Send Orders for Reprints to reprints@benthamscience.ae

The Open Automation and Control Systems Journal, 2015, *7*, 1051-1056

Extended Dynamic Fault Tree Algorithm Based on Stochastic Petri Net and Micro-Satellite On-Board Computer Case Analysis

Yu Nan[1,*] and Li Jun-Zhou[2]

[1]*Department of Public Computer, Kaifeng University, Kaifeng, Henan, 475000, China*
[2]*Colloge of Art and Design, Kaifeng University, Kaifeng, Henan, 475000, China*

Abstract: Extended dynamic fault tree (DFT) diagrams represent logical relationships between events. Fault tree model can be used to identify system reliability or potential security weaknesses, and for detecting system of fault-tolerant systems, redundant (or cold and hot spares) repairable system, and public library system with order dependencies for system reliability analysis (SRA). We use stochastic Petri net for the extended DFT analysis and improved its analytic reliability using the micro-satellite on-board computer.

Keywords: Extended dynamic fault tree, micro-satellite on-board computer, stochastic petri nets.

1. INTRODUCTION

Extended dynamic fault tree (DFT) is a fault tree, which contains at least one special dynamic logic gate. DFT recovery time correlation is introduced to solve dynamic characteristic of reliability modeling and analysis of systems or equipment problems. For some important dynamic behaviors (such as recovery and timing-related faults and application of cold storage, *etc*.), the fault causation cannot use traditional static structure function of failure tree [1], as described earlier. DFT extends traditional static fault trees, making them repairable systems with order dependencies, having a public library system, and features such as cold or hot spares. DFT analysis of existing algorithms falls into 3 main categories of analysis algorithm: 1) based on Markov state transition process; 2) based on Bayesian Network algorithm; 3) based on trapezoidal approximation algorithms. These methods are established for making a system of DFT model out of the existing large and complex known mathematical models, enabling analysis of dynamic systems, since the static methods of the fault tree analysis cannot be applied to solve the dynamic random access memory correlation of faults and system problems.

We also proposed an extended DFT analysis method based on stochastic Petri net (SPN) and static reliability analysis method using micro-satellite on-board computer as an example.

2. RESEARCH OF EXTENDED DYNAMIC FAULT TREE

2.1. Concept of Extended DFT

Extended fault tree diagrams represent logical relationships between events. DFT analysis model can be used to identify system reliability or potential security weaknesses, resulting in improved design, improved system reliability and security. In recent years, with the net development of complex technology, not only the issues relating to reliability of network equipment are paid more attention [2], but also on reliability studies that provided updated requirements information. DFT analysis is based on traditional or logical static analysis methods of failure mechanism, but unlike them, DFT analysis is a dynamic fault tolerant system embedded with redundant (or cold and hot backup) repairability systems, having a public library system, and reliability system analysis with order dependencies. For example, the Web server is the core of the network, its failure would cause network disruptions. Therefore, in the actual network server, a hot backup server is required to improve network reliability.

For example in the case of source servers, such as switch controller and the backup server systems, if the switch controller fails after a fault has occurred on the source server, the backup server has to work; this is when a system is required to identify and troubleshoot switching controller failure on the source server before the failure occurs, because the traditional backup server is unable to switch to a working state. Therefore, the failure mode of network servers is not only associated with combinations of events, but also associated with the sequence of events. As another example, network switches are used to connect several independent local area networks for data processing between one kind of network interconnected devices that can be used to solve the bottleneck of bandwidth and network switching. Switch has a fault tolerance features, such as the electric plug, power backup, and link fault tolerance, which cannot be described by a traditional DFT analysis. Additionally, for the system has cold and hot spare parts; so with the state change, its component lose efficiency since the change is not continuous. That is cold spare parts activity failure is higher than the hot spare parts which means that hot spare parts' efficiency loss is low compared to the cold spare parts, and both cold spare parts and hot spare parts get activated upon entering

*Address correspondence to this author at the Department of Public Computer, Kaifeng University, Kaifeng, Henan, 475000, China;
Tel: 13623785696; E-mail: fanruo@yeah.net

1874-4443/15

the work [3]. The system is thus stated to undergo frequent high and low efficiency loss which is reflected through its spare parts lost efficiency, but this change in state does not have continuity. Dynamic characteristic of these systems cannot be represented by the traditional DFT analysis model. At present, there are complex system reliability analysis (SRA) method for DFT analysis, binary decision diagram (BDD) and Markov chain method (Markov Chains) to analyze the systems.

DFT analysis method combines the advantages of both fault trees analysis and Markov chain method, by introducing the characterization of the dynamic characteristics of a new type of logic gate, to establish the appropriate fault tree, *i.e.* a DFT analysis, for addressing those dynamic SRA in effective ways. The main purpose of this paper is that the traditional DFT analysis model (both logical and mathematical expressions), analytical methods and technology, extended to dynamic characteristics of reliability, safety and maintainability design for complex systems analysis, dynamic SRA of complex systems problems are better addressed.

2.2. Survey of Studies on Domestic and International Levels

In foreign countries, the use of SRA of DFT analysis has a history of nearly 40 years. In 1960, the missile system was analyzed for reliability by using DFT analysis method. Since then, DFT analysis method has been greatly developed. At present, with the development of the theory of DFT analysis, DFT analysis technology is first used for SRA of fault-tolerant computer and control systems, including avionics systems, FTPP (fault-tolerant parallel processor) configuration, structure of mission avionics systems, fault-tolerant hypercube, space stations, and air traffic control systems, and so on. Duke University and the NASA (United States NASA) Langley Research Center developed the HARP (hybrid automatic reliability prediction) software packages to analyze expecting the higher level of the reliability of fault-tolerant systems. Wei HA provided a package according to system structure and proposed a fault recovery model through behavior decomposition, which uses behavior decomposition model, maintenance child model (FORM), and fault and errors processing child model (FEI Wei spit) for the decomposition of the fault occurred; Also the system structure of DFT analysis model is made to automatically convert into Markov model which combined the fault recovery information, this conversion has avoided the previous boring conversion of the system into Markov chain of model. In addition, Essay and M.K. in 1992, worked on the dynamic behavior of another type of model, using fault tree and Markov model. Professor Dugan at the Virginia University is recognized for his work on reliability analysis of the space station, as well as air traffic control and other complex systems. Based on Markov theory, a Combinatory is built on DFT analysis model in which Markov model and combination models can coexist, in order to avoid the whole systems DFT reliability analysis failure provided the fault tree size is too large to be calculated by DFT analysis graphs. Then, one can switch to Markov chain model. Professor Dugan presented three models of DFT analysis method to improve the efficiency of DFT analysis. DFT analysis method is as follows:

$$V = V(T_0, N) = \bigcup_{T=T_0+\Delta T}^{T_0+N*\Delta T} V_t \quad (1)$$

At the national level, there is little research on DFT analysis methods, and it is limited to homogeneous Markov chain method for calculating DFT analysis model and simulation of fault tree of complex system theory. With the software development, multifunctional DFT analysis software package was developed in 1983, by Tsinghua University for FTAP handling of static fault trees, its modular kernel algorithm however imposes larger limitations. In terms of research on dynamic fault tree, in the early 90's, the Institute of National University of defense system engineering (formerly seven) embarked on DFT analysis method to study on the research, development and application of software tools. In 1992, due to Fusel algorithm and its modular approach to developing Windows applications software tools FTAS10 [4], the software tool will combine traditional DFT analysis algorithm and simulation method to solve the "92,113" Project failure dependencies and characteristics of the DFT analysis at different working hours. But the DFT analysis software working on the size and speed of the system has certain limitations. In 1995, based on its own research BDD algorithm was proposed for reliability analysis to form a new software version FTA3.0, but the software cannot handle non-coherent systems such as, satellite rotation control unit fault tree. In 1999, they completed the non-coherent fault trees analysis technique based on BDD research, forming a FTA4.0. But FTA4.0 still cannot handle DFT analysis with dynamic logic gates.

2.3. Existing Problems

DFT analysis, as a new technology, having a history of only a few years, faces several problems waiting to be solved.

DFT analysis built-in model: DFT analysis involves more logic gates and is expressed as complex, especially introduction of dynamic logic gate, makes the DFT built-in model with the previous static fault tree different. Therefore, since reliability indicators established for DFT built-in model analysis caused much difficulty, so solving the DFT built-in model and established reliability indicators is one of the key problems.

Preprocessing of DFT: Analysis of DFT practical systems often requires great amounts of calculation, which sometimes cannot be solved even under the existing conditions [5]. Fault tree module is divided into a separate dynamic and static sub trees; static sub trees (sub tree that contains no dynamic logic gates) is solved by using BDD solution, whereas dynamic sub tree (containing at least one dynamic logic gate) is solved by using Markov models. Modular FT directly affects the complexity of solving.

As the number of parts increases, there is an exponential growth in the number of nodes in Markov chains. Due to the issues of memory and computation time, currently Markov chains works with fewer parts, so the complexity of Markov process for solving problems, as well as simplification is particularly important in the pretreatment of Markov.

Dynamic algorithm of qualitative and quantitative analysis of fault tree: Abroad and fewer domestic research rarely published details on the algorithm of qualitative and quantitative analysis of DFT, the rare contents of documents in this field, makes the study of qualitative and quantitative analysis of DFT algorithm very difficult, especially with regard to dynamic system with sequence dependent failure analysis of reliability and maintainability. For example, a traditional quality fault tree contains cut set of monotonic system failure modes and cut sets of non-monotonic systems failure modes, which is a combination of events. But in a dynamic fault tree, due to the introduction of dynamic logic gates, and order problems in the system failure modes, dynamic fault trees can no longer be characterized to have cut set of system failure modes, and therefore one has to find a new method. As another example, fault tree used structural importance, probability and importance of different units or components in the system such as the importance of dynamic fault tree. Due to the application of the Markov model, various methods of importance in the past are no longer applicable, so one must study Markov models for important issues.

Software development: DFT analysis techniques to be applied to engineering models, have been widely accepted and applied by engineers for developing a generalization of DFT analysis software for engineering tools. Therefore, study of DFT software tools is the key technology and difficulty of the project.

3. DESCRIPTION AND ANALYSIS OF THE STOCHASTIC PETRI NETWORK (SPN)

Along with social progress and the development of science and technology, especially information technology, computer technology, modern communications technology, the development and application of network technology; system faces more and more complex problems, making system analysis more difficult [6]. So, people started looking for a new approach to system modeling and analysis, and hence Petri nets came into being.

Petri nets are to describe and analyze a model tool for parallel systems. Since 1962, C.A. Petri introduced the basic concept of Petri nets, which after nearly 50 years of development, has been developed into a rigorous mathematical foundation, *i.e.* General NET theory of multiple levels of abstraction. Petri nets are the study and analysis of concurrent, parallel, asynchronous, synchronous, randomness, resource sharing, and other characteristics making a powerful tool of the system. Now, it has been widely used in the fields of computer science, communications, control, software, mechanical, electrical, and electronic.

3.1. Petri Net Basic Concepts

Classical Petri nets are defined by the library, as denoting change and flow relationships. As research advances, it gradually develops a variety of high-level Petri nets, such as generalized stochastic Petri nets (GSPN), random rewards network (SRN), stochastic high-level Petri nets, deterministic and SPN. This chapter focuses on the structure, properties and general theory of Petri nets, since it is the Petri net based knowledge that is the basis of other advanced networks.

In the middle of 20th century, Modern Monte Carlo methods of simulation in the course of development of nuclear weapons were proposed by Von Neumann and Ulla. Monte-Carlo simulation method is based on the method and theory of probability and statistics. The main idea is: to establish a probability model for the system, supposedly experimental sampling and statistical processing, resulting in the solution of the problem. Current theories based on Monte Carlo methods are widely used in various fields of science and engineering, such as particles in numerical simulation on transport issues, structural mechanics and analysis to evaluate the reliability of the system. Monte Carlo simulation used in reliability analysis of system simulation is mainly the system of life processes.

Since the middle of the last century, the Monte Carlo simulation has been applied as a less restrictive statistical simulation method to approximate the problem, many experts are concerned about the application of Monte Carlo simulation for reliability analysis. Wales Burnett proposes an exponential distribution model for application in certain conditions, which analyzes application of confidence interval of reliability index analysis based on Monte Carlo simulation method to solve the differences. Moore gives a general method for Monte Carlo simulation, but preconditions must be the known failure modes and parameters of joint distribution. Gilmore provides solution for finding the Mean Time Between Failure (MTBF) of complex systems, the applied approach is Bayesian integrated Monte Carlo simulation. Riley and Kamet consider the components of maintenance problems [7] that can be solved independently by Monte Carlo reliability evaluation method of confidence limits. Application updates of reliability evaluation method for assessing Monte Carlo simulation were presented by Komati in two ways; one is an associated fault-tree dagger that can be expressed as sampling; another is the Markov state transition diagram that can be represented as a smooth state transition of repairable system. Moore suggested that this method can determine the reliability of repairable system with confidence limits. Kim applies a statistical technique called Principal Component Analysis (PCA) to satisfy the following assumptions in giving the associated assessment of binomially distributed systems to approximate MTBF of the method. Assumptions are as follows: component independent of the state; new components to instantly replace failure components; ignore component replacement time; failure of a minimal path cut sets, which belongs to the minimal path cut sets of all components that stop working; known component's life and minimal path cut sets of distribution functions, and other fields. Petri net modeling formula is as follows:

$$R_s(t) = \prod_{i=1}^{n} R_i(t) = \exp(-\sum_{i=1}^{n} \lambda_i t) \quad (2)$$

3.2. Petri Nets Representation of Relationships Between Events

Petri network has two knot points: points and transitions that is location and changes. "location with circle", in fault analysis, requires the system to identify components of failure, environmental effects, software defects, artificial errors, and events. "Change with short-term", after changes, level

event spread to level event; Thus, a Petri network contains location, changes and arc.

Location and changes has two connections with arc: one "arc connecting a location to changes or changes to a location"; two a location or changes arc does not allow "in fault analysis the fault-facing direction with spreading rate". In Petri network there are three species of graphics symbols in that: the location of number is a non-zero of limited value; changes of number is non-zero; and the limited.

Petri network by description is a system of dynamic changes, and this dynamic change process is achieved through changes inspired by: "each of the changes which are included, at least identifies a location that it is entering; whether this is 'changes of inspired' or 'changes of makes' has to be determined." Worth noting is that a 'changes of inspired' does not means it was immediately inspired, instead it was inspired by possibilities just as "a changes of inspired' will lead to the reduced changes at each entered location that it identifies, *i.e.* one logo per output location.

3.3. The Basic Behavior of Petri Nets

In real systems, there is interdependence between factor and factor competition, coordinating relationships, such as "system must be able to express the relationship between concurrency and conflict."

Recently, researchers have put time to introduce Petri network in various ways, and identified two common specifications: first is that each location related Alliance is a time parameter; second is that each changes related Alliance is a time parameter. Currently, most literature used Petri network model as a system, because in this system an event occurred (usually with changes of inspired) must need time. So, time and changes related Alliance is compared naturally.

Concurrent expressions relationship to Petri nets allows two or more changes distinguishing both the enabling conditions T2 and T3, as shown in (Fig. **1**). Both of the enabling conditions do not interact in any way, and this situation is called concurrency of the Petri nets.

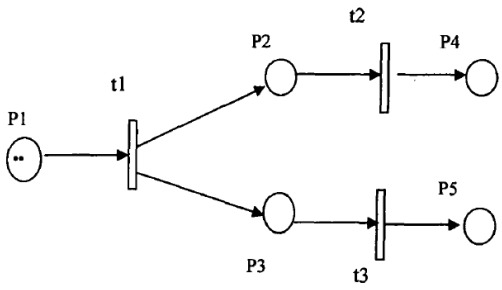

Fig. (1). The concurrent Petri nets.

Petri nets are inherently non-deterministic, concurrent computational models. Petri network work with parallel system of behavior under the following conditions "concurrence for its dynamic behavior for description and analysis brings amazing complexity". Because, in basic Petri network this complexity is limited, whereas artificial one provides unlimited: since changes of inspired is an instantaneous event and cannot be occurred while the above two events happening", such as occurrence of two species T2 and T3, in the inspired order as shown in Fig. (**1**).

Relationship conflicts: Petri nets allow two or more changes to the State, but they are not independent of each other [8], as inspired by any of these changes will not make the change enabled. Petri nets referred to this nature as conflict sex. As shown in Fig. (**2**), which is an example of a conflict, change of T1 and T2 in the enabled state, but any change of inspired would be destroyed in the transforming of T1 and T2 in another shooting condition. In this case, Petri nets run non-required event occur simultaneously excited by selecting the priority.

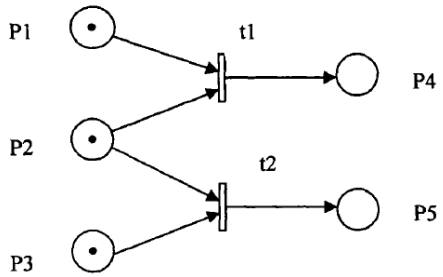

Fig. (2). Conflicting relation of petri nets.

Time concept of initial work in Petri network in the not using state: time parameter may damage Petri network structure established as real all because behavior and conception. However, many application fields, especially system performance quantitative analysis, need time concept, and related mathematics tools are not satisfactory at people attempts to work in Petri network in the set time constraint conditions (or established time parameter). Thus, application range of Petri network has been extended.

4. ANALYSIS OF RELIABILITY OF MICRO-SATELLITE ON-BOARD COMPUTER SYSTEM

On-board computer is a typical embedded computer system, but because of its work in a special space environment, it also has some particularities. Under normal circumstances, we believe that failure of hardware and software of a computer system can be restored to the original functionality, after testing, and repairing or replacing the devices. However, since the on-board computers, replacement devices or hardware maintenance are impractical and in contrast, software on-orbit repair can be achieved through link between satellite-ground communications after repair procedures. Therefore, this paper argues that on-board repair system is based on computer hardware systems; software on-orbit systems are repairable systems, whereas hardware on-board computer system is a non-repairable system which repairs parts of complex systems.

4.1. Reliability Analysis of Hardware Subsystems

This section only discusses the reliability of on-board computer hardware subsystems, without regard to anyone involved (or soft errors) due to system failure. That is, the scope of this section covers the hypothesis that soft failure does not necessarily belong to the system failure [9]. On-board computer hardware subsystem must be the system used, so this section uses reliability blocks diagram-based modeling system for single-CPU, and warm-start dual system for analysis.

Reliability analysis of CPU boards: CPU board involves CPU, FPGA, SRAM, FLASH, RS232, JTAG, Ethernet, dual CAN bus and SEL-resistant protection circuit. RS232 port and JTAG network interface are only used in the commissioning stage, and SEL is a circuit protective device used only for critical protection and does not cover the functional requirements of the CPU board. So, when establishing a reliability block diagram, the CPU board considers a few basic components such as: CPU, FPGA, SRAM, dual CAN bus and FLASH. Assess system reliability based on the following formula calculating Mean time to failure (MTTF):

$$MTTF = \frac{1}{\lambda}\sqrt{\frac{1}{2 * M}} \tag{3}$$

Inside the CPU board, in order to improve the reliability of veneer, FLASH has triple modular redundancy compared to CAN bus, so the CPU board reliability model is used for a parallel-series model. FLASH is used to prevent errors in triple modular redundancy voting machine implemented in the FPGA, where FPGA is equivalent to voter/machine rolls and 3 FALSH constitutes a 2/3 (G) system. SRAM EDAC codecs are also implemented in the FPGA. Therefore, these two parts are in line with in-line models feature. In addition, the dual CAN bus is clearly a parallel system.

Reliability analysis of dual temperature systems: From a hardware point of view, double machine paralleled warm standby system is a standby system with switch. Although two CPU boards are used in exactly the same hardware architecture, but there are certain differences between the job machine and backup machines due to different work patterns [10]. It is believed that the backup failure rates are less than job failure rates. In addition, before referring to the prototype system referred to in the previous chapter, a certain type of switch based on k-logic is realized by FPGA.

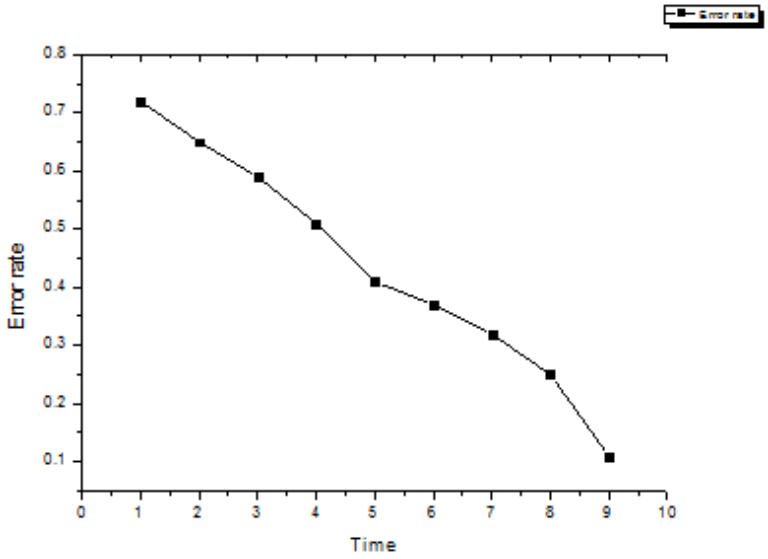

Fig. (3). The error rate of DFT using Petri net.

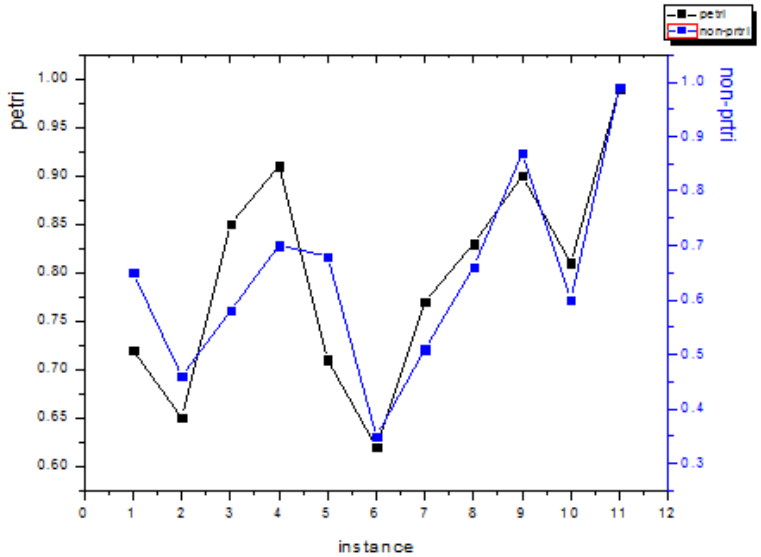

Fig. (4). Using and not using Petri net comparison of speed graph.

4.2. On-Board Computer System Instance Based on Extended SPN of DFT Analysis of Reliability

Efficiency of the extended DFT analysis based on SPN is compared with and without using Petri nets. Time accuracy can have an overall distinct advantage, as it will gradually reduce the chance of an error. Fig. (**3**) shows extended DFT analysis method failure rate curves using Petri nets over time.

Meanwhile, in the case of micro-satellite on-board computer, we calculated the same results of both cases; use of Petri optimization of dynamic fault trees can significantly increase the speed, which is shown in Fig. (**4**) *i.e.* using and not using Petri net time efficient DFT algorithm comparison chart. The picture clearly shows the speed upgradation.

Overview of algorithm reliability: Regarding the definition of algorithm reliability, there have been two schools of thought: one is based on viewpoint of pure computer experts; they think "algorithm reliability [11] should be closely associated with the correctness of the algorithm together. Without the right software to fail sooner or later, so reliability is 0, reliable and error-free software-1 ". Another view is from a probability perspective, which follows the general definition of reliability, and refers to algorithm for the software reliability under specified conditions and capacity within the specified time to complete the assigned functions. Error-free software however, is difficult to achieve in practice and errors in software are able to work within a certain range, to meet the demand. Therefore, the second definition of the kind of software reliability is preferred.

CONCLUSION

Stochastic Petri net (SPN) is a powerful modeling capability, and is complementary to conventional Petri nets. System dynamic reliability model can be obtained by SPN modeling, and analysis of SPN model of fault events can obtain the corresponding fault status indicator. In the application of DFT algorithm, SPN model demonstrated its powerful optimization capabilities, which could be possible to intuitively view from the onboard computer instances. Through the analysis of this combination of SPN and fault tree it is established that the combinatory has great prospects.

CONFLICT OF INTEREST

The authors confirm that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

Declared none.

REFERENCES

[1] Suprasad, D. Glenn, and H. Eileen, "A new approach to solve dynamic fault trees," IEEE In: *Proceedings Annual Reliability and Maintainability Symposium*, Tampa, FL, 2003, pp. 374-379.

[2] O. Yong, M. Leila, and B. D. Joanne, "Multi-phase reliability analysis for dynamic and static phases," In: *Proceedings of Annual Reliability and Maintainability Symposium*, Virginia, pp. 404-410, 2012.

[3] J. A. Peter, "Stochastic petri nets for modeling and simulation," In: *Proceedings of the Winter Simulation Conference*, 2004.

[4] X. Zhang, Q. Miao, and X. Fan, "Dynamic fault tree analysis based on petri nets," In: *Reliability, Maintainability and Safety*, 2009, *ICRMS 8th International Conference*, 2009, pp. 138-142.

[5] A. Adamyan, and D. He, "Sequential failure analysis using counters of petri net models," IEEE *Transactions on System, Man, and Cybernetics-Part A: Systems and Humans*, vol. 33, no.1, pp. 1-11, 2010.

[6] G.S. Hura, and J.W. Atwood, "The use of petri nets to analyze coherent fault trees," IEEE *Transactions on Reliability*, vol. 37, no. 5, pp. 469-473, 2011.

[7] H. Boudali, and J. B. Dugan, "A discrete-time Bayesian net-work reliability modeling and analysis framework," *Reliability Engineering and System Safety,* vol. 87, pp. 337-349, 2005.

[8] J. C. Geffroy, and G. Motet, *Designing of Dependable Computing Systems*, Kluwer Academic, USA, 2003.

[9] M. Witting, "Satellite onboard processing for multimedia applications,' *IEEE Communications Magazine*, pp. 134-140, 2010.

[10] M. Zhao, "Reliability design for analog parts of micro-satellite on board computer system," *Systems Engineering and Electronics*, vol. 28, no. 2, pp. 314-316, 2006.

[11] X. Ma, and X. Cao, "Study of reliability for on-board computer system," *Systems Engineering and Electronics*, vol. 24, no.8, pp. 127-129, 2002.

Received: September 16, 2014 Revised: December 23, 2014 Accepted: December 31, 2014