Reference Publication (RP)*, Sep. 01, 1995.
- [22] V. Kumar, L. K. Singh, P. Singh, K. V. Singh, A. K. Maurya, and A. K. Tripathi, "Parameter Estimation for Quantitative Dependability Analysis of Safety-Critical and Control Systems of NPP," *IEEE Transactions on Nuclear Science*, vol. 65, no. 5, pp. 1080–1090, May 2018, doi: 10.1109/TNS.2018.2827106.
- [23] S. S. Khairullah and A.-N. Sharkawy, "Design and Implementation of a Reliable and Secure Controller for Smart Home Applications Based on PLC," *Journal of Robotics and Control (JRC)*, vol. 3, no. 5, pp. 614–621, Sep. 2022, doi: 10.18196/jrc.v3i5.15972.
- [24] Y. Niu *et al.*, "Research on fault adaptive fault tolerant control of distributed wind solar hybrid generator," *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 2, pp. 1029–1040, Apr. 2023, doi: 10.11591/eei.v12i2.4242.
- [25] R. W. Butler and A. L. White, "SURE reliability analysis: Program and mathematics," *National Aeronautics and Space Administration Reference Publication (RP)*, Mar. 01, 1988.

BIOGRAPHIES OF AUTHORS






Shawkat Sabah Khairullah    graduated with a (B.Sc.) degree in July 2006 from College of Engineering, Department of Computer Engineering, University of Mosul. He received his M.Sc. degree in Computer Engineering in 2011. In December 2018, he received his Ph.D. degree from Virginia Commonwealth University, Richmond, United States of America. Khairullah has published more than 10 papers in international scientific journals and international scientific conferences. He serves as a reviewer for international journals and conferences. His research areas of interest include design and analysis of dependable hardware architectures, biologically inspired self-healing systems, fault-tolerance, and FPGA-based digital systems. He can be contacted at email: shawkat.sabah@uomosul.edu.iq.



Farah Natiq Qassabbashi    graduated with a (B.Sc.) degree in 2004 from College of Engineering, Department of Computer Engineering, University of Mosul. She received his M.Sc. degree in Computer Engineering in 2021 from College of Engineering, Computer Engineering Department, University of Mosul and followed this nomination as an assistant lecturer at the same university. She has published two papers in international scientific journals and international scientific conferences. Her research areas of interest include design and analysis of dependable hardware architectures, fault-tolerance, VLSI, and FPGA-based digital systems. She can be contacted at email: farah.qassabbashi@uomosul.edu.iq.



Jumana Abdullah Kareem    graduated with a (B.Sc.) degree in July 1997 from College of Technology, Department of Computer Engineering, from North Technical University. She received her M.Sc. degree in Computer Engineering in 2006 from Department of Computer Engineering, University of Mosul and followed this nomination as an assistant lecturer at the same university. Her research areas of interest include design and analysis of optical network system, networking, and information technology. She can be contacted at email: jumana.abdullah@uomosul.edu.iq.