Jestr

Journal of Engineering Science and Technology Review 17 (6) (2024) 59 - 65

Research Article

JOURNAL OF
Engineering Science and Technology Review

www.jestr.org

Design, Verification and Implementation of a Watchdog Timer for Drone Applications

Madhushankara M*., Ribu Mathew, Maneesh M. S. and Vignesh B.

Manipal School of Information Sciences, Manipal Academy of Higher Education, Manipal, India

Received 13 July 2024; Accepted 15 November 2024

Abstract

Drones are becoming popular in many industrial and commercial sectors for various applications, including photography, agriculture, surveillance, and delivery services. For the proper functioning of a system with multiple processors and peripherals, continuous monitoring in the form of a watchdog is essential. In this work, the design, verification, and implementation of a watchdog are presented. The system is modelled and verified via SystemVerilog hardware description language. The implementation of the design was carried out using 15 nm technology in an operating frequency range of 18.52 GHz to 20.41 GHz. A comparison of the area, power, and performance is performed with two different corner cases of process, voltage, and temperature. The standalone performance of the design is on the order of gigahertz with 94.47 pJ of power delay product and is suitable for industrial standard high-speed and low-power drone applications.

Keywords: Drone, Watchdog, Integrated Circuits, System Verilog, Industrial Standard, Area, Power, Performance

1. Introduction

Unremitting monitoring is an important aspect of many systems. Watchdogs monitor systems such as drones to perform various automatic tasks [1]. This ensures correct operation by providing a reset condition in case of failure to bring the system back into the normal mode of operation. Prevention of system hang-ups relies on real-time processing of the data. When heavy signal interference occurs in regions such as urban areas and military zones, watchdog timers monitor the correct operation of a drone's critical systems and resets if it fails or hangs. As drones depend on radio frequency signals for communication, signal interference from nearby electronic devices, buildings, or even natural factors can interrupt communication. In this scenario, the watchdog module monitors signal health and inevitably triggers corrective actions. When operating at high altitudes where atmospheric pressure is low and when the temperature is extreme, battery performance, sensor accuracy, and motor efficiency impact drones. By monitoring thermal sensors for overheating or undercooling, watchdogs can activate protective measures, such as regulating power or landing the drone. With continuous monitoring of the barometer or global positioning system, the watchdog system initiates the appropriate signals for correction for atmospheric pressure variations. A watchdog can detect system hang-ups and reset the system, preventing the drone from becoming passive at mid-flight.

The central parts of the drones are the processors, including the general purpose, graphic processing unit, and field programmable gate arrays (FPGA). System-on-chip (SoC) designs capable of handling multiple types of processing are also good candidates for drones. Figure 1 shows the block diagram of the generic multiprocessing SoC with peripherals. The bus system coordinates with the processor and peripherals of which the watchdog monitor notices when the processor fails to complete tasks within a specified time frame and triggers a reset. If the timer is not reset by the processor within a certain interval, it specifies a probable unfinished execution or hang state [2].

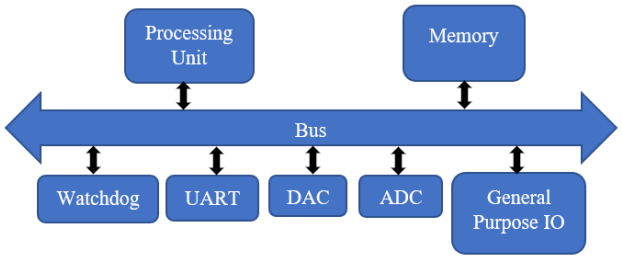

Fig. 1. SoC with peripherals

The design considerations for watchdog implementation should consider reliability and fault detection. Safety-critical embedded systems require high-reliability and fault detection mechanisms. Watchdog timers are used to automatically handle and recover from operation time-related failures [3-5].

Figure 2 shows the interaction of the watchdog with the processor. Several architectures from ARM Limited have provided a mechanism to connect processors with peripherals [6-8]. In this case, the same clock is applied to both units, and the processor sends the restart signal to the timer during the initiation of its operation. Any failure in subsequent restarting will result in reset of the processor by the timer. In some cases, the watchdog timer could also be included within the processor.

Typically, the watchdog timer is a slave device that continuously monitors the signal from the master to trigger restart. The software chooses the counter's initial value and restarts at regular intervals. The processor enters a defined state if the counter value reaches zero.

*E-mail address: madhushankar.m@manipal.edu
ISSN: 1791-2377
doi:10.25103/jestr.176.08

Applications in which devices used in space or in the deep sea cannot be controlled by humans are in a permanently disabled state if not restarted. Even the human response can be too late to meet the uptime requirements of the system in many cases.

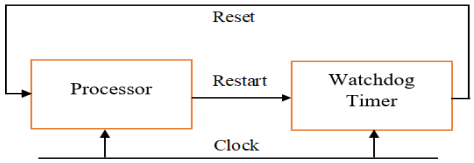

Fig. 2. Watchdog timer block diagram

2. Literature Review

Drones, mainly in safety and surveillance roles, demand precise watchdog requirements to ensure safe and effective operation. Farming, environmental monitoring, and infrastructure check-ups are the few examples. The authors of these reviews suggest that drones are at greater risk of collision depending on climate conditions and terrain and advocate the effective implementation of regulation policies [9 -10]. Kuantama et al. proposed drones as flying watchdogs to detect objects within 60 seconds [11]. Verdiesen et al. proposed a model to increase social and technological factors to monitor the drone process to alleviate human oversight [12].

Parekh et al. proposed a model to incorporate the failure of temperature and pressure units in space applications. The reset command from the watchdog module is triggered when a failure signal is asserted from the controller. In its initial stage, the model needs to be exhaustively verified for its functional correctness [13]. The drone communicates in the frequency bands 2.400–2.483 GHz and 5.725–5.825 GHz [14]. Drones predominantly use protocols such as millimetre wave systems, Wi-Fi, and free space optical communication systems while performing as communication providers, as consumers, and as relays of communication services, respectively [15]. WATCHDOG 150 and WATCHDOG 202 are the few commercial sensors used to detect drones from land on the basis of radio frequency. Park et al. proposed a watchdog system for autonomous vehicles to monitor the behavior of various sensors, such as cameras, LiDARs, and GPSs [16]. Dorr et al. prototyped a watchdog system that restores the internal states in a maximum of 5 milliseconds on a 32-bit data handling processor [17]. Fu et al. proposed an executable model for multipoint failure in automatically driven vehicles [18]. Various safety concerns, such as failure in sensor communication, component failure, and shared memory resource failure, are considered. Peserico et al. provided a framework for safety in Wi-Fi networks through a watchdog timer by controlling the timing behavior of the network [19]. Runtime monitoring is one of the keys to improving safety during flight. A GPS system coupled with a watchdog restricts the movements of the drone [20]. Wu et al. analysed the CubeSat model and utilized an external watchdog module to monitor the failure of multithreading applications, followed by recovery in 2--3 seconds [21].

Jain et al. verified the functionality of a watchdog module for temperature variations ranging from -40 °C to +105 °C [22]. Both the software and hardware controllability of the module are in two different forms. In the free running mode, 30% of the passes failed, and in the time window mode, 75% of the tests failed in the temperature range from 0--10 degrees. Singh et al. reported the area, power, and performance of a watchdog timer implemented with 180 nm technology [23].

Selvan et al. wrote hardware description language for the timer and implemented it on a programmable field device and reported that the maximum frequency of operation was approximately 250 MHz [24]. Chaithanya et al. verified the interrupt and rest modes of a watchdog module [25]

Ponkumar et al. developed a verification intellectual property, including the watchdog, in an SOC environment [26]. Eckel et al. defined a protocol for watchdogs used in the Internet of Things [27]. Huang et al. evaluated the performance of a watchdog in a critical digital review [28]. Using a voter and arbiter, Zhang and Qin provided a triple modular system for watchdogs used in a space application processor [29].

One of the potential challenges in actual hardware implementation is imperfections and variability due to the manufacturing process. The integration of sensors, transducers, and communication systems could lead to unanticipated performance. Sensor inaccuracies can cause uneven flight navigation, and actuators may not respond with the same efficiency assumed during simulations. To avoid such a situation, along with watchdog, continuous monitoring and calibration procedures need to be adopted. Vanathy et al. proposed hardware software codesign to ensure reliability in drones [30]. In the proposed method, the functional and performance requirements of the actuator, including electrical and mechanical travel, calibration, and step response, are monitored for acceptability via software applications from the ground. The adaptive estimation technique further enhances the flight conditions in an area-restricted environment [31].

The environmental factors of wind gusts can disrupt drones if the drone's aerodynamics are not tweaked to handle unanticipated turbulence. A light detection and ranging technique coupled with drones is able to regulate flight [32]. In the proposed proof-of-concept, researchers have demonstrated the detection of disturbance zones up to a radius of 2 meters. The sensor coupled with a temperature control circuit can compensate for the variation due to its effect [33]. The effect of signal interference in the downlink of the drone is another significant challenge. Warrier et al. proposed a deep learning algorithm to address signal-to interference and signal-to-noise ratio optimization to alleviate this problem [34].

3. Methodology

In this work, the specifications of the watchdog module, which is the most commonly used bus architecture from ARM Limited, are used. It is a peripheral used with the Advanced Microcontroller Bus Architecture (AMBA) available at [35]. Figure 3 depicts the block diagram of the watchdog module with 6 inputs and 2 outputs. The descriptions of the input and output are provided in Table 1.

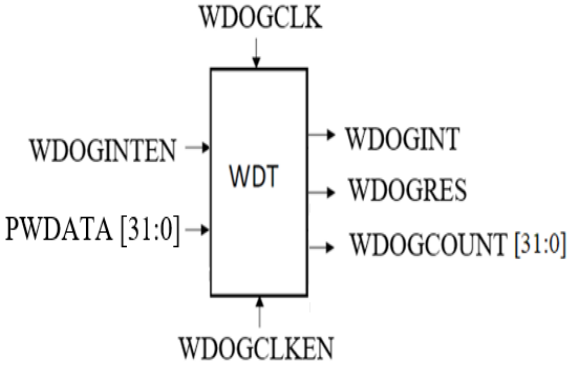

Fig. 3. Block diagram of the watchdog module

Table 1. Pinouts and their descriptions

Signal	Direction	Description
WDOGCLK	Input	1-bit, positive edge triggered clock
WDOGINTEN	Input	1-bit, active HIGH. Clears the generated interrupt
WDOGCLKEN	Input	1-bit, active HIGH. The counter decrements by one, on the positive edge of the clock.
PWDATA	Input	32-bit, write data bus to the peripheral during write operation
WDOGCOUNT	Output	32-bit, register to count down the value and store
WDOGINT	Output	1-bit, generates a regular interrupt signal when the counter value reaches zero if the previous interrupt is cleared
WDOGRES	Output	1-bit, generated if interrupt is not cleared by the system within the service time

Figure 4 depicts the flow chart of the watchdog module, which is based on a 32-bit down counter initialized from the bus PWDATA. The WDOGCOUNT decreases by one when WDOGCLKEN is high on each positive edge of WDOGCLK. The module generates regular interrupt WDOGINT when the count value reaches zero if there is no previous interrupt. Once the interrupt is generated, a service time is allotted to the system to clear the interrupt generated by the watchdog. When the system clears the generated interrupt, the WDOGINTEN signal is high. When WDOGINTEN is high, WDOGINT is cleared. If the interruption is not cleared within the service time, the module will generate a reset signal WDOGRES that will restart the system. Then, the counter will restart from the initial maximum value. The WDOGLOCK register is used to prevent corrupt software from disabling watchdog functionalities. It is a write-only register. Writing the value of 0x1ACCE551 enables write access to all the registers. Writing any other value disables write access. The module is enabled only by the enable signal WDOGCLKEN, which is an active high signal. The timer is disabled when this signal is low.

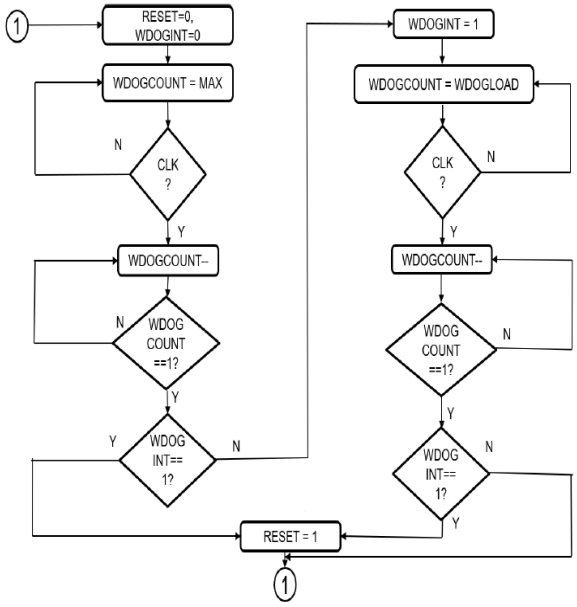

Fig. 4. Flowchart of the watchdog module

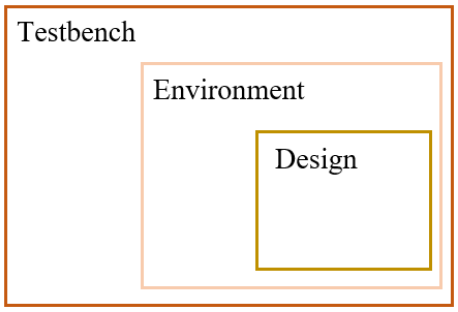

Fig. 5. Verification of the watchdog module

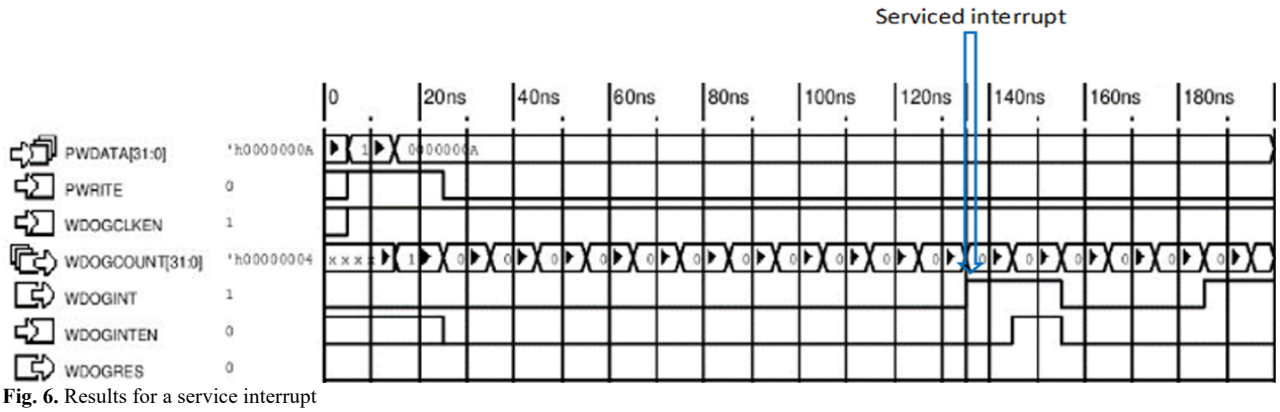

Fig. 6. Results for a service interrupt

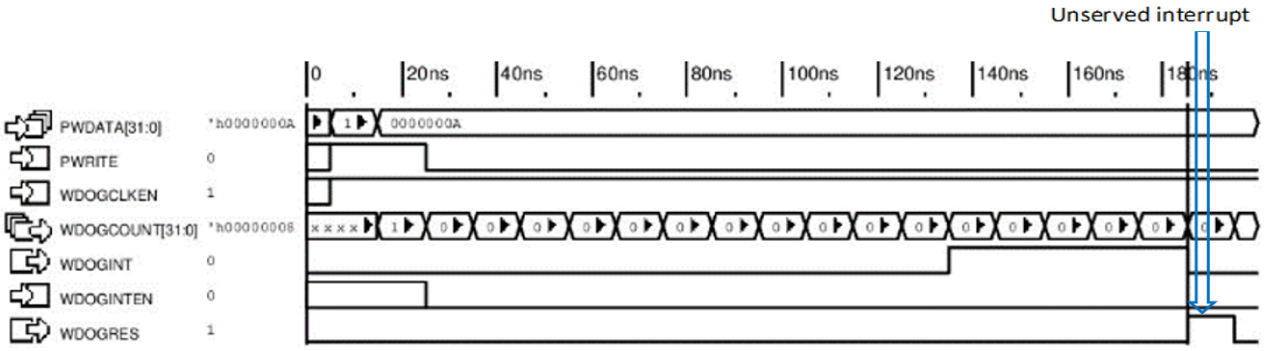

Fig. 7. Results for an unserviced interrupt

4. Results and Discussion

SystemVerilog modelling is written for the watchdog module described in section II. A complete verification environment is created for a thorough verification process (Reference). Figure 5 depicts the verification environment where the design of the watchdog module is a part of the closed loop system under the testbench. The environment is a class-based program consisting of a generator, driver, and monitor.

The design is functionally simulated via the Incisive 15.2 suite from Cadence for correctness, as depicted in Figures 6 and 7. Initially, the design is loaded with a hexa decimal value, 0x0A, to the counter after unlocking it by writing the value 0x1ACCE551, as represented in Figure 6. The interrupt signal is generated when the counter reaches 0. A logic HIGH value on WDOGINTEN indicated at 145 ns indicates that the interrupt is serviced, and thus, no reset signal is generated. The four-clock cycle is the time to service the interruption, which is indicated by the value of 0x04 at 135 ns, when the WDOGINTEN is logically high

An unserviced interrupt will generate a reset signal from the module, as indicated in Figure 7. The WDORES is logic high since there is no WDOGINTEN during the service period. Thus, we can observe the reset signal at a simulation time of 180 ns.

Figures 8 to 12 represent the different test cases for verifying the watchdog module. Figure 8 shows that until WDOGCLKEN is HIGH, the watchdog timer is disabled. The WDOGCOUNT will not fetch value from the WDOGLOAD register even when write access is enabled (i.e., WDOGLOCK = 0x1ACCE551). Figure 9 represents the generation of the interrupt. When the WDOGCOUNT value decreases to zero with no previous interruption, the WDOGINT interrupt signal is generated, and the service time is allotted.

Figure 10 shows successful reset signal generation, in which the WDOGCOUNT value decreases to zero with a previous interruption not being cleared by the system, a reset signal WDOGRES is generated, and WDOGCOUNT is loaded with the maximum value. Figure 11 shows that when the system clears the interruption through WDOGINTEN within the service time, a reset signal is not generated. The WDOGCOUNT is loaded with the maximum value. As described in Section III, write access is possible only when a particular value is written from the master. Figure 12 shows that the value 0x1ACCE551 enables write access to WDOGCOUNT.

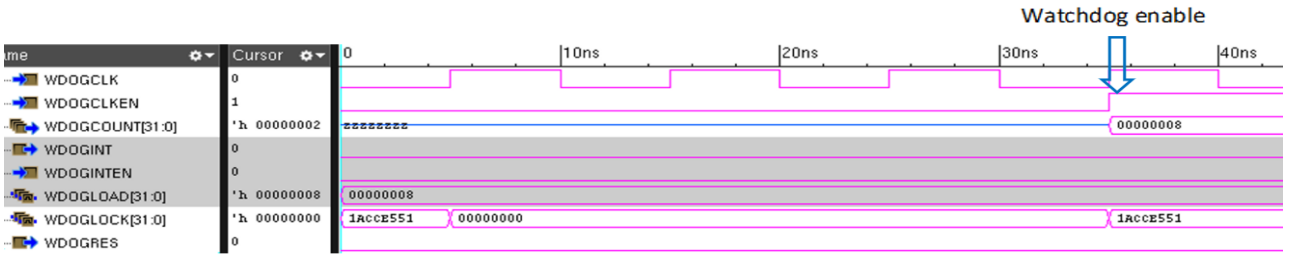

Fig. 8. Results of enabling watchdog

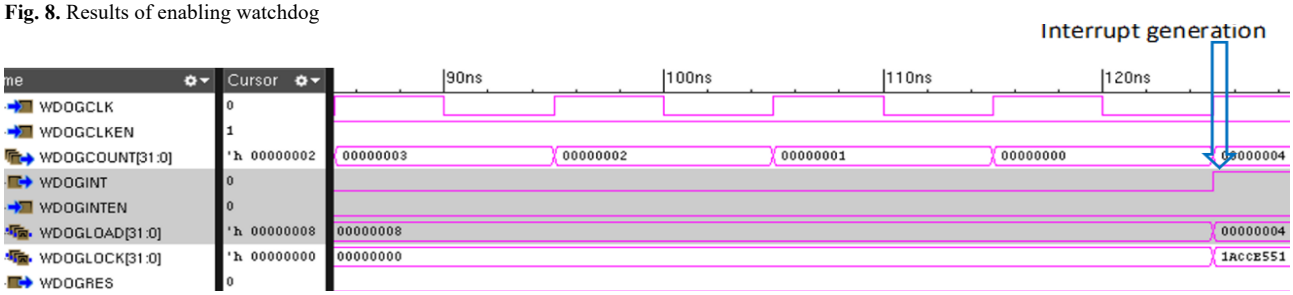

Fig. 9. Results of interrupt signal generation

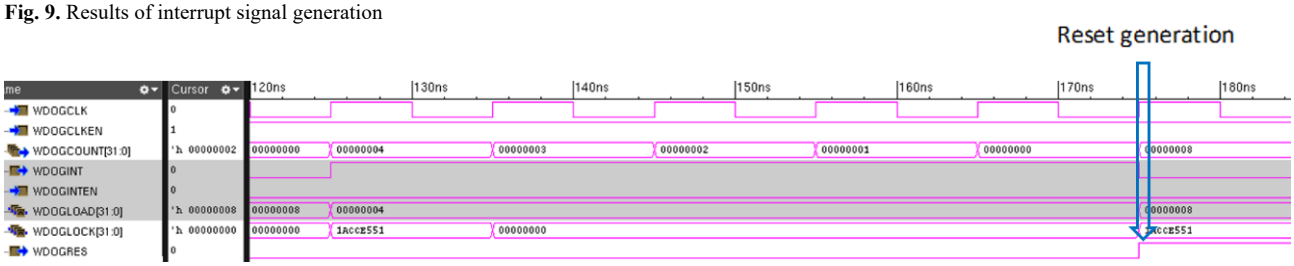

Fig. 10. Results of reset signal generation

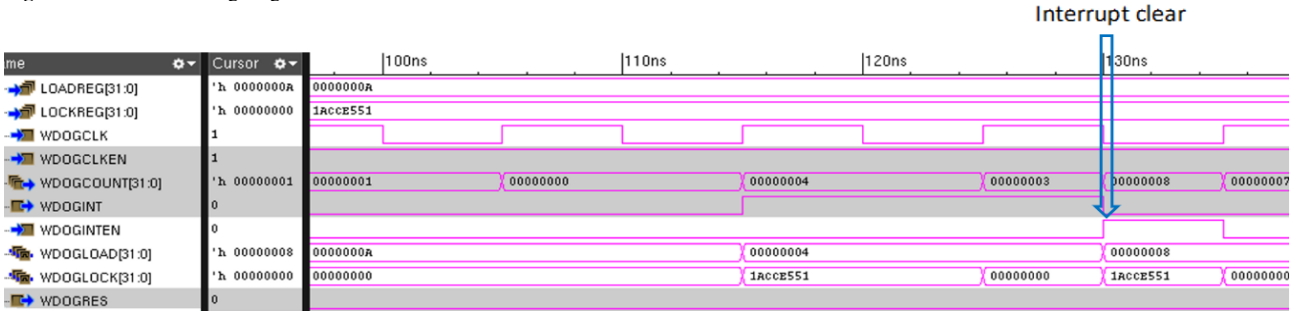

Fig. 11. Results of interrupting clear

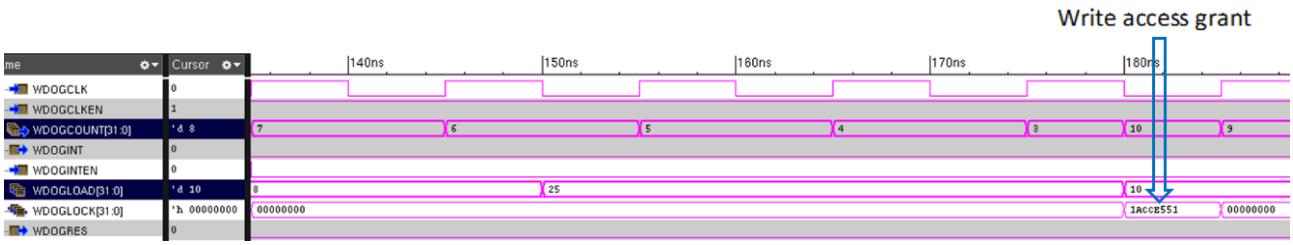

Fig. 12. Results of providing write access

Table 2. Characteristics of the design

Work	Technology	Delay (ns)	Resource/Area (μm^2)	Power (mW)
[36]	FPGA	2.576	-	-
[37]	FPGA/ASIC, 180 nm	12.508	221 LUTs/8250000	1.180
This work (Worst Case)	ASIC, 15 nm	0.054	217.842	1.7495
This work (Best Case)	ASIC, 15 nm	0.049	217.448	2.004

The proposed design is based on the use of Genus 20.1 from the Cadence Research bundle for two different operating conditions with the Nangate Open Library, 15 nm technology. A supply voltage of 0.88 V and a temperature of 0 °C are termed the best case, and a voltage of 0.72 V and a temperature are termed the worst-case scenario. For both operating conditions, a process value of 1 is used. The place, route and layout generation are performed via Innovus 20.1, as shown in Figure 13. Table 2 compares the results of the proposed design with those of the available literature on the implementation of watchdogs. Many researchers have applied FPGA platforms for watchdog module implementation. In [36], only the total delay in obtaining the result was presented without mentioning the FPGA used. In [38], a watchdog module along with a microcontroller was presented, which resulted in an overall delay on the order of microseconds. An application-specific integrated circuits (ASIC) approach was carried out in [37] to implement a generic watchdog module using both 180 nm technology and FPGA (Artix-7), which improved the performance and area compared with previous methods.

A commercial watchdog integrated circuit, TPS3431, has a time delay of 200 ms and requires a supply voltage of 1.8 V, whereas NCP302 requires 0.8 V and has a programmable delay. Another commercial watchdog module, WatchDog A150, is capable of sensing both temperature and humidity and is capable of gathering data for 111 days when the sampling interval is 30 minutes. The proposed work provides a detailed design, verification, and implementation in a lower technology node, 15 nm. The results indicate an operating frequency in the range of 18.52 GHz--20.41 GHz when the critical path delay for the worst and best cases is considered. The power delay products of the proposed design are 94.47 pJ and 98.82 pJ for two different conditions, suggesting that this work is suitable for portable devices where energy is a constraint.

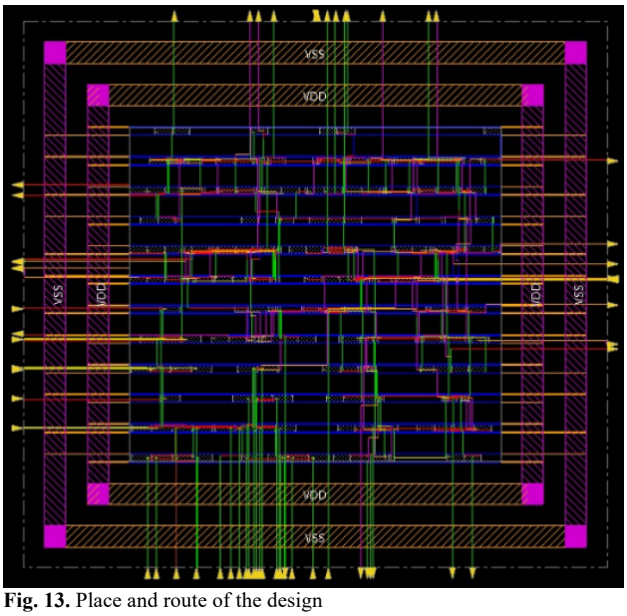

Fig. 13. Place and route of the design

The irregularities in software or hardware in drones cause their failure. To prevent specific drone failures, multiple watchdogs are necessary. In the case of a sensor malfunction, the watchdog resets the drone and should cause it to return to its original position on the ground. The drones used in surveillance operations face challenges due to high winds and signal interference. Coupling the watchdog module with an anemometer output to monitor the wind velocity and convert it to a continuously varying signal could track irregularities in its speed. The electromagnetic filters are designed to prevent inference to form the uninterrupted flight of the drones [39]. In the case of search and rescue drones, the watchdog needs to obtain data from multiple sensors, such as infrared sensors, navigation systems, and landscape maps.

Environmental stress factors such as humidity, atmospheric pressure changes, precipitation, sunlight, dust, and heavy rain can adversely affect the fight of drones. There is a major shift in temperature for most of these changes in environmental factors, where it has the greatest impact on the delay of the digital circuit. In the proposed work, the temperature variation is considered to range from -40 °C to +125 °C, and the delay variation is found to be less than 10 pico seconds. The packaging of these watchdog modules further prevents the adverse effects of precipitation, sunlight, and dust.

5. Conclusion

A complete flow of ASIC design and implementation is performed for the watchdog module in compliance with the well-known bus architecture. The functional verification of the slave module shows the proper operation of the device under various scenarios. The implementation results obtained via

state-of-the-art tools and a comparison with the literature show that the proposed method has better performance, less area, and less power dissipation and can be used under conditions where high-speed and low-power operation is necessary, as in the case of drones.

References

[1] W. Zhijun, C. Yu, S. Shengcai, D. Hao, L. Xiaobing, and X. Lijia, "Design and Experimental Analysis of Drone Rice Direct Seeding Device," *J. Eng. Sci. Techn. Rev.*, vol. 16, no. 5, pp. 132–139, Jan. 2023, doi: 10.25103/jestr.165.16.

[2] Wang, Z.-C. Fu, H.-S. Chen, and D.-S. Wang, "Characterizing the effects of intermittent faults on a processor for dependability enhancement strategy," *Sci. World J.*, vol. 2014, pp. 1–12, Jan. 2014, doi: 10.1155/2014/286084.

[3] R. K. Unni, P. Vijayanand, and Y. Dilip, "FPGA Implementation of an Improved Watchdog Timer for Safety-Critical Applications," in *2018 31st Int. Conf. VLSI Des. 2018 17th Int. Conf. Embedded Sys. (VLSID)*, Pune: IEEE, Jan. 2018, pp. 55–60. doi: 10.1109/VLSID.2018.37.

[4] "Design of Watchdog Timer for Real Time Applications," *Int. J. Innov. Techn. Explor. Engin.*, vol. 8, no. 9S2, pp. 695–697, Aug. 2019, doi: 10.35940/ijitee.i1143.0789s219.

[5] V. Kannaian and V. Palanisamy, "Energy-efficient scheduling for real-time tasks using dynamic slack reclamation," *Turkish J. Electr. Eng. Comp. Sci.*, vol. 27, no. 4, pp. 2746–2754, Jul. 2019, doi: 10.3906/elk-1806-170.

[6] H. S. Wang, A. B. Jambek, Z. A. Bin Abd Aziz, M. N. Md Isa, A. Harun, and S. N. Mohyar, "Design and implementation of bluetooth microcontroller in system-on-chip (SoC)," in *2nd Int. Conf. Adv. Earth Sci. Found. Eng.* (ICASF 2023): Advanced Earth Science and Foundation Engineering, Mohali, India, 2024, Art. no. 030008. doi: 10.1063/5.0192104.

[7] T. L. Harish and M. C. Chandrashekhar, "Review on Design and Verification of an Advanced Extensible Interface - 4 Slave Devices," *ACS J. Sci. Eng.*, vol. 3, no. 2, pp. 15–20, Sep. 2023, doi: 10.34293/acsjse.v3i2.80.

[8] H. Liu, "ARM-Based Embedded System Platform and Its Portability Research," *J. Comp. Commun.*, vol. 11, no. 11, pp. 51–63, Jan. 2023, doi: 10.4236/jcc.2023.1111003.

[9] M. R. Rezaee, N. A. W. A. Hamid, M. Hussin, and Z. A. Zukarnain, "Comprehensive Review of Drones Collision Avoidance Schemes: Challenges and Open Issues," *IEEE Trans. Intell. Transport. Sys.*, vol. 25, no. 7, pp. 6397–6426, Mar. 2024, doi: 10.1109/tits.2024.3375893.

[10] S. A. H. Mohsan, N. Q. H. Othman, Y. Li, M. H. Alsharif, and M. A. Khan, 'Unmanned aerial vehicles (UAVs): practical aspects, applications, open challenges, security issues, and future trends', *Intellig. Serv. Robot.*, vol. 16, no. 1, pp. 109–137, Mar. 2023.

[11] E. Kuantama, A. Seth, A. James, and Y. Zhang, "Flying Watchdog-Based Guard Patrol with Check Point Data Verification," *Fut. Intern.*, vol. 15, no. 10, p. 340, Oct. 2023, doi: 10.3390/fi15100340.

[12] Verdiesen, A. A. Tubella, and V. Dignum, "Integrating Comprehensive Human Oversight in Drone Deployment: A Conceptual Framework Applied to the Case of Military Surveillance Drones," *Information*, vol. 12, no. 9, p. 385, Sep. 2021, doi: 10.3390/info12090385.

[13] V. Parekh, P. Divya, K. Srilatha, and P. Chitra, "Design of the Configurable Watch Dog Timer using FPGA in Space Probe Application," *Int. J. Innov, Techn. Expl. Eng.*, vol. 8, no. 10, pp. 3555–3558, Aug. 2019, doi: 10.35940/ijitee.j9764.0881019.

[14] H. Lv, F. Liu, and N. Yuan, "Drone Presence Detection by the Drone's RF Communication," *J. Phys. Conf. Ser.*, vol. 1738, no. 1, Jan. 2021, Art. no 012044, doi: 10.1088/1742-6596/1738/1/012044.

[15] G. Alsuhli, A. Fahim, and Y. Gadallah, "A survey on the role of UAVs in the communication process: A technological perspective," *Comp. Commun.*, vol. 194, pp. 86–123, Jul. 2022, doi: 10.1016/j.comcom.2022.07.021.

[16] S. Park *et al.*, "A Research on Fail-Safe System by Watch Dog for Multi Sensor Fused Autonomous Vehicle," Sunyoung Park, *Korean Soc. Automot. Engin. Fall Conf. Exhib.*, Jeju, pp. 1204–1209, Sep. 2022

[17] T. Dorr, T. Sandmann, P. Friederich, A. Leitner, and J. Becker, "An Approach to Cost-Efficient Fault Tolerance in Inherently Redundant Fail-Operational Systems," in *2020 23rd Euromicro Conf. Dig. Sys. Design (DSD)*, Kranj, Slovenia: IEEE, Aug. 2020, pp. 630–637. doi: 10.1109/DSD51259.2020.00103.

[18] Y. Fu, A. Terechko, J. F. Groote, and A. K. Saberi, "A Formally Verified Fail-Operational Safety Concept for Automated Driving," *SAE Intl. J CAV*, vol. 5, no. 1, pp. 7–21, Jan. 2022, doi: 10.4271/12-05-01-0002.

[19] G. Peserico, T. Fedullo, A. Morato, F. Tramarin, and S. Vitturi, "Wi-Fi based Functional Safety: an Assessment of the Fail Safe over EtherCAT (FSoE) protocol," in *2021 26th IEEE Int. Conf. Emerg. Techn. Fact. Autom. (ETFA)*, Vasteras, Sweden: IEEE, Sep. 2021, pp. 1–8. doi: 10.1109/ETFA45728.2021.9613166.

[20] C. Torens, F. Nikodem, J. C. Dauer, S. Schirmer, and J. S. Dittrich, "Geofencing requirements for onboard safe operation monitoring," *CEAS Aeronautical J.*, vol. 11, no. 3, pp. 767–779, May 2020, doi: 10.1007/s13272-020-00451-0.

[21] T. Wu, W. Zhang, Y. Zhou, C. Wang, L. Ao, and S. Cao, "Research on electronics hardening technology of integrated electronic system of lunar exploration Cubesat," *J. Phys. Conf. Ser.*, vol. 2764, no. 1, May 2024, Art. no. 012085, doi: 10.1088/1742-6596/2764/1/012085.

[22] S. A. Jain, A. Bharadwaj, and C. M. B. N, "Characterizing WDT subsystem of a Wi-Fi controller in an Automobile based on MIPS32 CPU platform across PVT," *J. Ubiquitous Comp. Commun. Techn.*, vol. 2, no. 4, pp. 187–196, Nov. 2020, doi: 10.36548/jucct.2020.4.001.

[23] S. Singh, A. Kumar, A. Devrari, and A. Kumar, "ASIC Implementation of Programmable Timer Subsystems for WSN-SOC with WISHBONE Architecture on a Single Chip," *National Acad. Sci. Lett.*, vol. 45, no. 3, pp. 231–234, Mar. 2022, doi: 10.1007/s40009-022-01112-y.

[24] Dr. R. SenthamilSelvan, Dr. V. Mahalakshmi, Dr. S. P. Vijayaragavan, Dr. S. Arulselvi, and Jasmin, "A Novel Watchdog Timer for Real-Time Intensive Applications," *Proceed. First Int. Conf. Comp., Commun. Contr. Sys., I3CAC 2021, 7-8 June 2021, Bharath University, Chennai, India*, Jan. 2021, doi: 10.4108/eai.7-6-2021.2308611.

[25] C. D. J, I. Rashad, M. Thouqeer, M. T. Wahab, and S. B. Raj, "Microarchitecture and Design of a Watchdog Timer for aRISC-V based SoC," in *2023 Int. Conf. Innov. Data Commun. Techn. Applic. (ICIDCA)*, Uttarakhand, India: IEEE, Mar. 2023, pp. 984–988. doi: 10.1109/ICIDCA56705.2023.10099615.

[26] D. N. P. K. D and A. S. TS, "Implementation of VIP for bus interface logic of 32-bit processor using System Verilog," *Informacije MIDEM – J. Microelectron. Electr. Comp. Mat.*, pp. 205–211, Feb. 2019, doi: 10.33180/infmidem2018.402.

[27] M. Eckel, T. Gutsche, H. Lauer, and A. Rein, "A Generic IoT Quantum-Safe Watchdog Timer Protocol," *Proceedings of the 17th Int. Conf. Avail., Rel. Sec.*, vol. 1, pp. 1–10, Aug. 2023, doi: 10.1145/3600160.3605169.

[28] H.-W. Huang and W.-L. Yang, "Integration technique of digital I&C replacement and its Critical Digital Review procedure," *Ann. Nucl. Ener.*, vol. 51, pp. 146–155, Oct. 2012, doi: 10.1016/j.anucene.2012.08.010.

[29] M. Zhang and W. Qin, "Parametric Analysis of an Improved Fault Tolerant System," *Electr. Notes Theoret. Comp. Sci.*, vol. 207, pp. 121–136, Apr. 2008, doi: 10.1016/j.entcs.2008.03.089.

[30] B. Vanathy, V. G. Dikshit, A. Jacob, and G. Ranganath, "Onboard Digital Actuator Controller Software for Flight Control Actuators of UAV," *2022 6th Int. Conf. Computing, Commun., Contr. Autom. (ICCUBEA*, pp. 1–6, Sep. 2019, doi: 10.1109/iccubea47591.2019.9128619.

[31] V. Pritzl, M. Vrba, C. Tortorici, R. Ashour, and M. Saska, "Adaptive estimation of UAV altitude in complex indoor environments using degraded and time-delayed measurements with time-varying uncertainties," *Robot. Auton. Sys.*, vol. 160, Nov. 2022, Art. no. 104315, doi: 10.1016/j.robot.2022.104315.

[32] N. Vasiljević *et al.*, "Wind sensing with drone-mounted wind lidars: proof of concept," *Atmosph. Measur. Techniq.*, vol. 13, no. 2, pp. 521–536, Feb. 2020, doi: 10.5194/amt-13-521-2020.

[33] B. Al-Madani, M. Svirskis, G. Narvydas, R. Maskeliūnas, and R. Damaševičius, "Design of Fully Automatic Drone Parachute System with Temperature Compensation Mechanism for Civilian and Military Applications," *J. Adv. Transport.*, vol. 2018, pp. 1–11, Nov. 2018, doi: 10.1155/2018/2964583.

[34] Warrier, S. Al-Rubaye, G. Inalhan, and A. Tsourdos, "AI-Enabled Interference Mitigation for Autonomous Aerial Vehicles in Urban 5G Networks," *Aerospace*, vol. 10, no. 10, Oct. 2023, Art. no. 884, doi: 10.3390/aerospace10100884.

[35] T. Martin, *Designer's Guide to the Cortex-M Processor Family: A Tutorial Approach*. Oxford: Elsevier Science & Technology, 2013.

[36] V. R. Devi and J. Sreedhar, "Design and Implementation of an Improved Watchdog Timer for Memory Applications," in *2023 Global Conf. Inform. Techn. Commun. (GCITC)*, Bangalore, India: IEEE, Dec. 2023, pp. 1–4. doi: 10.1109/GCITC60406.2023.10426468.

[37] S. Singh, A. Kumar, A. Devrari, and A. Kumar, "ASIC Implementation of Programmable Timer Subsystems for WSN-SOC with WISHBONE Architecture on a Single Chip," *National Acad. Sci. Lett.*, vol. 45, no. 3, pp. 231–234, Mar. 2022, doi: 10.1007/s40009-022-01112-y.

[38] L. Blasi, F. Vigli, A. Cheikh, A. Mastrandrea, F. Menichelli, and M. Olivieri, "A RISC-V Fault-Tolerant Microcontroller Core Architecture Based on a Hardware Thread Full/Partial Protection and a Thread-Controlled Watch-Dog Timer," in *Lecture notes in Elect. Eng.*, 2020, pp. 505–511. doi: 10.1007/978-3-030-37277-4_59.

[39] Y. Zhang and K. Rasmussen, "Detection of Electromagnetic Interference Attacks on Sensor Systems," *2022 IEEE Symp. Secur. Priv. (SP)*, pp. 203–216, May 2020, doi: 10.1109/sp40000.2020.00001.