Reliability Block Diagrams based Analysis: A Survey

Osman Hasan and Waqar Ahmed*, Sofiène Tahar† and Mohamed Salah Hamdi**

*Sch. of Elect. Engg. & Comp. Sc., National University of Sciences and Technology (NUST), Islamabad, Pakistan
{osman.hasan,12dphdwahmed}@seecs.nust.edu.pk
†Department of Electrical and Computer Engineering, Concordia University, Montreal, QC, Canada
tahar@ece.concordia.ca
**Information Systems Department, Ahmed Bin Mohammed Military College, Doha, Qatar
mshamdi@abmmc.edu.qa

Abstract. Reliability Block Diagrams (RBDs) allow us to model the failure relationships of complex systems and their sub-components and are extensively used for system reliability, availability, dependability and maintainability analyses of many engineering systems. Traditionally, Reliability Block Diagrams (RBD) are analyzed using paper-and-pencil proofs or computer simulations. Recently, formal techniques, including Petri Nets and higher-order-logic theorem proving, have been used for their analysis as well. In this paper, we provide a concise survey of these available RBD analysis techniques and compare them based on their accuracy, user friendliness and computational requirements.

Keywords: Reliability Block Diagrams, Computer Simulations, Formal Methods, Theorem Proving, Computer Algebra Systems,
PACS: 03B15, 03B70, 03B35, 60Axx

INTRODUCTION

A reliability block diagram (RBD) [21] is used to asses various failure related characteristics, such as reliability [16], availability [13], dependability [22] and maintainability [7], of a wide range of engineering systems. The main idea is to represent the behavior of the given system in terms of a RBD, i.e., a graphical structure consisting of blocks and connectors (lines). For example, while assessing the reliability of a computational software, the blocks may represent the computational elements, with some given failure rate, and the connectors between them may be used to describe various alternative paths required for a successful computation using the given software [2]. Now, based on this RBD, the failure characteristics of the overall system can be judged based on the failure rates of individual components, whereas the overall system failure happens if all the paths for successful execution fail. The RBD-based analysis enables us to evaluate the impact of component failures on the overall system safety and reliability and thus is widely used for assessing the trade-offs of various possible system configurations at the system design stage.

Traditionally, the RBD-based analysis has been done using paper-and-pencil proof methods and computer simulations. However, these methods cannot ascertain absolute correctness due to their inherent limitations. To overcome the above-mentioned inaccuracy problems, formal methods have been proposed for the RBD-based analysis as well. However, these methods have a limited scope and thus cannot be used to analyze all kinds of complex engineering systems. In this paper, we provide a brief overview about the above-mentioned RBD based analysis techniques. Based on this description, the a concise comparison between them is also presented.

RELIABILITY AND RELIABILITY BLOCK DIAGRAMS

Reliability $R(t)$ is defined as the probability of a component performing its desired task over certain interval of time t.

$$R(t) = Pr(X > t) = 1 - Pr(X \leq t) = 1 - F_X(t) \tag{1}$$

where $F_X(t)$ is the CDF. The random variable X, in the above definition, models the time to failure of the system .

The RBD based reliability analysis of a system involves a three-step process: (i) partitioning the given system into segments and constructing its equivalent RBD, (ii) assessing the reliability of the individual segments and (iii) evaluating the reliability, availability, dependability and maintainability characteristics of the complete system based on the RBD and the reliability of its individual segments. The reliability of an individual segment is usually expressed

Proceedings of the International Conference on Numerical Analysis and Applied Mathematics 2014 (ICNAAM-2014)
AIP Conf. Proc. 1648, 850129-1–850129-4; doi: 10.1063/1.4913184

in terms of its failure rate λ and a random variable, like exponential [23] or Weibull random variable [15], which models the failure time. The most commonly used RBD configurations are described below:

Series Reliability Block Diagram: The reliability of a system with components connected in series is considered to be reliable at time t only if all of its components are functioning reliably at time t. If $A_i(t)$ is a mutually independent event that represents the reliable functioning of the i^{th} component of a serially connected system with N components at time t, then the overall reliability of the complete system can be expressed as [5]:

$$R_{series}(t) = Pr(A_1(t) \cap A_2(t) \cap A_3(t) \cdots \cap A_N(t)) = \prod_{i=1}^{N} R_i(t) \tag{2}$$

Parallel Reliability Block Diagram: The reliability of a system with parallel connected sub-modules mainly depends on the component with the maximum reliability. If $A_i(t)$ is a mutually independent event that represents the reliable functioning of the i^{th} component of a system with N parallel components at time t then its overall reliability is [5]:

$$R_{parallel}(t) = Pr(A_1 \cup A_2 \cup A_3 \cdots \cup A_N) = 1 - \prod_{i=1}^{N} (1 - R_i(t)) \tag{3}$$

Parallel-Series Reliability Block Diagram: Most of the safety-critical systems in the real-world contain many reserved sub-stages for backup and ensuring reliable operation. If the components in these reserved *subsystems* are connected serially then the structure is termed as a parallel-series structure. The parallel-series RBD is used to model such complex structures. If $A_i(t)$ is a mutually independent event that represents the reliable functioning of the j^{th} component connected in a i^{th} subsystem, then the reliability of the complete system can be expressed as [5]:

$$R_{Parallel-Series} = Pr(\bigcup_{i=1}^{M} \bigcap_{j=1}^{N} A_{ij}) = 1 - \prod_{i=1}^{M} (1 - \prod_{j=1}^{N} (R_{ij}(t))) \tag{4}$$

Series-Parallel Reliability Block Diagram: Just like the previous case, if in each serial stage the components are connected in parallel then the configuration is termed as a Series-Parallel RBD. If $A_i(t)$ is a mutually independent event that represents the reliable functioning of the j^{th} component connected in an i^{th} subsystem at time index t, then the reliability of the complete system can be expressed as [5]:

$$R_{Series-Parallel} = Pr(\bigcap_{i=1}^{N} \bigcup_{j=1}^{M} A_{ij}) = \prod_{i=1}^{N} (1 - \prod_{j=1}^{M} (1 - R_{ij}(t))) \tag{5}$$

ANALYSIS TECHNIQUES

Paper-and-Pencil proof Method: Due to the involvement of manual manipulation and simplification, this kind of analysis is error-prone and the problem gets more severe while analyzing large systems. Moreover, it is possible, in fact a common occurrence, that many key assumptions required for the analytical proofs are in the mind of the mathematician and are not documented. These missing assumptions are thus not communicated to the design engineers and are ignored in the system implementations, which may also lead to erroneous designs.

Computer Simulations: The RBD-based computer simulators, such as ReliaSoft [18] and ASENT [4], generate samples from the exponential and Weibull random variables to model the reliabilities of the sub-modules of the system. This data is then manipulated using computer arithmetic and numerical techniques to compute the reliability of the complete system. These software are more scalable than the paper-and-pencil proof methods. However, they cannot ensure absolute correctness as well due to the involvement of pseudo random numbers and numerical methods.

Petri Nets: Formal methods [6], which are computer based analytical analysis techniques, are known to overcome the above-mentioned limitations of traditional analysis techniques and have also been used in the context of RBD analysis. For instance, Petri nets have been used for the RBD based dependability analysis of a disaster tolerant model for cloud computing [20]. The technique has been used to automatically identify deadlocks in the given system and

TABLE 1. Comparison of RBD based Analysis Techniques

	Paper-and-Pencil Proof	Simulation	Petri Nets	Theorem Proving
Expressiveness	Yes	Yes	No	Yes
Scalability	No	No	No	Yes
Accuracy	Yes-**?**	No	Yes	Yes
RBD Configurations	Yes	Yes	Yes	No
Automation	No	Yes	Yes	No-**?**

verify some structural properties, such as reachabillity and liveness, but the analysis is not scalable for large systems due to the state-space explosion problem. Moreover, generic mathematical RBD relationships cannot be verified using such state-based petri nets techniques, which limits the scope of this approach. Similarly, a Colored Petri Nets (CPN) based tool is used to model dynamic RBDs (DRBDs) [19], which are used to describe dynamic reliability behavior of systems. The CPN verification tools, based on model checking principles, are then used to verify behavioral properties of the DRBDs models to identify design flaws [19]. However, due to the state-based model, only state related property verification, like deadlock checks, is supported by this approach and generic reliability relationships cannot be verified.

Higher-order-logic Theorem Proving: Higher-order logic [8] is a system of deduction with a precise semantics and can be used to formally model any system that can be described mathematically including recursive definitions, random variables, RBDs, and continuous components. Similarly, interactive theorem provers are computer based formal reasoning tools that allow us to verify higher-order-logic properties under user guidance. The foremost requirement for reasoning about reliability related properties of a system in a theorem prover is the availability of the higher-order-logic formalization of probability theory. Hurd's formalization of measure and probability theories [14] is a pioneering work in this regard. Building upon this formalization, most of the commonly-used continuous random variables [10] and some reliability theory fundamentals [11, 1] have been formalized using the HOL theorem prover. However, the foundational formalization of probability theory [14] only supports the whole universe as the probability space. This feature limits its scope in many aspects [17] and one of the main limitations, related to RBD-based analysis, is the inability to reason about multiple continuous random variables [10, 11]. Some recent probability theory formalizations [17, 12] allow using any arbitrary probability space that is a subset of the universe and thus are more flexible than Hurd's formalization of probability theory. Particularly, Mhamdi's probability theory formalization [17], which is based on extended-real numbers (real numbers including $\pm\infty$), has been recently used to reason about the RBD-based analysis of a series pipelines structure [3], which involves multiple exponential random variables. However, this is the only work that is available related to the theorem proving based analysis of RBD and in order to broaden the scope of this approach more RBD configurations, such as series, series-parallel and parallel-series need to be formalized.

DISCUSSION

The comparison of all the existing RBD based reliability analysis techniques is given in Table 1. These techniques are evaluated according to their expressiveness, scalability, accuracy, availability of all RBD configurations and the possibility of the automation of the analysis. Petri Nets are not expressive enough to model and verify all sorts of reliability properties due to their state-based nature. We mark paper-and-pencil based proofs, simulation and Petri nets are non-scalable because they cannot be used to analyze large systems, either due to the extensive manual effort (paper-and-pencil based proofs) or the computational limitations (simulations and Petri Nets). On the other hand, theorem proving is considered to be scalable due to the ability to verify generic; universally quantified, relationships using this method. The accuracy of the paper-and-pencil based proofs is questionable because they are prone to human errors. Simulation is inaccurate due to the involvement of pseudo random number generators and computer arithmetics along with its inherent sampling based nature. Theorem proving does not support all the RBD configurations as of now. Finally, the paper-pencil-proof methods and interactive theorem proving based analysis involve human guidance and then are not categorized as automatic. However, there is some automatic verification support (e.g. [9]) available for theorem proving, which can ease the human interaction in proofs and thus we cannot consider interactive theorem proving as a completely manual approach. These days engineering systems are extensively being used in many safety and financial critical applications, such as medicine, transportation and banking. Thus, the accuracy of their reliability analysis has become a dire need. As seen in Table 1, only Petri Nets and Theorem proving can fulfil these

requirements. However, Petri Nets have scalability and expressiveness limitations. Thus, we consider theorem proving to be a potential saviour for providing an accurate alternative for RBD based analysis of systems.

CONCLUSIONS

This paper provides a survey of the RBD based reliability analysis techniques while highlighting their strengths and weaknesses. Higher-order-logic theorem proving has been identified as the most accurate and suitable technique for analyzing the reliability of safety and financial-critical systems. In this regard, it has been proposed to build upon the foundations of [3] to formalize other commonly used RBDs, such as parallel, series-parallel and parallel-series.

ACKNOWLEDGMENTS

This publication was made possible by NPRP grant # [5 - 813 - 1 134] from the Qatar National Research Fund (a member of Qatar Foundation). The statements made herein are solely the responsibility of the author[s].

REFERENCES

1. N. Abbasi, O. Hasan, and S. Tahar. An Approach for Lifetime Reliability Analysis using Theorem Proving. *Journal of Computer and System Sciences*, 80(2):323–345, 2014.
2. A. Abd-Allah. *Extending Reliability Block Diagrams to Software Architectures*. Technical Report USC-CSE-97-501, Dept. of Computer Science, Univ. Southern California, USA, 1997.
3. W. Ahmad, O.Hasan, S. Tahar, and M.S. Hamdi. Towards the Formal Reliability Analysis of Oil and Gas Pipelines. In *Conferences on Intelligent Computer Mathematics*, volume 8543 of *LNAI*, pages 30–44. Springer, 2014.
4. ASENT RBD Analysis tool. https://www.raytheoneagle.com/asent/rbd.htm, 2014.
5. R. Bilintion and R.N. Allan. *Reliability Evaluation of Engineering System*. Springer, 1992.
6. P.P. Boca, J.P. Bowen, and J.I. Siddiqi. *Formal Methods: State of the Art and New Directions*. Springer, 2009.
7. H.D. Boyd and Locurto. Reliability And Maintainability For Fire Protection Systems. In *Fire Safety Science*, pages 963–970. IAFSS, 1986.
8. C.E. Brown. *Automated Reasoning in Higher-order Logic*. College Publications, 2007.
9. W. Denman and C. MuÃśoz. Automated Real Proving in PVS via MetiTarski. In *Formal Methods*, volume 8442 of *LNCS*, pages 194–199. Springer, 2014.
10. O. Hasan and S. Tahar. Formalization of the Continuous Probability Distributions. In *Automated Deduction*, volume 4603 of *LNAI*, pages 3–18. Springer, 2007.
11. O. Hasan, S. Tahar, and N. Abbasi. Formal Reliability Analysis using Theorem Proving. *IEEE Transactions on Computers*, 59(5):579–592, 2010.
12. J. Holzl and A. Heller. Three Chapters of Measure Theory in Isabelle/HOL. In *Interactive Theorem Proving*, volume 6172 of *LNCS*, pages 135–151. Springer, 2011.
13. D. Huffman and F. Antelme. Availability Analysis of a Solar Power System with Graceful Degradation. In *Reliability and Maintainability Symposium*, pages 348–352. IEEE, 2009.
14. J. Hurd. *Formal Verification of Probabilistic Algorithms*. PhD Thesis, University of Cambridge, UK, 2002.
15. K. Kolowrocki. Reliability and Risk Analysis Of Multi-State Systems With Degrading Components. *Electronic Journal of International Group On Reliability*, 2(1):86–104, 2009.
16. C. Lin, H. Teng, C. Yang, H. Weng, M. Chung, and C. Chung. A Mesh Network Reliability Analysis using Reliability Block Diagram. In *Industrial Informatics (INDIN)*, pages 975–979. IEEE, 2010.
17. T. Mhamdi, O. Hasan, and S. Tahar. On the Formalization of the Lebesgue Integration Theory in HOL. In *Interactive Theorem Proving*, volume 6172 of *LNCS*, pages 387–402. Springer, 2011.
18. ReliaSoft. http://www.reliasoft.com/, 2014.
19. R. Robidoux, H. Xu, L. Xing, and M. Zhou. Automated Modeling of Dynamic Reliability Block Diagrams Using Colored Petri Nets. *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, 40(2):337–351, 2010.
20. B. Silva, P. Maciel, E. Tavares, and A. Zimmermann. Dependability Models for Designing Disaster Tolerant Cloud Computing Systems. In *IEEE/IFIP International Conference on Dependable Systems and Networks*, pages 1–6. IEEE, 2013.
21. J. Soszynska. Reliability and Risk Evaluation of a Port Oil Pipeline Transportation System in Variable Operation conditions. *International Journal of Pressure Vessels and Piping*, 87(2-3):81–87, 2010.
22. B. Wei, C. Lin, and X. Kong. Dependability Modeling and Analysis for the Virtual Data Center of Cloud Computing. In *High Performance Computing and Communications (HPCC)*, pages 784–789. IEEE, 2011.
23. Z. Zhang and B. Shao. Reliability Evaluation of Different Pipe Section in Different Period. In *Service Operations and Logistics, and Informatics*, pages 1779–1782. IEEE, 2008.