Formal Dependability Modeling and Analysis: A Survey

Waqar Ahmed[1], Osman Hasan[1], and Sofiène Tahar[2]

[1] School of Electrical Engineering and Computer Science
National University of Sciences and Technology, Islamabad, Pakistan
{waqar.ahmad,osman.hasan}@seecs.nust.edu.pk
[2] Electrical and Computer Engineering Department
Concordia University, Montreal, Canada
tahar@ece.concordia.ca

Abstract. Dependability is an umbrella concept that subsumes many key properties about a system, including reliability, maintainability, safety, availability, confidentiality, and integrity. Various dependability modeling techniques have been developed to effectively capture the failure characteristics of systems over time. Traditionally, dependability models are analyzed using paper-and-pencil proof methods and computer based simulation tools but their results cannot be trusted due to their inherent inaccuracy limitations. The recent developments in probabilistic analysis support using formal methods have enabled the possibility of accurate and rigorous dependability analysis. Thus, the usage of formal methods for dependability analysis is widely advocated for safety-critical domains, such as transportation, aerospace and health. Given the complementary strengths of mainstream formal methods, like theorem proving and model checking, and the variety of dependability models judging the most suitable formal technique for a given dependability model is not a straightforward task. In this paper, we present a comprehensive review of existing formal dependability analysis techniques along with their pros and cons for handling a particular dependability model.

Keywords: Reliability Block Diagrams, Fault Tree, Markov Chain, Petri Nets, Model Checking, Higher-order Logic, Theorem Proving.

1 Introduction

The rapid advancement in technology in the past few decades has enabled us to develop many sophisticated systems that range from ubiquitous hand-held devices (like cell phones and tablets) to high-end computing equipment used in aircrafts, power systems, nuclear plants and healthcare devices. Ensuring the reliable functioning of these sophisticated systems is a major concern for design engineers. This concern is greatly amplified for safety-critical systems where a slight malfunction in the system may endanger human lives or lead to heavy financial set-backs. In order to avoid such scenarios beforehand, several dependability modeling techniques have been developed that can effectively model the failure characteristics of a system and thus analyze its failure behavior.

Dependability is primarily defined as the ability of a system to perform its desired function or tasks faultlessly in a certain environment on a time period [1]. Dependability is an umbrella concept which is evolved from *reliability* and *availability* considerations [1]. Many authors describe dependability of a system as a set attributes, such as reliability, maintainability, safety, availability, confidentiality, and integrity [2]. Some of these attributes, i.e. reliability and availability, are quantitative whereas some are qualitative, for instance, safety [1].

Reliability is defined as the probability of a system or a sub-component functioning correctly under certain conditions over a specified interval of time [1]. Availability is a closely related concept to reliability and it can be defined as the probability that a component will be available when demanded [1]. To understand the difference between reliability and availability, it is important to realize that reliability refers to failure-free operation during an interval, while availability refers to failure-free operation at a given instant of time [1]. Availability can be viewed as a special case of reliability and is thus commonly considered as an attribute of reliability [3]. The availability of a system is typically measured as a function of reliability and *maintainability*, which is defined as the the probability of performing a successful repair action of a system under a given time and stated conditions [1]. Additionally, if we keep the maintainability measure constant, the availability of the system is directly proportional to the reliability of the system [4]. This paper mainly focuses on reliability and availability attributes of dependability, since maintainability can be considered as a part of availability.

The first step in conducting the dependability analysis is the calculation of basic metrics of reliability and availability, such as mean-time to failure (MTTF) [1], mean-time between failure (MTBF) [1] and mean-time to repair (MTTR) [1], at the individual *component level* of the given system. The next step is the selection of an appropriate dependability modeling technique. Some of the widely used dependability modeling techniques include Reliability Block Diagrams (RBD) [5], Fault Trees (FT) [6] and Markov chains (MC) [7]. The selection among these modeling techniques depends upon numerous factors, which include the level of available details, size and complexity of the given communication network system. These modeling techniques allow us to estimate the reliability and availability of the system at the *system level* and play a particularly useful role at the design stage of a system for scrutinizing the design alternatives without building the actual system. Once the modeling technique is selected, the third and the last step is the choice of the appropriate *system level* reliability and availability analysis technique. The dependability models, formed using these techniques, are analyzed using paper-and-pencil based analytical methods or simulation. However, these analysis methods cannot ascertain absolute correctness of the analysis mainly because of the human error and manual manipulations involved in the former and the sampling based deduction and the usage of pseudo random numbers and computer arithmetic in the later. Formal methods, on the other hand, use mathematical logic to precisely model the system's intended behavior and deploy mathematical reasoning to construct an

irrefutable proof that the given system satisfies its requirements. This kind of mathematical modeling and analysis makes formal methods an accurate and rigorous analysis method compared to the traditional analytical and simulation based analysis. Thus, they are being strongly advocated for being used for the dependability analysis of safety-critical systems.

The purpose of this survey paper is to provide a generic overview of the formal methods that are being utilized for dependability analysis. These formal methods primarily include: (i) Petri Nets (ii) Model Checking and (iii) Higher-order Logic theorem proving as they have all been used for the dependability analysis using the three dependability modeling techniques: RBD, FT, and MC. The main focus of the paper is to study the utilization of formal methods in conjunction with the dependability modeling techniques for real-world applications and thus gain insights about the strengths and weaknesses of these formal methods and how to use them in the most effective manner. It is important to note that the paper is unique compared to existing surveys and tutorials on dependability analysis [8–10, 3] due to its exclusive focus on dependability modeling techniques and their analysis with formal methods. For instnace, in [8] a unified framework for reliability with Markov reward models is described and then a survey of existing reliability analysis software tools is presented. Similarly, a survey of work related to dependability modeling and analysis of software and systems specified with UML is presented in [9]. In [10] and [3], tools and methods that have been used for enhancing the dependability of Wireless Sensor networks (WSN) and communication networks are also surveyed, respectively. Unlike above work, this paper discusses about the pros and cons of modeling techniques and formal methods for the dependability analysis of a broad range of systems.

The organization of the paper is as follows: Section 2 briefly describes commonly used dependability modeling techniques. Section 3 presents a detailed survey of formal methods that have been used for conducting accurate and rigorous dependability analysis of real-world systems. Section 4 provides the insights and the common pitfalls of the dependability modeling techniques and also a comparison of formal methods with traditional dependability analysis techniques. Finally, Section 5 concludes the paper.

2 Dependability Modeling Techniques

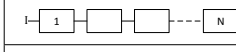
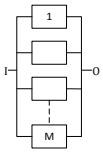
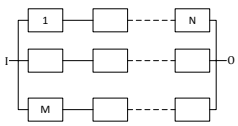
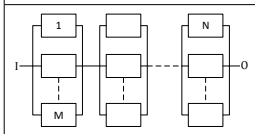
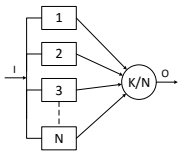
Dependability assessment techniques can be utilized in every design phase of the system or component including development, operation and maintenance. FT and RBD based models are usually used to provide reliability and availability estimates for both *early* and *later* stages of the design, where the system models are more refined and have more detailed specifications compared to the early stage system models [1]. While on the other hand, MC based models are mainly used in the *later* design phase to perform trade-off analysis among different design alternatives when the detailed specification of the design becomes available. In addition, when the system is deployed, these modeling techniques can be beneficial in order to estimate the frequency of maintenance and part replacement in the design, which allows us to determine the life cost of the system elements or components. In this section, we present a brief detail about some commonly

used dependability modeling techniques to facilitate the understanding of the next sections.

2.1 Reliability Block Diagrams

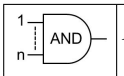
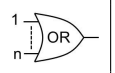
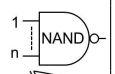
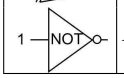
Reliability Block Diagrams (RBD) [11] are graphical structures consisting of blocks and connector lines. The blocks usually represent the system components and the connection of these components is described by the connector lines. The system is functional, if at least one path of properly functional components from input to output exists otherwise it fails.

Table 1: RBDs with their Mathematical Expressions

RBDs	Mathematical Expressions
	$R_{series}(t) = Pr(\bigcap_{i=1}^{N} A_i(t)) = \prod_{i=1}^{N} R_i(t)$
	$R_{parallel}(t) = Pr(\bigcup_{i=1}^{M} A_i) = 1 - \prod_{i=1}^{M}(1 - R_i(t))$
	$R_{parallel-series}(t) = Pr(\bigcup_{i=1}^{M}\bigcap_{j=1}^{N} A_{ij}(t)) = 1 - \prod_{i=1}^{M}(1 - \prod_{j=1}^{N}(R_{ij}(t)))$
	$R_{series-parallel}(t) = Pr(\bigcap_{i=1}^{N}\bigcup_{j=1}^{M} A_{ij}(t)) = \prod_{i=1}^{N}(1 - \prod_{j=1}^{M}(1 - R_{ij}(t)))$
	$R_{k\|n}(t) = Pr(\bigcup_{i=k}^{n}\{\textit{exactly } i \textit{ components functioning}\}) = \Sigma_{i=k}^{n}(\binom{n}{k} R^i(1-R)^{n-1})$

An RBD construction can follow any one of three basic patterns of component connections: (i) series (ii) active redundancy or (iii) standby redundancy. In the *series* connection, shown in Table 1, all components should be functional for the system to remain functional. The corresponding reliability expression is also shown in Table 1, where A_i represents the event corresponding to i^{th} component. In an *active* redundancy, all components in at least one of the redundant stages must be functioning in fully operational mode. The components in an active redundancy might be connected in a parallel structure or a combination of series and parallel structures as shown in Table 1. In a *standby* redundancy, all components are not required to be active. In other words, at least k out of n are required by the system to be functional, which can be seen in Table 1. There are three main requirements for building the RBD of a given system, i.e., the information about the (i) functional interaction of the system components; (ii)

Table 2: Probability of Failure of Fault Tree Gates

FT Gates	Failure Probability Expressions
	$F(t) = Pr(\bigcap_{i=2}^{N} A_i(t)) = \prod_{i=2}^{N} F_i(t)$
	$F(t) = Pr(\bigcup_{i=2}^{N} A_i(t)) = 1 - \prod_{i=2}^{N}(1 - F_i(t))$
	$F(t) = 1 - F_{OR}(t) = \prod_{i=2}^{N}(1 - F_i(t))$
	$F(t) = Pr(\bigcap_{i=2}^{k} \overline{A}_i(t) \cap \bigcap_{j=k}^{N} A_i(t)) = \prod_{i=2}^{k}(1 - F_i(t)) * \prod_{j=k}^{N}(F_j(t))$
	$F(t) = Pr(\bar{A}(t)B(t) \cup A(t)\bar{B}(t)) = F_A(t)(1 - F_B(t)) + F_B(t)(1 - F_A(t))$
	$F(t) = Pr(A(t)) = (1 - F_A(t))$

reliability of each component usually expressed in terms of failure distributions, such as exponential or Weibull, having appropriate failure rates; and (iii) mission times at which the reliability is desired. This information is then utilized by the design engineers to identify the appropriate RBD configuration (series, parallel or series-parallel) in order to determine the overall reliability of the given system. The detail about these commonly used RBD configurations and their corresponding mathematical expressions are presented in Table 1.

2.2 Fault Trees

Fault Tree (FT) [6] is a graphical technique for analyzing the conditions and the factors causing an undesired *top event*, i.e., a critical event, which can cause the whole system failure upon its occurrence. These causes of system failure are represented in the form of a tree rooted by the *top event*. The preceding nodes of the fault tree are represented by *gates*, which are used to link two or more *cause events* causing one fault in a prescribed manner. For example, an OR FT gate can be used when one fault suffices to enforce the fault. On the other hand, the AND FT gate is used when all the cause events are essential for enforcing the fault. Besides these gates, there are some other gates, such as exclusive OR FT gate, priority FT gate and inhibit FT gate, which can be used to model the occurrence of faults due to the corresponding cause events [6].

Once the fault tree model is constructed, both qualitative and quantitative analysis can be carried out. A qualitative analysis in this context allows the identification of all combinations of basic failure events, known as cut sets, which can cause the top event to occur. The *minimal* cut sets (MCS) are those cut sets that do not contain any subset of the basic cause events that are still a *cut set* and are obtained by applying Boolean algebraic operations on these cut sets. The smaller the number of basic cause events in these cut set, the more resilient to failures is the considered modeled system . The quantitative analysis is used

to evaluate the probability of occurrence of the top event by considering these minimal cut sets, which significantly contribute to the system failures.

In Fault Tree analysis (FTA), each FT gate has an associated failure probability expression as shown in Table 2. These expressions can be utilized to evaluate the reliability of the system. The first step in the FTA is the construction of the FT of the given system. This is followed by the assignment of the failure distributions to basic *cause-events* and the identification of the Minimal Cut Set (MCS) failure events, which contribute in the occurrence of the top event. These MCS failure events are generally modeled in terms of the *exponential* or *Weibull* random variables and the Probabilistic Inclusion-Exclusion (PIE) principle [11] is then used to evaluate the probability of failure of the given system.

2.3 Markov Chain

A MC [12] is a stochastic process that consists of a set of states, i.e., $S = \{s_0, s_1, ..., s_n\}$, and arcs, which are used to point the transition from one state to another. The initial state s_{ini} and the probability p_{ij} represent the starting state and the transition probability from state s_i to state s_j, respectively. The process starts from an initial state and transitions from the current state to the next state occur on the basis of transition probabilities, which only depend upon the current state based on the Markov or the memoryless property. Markov chains are usually classified into two categories: Discrete Time Markov Chains (DTMC) and Continuous Time Markov Chains (CTMC). Markovian models are frequently utilized for reliability analysis in scenarios where failure or repair events can occur at any point in time [12].

Markov modeling has also been utilized for analyzing the *dynamic* behavior of the other reliability models, i.e., RBD and FT. The notion of dynamic behavior, for reliability analysis, represents the evolution of system topology/configuration with respect to time. In the case of Dynamic Reliability Block Diagrams (DRBD) [13], the system is modeled in terms of *states* of the components and the evolution of these components states is carried out by a sequence of *events* [13]. A typical DRBD contains the following states: (i) *Active*: the state of proper functioning of the component; (ii) *Failed*: the failure state of the component; and (iii) *Standby*: the state depicting the case when the component is not in functional or in active condition but it can be activated. In addition, there are other states such as *Hot*, *Warm* and *Cold*, representing the conditions when the system or component is disabled but energized, partially and completely disabled, respectively [13].

3 Formal Dependability Analysis Techniques

3.1 Petri Nets

A Petri Net (PN) [14] is a bipartite directed graph consisting of disjoint sets of places P and transitions T. The former, which is represented by circles, models the condition while the latter, signified by bars, represents the events or activities that may occur in the system. The directed arcs $(P \times T)$ and $(T \times P)$, represented by arrows, describe the input places P for the transitions T and output places P for the transitions T, respectively. Places may be empty or contain more than

one token that is drawn by a block dot and term *marking* represents the tokens over the set of places. A transition is said to be enabled, in a given marking, if all its input places contain at least one token. An enabled transition can be $fired$ and as a result a token will be removed from the input places of the transition and added to its output places.

Petri Nets and its variants are widely used as a reliability analysis tool for many real-world systems due to their ability to efficiently handle large problems of dynamic nature. For instance, PNs have been used for the reliability assessment of Web services [15] and a wind turbine hydraulic variable pitch system [16]. Many existing work have utilized the PNs for *availability* analysis, for instance, the availability of a mechanical system is hierarchically analyzed by dividing the complete system into three levels [17]. A system level PN model is constructed by composing the PNs of the subsystem levels, which are also composed from the PNs of the component level. Similarly, PNs have been used to analyze the availability of computational servers that are processing the jobs in a queue [18], a replicated file system to reduce the overhead in a distributed environment [19], a subsea blowout preventer (BOP), which is essentially required to provide safety for drilling workers, rigs and natural environment [20] and the C160 series equipment that can modify its own modules based on different process plan and forms a new configuration [21]. In addition, a considerable amount of work has been done by utilizing PN in conjunction with the dependability modeling techniques, described in Section 2, for dependability analysis as follows:

Reliability Block Diagrams Many PN variants are extensively utilized to represent the RBDs to model the reliability of communication systems with dynamic nature. For instance, the live migration process in cloud computing networks makes the system dynamic and thus yields to a complex RBD model, which can be effectively handled using Petri Nets with the support of commercial tools, such as *SNOOPY* [22] and *CPN* [23]. Given the dynamic nature of visualization, due to the presence of hardware systems, software systems, live migration techniques, resource allocation algorithms and concurrent failures, virtualized networks are frequently modeled with RBDs, which are then transformed to Petri Nets for the reliability analysis [24]. The reliability of communication networks with *redundancy mechanisms* has also been efficiently analysed using RBD based Petri Nets [25].

PNs have also been used to ensure the security/safety aspects of networks in terms of reliability and availability by analyzing the safety/security aspects of network protocols, such as internet voting systems [26] and high-speed trains [27]. In addition to the communication network, PNs have been used to develop the RBDs to analyze the reliability of a logistic supply chain [28] and redundant electrical generator used to power-up the coast guard vessel [29]. Similarly, a Cojoint system model consisting of CPN and RBD has been effectively used to analyze the dependability and logistics of a fault-redundant space station [30].

Fault Trees The PN approach has also been utilized, in conjunction with FTs, for the reliability analysis of embedded systems by translating the PN reachability into provability of linear logic sequents, which empowers the analysis by

utilizing sequent calculus [31]. The *dynamic behavior* of networks components, such as timed behavioral nature, cannot be captured by simple FT models but PNs provide a very feasible alternative for this purpose. The system under consideration is modeled with a FT, which is then transformed into its corresponding PN based model for analysis. For example, the reliability of the broadband integrated service network (B-ISDN) has been assessed by modeling the dynamic re-routing mechanism of the traffic using the FT-based PN approach [32].

Markov Chains A considerable amount of work has been done on analyzing reliability of systems using PNs with Markov chains. Some other prominent work in this direction include the reliability analysis of a preemptive M/D/1/2/2 client-server queuing system [33], the dynamic reconfiguration of FPGA [34], the data communication systems of the WLAN based train control system [35], cellular networks [36] and Wireless Sensor Networks (WSN) [37]. Moreover, some network protocols, like the courier [38] and Fibre Distributed Data Interface (FDDI) token ring protocol [39], have also been analyzed using the Petri Net approach. Similarly, the reliability of a file server system [40], financial system [41], distributed memories [42] and Low Earth Orbit (LEO) satellite has also been analyzed using PNs based on Markov chains [43]. Moreover, a Markov regenerative PN has been introduced in [44] to extend the capability of stochastic PN analysis and then its effectiveness is illustrated by utilizing this approach to approximate client-server systems.

3.2 Model Checking

Model Checking [45] allows to describe the behavior of a given system in the form of a state machine and verify its temporal properties in a rigorous manner. Probabilistic model checking extends traditional model checking principles for the analysis of MCs and allows the verification of probabilistic properties. Some notable probabilistic model checking include *PRISM* [46] and *ETMCC* [47].

Probabilistic model checking techniques have been considerably adopted to verify the reliability and availability properties of many systems, for instance, the *PRISM* has been used to assess the reliability of e-health systems used in hospitals based on the Fast Health Interoperable Resources (FHIR) standard [48] and the Device Interoperability Middleware (DIM) used to bridge the gap between different healthcare vendors [49]. In addition, the *PRISM* model checker has been utilized for the reliability/safety analysis of airbone applications by augmenting it to the Matlab simulink [50], a RAID disk protocol used for reading the data from the disk sectors [51], multi-processor systems based on the Triple modular redundancy (TMR) model [52]. *PRISM* has also been utilized for quantitative reliability and availability analysis of a satellite system [53].

Fault Trees The *COMPASS* tool [54] supports the formal FT analysis, specifically for aerospace systems. For verification purposes, *COMPASS* provides support of several model checking tools, like *NuSMV* [55] and *MRMC* [56]. This tool provide various templates containing placeholders that have to be filled in by the user. These templates are primarily composed of the most frequently used patterns that allow easy specifications of properties by non-experts by hiding the

details of the underlying temporal logic. The tool generates several outputs, such as traces, FTs and Failure Mode and Effect Analysis (FMEA) tables, along with diagnostic and performance measures.

Markov Chains Probabilistic model checking extends traditional model checking principles for the analysis of MCs and allows the verification of probabilistic properties. Probabilistic model checking techniques have been considerably adopted to verify the reliability properties of many systems, such as NAND multiplexing [57], an airbag system, an industrial process control system and the Herschel-Planck satellite system [58]. In [59], the reliability analysis of the Fast And Secure Protocol (FASP) is carried out by first defining the successful data transmission using STL and then the communication network is modeled in the form of a sender, receiver and a communication channel module in *PRISM*. Finally, the reliability property is then verified against the communication network using the *PRISM* model checker.

3.3 Higher-order-Logic Theorem Proving

Interactive theorem provers, like *HOL4*, *Isabelle/HOL* and *Coq*, can be used to reason about probabilistic behaviors using the higher-order-logic formalizations of probability theory [60–62]. This feature has been widely used to conduct the dependability analysis of many systems. For instance, the probability theory in *HOL4* [61] has been used for the reliabililty analysis of combinational circuits [63] and reconfigurable memory arrays [64]. In these work, however, the reliability is evaluated based on probabilistic principles directly, i.e., no component to system-level assessment based on RBD or FT methods is done. Similarly, formally verified statistical properties of the continuous random variables have been used to reason about the fundamental reliability properties, including survival function and hazard rate [65]. These reliability properties are then used to analyzed the reliability of electronic system components [65].

Reliability Block Diagrams The higher-order logic theorem prover *HOL4* has been recently used for the formalization of RBDs, including series [66], parallel [67], parallel-series [67] and series-parallel [68]. These formalizations have been used for the reliability analysis of a simple oil and gas pipeline with serial components [66], WSN protocols [67] and logistic supply chains [67].

Fault Trees A higher-order-logic formalization of generic Fault Tree gates, i.e., AND, OR, NAND, NOR, XOR and NOT and the formal verification of their failure probability expressions have also been recently proposed in *HOL4* [69]. In addition, this work also presents a formalization of probabilistic inclusion-exclusion principle, which is then used to conduct the FT-based failure analysis of a solar array used in a Dong Fang Hong-3 (DFH-3) satellite [69].

Markov Chains A foundational formalization of time-homogeneous DTMC with finite state space has been presented in HOL4 [70] and *Isabelle/HOL* [71]. These formalizations have been successfully used to formally analyze a binary communication channel [70], ZeroConf [71] and anonymizing crowds protocols

[71]. None of these Markov chain formalizations has been used for reliability analysis so far.

4 Comparison and Discussion

4.1 Comparison of Dependability Modeling Techniques

The criteria for the selection of these modeling techniques, for a certain system, mainly depends upon the type of system and problem domain. A comparison among these modeling techniques is shown in Table 3. For instance, RBD is primarily used if we are interested in the successful working of the system while FT models the failure relationship due to the failure of individual components of the system. Also, both of these techniques utilize top-down analysis approach that starts at the system level and then proceeds downward to link system performance to failures at the component level. Due to this reason, these techniques work only for combinatorial types of problems, where a combination of components faults is used to determine the overall system failure. On the other hand, Markov chains are more flexible in terms of handling a wide variety of problems, as given in Table 3, including non-combinatorial problems, where systems are in different operational modes, such as active or failed. However, Markov chains fail to cater for large and complex systems due to the exponential growth in the number of states.

Table 3: Comparison of Dependability Modeling Techniques

Features	Reliability Block Diagram	Fault Tree	Markov Chain
Success Domain	✓		✓
Failure Domain		✓	✓
Top-Down Approach	✓	✓	✓
Identification and Prevention of Faults	✓	✓	✓
Combinatorial Problems	✓	✓	✓
Non-combinatorial Problems			✓
Large and Complex Systems	✓	✓	

Based on the survey conducted in Section 3, we have found that FTs have been the mostly utilized dependability modeling technique by formal methods. On the other hand, the utilization of RBD and MC models for the dependability analysis is rapidly increasing specifically by PNs. The usage of RBD models with model checking for the formal dependability analysis is an area that is almost unexplored. We believe that this combination of modeling and analysis technique has a huge potential for ensuring accurate reliability analysis of a wide variety of safety-critical system.

4.2 Comparison of Dependability Analysis Techniques

A summary of various dependability analysis techniques is presented in Table 4. These techniques are evaluated according to their expressiveness, accuracy and the possibility of automating the analysis. Model checking and Petri Nets

are not expressive enough to model and verify all sorts of reliability properties due to their state-based nature. 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 reliability analysis foundations as of now. Finally, the paper-and-pencil based proof methods and interactive theorem proving based analysis involve human guidance and therefore are not categorized as automatic. However, there is some automatic verification support (e.g. [72]) 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. All three formal methods techniques promise to provide accurate results and thus can be very useful for analyzing the dependability aspects of safety and financial-critical systems.

Table 4: Comparison of Reliability Analysis Techniques

Feature	Paper-and-pencil Proof	Simulation Tools	Petri Nets	Theorem Proving	Model Checking
Expressiveness	✓	✓		✓	
Accuracy	✓ (?)		✓	✓	✓
Automation		✓	✓		✓

We have used the question mark symbol in accuracy feature for paper-and-pencil to highlight its limitation of being prone to human error.

5 Conclusions

In this paper, we have discussed various dependability models constructed using the building blocks offered by the formalisms of reliability block diagrams, fault trees and Markov chains models. We have also presented a critical comparison, of the various dependability analysis techniques, i.e., analytical methods, simulation, and formal methods. Apart from providing the necessary background, we have also provided a detailed survey of the application of formal methods available in the open literature focused on studying dependability analysis of various real-world systems. The main contribution of this paper is that it is the first work presenting a comprehensive review of the various dependability modeling techniques in conjunction with formal methods along with a critical analysis describing their pros and cons in various contexts. Existing surveys on dependability analysis are either focused on software or communications networks and do not cover formal methods in depth.

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. Avizienis, A., Laprie, J.C., Randell, B.: Fundamental Concepts of Dependability. Technical Report CS-TR-739, Newcastle University, UK (2001) `http://pld.ttu.ee/IAF0530/16/avi1.pdf`.
2. Spitzer, C.R., Spitzer, C.: Digital Avionics Handbook. CRC Press (2000)
3. Al-Kuwaiti, M., Kyriakopoulos, N., Hussein, S.: A Comparative Analysis of Network Dependability, Fault-tolerance, Reliability, Security, and Survivability. Communications Surveys & Tutorials **11**(2) (2009) 106–124
4. Weibull: http://www.weibull.com/hotwire/issue26/relbasics26.htm (2015)
5. Čepin, M.: Reliability Block Diagram. In: Assessment of Power System Reliability. Springer (2011) 119–123
6. Vesely, W.E., Goldberg, F.F., Roberts, N.H., Haasl, D.F.: Fault tree handbook (NUREG-0492). Technical report, U.S. Nuclear Regulatory Commission (1981)
7. Gilks, W.R.: Markov chain Monte Carlo. Wiley Online Library (2005)
8. Trivedi, K.S., Malhotra, M.: Reliability and performability techniques and tools: A survey. In: Messung, Modellierung und Bewertung von Rechen-und Kommunikationssystemen. Springer (1993) 27–48
9. Bernardi, S., Merseguer, J., Petriu, D.C.: Dependability Modeling and Analysis of Software Systems Specified with UML. ACM Computing Surveys **45**(1) (2012) 1–48
10. Venkatesan, L., Shanmugavel, S., Subramaniam, C., et al.: A Survey on Modeling and Enhancing Reliability of Wireless Sensor Network. Wireless Sensor Network **5**(03) (2013) 41–51
11. Trivedi, K.S.: Probability & Statistics with Reliability, Queuing and Computer Science Applications. John Wiley & Sons (2008)
12. Fugua, N.: The Applicability of Markov Analysis Methods to Reliability, Maintainability, and Safety. Reliability Analysis Center START Sheet **10**(2) (2003) 1–8
13. Distefano, S., Xing, L.: A New Approach to Modeling the System Reliability: Dynamic Reliability Block Diagrams. In: Reliability and Maintainability Symposium, IEEE (2006) 189–195
14. Peterson, J.L.: Petri Net Theory and the Modeling of Systems. Prentice Hall (1981)
15. Zhong, D., Qi, Z.: A Petri Net based approach for Reliability Prediction of Web Services. In: On the Move to Meaningful Internet Systems. Volume 4277 of LNCS. (2006) 116–125
16. Yang, X., Li, J., Liu, W., Guo, P.: Petri Net Model and Reliability Evaluation for Wind Turbine Hydraulic Variable Pitch Systems. Energies **4**(6) (2011) 978–997
17. Kumar, G., Jain, V., Gandhi, O.: Reliability and Availability Analysis of Mechanical Systems using Stochastic Petri Net Modeling based on Decomposition Approach. International Journal of Reliability, Quality and Safety Engineering **19**(01) (2012) 1–39
18. Jian, S., Shaoping, W., Yaoxing, S.: Petri-nets based Availability Model of Fault-tolerant Server System. In: Robotics, Automation and Mechatronics, IEEE (2008) 444–449
19. Dugan, J.B., Ciardo, G.: Stochastic Petri Net Analysis of a Replicated File System. Software Engineering **15**(4) (1989) 394–401
20. Zengkai, L., Yonghong, L., Ju, L.: Availability and Reliability Analysis of Subsea Annular Blowout Preventer. In: International Conference on Energy. Volume 25., Science & Engineering Research Support Society (2013) 73–76

21. Beirong, Z., Xiaowen, X., Wei, X.: Availability Modeling and Analysis of Equipment based on Generalized Stochastic Petri Nets. Research Journal of Applied Sciences, Engineering and Technology **4**(21) (2012) 4362–4366
22. Heiner, M., Herajy, M., Liu, F., Rohr, C., Schwarick, M.: SNOOPY - A Unifying Petri Net Tool. In: Application and Theory of Petri Nets. Volume 7347 of LNCS. Springer (2012) 398–407
23. Beaudouin-Lafon, M., et al.: CPN/Tools: A Tool for Editing and Simulating Coloured Petri Nets. In: Tools and Algorithms for the Construction and Analysis of Systems. Volume 2031 of LNCS. Springer (2001) 574–577
24. Wei, B., Lin, C., Kong, X.: Dependability Modeling and Analysis for the Virtual Data Center of Cloud Computing. In: High Performance Computing and Communications, IEEE (2011) 784–789
25. Guimarães, A., Maciel, P., Matos Jr, R., Camboim, K.: Dependability Analysis in Redundant Communication Networks using Reliability Importance. In: Information and Network Technology. Volume 4., IACSIT Press (2011) 12–17
26. Omidi, A., Moradi, S.: Modeling and Quantitative Evaluation of an Internet Voting System based on Dependable Web Services. In: Computer and Communication Engineering, IEEE (2012) 825–829
27. Lijie, C., Tao, T., Xianqiong, Z., Schnieder, E.: Verification of the safety communication protocol in train control system using colored Petri net. Reliability Engineering & System Safety **100** (2012) 8–18
28. Li, Y.z., Yi, H.y.: Calculation Method on Reliability of Logistics Service Supply Chain Based on Stochastic Petri Nets. International Journal of u-and e-Service, Science and Technology **7**(1) (2014) 103–112
29. Robidoux, R., Xu, H., Xing, L., Zhou, M.: Automated Modeling of Dynamic Reliability Block Diagrams using Colored Petri Nets. Systems, Man and Cybernetics, Part A: Systems and Humans **40**(2) (2010) 337–351
30. Nebel, S., Bertsche, B.: Modeling and Simulation Methodology of the Operational Availability and Logistics using Extended Colored Stochastic Petri Netsan Astronautics Case Study. In: Reliability and Maintainability Symposium, IEEE (2008) 434–439
31. Sadou, N., Demmou, H.: Reliability Analysis of Discrete Event Dynamic Systems with Petri Nets. Reliability Engineering & System Safety **94**(11) (2009) 1848–1861
32. Balakrishnan, M., Trivedi, K.S.: Stochastic Petri Nets for the Reliability Analysis of Communication Network Applications with Alternate-routing. Reliability Engineering & System Safety **52**(3) (1996) 243–259
33. Radev, D., Rashkova, E., Denchev, V.: Analysis of Markov Reward Models with Stochastic Petri Nets. In: International Conference on Computer Systems and Technologies, ACM (2008) 1–6
34. Kohlík, M.: Dependability Models based on Petri Nets and Markov Chains (2009)
35. Zhu, L., Yu, F.R., Ning, B., Tang, T.: Service Availability Analysis in Communication-based Train Control systems using WLANs. In: Communications, IEEE (2012) 1383–1387
36. Jindal, V., Dharmaraja, S., Trivedi, K.S.: Markov Modeling Approach for Survivability Analysis of Cellular Networks. International Journal of Performability Engineering **7**(5) (2011) 429
37. Schoenen, R., Yanikomeroglu, H.: Erlang Analysis of Cellular Networks using Stochastic Petri Nets and User-in-the-loop Extension for Demand Control. In: Global Communication Conference, IEEE (2013) 298–303

38. Youness, O., Elkilani, W., El-Wahed, W.A., Torkey, F.: A Robust Methodology for Performance Evaluation of Communication Networks Protocols. In: Communication Networks and Services Research Conference, IEEE (2006) 1–10
39. Christodoulou, S., Zhou, M.: A Petri Net Approach to Modeling and Performance Analysis of Fiber Data Distributed Interface (FDDI) Network. In: Emerging Technologies and Factory Automation, IEEE (1994) 373–380
40. Ibe, O.C., Choi, H., Trivedi, K.S.: Performance Evaluation of Client-server Systems. Parallel and Distributed Systems **4**(11) (1993) 1217–1229
41. Tunik, A., Kharlashkin, I.: A Formalistic Method for the Performance Evaluation of Communication Networks of Distributed Computing Systems. In: Industrial Electronics. Volume 2., IEEE (1992) 874–878
42. Sun, X., Lin, C., Liu, W., Xiao, Y.: Survivability Evaluation of Distributed Service using Stochastic Petri Net. In: Communications and Networking in China, IEEE (2009) 1–5
43. Zeng, W., Hong, Z.G.: SPN-based Performance Analysis of LEO Satellite Networks with Multiple Users. In: Machine Learning and Cybernetics. Volume 3., IEEE (2011) 1425–1429
44. Choi, H., Kulkarni, V.G., Trivedi, K.S.: Markov Regenerative Stochastic Petri Nets. Performance Evaluation **20**(1) (1994) 337–357
45. Baier, C., Katoen, J.P.: Principles of Model Checking. MIT Press (2008)
46. Lin, C.M., Yang, C.W., Teng, H.K., Chung, M.C., Lang, K.C., Teng, H.F.: Modeling CAN Network using PRISM. In: Industrial Informatics, IEEE (2010) 390–394
47. Hermanns, H., Katoen, J.P., Meyer-Kayser, J., Siegle, M.: ETMCC: Model Checking Performability Properties of Markov Chains. In: Dependable Systems and Networking, IEEE (2003) 1
48. Pervez, U., Hasan, O., Latif, K., Tahar, S., Gawanmeh, A., Hamdi, M.S.: Formal Reliability Analysis of a Typical FHIR Standard based e-Health System using PRISM. In: e-Health Networking, Applications and Services, IEEE (2014) 43–48
49. Pervez, U., Mahmood, A., Hasan, O., Latif, K., Gawanmeh, A.: Formal Reliability analysis of Device Interoperability Middleware (DIM) based E-health system using PRISM. In: e-Health Networking, Applications and Services. (2015) 1–6
50. Gomes, A., Mota, A., Sampaio, A., Ferri, F., Buzzi, J.: Systematic Model-based Safety Assessment via Probabilistic Model Checking. In: Leveraging Applications of Formal Methods, Verification, and Validation. Volume 6415 of LNCS. Springer (2010) 625–639
51. Gopinath, K., Elerath, J., Long, D.: Reliability Modelling of Disk subsystems with Probabilistic Model Checking. Technical report, Technical Report UCSC-SSRC-09-05, University of California, Santa Cruz (2009) `http://www.crss.ucsc.edu/media/papers/ssrctr-09-05.pdf`.
52. Ge, X., Paige, R.F., McDermid, J.A.: Analysing System Failure Behaviours with PRISM. In: Secure Software Integration and Reliability Improvement Companion, IEEE (2010) 130–136
53. Peng, Z., Lu, Y., Miller, A., Johnson, C., Zhao, T.: A Probabilistic Model Checking Approach to Analysing Reliability, Availability, and Maintainability of a Single Satellite System. In: Modelling Symposium, IEEE (2013) 611–616
54. Bozzano, M., Cimatti, A., Katoen, J.P., Nguyen, V.Y., Noll, T., Roveri, M.: The COMPASS Approach: Correctness, Modelling and Performability of Aerospace Systems. In: Computer Safety, Reliability, and Security. Volume 5775 of LNCS. Springer (2009) 173–186

55. Cimatti, A., Clarke, E., Giunchiglia, E., Giunchiglia, F., Pistore, M., Roveri, M., Sebastiani, R., Tacchella, A.: NuSMV 2: An Opensource Tool for Symbolic Model Checking. In: Computer Aided Verification. Volume 2404 of LNCS. (2002) 359–364
56. Katoen, J.P., Khattri, M., Zapreev, I.S.: A Markov Reward Model Checker. In: Quantitative Evaluation of Systems, IEEE (2005) 243–244
57. Norman, G., Parker, D., Kwiatkowska, M., Shukla, S.: Evaluating the Reliability of NAND Multiplexing with PRISM. Computer-Aided Design of Integrated Circuits and Systems **24**(10) (2005) 1629–1637
58. Norman, G., Parker, D.: Quantitative Verification: Formal Guarantees for Timeliness, Reliability and Performance. Technical report (2014)
59. Conghua, Z., Meiling, C.: Analysis of Fast and Secure Protocol based on Continuous-time Markov Chain. Communications, China **10**(8) (2013) 137–149
60. Hurd, J.: Formal Verification of Probabilistic Algorithms. PhD Thesis, University of Cambridge, UK (2002)
61. Mhamdi, T., Hasan, O., Tahar, S.: On the Formalization of the Lebesgue Integration Theory in HOL. In: Interactive Theorem Proving. Volume 6172 of LNCS. Springer (2010) 387–402
62. Hölzl, J., Heller, A.: Three Chapters of Measure Theory in Isabelle/HOL. In: Interactive Theorem Proving. Volume 6898 of LNCS. Springer (2011) 135–151
63. Hasan, O., Patel, J., Tahar, S.: Formal Reliability Analysis of Combinational Circuits using Theorem Proving. Journal of Applied Logic **9**(1) (2011) 41–60
64. Hasan, O., Tahar, S., Abbasi, N.: Formal Reliability Analysis using Theorem Proving. Transactions on Computers **59**(5) (2010) 579–592
65. Abbasi, N., Hasan, O., Tahar, S.: Formal Lifetime Reliability Analysis using Continuous Random Variables. In: Logic, Language, Information and Computation. Volume 6188 of LNCS. Springer (2010) 84–97
66. Ahmed, W., Hasan, O., Tahar, S., Hamdi, M.S.: Towards the Formal Reliability Analysis of Oil and Gas Pipelines. In: Conferences on Intelligent Computer Mathematics. Volume 8543 of LNCS. Springer (2014) 30–44
67. Ahmed, W., Hasan, O., Tahar, S.: Formal Reliability Analysis of Wireless Sensor Network Data Transport Protocols using HOL. In: Wireless and Mobile Computing, Networking and Communications, IEEE (2015) 217–224
68. Ahmed, W., Hasan, O., Tahar, S.: Towards Formal Reliability Analysis of Logistics Service Supply Chains using Theorem Proving. In: Implementation of Logics. (2015) 111–121
69. Ahmed, W., Hasan, O.: Towards Formal Fault Tree Analysis Using Theorem Proving. In: Intelligent Computer Mathematics. Volume 9150 of LNCS. Springer (2015) 39–54
70. Liu, L., Hasan, O., Tahar, S.: Formal Reasoning About Finite-State Discrete-Time Markov Chains in HOL. Journal of Computer Science and Technology **28**(2) (2013) 217–231
71. Hölzl, J., Nipkow, T.: Interactive Verification of Markov Chains: Two Distributed Protocol Case Studies. arXiv preprint arXiv:1212.3870 (2012)
72. Slind, K., Norrish, M.: A Brief Overview of HOL4. In: Theorem Proving in Higher Order Logics. Volume 5170 of LNCS. Springer (2008) 28–32