University of Mosul

College of Engineering

Development of a Model-based Approach using Verification and Fault Tolerance Methods

Fayhaa Hamidi Kulaif Alshwichi

M.Sc. Thesis

Science in Computer Engineering / Computer Engineering

Supervised by

Assistant Professor Dr. Shawkat Sabah Khairullah

October/2023 A.D **Rabi Al-Akhar/1445 A.H**

ABSTRACT

The digital device systems have been used in different areas of our life such as industrial, medical, and transportation applications. Any fault or error occurrence in these systems can change the overall functionality of the safety-critical application and cause catastrophic consequences.

In addition, as complexity of these systems increases, it becomes difficult to find hazardous behaviors through traditional error detection techniques. To detect different types of errors and eliminate their effects on the system operation, new approaches of error detection and verification must be innovated in the system design and implementation.

One of these methods being employed to solve this issue is called formal verification which confirms that the system behavior meets the requirements early in the development process, before moving on to the implementation phase. As a result, the time and effort of design engineers will be decreasing, in addition to financial savings.

Our approach in this thesis is designing a digital system at a high level in terms of reliability and making it more dependable.

The first direction of this thesis was proving and verifying the safety-critical digital system that is compatible with the safety property, therefore our approach used the Simulink Design Verifier (SLDV) which is provided by MathWorks Simulink.

The verification model-based design (VMBD) approach in SLDV need for modeling the digital system and modeling the property. The property was formulated using Simulink blocks and truth table block, and because of the capabilities that Simulink

provided, MBD (model based design) of the system can be created easily.

The second direction focuses on how to make the system more dependable and work correctly even if a fault occurred during system operation at running time. The proposed hybrid fault tolerated TMR (triple module redundancy)technique which was able to detect the type of fault if permanent or transient, and isolate the failure system and replace it with an operational spare. The verification simulated experiments were performed on a computer that has the following specifications: Intel(R) Core(TM) i7-1065G7 CPU @ 1.30GHz 1.50 GHz processor and 16. GB RAM memory. Finally, the proposed model-based system was verified and proved that it is compatible with the required safety properties. Different types of safety properties were proved during the analysis time which is equal to 12 seconds and the PreProcessing Time is 10 seconds.

جامعة الموصل

كلية الهندسة

تطوير نهج قائم على النموذج باستخدام طرق التحقق والتسامح مع الأخطاء

فيحاء حميدي خليف الشويجي

رسالة ماجستير

علوم في هندسة الحاسوب / هندسة الحاسوب

بإشراف

أ.م.د. شوكت صباح خير الله

ربيع الآخر/1445 هـ

تشرين الاول/2023 م

الخلاصة

نظرا لان انظمة الاجهزة الرقمية (DDS) منتشرة بشكل واسع في حياتنا اليومية في العديد من مجالات الحياة سواء الطب، الصناعة ، المفاعلات النووية وغيرها من المجالات وان اي خطأ خلال تصميمها قد يودي الى خسائر كارثية قد تؤثر على حياة البشر او قد تسبب خسائر مادية كبيرة. لكشف هذه الاخطاء ومعالجتها والغائها خلال مرحلة التصميم ، تتطلب اقتراح طريقة تضمن النظام يعمل بشكل صحيح وموافق للمواصفات المطلوبة لكي يكون نظام موثوق (ReDDS). انشاء نظام رقمي موثوق ليس فقط ضمان خلوه من الاخطاء وموافق للمواصفات وانما ضمان استمرار عمله بشكل صحيح حتى اذا تعرض لأي خطا طارئ .اذن انشاء نظام عالي الوثوقية يتطلب ضمان عمله بشكل مطابق للمواصفات المطلوبة وخالي من اي اخطاء لا يمكن اكتشافها بطرق الفحص التقليدية ، وايضا يتطلب انشاء طريقة تضمن استمرار عمله عند تعرضه لاي خطا عابر او دائمي.

في هذا البحث تم اقتراح طريقة تتحقق رسميا من ان النظام يعمل بشكل صحيح وموافق للمواصفات المطلوبة في مرحلة مبكرة من التصميم قبل مرحلة التنفيذ. هي طريقة معقدة ولكن بنفس الوقت تحقق توفير في الوقت، وجهد المصمم وكذلك تحقق توفير مادي.

عملية التحقق الرسمية تحتاج الى استخدام لغة المنطق الزمني لصياغة المواصفات المطلوبة والتي عندها تكون عملية التحقق في درجة عالية من الدقة . في هذا البحث استخدمنا اداتين تحقق رسمية (SLDV TOOL BOX) التي يوفرها (Mathworks Simulink) هنا صياغة المواصفات كانت باستخدام الوحدات التي يوفرها المحاكي. بهذه الاداة يمكن تحليل النظام والتحقق منه وتتبع الخطأ في حالة عدم مطابقة النظام للمواصفات المطلوبة بسهوله نظرا للإمكانيات التي يقدمها البرنامج في هذا المجال. حيث تم استخدام البرنامج في نمذجة نظام الجهاز الرقمي(MBD) لحالة الدراسة التي تم استخدامها خلال البحث وفي نمذجة طريقة التحقق(VMBD). اما الاداة التحقق الرسمية الثانية فهي (NuSMV MODEL CHECKER) وهي اداة تحقق رسمية مشهورة، عملية التحقق تحتاج الى استخدام لغة المنطق الزمني ونمذجة تصرف عمل النظام بلغة (SMV). ايضا البحث تضمن اقتراح طريقة تضمن استمرار عمل النظام حتى اذا تعرض الى خطا دائمي ليس فقط ذلك وانما كشف نوع الخطأ ومكان الخطأ وعزل النظام المعطل واستبداله بنظام احتياط.