

**University of Mosul
College of Engineering**



Realization of Dependable Digital Systems for Safety-Critical Computer Systems using FPGAs

Farah Natiq Yaseen Qassab bashi

M.Sc. / Thesis

Science in Computer Engineering

Supervised by

Lect. Dr. Shawkat Sabah Khairullah

ABSTRACT

Digital systems are increasingly being used in safety-critical computer systems. These systems typically require high levels of reliability, safety, and performance to ensure the correct operation of the critical application in which the digital systems are embedded. To achieve the safety and functional objectives, many hardware-based digital systems that are built based on fault tolerance techniques, field-programmable-gate-arrays (FPGAs), and reliability analysis were proposed.

In this research, a new dependable hardware-based digital system (DeDS) that consists of fault-tolerant blocks (FTBs), spare functional blocks (SFBs), and synchronization units is presented. Markov-based chains have been used to model the correct operation of the proposed hardware system that is targeted to be realized on (FPGAs) based technology. This system was designed to be reliable against transient faults (TF) at repair rate 0.05 repair/ns, permanent faults (PF) at repair rate 0.001 repair/ns, and hardware common cause failures (CCF) at repair rate 0.01064 repair/ns. Mathworks Simulink tool was used in modeling the hardware components of the proposed system and verifying its functional and safety requirements, Vivado design tool was used to realize the hardware components of the proposed system. Furthermore, the dependability and reliability analysis of the system was achieved by using Markov-based chains and WinSure /WinStem programs. Moreover, to make it easier to program from a programmability point of view, the researcher used a Function Block Programming model similar to the international standard “IEC 61131-3 Programmable Logic Controllers”. Finally, a fault injecting of different transient, permanent, common cost faults was performed at different levels of the design to verify the correct operation of the internal components for the proposed digital system. The

maximum reliability that the proposed DeDS can be achieved is (0.9999999867) at a fault coverage (0.99999) and clock frequency (50) MHZ for (8760) hour.

الخلاصة

يتم استخدام الأنظمة الرقمية بشكل متزايد في أنظمة الكمبيوتر ذات الأهمية الأمنية. تتطلب هذه الأنظمة عادةً مستويات عالية من الموثوقية والامان والأداء لضمان التشغيل الصحيح للتطبيق المهم الذي يتم تضمين الأنظمة الرقمية فيه. لتحقيق أهداف السلامة والأداء الوظيفي، تم اقتراح العديد من الأنظمة الرقمية القائمة على الأجهزة والتي تم إنشاؤها بناءً على تقنيات تحمل الخطأ (FT)، مصفوفات البوابة القابلة للبرمجة حقلياً (FPGAs)، وتحليل الموثوقية.

في هذا البحث، تم اقتراح نظام رقمي جديد يمكن الاعتماد عليه (DeDS) يتكون من كتل تتحمل الأخطاء (FTBs)، وكتل وظيفية احتياطية (SFBS)، ووحدات التزامن، ووحدات إدخال وإخراج. تم استخدام السلاسل المستندة إلى ماركوف لنمذجة التشغيل الصحيح لنظام الأجهزة المقترح الذي يهدف إلى تحقيقه على التكنولوجيا القائمة على FPGA. تم تصميم هذا النظام ليكون موثوقاً به ضد الأعطال العابرة (TF) بمعدل تصلح 0.05 / نانو ثانية والأعطال الدائمة (PF) بمعدل تصلح 0.001 / نانو ثانية والأسباب الشائعة لفشل للأجهزة (CCF) بمعدل تصلح 0.01064 / نانو ثانية. تم استخدام أداة Mathworks Simulink في نمذجة مكونات الأجهزة للنظام المقترح والتحقق من متطلبات السلامة، وقد تم استخدام أداة التصميم Vivado لتحقيق مكونات الأجهزة للنظام المقترح. تم تحقيق تحليل الموثوقية للنظام باستخدام السلاسل المستندة إلى Markov وبرنامج WinStem / WinSure. علاوة على ذلك، لتسهيل البرمجة، تم الاعتماد على نموذج برمجة كتلة الوظائف مشابهاً للمعيار الدولي "IEC 61131-3". أخيراً، تم إجراء حقن لأخطاء عابرة ودائمة وشائعة على مستويات مختلفة من النظام المقترح للتحقق من التشغيل الصحيح للمكونات الداخلية للنظام الرقمي المقترح. الحد الأقصى من الموثوقية التي يمكن تحقيقها في DeDS المقترحة هي (0.9999999867) عند تغطية الخطأ (0.99999) وبتردد (50) ميغا هرتز لمدة (8760) ساعة.



جامعة الموصل
كلية الهندسة

تحقيق أنظمة رقمية آمنة معتمدة للأنظمة الحاسوبية الحرجة
باستخدام مصفوفات البوابة القابلة للبرمجة حقلياً"

فرح ناطق ياسين قصاب باشي

رسالة ماجستير
علوم في هندسة الحاسوب

بإشراف
م.د. شوكت صباح خير الله